

Secrecy Performance Analysis of Location-Based Beamforming in Rician Wiretap Channels

Shihao Yan and Robert Malaney

Abstract—We propose a new optimal Location-Based Beamforming (LBB) scheme for the wiretap channel, where both the main channel and the eavesdropper’s channel are subject to Rician fading. In our LBB scheme the two key inputs are the location of the legitimate receiver and the location of the potential eavesdropper. Notably, our scheme does not require as direct inputs any channel state information of the main channel or the eavesdropper’s channel, making it easy to deploy in a host of application settings in which the location inputs are known. Our beamforming solution assumes a multiple-antenna transmitter, a multiple-antenna eavesdropper, and a single-antenna receiver, and its aim is to maximize the physical layer security of the channel. To obtain our solution we first derive the secrecy outage probability of the LBB scheme in a closed-form expression that is valid for arbitrary values of the Rician K -factors of the main channel and the eavesdropper’s channel. Using this expression we then determine the location-based beamformer solution that minimizes the secrecy outage probability. To assess the usefulness of our new scheme, and to quantify the value of the location information to the beamformer, we compare our scheme to other schemes, some of which do not utilize any location information. Our new beamformer solution provides optimal physical layer security for a wide range of location-based applications.

Index Terms—Physical layer security, Rician fading, location-based beamforming, secrecy outage probability.

I. INTRODUCTION

Physical layer security guarantees secrecy regardless of an eavesdropper’s computational capability and does not require complex key distribution and management [1]. In early studies [2, 3], a wiretap channel model was proposed as the fundamental system model to examine such physical layer security in single-input single-output systems. In the wiretap channel, an eavesdropper (Eve) overhears the wireless communication between a transmitter (Alice) and an intended receiver (Bob). More recently, motivated by multiple-input multiple-output (MIMO) techniques, physical layer security in MIMO wiretap channels has garnered much interest (e.g., [4–9]). However, many of the works in MIMO-based physical layer security assume the (instantaneous) CSI of the *main channel* (the channel between Alice and Bob) is perfectly known by Alice or Bob (e.g., [4–6]). This assumption is usually very difficult to justify in practice (e.g., in massive MIMO techniques the CSI of a channel cannot be perfectly known even to a receiver due to pilot contamination issues [10–13]). Another assumption adopted in the literature is that the CSI of the *eavesdropper’s*

channel (the channel between Alice and Eve) is known to Alice, which is even harder to justify in practice.

However, there are many circumstances where *location information* of Bob and Eve could be available. For example, in some specific military application scenarios, Alice may obtain Bob’s location through direct communications, and Eve’s location through some (possibly *a priori*) surveillance. Other circumstances could be where Bob and Eve are known users of the system (but still requiring secret communications on an individual basis), and their location information is routinely broadcasted as per the requirements of the network protocol. Examples of such circumstances would be in IEEE 1609.2 for vehicular networks, or in some location-based social-media applications.

Regardless of the application scenario, the main point we focus on here is that if there is a line-of-sight (LOS) component in the main channel or the eavesdropper’s channel, it is possible to utilize location information directly in order to enhance the physical layer security. More specifically, we propose and analyze a new Location-Based Beamforming (LBB) scheme in the wiretap channel, where both the main channel and the eavesdropper’s channel are subject to Rician fading. Our scheme does not require the CSI of either the main channel or the eavesdropper’s channel - thus making it quite general, as well as pragmatic. The basic *modus operandi* of the scheme we propose is that given the input locations of Bob and Eve, we output the optimal beamformer solution and the security level (the secrecy outage probability) associated with this solution.¹ Detailing how these outputs are determined forms the core of our work.

Surprisingly, there has been little previous work in this area, with the closest works perhaps those of [14] and [15]. In [14], the ergodic secrecy rate was examined for multiple-antenna wiretap channels with Rician fading. However, in [14] it was assumed that the CSI of the main channel was perfectly known by Alice. The work of [15] analyzed the secrecy performance of orthogonal space-time block codes when the main channel is assumed to be subject to Rician fading. But the eavesdropper’s channel was assumed to be subject to Rayleigh fading in [15] and therefore Eve’s location information was not that useful.

The direction of this paper and our contributions are summarized as follows. (i) We first derive the secrecy outage probability of the LBB scheme in a closed-form expression,

S. Yan and R. Malaney are with the School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, NSW 2052, Australia (Emails: shihao.yan@unsw.edu.au; r.malaney@unsw.edu.au).

This work was funded by The University of New South Wales and Australian Research Council Grant DP120102607.

¹Although our scheme works for any input locations. It is possible that the secrecy outage probability approaches one (e.g., as Bob moves further from Alice whilst Eve moves closer). We leave it to the system operator to decide whether the secrecy outage predicted justifies the sending of data.

which is valid for arbitrary values of the Rician K -factors of the main channel and the eavesdropper's channel. (ii) We then determine the optimal location-based beamformer and the minimum secrecy outage probability for the scheme. (iii) In order to fully appreciate the gains of the LBB scheme, we also analyze, for comparison, the secrecy performance of a Non-Beamforming (NB) scheme. (iv) As a final comparison, we also consider the effect on the LBB scheme of the full CSI of Bob being made available to Alice, and the effect of Eve's location information becoming untrustworthy.

The rest of this paper is organized as follows. Section II details our system model; Section III provides our analytical solutions; Section IV provides numerical simulations; and Section V draws concluding remarks. Secrecy performances of the comparison schemes are provided in Appendices. We adopt the following notations in this work. Scalar variables are denoted by italic symbols. Vectors and matrices are denoted by lower-case and upper-case boldface symbols, respectively. Given a complex number z , $|z|$ denotes the modulus of z . Given a complex vector \mathbf{x} , $\|\mathbf{x}\|$ denotes the Euclidean norm, \mathbf{x}^T denotes the transpose of \mathbf{x} , \mathbf{x}^\dagger denotes the conjugate transpose of \mathbf{x} , and $\text{Re}(\mathbf{x})$ denotes the real part of \mathbf{x} . The $L \times L$ identity matrix is referred to as \mathbf{I}_L and $\mathbb{E}[\cdot]$ denotes expectation.

II. SYSTEM MODEL

Our LBB scheme was examined for the simpler case of a pure LOS channel in one of our previous works [16]. Here, we expand on that simple scenario by considering more generic and realistic channel conditions. That is, we will assume $K_B > 0$ and $K_E > 0$, where K_B and K_E are the Rician K -factors of the main channel and the eavesdropper's channel, respectively. The wiretap channel of interest is illustrated in Fig. 1, where Alice and Eve are equipped with uniform linear arrays (ULAs) with N_A and N_E antenna elements,² respectively; and Bob is equipped with a single antenna. As we will show later, our analysis provided in this work is also valid for other antenna arrays beyond ULAs at Eve. We assume that Alice, Bob, and Eve are static.

As shown in Fig. 1, we adopt the polar coordinate system, where Alice's location is selected as the origin, Bob's location is denoted as (d_B, θ_B) , and Eve's location is denoted as (d_E, θ_E) . For presentation convenience, without other statements we assume that the coordinate system is set up such that $0 \leq \theta_B \leq \pi$ and $0 \leq \theta_E \leq \pi$. The orientation of the ULA at Alice is also shown in this figure. We also assume that the main channel and the eavesdropper's channel are subject to quasi-static Rician fading with equal block length but different Rician K -factors, and that a K -factor map (K as a function of locations) is known in the vicinity of Alice via some *a priori* measurement campaigns. We further assume that the

²We will assume N_E is also known to Alice. This is reasonable in circumstances where Alice can determine physical constraints on the size of an eavesdropper's antenna, knowledge of which, coupled to the known frequency of transmission, can allow for a reliable upper bound on N_E to be set. If an upper bound on N_E is set, then our solutions become bounds (worst case scenarios). In other circumstances, where Eve is at times a legitimate user, we can assume N_E is known.

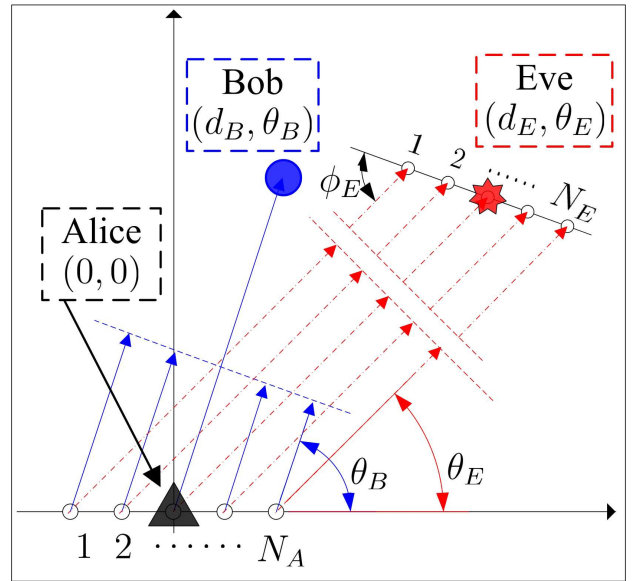


Fig. 1. Illustration of the Rician wiretap channel of interest.

CSI of the main channel is unknown to Alice, but that Bob's location is known to Alice.³ Additional assumptions are that Eve knows the CSI of the eavesdropper's channel and the beamformer adopted by Alice; that Eve applies Maximum Ratio Combining (MRC) in order to maximize the probability of successful eavesdropping [8, 9]; and that Eve's location is known to Alice. As we discuss later, our analysis also covers the case where Eve's location is unavailable at Alice.

As per the aforementioned assumptions, the $1 \times N_A$ main channel vector is given by

$$\mathbf{h} = \sqrt{\frac{K_B}{1 + K_B}} \mathbf{h}_o + \sqrt{\frac{1}{1 + K_B}} \mathbf{h}_r, \quad (1)$$

where \mathbf{h}_o is the LOS component, and \mathbf{h}_r is the scattered component. The entries of \mathbf{h}_r are independent and identically distributed (i.i.d) circularly-symmetric complex Gaussian random variables with zero mean and unit variance, i.e., $\mathbf{h}_r \sim \mathcal{CN}(0, \mathbf{I}_{N_A})$. Denoting ρ_A as the space between two antenna elements of the ULA at Alice, \mathbf{h}_o is given by [17]

$$\mathbf{h}_o = [1, \dots, \exp(j(N_A - 1)\tau_A \cos \theta_B)], \quad (2)$$

where $\tau_A = 2\pi f_0 \rho_A / c$, f_0 is the carrier frequency, and c is the speed of propagation of the plane wave. The $N_E \times N_A$ eavesdropper's channel matrix is given by

$$\mathbf{G} = \sqrt{\frac{K_E}{1 + K_E}} \mathbf{G}_o + \sqrt{\frac{1}{1 + K_E}} \mathbf{G}_r, \quad (3)$$

where \mathbf{G}_o is the LOS component, and \mathbf{G}_r is the scattered component represented by a matrix with i.i.d circularly-symmetric complex Gaussian random variables with zero mean and unit

³We note that using Bob's location saves feedback overhead relative to use of the CSI of the main channel. This is due to the following two facts: (i) the CSI varies during different fading blocks and has to be fed back for each fading block, meanwhile the location information only has to be fed back once for a static Bob; and (ii) the CSI is an N_A -dimension complex vector ($2N_A$ variables embedded), meanwhile Bob's location is determined by only two real numbers.

variance. Given the locations of Alice and Eve, \mathbf{G}_o can be written as [18]

$$\mathbf{G}_o = \mathbf{r}_o^T \mathbf{g}_o \quad (4)$$

where \mathbf{r}_o and \mathbf{g}_o are the array responses at Eve and Alice, respectively, which are given by

$$\mathbf{r}_o = [1, \dots, \exp(-j(N_E - 1)\tau_E \cos \phi_E)], \quad (5)$$

$$\mathbf{g}_o = [1, \dots, \exp(j(N_A - 1)\tau_A \cos \theta_E)]. \quad (6)$$

In (5), we have $\tau_E = 2\pi f_0 \rho_E / c$, where ρ_E is the space between two antenna elements of the ULA at Eve, and ϕ_E is the direction of arrival from Eve to Alice which is dependent on the orientation of the ULA at Eve. As we show later, the signal-to-noise ratio (SNR) of the eavesdropper's channel is independent of ϕ_E when Eve utilizes MRC to combine the received signals. As such, the secrecy performance of the LBB scheme does not depend on ϕ_E and thus Alice does not have to know ϕ_E .

The received signal at Bob is given by

$$y = \sqrt{g(d_B)} \mathbf{h} \mathbf{b} x + n_B, \quad (7)$$

where $g(d_B)$ is the path loss component of the main channel given by $g(d_B) = (c/4\pi f_0 d_0)^2 (d_0/d_B)^{\eta_B}$ (d_0 is a reference distance and η_B is the path loss exponent⁴ of the main channel), \mathbf{b} is a normalized beamformer (i.e., $\|\mathbf{b}\| = 1$), x is the Gaussian distributed information bearing signal satisfying $\mathbb{E}[|x|^2] = P$ (P is the total transmit power of Alice⁵), and n_B is the additive white Gaussian noise of the main channel with zero mean and variance σ_B^2 . Likewise, the received signal at Eve is given by

$$\mathbf{z} = \sqrt{g(d_E)} \mathbf{G} \mathbf{b} x + \mathbf{n}_E, \quad (8)$$

where $g(d_E)$ is the path loss component of the eavesdropper's channel given by $g(d_E) = (c/4\pi f_0 d_0)^2 (d_0/d_E)^{\eta_E}$ (η_E is the path loss exponent of the eavesdropper's channel), and \mathbf{n}_E is the additive white Gaussian noise vector of the eavesdropper's channel with zero mean and variance matrix $\sigma_E^2 \mathbf{I}_{N_E}$, i.e., $\mathbf{n}_E \sim \mathcal{CN}(\mathbf{0}, \sigma_E^2 \mathbf{I}_{N_E})$.

Then, the SNR of the main channel is given by

$$\gamma_B = \frac{Pg(d_B)|\mathbf{h} \mathbf{b}|^2}{\sigma_B^2} = \bar{\gamma}_B |\mathbf{h} \mathbf{b}|^2, \quad (9)$$

where $\bar{\gamma}_B$ is defined as $\bar{\gamma}_B \triangleq Pg(d_B)/\sigma_B^2$. Assuming Eve applies MRC to combine the received signals at different antennas, the SNR of the eavesdropper's channel is given by

$$\gamma_E = \frac{Pg(d_E)\|\mathbf{G} \mathbf{b}\|^2}{\sigma_E^2} = \bar{\gamma}_E \|\mathbf{G} \mathbf{b}\|^2, \quad (10)$$

where $\bar{\gamma}_E$ is defined as $\bar{\gamma}_E \triangleq Pg(d_E)/\sigma_E^2$.

⁴The path loss exponent η_B is dependent on the Rician K -factor K_B . For example, $\eta_B \rightarrow 2$ as $K_B \rightarrow \infty$. For simplicity, we assume η_B is known to Alice since K_B is known. This declaration also applies to the path loss exponent of the eavesdropper's channel η_E and the Rician K -factor K_E .

⁵It is straightforward to prove that the secrecy outage probability is a monotonically decreasing function of Alice's transmit power for given locations of Bob and Eve. As such, we assume that Alice always sets her transmit power at the maximum value P .

III. LOCATION-BASED BEAMFORMING SCHEME

In this section, we first examine the secrecy performance of our proposed LBB scheme in terms of the secrecy outage probability and the probability of non-zero secrecy capacity. We then determine the optimal location-based beamformer of the LBB scheme that minimizes the secrecy outage probability.

A. Preliminaries

In order to derive the secrecy performance metrics of our scheme (e.g., the secrecy outage probability), we first derive the probability density functions (pdfs) of γ_B and γ_E . Without loss of generality, we derive such pdfs for a general \mathbf{b} , which is independent of \mathbf{h}_r and \mathbf{G}_r . To this end, we first determine the distribution type of $|\mathbf{h} \mathbf{b}|$. As per (1), we have

$$\mathbf{h} \mathbf{b} = \underbrace{\sqrt{\frac{K_B}{1+K_B}} \mathbf{h}_o \mathbf{b}}_{\tilde{h}_o} + \underbrace{\sqrt{\frac{1}{1+K_B}} \mathbf{h}_r \mathbf{b}}_{\tilde{h}_r}. \quad (11)$$

Since \mathbf{b} is independent of \mathbf{h}_r , \tilde{h}_r is still a circularly-symmetric complex Gaussian random variable. Noting that \tilde{h}_o is deterministic, we conclude that $|\mathbf{h} \mathbf{b}|$ follows a Rician distribution. We next determine the parameters of this Rician distribution. Following (11), we have

$$|\tilde{h}_o|^2 = \frac{K_B}{1+K_B} |\mathbf{h}_o \mathbf{b}|^2 \quad (12)$$

and

$$\mathbb{E}[|\tilde{h}_r|^2] = \frac{1}{1+K_B} \mathbb{E}[|\mathbf{h}_r \mathbf{b}|^2] = \frac{1}{1+K_B}. \quad (13)$$

We note that $|\tilde{h}_o|^2$ is the power of the LOS (deterministic) component and $\mathbb{E}[|\tilde{h}_r|^2]$ is the average power of the non-LOS (random) component. As such, we conclude that $|\mathbf{h} \mathbf{b}|$ follows a Rician distribution with \tilde{K}_B and $\tilde{\gamma}_B$ as the Rician K -factor and total power, respectively, where \tilde{K}_B and $\tilde{\gamma}_B$ are given by

$$\tilde{K}_B \triangleq \frac{|\tilde{h}_o|^2}{\mathbb{E}[|\tilde{h}_r|^2]} = |\mathbf{h}_o \mathbf{b}|^2 K_B, \quad (14)$$

$$\tilde{\gamma}_B \triangleq \mathbb{E}[\gamma_B] = \bar{\gamma}_B \left(|\tilde{h}_o|^2 + \mathbb{E}[|\tilde{h}_r|^2] \right) = \frac{(K_B |\mathbf{h}_o \mathbf{b}|^2 + 1) \bar{\gamma}_B}{1+K_B}. \quad (15)$$

The pdf of Rician random variables involves the zero-order modified Bessel function of the first kind, which is not suitable for further analysis (e.g., deriving the secrecy outage probability). To make progress, it is convenient to interpret the Rician fading as a special case of Nakagami fading. As such, the pdf of γ_B is approximated as [20]

$$f_{\gamma_B}(\gamma) = \left(\frac{\tilde{m}_B}{\tilde{\gamma}_B} \right)^{\tilde{m}_B} \frac{\gamma^{\tilde{m}_B-1}}{\Gamma(\tilde{m}_B)} \exp\left(-\frac{\tilde{m}_B \gamma}{\tilde{\gamma}_B} \right), \quad (16)$$

where \tilde{m}_B is the Nakagami fading parameter given by $\tilde{m}_B = (\tilde{K}_B + 1)^2 / (2\tilde{K}_B + 1)$ and $\Gamma(\mu) = \int_0^\infty e^{-t} t^{\mu-1} dt$, $\text{Re}(\mu) > 0$, is the Gamma function.

Following (10), the SNR of the eavesdropper's channel can be rewritten as

$$\gamma_E = \sum_{i=1}^{N_E} \gamma_{E,i}, \quad (17)$$

where $\gamma_{E,i} = \bar{\gamma}_E |\mathbf{g}_i \mathbf{b}|^2$, \mathbf{g}_i is the $1 \times N_A$ channel vector between Eve's i -th antenna and Alice, i.e., \mathbf{g}_i is the i -th row of \mathbf{G} . As per (3), we have

$$\mathbf{g}_i = \sqrt{\frac{K_E}{1+K_E}} \epsilon_i \mathbf{g}_o + \sqrt{\frac{1}{1+K_E}} \mathbf{g}_{r,i}, \quad (18)$$

where $\epsilon_i = e^{-j(i-1)\tau_E \cos \phi_E}$ and $\mathbf{g}_{r,i}$ is the i -th row of \mathbf{G}_r . For any value of i ($i = 1, 2, \dots, N_E$), we have

$$|\epsilon_i \mathbf{g}_o \mathbf{b}| = |\mathbf{g}_o \mathbf{b}|. \quad (19)$$

As such, following a procedure similar to that used in obtaining $f_{\gamma_B}(\gamma)$, the pdf of $\gamma_{E,i}$ can be approximated as

$$f_{\gamma_{E,i}}(\gamma) = \left(\frac{\tilde{m}_E}{\tilde{\gamma}_E} \right)^{\tilde{m}_E} \frac{\gamma^{\tilde{m}_E-1} \exp\left(-\frac{\tilde{m}_E \gamma}{\tilde{\gamma}_E}\right)}{\Gamma(\tilde{m}_E)}, \quad (20)$$

where \tilde{m}_E is given by $\tilde{m}_E = (\tilde{K}_E + 1)^2 / (2\tilde{K}_E + 1)$, \tilde{K}_E is given by $\tilde{K}_E = |\mathbf{g}_o \mathbf{b}|^2 K_E$, and $\tilde{\gamma}_E$ is given by

$$\tilde{\gamma}_E \triangleq \mathbb{E}[\gamma_E] = \frac{(K_E |\mathbf{g}_o \mathbf{b}|^2 + 1) \bar{\gamma}_E}{1 + K_E}. \quad (21)$$

Since the $\gamma_{E,i}$ are independent, following (21) the pdf of γ_E can be approximated as

$$f_{\gamma_E}(\gamma) = \left(\frac{\tilde{m}_E}{\tilde{\gamma}_E} \right)^{N_E \tilde{m}_E} \frac{\gamma^{N_E \tilde{m}_E - 1} \exp\left(-\frac{\tilde{m}_E \gamma}{\tilde{\gamma}_E}\right)}{\Gamma(N_E \tilde{m}_E)}. \quad (22)$$

Following (19), we note that γ_E is independent of \mathbf{r}_o . This indicates that the SNR at Eve is independent of ϕ_E when Eve adopts MRC to combine received signals (we do not need to know the orientation of the ULA at Eve for our analysis). This also reveals that the SNR at Eve is independent of the type of antenna array at Eve (e.g., other antenna arrays beyond ULAs) since different antenna arrays only impact \mathbf{r}_o . As such, our following analysis is also valid for other antenna arrays at Eve (e.g., non-uniform linear arrays, circular arrays, rectangle arrays).

B. Secrecy Performance of the LBB Scheme

In the wiretap channel, the secrecy capacity is defined as

$$C_s = \begin{cases} C_B - C_E, & \gamma_B > \gamma_E \\ 0, & \gamma_B \leq \gamma_E, \end{cases} \quad (23)$$

where $C_B = \log_2(1 + \gamma_B)$ is the capacity of the main channel and $C_E = \log_2(1 + \gamma_E)$ is the capacity of the eavesdropper's channel. Since C_B and C_E are unavailable at Alice, the perfect secrecy cannot be guaranteed in the wiretap channel of interest. For this reason we adopt the secrecy outage probability and the probability of non-zero secrecy capacity as our secrecy performance metrics. The secrecy outage probability is defined as the probability of the secrecy capacity C_s being less than the target secrecy rate R_s (bits/channel-use), which can be formulated as [8, 9]⁶

$$\begin{aligned} \mathcal{O}(R_s) &= \Pr(C_s < R_s) \\ &= \int_0^\infty f_{\gamma_E}(\gamma_E) \left[\int_0^{2^{R_s(1+\gamma_E)-1}} f_{\gamma_B}(\gamma_B) d\gamma_B \right] d\gamma_E. \end{aligned} \quad (24)$$

⁶The secrecy outage probability is the most common metric used in physical layer security when CSI on the channels is unavailable at Alice. However, it is important to note this metric does not distinguish between reliability and security [19].

With regard to the secrecy performance of the LBB scheme, we first provide the following theorem.

Theorem 1: The secrecy outage probability of the LBB scheme for a given R_s is

$$\begin{aligned} \mathcal{O}(R_s) &= \\ &= \frac{\tilde{m}_B \tilde{m}_E \tilde{m}_E^{N_E} 2^{\tilde{m}_B R_s}}{\Gamma(N_E \tilde{m}_E) \tilde{\gamma}_B^{-N_E \tilde{m}_E} \tilde{\gamma}_E^{-\tilde{m}_B}} \sum_{n=0}^{+\infty} \frac{2^{n R_s} \exp\left(-\frac{\tilde{m}_B (2^{R_s-1})}{\tilde{\gamma}_B}\right)}{\tilde{m}_B \tilde{\gamma}_B^n \Gamma(\tilde{m}_B + n + 1)} \times \\ &= \sum_{l=0}^{+\infty} \frac{(\tilde{m}_B + n)^l (2^{R_s-1})^l (\tilde{\gamma}_B \tilde{\gamma}_E)^{n-l} \Gamma_G(\tilde{m}_B + N_E \tilde{m}_E + n - l)}{2^{l R_s} (2^{R_s} \tilde{m}_B \tilde{\gamma}_E + \tilde{m}_E \tilde{\gamma}_B)^{\tilde{m}_B + N_E \tilde{m}_E + n - l}}, \end{aligned} \quad (25)$$

where $\Gamma_G(\cdot)$ is the generalized gamma function (also valid for negative integers), which is given by [21]

$$\Gamma_G(\alpha) = \begin{cases} \frac{(-1)^{-\alpha}}{(-\alpha)!} \left(\sum_{i=1}^{-\alpha} \frac{1}{i} + \alpha \right), & \alpha \text{ is a negative integer,} \\ \Gamma(\alpha), & \text{otherwise.} \end{cases} \quad (26)$$

Proof: Substituting (16) into (24), $\mathcal{O}(R_s)$ is derived as

$$\mathcal{O}(R_s) = \int_0^\infty f_{\gamma_E}(\gamma_E) \frac{\gamma \left(\tilde{m}_B, \frac{2^{R_s(1+\gamma_E)-1}}{\tilde{m}_B^{-1} \tilde{\gamma}_B} \right)}{\Gamma(\tilde{m}_B)} d\gamma_E, \quad (27)$$

where $\gamma(\alpha, \mu) = \int_0^\mu e^{-t} t^{\alpha-1} dt$, $\text{Re}\{\alpha\} > 0$, is the lower incomplete gamma function. In order to obtain the result in (27), we have utilized the following identity [22, Eq. (3.381.1)]

$$\int_0^u t^{\nu-1} e^{-\mu t} dt = \mu^{-\nu} \gamma(\nu, \mu u). \quad (28)$$

To make progress, we adopt the following identity to expand $\gamma(\alpha, \mu)$ [22, Eq. (8.354.1)]

$$\gamma(\alpha, \mu) = \sum_{n=0}^{+\infty} \frac{\Gamma(\alpha) \mu^{\alpha+n} e^{-\mu}}{\Gamma(\alpha + n + 1)}. \quad (29)$$

As per (29), we have

$$\begin{aligned} & \gamma \left(\tilde{m}_B, \frac{2^{R_s(1+\gamma_E)-1}}{\tilde{m}_B^{-1} \tilde{\gamma}_B} \right) \\ &= \sum_{n=0}^{+\infty} \frac{\Gamma(\tilde{m}_B) \left(\frac{2^{R_s(1+\gamma_E)-1}}{\tilde{m}_B^{-1} \tilde{\gamma}_B} \right)^{\tilde{m}_B+n} \exp\left(-\frac{2^{R_s(1+\gamma_E)-1}}{\tilde{m}_B^{-1} \tilde{\gamma}_B}\right)}{\Gamma(\tilde{m}_B + n + 1)} \\ &= \sum_{n=0}^{+\infty} \frac{\Gamma(\tilde{m}_B) (2^{R_s} \gamma_E)^{\tilde{m}_B+n} \left(1 + \frac{2^{R_s-1}}{2^{R_s} \gamma_E}\right)^{\tilde{m}_B+n}}{\left(\frac{\tilde{\gamma}_B}{\tilde{m}_B}\right)^{\tilde{m}_B+n} \exp\left(\frac{2^{R_s(1+\gamma_E)-1}}{\tilde{m}_B^{-1} \tilde{\gamma}_B}\right) \Gamma(\tilde{m}_B + n + 1)} \\ &= \sum_{n=0}^{+\infty} \frac{\Gamma(\tilde{m}_B) \exp\left(-\frac{2^{R_s(1+\gamma_E)-1}}{\tilde{m}_B^{-1} \tilde{\gamma}_B}\right) (2^{R_s} \gamma_E)^{\tilde{m}_B+n}}{\left(\frac{\tilde{\gamma}_B}{\tilde{m}_B}\right)^{\tilde{m}_B+n} \Gamma(\tilde{m}_B + n + 1)} \\ & \quad \times \sum_{l=0}^{+\infty} \binom{\tilde{m}_B + n}{l} \left(\frac{2^{R_s-1}}{2^{R_s} \gamma_E} \right)^l, \end{aligned} \quad (30)$$

in which the identity [22, Eq. (1.110)]

$$(1 + \mu)^\alpha = \sum_{l=0}^{+\infty} \binom{\alpha}{l} \mu^l \quad (31)$$

is employed. Substituting (22) and (30) into (27), we have

$$\begin{aligned} \mathcal{O}(R_s) &= \int_0^\infty \left(\frac{\tilde{m}_E}{\tilde{\gamma}_E} \right)^{N_E \tilde{m}_E} \frac{\gamma_E^{N_E \tilde{m}_E - 1}}{\Gamma(N_E \tilde{m}_E)} \exp\left(\frac{-\tilde{m}_E \gamma_E}{\tilde{\gamma}_E} \right) \times \\ &\quad \sum_{n=0}^{+\infty} \frac{\exp\left(\frac{2^{R_s}(1+\gamma_E)-1}{\tilde{m}_B \tilde{\gamma}_B} \right) (2^{R_s} \gamma_E)^{\tilde{m}_B + n}}{\left(\frac{\tilde{\gamma}_B}{\tilde{m}_B} \right)^{\tilde{m}_B + n} \Gamma(\tilde{m}_B + n + 1)} \times \\ &\quad \sum_{l=0}^{+\infty} \binom{\tilde{m}_B + n}{l} \left(\frac{2^{R_s} - 1}{2^{R_s} \gamma_E} \right)^l d\gamma_E \\ &= \frac{\tilde{m}_B \tilde{m}_E \tilde{\gamma}_B^{N_E \tilde{m}_E} 2^{\tilde{m}_B R_s}}{\Gamma(N_E \tilde{m}_E) \tilde{\gamma}_B^{\tilde{m}_B} \tilde{\gamma}_E^{N_E \tilde{m}_E}} \sum_{n=0}^{+\infty} \frac{\tilde{m}_B^n 2^{n R_s} \exp\left(\frac{-\tilde{m}_B (2^{R_s} - 1)}{\tilde{\gamma}_B} \right)}{\tilde{\gamma}_B^n \Gamma(\tilde{m}_B + n + 1)} \\ &\quad \sum_{l=0}^{+\infty} \frac{\binom{\tilde{m}_B + n}{l} (2^{R_s} - 1)^l}{2^{l R_s}} \int_0^\infty \frac{\gamma_E^{\tilde{m}_B + N_E \tilde{m}_E + n - l - 1}}{\exp\left(\frac{(2^{R_s} \tilde{m}_B \tilde{\gamma}_B + \tilde{m}_E \tilde{\gamma}_B) \gamma_E}{\tilde{\gamma}_B \tilde{\gamma}_E} \right)} d\gamma_E. \end{aligned} \quad (32)$$

We then obtain the desirable result in (25) by solving the integral in (32) as per the following identity [22, Eq. (3.381.4)]

$$\int_0^\infty t^{\nu-1} e^{-\mu t} dt = \frac{1}{\mu^\nu} \Gamma_G(\nu). \quad (33)$$

We first note the secrecy outage probability derived in (25) is a function of Bob and Eve's locations and the beamformer \mathbf{b} , all of which are embedded in the parameters \tilde{m}_B , \tilde{m}_E , $\tilde{\gamma}_B$, and $\tilde{\gamma}_E$. We also note that (25) is valid for arbitrary \tilde{m}_B and \tilde{m}_E (\tilde{m}_B and \tilde{m}_E can be equal), and thus (25) is valid for arbitrary K_B and K_E . As such, our derived expression for the secrecy outage probability is of more generality than that presented in [8], which is only valid for integral \tilde{m}_B and \tilde{m}_E . Although the expression presented in (25) involves two infinite series, they both can be approximated by finite series accurately. We approximate the infinite series $\sum_{n=0}^{+\infty}$ and $\sum_{l=0}^{+\infty}$ by truncating them at finite numbers. As we will show in Section IV, the accuracy of such approximations is acceptable as long as the truncating numbers are larger than approximately 100.

An important performance parameter associated with the secrecy outage probability is the secrecy diversity order, which determines the slope of the curve for the secrecy outage probability (in dB) versus $\tilde{\gamma}_B$ (in dB) as $\tilde{\gamma}_B \rightarrow \infty$ for finite $\tilde{\gamma}_E$. Mathematically, the secrecy diversity order is defined as

$$\beta = \lim_{\tilde{\gamma}_B \rightarrow \infty} \frac{\log_{10} \mathcal{O}(R_s)}{\log_{10}(1/\tilde{\gamma}_B)}. \quad (34)$$

The secrecy diversity order of the LBB scheme is presented in the following corollary.

Corollary 1: The secrecy diversity order of the LBB scheme is \tilde{m}_B .

Following a procedure similar to that used in deriving the secrecy diversity order of the antenna selection schemes presented in [8, 9], we can obtain in a straightforward manner

the secrecy diversity order of the LBB scheme as \tilde{m}_B . As such, we omit the proof of the above corollary here. We note that maximum value of \tilde{m}_B is $(N_A K_B + 1)^2 / (2 N_A K_B + 1)$ due to $|\mathbf{h}_o \mathbf{b}|^2 \leq \|\mathbf{h}_o\|^2 \|\mathbf{b}\|^2 = N_A$.

The probability of non-zero secrecy capacity is defined as the probability that a positive secrecy capacity is achieved. As per (23), it can be formulated as

$$\begin{aligned} P_{non} &= \Pr(C_s > 0) \\ &= 1 - \int_0^\infty f_{\gamma_E}(\gamma_E) \left(\int_0^{\gamma_E} f_{\gamma_B}(\gamma_B) d\gamma_B \right) d\gamma_E. \end{aligned} \quad (35)$$

Then, the probability of non-zero secrecy capacity of the LBB scheme is presented in the following corollary.

Corollary 2: The probability of non-zero secrecy capacity of the LBB scheme is given by

$$\begin{aligned} P_{non} &= 1 - \frac{\tilde{m}_B \tilde{m}_E \tilde{\gamma}_B^{N_E \tilde{m}_E}}{\Gamma(N_E \tilde{m}_E) \tilde{\gamma}_B^{\tilde{m}_B} \tilde{\gamma}_E^{N_E \tilde{m}_E}} \sum_{n=0}^{+\infty} \frac{\tilde{m}_B^n \tilde{\gamma}_E^n}{\Gamma(\tilde{m}_B + n + 1)} \\ &\quad \times \frac{\Gamma(\tilde{m}_B + N_E \tilde{m}_E + n)}{\left(\tilde{m}_B \tilde{\gamma}_E + \tilde{m}_E \tilde{\gamma}_B \right)^{\tilde{m}_B + N_E \tilde{m}_E + n}}. \end{aligned} \quad (36)$$

Proof: As per (35), the probability of non-zero secrecy capacity can also be formulated as

$$P_{non} = 1 - \mathcal{O}(R_s = 0). \quad (37)$$

Substituting $R_s = 0$ into (25), we obtain the desirable result in (36). ■

We note that the expression for the probability of non-zero secrecy capacity is simpler than that for the secrecy outage probability and it only involves one infinite series. This infinite series can also be approximated by truncating it at a finite number. This approximation is very accurate even when the truncating number is small (e.g., 10).

C. Optimal Location-based Beamformer

A location-based beamformer can be written as

$$\mathbf{b} = \frac{1}{\sqrt{N_A}} [1, \dots, \exp(-j(N_A - 1)\tau_A \cos \psi)]^T, \quad (38)$$

where ψ ($0 \leq \psi \leq \pi$) is the beamforming direction. In this work we define the optimal location-based beamformer, \mathbf{b}^* , as the one that minimizes the secrecy outage probability for a given R_s . Therefore, defining

$$\psi^* = \underset{0 \leq \psi \leq \pi}{\operatorname{argmin}} \mathcal{O}(R_s), \quad (39)$$

and setting $\psi = \psi^*$ in (38) completely define the optimal beamformer \mathbf{b}^* . We note that the value range of ψ is selected based on the symmetric property of the ULA (e.g., $\psi = \pi/3$ and $\psi = -\pi/3$ lead to the same beamformer \mathbf{b}). We note that (39) is a one-dimensional optimization problem, which can be solved through numerical search. Substituting \mathbf{b}^* into (25), we achieve the minimum secrecy outage probability of the LBB scheme, which is denoted as $\mathcal{O}^*(R_s)$. We would like to highlight that ψ^* can be analytically determined in some special cases as detailed in the following corollaries.

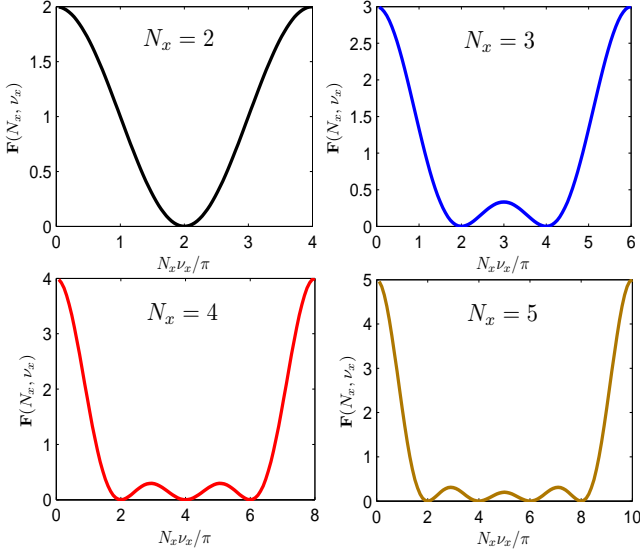


Fig. 2. $\mathbf{F}(N_x, \nu_x)$ versus $N_x \nu_x / \pi$ for different values of N_x .

Corollary 3: For $K_B > 0$, the solution to (39) is $\psi^* = \theta_B$ in the following cases: (i) when $\bar{\gamma}_B \rightarrow \infty$ for finite $\bar{\gamma}_E$, (ii) when $K_E = 0$, or (iii) when θ_E is unavailable at Alice.

Proof: In Case (i), as $\bar{\gamma}_B \rightarrow \infty$ the secrecy diversity order determines the secrecy outage probability. As such, as $\bar{\gamma}_B \rightarrow \infty$ the optimal location-based beamformer is to maximize the secrecy diversity order given in Corollary 1 (i.e., \tilde{m}_B) in order to minimize the secrecy outage probability. To this end, ψ^* is to maximize \tilde{K}_B . Following (14), ψ^* finally is to maximize $|\mathbf{h}_o \mathbf{b}|^2$. In Case (ii), there is no LOS component in the eavesdropper's channel due to $K_E = 0$ and ψ does not impact γ_E . As such, ψ^* is to maximize γ_B in order to minimize the secrecy outage probability. Following (9), ψ^* finally is to maximize $|\mathbf{h}_o \mathbf{b}|^2$ in this case. In Case (iii), Alice is not sure how ψ impacts γ_E since θ_E is unknown. Then, ψ is to maximize γ_B and thus to maximize $|\mathbf{h}_o \mathbf{b}|^2$ based on (9).

As we can see from the above discussion, in all three cases of the corollary the value of ψ^* is the one that maximizes $|\mathbf{h}_o \mathbf{b}|^2$. So, to complete the proof we now prove that this value is indeed θ_B . Denoting $\nu_A = \tau_A (\cos \theta_B - \cos \psi)$, as per (2) and (38), for $\nu_A \neq 0$ we have

$$\begin{aligned} \mathbf{h}_o \mathbf{b} &= \frac{1}{\sqrt{N_A}} \frac{\exp(jN_t \nu_A) - 1}{\exp(j\nu_A) - 1} \\ &= \frac{1}{\sqrt{N_A}} \frac{-e^{jN_A \nu_A / 2} (-e^{-jN_A \nu_A / 2} - e^{jN_A \nu_A / 2})}{-e^{j\nu_A / 2} (-e^{-j\nu_A / 2} - e^{j\nu_A / 2})} \\ &= \frac{1}{\sqrt{N_A}} \frac{\sin(\frac{1}{2}N_A \nu_A)}{\sin(\frac{1}{2}\nu_A)} e^{j\nu_A(N_A-1)/2}. \end{aligned} \quad (40)$$

For $\nu_A = 0$, we have $\mathbf{h}_o \mathbf{b} = \sqrt{N_A}$. Then, following (40) we have

$$|\mathbf{h}_o \mathbf{b}|^2 = \mathbf{F}(N_A, \nu_A), \quad (41)$$

where $\mathbf{F}(\cdot, \cdot)$ is defined as

$$\mathbf{F}(N_x, \nu_x) = \begin{cases} N_x, & \nu_x = 0, \\ \frac{1}{N_x} \left(\frac{\sin(\frac{1}{2}N_x \nu_x)}{\sin(\frac{1}{2}\nu_x)} \right)^2, & 0 \leq \nu_x < 2\pi. \end{cases} \quad (42)$$

It is straightforward to prove that the maximum value of $\mathbf{F}(N_x, \nu_x)$ is N_x , which is achieved for $\nu_x = 0$. This is also confirmed by Fig. 2, where we plot $\mathbf{F}(N_x, \nu_x)$ versus $N_x \nu_x / \pi$ for different value of N_x . As such, $|\mathbf{h}_o \mathbf{b}|^2$ is maximized when $\nu_A = 0$ and thus we have $\psi^* = \theta_B$ (we ignore the negative solutions due to $0 \leq \psi \leq \pi$) in order to maximize $|\mathbf{h}_o \mathbf{b}|^2$. ■

We note that for $\psi^* = \theta_B$ we have $\mathbf{b}^* = \mathbf{h}_o^\dagger / \sqrt{N_A}$ and $|\mathbf{h}_o \mathbf{b}|^2 = N_A$. As such, we have $\tilde{K}_B = N_A K_B$ and $\tilde{\gamma}_B = (N_A K_B + 1) \bar{\gamma}_B / (1 + K_B)$. We denote the secrecy outage probability of the LBB scheme with unknown Eve's location (i.e., $\psi^* = \theta_B$) as $\mathcal{O}_b(R_s)$.

Corollary 4: For $K_E > 0$, the (multiple) solution to (39) is $\psi^* = \arccos(\cos \theta_E + \frac{2n_A \pi}{N_A \tau_A})$, $n_A = 1, \dots, N_A - 1$, in the following cases: (i) when $\bar{\gamma}_E \rightarrow \infty$ for finite $\bar{\gamma}_B$, (ii) when $K_B = 0$, or (iii) when θ_B is unavailable at Alice.

Proof: Following similar arguments to those used in the proof of Corollary 3, we know that ψ^* is to minimize $|\mathbf{g}_o \mathbf{b}|^2$ for all three cases in Corollary 4. The value of $|\mathbf{g}_o \mathbf{b}|^2$ is given by

$$|\mathbf{g}_o \mathbf{b}|^2 = \mathbf{F}(N_A, \nu_E), \quad (43)$$

where $\nu_E = \tau_A (\cos \theta_E - \cos \psi)$. We note that the minimum value of $\mathbf{F}(N_x, \nu_x)$ is achieved when $\nu_x = 2n_x \pi$ for $n_x = 1, \dots, N_x - 1$, which is also confirmed by Fig. 2. As such, $|\mathbf{g}_o \mathbf{b}|^2$ is minimized when $\nu_E = 2n_A \pi$ for $n_A = 1, \dots, N_A - 1$, and thus we obtain Corollary 4. ■

IV. NUMERICAL RESULTS

In this section we present numerical simulations to verify our secrecy performance analysis of the LBB scheme, and examine the impact of different system parameters (e.g., K_B , K_E , $\bar{\gamma}_B$, and $\bar{\gamma}_E$) on the LBB scheme. To better illustrate the gains obtained by our scheme, we will also present simulations of the secrecy performance of the NB (non-beamforming) scheme. This latter scheme represents the case when an isotropic beamforming pattern is produced by Alice (see Appendix A for an analytical analysis of this scheme). To conduct simulations, we deploy Bob and Eve at specific locations and then map such locations into $\bar{\gamma}_B$ and $\bar{\gamma}_E$, respectively. Such a mapping is based on Alice's transmit power (i.e., P) and path loss exponents of the main channel and the eavesdropper's channel (i.e., η_B and η_E). For presentation convenience, we only specify the values of $\bar{\gamma}_B$ and $\bar{\gamma}_E$ adopted in our following simulations. We note that in the following figures we use "Theo" and "Simu" as the abbreviations of "Theoretic" and "Simulated", respectively.

In Fig. 3 we first verify our derived secrecy outage probabilities for Nakagami fading channels. To this end, we generate channel realizations as per the Nakagami fading channel, where we have set $\tilde{m}_B = 2m_B$, $\tilde{m}_E = m_E$, $\tilde{\gamma}_B = 3\bar{\gamma}_B$, and $\tilde{\gamma}_E = \bar{\gamma}_E$, where $m_B = (K_B + 1)^2 / (2K_B + 1)$ and $m_E = (K_E + 1)^2 / (2K_E + 1)$. The theoretic secrecy outage

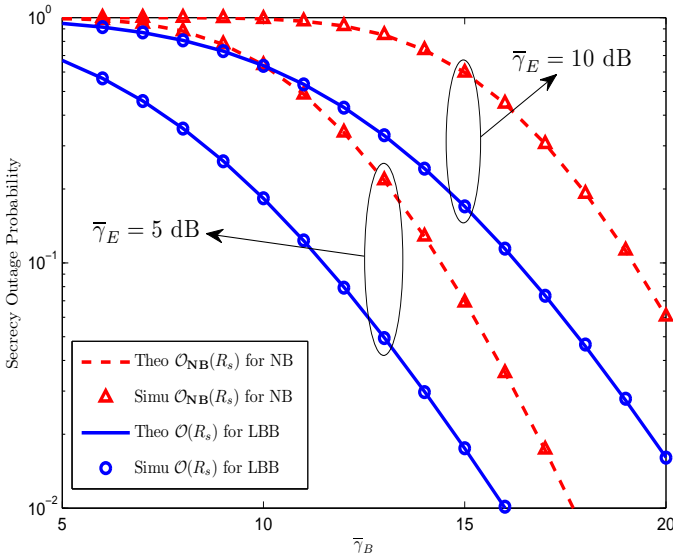


Fig. 3. Secrecy outage probabilities under Nakagami channels versus different values of $\bar{\gamma}_B$, where $m_B = 1.35$, $m_E = 1.33$, $\lambda_0 = 0.85$, $N_A = 3$, $N_E = 2$, and $R_s = 1$.

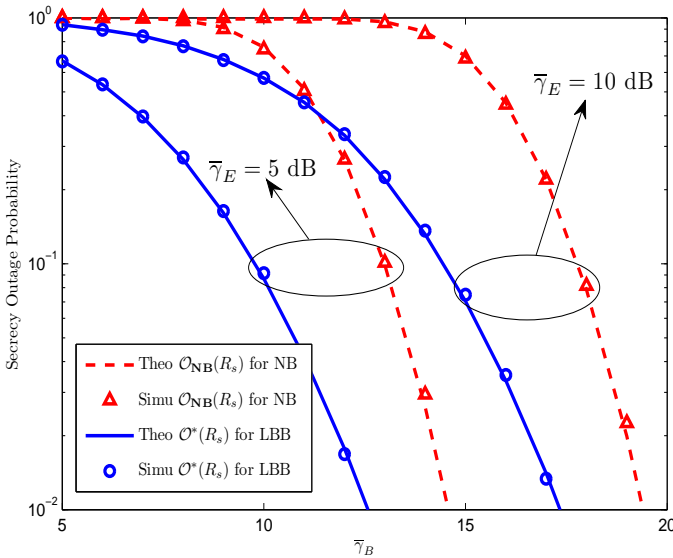


Fig. 4. Secrecy outage probabilities under Rician channels versus different values of $\bar{\gamma}_B$, where $N_A = 3$, $N_E = 2$, $K_B = 10$ dB, $K_E = 5$ dB, $\theta_B = \pi/3$, $\theta_E = \pi/4$, and $R_s = 1$.

probability of the LBB scheme, $\mathcal{O}(R_s)$, and the secrecy outage probability of the NB scheme, denoted as $\mathcal{O}_{NB}(R_s)$, are obtained through (25) and (49), respectively, where relevant infinite series are truncated at 100. In this figure, we observe that the theoretic $\mathcal{O}(R_s)$ and $\mathcal{O}_{NB}(R_s)$ precisely match the simulated $\mathcal{O}(R_s)$ and $\mathcal{O}_{NB}(R_s)$, respectively. This confirms the correctness of our derived secrecy outage probabilities.

Recall that for mathematical convenience, our analysis approximates a Rician channel with a Nakagami channel. To see the effect of this, in Fig. 4 we again plot the secrecy outage probabilities of the LBB scheme and the NB scheme, but this time for specific Rician fading channels. In this figure, we observe that the simulated minimum secrecy outage prob-

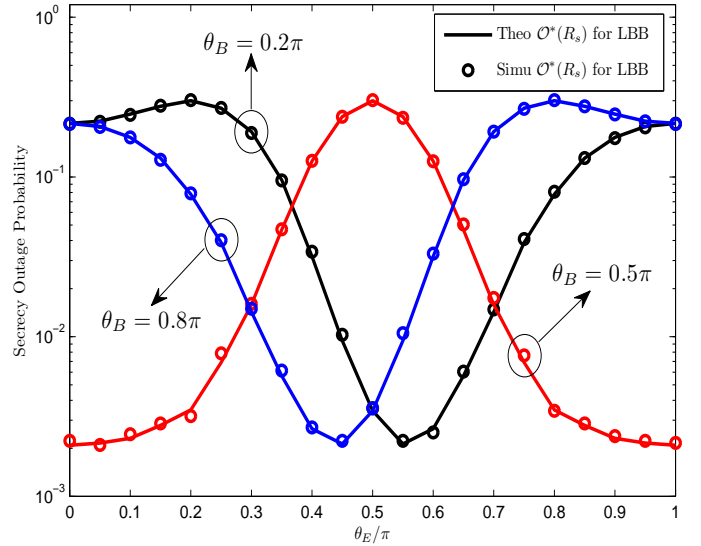


Fig. 5. Minimum secrecy outage probability of the LBB scheme versus different values of θ_E , where $N_A = 2$, $N_E = 2$, $K_B = 10$ dB, $K_E = 10$ dB, $\bar{\gamma}_B = 10$ dB, $\bar{\gamma}_E = 10$ dB, and $R_s = 1$.

ability of the LBB scheme, $\mathcal{O}^*(R_s)$, and the secrecy outage probability of the NB scheme, $\mathcal{O}_{NB}(R_s)$, match extremely well the theoretic $\mathcal{O}^*(R_s)$ and $\mathcal{O}_{NB}(R_s)$, respectively, thus confirming the validity of our channel approximation. We note that we have set θ_E very close to θ_B in Fig. 4 (i.e., $\theta_B = \pi/3$ and $\theta_E = \pi/4$). The gap between $\mathcal{O}^*(R_s)$ and $\mathcal{O}_{NB}(R_s)$ can even be larger when θ_E is not so close to θ_B .

In Fig. 5, we plot the minimum secrecy outage probability of the LBB scheme, $\mathcal{O}^*(R_s)$, versus different values of θ_E . Again we observe that the theoretic $\mathcal{O}^*(R_s)$ matches extremely well the simulated $\mathcal{O}^*(R_s)$, which again confirms the validity of our analysis. Fig. 5 is also useful in that it more visually represents how the minimum secrecy outage probability of the LBB scheme depends on the locations of Bob and Eve. For example, $\mathcal{O}^*(R_s)$ is maximized when $\theta_B = \theta_E$. In the simulations to obtain Fig. 5, we also observe that the optimal beamforming direction ψ^* shifts away from θ_B as θ_E approaches to θ_B .

In Fig. 6, we examine the secrecy outage probability of the LBB scheme without knowing Eve's location, $\mathcal{O}_b(R_s)$. As per Corollary 3, we know that $\mathbf{b}^* = \mathbf{h}^\dagger / \|\mathbf{h}\|$ when Eve's location is unavailable at Alice. In Fig. 6 we also compare the the solution with no information on Eve's location to the NB scheme. To conduct a fair comparison with the NB scheme, we assume Eve's location is uniformly distributed on a circle centered at Alice, i.e., θ_E uniformly distributes between 0 and 2π , $\theta_E \sim \mathcal{U}[0, 2\pi]$. We then average $\mathcal{O}_b(R_s)$ over θ_E to obtain the average secrecy outage probability, denoted as $\bar{\mathcal{O}}_b(R_s)$. As expected, we observe that $\bar{\mathcal{O}}_b(R_s)$ is lower than $\mathcal{O}_{NB}(R_s)$, which demonstrates that the LBB scheme still outperforms the NB scheme *on average*, even when Eve's location is unavailable at Alice. This is due to the fact that the LBB scheme improves the quality of the main channel based on Bob's location, which on average reduces the secrecy outage probability. However, the most important result obtained from

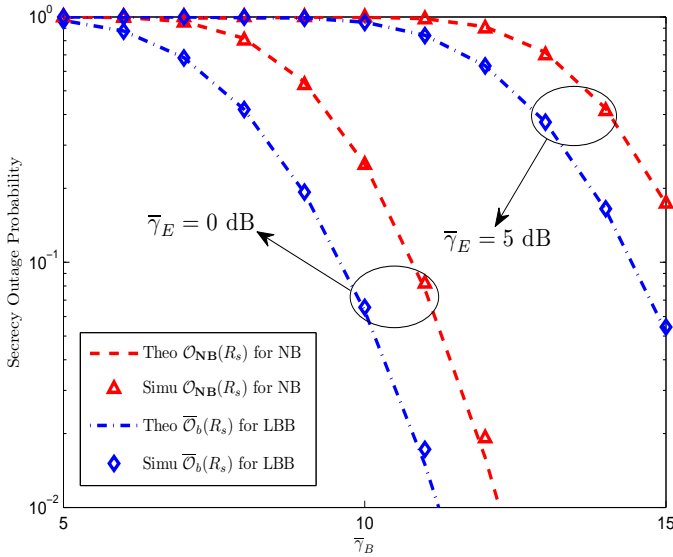


Fig. 6. Secrecy outage probabilities without Eve's location versus different values of $\bar{\gamma}_B$, where $N_A = 3$, $N_E = 4$, $K_B = 10$ dB, $K_E = 5$ dB, $\theta_B = \pi/3$, and $R_s = 1$.

the simulations of Fig. 6 is that the secrecy outage probability of the LBB scheme without Eve's location increases (e.g., by approximately a factor of 5 for $\bar{\gamma}_B = 10$ dB) relative to that of the LBB scheme with Eve's location. This quantifies the value of the location information of Eve to the beamformer solution.

It is worth mentioning how relaxations of some key assumptions we have made impact the results presented here. Of course, in reality it will never be the case that all reported locations, all K map information, and all path loss exponents are known with zero error. Errors in these quantities are intermingled in the sense that an error in one leads to an error in another. We have attempted to encompass such correlated errors in a range of additional simulations. Our general result is that a percentage error of 15% in any of these inputs leads to an approximately 10% percentage error in our reported outage probabilities. For anticipated error inputs, we can therefore say that our analysis remains reasonably accurate.

Finally, although outside the spirit of our low-complexity LBB scheme, it is perhaps worth discussing the gains to be made when the full CSI information of the main channel is made available to Alice (where the transmission scheme is named as the full-CSI scheme). If Eve's location is also available at Alice in the full-CSI scheme, the full-CSI scheme will of course outperform the LBB scheme for any values of system parameters. For example, under the simulation settings of Fig. 4, the secrecy outage probability of this full-CSI scheme with Eve's location is 15% lower than that of the LBB scheme for $\bar{\gamma}_B = 10$ dB and $\bar{\gamma}_E = 5$ dB (determined from simulations). If Eve's location is unavailable at Alice (in both schemes) then the full-CSI scheme outperforms the LBB scheme by 40% for $\bar{\gamma}_B = 10$ dB and $\bar{\gamma}_E = 0$ dB under the same simulation setting of Fig. 6 (determined from simulations and analysis). For completeness, the secrecy performance analysis of the full-CSI scheme is given in Appendix B.

V. CONCLUSIONS

We proposed and analyzed a novel beamforming scheme in the wiretap channel where both the main channel and the eavesdropper's channel are subject to Rician fading. Our new LBB scheme solely requires as inputs the location information of Bob and Eve, and does not require the CSI of the main channel or the eavesdropper's channel. We derived the secrecy outage probability of the LBB scheme in a closed-form expression valid for arbitrary values of K_B and K_E . We then determined the optimal location-based beamformer that minimizes the secrecy outage probability. Comparisons with a range of other schemes were then carried out so as to better understand the performance gains offered by our location-based solution. The work we presented will be important for a range of application scenarios in which Rician channels are expected to be dominant and where location information of potential users and adversaries are known.

APPENDIX A

SECURITY PERFORMANCE OF THE NB SCHEME

In the NB scheme, Alice distributes her total transmit power uniformly among the N_A orthogonal independent transmit directions (i.e., the covariance matrix of $\mathbf{b}x$ is $P\mathbf{I}_{N_A}/N_A$) [23, 24]. Then, the SNR at Bob is given by [23, 24]

$$\gamma_B^{\text{NB}} = \frac{\bar{\gamma}_B \|\mathbf{h}\|^2}{N_A}. \quad (44)$$

Interpreting Rician fading as a special case of Nakagami fading, the pdf of γ_B^{NB} can be approximated by

$$f_{\gamma_B^{\text{NB}}}(\gamma) = \frac{m_B^{N_A m_B} \gamma^{N_A m_B - 1} e^{-\frac{N_A m_B \gamma}{\bar{\gamma}_B}}}{\Gamma(N_A m_B) (\bar{\gamma}_B / N_A)^{N_A m_B}}. \quad (45)$$

We assume that Eve applies MRC to combine the received signals at different antenna elements. As such, the SNR at Eve is given by

$$\gamma_E^{\text{NB}} = \frac{\bar{\gamma}_E \|\mathbf{s}_0^\dagger \mathbf{G}\|^2}{N_A} = \frac{\bar{\gamma}_E \lambda_0^2}{N_A}, \quad (46)$$

where \mathbf{s}_0 is the $N_E \times 1$ eigenvector for the largest eigenvalue λ_0 of \mathbf{G} . The theoretical expression for the distribution of λ_0^2 has been derived in [25]. However, this expression is too complicated to be used for further analysis. To make progress, we adopt the simple approximation for the pdf of λ_0^2 proposed in [26]. As such, the pdf of γ_E^{NB} can be approximated by

$$f_{\gamma_E^{\text{NB}}}(\gamma) = \frac{(N_A m_E)^{N_A N_E m_E} \gamma^{N_A N_E m_E - 1}}{\Gamma(N_A N_E m_E) (\bar{\gamma}_E \bar{\lambda}_0)^{N_A N_E m_E}} \exp\left(-\frac{N_A m_E \gamma}{\bar{\gamma}_E \bar{\lambda}_0}\right), \quad (47)$$

where $\bar{\lambda}_0$ is the mean of the per-branch largest eigenvalue (i.e., $\bar{\lambda}_0 = \mathbb{E}[\lambda_0]/N_A N_E$). The value of $\bar{\lambda}_0$ can be approximated by [26]

$$\bar{\lambda}_0 = \begin{cases} \frac{K_E}{K_E + 1} + \frac{1}{K_E + 1} \frac{N_A + N_E}{N_A N_E + 1}, & K_E \geq 0.5, \\ \left(\frac{N_A + N_E}{N_A N_E + 1}\right)^{\frac{4 - K_E}{6}}, & K_E < 0.5. \end{cases} \quad (48)$$

We note that we have $\bar{\lambda}_0 = 1$ for arbitrary K_E when $N_E = 1$.

Following a similar procedure to that used in deriving $\mathcal{O}(R_s)$ in Theorem 1, the secrecy outage probability of the NB scheme is derived as

$$\begin{aligned} \mathcal{O}_{\text{NB}}(R_s) &= \int_0^\infty f_{\gamma_E^{\text{NB}}}(\gamma_E) \left[\int_0^{2^{R_s}(1+\gamma_E)^{-1}} f_{\gamma_B^{\text{NB}}}(\gamma_B) d\gamma_B \right] d\gamma_E \\ &= \frac{m_B^{N_A m_B} m_E^{N_A N_E m_E} 2^{N_A m_B R_s}}{\Gamma(N_A N_E m_E) \bar{\gamma}_B^{-N_A N_E m_E} (\bar{\gamma}_E \bar{\lambda}_0)^{-N_A m_B}} \times \\ &\quad \sum_{n=0}^{+\infty} \frac{m_B^n 2^{n R_s} \exp\left(-\frac{N_A m_B (2^{R_s} - 1)}{\bar{\gamma}_B}\right)}{\bar{\gamma}_B^n \Gamma(N_A m_B + n + 1)} \times \\ &\quad \sum_{l=0}^{+\infty} \frac{\binom{N_A m_B + n}{l} (2^{R_s} - 1)^l}{N_A^{-l} 2^{l R_s}} \times \\ &\quad \frac{(\bar{\gamma}_B \bar{\gamma}_E \bar{\lambda}_0)^{n-1} \Gamma_G(N_A m_B + N_A N_E m_E + n - l)}{(2^{R_s} m_B \bar{\gamma}_E \bar{\lambda}_0 + m_E \bar{\gamma}_B)^{N_A m_B + N_A N_E m_E + n - l}}. \quad (49) \end{aligned}$$

As per (49), we can see that the secrecy outage probability of the NB scheme is independent of θ_B and θ_E . However, (49) is a function of $\bar{\gamma}_B$ and $\bar{\gamma}_E$, which are dependent on d_B and d_E , respectively. We note that the secrecy diversity order of the NB scheme is $N_A m_B$, which is the full secrecy diversity order. Also, following a similar procedure to that used in deriving P_{non} in Corollary 2, the probability of non-zero secrecy capacity of the NB scheme is derived as

$$\begin{aligned} P_{\text{non}}^{\text{NB}} &= 1 - \frac{m_B^{N_A m_B} m_E^{N_A N_E m_E} \bar{\gamma}_B^{-N_A N_E m_E}}{\Gamma(N_A N_E m_E) (\bar{\gamma}_E \bar{\lambda}_0)^{-N_A m_B}} \times \\ &\quad \sum_{n=0}^{+\infty} \frac{m_B^n (\bar{\gamma}_E \bar{\lambda}_0)^n}{\Gamma(N_A m_B + n + 1)} \times \\ &\quad \frac{\Gamma(N_A m_B + N_A N_E m_E + n)}{(m_B \bar{\gamma}_E \bar{\lambda}_0 + m_E \bar{\gamma}_B)^{N_A m_B + N_A N_E m_E + n}}. \quad (50) \end{aligned}$$

APPENDIX B

SECURITY PERFORMANCE OF THE FULL-CSI SCHEME

In the full-CSI scheme, Alice knows the CSI of the main channel (Bob feeds back the CSI to Alice), but Alice does not know the CSI of the eavesdropper's channel or Eve's location. Then, Alice adopts $\mathbf{h}^\dagger/\|\mathbf{h}\|$ as the beamformer \mathbf{b} to maximize the SNR of the main channel [24, 27] in order to minimize the secrecy outage probability. The SNR at Bob of the full-CSI scheme is given by [24, 27]

$$\gamma_B^{\text{CSI}} = \bar{\gamma}_B \|\mathbf{h}\|^2. \quad (51)$$

Again using the Nakagami fading to approximate the Rician fading, the pdf of γ_B^{CSI} can be approximated by

$$f_{\gamma_B^{\text{CSI}}}(\gamma) = \frac{m_B^{N_A m_B} \gamma^{N_A m_B - 1} \exp\left(-\frac{m_B \gamma}{\bar{\gamma}_B}\right)}{\Gamma(N_A m_B) \bar{\gamma}_B^{-N_A m_B}}. \quad (52)$$

We assume that Eve knows \mathbf{h} by eavesdropping on the feedback from Bob to Alice. We also assume that Eve knows that Alice adopts $\mathbf{h}^\dagger/\|\mathbf{h}\|$ as the beamformer. Assuming that

Eve applies MRC to combine the received signals at different antenna elements, the SNR at Eve is given by

$$\gamma_E^{\text{CSI}} = \frac{\bar{\gamma}_E \|\mathbf{G}\mathbf{h}^\dagger\|^2}{\|\mathbf{h}\|^2} = \bar{\gamma}_E \sum_{i=1}^{N_E} \gamma_{E,i}^{\text{CSI}}, \quad (53)$$

where $\gamma_{E,i}^{\text{CSI}} = |\mathbf{g}_i \mathbf{h}^\dagger/\|\mathbf{h}\|$. In order to derive the pdf of γ_E^{CSI} , we next first derive the pdf of $\gamma_{E,i}^{\text{CSI}}$. As per (1) and (3), we have

$$\begin{aligned} \frac{\mathbf{g}_i \mathbf{h}^\dagger}{\|\mathbf{h}\|} &= \frac{1}{\|\mathbf{h}\|} (e_o \epsilon_i \mathbf{g}_o + e_r \mathbf{g}_r) (b_o \mathbf{h}_o + b_r \mathbf{h}_r)^\dagger \\ &= \frac{b_o e_o \epsilon_i \mathbf{g}_o \mathbf{h}_o^\dagger}{\|\mathbf{h}\|} + \frac{b_r e_o \epsilon_i \mathbf{g}_o \mathbf{h}_r^\dagger}{\|\mathbf{h}\|} + \frac{e_r \mathbf{g}_r \mathbf{h}^\dagger}{\|\mathbf{h}\|}, \quad (54) \end{aligned}$$

where

$$\begin{aligned} b_o &= \sqrt{\frac{K_B}{K_B + 1}}, & b_r &= \sqrt{\frac{1}{K_B + 1}}, \\ e_o &= \sqrt{\frac{K_E}{K_E + 1}}, & e_r &= \sqrt{\frac{1}{K_E + 1}}. \end{aligned}$$

To make progress, we make the following approximation

$$\frac{\mathbf{g}_i \mathbf{h}^\dagger}{\|\mathbf{h}\|} \approx \underbrace{\frac{b_o e_o \epsilon_i \mathbf{g}_o \mathbf{h}_o^\dagger}{\sqrt{N_A}}}_{h_o^{\text{CSI}}} + \underbrace{\frac{b_r e_o \epsilon_i \mathbf{g}_o \mathbf{h}_r^\dagger}{\sqrt{N_A}}}_{h_r^{\text{CSI}}} + \frac{e_r \mathbf{g}_r \mathbf{h}^\dagger}{\sqrt{N_A}}. \quad (55)$$

We note that in (55) h_o^{CSI} is deterministic and h_r^{CSI} is a circularly-symmetric complex Gaussian random variable. As such, $\mathbf{g}_i \mathbf{h}^\dagger/\sqrt{N_A}$ follows a Rician distribution. Following (55), we have

$$|h_o^{\text{CSI}}|^2 = \frac{b_o^2 e_o^2 |\mathbf{g}_o \mathbf{h}_o^\dagger|^2}{N_A} = \frac{K_B K_E |\mathbf{g}_o \mathbf{h}_o^\dagger|^2}{N_A (1 + K_B) (1 + K_E)},$$

and

$$\begin{aligned} \mathbb{E}[|h_r^{\text{CSI}}|^2] &= \frac{b_r^2 e_o^2}{N} \mathbb{E}[|\mathbf{g}_o \mathbf{h}_r^\dagger|^2] + \frac{e_r^2}{N} \mathbb{E}[|\mathbf{g}_r \mathbf{h}^\dagger|^2] \\ &= b_r^2 e_o^2 + e_r^2 \\ &= \frac{K_B + K_E + 1}{(K_B + 1)(K_E + 1)}. \end{aligned}$$

Then, the Rician K -factor of $\mathbf{g}_i \mathbf{h}^\dagger/\sqrt{N_A}$ is given by

$$\ddot{K}_E \triangleq \frac{|h_o^{\text{CSI}}|^2}{\mathbb{E}[|h_r^{\text{CSI}}|^2]} = \frac{K_B K_E |\mathbf{g}_o \mathbf{h}_o^\dagger|^2}{N_A (K_B + K_E + 1)}. \quad (56)$$

Following (55), we also have

$$\begin{aligned} \ddot{\gamma}_E &\triangleq \mathbb{E}[\gamma_{E,i}^{\text{CSI}}] = \bar{\gamma}_E (|h_o^{\text{CSI}}|^2 + \mathbb{E}[|h_r^{\text{CSI}}|^2]) \\ &= \frac{K_B K_E |\mathbf{g}_o \mathbf{h}_o^\dagger|^2 + N_A (K_B + K_E + 1)}{\bar{\gamma}_E^{-1} N_A (K_B + 1) (K_E + 1)}. \quad (57) \end{aligned}$$

Then, the pdf of $\gamma_{E,i}^{\text{CSI}}$ can be approximated by

$$f_{\gamma_{E,i}^{\text{CSI}}}(\gamma) = \left(\frac{\ddot{m}_E}{\ddot{\gamma}_E}\right)^{\ddot{m}_E} \frac{\gamma^{\ddot{m}_E - 1} \exp\left(-\frac{\ddot{m}_E \gamma}{\ddot{\gamma}_E}\right)}{\Gamma(\ddot{m}_E)}, \quad (58)$$

where $\ddot{m}_E = (\ddot{K}_E + 1)^2 / (2\ddot{K}_E + 1)$. Since $\gamma_{E,i}^{\text{CSI}}$ are independent from each other, the pdf of γ_E^{CSI} can be approximated by

$$f_{\gamma_E^{\text{CSI}}}(\gamma) = \left(\frac{\ddot{m}_E}{\ddot{\gamma}_E}\right)^{N_E \ddot{m}_E} \frac{\gamma^{N_E \ddot{m}_E - 1} \exp\left(-\frac{\ddot{m}_E \gamma}{\ddot{\gamma}_E}\right)}{\Gamma(N_E \ddot{m}_E)}. \quad (59)$$

Following a similar procedure to that used in deriving $\mathcal{O}(R_s)$ in Theorem 1, the secrecy outage probability of the full-CSI scheme is then derived as

$$\begin{aligned} \mathcal{O}_{\text{CSI}}(R_s) &= \int_0^\infty f_{\gamma_E^{\text{CSI}}}(\gamma_E) \left[\int_0^{2^{R_s(1+\gamma_E)-1}} f_{\gamma_B^{\text{CSI}}}(\gamma_B) d\gamma_B \right] d\gamma_E \\ &= \frac{m_B^{N_A m_B} \ddot{m}_E^{N_E \ddot{m}_E} 2^{N_A m_B R_s}}{\Gamma(N_E \ddot{m}_E) \bar{\gamma}_B^{-N_E \ddot{m}_E} \bar{\gamma}_E^{-N_A m_B}} \times \\ &\quad \sum_{n=0}^{+\infty} \frac{2^{n R_s} \exp\left(-\frac{m_B(2^{R_s}-1)}{\bar{\gamma}_B}\right)}{m_B^n \bar{\gamma}_E^{-n} \Gamma(N_A m_B + n + 1)} \times \\ &\quad \sum_{l=0}^{+\infty} \frac{\binom{N_A m_B + n}{l} (2^{R_s}-1)^l \Gamma_G(N_A m_B + N_E \ddot{m}_E + n - l)}{(\bar{\gamma}_B \bar{\gamma}_E)^l 2^{l R_s} (2^{R_s} m_B \bar{\gamma}_E + \ddot{m}_E \bar{\gamma}_B)^{N_A m_B + N_E \ddot{m}_E + n - l}}. \end{aligned} \quad (60)$$

As per (60), we know that the secrecy outage probability of the full-CSI scheme is dependent on the locations of both Bob and Eve. This means that we require Bob and Eve's locations for the secrecy performance analysis of the full-CSI scheme. The locations of both Bob and Eve are not only required by the LBB scheme. We note that the secrecy diversity order of the full-CSI scheme is also $N_A m_B$ (full diversity order). Again following a similar procedure of deriving P_{non} in Corollary 2, the probability of non-zero secrecy capacity of the full-CSI scheme is derived as

$$\begin{aligned} P_{\text{non}}^{\text{CSI}} &= 1 - \frac{m_B^{N_A m_B} \ddot{m}_E^{N_E \ddot{m}_E}}{\Gamma(N_E \ddot{m}_E) \bar{\gamma}_E^{-N_A m_B} \bar{\gamma}_B^{-N_E \ddot{m}_E}} \times \\ &\quad \sum_{n=0}^{+\infty} \frac{m_B^n \bar{\gamma}_E^{-n}}{\Gamma(N_A m_B + n + 1)} \times \\ &\quad \frac{\Gamma(N_A m_B + N_E \ddot{m}_E + n)}{(m_B \bar{\gamma}_E + \ddot{m}_E \bar{\gamma}_B)^{N_A m_B + N_E \ddot{m}_E + n}}. \end{aligned} \quad (61)$$

REFERENCES

- [1] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Commun. Mag.*, vol. 18, no. 5, pp. 66–74, Apr. 2011.
- [2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Techn. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
- [3] A. Wyner, "The wire-tap channel," *Bell Syst. Techn. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [4] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
- [5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
- [6] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.
- [7] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for secrecy in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.
- [8] N. Yang, P. L. Yeoh, M. El-kashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.
- [9] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1656–1667, Mar. 2014.
- [10] F. Rusek, D. Persson, B. K. Lau, E. G. Larsson, T. L. Marzetta, O. Edfors, and F. Tufvesson, "Scaling up MIMO: opportunities and challenges with very large arrays," *IEEE Signal Process. Mag.*, vol. 30, no. 1, pp. 40–46, Jan. 2013.
- [11] E. G. Larsson, F. Tufvesson, O. Edfors, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, Feb. 2014.
- [12] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3590–3600, Nov. 2010.
- [13] H. Yin, D. Gesbert, M. Filippou, and Y. Liu, "A coordinated approach to channel estimation in large-scale multiple antenna systems," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 2, pp. 264–273, Feb. 2013.
- [14] J. Li and A. P. Petropulu, "Ergodic secrecy rate for multiple-antenna wiretap channels with Rician fading," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 861–867, Sep. 2011.
- [15] N. S. Ferdinand, D. Benevides da Costa, and M. Latva-aho, "Physical layer security in MIMO OSTBC line-of-sight wiretap channels with arbitrary transmit/receive antenna correlation," *IEEE Wireless Comm. Lett.*, vol. 2, no. 5, pp. 467–470, Oct. 2013.
- [16] S. Yan and R. Malaney, "Line-of-sight based beamforming for security enhancements in wiretap channels," in *Proc. ICITCS2014 IEEE*, Oct. 2014, pp. 218–221.
- [17] J.-A. Tsai, R. Buehrer, and B. D. Woerner, "BER performance of a uniform circular array versus a uniform linear array in a mobile radio environment," *IEEE Trans. Wireless Commun.*, vol. 3, no. 3, pp. 695–700, May 2004.
- [18] G. Taricco and E. Riegler, "On the ergodic capacity of correlated Rician fading MIMO channels with interference," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4123–4137, Jul. 2011.
- [19] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.
- [20] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
- [21] B. Fisher and A. Kılıçman, "Some results on the Gamma function for negative integers," *Appl. Math. Inf. Sci.*, vol. 6, No. 2, pp. 173–176, May 2012.
- [22] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 7th ed., Academic, San Diego, CA, 2007.
- [23] E. Telatar, "Capacity of multi-antenna gaussian channels," *Eur. Trans. Telecommun.*, vol. 10, no. 6, pp. 585–596, Nov. 1999.
- [24] V. Annapureddy, D. Marathe, T. Ramya, and S. Bhashyam, "Outage probability of multiple-input single-output (MISO) systems with delayed feedback," *IEEE Trans. Commun.*, vol. 57, no. 2, pp. 319–326, Feb. 2009.
- [25] M. Kang, and M.-S. Alouini, "Largest eigenvalue of complex Wishart matrices and performance analysis of MIMO MRC systems," *IEEE J. Sel. Areas Commun.*, vol. 21, no. 3, pp. 418–426, Apr. 2003.
- [26] T. Taniguchi, S. Sha, Y. Karasawa, and M. Tsuruta, "Approximation of Largest Eigenvalue Distribution in Rician MIMO Channels," in *Proc. IEEE PIMRC*, Sep. 2007, pp. 1–5.
- [27] E. Biglieri, G. Caire, and G. Taricco, "Limiting performance of block-fading channels with multiple antennas," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1273–1289, May 2001.