A Robust Beamforming Approach to Guarantee Instantaneous Secrecy Rate

Jinho Choi, *Senior Member, IEEE*

***Abstract*—We consider a well-known beamforming approach that induces jamming signals to avoid eavesdropping from a transmitter equipped with an antenna array in this paper. With this beamforming, which is called masked beamforming, in order to guarantee a certain instantaneous secrecy rate, we formulate robust beamforming problems with a constraint that deals with the eavesdropper channel's uncertainty and find the solutions. Unlike a guaranteed ergodic secrecy rate, this guaranteed instantaneous secrecy rate allows us to use codes of short codewords for secure communications with masked beamforming over slow-fading channels. In addition, since the optimal solutions are found in closed form, we do not need to resort to any convex optimization solvers.**

***Index Terms*—Convex optimization, random masked beamforming, secure communications.**

I. Introduction

Wireless communications have become more popular as there are various applications that help people in daily life and business. Due to the broadcast nature, however, wireless communications are prone to various security threats such as eavesdropping. Thus, for secure communications, it is necessary to encrypt signals and actively employ various approaches in cryptography [1], [2]. Besides conventional cryptographic techniques that rely on eavesdroppers' limited computational resources, there are different approaches that can exploit inherent properties of wireless channels for secure communications based on the notion of information-theoretic security [3]–[6]. In general, these approaches belong to physical layer security where secure communications can be achieved using channel codes [7]–[9] and various signal processing techniques [10]–[12].

Among various approaches, the approach in [10] becomes widely studied where a beam of artificial noise is used to keep an eavesdropper ignorant when the transmitter is equipped with an antenna array. That is, artificial noise is generated to degrade the eavesdropper channel and as a result, a positive secrecy rate can be achieved. This approach is referred to as random masked beamforming in this paper. In [13], the secrecy rate of random masked beamforming is analyzed. In [12], [14], it is also shown that jamming signals can be generated from a legitimate receiver (which is equipped with an antenna array) using the full-duplex operation.

A salient feature of random masked beamforming is that it can generate artificial jamming signals without knowing instantaneous channel state information (CSI) of an eavesdropper [10], [15]. With known channel distribution information (CDI) or statistical properties of the eavesdropper channel, it is possible to obtain the ergodic secrecy rate from a transmitter to a legitimate receiver. For guaranteed performances, various optimization problems are considered [16]–[18] to decide the transmit beam as well as covariance matrix for artificial noise vector.

In this paper, we consider random masked beamforming and formulate optimization problems when a transmitter is equipped with an antenna array for beamforming. We are able to derive a closed-form solution of the formulated optimization problem. The main differences from existing approaches are as follows. We consider *instantaneous* secrecy rate with signal-to-interference-plus-noise ratio (SINR) constraints. Note that in [17], the ergodic (or average) secrecy rate is considered. For slow fading channels, the ergodic secrecy rate cannot help to decide the code rate unless the length of codewords is sufficiently long. Thus, we need to consider instantaneous secrecy rate. The approach in this paper allows to use a code of short codewords, which might be more practical over slow fading channels.

To guarantee an instantaneous secrecy rate, the knowledge of the eavesdropper channel is usually required, which is not generally available at the transmitter. Thus, CDI rather than instantaneous CSI can be considered. In this case, we may need to consider outage event. In [16], [18], the outage probability is taken into account as a constraint. On the other hand, in this paper, we consider a certain constraint or condition to deal with the eavesdropper channel's uncertainty, which allows us to formulate robust optimization problems for random masked beamforming, and derive a lower-bound on the probability that this constraint holds. From this lower-bound, we can see that this key constraint is satisfied with an overwhelming probability for a sufficiently large number of antennas at the transmitter.

An interesting finding in this paper is that the approach in [10] can be seen as an optimal solution of a certain problem except transmission powers. Note that a similar finding is also derived in [16].

In summary, the main contributions of the paper are as follows: *i)* a robust optimization problem is formulated to guarantee a certain instantaneous secrecy rate with a constraint on the eavesdropper channel's uncertainty, and its solution is

Manuscript received April 20, 2015; revised August 3, 2015; accepted September 21, 2015. Date of publication September 25, 2015; date of current version February 8, 2016. This work was supported in part by the Agency for Defense Development (the title of the project is *PHY/MAC-NETWORK Technologies Against Jamming Attack and Eavesdropping*) and in part by the "Basic Research Projects in High-tech Industrial Technology" Project through a grant provided by GIST in 2015. The associate editor coordinating the review of this paper and approving it for publication was Prof. Zhengdao Wang.

The author is with the School of Information and Communications, Gwangju Institute of Science and Technology (GIST), Gwangju 500-712, Korea (e-mail: jchoi0114@gist.ac.kr).

Digital Object Identifier 10.1109/TWC.2015.2482494

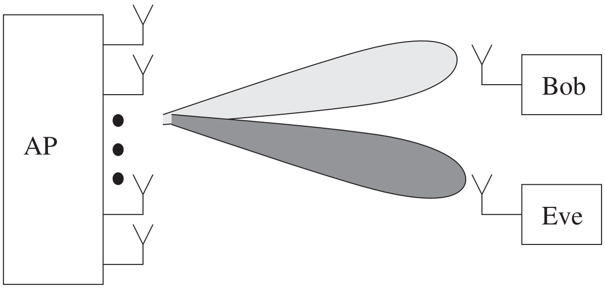


Fig. 1. Jamming for masked beamforming for secure communications.

derived as a set of simple closed-form expressions; *ii)* a lower-bound on the probability of a key constraint for the formulated optimization problem is derived, which shows that this constraint holds with an overwhelming probability for a sufficiently large number of antennas at the transmitter; *iii)* the optimality of the approach in [10] is shown by the formulated optimization problem and its solution.

The rest of the paper is organized as follows. Section II presents the system model for masked beamforming. Optimization problems are formulated in Section III to decide beams and their powers. In Section IV, the probability of a key constraint that is used in formulating optimization problems is studied and its lower-bound is derived. Simulation results are presented in Section V. Finally, the paper is concluded with some remarks in Section VI.

Notation: Matrices and vectors are denoted by upper- and lower-case boldface letters, respectively. The superscripts T and H denote the transpose and complex conjugate, respectively. The 2-norm of $\mathbf{a}$ is denoted by $||\mathbf{a}||$. The Kronecker product is denoted by $\otimes$. For a matrix $\mathbf{A}$, $[\mathbf{A}]_{p,q}$ denotes the (p, q)th element of $\mathbf{A}$. $\mathbb{E}[\cdot]$ denotes the statistical expectation. $\mathcal{CN}(\mathbf{a}, \mathbf{R})$ represents the distribution of circularly symmetric complex Gaussian (CSCG) random vectors with mean vector $\mathbf{a}$ and covariance matrix $\mathbf{R}$. $\mathsf{I}(X; Y)$ denotes the mutual information between X and Y.

II. System Model

In this section, we present a system model based on the approach in [10], where random masked beamforming is used for secure communications.

Suppose that an access point (AP) is equipped with an antenna array to communicate with users or sensors. The number of antenna elements of the array is denoted by L. For convenience, the AP is called Alice and the sensor or user for secure communications is called Bob. Furthermore, we assume that there is an eavesdropper, which could be another sensor or user, and call it Eve. As shown in Fig. 1, Alice can form a beam to Bob for secure communications as she has an antenna array for beamforming, while she can induce jamming signals with artificial noise to degrade the Eve's channel using another beam [10].

Let $\mathbf{h}^{\mathrm{H}}$ and $\mathbf{g}^{\mathrm{H}}$ denote the channel vectors of size $1 \times L$ from Alice to Bob and Eve, respectively. Alice uses a beamformer to form two beams. One beam, denoted by $\mathbf{w}$, is to transmit a secret message, denoted by s, to Bob and the other beam, denoted by $\mathbf{v}$, is a random beam that is used to confuse Eve (i.e., $\mathbf{v}$ is an artificial noise vector as in [10]). Let x and y be the received signals at Bob and Eve, respectively. Then, we have

$$\begin{aligned} x &= \mathbf{h}^{\mathrm{H}}(\mathbf{w}s + \mathbf{v}) + n_x; \\ y &= \mathbf{g}^{\mathrm{H}}(\mathbf{w}s + \mathbf{v}) + n_y, \end{aligned} \tag{1}$$

where $n_x \sim \mathcal{CN}(0, \sigma_{\mathrm{b}}^2)$ and $n_y \sim \mathcal{CN}(0, \sigma_{\mathrm{e}}^2)$ denote the background noises at Bob and Eve, respectively. Here, σ_{b}^2 and σ_{e}^2 are the variances of n_x and n_y, respectively.

Note that we assume a single receive antenna at Bob and Eve. This assumption can be extended to multiple receive antennas. If multiple receive antennas are employed at Bob, a multiple input multiple output (MIMO) channel can be considered, which might be denoted by $\mathbf{H}^{\mathrm{H}}$. Denote by $\mathbf{w}_{\mathrm{b}}^{\mathrm{H}}$ the receive beamforming vector at Bob (an optimal receive beamforming vector will be discussed at the end of Section III). Then, the beamformer output is given by

$$\begin{aligned} x &= \mathbf{w}_{\mathrm{b}}^{\mathrm{H}}(\mathbf{H}^{\mathrm{H}}(\mathbf{w}s + \mathbf{v}) + \mathbf{n}_x) \\ &= (\mathbf{H}\mathbf{w}_{\mathrm{b}})^{\mathrm{H}}(\mathbf{w}s + \mathbf{v}) + \mathbf{w}_{\mathrm{b}}^{\mathrm{H}}\mathbf{n}_x. \end{aligned} \tag{2}$$

Letting $\mathbf{h} = \mathbf{H}\mathbf{w}_{\mathrm{b}}$, we can have x in (1) with $n_x = \mathbf{w}_{\mathrm{b}}^{\mathrm{H}}\mathbf{n}_x$. Throughout this paper, since we will assume that $\mathbf{h}$ is available to Alice, the signal model in (1) remains unchanged even if multiple receive antennas are used at Bob. The impact of multiple receive antennas at Eve will be discussed later.

As mentioned earlier, we assume that the channel vector to Bob, $\mathbf{h}$, is available at Alice. If time division duplexing (TDD) is employed, a training signal transmitted by Bob can be used to estimate $\mathbf{h}$ at Alice. Furthermore, we assume that Eve performs passive eavesdropping. Therefore, Eve would not interfere with the training signal transmitted from Bob to Alice for the channel estimation. Note that active attack by Eve to hinder the channel estimation at Alice can be considered in TDD system [19]. However, in this paper, we only consider passive attack or eavesdropping by Eve.

From (1), we can have the SINRs[1] at Bob and Eve, respectively, as follows:

$$\gamma_{\mathrm{b}}(\mathbf{w}, \mathbf{v}) = \frac{|\mathbf{h}^{\mathrm{H}}\mathbf{w}|^2}{|\mathbf{h}^{\mathrm{H}}\mathbf{v}|^2 + \sigma_{\mathrm{b}}^2} \text{ and } \gamma_{\mathrm{e}}(\mathbf{w}, \mathbf{v}) = \frac{|\mathbf{g}^{\mathrm{H}}\mathbf{w}|^2}{|\mathbf{g}^{\mathrm{H}}\mathbf{v}|^2 + \sigma_{\mathrm{e}}^2}, \tag{3}$$

where $\mathbb{E}[|s|^2] = 1$ for normalization purposes. We assume that s is Gaussian. For convenience, let

$$\begin{aligned} R_s(\mathbf{w}, \mathbf{v}) &= \mathsf{I}(x; s) - \mathsf{I}(y; s) \\ &= \log_2(1 + \gamma_{\mathrm{b}}(\mathbf{w}, \mathbf{v})) - \log_2(1 + \gamma_{\mathrm{e}}(\mathbf{w}, \mathbf{v})), \end{aligned} \tag{4}$$

which is the conditional secrecy rate for given $\mathbf{w}$ and $\mathbf{v}$, and the secrecy capacity can be given by

$$C_s = \max_{\mathbf{w},\mathbf{v}} R_s(\mathbf{w}, \mathbf{v}) \tag{5}$$

[1] In (3), we consider $\mathbf{v}$ is fixed. However, $\mathbf{v}$ can be a random vector or artificial noise vector that can increase the effective noise variance. In this case, the denominators of the SINRs in (3) should be replaced with $\mathbf{h}^{\mathrm{H}}\mathbb{E}[\mathbf{v}\mathbf{v}^{\mathrm{H}}]\mathbf{h} + \sigma_{\mathrm{b}}^2$ and $\mathbf{g}^{\mathrm{H}}\mathbb{E}[\mathbf{v}\mathbf{v}^{\mathrm{H}}]\mathbf{g} + \sigma_{\mathrm{e}}^2$ for γ_{b} and γ_{e}, respectively, provided that $\mathbb{E}[\mathbf{v}] = \mathbf{0}$.

with a total power constraint, e.g., $||\mathbf{w}||^2 + ||\mathbf{v}||^2 \le P_\mathrm{T}$. Then, the transmission rate of s for secure communications, denoted by R_s, can be decided as $R_s \le C_s$.

There are few remarks as follows.

- The secrecy rate in (4) is valid if s is Gaussian and $\mathbf{v}$ also delivers Gaussian signals (thus, $\mathbf{v}$ is to be replaced with $\mathbf{v}d$, where d is a random signal, which is a Gaussian random variable with $\mathbb{E}[d] = 0$ and $\mathbb{E}[|d|^2] = 1$) [20].
- It is expected to have a non-negative secrecy rate in (4). Thus, it is implicitly assumed that $\gamma_\mathrm{b}(\mathbf{w}, \mathbf{v}) \ge \gamma_\mathrm{e}(\mathbf{w}, \mathbf{v})$ (i.e., the Eve's channel is a degraded wiretap channel). Otherwise, $R_s(\mathbf{w}, \mathbf{v}) = 0$.
- The transmission of random signals using beam $\mathbf{v}$ is similar to the use of random bits to confuse Eve in coset coding [7].

III. Masked Beamforming Approach

The secrecy capacity in (5) depends on the channel vectors, $\mathbf{h}$ and $\mathbf{g}$. As mentioned earlier, $\mathbf{h}$ is usually available at Alice for beamforming. However, $\mathbf{g}$ is not known in general. Therefore, C_s is unknown and the determination of the transmission rate of s for secure communications is not easy. To avoid this problem, in [10], [13], the average secrecy rate is considered for known statistical properties of $\mathbf{h}$ and $\mathbf{g}$. The average secrecy rate is valid for sufficiently long codewords that can span all possible states of the fading channels. However, if the channel vectors are static or varying slowly or the length of codewords is short, it is difficult to decide the transmission rate of s to be secure according to the ergodic or average secrecy rate. In this case, it is desirable to guarantee an instantaneous secrecy rate for given $\mathbf{h}$ and any available information of $\mathbf{g}$. In this section, we employ the notion of robust beamforming to decide $\mathbf{w}$ and $\mathbf{v}$ with a guaranteed secrecy rate.

A. Robust Beamforming

As in [21], we consider the following problem:

$$\begin{aligned} &\min_{\mathbf{w},\mathbf{v}} ||\mathbf{w}||^2 + ||\mathbf{v}||^2 \\ &\text{subject to} \begin{cases} \gamma_\mathrm{b}(\mathbf{w}, \mathbf{v}) & \ge \Gamma_\mathrm{b} \\ \gamma_\mathrm{e}(\mathbf{w}, \mathbf{v}) & \le \Gamma_\mathrm{e}, \end{cases} \end{aligned} \tag{6}$$

where Γ_b and Γ_e are the threshold SINRs for Bob and Eve, respectively, where $\Gamma_\mathrm{b} > \Gamma_\mathrm{e}$ so that a positive secrecy rate can be achieved.

Let

$$\mathbf{w}\mathbf{w}^\mathrm{H} = \mathbf{W} \text{ and } \mathbf{v}\mathbf{v}^\mathrm{H} = \mathbf{V}.$$

Then, the constraints in (6) become

$$\mathbf{h}^\mathrm{H} \left(\frac{1}{\Gamma_\mathrm{b}} \mathbf{W} - \mathbf{V} \right) \mathbf{h} \ge \sigma_\mathrm{b}^2 \tag{7}$$

$$\mathbf{g}^\mathrm{H} \left(\frac{1}{\Gamma_\mathrm{e}} \mathbf{W} - \mathbf{V} \right) \mathbf{g} \le \sigma_\mathrm{e}^2. \tag{8}$$

In order to solve (6), we need to know the channel vectors, $\mathbf{h}$ and $\mathbf{g}$. Since $\mathbf{h}$ is the channel vector to Bob, a legitimate user or sensor, we can assume that $\mathbf{h}$ is known by Alice. However, the channel vector to Eve, $\mathbf{g}$, is not known by Alice. Therefore, it is not possible to determine the beamforming vectors, $\mathbf{w}$ and $\mathbf{v}$, through (6).

In general, Eve may want to be close to Bob for better eavesdropping. However, there might be a limit as Bob should be aware the presence of Eve if Eve is too close. We can consider this limit to deal with unknown Eve's channel vector $\mathbf{g}$ in random masked beamforming. That is, $\mathbf{g}$ may not be perfectly correlated with $\mathbf{h}$. Thus, we consider the following additional constraint:

$$|\mathbf{g}^\mathrm{H}\mathbf{h}|^2 \le \omega ||\mathbf{g}||^2 ||\mathbf{h}||^2, \tag{9}$$

where $0 < \omega < 1$, which is referred to as the correlation factor throughout the paper.

Lemma 1: If a $\mathbf{g}$ satisfies (9), $c\mathbf{g}$ also satisfies (9) for any $c \in \mathbb{C}$.

The property in Lemma 1 is referred to as the scale invariant property. From this property, we can see that (9) could hold, although $||\mathbf{g}|| \gg ||\mathbf{h}||$ as long as $\mathbf{g}$ and $\mathbf{h}$ are not perfectly correlated (i.e., $\omega < 1$). Note that $||\mathbf{g}||$ can be large if Eve is closer than Bob to Alice (in this case, the signal-to-noise ratio (SNR) at Eve can be higher than that at Bob) or Eve has more receive antennas for a higher SNR. However, we can see that the correlation between $\mathbf{g}$ and $\mathbf{h}$ is important regardless of Eve's channel gain $||\mathbf{g}||$ or SNR in (9). To ensure a low correlation, $\mathbf{h}$ needs to be highly random. In other words, rich scattering environments are desirable to have highly random $\mathbf{h}$. For this, Alice may have an array with sufficient antenna spacing [22]. We will discuss this issue in Section IV.

We now reformulate the constraints for the problem in (6) to accommodate (9). Let $\mathbf{D} = \Gamma_\mathrm{e}\mathbf{V} - \mathbf{W}$. Then, (8) becomes

$$\begin{bmatrix} \mathbf{g}^\mathrm{H} & 1 \end{bmatrix} \underbrace{\begin{bmatrix} \mathbf{D} & \mathbf{0} \\ \mathbf{0}^\mathrm{H} & \Gamma_\mathrm{e}\sigma_\mathrm{e}^2 \end{bmatrix}}_{=\Psi_1} \begin{bmatrix} \mathbf{g} \\ 1 \end{bmatrix} \ge 0. \tag{10}$$

Furthermore, (9) can be reformulated as

$$\begin{bmatrix} \mathbf{g}^\mathrm{H} & 1 \end{bmatrix} \underbrace{\begin{bmatrix} \omega||\mathbf{h}||^2\mathbf{I} - \mathbf{h}\mathbf{h}^\mathrm{H} & \mathbf{0} \\ \mathbf{0}^\mathrm{H} & 0 \end{bmatrix}}_{=\Psi_2} \begin{bmatrix} \mathbf{g} \\ 1 \end{bmatrix} \ge 0. \tag{11}$$

Since $\mathbf{W}$ and $\mathbf{V}$ should satisfy the constraint in (10) for all $\mathbf{g}$ lies in the set described by (11), we have the following constraint using the S-lemma [23]:

$$\Psi_1 \succeq \lambda\Psi_2, \ \lambda \ge 0 \tag{12}$$

or

$$\Psi(\lambda) = \Psi_1 - \lambda\Psi_2 \succeq \mathbf{0}, \ \lambda \ge 0. \tag{13}$$

Then, a robust optimization problem is formulated as follows:

$$\begin{aligned} &\min_{\mathbf{W},\mathbf{V}} \operatorname{tr}(\mathbf{W}) + \operatorname{tr}(\mathbf{V}) \\ &\text{subject to} \begin{cases} \mathbf{h}^\mathrm{H}(\mathbf{W} - \Gamma_\mathrm{b}\mathbf{V})\mathbf{h} - \Gamma_\mathrm{b}\sigma_\mathrm{b}^2 & \ge 0 \\ \Psi(\lambda) & \succeq \mathbf{0} \\ \lambda & \ge 0. \end{cases} \end{aligned} \tag{14}$$

Without the rank-one constraint for **W** and **V**, we can consider the following additional constraints:

$$\mathbf{W}, \mathbf{V} \succeq \mathbf{0}, \tag{15}$$

which makes (14) a semidefinite programming (SDP) problem. Thus, the resulting problem, which is referred to as **Problem I** throughout the paper, becomes convex and tractable. For convenience, this beamforming approach is referred to as the joint masked beamforming since both **W** and **V** are jointly optimized.

B. Relation to Zero-Forcing Masked Beamforming

In this subsection, we consider a subproblem of **Problem I** in (14) and show that the solution of this subproblem is related to the random masked beamforming approach proposed in [10], which helps us to see its optimality.

Suppose that the sequence of random **v** is chosen to be complex-valued random vectors in the null space of **h** [10], i.e.,

$$\mathbf{v} \perp \mathbf{h}. \tag{16}$$

In addition, as **h** is known, the beamforming vector that maximizes the SNR at Bob becomes $\mathbf{w} \propto \mathbf{h}$. Then, for a given $\Gamma_{\rm b}$, Alice can decide the beamforming vector **w** as follows:

$$\hat{\mathbf{w}} = \sqrt{P_w}\bar{\mathbf{h}}, \tag{17}$$

where $\bar{\mathbf{h}} = \frac{\mathbf{h}}{||\mathbf{h}||}$ and P_w denotes the transmission power of the signal to Bob, which is given by

$$P_w = \frac{\Gamma_{\rm b}\sigma_{\rm b}^2}{||\mathbf{h}||^2}. \tag{18}$$

Let us formulate an optimization problem to decide **V** with given $\mathbf{w} = \hat{\mathbf{w}}$ in (17). We can consider the following constraints:

$$\begin{aligned} \mathbf{h}^{\rm H}\mathbf{V}\mathbf{h} &\le P_w||\mathbf{h}||^2 - \Gamma_{\rm b}\sigma_{\rm b}^2 = 0 \\ \mathbf{g}^{\rm H}\left(\Gamma_{\rm e}\mathbf{V} - \hat{\mathbf{w}}\hat{\mathbf{w}}^{\rm H}\right)\mathbf{g} &\ge -\Gamma_{\rm e}\sigma_{\rm e}^2. \end{aligned} \tag{19}$$

The first constraint in (19) results from (16), while the second constraint is due to the SINR constraint for Eve. Using the S-lemma, we can combine the constraint in (9) and formulate the following problem to decide **V**:

$$\min_{\mathbf{V}} \operatorname{tr}(\mathbf{V})$$
$$\text{subject to } \mathbf{V} \succeq \mathbf{0} \text{ and } \begin{cases} \mathbf{h}^{\rm H}\mathbf{V}\mathbf{h} & \le 0 \\ \Psi_{\rm zf}(\lambda) & \succeq \mathbf{0} \\ \lambda & \ge 0, \end{cases} \tag{20}$$

where

$$\Psi_{\rm zf}(\lambda) = \begin{bmatrix} \Gamma_{\rm e}\mathbf{V} - \hat{\mathbf{w}}\hat{\mathbf{w}}^{\rm H} & \mathbf{0} \\ \mathbf{0}^{\rm H} & \Gamma_{\rm e}\sigma_{\rm e}^2 \end{bmatrix} - \lambda\Psi_2. \tag{21}$$

For convenience, the optimization problem in (20) is referred to as **Problem II** and the resulting beamforming approach is referred to as the zero-forcing (ZF) masked beamforming since $\mathbf{v} \perp \mathbf{w}$, while **w** is fixed as in (17).

Lemma 2: The solution of **Problem II** has the following form:

$$\mathbf{V} = c_v\mathbf{P}_{\mathbf{h}}, \tag{22}$$

where $c_v > 0$ is constant and $\mathbf{P}_{\mathbf{h}} = \mathbf{I} - \frac{1}{||\mathbf{h}||^2}\mathbf{h}\mathbf{h}^{\rm H}$.

Proof: In (20), $\mathbf{h}^{\rm H}\mathbf{V}\mathbf{h} \le 0$ implies that Range(**V**) $\perp$ **h** as **V** is positive semidefinite. Let $\mathbf{u}_1, \ldots, \mathbf{u}_{L-1}$ denote orthonormal basis vectors that are orthogonal to **h**, i.e., $\mathbf{u}_l^{\rm H}\mathbf{h} = 0$ for $l = 1, \ldots, L-1$. Since **V** is also Hermitian, **V** should have the following form:

$$\mathbf{V} = \sum_{l=1}^{L-1} \psi_l \mathbf{u}_l \mathbf{u}_l^{\rm H},$$

where $\psi_l \ge 0$. With $\hat{\mathbf{w}}$ in (17), it follows

$$\mathbf{Z} = [\Psi_{\rm zf}(\lambda)]_{1:L-1,1:L-1} = \Gamma_{\rm e}\mathbf{V} - c\bar{\mathbf{h}}\bar{\mathbf{h}}^{\rm H} - d\mathbf{I} \succeq \mathbf{0}, \tag{23}$$

where c is constant and $d = \lambda\omega||\mathbf{h}||^2 > 0$. Note that since $[\Psi_{\rm zf}(\lambda)]_{L,L} \ge 0$, the constraint in (23) is equivalent to $\Psi_{\rm zf}(\lambda) \succeq \mathbf{0}$. Consider a vector lies in the subspace spanned by $\{\mathbf{u}_1, \ldots, \mathbf{u}_{L-1}\}$, which is denoted by **u**. Then, from (23), it follows

$$\mathbf{u}^{\rm H}\mathbf{Z}\mathbf{u} \ge 0.$$

From this, we have

$$\Gamma_{\rm e}\mathbf{u}^{\rm H}\sum_{l=1}^{L-1}\psi_l\mathbf{u}_l\mathbf{u}_l^{\rm H}\mathbf{u} + d||\mathbf{u}||^2 = \sum_{l=1}^{L-1}(\Gamma_{\rm e}\psi_l - d)|m_l|^2 \ge 0,$$

where $m_l = \mathbf{u}_l^{\rm H}\mathbf{u}$. Since $\operatorname{tr}(\mathbf{V}) = \sum_{l=1}^{L}|\psi_l|^2$, for given d, the optimization problem in (20) is to find $\{\psi_l\}$ and can be compactly written as

$$\min_{\{\psi_l \ge 0\}} \sum\nolimits_{l=1}^{L-1} \psi_l$$
$$\text{subject to } \sum\nolimits_{l=1}^{L-1}(\Gamma_{\rm e}\psi_l - d)|m_l|^2 \ge 0, \text{ for any } m_l. \tag{24}$$

The optimal solution is

$$\psi_l = \frac{d}{\Gamma_{\rm e}}, \; l = 1, \ldots, L-1.$$

Since $\mathbf{P}_{\mathbf{h}} = \sum_{l=1}^{L-1}\mathbf{u}_l\mathbf{u}_l^{\rm H}$, we can see that the optimal solution has the form in (22). ■

Note that d depends on the Lagrange multiplier λ. Thus, we need to decide λ in order to find the optimal solution of **Problem II**.

Theorem 1: The optimal solution of **Problem II** is given by

$$\mathbf{V} = \frac{\omega P_w}{(1-\omega)\Gamma_{\rm e}}\mathbf{P}_{\mathbf{h}}. \tag{25}$$

Proof: From Lemma 2, we only need to decide $c_v = d$ or λ as $d = \lambda\omega||\mathbf{h}||^2$. With (22), the constraint that $\mathbf{Z} \succeq \mathbf{0}$ in (23) is equivalent to

$$\begin{aligned} \Gamma_{\mathrm{e}} c_v - \lambda\omega||\mathbf{h}||^2 \geq 0 \\ -P_w - \lambda\omega||\mathbf{h}||^2 + \lambda||\mathbf{h}||^2 \geq 0. \end{aligned} \tag{26}$$

Since $\mathrm{tr}(\mathbf{V})$ is to be minimized, we need to find the minimum c_v that satisfies (26) for $\lambda \geq 0$. From (26), we have

$$c_v \geq \frac{\lambda\omega||\mathbf{h}||^2}{\Gamma_{\mathrm{e}}} \text{ and } \lambda \geq \frac{P_w}{(1-\omega)||\mathbf{h}||^2} \geq 0. \tag{27}$$

Since $\omega \in (0, 1)$, the minimum c_v that satisfies (27) is

$$\min c_v = \frac{\omega P_w}{(1-\omega)\Gamma_{\mathrm{e}}}.$$

This completes the proof. ■

From Theorem 1, we can have a closed-form expression for the solution of **Problem II** without resorting to any convex optimization solvers. Based on this result and Lemma 2, we have few remarks as follows.

- Due to the relaxation, $\mathbf{V}$ is actually the covariance matrix of $\mathbf{v}$ for random masked beamforming. That is, $\mathbf{v}$ is randomly drawn from the Gaussian distribution of mean $\mathbf{0}$ and covariance matrix $\mathbf{V}$ (i.e., $\mathbf{v} \sim \mathcal{CN}(\mathbf{0}, \mathbf{V})$) as artificial noise, where $\mathbf{V}$ is the solution of **Problem II**, at Eve, the SINR becomes
$$\gamma_{\mathrm{e}} = \frac{|\mathbf{g}^{\mathrm{H}}\mathbf{w}|^2}{\mathbf{g}^{\mathrm{H}}\mathbf{V}\mathbf{g} + \sigma_{\mathrm{e}}^2}$$
and the constraint that $\gamma_{\mathrm{e}} \leq \Gamma_{\mathrm{e}}$ is satisfied with the relaxation.
- From Lemma 2, we can see the optimality of the random masked beamforming approach proposed in [10], in which $\mathbf{v}$ is assumed to be drawn from $\mathcal{CN}(0, \sigma_v^2\mathbf{P}_{\mathbf{h}})$ with $\mathbf{w}$ in (17) and the average secrecy rate is considered with σ_v^2. It is noteworthy that, there is a minor difference between the approach in [10] and the solution of **Problem II** in deciding the transmission power for $\mathbf{v}$. While the transmission power for $\mathbf{v}$ is considered with *average* secrecy rate in the approach in [10], it is decided to satisfy *instantaneous* secrecy rate in **Problem II** with an additional constraint, i.e., (9).
- In [16], a different optimization problem has been studied, and it is shown that its solution approach for random masked beamforming becomes that in [10] by simulations and partially some analytical results under the isotropic Gaussian channel assumption, $\mathbf{g} \sim \mathcal{CN}(\mathbf{0}, \sigma_g^2\mathbf{I})$. On the other hand, the optimality of the approach in [10] in this paper is complete and shown without any particular statistical assumptions on $\mathbf{g}$.

Although the solution of **Problem II** is easily obtained, it would be suboptimal for **Problem I**. However, we can show that the solution of (14) is identical to that of (20) (i.e., the optimal solution of $\mathbf{w}$ and $\mathbf{V}$ of **Problem I** are given in (17) and in (25), respectively). To this end, we can consider few properties of **Problem I**, which are shown below.

Lemma 3: The solution matrix $\mathbf{W}$ of **Problem I** in (14) has the following form:

$$\mathbf{W} = \alpha_1 \bar{\mathbf{h}}\bar{\mathbf{h}}^{\mathrm{H}}, \tag{28}$$

where α_1 is a positive constant.

Proof: As in (15), $\mathbf{W}$ is positive semidefinite and Hermitian. Thus, we assume that

$$\mathbf{W} = \alpha_1 \bar{\mathbf{h}}\bar{\mathbf{h}}^{\mathrm{H}} + \tilde{\mathbf{W}}, \tag{29}$$

where $\alpha_1 > 0$ is a positive constant and $\tilde{\mathbf{W}}$ is positive semidefinite and Hermitian with $\mathrm{Range}(\tilde{\mathbf{W}}) \perp \mathbf{h}$. Note that $\mathrm{tr}(\mathbf{W}) = \alpha_1 + \mathrm{tr}(\tilde{\mathbf{W}}) \geq \alpha_1$.

For convenience, let

$$\mathbf{g} = c_1(\mathbf{h} + \mathbf{e}), \tag{30}$$

where c_1 is constant and $\mathbf{e} \perp \mathbf{h}$. Here, $\mathbf{e} \neq 0$ as $\omega < 1$ from (9). This implies that $||\mathbf{e}|| > 0$. Let $\mathbf{W}_1 = \alpha_1 \bar{\mathbf{h}}\bar{\mathbf{h}}^{\mathrm{H}}$ and $\mathbf{W}_2 = \mathbf{W}$ in (29). Suppose that both $\mathbf{W}_1$ and $\mathbf{W}_2$ satisfy the constraints in (7) and (8). Then, since $\mathrm{tr}(\mathbf{W}_1) \leq \mathrm{tr}(\mathbf{W}_2)$, we do not need to consider $\mathbf{W}_2$ as a solution of the optimization problem in (14).

Since $\mathbf{h}^{\mathrm{H}}\mathbf{W}_1\mathbf{h} = \mathbf{h}^{\mathrm{H}}\mathbf{W}_2\mathbf{h}$, if $\mathbf{W}_1$ satisfies (7), $\mathbf{W}_2$ does, and vice versa. From (29) and (30), it can be shown that

$$\begin{aligned} \mathbf{g}^{\mathrm{H}}\mathbf{W}_2\mathbf{g} &= |c_1|^2(\mathbf{h} + \mathbf{e})^{\mathrm{H}}\mathbf{W}_2(\mathbf{h} + \mathbf{e}) \\ &= |c_1|^2\left(\alpha_1||\mathbf{h}||^2 + \mathbf{e}^{\mathrm{H}}\tilde{\mathbf{W}}\mathbf{e}\right) \\ &\geq \mathbf{g}^{\mathrm{H}}\mathbf{W}_1\mathbf{g}. \end{aligned}$$

Thus, if $\mathbf{W}_2$ satisfies (8), $\mathbf{W}_1$ does.

In summary, if $\mathbf{W}_2$ satisfies (7) and (8), $\mathbf{W}_1$ does. However, $\mathrm{tr}(\mathbf{W}_1) \leq \mathrm{tr}(\mathbf{W}_2)$ as shown earlier. Therefore, $\mathbf{W}_2$ cannot be the solution. This shows that the solution has the form as $\mathbf{W}_1 = \alpha_1 \bar{\mathbf{h}}\bar{\mathbf{h}}^{\mathrm{H}}$. ■

Lemma 4: The solution of $\mathbf{V}$ of **Problem I** satisfies

$$\mathrm{Range}(\mathbf{V}) \perp \mathbf{h}. \tag{31}$$

Proof: Let

$$\mathbf{V}_1 = \tilde{\mathbf{V}} \text{ and } \mathbf{V}_2 = \tilde{\mathbf{V}} + \alpha_2 \bar{\mathbf{h}}\bar{\mathbf{h}}^{\mathrm{H}},$$

where $\tilde{\mathbf{V}}$ is positive semidefinite and Hermitian with $\mathrm{Range}(\tilde{\mathbf{V}}) \perp \mathbf{h}$ and $\alpha_2 > 0$. Clearly, $\mathrm{tr}(\mathbf{V}_1) \leq \mathrm{tr}(\mathbf{V}_2)$.

It can be shown that

$$\mathbf{h}^{\mathrm{H}}\mathbf{V}_1\mathbf{h} \leq \mathbf{h}^{\mathrm{H}}\mathbf{V}_2\mathbf{h}.$$

Thus, if $\mathbf{V}_2$ satisfies (7), $\mathbf{V}_1$ does. In addition, with (30), we have

$$\mathbf{g}^{\mathrm{H}}\mathbf{V}_2\mathbf{g} = |c_1|^2\left(\alpha_2||\mathbf{h}||^2 + \mathbf{e}^{\mathrm{H}}\tilde{\mathbf{V}}\mathbf{e}\right) \geq \mathbf{g}^{\mathrm{H}}\mathbf{V}_1\mathbf{g}.$$

This implies that if $\mathbf{V}_2$ satisfies (8), $\mathbf{V}_1$ does. In summary, if $\mathbf{V}_2$ satisfies (7) and (8), $\mathbf{V}_1$ does and its trace is smaller than or equal to that of $\mathbf{V}_2$. Consequently, $\mathbf{V}$ should have the constraint in (31). ■

Based on Lemmas 3 and 4, we can have the following result.

Theorem 2: **Problem I** in (14) is reduced to **Problem II** in (20).

Proof: From Lemma 3, let $\mathbf{W} = \alpha_1 \bar{\mathbf{h}}\bar{\mathbf{h}}^{\mathrm{H}}$. Then, we have $\mathrm{tr}(\mathbf{W}) = \alpha_1$, which is the transmission power for $\mathbf{w}$ to be optimized. From Lemmas 3 and 4, the problem in (14) can be formulated as

$$\min \alpha_1 + \mathrm{tr}(\tilde{\mathbf{V}})$$
$$\text{subject to} \begin{cases} \alpha_1 ||\mathbf{h}||^2 & \geq \sigma_{\mathrm{b}}^2; \\ \frac{1}{\Gamma_{\mathrm{e}}} \mathbf{e}^{\mathrm{H}} \tilde{\mathbf{V}} \mathbf{e} & \geq \alpha_1 ||\bar{\mathbf{h}}||^2 + \frac{\sigma_{\mathrm{e}}^2}{|c_1|^2}; \\ (9). \end{cases} \tag{32}$$

For any $\tilde{\mathbf{V}}$, the optimal solution of α_1 is P_w in (18). This implies that the optimal solution of $\mathbf{w}$ is given in (17) and the problem in (20) has the same solution as that in (14). ■

In summary, the optimal solution of **Problem I** in (14) can be found without resorting to any convex optimization solvers, as it is given in (17) and (25), which shows that the random masked beamforming approach in [10] is an optimal approach. In addition to showing this optimality, we are able to decide the minimum transmission powers, P_w and $P_v = \mathrm{tr}(\mathbf{V})$, according to SINR constraints by closed-form expressions for a given target (instantaneous) secrecy rate in this section.

Note that in Section II, we discuss the case that Bob receive the desired signal with the receive beamforming vector $\mathbf{w}_{\mathrm{b}}$ using a receive antenna array. However, we do not address an optimal receive beam yet. From Lemma 3, it is now possible to derive the optimal receive beamforming vector in terms of the SNR. Since $\mathbf{w} \propto \mathbf{h}$ as in Lemma 3, from (2), the SNR at Bob is given by

$$\mathrm{SNR} \propto |\mathbf{w}_{\mathrm{b}}^{\mathrm{H}} \mathbf{H}^{\mathrm{H}} \mathbf{w}|^2 \propto |\mathbf{w}_{\mathrm{b}}^{\mathrm{H}} \mathbf{H}^{\mathrm{H}} \mathbf{H} \mathbf{w}_{\mathrm{b}}|^2. \tag{33}$$

Thus, we can see that the optimal $\mathbf{w}_{\mathrm{b}}$ is the right singular vector corresponding to the largest singular value of $\mathbf{H}$.

IV. Probability of (9) and Determination of ω

Since $\mathbf{g}$ is not available, the crucial constraint for secure communication in random masked beamforming is (9). In particular, the determination of ω in (9) plays a key role in guaranteeing a certain secrecy. In order to see the role of ω, suppose that $\omega = 1$. Then, (9) holds with probability 1 for any $\mathbf{h}$ and $\mathbf{g}$ due to the Cauchy-Schwarz inequality. However, in this case, since the constraint in (9) also holds for $\mathbf{h} = \mathbf{g}$, which results in $\gamma_{\mathrm{e}} = \gamma_{\mathrm{b}}$, there is no feasible solution, if $\Gamma_{\mathrm{b}} > \Gamma_{\mathrm{e}}$ is required for a non-zero secrecy rate. In this section, we focus on (9) and derive a lower-bound on the probability that (9) holds for a given ω.

Suppose that Eve can be located near Bob and assume that

$$\mathbf{g} = \alpha(\mathbf{h} + \mathbf{c}),$$

where $\mathbf{c}$ is the independent random vector and α is the relative gain of the Eve's channel to the Bob's channel. Due to the scale invariant property in Lemma 1, it is possible to assume that $\alpha = 1$ for convenience. Thus, in this section, we assume that

$$\mathbf{g} = \mathbf{h} + \mathbf{c}. \tag{34}$$

In this section, we consider a specific case where the antenna array at the AP is deployed under a rich scattering environment and the channel vectors are spatially uncorrelated. Note that the role of $\mathbf{h}$ is similar to that of secret key in an encryption scheme. Eve may want to have her channel $\mathbf{g}$ as close to $\mathbf{h}$ as possible (i.e., Eve can attempt to access the secret key). However, if $\mathbf{h}$ is random or spatially[2] uncorrelated, it may not be easy to have $\mathbf{g} \approx \mathbf{h}$. Thus, to Alice, the more random $\mathbf{h}$, the more secure masked beamforming.

In order to have spatially uncorrelated channel vectors, the antenna spacing has to be large enough. In [24], it is shown that the antenna spacing greater than a half-wavelength could be sufficient for uncorrelated spatial channels if the antenna array is deployed under a rich scattering environment. Thus, Alice needs to deploy the antenna array under a rich scattering environment with a sufficiently large antenna spacing. As a result, $\mathbf{h}$ and $\mathbf{g}$ can be considered as spatially white Gaussian random vectors. In particular, we have the following assumption.

A) Assume that

$$\mathbf{c} \sim \mathcal{CN}(0, \sigma_c^2 \mathbf{I}) \text{ and } \mathbf{h} \sim \mathcal{CN}(0, \sigma_h^2 \mathbf{I}), \tag{35}$$

where σ_c^2 and σ_h^2 are the variances of each element of $\mathbf{c}$ and that of $\mathbf{h}$, respectively.

In Assumption **A)**, we do not consider any correlation between $\mathbf{g}$ and $\mathbf{h}$. Suppose that

$$\mathbf{a} = [\mathbf{h}^{\mathrm{T}}\ \mathbf{g}^{\mathrm{T}}]^{\mathrm{T}} \sim \mathcal{CN}(\mathbf{0}, \mathbf{R}), \tag{36}$$

where

$$\mathbf{R} = \begin{bmatrix} 1 & \rho \\ \rho^* & 1 \end{bmatrix} \otimes \mathbf{I} = \begin{bmatrix} \mathbf{I} & \rho \mathbf{I} \\ \rho^* \mathbf{I} & \mathbf{I} \end{bmatrix}. \tag{37}$$

Here, ρ is the correlation between the received signals at Bob and Eve and each element of $\mathbf{h}$ and $\mathbf{g}$ is assumed to have unit variance for normalization purposes. The spatially correlated channels in (36) is based on the Kronecker channel model of MIMO channels [25]. With Bob and Eve together, we can model the overall channel as a MIMO channel where the two outputs are the received signals at Bob and Eve, while the multiple inputs are the transmitted signals from the beamformer at Alice. Then, it can be shown that

$$\mathbf{c} = \mathbf{g} - \mathbf{h} \sim \mathcal{CN}(\mathbf{0}, 2(1 - \rho_r)\mathbf{I}), \tag{38}$$

where $\rho_r = \Re(\rho)$. That is, letting $\sigma_c^2 = 2(1 - \rho_r)$, we can see that the channel model in (36) implies Assumption **A)**. In what follows, we only consider Assumption **A)**, not the channel model in (36). Thus, the correlation between $\mathbf{h}$ and $\mathbf{c}$ is not to be exploited in deriving a lower-bound on the probability of (9).

For convenience, let

$$\Delta = \frac{||\mathbf{c}||^2}{||\mathbf{h}||^2}. \tag{39}$$

[2] If $\mathbf{h}$ is spatially uncorrelated, its entropy (or its randomness) can be maximized.

Furthermore, define $Z = \mathbf{c}^{\mathrm{H}}\mathbf{h}$, and let $Z_1 = \Re(Z)$ and $Z_2 = \Im(Z)$.

Lemma 5: Under **A)**, we have

$$\begin{aligned}&\Pr(|\mathbf{g}^{\mathrm{H}}\mathbf{h}|^2 \leq \omega||\mathbf{g}||^2||\mathbf{h}||^2 \,|\, \mathbf{h}) \\ &\geq \left(1 - \mathcal{Q}\left(\sqrt{\mu}, \sqrt{x(\omega, \bar{\delta})}\right)\right)\Pr(\Delta \geq \bar{\delta}),\end{aligned} \tag{40}$$

where $A = ||\mathbf{h}||^2$, $B = ||\mathbf{c}||^2$, $\mu = \frac{2(1-\omega)}{\sigma_c^2}$, and

$$x(\omega, \bar{\delta}) = \frac{2\omega A}{\sigma_c^2}(\bar{\delta} - (1 - \omega)). \tag{41}$$

Here, $\mathcal{Q}(a, b)$ denotes the Marcum Q-function and $\bar{\delta} \in (0, 1)$ is constant.

Proof: Let

$$p(\omega, A) = \Pr(|\mathbf{g}^{\mathrm{H}}\mathbf{h}|^2 \leq \omega||\mathbf{g}||^2||\mathbf{h}||^2 \,|\, \mathbf{h}).$$

Since $\mathbf{g} = \mathbf{h} + \mathbf{c}$, we can show that

$$\begin{aligned}p(\omega, A) &= \Pr\left(|A + Z|^2 \leq \omega A(A + 2Z_1 + B)\right) \\ &= \Pr\left(X \leq \frac{2\omega}{\sigma_c^2}(B - (1 - \omega)A)\right),\end{aligned}$$

where

$$X = \frac{((1 - \omega)A + Z_1)^2 + Z_2^2}{\frac{A}{2}\sigma_c^2}.$$

Under **A)**, since $Z \sim \mathcal{CN}(0, A\sigma_c^2)$ or $Z_1, Z_2 \sim \mathcal{N}(0, \frac{A\sigma_c^2}{2})$, X becomes a noncentral chi-squared random variable with $k = 2$ degrees of freedom and mean $k + \mu = 2 + \mu$. The cumulative distribution function (cdf) of X with 2 degrees of freedom is given by

$$\Pr(X \leq x) = 1 - \mathcal{Q}(\sqrt{\mu}, \sqrt{x}). \tag{42}$$

Letting $q = \Pr(B \geq \bar{\delta}A) = \Pr(\Delta \geq \bar{\delta})$, we have

$$\begin{aligned}p(\omega, A) &\geq \Pr\left(X \leq \frac{2\omega}{\sigma_c^2}(\bar{\delta}A - (1 - \omega)A)\right)q + 0 \times (1 - q) \\ &= \left(1 - \mathcal{Q}\left(\sqrt{\mu}, \sqrt{x(\omega, \bar{\delta})}\right)\right)\Pr(\Delta \geq \bar{\delta}).\end{aligned} \tag{43}$$

This completes the proof. ■

Lemma 6: Let $x_l \sim \mathcal{N}(0, 1)$ and x_l's are independent. Then, for $\mathbf{x} = [x_1 \; \ldots \; x_d]^{\mathrm{T}}$ with $\epsilon > 0$,

$$\begin{aligned}\Pr\left(||\mathbf{x}||^2 \leq d(1 - \epsilon)\right) &\leq \exp\left(-\frac{1}{4}d\epsilon^2\right); \\ \Pr\left(||\mathbf{x}||^2 \geq d(1 + \epsilon)^2\right) &\leq \exp\left(-\frac{3}{4}d\epsilon^2\right).\end{aligned} \tag{44}$$

Proof: See [26]. ■

The following result shows that the inequality that $B \geq \bar{\delta}A$ holds with an overwhelming probability for a sufficiently large L.

Lemma 7: For a given $\epsilon \in (0, 1)$, if

$$\bar{\delta} \geq \frac{\sigma_c^2(1 - \epsilon)}{\sigma_h^2(1 + \epsilon)^2}, \tag{45}$$

the probability $\Pr(\Delta \leq \bar{\delta}) = \Pr(B \leq \bar{\delta}A)$ exponentially decreases with L.

Proof: From Lemma 6, noting that $\frac{2||\mathbf{h}||^2}{\sigma_h^2}$ is a chi-squared random variable with $2L$ degrees of freedom, we can show that

$$\Pr(A \in \mathcal{A}_\epsilon) \geq 1 - \exp\left(-\frac{L\epsilon^2}{2}\right) - \exp\left(-\frac{3L\epsilon^2}{2}\right), \tag{46}$$

where $\mathcal{A}_\epsilon = [A_l, A_u]$. Here,

$$A_u = L\sigma_h^2(1 + \epsilon)^2 \text{ and } A_l = L\sigma_h^2(1 - \epsilon). \tag{47}$$

In addition, we have

$$\begin{aligned}\Pr(B \geq \bar{\delta}A \mid A \in \mathcal{A}_\epsilon) &= 1 - \Pr(B \leq \bar{\delta}A \mid A \in \mathcal{A}_\epsilon) \\ &\geq 1 - \Pr(B \leq \bar{\delta}A_u).\end{aligned} \tag{48}$$

Thus, it follows

$$\begin{aligned}\Pr(B \geq \bar{\delta}A) &\geq \Pr(B \geq \bar{\delta}A \mid A \in \mathcal{A}_\epsilon)\Pr(A \in \mathcal{A}_\epsilon) \\ &\geq \left(1 - \Pr(B \leq \bar{\delta}A_u)\right)\Pr(A \in \mathcal{A}_\epsilon).\end{aligned} \tag{49}$$

Since

$$\Pr(B \leq L\sigma_c^2(1 - \epsilon)) \leq e^{-\frac{L\epsilon^2}{2}}, \tag{50}$$

if (45) holds, we can see that $\Pr(B \leq \bar{\delta}A_u)$ decreases exponentially with L. Then, substituting (46) into (49), we have

$$\Pr(B \leq \bar{\delta}A) \leq \bar{P}_\epsilon = 1 - \left(1 - e^{-\frac{L\epsilon^2}{2}} - e^{-\frac{3L\epsilon^2}{2}}\right)\left(1 - e^{-\frac{L\epsilon^2}{2}}\right), \tag{51}$$

which shows that $\Pr(B \leq \bar{\delta}A)$ decreases exponentially with L. It completes the proof. ■

From (43) and (51), under (45), we can have the following lower-bound on the probability of (9):

$$p(\omega, A) \geq \left(1 - \mathcal{Q}\left(\sqrt{\mu}, \sqrt{x(\omega, \bar{\delta})}\right)\right)\bar{P}_\epsilon. \tag{52}$$

As will be shown in Section V, this bound is not tight. However, together with the following result (i.e., Lemma 8), this lower-bound can show that $p(\omega, A)$ is overwhelming for a large L and can approach 1 as L increases.

Lemma 8: Let

$$\omega = \bar{\omega} \overset{\triangle}{=} 1 - \frac{\bar{\delta}}{2}. \tag{53}$$

Then, in (40), we have

$$\mathcal{Q}\left(\sqrt{\mu}, \sqrt{x(\bar{\omega}, \bar{\delta})}\right) \leq \exp\left(-\frac{1 - \bar{\omega}}{2\sigma_c^2}(\sqrt{\bar{\omega}}||\mathbf{h}|| - 1)^2\right). \tag{54}$$

Proof: From [27], we have an upper-bound on the Marcum Q-function, $\mathcal{Q}(\alpha, \beta)$, which is given by

$$\mathcal{Q}(\alpha, \beta) \leq \exp\left(-\frac{(\beta - \alpha)^2}{2}\right), \tag{55}$$

where $\beta > \alpha \geq 0$. From (53), we have

$$x(\bar{\omega}, \bar{\delta}) = \bar{\omega}\bar{\delta}\frac{A}{\sigma_c^2}.$$

It follows

$$\sqrt{x(\bar{\omega}, \bar{\delta})} - \sqrt{\mu} = \sqrt{\frac{\bar{\delta}}{\sigma_c^2}}\left(\sqrt{\bar{\omega}A} - 1\right).$$

Substituting this into the upper-bound in (55), we obtain (54). ■

From (54), we can see that $\mathcal{Q}\left(\sqrt{\mu}, \sqrt{x(\bar{\omega}, \bar{\delta})}\right)$ decreases with $||\mathbf{h}||$. In other words, if L is sufficiently large, we have a large $||\mathbf{h}||$, which makes $\mathcal{Q}\left(\sqrt{\mu}, \sqrt{x(\bar{\omega}, \bar{\delta})}\right)$ small. From (40), we can see that the constraint in (9) holds with an overwhelming probability for a sufficiently large L. Furthermore, under a rich scattering environment or **A)**, from (44), we have

$$\Pr(||\mathbf{h}||^2 \leq L\sigma_h^2(1 - \epsilon)) < \epsilon_L,$$

where ϵ_L approaches 0 as $L \to \infty$. Thus, $||\mathbf{h}||$ increases with L and this implies that $\mathcal{Q}\left(\sqrt{\mu}, \sqrt{x(\bar{\omega}, \bar{\delta})}\right) \to 0$ as $L \to \infty$ from (54). Consequently, we can see that the probability of (9) approaches 1 as $L \to \infty$ using the lower-bound in (52).

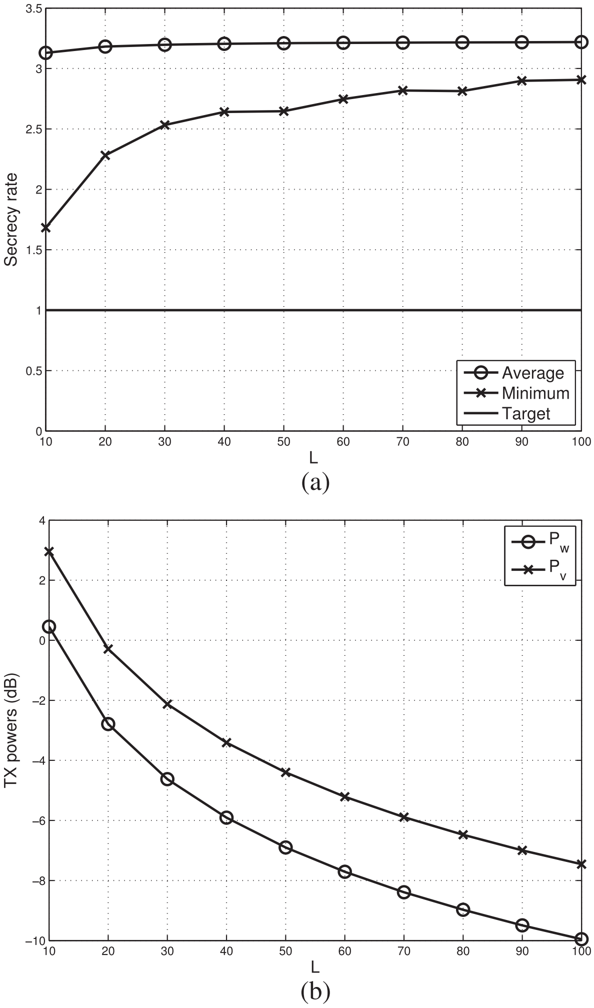
In order to determine the value of ω in finding $\mathbf{V}$ from (20), we can have (53), i.e., $\omega = \bar{\omega}$. This certainly requires to find $\bar{\delta}$ or σ_c^2 in (45). If Bob can make sure that there are no other receivers or antennas within a certain distance, we can assume that $\mathbf{g}$ is sufficiently uncorrelated with $\mathbf{h}$. As mentioned earlier, under rich scattering environments, a distance of half-wavelength could be sufficient for a low spatial correlation in [24]. That is, if Bob can guarantee no other antennas within a distance of half-wavelength, we may expect a sufficiently low correlation between $\mathbf{g}$ and $\mathbf{h}$. For example, if we assume that the correlation between $\mathbf{g}$ and $\mathbf{h}$ is at most 0.5 (i.e., $\rho = \frac{1}{2}$ in (37) as the worst case), the variance of each element of $\mathbf{c}$ is at most the same as that of $\mathbf{h}$ or $\sigma_c^2 = \sigma_h^2$. Then, (45) becomes

$$\bar{\delta} \geq \frac{1 - \epsilon}{(1 + \epsilon)^2}.$$

If $\epsilon = \frac{1}{2}$, we can set $\bar{\delta} = \frac{2}{9}$ and $\bar{\omega} = \frac{8}{9}$.

V. Simulation Results

In this section, we present simulation results using the channel model in (36) for the ZF masked beamforming approach (since it is equivalent to the joint masked beamforming approach, we only consider the ZF masked beamforming approach). In addition, we consider $\omega = \frac{8}{9}$ under the assumption that the *nominal* spatial correlation between $\mathbf{h}$ and $\mathbf{g}$ is $\rho_{\text{nom}} = \frac{1}{2}$ (Bob needs to guarantee that there is no Eve within a certain distance).



(a)

(b)

Fig. 2. Performance for various values of L when $\rho = \frac{1}{2}$, $\Gamma_{\text{b}} = 10$ and $\Gamma_{\text{e}} = 4.5$: (a) secrecy rate; (b) (average) transmission powers.

We assume the target secrecy rate is 1 when $\Gamma_{\text{b}} = 10$ dB. Thus, $\Gamma_{\text{e}} = 6.532$ dB. Fig. 2 shows the simulation results for the secrecy rate and transmission powers when the actual correlation is set to $\rho = \frac{1}{2}$. For each value of L, we have 100,000 runs (in each run, $\mathbf{h}$ and $\mathbf{g}$ are randomly drawn according to (36)) to obtain the average and minimum values of 100,000 instantaneous secrecy rates. Since the minimum value of secrecy rates is higher than the target secrecy rate in Fig. 2 (a), we can confirm that there is no event that the instantaneous secrecy rate is lower than the target secrecy rate among 100,000 runs. It is interesting to note that the minimum value of secrecy rates increases with L, which means that the secrecy rates can be more concentrated around the average value for a larger L. In addition, as shown in Fig. 2 (b), the transmission powers can be lower as L increases. This implies that as the beam becomes narrower (by increasing L), the target secrecy rate can be achieved with lower transmission powers.

A lower-bound on the probability of (9) is derived in Section IV, which shows that the probability of (9) can approach 1 as L increases. Low-bounds and simulation results are shown in Fig. 3 for various values of L. According to Fig. 3 (a), there is no event that the constraint in (9) does not hold among 100,000 runs. Thus, according to the simulation results, the probability of (9) is always 1 for all L's. In Fig. 3, we can see that the lower-bound from (52) is not tight, especially

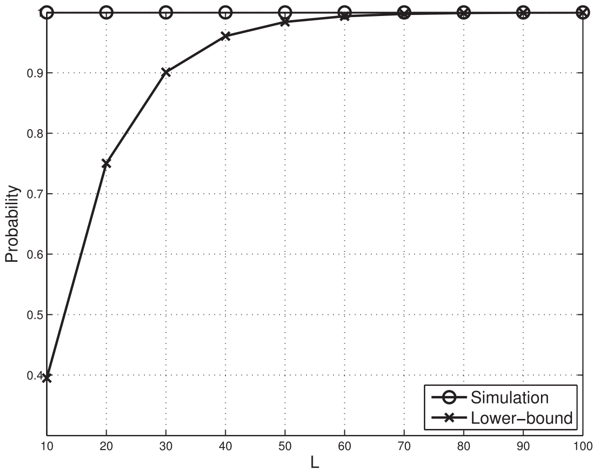
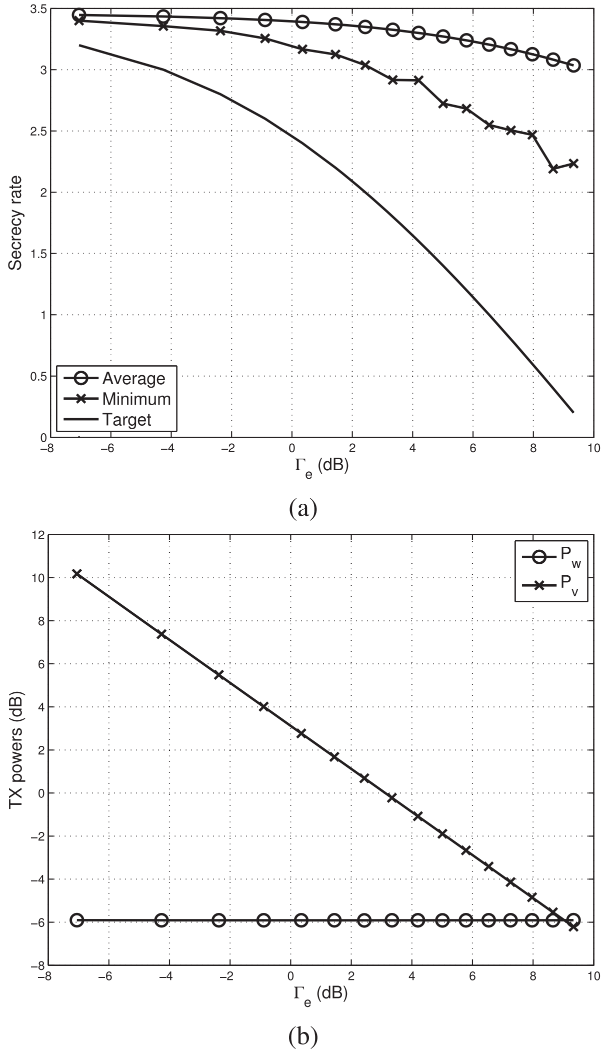


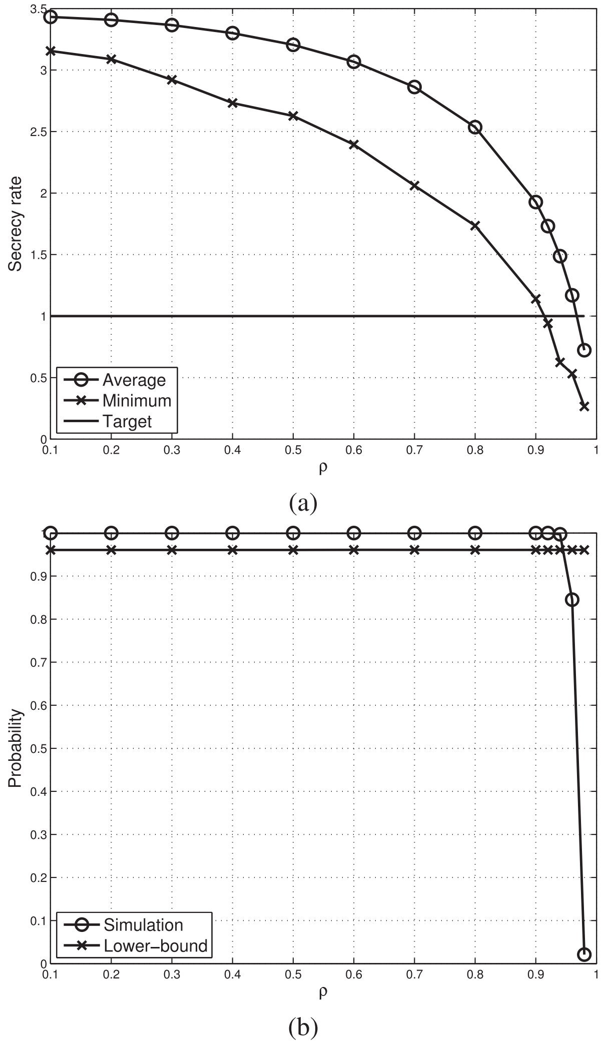
Fig. 3. The probability of (9) for various values of L when $\rho = \frac{1}{2}$, $\Gamma_{\mathrm{b}} = 10$ and $\Gamma_{\mathrm{e}} = 4.5$.



(a)

(b)

Fig. 4. Performance for various values of Γ_{e} when $\rho = \frac{1}{2}$, $L = 40$, and $\Gamma_{\mathrm{b}} = 10$: (a) secrecy rate; (b) (average) transmission powers.



(a)

(b)

Fig. 5. Performance for various values of ρ when $L = 40$, $\Gamma_{\mathrm{b}} = 10$ and $\Gamma_{\mathrm{e}} = 4.5$: (a) secrecy rate; (b) probability of (9).

for small L's. A tighter bound might be desirable, which may be considered as a further research topic.

In the ZF masked beamforming, we can set various target secrecy rates. For a fixed Γ_{b}, the target secrecy rate can be set to any value between 0 and $\log_2(1 + \Gamma_{\mathrm{b}})$ by deciding Γ_{e} accordingly, i.e.,

$$\Gamma_{\mathrm{e}} = 2^{R_{\mathrm{b}} - \hat{R}_s} - 1,$$

where $R_{\mathrm{b}} = \log_2(1 + \Gamma_{\mathrm{b}})$ and $\hat{R}_s$ is the target secrecy rate. Fig. 4 shows the performances of the ZF masked beamforming for various values of the target secrecy rate with $L = 40$ and $\rho = \frac{1}{2}$. The average and minimum values of secrecy rates are found from 100,000 runs. From Fig. 4 (a), we can see that the minimum value of the secrecy rate is higher than the target secrecy rate. Thus, we can always guarantee the target secrecy rate. As Γ_{e} increases (or the target secrecy rate decreases), we can also observe that the power of the artificial noise transmitted by $\mathbf{v}$, P_v, can be lower as shown in Fig. 4 (b), while P_w is fixed to keep the same SINR at Bob, i.e., $\Gamma_{\mathrm{b}} = 10$ dB.

Note that the lower-bound on the probability of (9) is slightly greater than 0.96 regardless of the value of Γ_{e} as it is decided by the channels and ω, which is fixed.

So far, the spatial correlation, ρ, is assumed to be the same as the nominal one, $\rho_{\mathrm{nom}} = \frac{1}{2}$. In practice, the spatial correlation can be higher than the nominal one if Bob underestimates the spatial correlation. In this case, the target secrecy rate may not be guaranteed. Simulations are carried out with $L = 40$ to see the impact of the gap between the actual spatial correlation, ρ, and the nominal (or estimated) one, $\rho_{\text{nom}} = \frac{1}{2}$, on the performances. Fig. 5 (a) shows the average and minimum values of instantaneous secrecy rates from 100,000 runs. It is shown that for a large ρ, the target secrecy rate cannot be guaranteed. The probability of (9) decreases rapidly as ρ is closer to 1. However, if ρ is not too large (say, less than 0.8), we can see that there is a good gap between the minimum value of the secrecy rate and the target secrecy rate.

Consequently, the results in Fig. 5 demonstrate that it is important for Bob to make sure that there is no Eve's antenna in the vicinity of him.

VI. Concluding Remarks

In this paper, we studied random masked beamforming to guarantee an instantaneous secrecy rate. To deal with Eve's channel uncertainty, we considered a constraint and formulated SDP problems for robust beamforming. The key difference from existing approaches is that since we considered instantaneous secrecy rate, the resulting beamforming approaches could be used with channel coding of short codewords over slow fading channels. By showing that the joint masked beamforming and ZF masked beamforming problems (i.e., **Problem I** and **Problem II**) have the same solution, the optimality of the well-known approach proposed in [10] was also shown. Furthermore, a set of simple closed-form expressions for the solution of the ZF masked beamforming problem was derived, which allows us to find beams and assign transmission powers without resorting to any convex optimization solvers. A lower-bound on the probability of a key constraint has been derived, which showed that this constraint can hold with an overwhelming probability for a sufficiently large number of transmit antennas at Alice, L, and this probability approaches 1 as $L \to \infty$.

References

[1] W. Trappe and L. C. Washington, *Introduction to Cryptography With Coding Theory*, 2nd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2006.

[2] J. Katz and Y. Lindell, *Introduction to Modern Cryptography: Principles and Protocols*. London, U.K.: Chapman & Hall/CRC Press, 2007.

[3] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[4] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[5] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[6] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "Bounds on secrecy capacity over correlated ergodic fading channels at high SNR," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 1975–1983, Apr. 2011.

[7] L. Ozarow and A. Wyner, "Wire-tap channel II," *AT T Bell Lab. Tech. J.*, vol. 63, pp. 2135–2157, Dec. 1984.

[8] D. Klinc, J. Ha, S. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Forensics Sec.*, vol. 6, no. 3, pp. 532–540, Sep. 2011.

[9] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, Oct. 2011.

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

[11] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[12] G. Zheng, I. Krikidis, J. Li, A. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[13] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 2515–2534, Jul. 2010.

[14] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Trans. Signal Process.*, vol. 62, no. 24, pp. 6391–6401, Dec. 2014.

[15] A. Mukherjee and A. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[16] Q. Li, W.-K. Ma, and A.-C. So, "Safe convex approximation to outage-based MISO secrecy rate optimization under imperfect CSI and with artificial noise," in *Proc. Conf. Rec. 45th Asilomar Conf. Signals Syst. Comput.*, Nov. 2011, pp. 207–211.

[17] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[18] K.-Y. Wang, A.-C. So, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Outage constrained robust transmit optimization for multiuser MISO downlinks: Tractable approximations by conic optimization," *IEEE Trans. Signal Process.*, vol. 62, no. 21, pp. 5690–5705, Nov. 2014.

[19] S. Im, H. Jeon, J. Choi, and J. Ha, "Secret key agreement under an active attack in MU-TDD systems with large antenna arrays," in *Proc. Global Commun. Conf.*, Dec. 2013, pp. 1849–1855.

[20] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[21] T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Worst-case robust multiuser transmit beamforming using semidefinite relaxation: Duality and implications," in *Proc. 45th Asilomar Conf. Signals Syst. Comput.*, Nov. 2011, pp. 1579–1583.

[22] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[23] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2009.

[24] P.-S. Kildal and K. Rosengren, "Correlation and capacity of mimo systems and mutual coupling, radiation efficiency, and diversity gain of their antennas: Simulations and measurements in a reverberation chamber," *IEEE Commun. Mag.*, vol. 42, no. 12, pp. 104–112, Dec. 2004.

[25] D.-S. Shiu, G. J. Foschini, M. J. Gans, and J. M. Khan, "Fading correlation and its effect on the capacity of multielement antenna systems," *IEEE Trans. Commun.*, vol. 48, no. 3, pp. 502–513, Mar. 2000.

[26] B. Laurent and P. Massart, "Adaptive estimation of a quadratic functional by model selection," *Ann. Statist.*, vol. 28, pp. 1302–1338, Oct. 2000.

[27] M. K. Simon and M.-S. Alouini, "Exponential-type bounds on the generalized Marcum Q-function with application to error probability analysis over fading channels," *IEEE Trans. Commun.*, vol. 48, no. 3, pp. 359–366, Mar. 2000.

Jinho Choi (SM'02) was born in Seoul, Korea. He received the B.E. (*magna cum laude*) degree in electronics engineering from Sogang University, Seoul, South Korea, in 1989, and the M.S.E. and Ph.D. degrees in electrical engineering from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea, in 1991 and 1994, respectively. Currently, he is a Professor with Gwangju Institute of Science and Technology (GIST), Gwangju, Korea. Prior to joining GIST in 2013, he was as a Professor/Chair in Wireless with the College of Engineering, Swansea University, Swansea, Wales, U.K. He has authored two books published by Cambridge University Press, in 2006 and 2010. His research interests include wireless communications and array/statistical signal processing. Since 2005, he has been an Associate Editor of the IEEE Communications Letters and an Editor of *Journal of Communications and Networks* (JCN), and from 2005 to 2007, he served as an Associate Editor of the IEEE Transactions on Vehicular Technology and ETRI journal. He was the recipient of the 1999 Best Paper Award for signal processing from EURASIP, the 2009 Best Paper Award from WPMC (Conference).