Secret Communication using Artificial Noise

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

Abstract— **The problem of secret communication between two nodes over a wireless link is considered, where a passive eavesdropper may overhear the communication. It is desired that the eavesdropper be unable to decode the message. We show that secrecy can be achieved by adding artificially generated noise to the information bearing signal such that it does not degrade the intended receiver's channel. We consider two different scenarios; one in which the transmitter has multiple transmit antennas and the other in which the transmitter has a single antenna but 'helper' nodes are available. In the multiple antenna scenario, the degrees of freedom provided by the multiple antennas is used to generate artificial noise intelligently so that it degrades only the eavesdropper's channel. In the multiple helper scenario, even though the transmitter does not have multiple antennas, the helper nodes simulate the effect of multiple antennas and allow the transmitter to generate artificial noise as in the previous case.**

Keywords: Privacy, secrecy capacity, wireless

I. Introduction

The broadcast nature of wireless medium gives rise to a number of security issues. In particular, it makes it hard to limit access to wireless networks and makes it easy to eavesdrop, even from a distance. Secrecy problems involve three nodes; transmitter, receiver and an eavesdropper. The transmitter wants to communicate with the intended receiver without the eavesdropper being able to decode the secret message. We consider the problem of secret communication in the wireless environment, where a passive eavesdropper may overhear the communication. Since the eavesdropper is assumed to be passive, in general its location and even its presence will not be known to the transmitter. Hence, any secrecy scheme for this situation must not assume knowledge about the eavesdropper's location or its presence.

Our approach is inspired by the result in [1], which showed that secret communication is possible if the eavesdropper's channel is worse than the receiver's channel. [1] 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 the eavesdropper is closer to the transmitter than is the receiver). In this paper, we show 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. In a simple case, it is possible to create such artificial noise if the transmitter has multiple antennas. However, even if the transmitter has a single antenna but there are 'helper nodes' available, such noise can still be produced and *perfect secrecy* can be achieved. Note that this paper considers information theoretic security which makes no assumptions about the eavesdropper's computing power, i.e. the security cannot be broken even if the eavesdropper has infinite computational resources [3].

A technique for secret communication using channel state information (CSI) as the secret key was described in [5] and was generalized for the multi-antenna scenario by [4]. An abstract characterization of secrecy capacity of the kind discussed by [5] was obtained by [2]. In contrast, our paper assumes that the CSI is publicly available, so that it cannot be used to obtain a secret key.

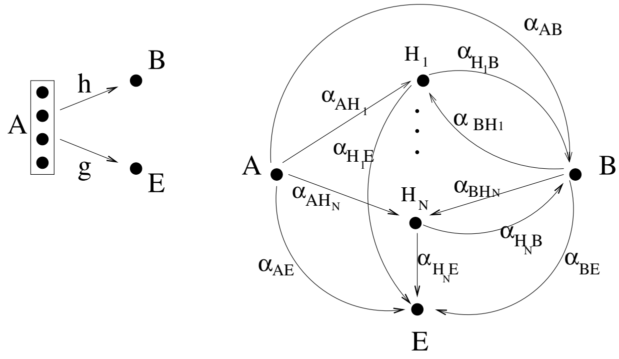
Section II formally introduces the problem of secret communication in the wireless environment. Section III develops the concept of artificial noise. Two scenarios are considered; one where the transmitter has multiple antennas and the other when the transmitter does not have multiple antennas but helper nodes are available. Simulation results are presented in Section IV. Finally, Section V concludes the paper.

II. Problem Scenario

Vectors are denoted by bold font. † denotes the Hermitian operator. For convenience, we measure information in nats instead of bits (i.e. $\log_e(\cdot)$ is assumed for entropy). Wherever applicable, we assume that transmissions of all nodes are synchronized (which is clearly an idealistic assumption). We consider two different scenarios.

Scenario 1 (Multiple antennas): Fig. 1(a) shows a transmitter A with N antennas and a receiver B and eavesdropper E with only one antenna each. We assume that multiple eavesdroppers (if they exist) cannot collude to form a multiple antenna receiver. An example of such a scenario is a wireless LAN with the base station as the transmitter. The channel gain vectors for channels from A to B and E, at time k, are given by $\mathbf{h}_k$ and $\mathbf{g}_k$ respectively. We assume that both channels are flat fading and the receiver can estimate $\mathbf{h}_k$ perfectly and feed it back to the transmitter without errors. Also, we assume that the transmitter can *authenticate* the fed back $\mathbf{h}_k$ (perhaps using a shared initial key). We assume that the eavesdropper is passive (i.e., listens, but does not transmit). Thus, the

This work was supported in part by Cylab, CMU under grant DAAD19-02-1-0389 from the Army Research Office.



(a) Scenario 1: Multiple Antennas (b) Scenario 2: Multiple Helpers

Fig. 1. Framework for Secrecy Capacity

transmitter does not know the eavesdropper's channel gain $\mathbf{g}_k$. However, the eavesdropper may know both $\mathbf{h}_k$ and $\mathbf{g}_k$.

Scenario 2 (Multiple helpers): Fig. 1(b) shows a transmitter A, intended receiver B and eavesdropper E with only a single antenna each. But several 'helper' nodes $(H_1, H_2, \ldots, H_N)$ exist to aid secret communication from A to B. As opposed to Scenario 1, the helper node antennas are not under direct control of the transmitter. The channel gain from X to Y is denoted α_{XY}. Note that the channels are not assumed to be reciprocal, i.e. in general $\alpha_{XY} \neq \alpha_{YX}$. It is assumed that the channel gains between A, B and the helper nodes are known to all nodes (possibly, even to the eavesdropper). *The secrecy of our communication scheme does not depend on secrecy of channel gains.*

III. Secret communication using artificial noise

The key idea in this paper is that a transmitter, perhaps in cooperation with the helper nodes, can generate noise artificially to conceal the secret message that it is transmitting. The noise is generated such that only the eavesdropper is affected but not the intended receiver. We first consider the simpler Scenario 1.

Scenario 1 (Multiple antennas): Here, the transmitter can use its multiple antennas to transmit artificial noise in the null space of the intended receiver's channel, and thus, not affect the receiver, while degrading the eavesdropper's channel. Let the transmitter transmit $\mathbf{x}_k$ at time k. The signals received by the legitimate receiver (B) and the eavesdropper (E) are, respectively,

$$\begin{aligned} z_k &= \mathbf{h}_k^\dagger \mathbf{x}_k + n_k, \qquad (1) \\ y_k &= \mathbf{g}_k^\dagger \mathbf{x}_k + e_k \qquad (2) \end{aligned}$$

where n_k and e_k are AWGN noise samples. The transmitter chooses $\mathbf{x_k}$ to be the sum of $\mathbf{p}_k u_k$ and $\mathbf{w}_k$, where u_k is the Gaussian distributed information bearing signal and $\mathbf{w}_k$ is a statistically independent, Gaussian distributed artificial noise vector, so that

$$\mathbf{x}_k = \mathbf{p}_k u_k + \mathbf{w}_k. \qquad (3)$$

Here, $\mathbf{w}_k$ is chosen such that $\mathbf{h}_k^\dagger \mathbf{w}_k = \mathbf{0}$, i.e. $\mathbf{w}_k$ lies in the null space of $\mathbf{h}_k^\dagger$. $\mathbf{p}_k$ is chosen such that $\mathbf{h}_k^\dagger \mathbf{p}_k \neq \mathbf{0}$ and $\mathbf{p}_k$ is normalized so that $\|\mathbf{p}_k\| = 1$. Then, the signals received by B and E are given by

$$\begin{aligned} z_k &= \mathbf{h}_k^\dagger \mathbf{p}_k u_k + n_k, \qquad (4) \\ y_k &= \mathbf{g}_k^\dagger \mathbf{p}_k u_k + \mathbf{g}_k^\dagger \mathbf{w}_k + e_k. \qquad (5) \end{aligned}$$

Note how the artificial noise lies in the null-space of $\mathbf{h}_k^\dagger$, so that it does not affect the intended receiver, while the eavesdropper's channel is degraded with high probability. If $\mathbf{w}_k$ is chosen to have a fixed direction, the secrecy capacity will be small if $\mathbf{g}_k^\dagger \mathbf{w}_k$ is small. To avoid this, $\{\mathbf{w}_k\}$ are chosen to be i.i.d. Gaussian random vectors in the null space of $\mathbf{h}_k^\dagger$, i.e.

$$\mathbf{w}_k = \mathbf{\Gamma}_k \mathbf{v}_k, \qquad (6)$$

where $\mathbf{\Gamma}_k$ is a null space matrix of $\mathbf{h}_k^\dagger$. It is assumed that $\mathbf{\Gamma}_k$ is chosen to be an orthogonal basis of the null space so that $\mathbf{\Gamma}_k^\dagger \mathbf{\Gamma}_k = I$ holds. The components of $\mathbf{v}_k$ are chosen to be i.i.d. Gaussian with zero mean and variance σ_v^2. Then, the secrecy capacity is given by [1]

$$\begin{aligned} \tilde{C}_{sec}^a &\geq I(Z;U) - I(Y;U) \qquad (7) \\ &= \log(1+\frac{|\mathbf{h}_k^\dagger \mathbf{p}_k|^2 \sigma_u^2}{\sigma_n^2}) - \log(1+\frac{|\mathbf{g}_k^\dagger \mathbf{p}_k|^2 \sigma_u^2}{\mathbf{E}|\mathbf{g}_k^\dagger \mathbf{w}_k|^2 + \sigma_e^2}), \qquad (8) \end{aligned}$$

where $\mathbf{E}|\mathbf{g}_k^\dagger \mathbf{w}_k|^2 = (\mathbf{g}_k \mathbf{\Gamma}_k \mathbf{\Gamma}_k^\dagger \mathbf{g}_k^\dagger)\sigma_v^2$. Thus, secrecy capacity is the difference of the mutual information between the transmitter and the intended receiver versus the eavesdropper. For a passive eavesdropper, $\mathbf{g}_k$ is not known to the transmitter, so the secrecy capacity is maximized by choosing $\mathbf{p}_k = \mathbf{h}_k/\|\mathbf{h}_k\|$. Clearly, with this choice of $\mathbf{p}_k$, $\mathbf{p}_k u_k$ lies in the range space of $\mathbf{h}_k$. Hence, the information bearing signal is transmitted in the range space of $\mathbf{h}_k$ whereas the artificial noise is transmitted in the null space of $\mathbf{h}_k^\dagger$. Thus, the two spaces are well separated.

Scenario 2 (Multiple helpers): When multiple antennas are not available at the transmitter, coordination with the helper nodes can, hopefully, allow the previous method to work. However, the helper nodes 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 helpers)? A novel 2-stage protocol achieves this, as described below. In the first stage, the transmitter and the intended receiver both transmit independent artificial noise signals to the helper nodes. The helper nodes and the eavesdropper receive different weighted versions of these two signals. In the second stage, the helper nodes simply replay a weighted version of the received signal, using a publicly available sequence of weights. At the same time, the transmitter transmits its secret message, while also cancelling the artificial noise at the intended receiver. Formally,

Stage 1

In the first stage, A and B transmit $\alpha_{AB}\, x$ and y respectively. The signals received by H_i and E are r_{H_i} and $r_{E,1}$ respectively. It is assumed that a node cannot transmit and receive at the same time.

$$\begin{aligned} r_{H_i} &= \alpha_{AH_i}\,\alpha_{AB}\,x + \alpha_{BH_i}\,y + n_i \qquad (9)\\ r_{E,1} &= \alpha_{AE}\,\alpha_{AB}\,x + \alpha_{BE}\,y + e_1 \qquad (10)\end{aligned}$$

Stage 2

In the second stage, A and H_i transmit $-\sum_i \beta_i\ \alpha_{AH_i}\ \alpha_{H_iB}\ x + z$ and $\beta_i\ r_{H_i}$ respectively. The signals received by B and E are r_B and $r_{E,2}$ respectively.

$$\begin{aligned} r_B &= \alpha_{AB}\,z + \sum_i \beta_i\,\alpha_{BH_i}\,\alpha_{H_iB}\,y + \\ &\quad \sum_i \beta_i\,\alpha_{H_iB}\,n_i + e_2 \qquad (11)\\ r_{E,2} &= \alpha_{AE}\,z + [\alpha_{AB}\sum_i \beta_i\,\alpha_{AH_i}\,\alpha_{H_iE} - \\ &\quad \alpha_{AE}\sum_i \beta_i \alpha_{AH_i}\alpha_{H_iB}]\,x + \sum_i \beta_i \alpha_{BH_i}\,\alpha_{H_iE}\,y + \\ &\quad \sum_i \beta_i\,\alpha_{H_iE}\,n_i + e_3 \qquad (12)\end{aligned}$$

Here, $e_1,\ e_2,\ e_3,\ \{n_i\}_{i=1}^N$ are AWGN noise samples. β_i are the random weights used by the helper nodes (known publicly). z is the information bearing signal while x and y are transmitted to conceal the transmission of z. Note how A's transmission of $-\sum_i \beta_i \alpha_{AH_i}\alpha_{H_iB}x$ cancels out the transmission of the helper nodes precisely, only at the intended receiver, but not at the eavesdropper, thus causing artificial noise in the latter. The equivalent channel from A to B is given by

$$\tilde{r}_B = \alpha_{AB} z + \sum_i \beta_i \alpha_{H_iB} n_i + e_2. \qquad (13)$$

Note that y is known to B and hence is not included in the equivalent channel. Varying $\beta_i's$ performs the same function as varying the direction of $\mathbf{w}_k$ in Scenario 1, and thus, reduces the probability of the artificial noise being nulled at the eavesdropper. The channel between A and E can be written as

$$\mathbf{r}_E = \mathbf{h}_z z + \mathbf{H}_{xy}\begin{pmatrix} x \\ y \end{pmatrix} + \mathbf{n}, \qquad (14)$$

$$\mathbf{h}_z = \begin{pmatrix} 0 \\ \alpha_{AE} \end{pmatrix}, \mathbf{n} = \begin{pmatrix} e_1 \\ \sum_i \beta_i\ \alpha_{H_iE}\ n_i + e_3 \end{pmatrix}, \qquad (15)$$

$$\mathbf{H}_{xy} = \begin{pmatrix} \alpha_{AB}\ \alpha_{AE} & \alpha_{BE} \\ \gamma & \sum_i \beta_i \alpha_{BH_i}\ \alpha_{H_iE} \end{pmatrix}, \qquad (16)$$

where, $\gamma = \alpha_{AB}\sum_i \beta_i\ \alpha_{AH_i}\ \alpha_{H_iE} - \alpha_{AE}\sum_i \beta_i \alpha_{AH_i}\alpha_{H_iB}$. Equation (14) represents a SIMO (Single Input Multiple Output) channel which is degraded by both AWGN noise and interference. The capacity for this channel is given by [7],

$$\begin{aligned} C &= \log|\mathbf{h}_z\mathbf{h}_z^\dagger \sigma_z^2 + \mathbf{K}| - \log|\mathbf{K}|, \qquad (17)\\ \mathbf{K} &= \mathbf{H}_{xy}\begin{pmatrix} \sigma_x^2 & 0 \\ 0 & \sigma_y^2 \end{pmatrix}\mathbf{H}_{xy}^\dagger + \\ &\quad \begin{pmatrix} \sigma_{e_1}^2 & 0 \\ 0 & \sum_i |\alpha_{H_iE}|^2 \sigma_{\beta_i}^2 \sigma_{n_i}^2 + \sigma_{e_3}^2 \end{pmatrix}. \qquad (18)\end{aligned}$$

Thus, the secrecy capacity is given by

$$\begin{aligned} \tilde{C}_{sec}^h &\geq I(Z;\tilde{R}_B) - I(Z;R_{E,1},R_{E,2}) \qquad (19)\\ &= \log(1+\frac{|\alpha_{AB}|^2\sigma_z^2}{\sigma_{n_B}^2}) - \log\frac{|\mathbf{h}_z\mathbf{h}_z^\dagger\sigma_z^2 + \mathbf{K}|}{|\mathbf{K}|}, \qquad (20)\end{aligned}$$

where, $\sigma_{n_B}^2 = \sum_i |\alpha_{H_iB}|^2 \sigma_{\beta_i}^2 \sigma_{n_i}^2 + \sigma_{e_2}^2$. The secrecy capacity obtained in (8) and (20) is a function of random channel gains. Therefore, the expected secrecy capacity, as well as the outage probability (cumulative distribution function) of the secrecy capacity can be computed for the two scenarios, using Monte Carlo simulations.

In both the scenarios, we assume that the total power transmitted per transmission is constrained to P_0. The total transmitted power in the multiple antenna scenario is given by

$$f_1(\sigma_u^2,\sigma_v^2) = \sigma_u^2 + (N_T - 1)\sigma_v^2. \qquad (21)$$

The combination of powers (σ_u^2, σ_v^2) is chosen such that it maximizes the lower bound on the expected secrecy capacity. Thus,

$$\begin{aligned} C_{sec}^a &\geq \max_{f_1(\sigma_u^2,\sigma_v^2)\leq P_0} \mathop{\mathbf{E}}_{\mathbf{h}_k,\mathbf{g}_k}[\log(1+\frac{|\mathbf{h}_k^\dagger \mathbf{p}_k|^2\sigma_u^2}{\sigma_n^2}) - \\ &\quad \log(1+\frac{|\mathbf{g}_k^\dagger \mathbf{p}_k|^2\sigma_u^2}{\mathbf{E}|\mathbf{g}_k^\dagger \mathbf{w}_k|^2 + \sigma_e^2})]. \qquad (22)\end{aligned}$$

The total transmitted power in the multiple helper case is given by

$$f_2(\sigma_x^2,\sigma_y^2,\sigma_z^2,\xi) = (2N_H\xi+1)\sigma_x^2 + (N_H\xi+1)\sigma_y^2 + \sigma_z^2 + N_H\xi, \qquad (23)$$

where we choose $\sigma_{\beta_i} = \xi \quad \forall i$ for simplicity. Further, it is assumed that $\mathbf{E}[|\alpha_{XY}|^2] = 1$. In this case, the combination of powers $(\sigma_x^2,\sigma_y^2,\sigma_z^2,\xi)$ is chosen to maximize the lower bound on the expected secrecy capacity and hence,

$$\begin{aligned} C_{sec}^h &\geq \max_{f_2(\sigma_x^2,\sigma_y^2,\sigma_z^2,\xi)\leq P_0} \mathbf{E}[\log(1+\frac{|\alpha_{AB}|^2\sigma_z^2}{\sigma_{n_B}^2}) - \\ &\quad \log\frac{|\mathbf{h}_z\mathbf{h}_z^\dagger\sigma_z^2 + \mathbf{K}|}{|\mathbf{K}|}], \qquad (24)\end{aligned}$$

where the expectation is over all the channel gains. For computing the outage probabilities for a given number of transmit antennas (or number of helper nodes) and total transmit power P_0, the combination of powers used is the one found by performing the optimization in (22) (or (24)).

IV. Simulation Results

We compute the expected secrecy capacity for the two scenarios, after optimizing the transmit powers, subject to the total power constraint of P_0. We compare it with the capacity of the transmitter-receiver link, for the same power constraint. The difference of the two provides an upper bound on the loss in capacity because of the secrecy requirement. We study the variation of the expected value and the outage probability of secrecy capacity with the number of transmit antennas and the total available power P_0. In the multiple

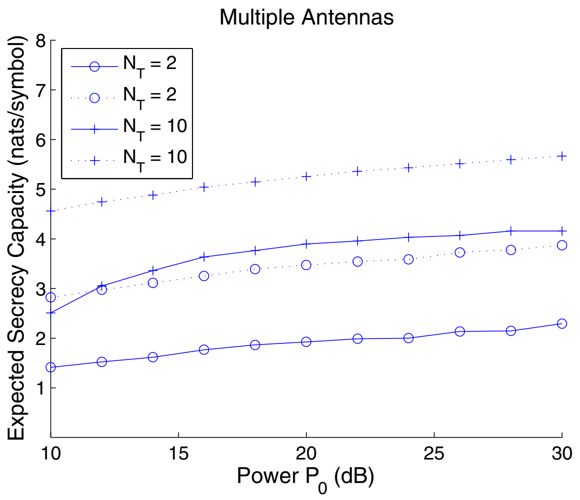


Fig. 2. Expected Secrecy Capacity: Multiple antenna scenario

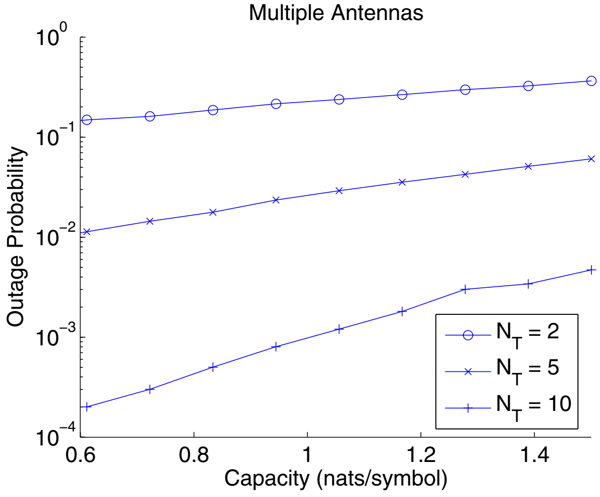


Fig. 4. Outage Probability: Multiple antenna scenario

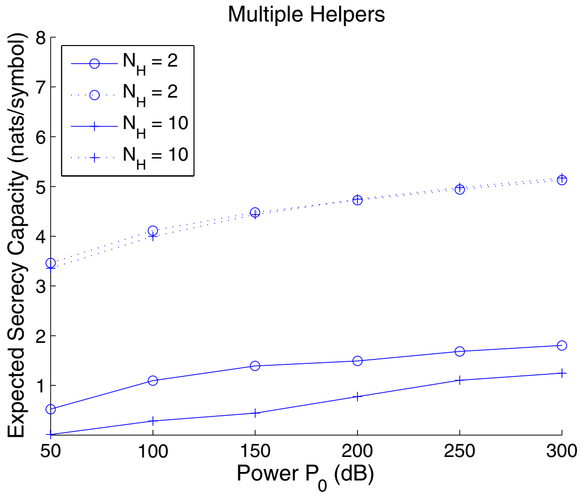


Fig. 3. Expected Secrecy Capacity: Multiple helpers scenario

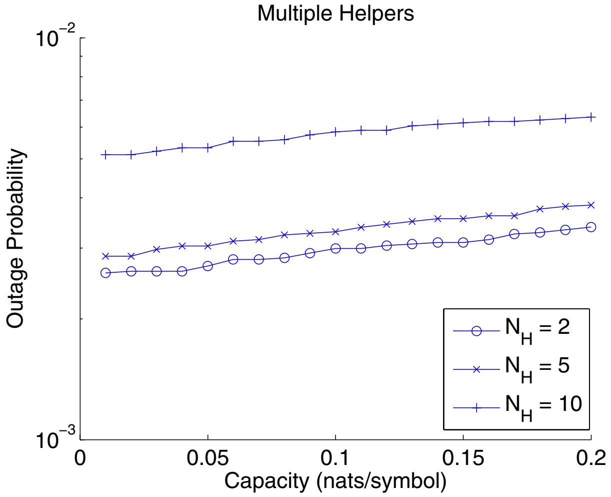


Fig. 5. Outage Probability: Multiple helper scenario

antenna scenario, the components of $\mathbf{h}_k$ and $\mathbf{g}_k$ are assumed to be i.i.d. Rayleigh distributed with $\mathbf{E}[|h_i|^2] = \mathbf{E}[|g_i|^2] = 1$. It is assumed that P_0 has been normalized by the power of AWGN noise variable n_k, $\sigma_n^2 \doteq \mathbf{E}[|n_k|^2]$. Further, it is assumed that the AWGN noise variables n_k and e_k have the same power, i.e. $\sigma_e^2 \doteq \mathbf{E}[|n_k|^2] = \sigma_n^2$. Similar normalization is assumed in the multiple helper scenario, along with the assumption that all AWGN noise variables have equal power. The channel gains are assumed to be i.i.d. Rayleigh distributed with $\mathbf{E}[|\alpha_{XY}|^2] = 1$.

The expected secrecy capacity and the outage probability for secrecy capacity are computed using Monte Carlo simulations. In the multiple antenna scenario, for each $\mathbf{h}_k^\dagger$, its null space matrix $\mathbf{\Gamma}_k$ is computed. Then, given $\mathbf{h}_k$ and $\mathbf{g}_k$, secrecy capacity is computed using (8). The expected secrecy capacity is obtained by averaging over the various realizations of $\mathbf{h}_k$ and $\mathbf{g}_k$. The combination of powers (σ_u^2, σ_v^2) is chosen to maximize the expected secrecy capacity, according to (22). This is done by performing an exhaustive search over a discretized space. Similarly, in the multiple helper scenario, given a set of channel gains, secrecy capacity is computed using (20). The combination of powers (σ_x^2, σ_y^2, σ_z^2, ξ) is chosen according to (24), using an exhaustive search over a discretized space.

Fig. 2 and 3 show the expected secrecy capacities for the multiple antenna and multiple helper scenario respectively. Fig. 4 shows the outage probabilities for the multiple antenna scenario with $P_0 = 13$ dB, while Fig. 5 shows the outage probabilities for the multiple helper scenario with $P_0 = 40$ dB. The powers (P_0) were chosen to achieve low enough outage probabilities.

Fig. 2 and 3 show that the variation of expected secrecy capacity (solid lines) with power is similar to that of capacity (dashed lines). Thus, secrecy capacity behaves like capacity in both the scenarios and the difference between the two represents the loss because of the secrecy requirement. Further, in the case of multiple antenna scenario, Fig. 2 shows that both capacity and secrecy capacity increase with the number of transmit antennas. The variation of expected secrecy capacity with power is governed by two factors. Equations (7) and (22) show that the expected secrecy capacity is lower bounded by the difference of two terms, $I(Z; U^*)$ and $I(Y; U^*)$, where U^* is found by performing the optimization in (22). Since, $\mathbf{p}_k$ is chosen as $\mathbf{p}_k = \mathbf{h}_k/\|\mathbf{h}_k\|$, $I(Z; U^*)$ is equal to the capacity on the transmitter-receiver link. The only difference is that the power available on this link for information transmission is σ_u^2, which is in general less than P_0. The loss in capacity because of secrecy requirement occurs because of two factors; the first one arises because only part of the total power is available for information transfer and the other factor is the mutual information $I(Y; U^*)$, which represents the amount of information that the eavesdropper has about the information bearing signal. Simulation results (Fig. 2) show that the combined effect of these two factors remains roughly constant as power P_0 is varied.

Fig. 2 and 4 show that as the number of transmit antennas (N_T) increases, the expected secrecy capacity increases while the outage probability decreases. Intuitively, as N_T increases, the dimensions of the null space of $\mathbf{h}_k^\dagger$ $(= N_T - 1)$ also increases. However, the range space of $\mathbf{h}_k$ is still one-dimensional. Thus, the probability of $\mathbf{g}_k$ having a large component along $\mathbf{h}_k$ reduces rapidly as N_T increases. On the other hand, its component in the null space of $\mathbf{h}_k^\dagger$ tends to be much larger. Therefore, as N_T increases, with a high probability, $|\mathbf{g}_k^\dagger \mathbf{p}_k|$ is small and so is $I(Y; U^*)$. Equation (7) shows that as $I(Y; U^*)$ decreases, secrecy capacity increases. Further, for a fixed σ_u^2 the capacity on the transmitter-receiver link ($I(Z; U^*)$) increases as N_T increases because it is a MISO (Multiple Input Single Output) link [6]. Thus, as N_T increases, the probability of secrecy capacity having a small value reduces rapidly. This phenomenon increases the expected secrecy capacity and also reduces the outage probability of secrecy capacity, as shown by Fig. 4. The figure also shows that fairly low outage probabilities are achievable as number of transmit antennas are increased.

The multiple helper scenario explores the case when the transmitter does not have multiple antennas. Instead multiple helper nodes are available which help the transmitter in generating artificial noise. We study the problem under the constraint on total power transmitted by all nodes. Fig. 3 shows that the expected secrecy capacity reduces as the number of helper nodes increases. The primary reason for this behavior is that as the number of helper nodes increases, the power available per node reduces. As opposed to the multiple antenna scenario, the helper nodes are not under the direct control of the transmitter. Any cooperation between the transmitter and the helper nodes (or among the helper nodes themselves) requires multiple transmissions. Thus, for every transmission of the secret information signal, several transmissions must occur for the artificial noise to be produced, which makes this scheme inefficient in comparison with the multiple antenna scheme. Fig. 5 shows that the outage probability increases as the number of helper nodes increases, primarily because the power available per node becomes more limited. However, we note in multiple helper scenario, that if there is more than one colluding eavesdropper, we will need to use more than one helper node to ensure secrecy. The variation of secrecy capacity and outage probability with the number of helper nodes implies that the minimum required number of helpers should be used (which is equal to the number of colluding eavesdroppers).

V. Conclusion

We considered the problem of secret communication in the wireless environment, in the presence of a passive eavesdropper. We showed how artificially generated noise can be added to the information bearing signal to achieve secrecy. In the multiple antenna scenario, the transmitter can use the multiple antennas to generate the artificial noise intelligently such that it degrades only the eavesdropper's channel. Further, we showed that even if the transmitter does not have multiple transmit antennas, helper nodes can simulate the effect of multiple antennas and the transmitter can still produce artificial noise. We showed that non-negligible rates are achievable for secret communication. Further, fairly low outage probabilities of secrecy capacity can be achieved. Future work will investigate the behavior of secrecy capacity in presence of multiple colluding eavesdroppers, and attempt to design practical schemes to achieve secrecy by using artificial noise.

References

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

[2] U. M. Maurer, S. Wolf, "Unconditionally Secure Key Agreement and the Intrinsic Conditional Information," *IEEE Trans. Info. Theory*, vol. 45, no. 2, pp. 499-514, March 1999.

[3] U. M. Maurer, "Secret Key Agreement by Public Discussion from Common Information," *IEEE Trans. Info. Theory*, vol. 39, no. 3, pp. 733-742, May 1993.

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

[7] G. J. Foschini, D. Chizhik, M. J. Gans, C. Papadias, R. A. Valenzuela, "Analysis and Performance of Some Basic Space-Time Architectures," *IEEE J. Select. Areas Comm.*, vol. 21, no. 3, pp. 303-320, April 2003.