SECRET COMMUNICATION IN PRESENCE OF COLLUDING EAVESDROPPERS

Satashu Goel and Rohit Negi
ECE Department, Carnegie Mellon University
Pittsburgh, PA 15213, USA
{satashug,negi}@ece.cmu.edu

ABSTRACT

We consider the problem of secret communications between two nodes over a wireless link in the presence of multiple passive eavesdroppers which may collude. Both the transmitter and the receiver are assumed to have multiple antennas and the multiple colluding eavesdroppers are modeled by an eavesdropper with multiple antennas. Communication is secret if the eavesdropper is unable to decode the message whereas the receiver can decode the message without making any errors. Thus, we deal with the problem of secrecy in a MIMO scenario. It is shown how the transmitter can use the multiple antennas to add artificially generated noise to the information signal such that the artificial noise only degrades the eavesdropper's channel. Thus, even if the eavesdropper has a 'better' channel than the receiver, secret communication is made possible by selectively degrading the eavesdropper's channel. The secrecy of communication is achieved by exploiting the physical characteristics of the wireless medium and it is independent of the secrecy of channel state information (CSI).

Keywords: Privacy, secrecy capacity, wireless

I. INTRODUCTION

Multiple Input Multiple Output (MIMO) communication systems have gained prominence in recent years, both as a research area, as well as for development efforts. Several results characterize the capacity of MIMO systems, showing a linear increase in capacity with the minimum of the number of transmit and receive antennas [8]. The promising result has therefore led to intense development efforts for MIMO systems. Other results have concentrated on demonstrating practical transmission and decoding methods, to achieve the promised MIMO capacity [6], [7], [9].

We consider the problem of *secret* communication in the wireless environment using MIMO systems. The broadcast nature of the wireless medium presents a unique set of security issues. In particular, it is difficult to control access to a wireless network because of the broadcast nature and hence eavesdropping becomes easy. Secrecy problems involve three nodes; transmitter, receiver and an eavesdropper. The transmitter wants to communicate with the receiver while preventing the eavesdropper from decoding the message. [5] described a technique for secret communication using channel state information (CSI) as the secret key. This was generalized for the multi-antenna scenario by [4]. An abstract characterization of secrecy capacity of the kind discussed by [5] was obtained by [3]. In contrast, our paper assumes that the CSI is publicly available, so that it cannot be used to obtain a secret key. Our approach is inspired by the result in [2], which showed that secret communication is possible if the eavesdropper's channel is worse than the receiver's channel. [2] also defined a notion of 'secrecy capacity', which essentially is the maximum rate at which the intended receiver's decoding error probability tends to zero, while the eavesdropper's error probability tends to one.

However, in general, there is no guarantee that the receiver will have better channel than the eavesdropper (e.g., consider the case where eavesdropper is closer to the transmitter than is the receiver). In [1], we showed an interesting application of multiple antennas, where this condition can be satisfied by producing 'artificial noise'. This noise is created such that it degrades the eavesdropper's channel but does not affect the channel of the intended receiver, thus allowing perfectly secure communication. It is possible to create such artificial noise if the transmitter has multiple antennas. Thus, in [1], we analyzed secrecy capacity for a system with multiple transmit antennas, and one receive antenna each at the intended receiver and the eavesdropper. That paper introduced the idea of artificial noise and showed its benefit in obtaining secrecy capacity.

The focus of the present paper is to extend the idea of secrecy capacity using artificial noise, for the case where, a) either the eavesdropper (and the intended receiver) has multiple receive antennas or b) several eavesdroppers (with perhaps one antenna each) collude. The latter case of collusion can be modelled 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. Whereas the case with multiple receive antennas is a natural and useful generalization of the single receive antenna result of [1] (especially since the possibility of eavesdropper collusion is expected to be a problem in practical scenarios), this case is interesting also in terms of quantifying 'MIMO secrecy capacity'. As the results will show, MIMO secrecy capacity behaves quite unlike the usual MIMO capacity. For example, it is not true that secrecy capacity monotonically increases with the minimum of the number of transmit and receive antennas, as opposed to the celebrated result on usual MIMO capacity. Thus this paper provides insights into the effect of the secrecy requirement on MIMO capacity.

The paper is organized as follows. Section II formulates the problem of secrecy capacity. Section III shows how MIMO secrecy capacity (or alternatively, secrecy capacity in the presence of colluding eavesdroppers) can be obtained by transmitting artificial noise in the subspace orthogonal to the channel of the intended receiver. Section IV shows simulation results that demonstrate the behavior of MIMO secrecy capacity. Section V concludes the paper.

II. PROBLEM SCENARIO

We denote vectors and matrices with bold font. † is used to denote the Hermitian operator. All the nodes are assumed to have multiple antennas. Figure 1 shows a transmitter A with N_T antennas, a receiver B with N_R antennas and an eavesdropper with N_E antennas. The eavesdropper is an abstraction of multiple colluding eavesdroppers with a total of N_E antennas. $\mathbf{H}_k$ and $\mathbf{G}_k$ denote the channels of the receiver and the eavesdropper respectively, at time k. The transmitter (A) transmits $\mathbf{x}_k$ at time k. The signals received by the legitimate receiver (B) and the eavesdropper (E) are, respectively,

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{x}_k + \mathbf{n}_k, \qquad (1)$$
$$\mathbf{y}_k = \mathbf{G}_k \mathbf{x}_k + \mathbf{e}_k \qquad (2)$$

where the components of $\mathbf{n}_k$ and $\mathbf{e}_k$ are i.i.d. AWGN samples with variance σ_n^2 and σ_e^2 respectively. For simplicity, it is assumed that (1) has been normalized so that $\sigma_n^2 = 1$. The elements of $\mathbf{H}_k$ and $\mathbf{G}_k$ are assumed to be i.i.d. and independent of each other. It is assumed that the receiver is able to estimate its channel $\mathbf{H}_k$ perfectly and its feedback to the transmitter is noiseless. Further, we assume that the transmitter can *authenticate* the fed back channel gain, perhaps using some shared initial key. Block fading is assumed, meaning that the channel gains remain constant long enough so that information theoretic
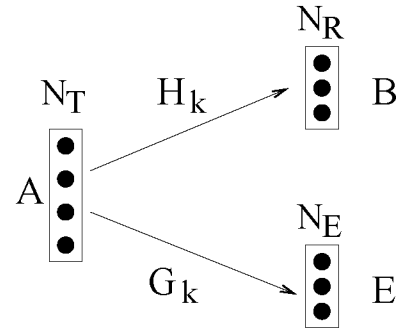

Fig. 1. Framework for Secrecy Capacity

results can be used and that the channel gains in different blocks are independent. The eavesdropper is assumed to be passive, which means that the eavesdropper only listens but does not transmit. Hence, the transmitter may not know the eavesdropper's channel $\mathbf{G}_k$. However, it is assumed that the eavesdropper may know both the receiver's and its own channel. The transmitter is assumed to have a power constraint of P_0.

III. SECRET COMMUNICATION USING ARTIFICIAL NOISE

The key idea of this paper is that the transmitter can use multiple antennas to add artificially generated noise to the information signal, such that it lies in the null space of the receiver's channel. Thus, the receiver's channel nulls out the artificial noise and hence the receiver remains unaffected by the noise. The information signal is transmitted in the range space of the receiver's channel, while the artificial noise is created in the null space, and thus, there is a clean separation between the two. The null and range spaces of the eavesdropper's channel will, in general, be different from those of the receiver's channel. Thus, the eavesdropper's channel will be degraded because some component of the artificial noise will lie in its range space. An increase in the number of receive antennas affects two aspects of secrecy capacity, the MIMO capacity 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. However, more receive antennas reduces the number of dimensions available for generating artificial noise, limiting the ability to degrade the eavesdropper's channel. These two opposing effects suggest that there may be interesting trade-offs to be made between them.

Assuming that $N_R \leq N_T$ and that $\mathbf{H}_k$ is full rank (i.e. has rank N_R), N_R dimensions can be used for information transmission while $N_T - N_R$ dimensions can be used to create artificial noise. The eavesdropper can use N_E

dimensions to receive information, of which some, or all, may be degraded by artificial noise. We need to study the variation of secrecy capacity with N_T, N_R and N_E. The effect of number of transmit antennas on secrecy capacity was shown in [1]. In this paper, we investigate the effect of multiple receive antennas and multiple colluding eavesdroppers (represented by $N_E > 1$) on secrecy capacity.

We now describe how the transmitter can generate artificial noise to degrade the eavesdropper's channel. Consider the channel equations (1), (2). The transmitter chooses $\mathbf{x}_k$ as the sum of information bearing signal ($\mathbf{s}_k$) and the artificial noise signal ($\mathbf{w}_k$),

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

where $\mathbf{w}_k$ is chosen such that $\mathbf{H}_k\mathbf{w}_k = 0$, i.e. $\mathbf{w}_k = \mathbf{Z}_k\mathbf{v}_k$ where $\mathbf{Z}_k$ is a null space matrix of $\mathbf{H}_k$. The transmitter chooses components of $\mathbf{v}_k$ to be i.i.d. Gaussian *random* variables with variance σ_v^2. The components of $\mathbf{w}_k$ are Gaussian distributed but are not statistically independent. The signals received by the receiver and the eavesdropper are given by, respectively,

$$\mathbf{z}_k = \mathbf{H}_k\mathbf{s}_k + \mathbf{n}_k, \tag{4}$$
$$\mathbf{y}_k = \mathbf{G}_k\mathbf{s}_k + \mathbf{G}_k\mathbf{w}_k + e_k. \tag{5}$$

Note how the artificial noise ($\mathbf{w}_k$) is nulled out by the receiver's channel but not 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 $\|\mathbf{G}_k\mathbf{w}_k\|$ turned out to be small. To avoid this possibility, $\{\mathbf{w}_k\}$ are chosen to be Gaussian random vectors in the null space of $\mathbf{H}_k$, as described above.

Based on (5), the eavesdropper (E) observes Gaussian noise with covariance

$$\mathbf{K} = (\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger)\sigma_v^2 + \mathbf{I}\sigma_e^2, \tag{6}$$

and thus, E first needs to whiten the noise by premultiplying the received signal by $\mathbf{K}^{-1/2}$. Now, secrecy capacity is bounded below by the difference in mutual information between the transmitter and receiver versus the transmitter and eavesdropper [2], [10]

$$Secrecy\ Capacity \geq C_{sec} = I(\mathbf{Z}; \mathbf{S}) - I(\mathbf{Y}; \mathbf{S}) \tag{7}$$

$$= \log|\mathbf{I} + \mathbf{H}_k\mathbf{Q}_\mathbf{s}\mathbf{H}_k^\dagger| - \log\left(\frac{|\mathbf{K} + \mathbf{G}_k\mathbf{Q}_\mathbf{s}\mathbf{G}_k^\dagger|}{|\mathbf{K}|}\right), \tag{8}$$

where $\mathbf{Q}_\mathbf{s} = \mathbf{E}[\mathbf{s}_k\mathbf{s}_k^\dagger]$ and $\mathbf{s}_k$ is Gaussian distributed. Note that C_{sec} is a lower bound on secrecy capacity which can be computed using the above equations. To study the behavior of C_{sec}, we can study the terms $I(\mathbf{Z}; \mathbf{S})$ and $I(\mathbf{Y}; \mathbf{S})$ separately, each of which corresponds to mutual information on a MIMO link. Since we have assumed that the transmitter is unaware of the eavesdropper's channel gain, it chooses $\mathbf{Q}_\mathbf{s}$ to maximize the capacity of the link to the receiver by using eigenvector transmission [10]. Let the Singular Value Decomposition (SVD) of $\mathbf{H}_k$ be given by

$$\mathbf{H}_k = \mathbf{U}_k\mathbf{\Lambda}_k\mathbf{V}_k^\dagger. \tag{9}$$

The transmitter chooses $\mathbf{s}_k = \mathbf{V}_k\mathbf{r}_k$ and 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

$$\tilde{\mathbf{z}}_k = \mathbf{\Lambda}_k\mathbf{r}_k + \tilde{\mathbf{n}}_k, \tag{10}$$

where components of $\tilde{\mathbf{n}}_k$ are i.i.d. Gaussian with mean 0 and variance 1. To maximize the mutual information between the transmitter and the receiver, the transmitter chooses $\mathbf{Q_r}$ as

$$\mathbf{Q_r} = \mathbf{E}[\mathbf{r}_k\mathbf{r}_k^\dagger] = diag(\sigma_{r,1}^2, \sigma_{r,2}^2, \ldots, \sigma_{r,N_T}^2), \tag{11}$$

with $\{\sigma_{r,i}^2\}_{i=1}^{N_T}$ chosen according to the waterfilling solution with total power constraint $P_{info} \leq P_0$. Then, secrecy capacity is lower bounded by,

$$C_{sec} = \log|\mathbf{I} + \mathbf{\Lambda}_k\mathbf{Q_r}\mathbf{\Lambda}_k^\dagger| - \log\left(\frac{|\mathbf{K} + \mathbf{G}_k\mathbf{V}_k\mathbf{Q_r}\mathbf{V}_k^\dagger\mathbf{G}_k^\dagger|}{|\mathbf{K}|}\right), \tag{12}$$

Note that C_{sec} is a random variable because it is a function of $\mathbf{H}_k$ and $\mathbf{G}_k$. Therefore, average secrecy capacity and outage probability can be computed, using Monte Carlo simulations. Since, the transmitter has a total power constraint of P_0, it distributes P_0 between the power of the information signal $P_{info} = tr(\mathbf{E}[\mathbf{s}_k\mathbf{s}_k^\dagger]) = tr(\mathbf{V}_k\mathbf{Q_r}\mathbf{V}_k^\dagger)$ and the power of the artificial noise signal $P_0 - P_{info}$ so as to maximize the lower bound on average secrecy capacity,

$$C_{sec} = \max_{tr(\mathbf{V}_k\mathbf{Q_r}\mathbf{V}_k^\dagger) \leq P_0} \mathbf{E}[\log|\mathbf{I} + \mathbf{\Lambda}_k\mathbf{Q_r}\mathbf{\Lambda}_k^\dagger| -$$

$$\log\left(\frac{|\mathbf{K} + \mathbf{G}_k\mathbf{V}_k\mathbf{Q_r}\mathbf{V}_k^\dagger\mathbf{G}_k^\dagger|}{|\mathbf{K}|}\right)], \tag{13}$$

where the expectation is over the random gains $\mathbf{H}_k$, $\mathbf{G}_k$. This optimal choice of P_{info} is used while computing outage probability.

IV. SIMULATION RESULTS

We compute the lower bound on average secrecy capacity C_{sec} under a power constraint of P_0. It is compared with the average capacity of the transmitter-receiver link (without secrecy requirements) under the same power constraint. The difference between the two ($C - C_{sec}$) is an upper bound on the loss in capacity because of the secrecy requirement. Further, given an outage capacity C_{outage}, we
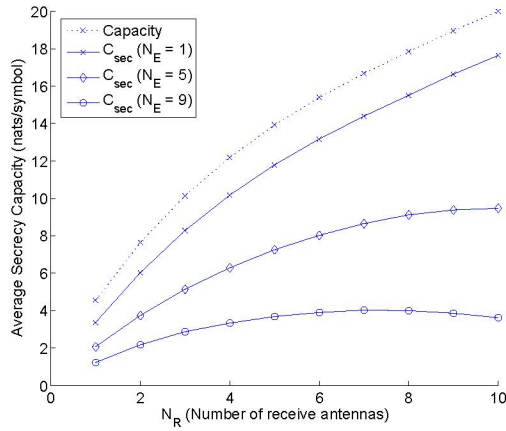
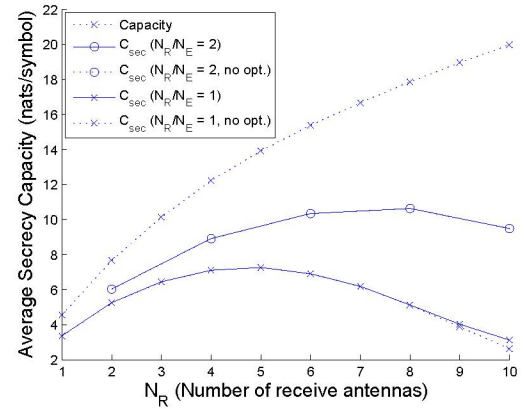Fig. 2. Average Secrecy Capacity: Variation with N_E and N_R

Fig. 3. Average Secrecy Capacity: Fixed ratio of N_E and N_R

compute the outage probabilities $Pr\{C_{sec} < C_{outage}\}$, hoping that low outage probabilities can be achieved. The effect of the number of transmit antennas (N_T) on secrecy capacity was considered in [1]. In this paper, the effect of the number of antennas at the receiver (N_R) and the eavesdropper (N_E) is considered, while keeping the number of transmit antennas (N_T) fixed. In the following discussions, references to average secrecy capacity should be interpreted to be the lower bound C_{sec}.

The average secrecy capacity and outage probability are computed using Monte Carlo simulations. For each given $\mathbf{H}_k$, its SVD is computed. The singular values of $\mathbf{H}_k$ are used to find the optimal covariance matrix $\mathbf{Q_r}$ as the waterfilling solution (with fixed P_{info}). The null space matrix, obtained from the SVD, determines the subspace (of dimension $N_T - N_R$) in which artificial noise is produced (with power $P_0 - P_{info}$). The average secrecy capacity is computed by averaging over various realizations of $\mathbf{H}_k$ and $\mathbf{G}_k$. The optimal P_{info} is found by performing an exhaustive line search.

For the simulations, it was assumed that elements of $\mathbf{H}_k$ and $\mathbf{G}_k$ are statistically independent Complex Gaussian random variables with $\mathbf{E}[|h_{i,j}|^2] = \mathbf{E}[|g_{i,j}|^2] = 1$. N_T was fixed to be 10 while N_R and N_E were varied. In Figure 2, average capacity (which is independent of N_E) and average secrecy capacity were plotted for fixed values of N_E. In Figure 3, the ratio between N_R and N_E was kept constant. Specifically, the case with $N_R = N_E$ guarantees fairness, as both the eavesdropper and the receiver nodes are assumed to have similar capabilities. Figure 4 shows the variation of average secrecy capacity with the distance between the transmitter and eavesdropper. The variation in distance is modeled by varying σ_e^2. The distance between the transmitter and receiver is assumed to remain constant. Figures 5 and 6 show the variation of outage probability

with N_R, with the ratio between N_R and N_E kept constant. For all simulations, the SNR per antenna $P_0/\sigma_{n,i}^2$ was fixed at 10 dB.

Figures 2 and 3 show that the average capacity of the link between the transmitter and the receiver is an upper bound on the average secrecy capacity between them. The former is independent of N_E and its behavior is given by the standard results for MIMO channels [6]. The gap between capacity and secrecy capacity represents the loss in capacity because of the secrecy requirement. The loss in capacity occurs because of two reasons. Firstly, only part of the power P_0 is used for the information bearing signal (P_{info}) while the rest of the power ($P_0 - P_{info}$) is used for creating artificial noise. This reduces the mutual information $I(\mathbf{Z}; \mathbf{S})$ between the information signal and the signal received by the receiver. Secondly, the amount of information that the eavesdropper gains about the information bearing signal $I(\mathbf{Y}; \mathbf{S})$ reduces secrecy capacity, based on (7).

Note that in Figure 2, it was assumed that all the available dimensions were used for information transmission. Clearly, the optimum number of receive antennas ($\leq N_R$) could have been found. This optimization was not done here, because we are interested in characterizing the behavior of secrecy capacity with N_R and N_E. However, for other figures, the above mentioned optimization was performed. Note that in order to optimize over the number of receive antennas to be used, N_E must be known (which was assumed in the following results).

Figure 3 shows the variation of average secrecy capacity with N_R, where a constant ratio was maintained between N_R and N_E. Two cases are considered, one with $N_R = N_E$ and the other with $N_R = 2N_E$. For either case, secrecy capacity is computed both with and without optimization over number of receive antennas used.
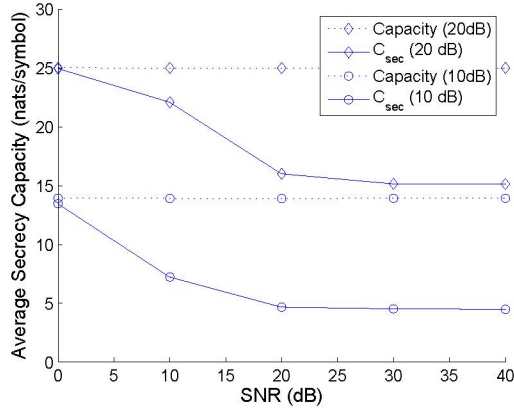
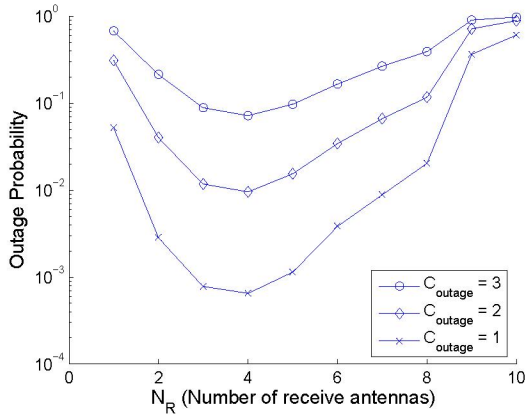Fig. 4.   Average Secrecy Capacity: Variation with distance

Fig. 6.   Outage Probability ($N_R = 2N_E$)

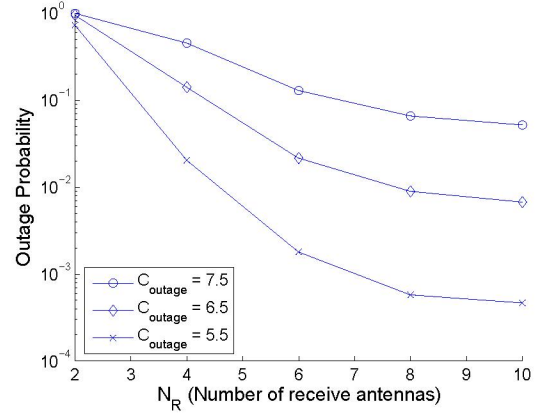Fig. 5.   Outage Probability ($N_R = N_E$)

The results with no optimization are plotted using dotted lines while those with optimization are plotted using solid lines. The optimization leads to a small difference for the case with $N_R = N_E$ when N_E is close to N_T. When N_R and N_E are close to N_T, the artificial noise can be produced in very few dimensions, and hence, most of the eavesdropper's channels are noise limited. In this case, it is beneficial to leave some of the receive antennas unused so that more dimensions can be used for producing artificial noise. An interesting phenomenon is observed when $N_R = N_E$; secrecy capacity attains a maximum at a value of $N_R < N_T$, rather than at $N_R = N_T$, as would be the case with usual MIMO capacity. We analyze the asymptotic case of large N_T to get some intuition into this phenomenon. When N_R is small (and so is N_E), all parallel channels of the eavesdropper are interference limited, with a high probability. $I(\mathbf{Y}; \mathbf{S})$ is small while $I(\mathbf{Z}; \mathbf{S})$ is proportional to N_R and hence secrecy capacity is proportional to N_R. For large N_R (close to N_T), roughly $N_T - N_R$ out of the N_E ($= N_R$) parallel channels of the

eavesdropper are interference limited. Hence, $I(\mathbf{Y}; \mathbf{S})$ is roughly proportional to $N_E - (N_T - N_R) = 2N_R - N_T$. $I(\mathbf{Z}; \mathbf{S})$ is still proportional to N_R, and, hence secrecy capacity roughly goes as $N_R - (2N_R - N_T) = N_T - N_R$. Thus, this intuitive argument shows that the maximum should occur at approximately $N_R = N_T/2$. This intuition is confirmed in Figure 3 where we find that the maximum occurs at $N_R = N_T/2 = 5$. A similar trend is observed for the case $N_R = 2N_E$, showing that secrecy capacity does not behave like the usual MIMO capacity (without secrecy requirements).

Figure 4 shows the effect of the eavesdropper's distance from the transmitter, on the average secrecy capacity. The variation in eavesdropper's distance was modeled by varying the per antenna SNR at the eavesdropper P_0/σ_e^2, which in turn was achieved by varying σ_e^2. The per antenna SNR at the receiver was kept fixed at 10 dB and 20 dB, for two different cases. Figure 4 shows that 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), the average secrecy capacity is close to the average capacity, as expected. As the eavesdropper comes closer to the transmitter, the average secrecy capacity reduces. However, instead of becoming arbitrarily small, it ultimately approaches a floor. Thus, even if the eavesdropper is very close to the transmitter, secret communication at non-trivial rates is possible.

Figures 5 and 6 show the variation of outage probability with N_R (with a fixed ratio between N_R and N_E) for a fixed outage capacity. For the case with $N_R = N_E$, the same interesting phenomenon as described earlier for average secrecy capacity, is observed; the outage probability is minimized at a value of $N_R < N_T$ (4 in this case). 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. For large N_R, there are roughly $2N_R - N_T$ parallel channels of the eavesdropper that are noise limited, using the same arguments described earlier for average secrecy capacity. Therefore, secrecy capacity is roughly given by the sum capacity of $N_R - (2N_R - N_T) = N_T - N_R$ parallel channels of the receiver. Thus, as N_R increases, the diversity provided by the parallel channels reduces and outage probability increases. For the case with $N_R = 2N_E$ on the other hand, the outage probability decreases monotonically with N_R. The curves in this case, are similar to the left half of the curves in Figure 5, where $N_E < N_T/2$.

V. Conclusion

This paper considered the problem of secret communication when multiple colluding eavesdroppers may be present. Further, we allowed the receiver nodes to have multiple antennas, and thus, tried to characterize 'MIMO secrecy capacity'. It was shown how artificial noise can be used to degrade only the eavesdropper's channel, and thus, allow secret communication under generic channel conditions. This was done by cleanly separating the information bearing signal and the artificial noise, by transmitting them in the range space and null space of the receiver's channel respectively. The effect of multiple antennas on the receiver and the eavesdropper (the latter modeling colluding eavesdroppers) was shown using simulation results. Results show that both, the number of antennas at the receiver and the eavesdropper, have a strong influence on the behavior of secrecy capacity. It was shown that even if the eavesdropper has a much 'better' channel than the receiver, secret communication at non-trivial rates is possible, using the artificial noise method. It was also shown that the behavior of MIMO secrecy capacity is different from that of the usual MIMO capacity without secrecy requirements, and thus, we need a different viewpoint when thinking about secrecy capacity.

References

[1] R. Negi, S. Goel, "Secret Communication using Artificial Noise," *To appear in Proceedings VTC Fall '05, Sept. 2005.*

[2] I. Csiszar, J. Korner, "Broadcast Channels with Confidential Messages," *IEEE Trans. Info. Theory*, pp. 339-348, May 1978.

[3] U. M. Maurer, "Unconditionally Secure Key Agreement and the Intrinsic Conditional Information," *IEEE Trans. Info. Theory*, pp. 499-514, March 1999.

[4] A. E. Hero, "Secure Space-Time Communication," *IEEE Trans. Info. Theory*, pp. 3235-3249, Dec. 2003.

[5] H. Koorapaty, A. A. Hassan, S. Chennakeshu, "Secure Information Transmission for Mobile Radio," *IEEE Trans. Wireless Communications*, pp. 52-55, July 2003.

[6] G. J. Foschini, D. Chizhik, M. J. Gans, C. Papadias, R. A. Valenzuela, "Analysis and performance of some basic spacetime architectures," *IEEE J. Select. Areas Commun., Special Issue on MIMO Systems*, pt. I, vol. 21, pp. 303-320, Apr. 2003.

[7] G. J. Foschini, "Layered space-time architecture for wireless communication in fading environments when using multi-element antennas," *Bell Labs Tech. Journal*, pp. 41-59, 1996.

[8] G. J. Foschini, 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.

[9] V. Tarokh, N. Sheshardri, A. R. Calderbank, "Space-time codes for high data rate wireless communications: Performance analysis and code construction," *IEEE Trans. Inform. Theory*, vol. 44, pp. 744-765, Mar. 1998.

[10] E. Telatar, "Capacity of multi-antenna Gaussian channels," *Eur. Trans. Telecomm. ETT*, vol. 10, no. 6, pp. 585-596, Nov. 1999.