Optimal Analysis of Joint Masked-Beamforming in Secure Wireless Communication

Yongkai Zhou
Department of Electronic Engineering
Shanghai Jiaotong University
Shanghai, China
Email: ssmailzyk@sjtu.edu.cn

Yan Zhu, Fangbiao Li
Department of Electronic Engineering
Shanghai Jiaotong University
Shanghai, China
Email: {topbestzy, flyingli}@sjtu.edu.cn

Xiao Chen, Xinxing Yin
Department of Electronic Engineering
Shanghai Jiaotong University
Shanghai, China
Email: {xiaochen, yinxinxin}@sjtu.edu.cn

Liang Pang, Zhi Xue
Department of Electronic Engineering
Shanghai Jiaotong University
Shanghai, China
Email: {pangliang, zxue}@sjtu.edu.cn

***Abstract*—In this paper, we considered the joint masked-beamforming in secure wireless transmission in which artificial noise is sent by the transmitter (Alice) and the receiver (Bob) jointly. A new and efficient optimization scheme is proposed to separately allocate the power ratio for Alice and assign the transmit antenna for Bob. It is proved that when Bob's artificial noise is high enough, Alice should allocate less proportion of her power to the artificial noise. The proposed model combined with proper parameter design can achieve optimal secrecy performance.**

***Index Terms*—Artificial Noise, Masked Beamforming, Secrecy Capacity, Power Allocation Ratio.**

I. Introduction

Wireless communication between two nodes (Alice and Bob) is vulnerable to be eavesdropped by the malicious third party (Eve). A lot of efforts have been made to deal with this problem [1–4]. Recently, the method of artificial noise [5, 6] proposed by Goel *et al.* has become a new way to increase secrecy capacity. In their scheme, by taking advantage of multiple antennas or helper nodes, artificial noise can be generated and injected into Eve's channel. This can effectively degrades Eve's received signal, without affecting Bob by adopting the masked-beamforming technique.

In the framework of model in [6], Alice's transmit signal design is of key importance. The beamforming issue has been solved perfectly in that paper. Another design parameter is the ratio of power allocated between information bearing signal and artificial noise. [10, 11] adopted complex convex optimization to solved the power allocation problem, but their optimization is based on the assumption that Eve's instantaneous CSI is pre-known. Obviously, such an assumption is too strong, compared with the original idea of [6].

In this paper, we consider a new approach that both Alice and Bob send artificial noise. Although authors in [9] also mentioned such configuration, but they mainly deal with the case that only Bob sends artificial noise. No optimal design is yet available for this model. In the following work, we will propose our solution to the design of Alice and Bob's transmission signals, and show that these problems can be solved separately and with efficiency.

The rest of this paper is organized as follows. We will describe system model in section II. In section III, optimal power design will be analysed. Simulation results are shown in section IV, and conclusion will be given in section V.

This work was supported in part by the Natural Science Foundation of China (NSFC) under Grant No. 60932003 and No. 61271220.

II. System Model

Suppose Alice is equipped with N_A $(N_A \geq 2)$ antennas. Bob has N_B $(N_B \geq 2)$ antennas, with the $\mathbf{i}th\,(1 \leq i \leq N_B)$ antenna used as receive antenna, and others as artificial noise emitting antennas. Eve has just one antenna for eavesdropping the transmission signal between Alice and Bob. We assume that the channel between Alice and Bob is known to all parties, but they do not hold any information about the CSI of Eve.

In our model, both Alice and Bob send artificial noise, thus the signal received by Bob is

$$y_b = \mathbf{h}_{\mathbf{ab}}^{(\mathbf{i})\dagger} \cdot \mathbf{x} + \mathbf{h}_{\mathbf{bb}}^{(\mathbf{i})\dagger} \cdot \mathbf{n} + n_b \tag{1}$$

where $\mathbf{h}_{\mathbf{ab}}^{(\mathbf{i})}$ denotes the channel vector between Alice and the $\mathbf{i}th$ antenna of Bob, which is an $N_A \times 1$ complex Gaussian vector. $\mathbf{h}_{\mathbf{bb}}^{(\mathbf{i})}$ is the channel between the transmit and receive antennas of Bob, which is an $(N_B - 1) \times 1$ vector. n_b is the white noise at Bob, modeled as a complex Gaussian random variable with zero-mean and covariance $\sigma_{n_b}^2$. $\mathbf{x}$ is the signal transmitted by Alice, while $\mathbf{n}$ is the artificial noise emitted by Bob.

Similarly, the received signal at Eve is given by:

$$y_e = \mathbf{h}_{\mathbf{ae}}^{\dagger} \cdot \mathbf{x} + \mathbf{h}_{\mathbf{be}}^{(\mathbf{i})\dagger} \cdot \mathbf{n} + n_e \tag{2}$$

where $\mathbf{h}_{\mathbf{ae}}$ and $\mathbf{h}_{\mathbf{be}}^{(\mathbf{i})}$ is the channels between Alice and Eve, Bob and Eve respectively.

III. Secrecy Capacity and Parameter Design

In this part, we will study the design of Alice and Bob's transmission signal so that maximum secrecy capacity between them can be achieved. An efficient scheme will be proposed to address these problems.

A. Masked Beamforming Signal

Since the location and channel condition of Eve is unknown to Bob, the beamforming of $\mathbf{n}$ is just to generate random Gassian noise, so $\mathbf{n}$ becomes an $(N_B-1)\times 1$ complex random Gaussian vector with variance $\sigma_n^2 = E(\mathbf{n}^\dagger \cdot \mathbf{n})$.

For Alice, the transmitted signal $\mathbf{x}$ can be decomposed into information part and artificial noise part:

$$\mathbf{x} = \mathbf{w_1} \cdot u + \mathbf{W_2} \cdot \mathbf{v} \tag{3}$$

according to the beamforming solution by [6], $(\mathbf{w_1}, \mathbf{W_2})$ forms an orthogonal basis of $\mathbb{C}_{N_A}$, in which $\mathbf{w_1} = \mathbf{h_{ab}^{(i)}} / \left\|\mathbf{h_{ab}^{(i)}}\right\|$, while $\mathbf{W_2}$ spans the null space of $\mathbf{h_{ab}}$. u stands for the information symbol with covariance σ_u^2, and $\mathbf{v}$ is a Gaussian vector composed of N_A-1 i.i.d. complex elements, with $\sigma_v^2 = E(\mathbf{v}^\dagger \cdot \mathbf{v})$, thus (1) and (2) can be further written as

$$\begin{aligned} y_b(k) &= \mathbf{h_{ab}^{(i)\dagger}} \cdot (\mathbf{w_1} \cdot u + \mathbf{W_2} \cdot \mathbf{v}) + \mathbf{h_{bb}^{(i)\dagger}} \cdot \mathbf{n} + n_b \\ &= \left\|\mathbf{h_{ab}^{(i)}}\right\| \cdot u + \mathbf{h_{bb}^{(i)\dagger}} \cdot \mathbf{n} + n_b \end{aligned} \tag{4}$$

$$\begin{aligned} y_e(k) &= \mathbf{h_{ae}^{\dagger}} \cdot (\mathbf{w_1} \cdot u + \mathbf{W_2} \cdot \mathbf{v}) + \mathbf{h_{be}^{(i)\dagger}} \cdot \mathbf{n} + n_e \\ &= \frac{\mathbf{h_{ae}}^\dagger \cdot \mathbf{h_{ab}^{(i)}}}{\left\|\mathbf{h_{ab}^{(i)}}\right\|} \cdot u + \mathbf{h_{ae}} \cdot \mathbf{W_2} \cdot \mathbf{v} + \mathbf{h_{be}^{(i)\dagger}} \cdot \mathbf{n} + n_e \end{aligned} \tag{5}$$

B. Secrecy Capacity

For Alice, we consider a total power consumption P_A, in which a proportion of ϕ $(0 \le \phi \le 1)$ is allocated to information signal, and others left as artificial noise. Hence, we have the following relationships:

$$\sigma_u^2 = \phi P_A \tag{6}$$

$$\sigma_{\mathbf{v}}^2 = (1-\phi) P_A \tag{7}$$

For Bob, he uses all his power P_B for artificial noise transmission. Hence,

$$\sigma_{\mathbf{n}}^2 = P_B \tag{8}$$

For MIMO wiretap channels, the results in [3] showed that the secrecy capacity is bounded by the difference in the channel capacity between Alice and Bob and that between Alice and Eve, that is,

$$Cs = Cs_1 - Cs_2 \tag{9}$$

$$\begin{aligned} Cs_1 &= E_u\left\{log_2(1 + (\left\|\mathbf{h_{ab}^{(i)}}\right\| \cdot u)^2 / \sigma_{n_b}^2)\right\} \\ &= log_2(1 + \phi \cdot P_A \cdot \left\|\mathbf{h_{ab}^{(i)}}\right\|^2 / \sigma_{n_b}^2) \end{aligned} \tag{10}$$

There's no $\mathbf{h_{bb}^{\dagger}} \cdot \mathbf{n}$ item in the calculation of Cs_1, because it is possible for Bob to cancel the artificial noise exerted on himself through interference cancellation, which is stated in [9].

$$\begin{aligned} & Cs_2 \\ &= E_{\mathbf{h_{be}^{(i)}}, \mathbf{h_{ae}}}\left\{ log_2\left(1 + \frac{(\frac{\mathbf{h_{ae}}^\dagger \cdot \mathbf{h_{ab}^{(i)}}}{\left\|\mathbf{h_{ab}^{(i)}}\right\|} \cdot)^2 \cdot \sigma_u^2}{\left\|\mathbf{h_{ae}} \cdot \mathbf{W_2} \cdot \mathbf{v}\right\|^2 + \left\|\mathbf{h_{be}^{(i)\dagger}} \cdot \mathbf{n}\right\| + \sigma_{n_e}^2}\right)\right\} \\ &= E_{\mathbf{h_{be}^{(i)}}, \mathbf{h_{ae}}}\left\{ log\left(1 + \frac{\phi \cdot P_A \cdot \left\|\mathbf{h_{ab}^{(i)}}\right\|^2}{\frac{(1-\phi)P_A}{Na-1}\left\|\mathbf{h_{ae}^{\dagger}}\mathbf{W_2}\right\|^2 + \frac{P_B}{N_B-1}\left\|\mathbf{h_{be}^{(i)}}\right\| + \sigma_{n_e}^2}\right)\right\} \end{aligned} \tag{11}$$

C. Antenna Assignation for Bob

We first study Cs_2 in Equ. (11), the item related to i is $P_B \cdot \left\|\mathbf{h_{be}^{(i)}}\right\|^2$. Since the channel between Bob and Eve is unknown to Bob, and considered to be randomized, any combination of the Bob's artificial noise transmit antennas will achieve the same effect on average.

For (10), it is easy to check that Cs_1 increases with $\left\|\mathbf{h_{ab}^{(i)}}\right\|$, so we just need to maximize $\left\|\mathbf{h_{ab}^{(i)}}\right\|$.

Finally, the assignation of Bob's antenna becomes a relatively simple problem, that is, to

$$find \text{ i, } s.t. \left\|\mathbf{h_{ab}^{(i)}}\right\| \ is maximized. \tag{12}$$

Bob then assigns the ith antenna as receive antenna, and the others as artificial noise transmit antennas.

D. Power Allocation for Alice

In [7], X. Zhou *et al.* studied the optimal power allocation for Alice to achieve maximum secrecy capacity when only Alice sends the artificial noise. They adopted an analytical way to find the optimal power allocation ratio ϕ^o. Back to our scenario, too many random variables (such as $\mathbf{h_{ae}}$, $\mathbf{h_{be}}$ and $\mathbf{W_2}$) are involved and correlated, which makes it difficult to derive the optimal ϕ^* analytically. But still we have the following proposition:

Proposition 3.1: Let ϕ^o denotes the power optimization ratio for the condition that only Alice sends artificial noise (which is derived analytically in [7]), and ϕ^* denotes the optimal power allocation when both Alice and Bob send artificial noise, then $\phi^* \in (\phi^o, 1)$

Proof: We prove by contradiction, suppose $\phi^* < \phi^o$, Since ϕ^* is the optimal power allocation when both Alice and Bob send artificial noise, We have $Cs(\phi^*) > Cs(\phi^o)$, that is,

$$\begin{aligned} & Cs_1(\phi^*) - Cs_2(\phi^*) > Cs_1(\phi^o) - Cs_2(\phi^o) \\ \Leftrightarrow\ & Cs_1(\phi^*) - Cs_1(\phi^o) > Cs_2(\phi^*) - Cs_2(\phi^o) \end{aligned} \tag{13}$$

On the other hand, when only Alice sends artificial noise, the secrecy capacity can be denoted as $\overline{Cs}=\overline{Cs_1}-\overline{Cs_2}$, where $\overline{Cs_1}(\phi) = Cs_1(\phi)$, and $\overline{Cs_2}(\phi) = E_{\mathbf{h_{be}^{(i)}}, \mathbf{h_{ae}}}\left\{ log_2\left(1 + \frac{\frac{\phi \cdot P_A}{N_a} \cdot \left\|\mathbf{h_{ab}^{(i)}}\right\|^2}{\frac{(1-\phi)\cdot P_A}{Na} \cdot \left\|\mathbf{h_{ae}^{\dagger}} \cdot \mathbf{W_2}\right\|^2 + \sigma_{n_e}^2}\right)\right\}$, which excludes the item of artificial noise sent by Bob, compared to $Cs_2(\phi)$.

Since ϕ^o is the power optimization ratio for the condition that only Alice sends artificial noise, then

$$\begin{aligned}&\overline{Cs}(\phi^o) > \overline{Cs}(\phi^*)\\ \Leftrightarrow&\overline{Cs_1}(\phi^o) - \overline{Cs_2}(\phi^o) > \overline{Cs_1}(\phi^*) - \overline{Cs_2}(\phi^*)\\ \Leftrightarrow&\overline{Cs_2}(\phi^*) - \overline{Cs_2}(\phi^o) > \overline{Cs_1}(\phi^*) - \overline{Cs_1}(\phi^o)\\ =&Cs_1(\phi^*) - Cs_1(\phi^o) \end{aligned} \quad (14)$$

From (13) and (14), we have

$$\begin{aligned}&\overline{Cs_2}(\phi^o) - \overline{Cs_2}(\phi^*) < Cs_2(\phi^o) - Cs_2(\phi^*)\\ \Leftrightarrow\ & E_{\mathbf{h_{ae}},\mathbf{h_{be}}^{(i)\dagger}}\{log_2(\frac{1+\frac{\phi^o\cdot a}{(1-\phi^o)\cdot b}}{1+\frac{\phi^*\cdot a}{(1-\phi^*)\cdot b}})\}\\ &< E_{\mathbf{h_{ae}},\mathbf{h_{be}}^{(i)\dagger}}\{log_2(\frac{1+\frac{\phi^o\cdot a}{(1-\phi^o)\cdot b+c}}{1+\frac{\phi^*\cdot a}{(1-\phi^*)\cdot b+c}})\} \end{aligned} \quad (15)$$

where $a = P_A \cdot \left\|\mathbf{h_{ab}^{(i)}}\right\|^2$, $b = \frac{P_A}{Na-1}\left\|\mathbf{h_{ae}^\dagger W_2}\right\|^2$, and $c = \frac{P_B}{N_B-1}\left\|\mathbf{h_{be}^{(i)}}\right\|$.

But for $f(\theta) = \frac{1+\frac{\phi^o\cdot a}{(1-\phi^o)\cdot b+\theta}}{1+\frac{\phi^*\cdot a}{(1-\phi^*)\cdot b+\theta}}$, it is easy to prove by analytical method that if $\phi^* < \phi^o$, $f(\theta)$ decreases monotonically with θ, which means that $f(0) > f(c)$. since log increases in a monotone way, we have $\log_2\{\frac{1+\frac{\phi^o\cdot a}{(1-\phi^o)\cdot b}}{1+\frac{\phi^*\cdot a}{(1-\phi^*)\cdot b}}\} > \log_2\{\frac{1+\frac{\phi^o\cdot a}{(1-\phi^o)\cdot b+c}}{1+\frac{\phi^*\cdot a}{(1-\phi^*)\cdot b+c}}\}$, which contradicts with (15), so the assumption $\phi^* < \phi^o$ doesn't hold. Hence, we proved $\phi^* < \phi^o$. ■

We can then find the optimal ϕ^* by one-dimensional search. From the above proposition, we have limited the search range to $(\phi^o, 1)$, which would greatly reduce the search overhead.

E. Effect of Path-loss

From (9)-(11), we can see that the secrecy capacity is the expectation over $\mathbf{h_{be}^{(i)}}$ and $\mathbf{h_{ae}}$, which depends on the statistical channel condition of Eve. If the path-loss effect is considered, $\mathbf{h_{be}^{(i)}}$ is inversely proportional to the distance between Bob and Eve, r_{be}.

$$\mathbf{h_{be}^{(i)}} \propto r_{be}^{-\alpha} \quad (16)$$

where α stands for the pass-loss exponent. It is similar for $\mathbf{h_{ab}^{(i)}}$ and $\mathbf{h_{ae}}$, that is,

$$\mathbf{h_{ab}^{(i)}} \propto r_{ab}^{-\alpha} \quad (17)$$

$$\mathbf{h_{ae}} \propto r_{ae}^{-\alpha} \quad (18)$$

Therefore Cs is the result of spatial expectation over r_{ae} and r_{be} as well as the temporal average over $\mathbf{v}$, $\mathbf{n}$, $\mathbf{h_{be}^{(i)}}$ and $\mathbf{h_{ae}}$.

To take spatial expectation over r_{ae} and r_{be}, we can assume some geometry distribution of Eve. In our simulation, we delimit a certain region (which is an area within a radius of $2 \cdot d_{ab}$ around Alice and Bob). A military terminology is adopted to name such a region as 'Defence Identification Zone'. Outside this region, Eve is considered to have little impact on the secure communication, since the high pass-loss makes the faraway Eve hard to decode the information signal.

IV. Simulation Results

In our simulation scenario, Alice and Bob are located at (-0.5,0) and (0.5,0) respectively, and both of them are equipped with 4 antennas. For ease of comparison, most of the simulation parameters are calculated from [9]. $P_A = P_B = 1W$, $\lambda = 10^{-12.81}$, $\alpha = 3.76$. The noise power is $5{*}10^{-15}W$. Such a configuration will result in a signal-to-noise ratio (SNR) of about 15.2dB at Bob. We model the channel between Alice and Bob as follows:

$$\mathbf{h_{ab}} = \begin{pmatrix} 1.20+0.65i & 0.10-0.92i & -0.55+0.41i & 0.57-0.96i\\ -0.36+0.18i & 0.99-0.29i & 0.40-0.71i & 0.15+0.24i\\ -0.00+0.45i & 0.73+0.86i & -0.97+0.04i & 0.62-0.12i\\ 0.65+0.30i & 0.20-0.03i & 0.17+0.42i & 1.44-0.66i \end{pmatrix}$$

, which is generated randomly.

First, we analyse the optimal design of this scenario. For Bob, $\mathbf{h_{ab}^{(i)}}$ is 1.66, 1.81, 1.52, 2.06 for $i = 1, 2, 3, 4$ respectively. Therefore, Bob will take the 4th antenna as receive antenna, and other 3 antennas as artificial noise transmit antennas.

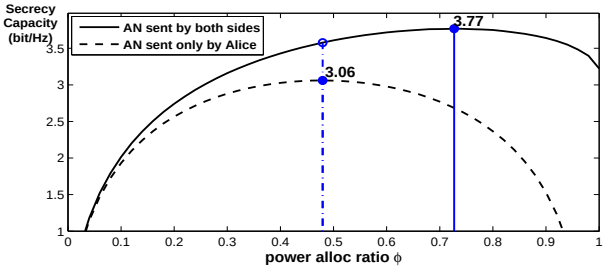

Fig. 1: Secrecy capacity versus the power allocation ratio, ϕ

If only Alice sends artificial noise, the optimal ratio calculated by the formula in [7] is $\phi^o = 0.48$. Fig. (1) shows the power allocation ratio ϕ and the corresponding secrecy capacity. As can be seen, $\phi^* = 0.73 > \phi^o$, which verifies proposition 3.1.

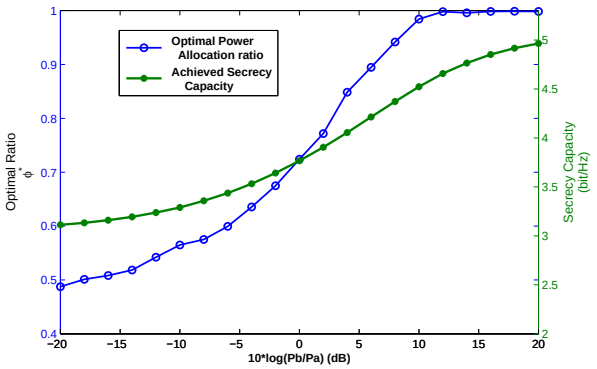

Fig. 2: Secrecy capacity and optimal ϕ^* versus the relative power of artificial noise transmitted by Bob

Next, we study how the power of Bob's artificial noise, P_B, influences the secrecy capacity and the optimal power allocation ratio, shown in Fig. (2). ϕ^* grows monotonically with P_B/P_A, which means that more power can be allocated

to send information signal as P_B/P_A increases. When P_B is high enough, ϕ^* tends to 1, Alice can use all of her power for information signal. The corresponding secrecy capacity can approach to channel capacity in this extreme case.

V. Conclusion

In this paper, we studied the secure transmission in wireless communication that Alice and Bob jointly send the artificial noise (AN) to jam the eavesdropper (Eve). A new and efficient optimization scheme is proposed for this model, which includes a series of techniques to assign the transmit antenna for Bob, allocate the power ratio of Alice and design the beamforming vector. All of these optimizations can be done separately and with high efficiency. Simulation results showed that the proposed model combined with proper parameter design can achieve a good secrecy performance.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355-1387, 1975.

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. on Inf. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[3] F. Oggier and B. Hassibi, "The Secrecy Capacity of the MIMO Wiretap Channel," *IEEE Trans. on Inf. Theory*, vol. 57, pp. 4961-4972, Aug. 2011.

[4] Y. Liang, H. V. Poor and S. Shamai, "Secure Communication Over Fading Channels," *IEEE Trans. on Inf. Theory*, vol. 54, pp. 2470-2492, June 2008.

[5] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. VTC Fall 2005*, vol. 3, pp. 1501-1506, Sept. 2005.

[6] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," *IEEE Trans. on Wireless Commun.*, vol. 7, pp. 2180-2189, Jun. 2008.

[7] X. Zhou and M. R. McKay, "Physical layer security with artificial noise: Secrecy capacity and optimal power allocation," in *3rd International Conference on ICSPCS 2009*, pp. 1-5, Sept. 2009.

[8] N. R. Zurita, D. McLernon, M. Ghogho and A. Swami, "PHY Layer Security Based on Protected Zone and Artificial Noise," *IEEE Signal Processing Letters*, vol. 20, no. 5, pp. 487-490, May 2013.

[9] W. Li, M. Ghogho, B. Chen and C. Xiong, "Secure Communication via Sending Artificial Noise by the Receiver: Outage Secrecy Capacity/Region Analysis," *IEEE Communications Letters*, vol. 16, no. 10, pp. 1628-1631, Oct. 2012.

[10] A. Mukherjee and A. L. Swindlehurst, "Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels," in *IEEE International Conference on SPAWC 2009*, pp. 344-348, June 2009.

[11] Y. Yang, Q. Li, W. Ma, J. Ge and P. C. Ching, "Cooperative Secure Beamforming for AF Relay Networks With Multiple Eavesdroppers," *IEEE Signal Processing Letters*, vol. 20, no. 1, pp. 35-38, Jan. 2013.