On Secrecy Rate of the Generalized Artificial-Noise Assisted Secure Beamforming for Wiretap Channels

Pin-Hsun Lin   Szu-Hsiang Lai   Shih-Chun Lin   Hsuan-Jung Su

Abstract

In this paper we consider the secure transmission in fast Rayleigh fading channels with full knowledge of the main channel and only the statistics of the eavesdropper's channel state information at the transmitter. For the multiple-input, single-output, single-antenna eavesdropper systems, we generalize Goel and Negi's celebrated artificial-noise (AN) assisted beamforming, which just selects the directions to transmit AN heuristically. Our scheme may inject AN to the direction of the message, which outperforms Goel and Negi's scheme where AN is only injected in the directions orthogonal to the main channel. The ergodic secrecy rate of the proposed AN scheme can be represented by a highly simplified power allocation problem. To attain it, we prove that the optimal transmission scheme for the message bearing signal is a beamformer, which is aligned to the direction of the legitimate channel. After characterizing the optimal eigenvectors of the covariance matrices of signal and AN, we also provide the necessary condition for transmitting AN in the main channel to be optimal. Since the resulting secrecy rate is a non-convex power allocation problem, we develop an algorithm to efficiently solve it. Simulation results show that our generalized AN scheme outperforms Goel and Negi's, especially when the quality of legitimate channel is much worse than that of eavesdropper's. In particular, the regime with non-zero secrecy rate is enlarged, which can significantly improve the connectivity of the secure network when the proposed AN assisted beamforming is applied.

I. INTRODUCTION

In a wiretap channel, a source node wishes to transmit confidential messages securely to a legitimate receiver and to keep the eavesdropper as ignorant of the message as possible. As a special case of the broadcast channels with confidential messages [1], Wyner [2] characterized the secrecy capacity of the discrete memoryless wiretap channel. The secrecy capacity is the largest rate communicated between the source and destination nodes with the eavesdropper knowing no information of the messages. Motivated by the demand of high data rate transmission and improving the connectivity of the network [3], the multiple antenna systems with security concern are considered by several authors. With full channel state information at the transmitter (CSIT), Shafiee and Ulukus [4] first proved the secrecy capacity of a Gaussian channel with two-input, two-output, single-antenna-eavesdropper. Then the authors of [5]–[7] extended the secrecy capacity to the Gaussian multiple-input multiple-output (MIMO), multiple-antenna-eavesdropper channel using different techniques. On the other hand, due to the characteristics of wireless channels, the impacts of fading channels on the secrecy transmission were considered in [5], [8] with full CSIT. Considering practical issues such as the limited bandwidth of the feedback channels or the speed of the channel estimation at the receiver, the perfect CSIT may not be available. Therefore, several works considered the secrecy transmission with partial CSIT [9]–[13]. In [9]–[11], the authors naively chose the directions of signal and AN without optimization and the resulting performance is suboptimal. In addition, they solved the power allocation via full search, which is inefficient. Furthermore, they did not prove the equality of the power constraint is hold (using all power is optimal). In [12], a single antenna system is considered, thus the authors did not solve the beamformer and power allocation problems. Also, the authors did not prove the rate increases with increasing total power. In [13], the authors did not consider the AN in the transmission, and thus their scheme is a special case of ours. Indeed, as shown in [9], [11], adding AN in transmission is crucial in increasing the secrecy rate in fading wiretap channels. Also under the case that the main channel is fully known at transmitter, the optimal direction for signals is not solved analytically in [13]. However, the secrecy capacities for channels with partial CSIT are known only for some limited cases, i.e., the transmitter has single antenna with block fading [10] and only the statistics

of both the main and eavesdropper's channels are known at the transmitter [14].

In this paper, we consider an important type of wiretap channels with partial CSIT, namely, the multiple-input single-output single-antenna-eavesdropper (MISOSE) fading wiretap channels. We assume that the main channel has a constant channel gain and the eavesdropper channel is fast faded, respectively. We also assume that the transmitter has perfect knowledge of the main channel and only the statistics of the eavesdropper channel. We adopt the artificial noise (AN) assisted secure beamforming as our transmission scheme, where the AN is used to disrupt the eavesdropper's reception [11] [9]. Although the secrecy capacity of the considered channel is unknown, the performance of the AN-assisted beamforming has been shown to be capacity-achieving in the high signal to noise ratio (SNR) regime when the transmitter is equipped with a large number of antennas [11]. However, in other operation regimes, the heuristically selected directions in [11] [9] to transmit AN may not be optimal, where the AN is restricted to be in the null space of the legitimate channel. This motivates our study on optimizing the AN assisted secure beamforming. Note that the assumption that the statistics of the eavesdropper's channel are known at transmitter was also used in [9] to design the power allocation between the signal and the AN (see [9, (8)]). Thus our comparison to the method in [9] in Section V is reasonable and fair.

The main contribution of our paper is that we propose a general AN scheme, which outperforms [9]. More specifically, the optimal AN may be full rank under some channel conditions rather than low rank, as restricted in [9]. In addition, we provide a simplified power allocation problem to describe the ergodic secrecy rate, which highly reduces the complexity of solving the rate. To attain it, we characterize the optimal beamforming directions and the power allocation strategies for AN. We also provide the necessary condition for transmitting AN in the main channel to be optimal. After characterizing the eigenvectors of the covariance matrices of signal and AN, the resulting rate becomes a non-convex power allocation problem and we develop an algorithm to efficiently solve it. Simulation results confirm that the full-rank AN provides rate gains over [9], especially through the enlarged non-zero rate region. Note that the secure connectivity in a network is assured by the non-zero secrecy rate of the transmitter-receiver pairs [3]. Thus our scheme is very useful for the large scale wireless network applications, which is an important type

of applications of the MISOSE wiretap channels [3].

The rest of the paper is organized as follows. In Section II we introduce the considered system model. In Section III an intuitive explanation of the rate gain from the proposed scheme is provided. We then develop our main result, i.e., the ergodic secrecy rate, via three steps. In this section we also provide the necessary condition to have a full rank optimal covariance matrix of AN. In Section IV, we provide an iterative algorithm to solve the power allocation problem. In Section V we demonstrate the simulation results. Finally, Section VI concludes this paper.

II. SYSTEM MODEL

In this paper, lower and upper case bold alphabets denote vectors and matrices, respectively. The superscript $(.)^H$ denotes the transpose complex conjugate. $|\mathbf{A}|$ and $|a|$ represent the determinant of the square matrix $\mathbf{A}$ and the absolute value of the scalar variable a, respectively. A diagonal matrix whose diagonal entries are $a_1 \ldots a_k$ is denoted by $diag(a_1 \ldots a_k)$. The trace of $\mathbf{A}$ is denoted by $\text{tr}(\mathbf{A})$. We define $C(x) \triangleq \log(1+x)$ and $(x)^+ \triangleq \max\{0, x\}$. $\mathbf{A}^\perp$ is the null space of $\mathbf{A}$. The mutual information between two random variables is denoted by $I(;)$. $\mathbf{I}_n$ denotes the n by n identity matrix. $\mathbf{A} \succ 0$ and $\mathbf{A} \succeq 0$ denote that $\mathbf{A}$ is a positive definite and positive semi-definite matrix, respectively. $\mathbf{a} \succ \mathbf{b}$ denotes $\mathbf{a}$ majorizes $\mathbf{b}$.

We consider the MISOSE system as shown in Fig. 1, where the transmitter (Alice) has n_T antennas and the legitimate receiver (Bob) and the eavesdropper (Eve) each has single antenna. The received signals at Bob and Eve can be respectively represented as

$$y_k = \mathbf{h}^H \mathbf{x}_k + n_{1,k}, \tag{1}$$

$$z_k = \mathbf{g}_k^H \mathbf{x}_k + n_{2,k}, \tag{2}$$

where $\mathbf{x}_k \in \mathbb{C}^{n_T \times 1}$ is the transmit vector, k is the time index, $\mathbf{h}$ is the constant main channel vector, $\mathbf{g}_k \sim CN(0, \mathbf{I}_{n_T})$ is the random eavesdropper's channel, and $n_{1,k}$ and $n_{2,k}$ are circularly symmetric complex additive white Gaussian noises with variances one at Bob and Eve, respectively. In this system model, we assume that full CSI of the legitimate channel and only the statistics of Eve's channel are known at transmitter. Without loss of generality, in the following we omit the time index to simplify the notation.

The perfect secrecy and secrecy capacity are defined as follows. Consider a $(2^{nR}, n)$-code with an encoder that maps the message $w \in \mathcal{W} = \{1, 2, \ldots, 2^{nR}\}$ into a length-n codeword, and a decoder at the legitimate receiver that maps the received sequence y^n (the collections of y over code length n) from the MISOSE channels (1) to an estimated message $\hat{w} \in \mathcal{W}$. We then have the following definition of secrecy capacity.

Definition 1 (Secrecy Capacity [10]): Perfect secrecy is achievable with rate R if, for any positive ε and ε', there exists a sequence of $(2^{nR}, n)$-codes and an integer n_0 such that for any $n > n_0$

$$I(w; z^n, \mathbf{h}^n, \mathbf{g}^n)/n < \varepsilon, \text{ and } \Pr(\hat{w} \neq w) \leq \varepsilon', \tag{3}$$

where w is the secret message, z^n, $\mathbf{h}^n$, and $\mathbf{g}^n$ are the collections of z, $\mathbf{h}$, and $\mathbf{g}$ over code length n, respectively. The secrecy capacity C_s is the supremum of all achievable secrecy rates.

From Csiszár and Körner's argument [1], we know that the general secrecy capacity can be represented by

$$C = \max_{p(\mathbf{x}|\mathbf{u}), p(\mathbf{u})} I(\mathbf{u}; y) - I(\mathbf{u}; z|\mathbf{g}). \tag{4}$$

However, for our considered CSIT setting, which is not full CSIT, the optimal $p(\mathbf{x}|\mathbf{u})$ and $p(\mathbf{u})$ are still unknown. We propose to apply the linear channel prefixing and Gaussian signaling to $f(x|u)$ as

$$\mathbf{x} = \mathbf{u} + \mathbf{v}, \tag{5}$$

where $\mathbf{u} \sim CN(0, \mathbf{S_u})$ and $\mathbf{v} \sim CN(0, \mathbf{S_v})$ are independent vectors to convey the message and AN, respectively. In addition, the feasible channel input matrices of signal and AN belong to the set

$$S = \{(\mathbf{S_u}, \mathbf{S_v}) : \text{tr}(\mathbf{S_u} + \mathbf{S_v}) \leq P_T, \mathbf{S_u} \succeq 0, \mathbf{S_v} \succeq 0\}. \tag{6}$$

Substituting (1), (2), and (5) into (4), we have the ergodic secrecy rate with generalized AN (GAN) as

$$R_{GAN} = \max_{\mathbf{S_u}, \mathbf{S_v} \in S} \left(\log \left(\frac{1 + \mathbf{h}^H (\mathbf{S_u} + \mathbf{S_v}) \mathbf{h}}{1 + \mathbf{h}^H \mathbf{S_v} \mathbf{h}} \right) - \mathbf{E} \left[\log \left(\frac{1 + \mathbf{g}^H (\mathbf{S_u} + \mathbf{S_v}) \mathbf{g}}{1 + \mathbf{g}^H \mathbf{S_v} \mathbf{g}} \right) \right] \right)^+. \tag{7}$$

Note that we do not limit the covariance matrix $\mathbf{S_v}$ of the AN $\mathbf{v}$ to have any special structure besides the conventional one (6). Thus our GAN scheme generalizes the AN in [9], which is *only* allowed to

be transmitted in the null space of the main channel. On the contrary, our GAN can be transmitted in all possible directions. We then solve the ergodic secrecy rate optimization problem (7) for the proposed GAN beamforming (GAN-BF) scheme in the following sections.

III. OPTIMIZATION OF THE ERGODIC SECRECY RATE

In this section, we identify the structure of the optimal solutions $\mathbf{S}_\mathbf{u}^*$ and $\mathbf{S}_\mathbf{v}^*$ for the GAN-BF optimization problem (7), where AN is not restricted in the null space of the main channel. By exploiting the optimal structure, we transform the complicated optimization problem over the covariance matrices (7) as a much simpler one in Theorem 1. In the following Theorem 1, the optimized ergodic secrecy rate of the GAN-BF is merely characterized by the power allocations among the message bearing signal, AN in the direction of the main channel, and AN in the directions orthogonal to the main channel.

Theorem 1: For the MISOSE fast fading wiretap channel with the perfect information of the legitimate channel $\mathbf{h}$, and only the statistics of the eavesdropper's channel $\mathbf{g} \sim CN(0, \mathbf{I}_{n_T})$ known at the transmitter, the optimization of the secrecy rate in (7) can be reduced to the following optimization problem

$$R_{GAN} = \max_{\substack{P_U, P_{V_1}, P_{V_2}: \\ P_U + P_{V_1} + (n_T - 1)P_{V_2} = P_T}} \left(\log\left(1 + \frac{||\mathbf{h}||^2 P_U}{1 + ||\mathbf{h}||^2 P_{V_1}}\right) - \mathbf{E}\left[\log\left(1 + \frac{\tilde{G}_1 P_U}{1 + \tilde{G}_1 P_{V_1} + \left(\sum_{i=2}^{n_T} \tilde{G}_i\right) P_{V_2}}\right)\right] \right)^+,$$

(8)

where P_U, P_{V_1}, and, P_{V_2} are the powers of the signal, the AN in the main channel, and the AN in the null space of the main channel, respectively. $\tilde{G}_i \triangleq |g_i|^2 \sim EXP(1)$, which is the exponential distribution with mean equal to 1, for $i = 1, 2, \ldots, n_T$.

Comparing (7) to (8) we can easily find that the optimization problem is vastly simplified from solving two matrices to three scalar variables. Note that we divide the proof of Theorem 1 into three parts for the tractability and each part corresponds to Theorem 2, Lemma 3, and Lemma 4, respectively. Before proving (8), we introduce two important lemmas to proceed.

Lemma 1: Given a diagonal matrix $\mathbf{D} = diag(d_1, d_2, \cdots, d_n) \in \mathbb{C}^{n \times n}$. Assume $d_1 \geq d_2 \geq \cdots \geq d_n$ and $\mathbf{U}$ is unitary. Then $\mathbf{U} = [\mathbf{h}/||\mathbf{h}||, \mathbf{h}^\perp/||\mathbf{h}||]$ and $\mathbf{U} = [\mathbf{h}^\perp/||\mathbf{h}||, \mathbf{h}/||\mathbf{h}||]$ maximizes and minimizes $\mathbf{h}^H \mathbf{U} \mathbf{D} \mathbf{U}^H \mathbf{h}$,

respectively.

Proof: We can rewrite the maximization problem in the statement of the lemma as

$$\max \sum_{i=1}^{n} d_i |\tilde{h}_i|^2, s.t. \sum_{i=1}^{n} |\tilde{h}_i|^2 = ||\mathbf{h}||^2, \tag{9}$$

where $\tilde{\mathbf{h}} = \mathbf{U}^H \mathbf{h}$, $\tilde{h}_i$ is the ith entry of $\tilde{\mathbf{h}}$. Then it can be easily seen that $|\tilde{h}_1| = ||\mathbf{h}||$ with $|\tilde{h}_2| = |\tilde{h}_3| = \cdots = |\tilde{h}_n| = 0$ can optimize (9). Therefore, it is clear that $\mathbf{U} = [\mathbf{h}/||\mathbf{h}||, \mathbf{h}^{\perp}/||\mathbf{h}||]$. The minimization part can be proved similarly. ∎

Now, we identify the eigenvectors of the optimal $\mathbf{S}_{\mathbf{u}}^*$ and $\mathbf{S}_{\mathbf{v}}^*$ through the following lemma.

Lemma 2: The optimal covariance matrices of the signal and AN $\mathbf{S}_{\mathbf{u}}^*$ and $\mathbf{S}_{\mathbf{v}}^*$ for (7) have the same eigenvectors as $[\mathbf{h}/||\mathbf{h}||, \mathbf{h}^{\perp}/||\mathbf{h}||]$.

Proof: Assume $\mathbf{S}_{\mathbf{u}} + \mathbf{S}_{\mathbf{v}}$ and $\mathbf{S}_{\mathbf{v}}$ are eigen-decomposed as $\mathbf{U}\mathbf{D}_1\mathbf{U}^H$ and $\mathbf{V}\mathbf{D}_2\mathbf{V}^H$, respectively. First, we can reform (14) as

$$\max_{\mathbf{S}_{\mathbf{u}}, \mathbf{S}_{\mathbf{v}}} R = \max_{\mathbf{D}_1, \mathbf{D}_2} \max_{\mathbf{U}, \mathbf{V}} R = \max_{\mathbf{D}_1, \mathbf{D}_2} \max_{\mathbf{U}, \mathbf{V}} \left(\log \left(\frac{1 + \mathbf{h}^H \mathbf{U}\mathbf{D}_1\mathbf{U}^H \mathbf{h}}{1 + \mathbf{h}^H \mathbf{V}\mathbf{D}_2\mathbf{V}^H \mathbf{h}} \right) - \mathbf{E} \left[\log \left(\frac{1 + \mathbf{g}^H \mathbf{U}\mathbf{D}_1\mathbf{U}^H \mathbf{g}}{1 + \mathbf{g}^H \mathbf{V}\mathbf{D}_2\mathbf{V}^H \mathbf{g}} \right) \right] \right)^+. \tag{10}$$

Since $\mathbf{g}$ is isotropically distributed,

$$\mathbf{E} \left[\log \left(\frac{1 + \mathbf{g}^H \mathbf{U}\mathbf{D}_1\mathbf{U}^H \mathbf{g}}{1 + \mathbf{g}^H \mathbf{V}\mathbf{D}_2\mathbf{V}^H \mathbf{g}} \right) \right] = \mathbf{E} \left[\log \left(\frac{1 + \mathbf{g}^H \mathbf{D}_1 \mathbf{g}}{1 + \mathbf{g}^H \mathbf{D}_2 \mathbf{g}} \right) \right],$$

which is independent of $\mathbf{U}$ and $\mathbf{V}$. Thus the inner optimization problem on the right hand side (RHS) of (10) becomes

$$(\mathbf{U}^*, \mathbf{V}^*) = \arg \max_{\mathbf{U}, \mathbf{V}} \log \left(\frac{1 + \mathbf{h}^H \mathbf{U}\mathbf{D}_1\mathbf{U}^H \mathbf{h}}{1 + \mathbf{h}^H \mathbf{V}\mathbf{D}_2\mathbf{V}^H \mathbf{h}} \right). \tag{11}$$

Then from Lemma 1 we know that $\mathbf{U} = \Pi_{\mathbf{U}}[\mathbf{h}/||\mathbf{h}||, \mathbf{h}^{\perp}/||\mathbf{h}||]$ and $\mathbf{V} = \Pi_{\mathbf{V}}[\mathbf{h}/||\mathbf{h}||, \mathbf{h}^{\perp}/||\mathbf{h}||]$ can simultaneously maximize and minimize the numerator and denominator, respectively, where $\Pi_{\mathbf{U}}$ and $\Pi_{\mathbf{V}}$ are the permutation matrices such that the eigenvector $\mathbf{h}/||\mathbf{h}||$ is in the direction of the maximum and minimum entries of $\mathbf{D}_1$ and $\mathbf{D}_2$, respectively. Therefore, R is maximized. As a result, $\mathbf{S}_{\mathbf{u}}$ and $\mathbf{S}_{\mathbf{v}}$ have the same eigenvectors. ∎

We then introduce the interlacing theorem in Lemma 3 [15, p.182] which will be used in proving beamforming is optimal (Theorem 2).

Lemma 3 (Interlacing theorem): Let $\mathbf{M} \in \mathbb{C}^{n \times n}$ be a Hermitian matrix and let $\mathbf{a} \in \mathbb{C}^n$ be a given vector. We then have

$$\text{(a)} \quad \lambda_k(\mathbf{M} \pm \mathbf{a}\mathbf{a}^H) \leq \lambda_{k+1}(\mathbf{M}) \leq \lambda_{k+2}(\mathbf{M} \pm \mathbf{a}\mathbf{a}^H), \quad k = 1, 2, \ldots, n-2, \tag{12}$$

$$\text{(b)} \quad \lambda_k(\mathbf{M}) \leq \lambda_{k+1}(\mathbf{M} \pm \mathbf{a}\mathbf{a}^H) \leq \lambda_{k+2}(\mathbf{M}), \quad k = 1, 2, \ldots, n-2, \tag{13}$$

where $\lambda_k(\mathbf{A})$ is the kth eigenvalue of $\mathbf{A}$ in ascending order.

First, we identify the rank property of the optimal $\mathbf{S_u}^*$.

Theorem 2: For the MISOSE fast fading wiretap channel with the perfect information of the legitimate channel $\mathbf{h}$, and only the statistics of the eavesdropper channel $\mathbf{g} \sim CN(0, \mathbf{I}_{n_T})$ known at the transmitter, with the proposed GAN-BF, the optimal covariance matrix of signal for (7) is $\mathbf{S_u^*} = \frac{P_U}{\|\mathbf{h}\|^2}\mathbf{h}\mathbf{h}^H$.

Proof: Since the secrecy rate optimization problem (7) is non-convex, we can use the Karush-Kuhn-Tucker (KKT) conditions to find the necessary conditions for the optimal solutions. We first transform (7) into the following form to simplify the KKT conditions

$$R_{GAN} = \left(\max_{\mathbf{S_u}, \mathbf{S_v} \in S} \log \left(\frac{1 + \mathbf{h}^H (\mathbf{S_u} + \mathbf{S_v}) \mathbf{h}}{1 + \mathbf{h}^H \mathbf{S_v} \mathbf{h}} \right) - \mathbf{E} \left[\log \left(\frac{1 + \mathbf{g}^H (\mathbf{S_u} + \mathbf{S_v}) \mathbf{g}}{1 + \mathbf{g}^H \mathbf{S_v} \mathbf{g}} \right) \right] \right)^+. \tag{14}$$

Compared with (7), in (14), we place the maximum inside the operation $(.)^+$. The equivalence of (7) and (14) comes from the fact that we can represent R_{GAN} by range of the objective inside $()^+$ in (7) as the union of the sets of positive and negative rates R^+ and R^-, respectively, as $R_{GAN} = \max(R^+ \bigcup R^-)^+ = \max(R^+, R^-)^+$, which is $\max(R^+)$ when R^+ is a nonempty set and zero, otherwise. On the other hand, $(\max(R^+ \bigcup R^-))^+$ is also $\max(R^+)$ when R^+ is a nonempty set and zero, otherwise. Thus we know (7) and (14) are equivalent. Let $\lambda \geq 0$, $\psi_{\mathbf{u}} \succeq 0$, and $\psi_{\mathbf{v}} \succeq 0$ be the Lagrange multipliers of the three constraints

in (6), respectively, the KKT conditions of (7) is

$$\Theta_1 = \mathbf{S_u^*} = \mathbf{A}(\mathbf{S_u^*}, \mathbf{S_v^*}) - \lambda \mathbf{I}_{n_T} + \psi_\mathbf{u}^T = \mathbf{0}, \tag{15}$$

$$\Theta_2 = \mathbf{S_v^*} = \mathbf{A}(\mathbf{S_u^*}, \mathbf{S_v^*}) - \frac{\mathbf{hh}^H}{1 + \mathbf{h}^H \mathbf{S_v^*} \mathbf{h}} + \mathbf{E}\left[\frac{\mathbf{gg}^H}{1 + \mathbf{g}^H \mathbf{S_v^*} \mathbf{g}}\right] - \lambda \mathbf{I}_{n_T} + \psi_\mathbf{v}^T = \mathbf{0}, \tag{16}$$

$$\psi_\mathbf{u} \mathbf{S_u^*} = \mathbf{S_u^*} \psi_\mathbf{u} = \mathbf{0}, \tag{17}$$

$$\psi_\mathbf{v} \mathbf{S_v^*} = \mathbf{S_v^*} \psi_\mathbf{v} = \mathbf{0}, \tag{18}$$

$$\text{tr}(\mathbf{S_u^*} + \mathbf{S_v^*}) \leq P_T, \ \mathbf{S_u^*} \succeq \mathbf{0}, \ \mathbf{S_v^*} \succeq \mathbf{0}, \tag{19}$$

where

$$\mathbf{A}(\mathbf{S_u^*}, \mathbf{S_v^*}) \triangleq \mathbf{aa}^H + \mathbf{M}, \tag{20}$$

$$\mathbf{aa}^H \triangleq \frac{\mathbf{hh}^H}{1 + \mathbf{h}^H (\mathbf{S_u^*} + \mathbf{S_v^*}) \mathbf{h}}, \tag{21}$$

$$\mathbf{M} \triangleq -\mathbf{E}\left[\frac{\mathbf{gg}^H}{1 + \mathbf{g}^H (\mathbf{S_u^*} + \mathbf{S_v^*}) \mathbf{g}}\right], \tag{22}$$

and $\mathbf{S_u^*}$ and $\mathbf{S_v^*}$ are the optimal input covariance matrices of $\mathbf{u}$ and $\mathbf{v}$, respectively. In the following we denote $\mathbf{A}(\mathbf{S_u^*}, \mathbf{S_v})$ by $\mathbf{A}^*$ to simplify the notation. After left and right multiplying (15) by $(\mathbf{S_u^*})^T$, with (17), we have the relation $\mathbf{A}^*(\mathbf{S_u}^*)^T = (\mathbf{S_u}^*)^T \mathbf{A}^* = \lambda (\mathbf{S_u^*})^T$, where $\lambda = \frac{\text{tr}(\mathbf{A}^*(\mathbf{S_u}^*)^T)}{\text{tr}((\mathbf{S_u}^*)^T)}$. Then we can apply [13, Lemma 8] to ensure $\lambda > 0$, if $R > 0$. Since $\mathbf{A}^*$ and $(\mathbf{S_u^*})^T$ commute, they have the same eigenvectors. Therefore, we have

$$\mathbf{\Lambda_{A^*}} \mathbf{\Lambda_{S_u^*}} = \mathbf{\Lambda_{S_u^*}} \mathbf{\Lambda_{A^*}} = \lambda \mathbf{\Lambda_{S_u^*}}, \tag{23}$$

where $\mathbf{\Lambda_{A^*}}$ and $\mathbf{\Lambda_{S_u^*}}$ are the eigenvalue matrices of $\mathbf{A}^*$ and $\mathbf{S_u^*}$, respectively. Due to $\mathbf{M}$ in (20) is a negative-definite matrix [13, Lemma4], from Lemma 3, we know that all eigenvalues of $\mathbf{A}^*$ are smaller to zero except for the largest one. This can be explained as following. By using Lemma 3 and letting $k = n_T - 2$ in (13), we have $\lambda_{n_T-1}(\mathbf{A}^*) \leq \lambda_{n_T}(\mathbf{M})$. Note that $\mathbf{M}$ is a negative definite matrix, i.e., $\lambda_{n_T}(\mathbf{M}) < 0$. So we have $\lambda_i(\mathbf{A}^*) < 0$ for $i = 1, 2, \ldots, n_T - 1$. Since λ is positive, from (23) we know that it must be the largest eigenvalue of $\mathbf{A}^*$, i.e. $\lambda = \lambda_{n_T}(\mathbf{A}^*)$. In order to make the equality $\mathbf{\Lambda_{A^*}} \mathbf{\Lambda_{S_u^*}} = \lambda \mathbf{\Lambda_{S_u^*}}$ valid, the eigenvalues of $\mathbf{S_u^*}$ corresponding to non-positive eigenvalues of $\mathbf{A}^*$ must be all zeros. Therefore, we obtain that $\mathbf{S_u^*}$

has only one nonzero eigenvalue. So the covariance matrix of $\mathbf{S_u^*}$ is rank one if $R > 0$. Then with Lemma 2, we conclude the proof. ∎

In the following we prove an important property, that is, using all the power is optimal for the proposed AN scheme.

Lemma 4: To maximize (7), the sum power constraint in (6) is hold with equality.

Proof: Similar to Theorem 2, the key observation here is that with the selection of eigenvectors of signal and AN in Lemma 2, the first term on the RHS of (10) is independent of the power of AN in the null space of the legitimate channel. Thus to find P_{V_i} for $i = 2, 3, \ldots, n_T$ given P_U and P_{V_1}, the objective function becomes

$$\min_{P_{V_2} \cdots P_{V_{n_T}}} \mathbf{E} \left[\log \left(1 + \frac{\tilde{G}_1 P_U}{1 + \tilde{G}_1 P_{V_1} + \sum_{i=2}^{n_T} \tilde{G}_i P_{V_i}} \right) \right]. \tag{24}$$

From (24) it can be easily seen that given P_U and P_{V_1}, the value of the objective function decreases with increasing P_T. Thus we may change the first inequality constraint in (6) as an equality one. ∎

Based on Lemma 2 and 4, we have the following property for AN.

Lemma 5: For the optimization problem (7), the optimal covariance matrix of AN is

$$\mathbf{S_v}^* = \frac{1}{n_T - 1} \left(\frac{n_T P_{V_1} - P_T + P_U}{||\mathbf{h}||^2} \mathbf{h}\mathbf{h}^H + (P_T - P_U - P_{V_1})\mathbf{I} \right).$$

Proof: To proceed, we transform (24) as

$$\max_{P_{V_2} \cdots P_{V_{n_T}}} \mathbf{E} \left[\log \left(1 + \tilde{G}_1 P_{V_1} + \sum_{i=2}^{n_T} \tilde{G}_i P_{V_i} \right) - \log \left(1 + \tilde{G}_1 (P_U + P_{V_1}) + \sum_{i=2}^{n_T} \tilde{G}_i P_{V_i} \right) \right] = \max_{P_{V_2} \cdots P_{V_{n_T}}} \mathbf{E}_{\tilde{G}_1} \left[f(x) \Big| \tilde{G}_1 \right],$$

$$\tag{25}$$

where the equality comes from the conditional mean, $f(x) \triangleq \mathbf{E} \left[\log(a + x) - \log(b + x) \right]$ and we denote $1 + \tilde{G}_1 P_{V_1}$, $1 + \tilde{G}_1 (P_U + P_{V_1})$, and $\sum_{i=2}^{n_T} \tilde{G}_i P_{V_i}$ by a, b, and x, respectively. If given $\tilde{G}_1 = g_1, \forall g_1$, the optimal power allocation of $f(x)$ is $P_{V_2} = P_{V_3} = \cdots = P_{V_{n_T}}$, then for the problem on the left hand side (LHS) of (25), this power allocation is also optimal. This is due to the fact that $\tilde{G}_i$ is unknown at transmitter by whom can not be used to change the power allocation. Therefore, we want to prove that under $\sum_{i=2}^{n_T} P_{V_i} = P_T - P_U - P_{V_1}$

$$f \left(\frac{P_T - P_U - P_{V_1}}{n_T - 1} \sum_{i=2}^{n_T} \tilde{G}_i \right) \geq f \left(\sum_{i=2}^{n_T} \tilde{G}_i P_{V_i} \right), \forall P_{V_i}, i = 2, \cdots, n_T. \tag{26}$$

Here we introduce some results from the *stochastic ordering theory* [16] to prove the desired result.

Definition 2: [16, p.234] A function $\psi : [0, \infty) \to \mathbb{R}$ is completely monotone if for all $x > 0$ and $n = 0, 1, 2, \cdots$, its derivative $\psi^{(n)}$ exists and $(-1)^n \psi^{(n)}(x) \geq 0$.

Definition 3: [16, (5.A.1)] Let B_1 and B_2 be two nonnegative random variables such that $\mathbf{E}[e^{-sB_1}] \geq \mathbf{E}[e^{-sB_2}]$, for all $s > 0$. Then B_1 is said to be smaller than B_2 in the Laplace transform order, denoted as $B_1 \leq_{LT} B_2$.

Lemma 6: [16, Th. 5.A.4] Let B_1 and B_2 be two nonnegative random variables. If $B_1 \leq_{LT} B_2$ then $\mathbf{E}[f(B_1)] \leq \mathbf{E}[f(B_2)]$, where the first derivative ψ of a differentiable function f on $[0, \infty)$ is completely monotone, provided that the expectations exist.

To prove (26), we let $B_1 = \sum_{i=2}^{n_T} \tilde{G}_i P_{V_i}$, $B_2 = \sum_{i=2}^{n_T} \tilde{G}_i P_{V_i}^*$ to invoke Lemma 6, where $P_{V_i}^*$ denotes the optimal value of P_{V_i}. It can be easily verified that $\psi(x)$, the first derivative of $f(x)$, satisfies Definition 2. More specifically, the nth derivative of ψ meets

$$\psi^{(n)}(x) = \begin{cases} \dfrac{n!}{(a+x)^{n+1}} - \dfrac{n!}{(b+x)^{n+1}} > 0, & \text{if } n \text{ is even,} \\[2mm] \dfrac{-n!}{(a+x)^{n+1}} + \dfrac{n!}{(b+x)^{n+1}} < 0, & \text{if } n \text{ is odd,} \end{cases} \tag{27}$$

when $x > 0$, since by definition, $b > a > 0$ when $R > 0$. Now from Lemma 6 and Definition 3, we know that to prove (26) is equivalent to proving $\mathbf{E}[e^{-sB_1}] \geq \mathbf{E}[e^{-sB_2}]$ or $\log(\mathbf{E}[e^{-sB_1}]/\mathbf{E}[e^{-sB_2}]) \geq 0, \forall s > 0$. From [17, p.40], we know that

$$\log\left(\frac{\mathbf{E}[e^{-sB_1}]}{\mathbf{E}[e^{-sB_2}]}\right) = \sum_{k=2}^{n_T} \log(1 + 2P_{V_k}^* s) - \sum_{k=2}^{n_T} \log(1 + 2P_{V_k} s). \tag{28}$$

To show the above is nonnegative, we resort to the majorization theory [18]. Note that $\sum_{k=2}^{n_T} \log(1 + 2\check{P}_{V_k} s)$ is a Schur-concave function in $(\check{P}_{V_2}, \ldots, \check{P}_{V_{n_T}})$, $\forall s > 0$, and by the definition of majorization

$$(P_{V_2}^*, \cdots, P_{V_{n_T}}^*) = \left(\frac{P_T - P_U - P_{V_1}}{n_T - 1}, \frac{P_T - P_U - P_{V_1}}{n_T - 1}, \cdots, \frac{P_T - P_U - P_{V_1}}{n_T - 1}\right) \prec (P_{V_2}, \cdots, P_{V_{n_T}}),$$

we know that the RHS of (28) is nonnegative, $\forall s > 0$. Then (26) is valid. From Lemma 2 and 5, we can conclude that

$$\mathbf{S}_{\mathbf{v}}^* = \left[\mathbf{h}/||\mathbf{h}||, \mathbf{h}^\perp/||\mathbf{h}||\right] diag\left(P_{V_1}, \frac{P_T - P_U - P_{V_1}}{n_T - 1}, \cdots, \frac{P_T - P_U - P_{V_1}}{n_T - 1}\right) \left[\mathbf{h}/||\mathbf{h}||, \mathbf{h}^\perp/||\mathbf{h}||\right]^H. \tag{29}$$

Then with the expansion

$$\frac{\mathbf{h}\mathbf{h}^H}{||\mathbf{h}||^2} + \frac{\mathbf{h}^\perp(\mathbf{h}^\perp)^H}{||\mathbf{h}||^2} = \mathbf{I},$$

we conclude the proof. ∎

After substituting the $\mathbf{S_u^*}$ from Theorem 2 and $\mathbf{S_v^*}$ from Lemma 5 into (7), we can get (8). Note that when the main channel is fast faded but perfectly known at transmitter, as [12], the achievable secrecy rate for this setting can be easily obtained from results in Theorem 1.

IV. The iterative algorithm for power allocations between signal and generalized artificial noise

Although we have simplified the optimization problem in (7) to (8), since (8) is a non-convex stochastic optimization problem, it is still difficult to analytically solve the optimal power allocation P_U, P_{V_1}, and P_{V_2} in (8). Thus in this section we propose an iterative power allocation algorithm summarized in Table I, which can find solutions almost the same as the brute-force search. However, the complexity of the proposed algorithm is much lower than the one based on brute-force search. More specifically, the brute force search requires searching on a plane for the three variables P_U, P_{V_1}, and P_{V_2}, simultaneously. However, the proposed algorithm divide the search into two sub-problems which costs much less complexity. Before introducing the iterative algorithm, we first provide a necessary condition in Theorem (3) for the optimal covariance matrix $\mathbf{S_v^*}$ of the GAN to be full rank. This condition will be useful to test the correctness of power allocation found in proposed algorithm.

First define

$$F_k(x) = \int_0^\infty \frac{xe^{-t}}{(1+xt)^k} dt = e^{1/x} E_k(1/x),$$

where $E_k(x)$ is the En-function [19].

Then we have the necessary condition in the following.

Theorem 3: The necessary condition for the power allocation (P_U, P_{V_1}, P_{V_2}) to be optimal for (8) is

$$
\frac{1}{1+||\mathbf{h}||^2 P_{V_1}} - \frac{1+||\mathbf{h}||^2 P_U}{1+||\mathbf{h}||^2(P_U+P_{V_1})} + \left(1+\frac{P_{V_2}}{P_{V_1}}\right) A_1 F_1(P_{V_1}) + A_2 F_2(P_{V_1})
$$

$$
+ \left(n_T - 1 + \frac{P_{V_1}}{P_{V_2}}\right) \sum_{k=1}^{n_T} \frac{B_k}{P_{V_2}} F_k(P_{V_2}) - \frac{P_{V_1}}{P_{V_2}} B_{n_T} F_{n_T}(P_{V_2}) - (P_{V_1} + (n_T-1)P_{V_2}) \frac{A_1^{'}}{P_U+P_{V_1}} F_1(P_U+P_{V_1})
$$

$$
- \frac{P_{V_1} A_2^{'}}{P_U+P_{V_1}} F_2(P_U+P_{V_1}) - \left(n_T - 1 + \frac{P_{V_1}}{P_{V_2}}\right) \sum_{k=1}^{n_T} B_k^{'} F_k(P_{V_2}) + \frac{P_{V_1}}{P_{V_2}} B_{n_T}^{'} F_{n_T}(P_{V_2}) \gtreqless 0, \tag{30}
$$

then

$$
\left(\frac{A_1}{P_{V_1}} F_1(P_{V_1}) + \frac{A_2}{P_{V_1}} F_2(P_{V_1})\right) + \sum_{k=1}^{n_T-1} \frac{B_k}{P_{V_2}} F_k(P_{V_2}) - \frac{A_1^{'}}{P_U+P_{V_1}} F_1(P_U+P_{V_1}) - \frac{A_2^{'}}{P_U+P_{V_1}} F_2(P_U+P_{V_1})
$$

$$
- \sum_{k=1}^{n_T-1} \frac{B_k^{'}}{P_{V_2}} F_k(P_{V_2}) \gtreqless \frac{||\mathbf{h}||^4 P_U}{\left(1+||\mathbf{h}||^2 P_{V_1}\right)\left(1+||\mathbf{h}||^2 (P_U+P_{V_1})\right)}, \tag{31}
$$

where

$$
A_1 = \frac{1-n_T}{\left(1-\frac{P_{V_2}}{P_{V_1}}\right)^{n_T}} \frac{P_{V_2}}{P_{V_1}}, \quad A_2 = \frac{1}{\left(1-\frac{P_{V_2}}{P_{V_1}}\right)^{n_T-1}}, \quad B_k = \frac{(n_T-k)\left(-\frac{P_{V_1}}{P_{V_2}}\right)^{n_T-1-k}}{\left(1-\frac{P_{V_2}}{P_{V_1}}\right)^{n_T-k+1}},
$$

$$
A_1^{'} = \frac{1-n_T}{\left(1-\frac{P_{V_2}}{P_U+P_{V_1}}\right)^{n_T}} \frac{P_U+P_{V_1}}{P_{V_2}}, \quad A_2^{'} = \frac{1}{\left(1-\frac{P_{V_2}}{P_U+P_{V_1}}\right)^{n_T-1}}, \quad B_k^{'} = \frac{(n_T-k)\left(-\frac{P_U+P_{V_1}}{P_{V_2}}\right)^{n_T-1-k}}{\left(1-\frac{P_{V_2}}{P_U+P_{V_1}}\right)^{n_T-k+1}}, \tag{32}
$$

with the requirement $P_{V_1} > 0$.

Now we present the derivation for the proposed iterative algorithm. The key idea of the proposed algorithm is as following. To prevent the high complexity of simultaneously solving P_U, P_{V_1}, and P_{V_2}, we try to divide the problem as smaller ones and we can simply use bisection method to solve them. More specifically, we start from the KKT conditions, by eliminating the Lagrange multipliers, we form two equations each has different variables to solve. Then iteratively solve these two equations, we can find the power allocation. With the Lagrange multipliers $\lambda \geq 0$, $\mu \geq 0$, $\mu_1 \geq 0$, and $\mu_2 \geq 0$, by the KKT

conditions of (8), we then have

$$g_1 \triangleq \frac{||\mathbf{h}||^2}{1+||\mathbf{h}||^2\left(P_U^* + P_{V_1}^*\right)} - \mathbf{E}\left[\frac{\tilde{G}_1}{1+(P_U^* + P_{V_1}^*)\tilde{G}_1 + P_{V_2}\sum_{i=2}^{n_T}\tilde{G}_i}\right] - \lambda + \mu = 0, \tag{33}$$

$$g_2 \triangleq \frac{||\mathbf{h}||^2}{1+||\mathbf{h}||^2\left(P_U^* + P_{V_1}^*\right)} - \frac{||\mathbf{h}||^2}{1+||\mathbf{h}||^2 P_{V_1}^*}$$

$$- \mathbf{E}\left[\frac{\tilde{G}_1}{1+(P_U^* + P_{V_1}^*)\tilde{G}_1 + P_{V_2}\sum_{i=2}^{n_T}\tilde{G}_i}\right] + \mathbf{E}\left[\frac{\tilde{G}_1}{1+P_{V_1}^*\tilde{G}_1 + P_{V_2}^*\sum_{i=2}^{n_T}\tilde{G}_i}\right] - \lambda + \mu_1 = 0, \tag{34}$$

$$g_3 \triangleq -\mathbf{E}\left[\frac{\sum_{i=2}^{n_T}\tilde{G}_i}{1+(P_U^* + P_{V_1}^*)\tilde{G}_1 + P_{V_2}^*\sum_{i=2}^{n_T}\tilde{G}_i}\right] + \mathbf{E}\left[\frac{\sum_{i=2}^{n_T}\tilde{G}_i}{1+P_{V_1}^*\tilde{G}_1 + P_{V_2}^*\sum_{i=2}^{n_T}\tilde{G}_i}\right] - (n_T-1)\lambda + \mu_2 = 0, \tag{35}$$

$$\mu P_U^* = 0, \tag{36}$$

$$\mu_1 P_{V_1}^* = 0, \tag{37}$$

$$\mu_2 P_{V_2}^* = 0. \tag{38}$$

Assume that P_U^*, $P_{V_1}^*$, and $P_{V_2}^*$ are all non-zeros. Combining (33), (34), (36), and (37) we have

$$f_1(P_{V_1}^*, P_{V_2}^*) \triangleq \frac{P_U^* P_{V_1}^* g_1 - P_U^* P_{V_1}^* g_2}{P_U^* P_{V_1}^*} = \frac{||\mathbf{h}||^2}{1+||\mathbf{h}||^2 P_{V_1}^*} - \mathbf{E}\left[\frac{\tilde{G}_1}{1+P_{V_1}^*\tilde{G}_1 + P_{V_2}^*\sum_{i=2}^{n_T}\tilde{G}_i}\right] = 0. \tag{39}$$

Similarly, combining (33), (35), (36), and (38), and using the fact that

$$\mathbf{E}\left[\frac{\sum_{i=2}^{n_T}\tilde{G}_i}{1+P_{V_1}^*\tilde{G}_1 + P_{V_2}^*\sum_{i=2}^{n_T}\tilde{G}_i}\right] = (n_T-1)\mathbf{E}\left[\frac{\tilde{G}_2}{1+P_{V_1}^*\tilde{G}_1 + P_{V_2}^*\sum_{i=2}^{n_T}\tilde{G}_i}\right], \tag{40}$$

since the channel gain of each antenna is independent and identically distributed (i.i.d.), we have

$$f_2(P_U^*, P_{V_1}^*, P_{V_2}^*) \triangleq \frac{P_U^* P_{V_2}^* g_1 - P_U^* P_{V_2}^* \frac{1}{n_T-1}g_3}{P_U^* P_{V_2}^*}$$

$$= \frac{||\mathbf{h}||^2}{1+||\mathbf{h}||^2\left(P_U^* + P_{V_1}^*\right)} - \mathbf{E}\left[\frac{\tilde{G}_1}{1+(P_U^* + P_{V_1}^*)\tilde{G}_1 + P_{V_2}^*\sum_{i=2}^{n_T}\tilde{G}_i}\right]$$

$$+ \mathbf{E}\left[\frac{\tilde{G}_2}{1+(P_U^* + P_{V_1}^*)\tilde{G}_1 + P_{V_2}^*\sum_{i=2}^{n_T}\tilde{G}_i}\right] - \mathbf{E}\left[\frac{\tilde{G}_2}{1+P_{V_1}^*\tilde{G}_1 + P_{V_2}^*\sum_{i=2}^{n_T}\tilde{G}_i}\right] = 0. \tag{41}$$

Now for the ith iteration, with a given $P_{V_1}^{(i)}$, we can find new (P_U, P_{V_2}) such that $f_2(P_U, P_{V_1}^{(i)}, P_{V_2}) = 0$ according to (41). We can set $P_U = (P_T - P_{V_2} - P_{V_1}^{(i)})/(n_T - 1)$ then $f_2(P_U, P_{V_1}, P_{V_2})$ becomes a function with only one variable P_{V_2}. We let the resulted P_{V_2} as $P_{V_2}^{(i+1)}$. Then with a given $P_{V_2}^{(i+1)}$, we can numerically solve a new P_{V_1} such that $f_1(P_{V_1}, P_{V_2}^{(i+1)}) = 0$ according to (39). We let the resulted P_{V_1} as $P_{V_1}^{(i+1)}$ and the iterative algorithm follows. The bisection method can be used to perform the numerical search.

Based on the concept described above, we explain each step in Table I in detail. First, numerically finding the tuple (P_{V_1}, P_{V_2}, P_U) which exactly meet the equality (39) (or (41)) is very hard. Therefore we relax (39) and (41) by inequalities

$$|f_1(P_{V_1}, P_{V_2})| < \varepsilon_1 \text{ and } |f_2(P_U, P_{V_1}, P_{V_2})| < \varepsilon_1, \tag{42}$$

respectively, where ε_1 is a small constant. Once the values from the bisection search validate the above inequalities, they are treated as the solutions of these inequalities. Together with the iteration step described in the end of the previous paragraph, we obtain Step 2 and 3 in Table I. Second, relaxing equalities (39) and (41) to inequalities (42) make solutions obtained depend on ε_1 and may not satisfy the KKT conditions. Also the expectations in functions f_1 and f_2 ((39) and (41)) are calculated numerically via generation of the channel realizations. Thus as in Step 4 of Table I, we use the analytical results in Theorem 3 to verify the correctness of the solutions. Finally, the initial values for the first iteration in Step 1 are as follows. Note that two initial values are needed for specifying the search region of the bisection method. For initializing Step 2, the two initial values for P_U are 0 and $P_T - P_{V_1}^{(i)}$, such that the corresponding values of function f_2 will have opposite signs. And there exists at least one solution in the interval $[0, P_T - P_{V_1}^{(i)}]$. By the same reason, for initializing Step 3, the two initial values for $P_{V_1}^{(i)}$ are 0 and $P_T - P_{V_2}(n_T - 1)$. In the ith iteration, the search regions are $[0, P_T - P_{V_1}^{(i)}]$ and $[0, P_T - (n_T - 1)P_{V_2}^{(i)}]$ for f_2 and f_1, respectively.

However, the bisection method may not always work for searching solutions for $|f_2| < \varepsilon_1$ in Step 2 of Table I. Note that for the initial value $P_U = P_T - P_{V_1}^{(i)}$, $f_2(P_T - P_{V_1}^{(i)}, P_{V_1}^{(i)}, 0) < 0$ given $P_{V_1}^{(i)}$. On the other hand, given $P_{V_1}^{(i)}$, there exist two cases for f_2 at initial value $P_U = 0$: one is that $f_2(0, P_{V_1}^{(i)}, P_{V_2}^{(i)}) < 0$ as depicted in Figure 2 (a), and the other is $f_2(0, P_{V_1}^{(i)}, P_{V_2}^{(i)}) > 0$ as depicted in Figure 2 (b). In the later case, the bisection method works. However, if the former case happens, the function values have the same sign,

and the bisection method does not work. To solve this problem, we can use the *golden section method* [20], which is a technique for finding the maximum in the interval $[0, P_T - P_{V_1}^{(i)}]$, i.e., to numerically find $\tilde{P}_U$ first such that given $P_{V_1}^{(i)}$, $f_2(\tilde{P}_U, P_{V_1}^{(i)}, P_{V_2}^{(i)})$ is positive. After that we can follow the step 2 in Table I to solve P_U in the interval $[\tilde{P}_U, P_T - P_{V_1}^{(i)}]$. If the maximum of $f_2(P_U, P_{V_1}^{(i)}, P_{V_2}^{(i)})$ in the interval $[0, P_T - P_{V_1}^{(i)}]$ is still negative, we know that there does not exist any P_U in this interval such that $f_2(P_U, P_{V_1}^{(i)}, P_{V_2}^{(i)}) = 0$ given $P_{V_1}^{(i)}$. In this case, we set $P_U = 0$ as the solution of $f_2(P_U, P_{V_1}^{(i)}, P_{V_2}^{(i)}) = 0$ given $P_{V_1}^{(i)}$. From simulation results, according to the iterative algorithm in Table I, the power $P_U^{(i)}$, $P_{V_1}^{(i)}$, and $P_{V_2}^{(i)}$ will converge to the optimal solution P_U^*, $P_{V_1}^*$, and $P_{V_2}^*$, respectively, which satisfy the KKT necessary conditions.

Remark 1: Note that in Section IV we assume that P_U, P_{V_1}, and P_{V_2} are all non-zeros to eliminate the multipliers. For channel conditions under which low rank AN covariance matrix is optimal, the proposed algorithm may have P_{V_1} converge to a value approximately zero. When this value is smaller than a predefined threshold ε_2, we claim that $P_{V_1} = 0$ is optimal.

V. SIMULATION RESULTS

In this section, we illustrate the performance gain of the proposed transmission scheme over Goel and Negi's scheme. We use a 2 by 1 by 1 channel as an example. Assume that the noise variances of Bob and Eve are normalized to 1. From (8) we know that the rate R_{GAN} only depends on the norm of the main channel. Therefore, we use $||\mathbf{h}||^2 = 0.05, 0.1$, and 0.2 to indicate different channel conditions in the simulation. For the statistics of the eavesdropper's channel, we set $\mathbf{E}[\tilde{G}_1] = \mathbf{E}[\tilde{G}_2] = 1$. In Fig. 3, 4, and 5, which correspond to $||\mathbf{h}||^2 = 0.05, 0.1$, and 0.2, respectively, we compare the rates of Goel and Negi's scheme to that of our proposed signaling with the generalized AN. The blue and black curves represent searching the optimal power allocations exhaustively and by the proposed iterative algorithm, respectively. In the iterative algorithm, we set the iteration number *MAXIT* as 20, *MAXCheck* as 5, and $\varepsilon_1 = \varepsilon_2 = 10^{-5}$. From Fig. 3, 4, and 5, we can easily see that the proposed generalized AN scheme indeed provides apparent rate gains over Goel and Negi's scheme in the moderate SNR regions. In addition, we can observe that the rate gains decrease with increasing $||\mathbf{h}||^2$, which is consistent with the results in [12]. We can also find that the value of P_T which provides the largest rate gain also decreases with increasing

$||\mathbf{h}||^2$. This is because AN in the signal direction provides much more rate gains when Bob's received SNR is relatively small compared to Eve's. Furthermore, the power allocations of the proposed iterative algorithm indeed converges to those by exhaustive search. In and Fig. 6 we show the convergence rate of the proposed algorithm under $||\mathbf{h}||^2 = 0.1$ with different P_T. It can be found that the proposed algorithm converges fast under different P_T, i.e., it costs at most 7 iterations to the final value, which verifies the complexity of solving the power allocation is much lower than the full search.

As another example, we also illustrate the optimal power allocation among P_U, P_{V_1}, and P_{V_2} under $||\mathbf{h}||^2 = 0.05$ in Fig. 7. It can be easily seen that as the received SNR increases, the power allocated to P_{V_1} decreases and the rate gain over Goel and Negi's scheme also decreases.

VI. CONCLUSION

In this paper we generalized Goel and Negi's artificial noise (AN) for fast fading secure transmission with full knowledge of the main channel and only the statistics of the eavesdropper's channel state information at the transmitter. Instead of transmitting AN in the null space of the legitimate channel, we considered injecting AN in all directions, including the direction for conveying the dedicated messages. Our main result provides a highly simplified power allocation problem to describe the ergodic secrecy rate. To attain it, we proved that for a multiple-input single-output single-antenna-eavesdropper system with the proposed AN injecting scheme, the optimal transmission scheme is a beamformer which is aligned to the direction of the legitimate channel. In addition, we provided the necessary condition for the optimal covariance matrix of AN to be full rank. After characterizing the optimal eigenvectors of the covariance matrices of signal and AN, we also developed an algorithm to efficiently solve the non-convex power allocation problem. Through simulations, we verified that the proposed scheme outperforms Goel and Negi's AN scheme under certain channel conditions, especially when the legitimate channel is poor.

VII. APPENDIX

Before proving Theorem 3, we first introduce the following lemma which will be used.

Lemma 7: Given $\mathbf{D}_1 \succ \mathbf{D}_2$,

$$\mathbf{Y} \triangleq \mathbf{E}\left[\frac{\mathbf{g}\mathbf{g}^H}{1+\mathbf{g}^H\mathbf{D}_2^H\mathbf{g}}\right] - \mathbf{E}\left[\frac{\mathbf{g}\mathbf{g}^H}{1+\mathbf{g}^H\mathbf{D}_1^H\mathbf{g}}\right] \succ 0. \tag{43}$$

Proof: We first write the expectation in (43) in the following integral,

$$\mathbf{Y}_{1,1} = \int_0^\infty e^{-t}\frac{1}{(1+P_{V_1}t)^2}\frac{1}{(1+P_{V_2}t)^{n_T-1}}dt - \int_0^\infty e^{-t}\frac{1}{(1+(P_U+P_{V_1})t)^2}\frac{1}{(1+P_{V_2}t)^{n_T-1}}dt$$

$$= \int_0^\infty e^{-t}\left(\frac{1}{(1+P_{V_1}t)^2} - \frac{1}{(1+(P_U+P_{V_1})t)^2}\right)\frac{1}{(1+P_{V_2}t)^{n_T-1}}dt > 0, \tag{44}$$

and

$$\mathbf{Y}_{i,i} = \int_0^\infty e^{-t}\frac{1}{1+P_{V_1}t}\frac{1}{(1+P_{V_2}t)^{n_T}}dt - \int_0^\infty e^{-t}\frac{1}{1+(P_U+P_{V_1})t}\frac{1}{(1+P_{V_2}t)^{n_T}}dt$$

$$= \int_0^\infty e^{-t}\left(\frac{1}{1+P_{V_1}t} - \frac{1}{1+(P_U+P_{V_1})t}\right)\frac{1}{(1+P_{V_2}t)^{n_T}}dt > 0, \tag{45}$$

for $i = 2, 3, \ldots, n_T$, and from [13, Lemma 4], we know that the non-diagonal entries of both the first and second terms of $\mathbf{Y}$ in (7) are zeros, then $\mathbf{Y}_{i,j} = 0$ for $i \neq j$. Therefore, we know that $\mathbf{Y}$ is a diagonal matrix and each diagonal entry from (44) and (45) is larger than zero, which completes the proof. ∎

We now provide the proof of Theorem 3

Proof: We first rearrange (16) as

$$\mathbf{\Theta}_2 = \mathbf{C} - \lambda\mathbf{I}_{n_T} + \boldsymbol{\psi}_{\mathbf{v}}^T = \mathbf{0},$$

where

$$\mathbf{C} \triangleq \mathbf{U}\mathbf{Y}\mathbf{U}^H - \mathbf{c}\mathbf{c}^H, \tag{46}$$

$$\mathbf{Y} \triangleq \mathbf{E}\left[\frac{\mathbf{U}^H\mathbf{g}\mathbf{g}^H\mathbf{U}}{1+\mathbf{g}^H\mathbf{U}\mathbf{D}_2\mathbf{U}^H\mathbf{g}}\right] - \mathbf{E}\left[\frac{\mathbf{U}^H\mathbf{g}\mathbf{g}^H\mathbf{U}}{1+\mathbf{g}^H\mathbf{U}\mathbf{D}_1\mathbf{U}^H\mathbf{g}}\right] = \mathbf{E}\left[\frac{\mathbf{g}\mathbf{g}^H}{1+\mathbf{g}^H\mathbf{D}_2^H\mathbf{g}}\right] - \mathbf{E}\left[\frac{\mathbf{g}\mathbf{g}^H}{1+\mathbf{g}^H\mathbf{D}_1^H\mathbf{g}}\right], \tag{47}$$

$$\mathbf{c} \triangleq \left(\frac{\mathbf{h}^H\mathbf{S}_{\mathbf{u}}\mathbf{h}}{(1+\mathbf{h}^H\mathbf{S}_{\mathbf{v}}^*\mathbf{h})(1+\mathbf{h}^H(\mathbf{S}_{\mathbf{u}}+\mathbf{S}_{\mathbf{v}}^*)\mathbf{h})}\right)^{1/2}\mathbf{h}. \tag{48}$$

Similar to (23), we have

$$\mathbf{\Lambda}_{\mathbf{C}}\mathbf{\Lambda}_{\mathbf{S}_{\mathbf{v}}^*} = \mathbf{\Lambda}_{\mathbf{S}_{\mathbf{v}}^*}\mathbf{\Lambda}_{\mathbf{C}} = \mathrm{tr}(\mathbf{C}\mathbf{S}_{\mathbf{v}}^*)\mathbf{\Lambda}_{\mathbf{S}_{\mathbf{v}}^*}. \tag{49}$$

And we know that the necessary condition for the optimal AN to be full rank is that when $\mathrm{tr}(\mathbf{C}\mathbf{S}_{\mathbf{v}}^*) > 0$, $\mathbf{C}$ does not have any negative eigenvalues; or, when $\mathrm{tr}(\mathbf{C}\mathbf{S}_{\mathbf{v}}^*) < 0$, $\mathbf{C}$ does not have any positive eigenvalues.

To verify this property, we resort to the fact from [13, Lemma 5] that if all eigenvalues λ of $\mathbf{a}\mathbf{a}^H - \mathbf{A}$ are negative, then $l(0) > 0$, where $l(\lambda)$ is defined as,

$$l(\lambda) \triangleq 1 - \mathbf{a}^H \left(\mathbf{A} + \lambda \mathbf{I}_{n_T}\right)^{-1} \mathbf{a}, \tag{50}$$

and $\mathbf{A} \succ 0$. Note that $l(\lambda)$ is a strictly increasing function when $\lambda > 0$. Note also that $\mathbf{C}$ in (46) is negated of $\mathbf{a}\mathbf{a}^H - \mathbf{A}$. Thus all eigenvalues of $\mathbf{C}$ are positive implies $l(0) > 0$. Thus by substituting $\mathbf{c}$ and $\mathbf{U}\mathbf{Y}\mathbf{U}^H$ into $\mathbf{a}$ and $\mathbf{A}$, respectively, we have

$$l(\lambda) = 1 - \mathbf{c}^H \left(\mathbf{U}\mathbf{Y}\mathbf{U}^H + \lambda \mathbf{I}_{n_T}\right)^{-1} \mathbf{c}. \tag{51}$$

By Lemma 7 we know $\left(\mathbf{U}\mathbf{Y}\mathbf{U}^H\right)^{-1}$ exists. Then we can expand $l(0) > 0$ from (51) as

$$1 > \mathbf{c}^H \left(\mathbf{U}\mathbf{Y}\mathbf{U}^H\right)^{-1} \mathbf{c}. \tag{52}$$

Then after substituting $\mathbf{c}$ from (48) to (52), and using Theorem 2 and Lemma 2, we have

$$\left[\mathbf{Y}^{-1}\right]_{1,1} < \frac{\left(1 + ||\mathbf{h}||^2 P_{V_1}\right)\left(1 + ||\mathbf{h}||^2 \left(P_U + P_{V_1}\right)\right)}{||\mathbf{h}||^4 P_U}.$$

From [13, Lemma 4] we know that $\mathbf{Y}$ is diagonal. In addition, with $\mathbf{Y}$ is invertible from the proof of Lemma 7, we can further rearrange the above as

$$\left[\mathbf{Y}\right]_{1,1} > \frac{||\mathbf{h}||^4 P_U}{\left(1 + ||\mathbf{h}||^2 P_{V_1}\right)\left(1 + ||\mathbf{h}||^2 \left(P_U + P_{V_1}\right)\right)}.$$

Then by the definition of $\mathbf{Y}$ in (47), and the fractional expansion, we can further express the above as

$$\left(\frac{A_1}{P_{V_1}} F_1(P_{V_1}) + \frac{A_2}{P_{V_1}} F_2(P_{V_1})\right) \mathbf{1}_{P_{V_1} \neq 0} + \sum_{k=1}^{n_T - 1} \frac{B_k}{P_{V_2}} F_k(P_{V_2}) - \frac{A_1'}{P_U + P_{V_1}} F_1(P_U + P_{V_1}) - \frac{A_2'}{P_U + P_{V_1}} F_2(P_U + P_{V_1})$$

$$- \sum_{k=1}^{n_T - 1} \frac{B_k'}{P_{V_2}} F_k(P_{V_2}) > \frac{||\mathbf{h}||^4 P_U}{\left(1 + ||\mathbf{h}||^2 P_{V_1}\right)\left(1 + ||\mathbf{h}||^2 \left(P_U + P_{V_1}\right)\right)}, \tag{53}$$

where $A_1, A_2, A_1', A_2', B_k,$ and B_k' for $k = 1, 2, \ldots, n_T - 1$ are defined in the statement of the theorem. In addition, $\mathrm{tr}(\mathbf{C}\mathbf{S}_{\mathbf{v}}^*) > 0$ implies

$$\frac{1}{1 + ||\mathbf{h}||^2 P_{V_1}} - \frac{1 + ||\mathbf{h}||^2 P_U}{1 + ||\mathbf{h}||^2 (P_U + P_{V_1})} + \mathbf{E}\left[\frac{1 + \mathbf{g}^H(\mathbf{D}_1 - \mathbf{D}_2)\mathbf{g}}{1 + \mathbf{g}^H \mathbf{D}_1 \mathbf{g}}\right] - \mathbf{E}\left[\frac{1}{1 + \mathbf{g}^H \mathbf{D}_2 \mathbf{g}}\right] > 0. \tag{54}$$

After some arrangement, (54) can be further represented by

$$\frac{1}{1+||\mathbf{h}||^2 P_{V_1}} - \frac{1+||\mathbf{h}||^2 P_U}{1+||\mathbf{h}||^2(P_U+P_{V_1})} + \left(1+\frac{P_{V_2}}{P_{V_1}}\right)A_1 F_1(P_{V_1}) + A_2 F_2(P_{V_1}) + \left(n_T - 1 + \frac{P_{V_1}}{P_{V_2}}\right)\sum_{k=1}^{n_T}\frac{B_k}{P_{V_2}}F_k(P_{V_2})$$

$$-\frac{P_{V_1}}{P_{V_2}}B_{n_T}F_{n_T}(P_{V_2}) - (P_{V_1}+(n_T-1)P_{V_2})\frac{A_1^{'}}{P_U+P_{V_1}}F_1(P_U+P_{V_1}) - \frac{P_{V_1}A_2^{'}}{P_U+P_{V_1}}F_2(P_U+P_{V_1})$$

$$-\left(n_T - 1 + \frac{P_{V_1}}{P_{V_2}}\right)\sum_{k=1}^{n_T}B_k^{'}F_k(P_{V_2}) + \frac{P_{V_1}}{P_{V_2}}B_{n_T}^{'}F_{n_T}(P_{V_2}) > 0. \tag{55}$$

$\blacksquare$

REFERENCES

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

[2] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

[3] X. Zhou, R. K. Ganti, and J. G. Andews, "Secure wireless network connectivity with multi-antenna transmission," vol. 10, no. 2, pp. 425–430, Feb. 2011.

[4] S. Shafiee and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: the 2-2-1 channel," *IEEE Trans. Inform. Theory*, vol. 55, no. 9, pp. 4033–4039, Sept. 2009.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-II: The MIMOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov 2010.

[6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inform. Theory*, vol. 57, no. 8, Aug. 2011.

[7] T. Liu and S. S. (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[8] Y. Liang, V. Poor, and S. S. (Shitz), "Secure communication over fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

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

[10] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[11] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-I: The MISOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[12] Z. Li, R. Yates, and W. Trappe, "Achieving secret communication for fast Rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 9, pp. 2792 – 2799, Sep. 2010.

[13] J. Li and A. Petropulu, "On ergodic secrecy rate for Gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176–1187, Apr. 2011.

[14] S. C. Lin and P. H. Lin, "On ergodic secrecy capacity of multiple input wiretap channel with statistical CSIT," *http://arxiv.org/abs/1201.2868*, Jan. 2012.

[15] R. A. Horn and C. R. Johnson, *Matrix analysis*. Cambridger University Press, 1985.

[16] M. Shaked and J. G. Shanthikumar, *Stochastic Orders*. Springer, 2007.

[17] A. M. Mathai and S. B. Provost, *Quadratic forms in random variables*. Marcel Dekker, New York, 1992.

[18] A. W. Marshall and I. Olkin, *Inequalities: theory of majorization and its application*.

[19] M. M. Abramowitz and I. A. I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*. New York: Dover, 1972.

[20] M. T. Heath, *Scientific computing: an introductory survey*, 2nd ed. McGraw-Hill.

TABLE I

THE ITERATIVE ALGORITHM FOR POWER ALLOCATION BETWEEN SIGNAL AND GENERALIZED AN

Step 1   Set $i = 0$, $P_{V_1}^{(0)} = 0$, and initialize search region for the bisection method.

Step 2   Given $P_{V_1}^{(i)}$ and the total power constraint (6), find P_{V_2} (and thus $P_U = (P_T - P_{V_2} - P_{V_1}^{(i)})/(n_T - 1)$)

        such that $|f_2(P_U, P_{V_1}^{(i)}, P_{V_2})| < \varepsilon_1$, where f_2 is defined in (41).

        Set $P_{V_2}^{(i+1)} = P_{V_2}$

Step 3   Given $P_{V_2}^{(i+1)}$ and the total power constraint (6), find P_{V_1}

        such that $|f_1(P_{V_1}, P_{V_2}^{(i+1)})| < \varepsilon_1$, where f_1 is defined in (39)

        Set $P_{V_1}^{(i+1)} = P_{V_1}$.

Step 4   Let $i = i+1$ and repeat Step 2 to Step 3 until *MAXIT*.

Step 5   Check the whether the final power allocations meet Theorem 3.

        If not, randomly re-initialize $P_{V_1}^{(0)}$ and run Step 1-4 until *MAXCheck*.
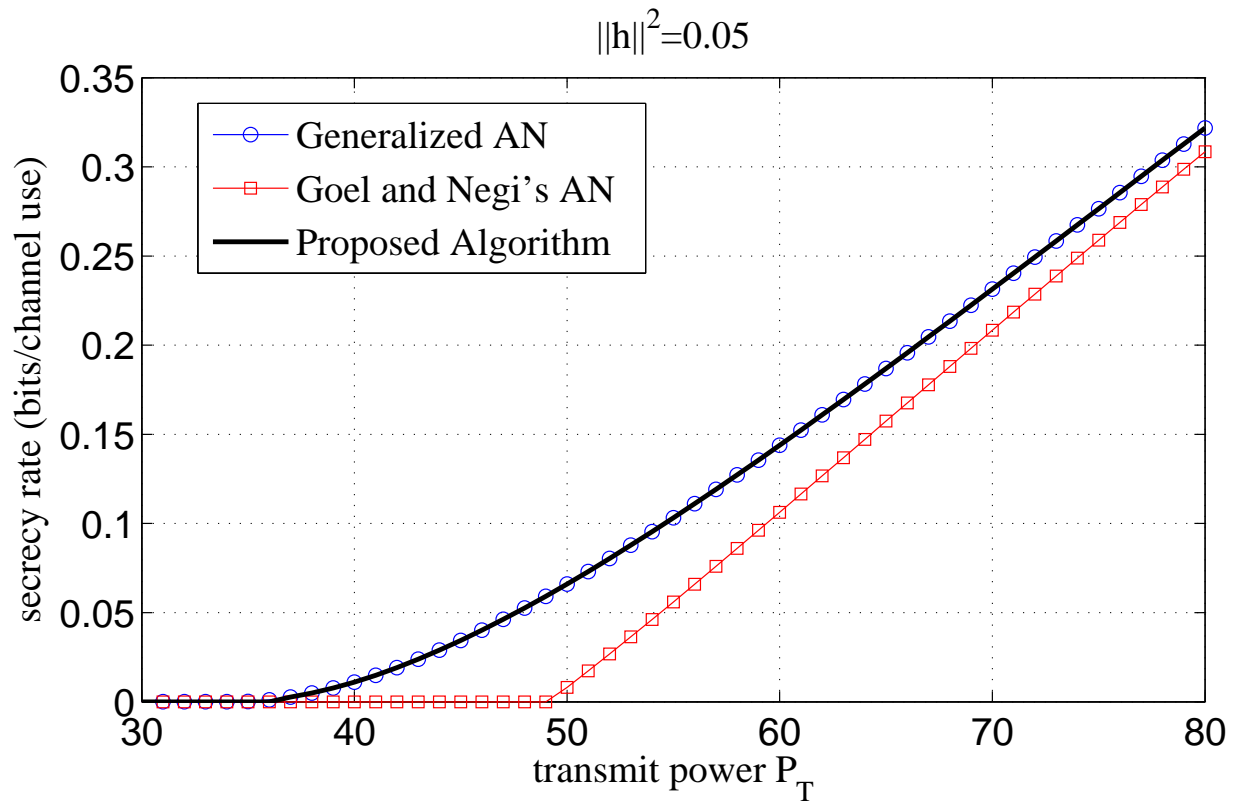
Fig. 1.   System model.

Fig. 2.   Characteristic of $f_2(P_U, P_{V_1}, P_{V_2})$ given P_{V_1}.

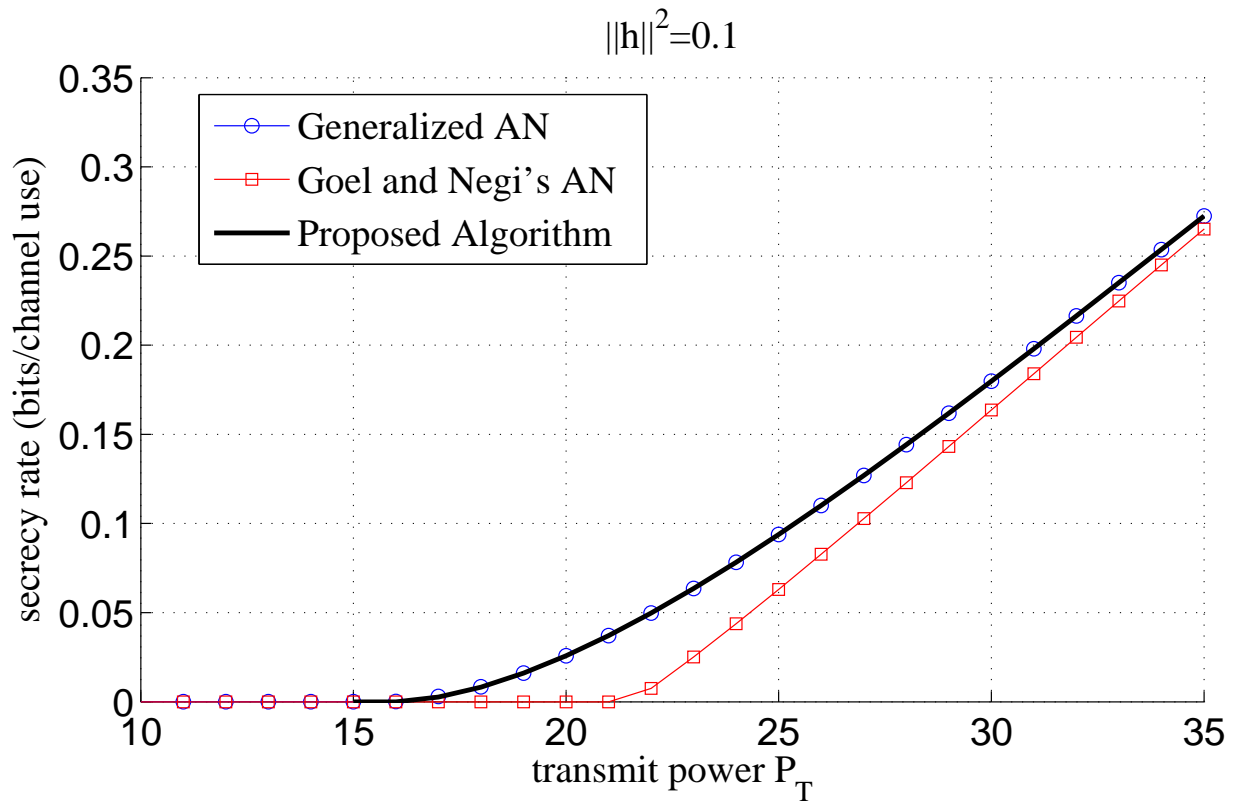Fig. 3.   Secrecy rate versus transmit power under $||\mathbf{h}||^2 = 0.05$.

Fig. 4.   Secrecy rate versus transmit power under $||\mathbf{h}||^2 = 0.1$.
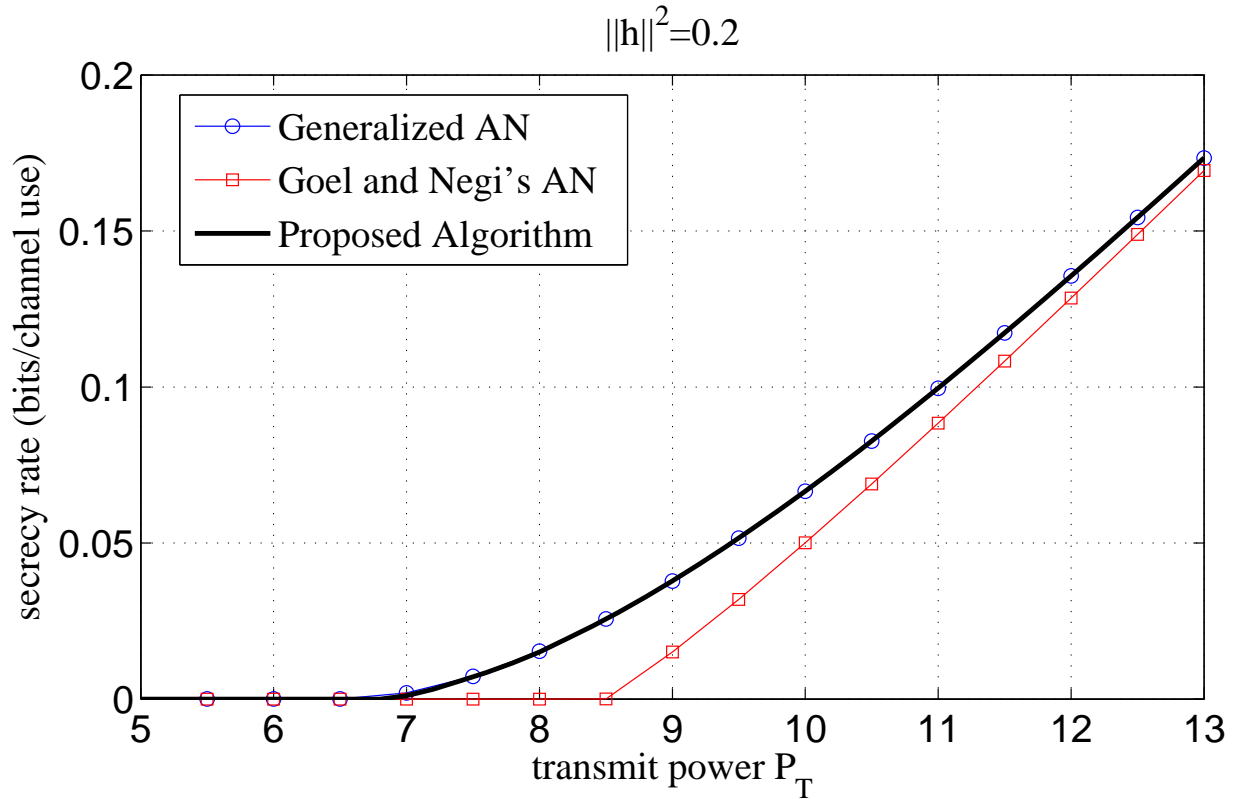

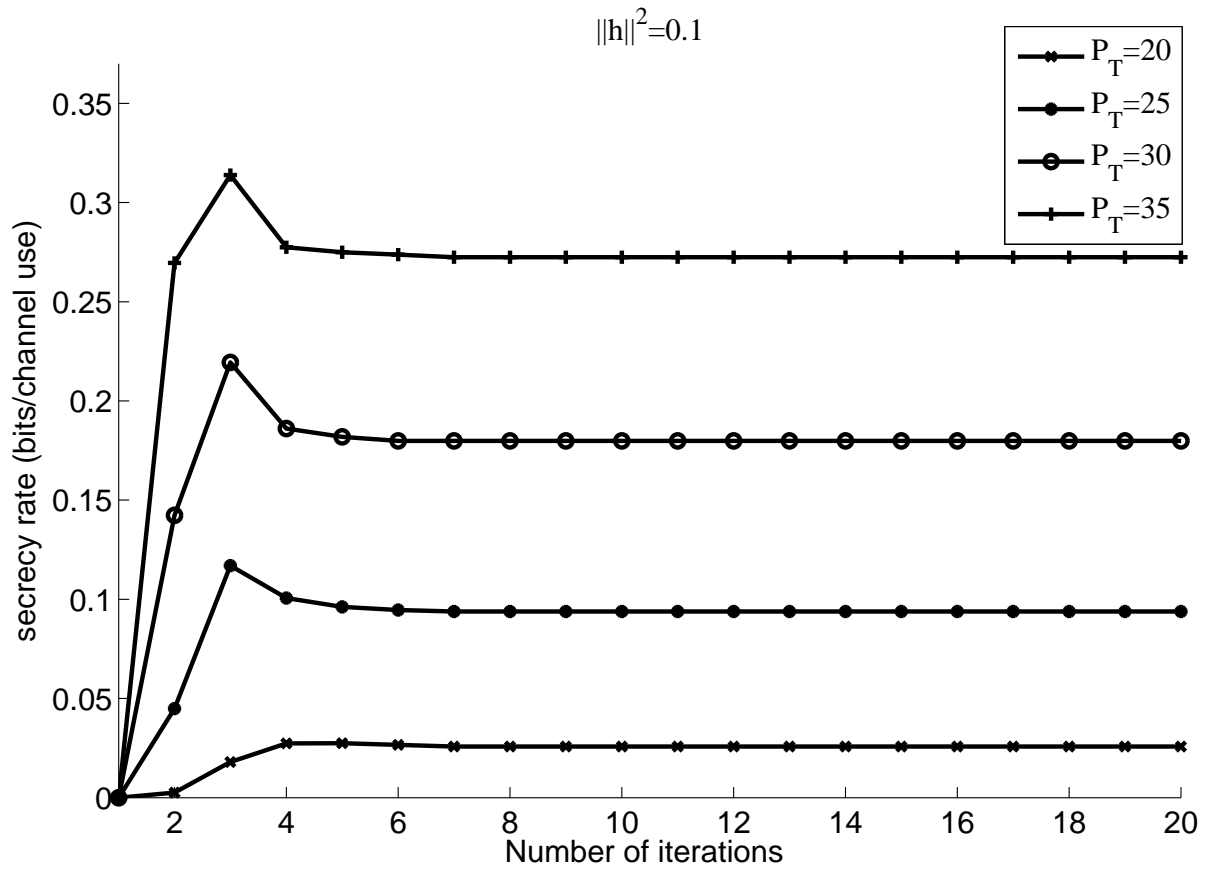Fig. 5.   Secrecy rate versus transmit power under $||\mathbf{h}||^2 = 0.2$.

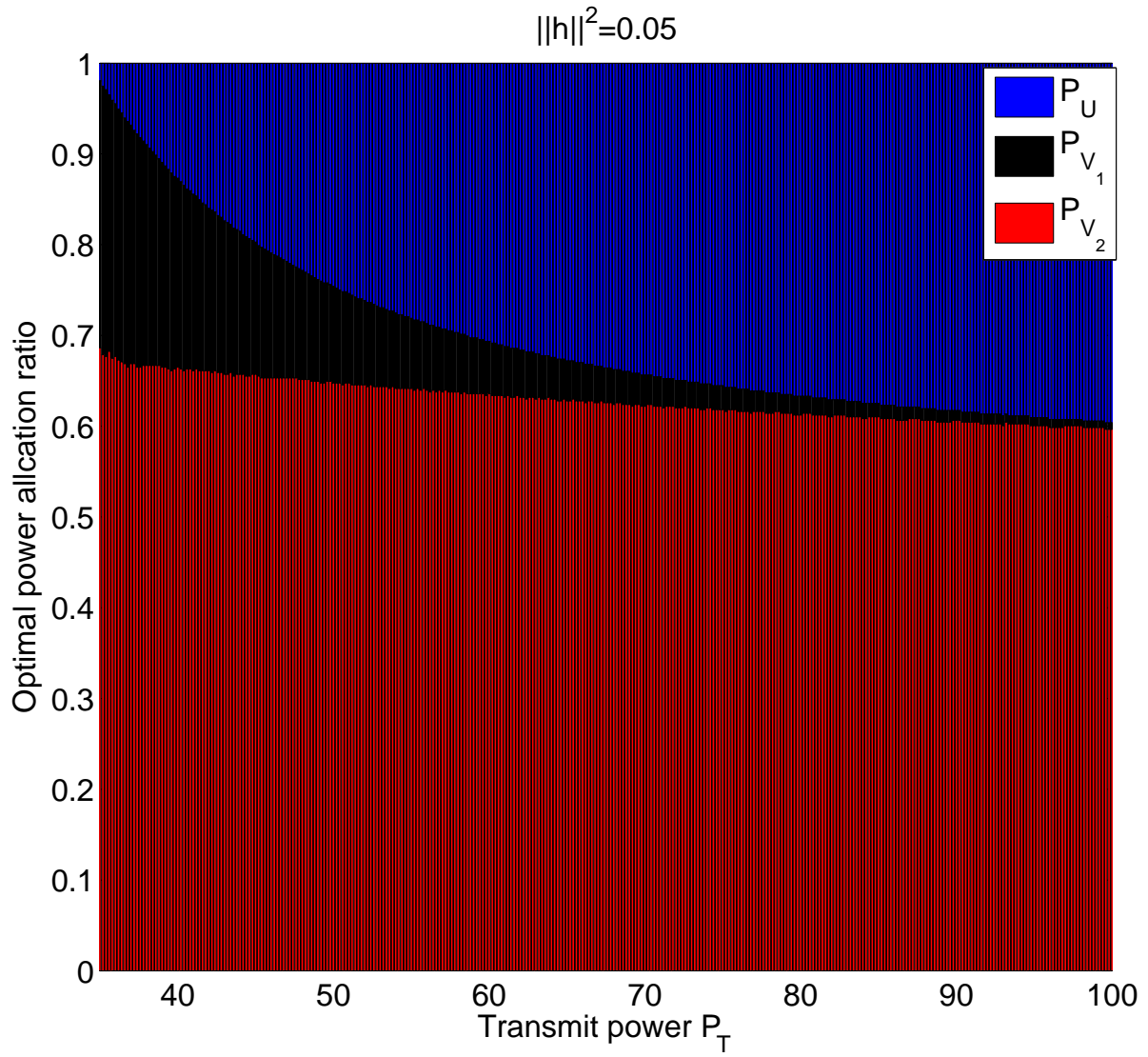Fig. 6.   Secrecy rate versus the number of iteration under $||\mathbf{h}||^2 = 0.1$.

Fig. 7.   Power allocation among P_U, P_{V_1}, and P_{V_2} under $||\mathbf{h}||^2 = 0.05$.