Physical Layer Security with Artificial Noise: Secrecy Capacity and Optimal Power Allocation

Xiangyun Zhou* and Matthew R. McKay†
*College of Engineering and Computer Science, The Australian National University, Australia
†Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology, Hong Kong

***Abstract*—We consider the problem of secure communication in wireless fading channels in the presence of non-colluding passive eavesdroppers. The transmitter has multiple antennas and is able to simultaneously transmit an information bearing signal to the intended receiver and artificial noise to the eavesdroppers. We obtain an analytical closed-form lower bound for secrecy capacity, which is used as the objective function to optimize transmit power allocation between the information signal and the artificial noise. Our analytical and numerical results show that equal power allocation is a simple and generic strategy which achieves near optimal capacity performance. We also find that adaptive power allocation based on each channel realization provides no or insignificant capacity improvement over equal power allocation.**

I. Introduction

Security is a fundamental problem in wireless communications due to the broadcast nature of the wireless medium. Traditionally, secure communication is achieved by using cryptographic technologies such as encryption. However, the perfect secrecy of encryption cannot be guaranteed if the eavesdroppers have infinite computational power. On the other hand, the studies from an information-theoretic viewpoint have found conditions for reliable secure communication. In the pioneering works on information-theoretic security, Wyner introduced the wiretap channel for single point-to-point communication [1], which was extended to broadcast channels by Csiszár and Körner [2]. The results in these early works showed that a positive secrecy capacity can be achieved if the receiver has a better channel than the eavesdropper.

Recently, various physical-layer techniques were proposed to achieve secure communication even if the receiver's channel is worse than the eavesdropper's channel. One of the main techniques is the use of interference or artificial noise to confuse the eavesdropper. With two base stations connected by a high capacity, typically wired, backbone, one base station can simultaneously transmit an interfering signal to secure the uplink communication for the other base station [3, 4]. In the scenario where the transmitter has a helping interferer, the secrecy level can also be increased by having the interferer to send random codewords at a rate that ensures it can be decoded by the receiver but not by the eavesdropper [5]. When multiple antennas are available at the transmitter, it is possible to simultaneously transmit both the information bearing signal and artificial noise to achieve secrecy in a fading environment [6–8]. In this multi-antenna scenario, the transmit power allocation between the information signal and the artificial noise becomes an important design parameter, which has not been investigated in [6, 7]. A sub-optimal power allocation strategy which achieves a target signal to interference and noise ratio (SINR) at the receiver was proposed in [8]. However, it is not clear whether this strategy performs well in terms of the secrecy capacity or not.

In this paper, we study the problem of secure communication in fading channels with a multi-antenna transmitter capable of generating artificial noise. We derive an exact closed-form expression for the average secrecy capacity lower bound in Section III. Using the closed-form capacity expression as the objective function, we investigate the optimal transmit power allocation between the information bearing signal and the artificial noise in Section IV. Our results show that the equal power allocation is a simple yet near optimal strategy at any SNR values for systems with any practical number of transmit antennas. In addition, we find that adaptive power allocation based on each realization of the channel gain provide no or insignificant capacity gain over the equal power allocation.

Throughout the paper, the following notations will be used: Boldface upper and lower cases denote matrices and vectors, respectively. $[\cdot]^*$ denotes the complex conjugate operation, and $[\cdot]^\dagger$ denotes the conjugate transpose operation. The notation $E\{\cdot\}$ denotes the mathematical expectation. $|\cdot|$ denotes the absolute value of a scalar, and $\|\cdot\|$ denotes the norm of a vector.

II. System Model

We consider that the transmitter (A) has N_A antennas ($N_A > 1$) and the receiver (B) has a single antenna. This scenario is representative, for example, of downlink transmission in cellular systems and wireless local area networks (LAN). In addition, we allow non-colluding eavesdroppers (E) to individually overhear the communication between A and B without any central processing. We also assume that the eavesdroppers are passive, hence they cannot transmit jamming signals. We denote the channel between A and B and the channel between A and E as $\boldsymbol{h}$ and $\boldsymbol{g}$, respectively, both of which are $1 \times N_A$ vectors. The elements of $\boldsymbol{h}$ and $\boldsymbol{g}$ are independent and identically distributed (i.i.d.) complex Gaussian random variables. The knowledge of $\boldsymbol{h}$ can be obtained at A either from uplink (or reverse) training if channel reciprocity holds or using a feedback link from B to A. Similar to [6], we assume that the knowledge of both $\boldsymbol{h}$ and $\boldsymbol{g}$ is

978-1-4244-4474-8/09/$25.00 ©2009 IEEE

available at E, which makes the secrecy of communication independent of the secrecy of channel gains.

The key idea of guaranteeing secure communication using artificial noise proposed in [6] is described as follows. The transmitter utilizes multiple antennas to transmit the information bearing signal into the receiver's channel, at the same time generating a noise-like signal into the null space of the receiver's channel. We let an $N_A \times N_A$ matrix $\boldsymbol{W} = [\boldsymbol{w}_1 \ \boldsymbol{W}_2]$ be an orthonormal basis of $\mathbb{C}^{N_A}$, where $\boldsymbol{w}_1 = \boldsymbol{h}^\dagger/\|\boldsymbol{h}\|$. The transmitted symbol vector at A is given by $\boldsymbol{x} = \boldsymbol{w}_1 u + \boldsymbol{W}_2 \boldsymbol{v}$, where the variance of the information symbol u is σ_u^2 and the $N_A - 1$ elements of $\boldsymbol{v}$ are i.i.d. complex Gaussian random variables each with variance σ_v^2. Therefore, the received symbols at B and E are given by, respectively,

$$y_B = \boldsymbol{h}\boldsymbol{x} + n = \boldsymbol{h}\boldsymbol{w}_1 u + \boldsymbol{h}\boldsymbol{W}_1 \boldsymbol{v} + n = \|\boldsymbol{h}\| u + n, \quad (1)$$

$$y_E = \boldsymbol{g}\boldsymbol{x} + e = \boldsymbol{g}\boldsymbol{w}_1 u + \boldsymbol{g}\boldsymbol{W}_2 \boldsymbol{v} + e, \quad (2)$$

where n and e are the additive white Gaussian noises (AWGN) at B and E with variance σ_n^2 and σ_e^2, respectively. We see in (1) that $\boldsymbol{W}_1$ spans the null space of $\boldsymbol{h}$, hence the artificial noise $\boldsymbol{v}$ does not affect the received signal at B.

We consider a total power per transmission denoted by P, that is, $P = \sigma_u^2 + (N_A - 1)\sigma_v^2$. We refer to P/σ_n^2 as the transmit signal to noise ratio (SNR). One important design parameter is the ratio of power allocated to the information bearing signal and the artificial noise. We denote the fraction of total power allocated to the information signal as ϕ. Hence, we have the following relationships:

$$\sigma_u^2 = \phi P, \quad (3)$$

$$\sigma_v^2 = (1 - \phi)P/(N_A - 1). \quad (4)$$

In the rest of this paper, we investigate the optimal values of ϕ by first deriving a closed-form expression for an average secrecy capacity lower bound, and then employing this lower bound as the objective function.

III. Secrecy Capacity Lower Bound

The secrecy capacity is the maximum rate of transmission at which the receiver can decode the data with arbitrarily small error while the eavesdropper's error probability of decoding approaches one. It is bounded from below by the difference in the capacity of the channel between A and B and that between A and E [2].

The capacity of the channel between A and B is given by

$$C_1 = E_{\boldsymbol{h}}\{\log_2(1 + \sigma_u^2/\sigma_n^2 \|\boldsymbol{h}\|^2)\} = E_{\boldsymbol{h}}\{\log_2(1 + \phi P/\sigma_n^2 \|\boldsymbol{h}\|^2)\}. \quad (5)$$

Since $\boldsymbol{h}$ is known at the transmitter, the power allocation parameter ϕ can be designed based on each realization of $\boldsymbol{h}$. We refer to this strategy as the adaptive power allocation strategy. Alternatively, the transmitter can choose a fixed value for ϕ regardless of the channel gain, which we refer to as the non-adaptive power allocation strategy.

Without loss of generality, we normalize the variance of each element of $\boldsymbol{h}$ to unity. It is then easy to see that $\|\boldsymbol{h}\|^2$ follows a Gamma distribution with parameters $(N_A, 1)$. Therefore, for systems with non-adaptive power allocation strategy, we can rewrite (5) in an integral form as

$$C_1 = \frac{1}{\ln 2} \int_0^\infty \ln(1 + \phi P/\sigma_n^2 x) x^{N_A - 1} \frac{e^{-x}}{\Gamma(N_A)} \mathrm{d}x,$$

where $\Gamma(\cdot)$ is the Gamma function. Using the following identity from [9]

$$\int_0^\infty \ln(1 + bx) x^{c-1} e^{-x} \mathrm{d}x = \frac{(c-1)!}{e^{-1/b}} \sum_{k=1}^{c} \mathrm{E}_k(1/b),$$

where $\mathrm{E}_n(\cdot)$ is the generalized exponential integral, $b \geq 0$ and $c \geq 1$, we get

$$C_1 = \frac{\exp(z\sigma_n^2/P)}{\ln 2} \sum_{k=1}^{N_A} \mathrm{E}_k(z\sigma_n^2/P), \quad (6)$$

where we have defined $z = \phi^{-1}$.

Next, we obtain an upper bound on the capacity of the channel between A and E. When multiple eavesdroppers are present, the noise at each eavesdropper may be different. Similar to [7], we consider the worst case scenario, where the noise at E is arbitrarily small, e.g., $\sigma_e^2 \to 0$. Therefore, the capacity of the channel between A and a typical E can be bounded from above by

$$C_2 = E_{\boldsymbol{h}, g_1, \boldsymbol{g}_2}\Big\{ \log_2 \Big(1 + \frac{\sigma_u^2 |g_1|^2}{\sigma_v^2 \|\boldsymbol{g}_2\|^2}\Big)\Big\} = E_{\boldsymbol{h}, g_1, \boldsymbol{g}_2}\Big\{ \log_2 \Big(1 + \frac{\phi(N_A - 1)|g_1|^2}{(1-\phi)\|\boldsymbol{g}_2\|^2}\Big)\Big\}, \quad (7)$$

where we have defined $g_1 = \boldsymbol{g}\boldsymbol{w}_1$ and $\boldsymbol{g}_2 = \boldsymbol{g}\boldsymbol{W}_2$. The expectation over $\boldsymbol{h}$ in (7) is due to the fact that ϕ may be dependent on $\boldsymbol{h}$. We see in (7) that the variance of each element of $\boldsymbol{g}$ does not affect the upper bound C_2. Hence, C_2 in (7) is valid for any eavesdropper's channel and we can normalize the variance of the elements of $\boldsymbol{g}$ to unity without loss of generality.

Since $\boldsymbol{W}$ is a unitary matrix, $\boldsymbol{g}\boldsymbol{W} = [g_1 \ \boldsymbol{g}_2]$ has the same distribution as $\boldsymbol{g}$, i.e., a multivariate Gaussian distribution. Also, g_1 and the elements of $\boldsymbol{g}_2$ are orthogonal due to the orthogonality between $\boldsymbol{w}_1$ and the columns of $\boldsymbol{W}_2$. Therefore, we conclude that g_1 and the elements of $\boldsymbol{g}_2$ are independent. Consequently, $|g_1|^2/2$ and $\|\boldsymbol{g}_2\|^2/(2N_A - 2)$ have independent Chi-square distributions, and their ratio follows an F-distribution with parameter $(2, 2N_A - 2)$. The probability density function of a random variable X having an F-distribution with parameter $(2, 2N_A - 2)$ is given by

$$f_X(x) = \frac{\sqrt{\frac{(2x)^2 (2N_A - 2)^{2N_A - 2}}{(2x + 2N_A - 2)^{2N_A}}}}{x \mathrm{B}(1, N_A - 1)} = \frac{(N_A - 1)^{N_A}}{(x + N_A - 1)^{N_A}},$$

where $\mathrm{B}(y, z) = \frac{\Gamma(y)\Gamma(z)}{\Gamma(y+z)}$ is the Beta function. Therefore, we can rewrite (7) in integral form as

$$C_2 = E_{\boldsymbol{h}}\Big\{ \int_0^\infty \log_2 \Big(1 + \frac{\phi}{1-\phi} x\Big) f_X(x) \mathrm{d}x \Big\} = E_{\boldsymbol{h}}\Big\{ \frac{(N_A - 1)^{N_A}}{\ln 2} \int_0^\infty \ln \Big(1 + \frac{\phi}{1-\phi} x\Big) \frac{1}{(x + N_A - 1)^{N_A}} \mathrm{d}x \Big\}.$$

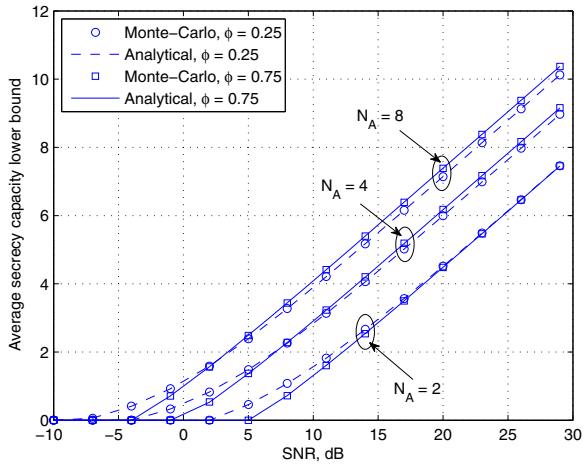

Fig. 1. Average secrecy capacity lower bound C versus SNR P/σ_n^2 with different power ratios ϕ and numbers of transmit antennas N_A. The lines (solid and dashed) are obtained using the closed-form expression in (10). The markers (circles and squares) are obtained from Monte-Carlo simulations.

Using the following identity derived in Appendix A

$$\int_0^\infty \frac{\ln(1+bx)}{(x+a)^c}\mathrm{d}x = \frac{b^{c-1}}{(c-1)^2}\,{}_2\mathrm{F}_1(c-1,c-1;c;1-ab),$$

where $b \geq 0$, $c > 1$ and ${}_2\mathrm{F}_1(\cdot)$ is the Gauss hypergeometric function, we get

$$C_2 = E_{\boldsymbol{h}}\Big\{\frac{(N_A-1)^{N_A-2}}{(z-1)^{N_A-1}\ln 2}\,{}_2\mathrm{F}_1\Big(N_A-1,N_A-1;N_A;\frac{z-N_A}{z-1}\Big)\Big\}, \tag{8}$$

where we have used $z = \phi^{-1}$.

Therefore, a lower bound on the average secrecy capacity is given by $C = C_1 - C_2$. For systems with adaptive power allocation, the average secrecy capacity lower bound is given as

$$C = \Big[E_{\boldsymbol{h}}\Big\{\log_2(1+z^{-1}P/\sigma_n^2\|\boldsymbol{h}\|^2) - \frac{(N_A-1)^{N_A-2}}{(z-1)^{N_A-1}\ln 2} \times {}_2\mathrm{F}_1\Big(N_A-1,N_A-1;N_A;\frac{z-N_A}{z-1}\Big)\Big\}\Big]^+, \tag{9}$$

where $[a]^+ = \max\{0,a\}$ and z is a function of $\boldsymbol{h}$. For systems with non-adaptive power allocation, the average secrecy capacity lower bound is given as

$$C = \Big[\frac{\exp(z\sigma_n^2/P)}{\ln 2}\sum_{k=1}^{N_A}\mathrm{E}_k(z\sigma_n^2/P) - \frac{(N_A-1)^{N_A-2}}{(z-1)^{N_A-1}\ln 2} \times {}_2\mathrm{F}_1\Big(N_A-1,N_A-1;N_A;\frac{z-N_A}{z-1}\Big)\Big]^+, \tag{10}$$

where z is a constant independent of $\boldsymbol{h}$.

Fig. 1 shows the average secrecy capacity lower bound in (10) versus SNR. The results are shown for different power allocation ratios as well as different numbers of transmit antennas. We see that the markers match perfectly with the lines for all cases. Therefore, the analytical closed-form expression in (10) is exact and can be used to optimize the power allocation between the information signal and the artificial noise.

IV. Optimal Power Allocation

In this section, we study the optimal power allocation between the information bearing signal and the artificial noise. The objective function for this optimization problem is the average secrecy capacity lower bound. As we have discussed, the power allocation strategy can be either adaptive or non-adaptive. The former depends on each realization of the channel gain while the latter is fixed for all channel realizations. In particular, we investigate the following two practical design questions:

- Is there a simple and generic power allocation strategy which gives near optimal performance in terms of the average secrecy capacity lower bound?
- How much secrecy capacity improvement can one achieve by adopting the adaptive power allocation strategy over the non-adaptive strategy?

The closed-form capacity expressions derived in the previous section greatly reduce the computational complexity of the optimization process. Furthermore, these capacity expressions enable us to analytically find the optimal power allocation in the high SNR regime as follows.

In the high SNR regime, i.e., $P/\sigma_n^2 \to \infty$, (5) can be approximated as

$$C_1 \approx \log_2(\phi P/\sigma_n^2\|\boldsymbol{h}\|^2) = \kappa - \frac{\ln z}{\ln 2}, \tag{11}$$

where κ is some constant independent of z. It is clear from (11) that the optimal value of z is independent of $\boldsymbol{h}$. The derivative of C_1 w.r.t. z is equal to $-1/(z\ln 2)$.

Using the derivative of the Gauss hypergeometric function [10], we obtain the derivative of C_2 in (8) as

$$\frac{\mathrm{d}C_2}{\mathrm{d}z} = \frac{(N_A-1)^{N_A-1}}{(z-1)^{N_A}\ln 2}\Big(\frac{(N_A-1)^2}{N_A(z-1)}\,{}_2\mathrm{F}_1(N_A,N_A;N_A+1;\frac{z-N_A}{z-1}) - {}_2\mathrm{F}_1(N_A-1,N_A-1;N_A;\frac{z-N_A}{z-1})\Big). \tag{12}$$

Therefore, the solution to the optimal power allocation at high SNR satisfies

$$\frac{\mathrm{d}C}{\mathrm{d}z} = -\frac{1}{z\ln 2} - \frac{\mathrm{d}C_2}{\mathrm{d}z} = 0, \tag{13}$$

where $\frac{\mathrm{d}C_2}{\mathrm{d}z}$ is given in (12).

In the special case of $N_A = 2$, we have [10]

$${}_2\mathrm{F}_1\Big(N_A-1,N_A-1;N_A;\frac{z-N_A}{z-1}\Big) = {}_2\mathrm{F}_1\Big(1,1;2;1-\frac{1}{z-1}\Big) = \frac{z-1}{z-2}\ln(z-1).$$

Therefore, (8) reduces to

$$C_2 = \frac{1}{\ln 2}\frac{1}{z-2}\ln(z-1). \tag{14}$$

And (13) simplifies to

$$-\frac{1}{z} - \frac{1}{(z-2)(z-1)} + \frac{\ln(z-1)}{(z-2)^2} = 0. \tag{15}$$

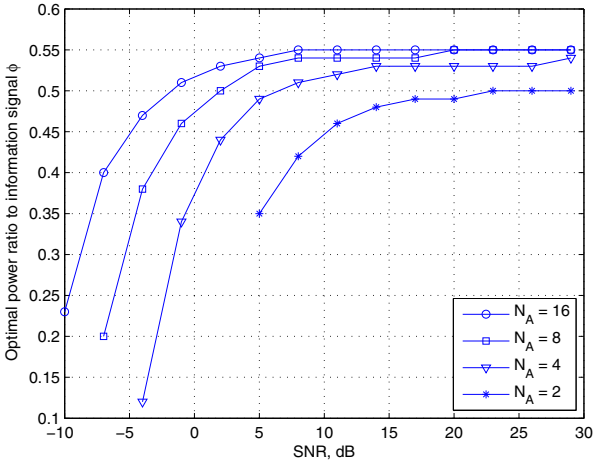

Fig. 2. Optimal ratio of power allocation ϕ versus SNR P/σ_n^2 for different numbers of transmit antennas N_A. The average secrecy capacity lower bound in (10) is used as the objective function, hence the non-adaptive power allocation strategy is used. The values of ϕ are shown for SNRs at which the secrecy capacity lower bound is positive.

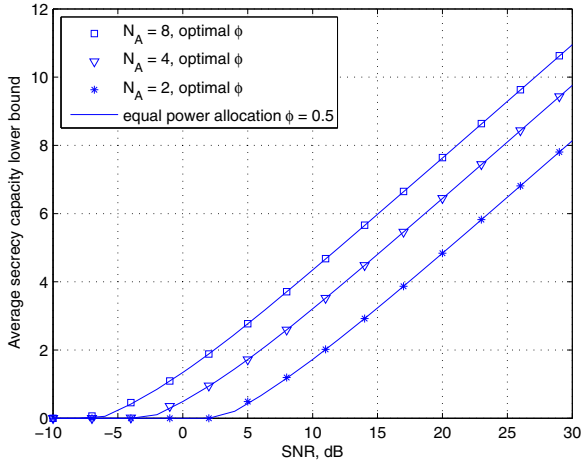

Fig. 3. Average secrecy capacity lower bound C in (10) versus SNR P/σ_n^2 for different numbers of transmit antennas N_A. The non-adaptive power allocation strategy is used. The average capacity lower bound with equal power allocation for each case (i.e., the solid line) is also shown for comparison.

The solution to (15) is given by $z = 2$. It can be shown that $\lim_{z\to 2} \frac{\mathrm{d}^2 C}{\mathrm{d}z^2} < 0$. Hence the optimal ratio of power allocation is given by $\phi = 0.5$, that is to say, equal power allocation between the information signal and the artificial noise is the optimal strategy in the high SNR regime for $N_A = 2$.

Fig. 2 shows the optimal values of ϕ using the non-adaptive power allocation strategy for systems with different numbers of transmit antennas. The values of ϕ are shown for SNRs at which the average secrecy capacity lower bound is positive. The general trend is that more power needs to be allocated to the information signal as SNR increases. In the high SNR regime, we see that the optimal values of ϕ converge to some constant values. For $N_A = 2$, the optimal value of ϕ converges to 0.5, which agrees with our analytical result. Furthermore, this constant value only increases slightly with N_A. For example, the optimal value of ϕ at high SNR ranges from 0.50 to 0.55 for N_A ranging from 2 to 16. This observation suggests that a near optimal yet simple power allocation strategy at moderate to high SNR values is the equal power allocation between the information signal and the artificial noise.

Fig. 3 shows the average secrecy capacity lower bound with the optimized ϕ using the non-adaptive strategy for systems considered as in Fig. 2. For comparison, we also include the capacity lower bound with equal power allocation, i.e., $\phi = 0.5$, indicated by the solid lines. We see that the equal power allocation strategy achieves nearly the optimal capacity performance in all cases over the entire range of SNR values. This confirms that equal power allocation is a simple and generic strategy which yields close to optimal capacity performance.

Fig. 4 shows the average secrecy capacity lower bound with the optimized ϕ, using both the adaptive and non-adaptive power allocation strategies, for systems with different numbers of transmit antennas. We see that there is no or insignificant difference between the capacity achieved by the adaptive and non-adaptive strategies in all cases over the entire range of SNR values. This result suggests that the non-adaptive power allocation strategy is sufficient to achieve almost the best possible capacity performance. Furthermore, from the observations in Fig. 3, it is clear that the use of equal power allocation achieves nearly the same capacity performance as that achieved by both the adaptive and non-adaptive power allocation strategies.

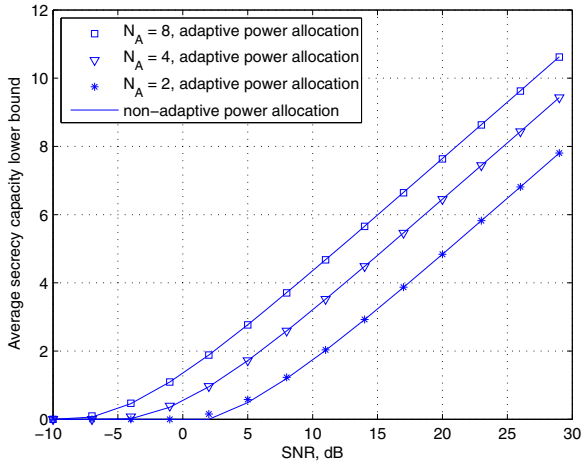

Fig. 4. Average secrecy capacity lower bound C versus SNR P/σ_n^2 for different numbers of transmit antennas N_A. Both the adaptive and non-adaptive power allocation strategies are used, indicated by the markers and the lines, respectively.

V. Conclusion and Future Work

In this paper, we considered the secure communication in the wireless environment where the transmitter sends artificial noise to the eavesdroppers. We obtained closed-form expressions for the average secrecy capacity lower bounds, which were used to study the optimal power allocation between the information bearing signal and the artificial noise. We analytically showed that the equal power allocation is the optimal strategy at high SNR for the case of two transmit antennas. From the numerical results, we also showed that the equal power allocation is a simple yet near optimal strategy at any SNR values for systems with any practical number of transmit antennas. Furthermore, we found that adaptive power allocation based on each realization of the channel gain provides no or insignificant capacity gain over the equal power allocation.

When the multiple eavesdroppers can collude, this scenario can be modeled as a single eavesdropper with multiple antennas. In this case, the optimal power allocation can be very different from that for non-colluding eavesdroppers. Furthermore, the transmitter can only adopt sub-optimal power allocation strategy if it does not have accurate knowledge about the number of eavesdroppers that are colluding. We are currently investigating this multiple-colluding eavesdropper scenario.

Appendix A
Derivation of an Integral Identity

Letting $f(x) = \ln(1+bx)$ and $g(x) = \frac{(x+a)^{1-c}}{1-c}$, we have $f'(x) \triangleq \frac{\mathrm{d}}{\mathrm{d}x} f(x) = \frac{b}{1+bx}$ and $g'(x) \triangleq \frac{\mathrm{d}}{\mathrm{d}x} g(x) = (x+c)^{-c}$. Using integration by parts, we have

$$\int_0^\infty \frac{\ln(1+bx)}{(x+a)^c}\mathrm{d}x = \int_0^\infty f(x)g'(x)\mathrm{d}x$$
$$= f(x{=}\infty)g(x{=}\infty) - f(x{=}0)g(x{=}0) - \int_0^\infty f'(x)g(x)\mathrm{d}x$$

For $b \geq 0$ and $c > 1$, it is easy to show that both $f(x = \infty)g(x = \infty)$ and $f(x = 0)g(x = 0)$ are equal to zero. Hence, we have

$$\int_0^\infty \frac{\ln(1+bx)}{(x+a)^c}\mathrm{d}x = -\int_0^\infty \frac{b}{1+bx}\frac{(x+a)^{1-c}}{1-c}\mathrm{d}x$$

We will evaluate the integral for $a > b^{-1}$. The case of $a < b^{-1}$ can be treat in a similar manner, and the case of $a = b^{-1}$ is straightforward. Indeed, it can be shown that all three cases yield the same result.

For $a > b^{-1}$, we have

$$\int_0^\infty \frac{\ln(1+bx)}{(x+a)^c}\mathrm{d}x$$
$$= -\frac{1}{(1-c)(a-b^{-1})^c}\int_0^\infty \frac{\left(\frac{x+b^{-1}}{a-b^{-1}}\right)^{-1}}{\left(1+\frac{x+b^{-1}}{a-b^{-1}}\right)^{c-1}}\mathrm{d}x$$
$$= -\frac{1}{(1-c)(a-b^{-1})^c}\int_{\frac{1}{ab-1}}^\infty \frac{y^{-1}}{(1+y)^{c-1}}\mathrm{d}x,$$

where we have defined $y = \frac{x+b^{-1}}{a-b^{-1}}$. Using the following identity from [11]

$$\int_u^\infty \frac{y^{\mu-1}\mathrm{d}y}{(1+\beta y)^\nu} = \frac{u^{\mu-\nu}}{\beta^\nu(\nu-\mu)}\,{}_2\mathrm{F}_1\Big(\nu, \nu-\mu; \nu-\mu+1; -1/(\beta u)\Big),$$

where $\nu > \mu$, we have

$$\int_{\frac{1}{ab-1}}^\infty \frac{y^{-1}}{(y+1)^{c-1}}\mathrm{d}y = \frac{b^{c-1}}{(c-1)^2}\,{}_2\mathrm{F}_1(c-1, c-1; c; 1-ab).$$

References

[1] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] M. L. Jorgensen, B. R. Yanakiev, F. E. Kirkelund, P. Popovski, H. Yomo, and T. Larsen, "Shout to secure: physical-layer wireless security with known interference," in *Proc. IEEE Global Commun. Conf. (Globecom)*, Washington, DC, Nov. 2007, pp. 33–38.

[4] O. Simeone and P. Popovski, "Secure communications via cooperating base stations," *IEEE Commun. Lett.*, vol. 12, no. 3, pp. 188–190, Mar. 2008.

[5] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference-assisted secrect communication," in *Proc. IEEE Inform. Theory Workshop (ITW)*, Porto, Portugal, May 2008, pp. 164–168.

[6] R. Negi and S. Goel, "Secret communications using artificial noise," in *Proc. IEEE Veh. Tech. Conf. (VTC)*, Dallas, TX, Sept. 2005, pp. 1906–1910.

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

[8] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE Int. Conf. on Acoustic, Speech and Signal Processing (ICASSP)*, Taipei, Taiwan, Apr. 2009, pp. 2437–2440.

[9] G. Alfano, A. Lozano, A. M. Tulino, and S. Verdú, "Mutual information and eigenvalue distribution of MIMO Ricean channels," in *Proc. Int. Symp. on Inform. Theory and its Appl. (ISITA)*, Parma, Italy, Oct. 2004.

[10] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulaes, Graphs, and Mathematical Tables*. New York: Dover Publications Inc., 1974.

[11] I. S. Gradshteyn and I. M. Ryzhik, *Tables of Integrals, Series, and Products*, 7th ed. Academic Press, 2007.