Location-Based Beamforming for Enhancing Secrecy in Rician Wiretap Channels

Shihao Yan, *Member, IEEE,* and Robert Malaney, *Member, IEEE*

***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 any channel state information of the main channel or the eavesdropper's channel being available at the transmitter. This makes our scheme easy to deploy in a host of application settings in which the location inputs are known. Our beamforming solution assumes a multiple-antenna transmitter and a multiple-antenna eavesdropper, 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 an easy-to-evaluate expression that is valid for arbitrary real 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 physical layer security, 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, a wiretap channel model was proposed as the fundamental model for investigating such physical layer security in single-input single-output systems [2, 3]. 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 gained much interest (e.g., [4–13]). However, many of the works in MIMO wiretap channels assume the (instantaneous) channel state information (CSI) of the *main channel* (the channel between Alice and Bob) is perfectly known by Alice (e.g., [4–6]). This assumption is usually very difficult to justify in practice. Also, feeding back the CSI of the main channel from Bob to Alice costs large feedback overhead. Other assumptions adopted in the literature are that the statistical CSI of the *eavesdropper's channel* (the channel between Alice and Eve) is known to Alice (e.g., [8, 9, 14]), or even more unrealistically the full CSI of the eavesdropper's channel is known to Alice (e.g., [7]). Such assumptions are usually made simply for tractable analysis of the problem, but can rarely be justified in pragmatic systems. In this work we will not adopt such strong assumptions regarding the nature of the eavesdropper's channel.

In practice, there are many circumstances where *location information* of Bob and/or Eve could be available. For example, in cellular networks a base station can request a legitimate mobile user to feedback its location information (the mobile user can obtain its own location through GPS, for example). In comparison, estimation and feedback of the full CSI of a channel cost a relatively larger amount of system resources, and accurate estimation of the CSI may not be achieved in massive MIMO techniques due to pilot contamination issues [15–18]. Alice can potentially know Eve's location through some form of *a priori* surveillance (e.g., [19, 20]). For instance, in a military environment enemy locations can be determined via visual or electronic reconnaissance. Other circumstances in which Eve's location is known could be where Bob and Eve are normal users of the system served by Alice (but still requiring secret communications on an individual basis), with their location information being routinely broadcasted as per the requirements of a specific network protocol. Examples of such circumstances would be in IEEE 1609.2 for vehicular networks, or in some location-based social-media applications. We also note that the application scenarios of interest can be extended to circumstances where only Bob or Eve's location is available at Alice.

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 being available at Alice - 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/or Eve, we output the optimal beamformer solution and the security level (the secrecy outage

Manuscript received Jul. 5, 2015; revised Nov. 7, 2013; accepted Dec. 15, 2013. The associate editor coordinating the review of this paper and approving it for publication was Dr. C. Zhong.

S. Yan is currently with the Research School of Engineering, The Australia National University, Canberra, ACT, Australia. He was with the School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, NSW, Australia (email: shihao.yan@anu.edu.au).

R. Malaney is with the School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, NSW, Australia (email: r.malaney@unsw.edu.au).

probability) associated with this solution. These outputs are dependent on the locations of Bob and Eve through path loss (distance) and angle-of-arrival of the incoming wave front, and thus we refer to our scheme as the LBB scheme. Detailing how these outputs are determined forms the core of our work. [1]

Surprisingly, there has been little previous work in this area, with the closest works perhaps those of [21] and [22]. In [21], the ergodic secrecy rate was examined for multiple-antenna wiretap channels with Rician fading. However, in [21] it was assumed that the CSI of the main channel was perfectly known by Alice. The work of [22] analyzed the secrecy performance of orthogonal space-time block codes when the main channel is assumed to be subject to a special Rician fading (the Rician K-factor equals one), but with the eavesdropper's channel subject to pure Rayleigh fading. That is, in [22] no LOS component between Alice and Eve exists. This means Eve's location information would not be useful in the design of transmission schemes at Alice. Different from [22] we consider the scenario where the main channel and the eavesdropper's channel are subject to general Rician fading (the Rician K-factors of the two channels can be arbitrary real values). In many circumstances the secrecy outage probability for a Rician-fading eavesdropper's channel is higher than the outage probability for a Rayleigh-fading eavesdropper's channel (i.e. Eve prefers that a LOS component exists between her and Alice). We note that in such circumstances it is more probable that the eavesdropper's channel is subject to Rician fading (since Eve would try to select a location that ensures a LOS component between her and Alice). We also note that the Rician-fading channel with small values of the Rician K-factor can be utilized to approximate a Rayleigh-fading channel. Therefore, our system model is more general than that considered in [22].

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 an easy-to-evaluate expression, which is valid for arbitrary real 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 VI 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.

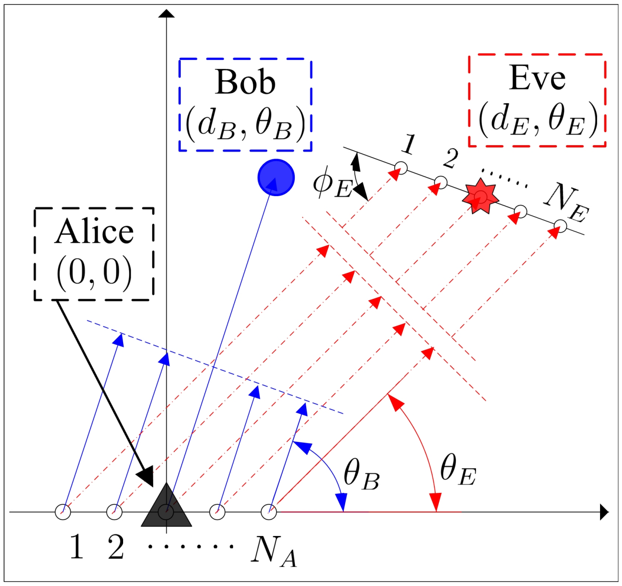

Fig. 1. Illustration of the Rician wiretap channel of interest with a multiple-antenna Alice, a single-antenna Bob, and a multiple-antenna Eve.

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 [19]. Here, we expand on that simple scenario by considering more generic and realistic Rician fading channels. We note that the Rician fading channel model is more general than the widely used Rayleigh fading channel model, i.e., the Rayleigh fading channel is a special case of the Rician fading channel with a zero Rician K-factor. We 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. In this work, we consider not only the single-antenna Bob scenario but also the multiple-antenna Bob scenario. A single-antenna Bob has been widely adopted in previous investigations of physical layer security (e.g., [21, 23, 24]), since in some scenarios a low-complexity receiver structure is more relevant (e.g., low-cost sensor devices). A multiple-antenna Bob requires additional hardware and more sophisticated signal processing techniques. 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. As we will

[1] Although 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.

[2] We 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.

show later, our analysis provided in this work is also valid for other antenna arrays beyond ULAs at Eve.

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 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. We note that the assumptions that Eve knows the CSI of channel between her and Alice, and the beamformer adopted by Alice, are widely adopted in the literature on physical layer security (e.g., [4, 7, 9]). This is due to the fact that we normally investigate security issues from a conservative point of view, and this assumption captures the worst-case scenario. Note also, that under the conservative worst-case scenario, Eve knows everything that is known by Alice. As such, we will also assume Eve can determine the optimal beamformer.

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

$$\mathbf{h} = \sqrt{\frac{K_B}{1+K_B}}\mathbf{h}_o + \sqrt{\frac{1}{1+K_B}}\mathbf{h}_r, \tag{1}$$

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 [25]

$$\mathbf{h}_o = \left[1, \cdots, \exp(j(N_A - 1)\tau_A \cos\theta_B)\right], \tag{2}$$

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

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

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 variance. Although $\mathbf{G}_o$ is a rank-1 matrix, we highlight that $\mathbf{G}$ is not rank-1 since $\mathbf{G}_r$ is full-rank. Given the locations of Alice and Eve, $\mathbf{G}_o$ can be written as [26]

$$\mathbf{G}_o = \mathbf{r}_o^T \mathbf{g}_o \tag{4}$$

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

$$\mathbf{r}_o = \left[1, \cdots, \exp(-j(N_E - 1)\tau_E \cos\phi_E)\right], \tag{5}$$

$$\mathbf{g}_o = \left[1, \cdots, \exp(j(N_A - 1)\tau_A \cos\theta_E)\right]. \tag{6}$$

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

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

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 exponent[4] 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 Alice[5]), 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

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

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

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

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

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

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

[3] We note that using Bob's location saves feedback overhead relative to using 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.

[4] The path loss exponent η_B is dependent on the Rician K-factor K_B. For example, $\eta_B \to 2$ as $K_B \to \infty$. 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.

[5] It 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 $|\mathbf{hb}|$. As per (1), we have

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

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 $|\mathbf{hb}|$ follows a Rician distribution. We next determine the parameters of this Rician distribution. Following (11), we have

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

and

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

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 $\sqrt{\gamma_B} = \sqrt{\overline{\gamma}_B}|\mathbf{hb}|$ follows a Rician distribution with $\widetilde{K}_B$ and $\widetilde{\overline{\gamma}}_B$ as the Rician K-factor and total power, respectively, where $\widetilde{K}_B$ and $\widetilde{\overline{\gamma}}_B$ are given by

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

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

The pdf of a Rician random variable 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 [27]

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

where $\widetilde{m}_B$ is the Nakagami fading parameter given by $\widetilde{m}_B = (\widetilde{K}_B+1)^2/(2\widetilde{K}_B+1)$ and $\Gamma(\mu) = \int_0^\infty e^{-t}t^{\mu-1}dt$, $\mathrm{Re}(\mu) > 0$, is the Gamma function. As we have numerically verified, the approximation accuracy of (16) is very high, and this accuracy increases as K_B increases.

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

$$\gamma_E = \sum_{i=1}^{N_E}\gamma_{E,i}, \tag{17}$$

where $\gamma_{E,i} = \overline{\gamma}_E|\mathbf{g}_i\mathbf{b}|^2$, $\mathbf{g}_i$ 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

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

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 ($i = 1, 2, \ldots, N_E$), we have

$$|\epsilon_i\mathbf{g}_o\mathbf{b}| = |\mathbf{g}_o\mathbf{b}|. \tag{19}$$

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

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

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

$$\widetilde{\overline{\gamma}}_E \triangleq \mathbb{E}[\gamma_E] = \frac{\left(K_E|\mathbf{g}_o\mathbf{b}|^2+1\right)\overline{\gamma}_E}{1+K_E}. \tag{21}$$

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

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

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 the received signals. As such, 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 at Eve 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

$$C_s = \begin{cases} C_B - C_E \ , & \gamma_B > \gamma_E \\ 0 \ , & \gamma_B \le \gamma_E, \end{cases} \tag{23}$$

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_E is 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]

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

We now derive the secrecy outage probability for the LBB scheme in the following theorem.

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

$$\mathcal{O}(R_s) =$$

$$\frac{\widetilde{m}_B^{\widetilde{m}_B}\widetilde{m}_E^{N_E\widetilde{m}_E}2^{\widetilde{m}_B R_s}}{\Gamma(N_E\widetilde{m}_E)\widetilde{\widetilde{\gamma}}_B^{-N_E\widetilde{m}_E}\widetilde{\widetilde{\gamma}}_E^{-\widetilde{m}_B}}\sum_{n=0}^{+\infty}\frac{2^{nR_s}\exp\left(-\frac{\widetilde{m}_B\left(2^{R_s}-1\right)}{\widetilde{\widetilde{\gamma}}_B}\right)}{\widetilde{m}_B^{-n}\widetilde{\widetilde{\gamma}}_B^{n}\Gamma(\widetilde{m}_B+n+1)}\times$$
$$\sum_{l=0}^{+\infty}\frac{\binom{\widetilde{m}_B+n}{l}\left(2^{R_s}-1\right)^l\left(\widetilde{\widetilde{\gamma}}_B\widetilde{\widetilde{\gamma}}_E\right)^{n-l}\Gamma_G(\widetilde{m}_B+N_E\widetilde{m}_E+n-l)}{2^{lR_s}\left(2^{R_s}\widetilde{m}_B\widetilde{\widetilde{\gamma}}_E+\widetilde{m}_E\widetilde{\widetilde{\gamma}}_B\right)^{\widetilde{m}_B+N_E\widetilde{m}_E+n-l}}, \quad (25)$$

where $\Gamma_G(\cdot)$ is the generalized gamma function (also valid for negative integers), which is given by [29]

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

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

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

where $\gamma\left(\alpha,\mu\right) = \int_0^{\mu}e^{-t}t^{\alpha-1}dt$, $\mathrm{Re}\{\alpha\} > 0$, is the lower incomplete gamma function. In order to obtain the result in (27), we have utilized the following identity [30, Eq. (3.381.1)]

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

We note that our pdfs of γ_B and γ_E given by (16) and (22), respectively, are valid for arbitrary real values of K_B and K_E. In terms of theoretical analysis, this means the power/exponent parameters (e.g., $\widetilde{m}_B - 1$, $N_E\widetilde{m}_E - 1$) in these pdfs are arbitrary real values. The presence of such real numbers results in considerable challenges in solving the integral given in (27). This is due to the fact that (27) now involves several types of functions (e.g., Gamma functions, lower incomplete gamma functions, and exponential functions). All these issues will lead to complications in the following derivations.

To make progress, we adopt the following identity to expand $\gamma\left(\alpha,\mu\right)$ [30, Eq. (8.354.1)]

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

As per (29), we have

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

in which the identity [30, 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

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

We then obtain the desirable result in (25) by solving the integral in (32) as per the following identity [30, 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 $\widetilde{m}_B$, $\widetilde{m}_E$, $\widetilde{\widetilde{\gamma}}_B$, and $\widetilde{\widetilde{\gamma}}_E$. We also note that (25) is valid for arbitrary real $\widetilde{m}_B$ and $\widetilde{m}_E$ ($\widetilde{m}_B$ and $\widetilde{m}_E$ can be equal), and thus (25) is valid for arbitrary real K_B and K_E. Although (25) is by construction bounded by 1, it does involve two infinite series. However, these two series can both be approximated by finite series accurately. This is due to the fact that (25) is convergent, as

[6] The secrecy outage probability is the most common metric used in physical layer security when CSI of the wiretap channel is unavailable at Alice. However, it is important to note this metric does not distinguish between reliability and security [28].

we now discuss. The two infinite series, $\sum_{n=0}^{+\infty}$ and $\sum_{l=0}^{+\infty}$, involved in (25) arise from (29) and (31), respectively. But, we note that (31) is utilized only to expand individual terms (i.e., within each n-th summation term) within (29). Therefore, as long as (29) is convergent we can conclude (25) is convergent. As proven elsewhere, (29) is indeed convergent [31]. As such, we can conclude that (25) is convergent (we have also numerically confirmed this).

In order to calculate $\mathcal{O}(R_s)$ efficiently, we adopt $\widetilde{\mathcal{O}}(R_s, N, L)$ as an approximation. This closed-form approximation to $\mathcal{O}(R_s)$ is obtained by truncating its $\sum_{n=0}^{+\infty}$ and $\sum_{l=0}^{+\infty}$ series at the N-th and L-th terms, respectively. We have numerically confirmed $\widetilde{\mathcal{O}}(R_s, N, L)$ offers accurate approximation even with small values of N and L. Defining $\epsilon = |\widetilde{\mathcal{O}}(R_s, N, L) - \overline{\mathcal{O}}(R_s)|/\overline{\mathcal{O}}(R_s)$ as the relative approximation error (where $\overline{\mathcal{O}}(R_s)$ is the numerically evaluated result of (27) and the evaluation error of (27) is less than 10^{-12}), our numerical verifications indicate that ϵ is less than 10% even when $N = L = 5$. Furthermore, ϵ decreases significantly as N increases. For example, ϵ is around 10^{-3} for $N = 10$ and $L = 5$; and ϵ is around 10^{-6} for $N = 20$ and $L = 5$. In addition to the computational advantages offered by a truncated approximation to (25), we also note that this approximation represents a lower bound to the secrecy outage probability.

Moreover, we note that we can draw many useful insights from the derivation of (25), which cannot be obtained by numerically evaluating (27). For example, following a similar procedure to derive (25) we can determine the secrecy diversity order and secrecy coding gain of our LBB scheme. The secrecy diversity order is an important performance parameter associated with the secrecy outage probability, which determines the slope of the curve for the secrecy outage probability (in dB) versus $\overline{\gamma}_B$ (in dB) as $\overline{\gamma}_B \to \infty$ for finite $\overline{\gamma}_E$. Mathematically, the secrecy diversity order for finite $\overline{\gamma}_E$ is defined as

$$\beta = \lim_{\overline{\gamma}_B \to \infty} \frac{\log_{10} \mathcal{O}\left(R_s\right)}{\log_{10}(1/\overline{\gamma}_B)}. \tag{34}$$

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

***Corollary** 1:* The secrecy diversity order of the LBB scheme at fixed $\overline{\gamma}_E$ is $\widetilde{m}_b$, i.e. $\beta = \widetilde{m}_b$.

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 $\widetilde{m}_B$. As such, we omit the proof of the above corollary here. We note that maximum value of $\widetilde{m}_B$ is $(N_A K_B + 1)^2/(2N_A K_B + 1)$ due to $|\mathbf{h}_o \mathbf{b}|^2 \leq \|\mathbf{h}_o\|^2 \|\mathbf{b}\|^2 = N_A$. The secrecy diversity order given in (34) is widely utilized in the literature (e.g., [32, 33]), and to be consistent with other works we will adopt this definition as well. However, we do note it is only formally defined for $\overline{\gamma}_B \to \infty$ at fixed $\overline{\gamma}_E$. It is therefore most useful in special cases, such as when Bob approaches very close to Alice whilst Eve remains at a fixed distance further from Alice. Note also, the secrecy diversity order will be zero if $\overline{\gamma}_E \to \infty$, since the secrecy outage probability will be zero for $\overline{\gamma}_E \to \infty$ [32]. Following Corollary 1 and the definition of $\widetilde{m}_B$, we know that the secrecy diversity order of the LBB scheme is related to the Rician K-factor of the main channel (i.e., the secrecy diversity order increases as K_B increases). Intuitively, this is due to the fact that the channel quality increases as K_B increases. Theoretically, this is due to the fact that the pdf of γ_B given in (16) involves the term $\gamma^{\widetilde{m}_B - 1}$. In order to derive the secrecy diversity order, we have to obtain the asymptotic pdf of γ_B based on the Taylor series expansion, in which $\gamma^{\widetilde{m}_B - 1}$ remains in the non-zero term. We note that a similar conclusion was drawn for Nakagami fading channels in [8], which states that the secrecy diversity order increases as the Nakagami fading parameter of the main channel increases.

Then, the probability of non-zero secrecy capacity of the LBB scheme is presented in the following corollary, which is defined as the probability that a positive secrecy capacity is achieved.

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

$$P_{non} = 1 - \frac{\widetilde{m}_B^{\widetilde{m}_B} \widetilde{m}_E^{N_E \widetilde{m}_E}}{\Gamma(N_E \widetilde{m}_E) \widetilde{\overline{\gamma}}_E^{-\widetilde{m}_B} \widetilde{\overline{\gamma}}_B^{-N_E \widetilde{m}_E}} \sum_{n=0}^{+\infty} \frac{\widetilde{m}_B^n \widetilde{\overline{\gamma}}_E^n}{\Gamma(\widetilde{m}_B + n + 1)} \times \frac{\Gamma\left(\widetilde{m}_B + N_E \widetilde{m}_E + n\right)}{\left(\widetilde{m}_B \widetilde{\overline{\gamma}}_E + \widetilde{m}_E \widetilde{\overline{\gamma}}_B\right)^{\widetilde{m}_B + N_E \widetilde{m}_E + n}}. \tag{35}$$

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

$$P_{non} = 1 - \mathcal{O}(R_s = 0). \tag{36}$$

Substituting $R_s = 0$ into (25), we obtain the desirable result in (35). ■

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). We now extend our analysis by considering multiple antennas at Bob. Various combining techniques can be applied at a multiple-antenna Bob. Here, we restrict ourselves to the MRC technique and derive an easy-to-evaluate expression for the secrecy outage probability. We note that MRC requires the CSI of the main channel being available at Bob. We also note that in our following analysis we assume Alice still transmits a single data stream to Bob.

Following a similar procedure to derive (22), the pdf of the SNR at Bob, who is equipped with multiple antennas and applies MRC to combine the received signals, can be approximated by

$$f_{\gamma_B}^{N_B}(\gamma) = \left(\frac{\widetilde{m}_B}{\widetilde{\overline{\gamma}}_B}\right)^{N_B \widetilde{m}_B} \frac{\gamma^{N_B \widetilde{m}_B - 1}}{\Gamma(N_B \widetilde{m}_B)} \exp\left(\frac{-\widetilde{m}_B \gamma}{\widetilde{\overline{\gamma}}_B}\right), \tag{37}$$

where N_B denotes the number of antennas at Bob. Then, following a similar procedure as given in the proof of Theorem 1 we derive the secrecy outage probability for the multiple-antenna Bob to be

$$\mathcal{O}^{N_B}(R_s) = \frac{\widetilde{m}_B^{\widetilde{m}_B}\widetilde{m}_E^{N_E\widetilde{m}_E}2^{N_B\widetilde{m}_B R_s}}{\Gamma(N_E\widetilde{m}_E)\widetilde{\overline{\gamma}}_B^{-N_E\widetilde{m}_E}\widetilde{\overline{\gamma}}_E^{-N_B\widetilde{m}_B}}\times \sum_{n=0}^{+\infty}\frac{2^{nR_s}\exp\left(-\frac{\widetilde{m}_B\left(2^{R_s}-1\right)}{\widetilde{\overline{\gamma}}_B}\right)}{\widetilde{m}_B^{-n}\widetilde{\overline{\gamma}}_B^{n}\Gamma(N_B\widetilde{m}_B+n+1)}\times \sum_{l=0}^{+\infty}\frac{\binom{N_B\widetilde{m}_B+n}{l}\left(2^{R_s}-1\right)^l\Gamma_G(N_B\widetilde{m}_B+N_E\widetilde{m}_E+n-l)}{2^{lR_s}\left(\widetilde{\overline{\gamma}}_B\widetilde{\overline{\gamma}}_E\right)^{n-l}\left(2^{R_s}\widetilde{m}_B\widetilde{\overline{\gamma}}_E+\widetilde{m}_E\widetilde{\overline{\gamma}}_B\right)^{N_B\widetilde{m}_B+N_E\widetilde{m}_E+n-l}}. \tag{38}$$

We note that the expression present in (38) provides a lower bound for the secrecy outage probability if some other combining technique other than MRC is utilized at Bob. This is due to the fact that MRC maximizes the SNR at Bob relative to other combining techniques. Comparing (37) with (16) we can see that the N_B antennas at Bob increase both $\widetilde{m}_B$ and $\widetilde{\overline{\gamma}}_B$ by a factor of N_B. Therefore, multiple antennas result in the secrecy outage probability given in (38) being lower than that given in (25). The values of $\widetilde{m}_B$ and $\widetilde{\overline{\gamma}}_B$ impact the optimal location-based beamformer. As such, the optimal location-based beamformer for a single-antenna Bob is different from that for a multiple-antenna Bob.

C. Optimal Location-based Beamformer

A location-based beamformer can be written as

$$\mathbf{b} = \frac{1}{\sqrt{N_A}}\left[1,\cdots,\exp(-j(N_A-1)\tau_A\cos\psi)\right]^T, \tag{39}$$

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

$$\psi^* = \underset{0\leq\psi\leq\pi}{\operatorname{argmin}}\,\mathcal{O}(R_s), \tag{40}$$

and setting $\psi = \psi^*$ in (39) completely determine 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 (40) is a one-dimensional optimization problem, which can be solved through Algorithm 1 given below.

Algorithm 1 Grid Search Algorithm to determine ψ^*

```
1: Uniformly sample $\psi_i$ over $[0,\pi]$ for $I$ times, i.e., $\psi_i = \frac{(i-1)\pi}{I-1}$, $i = 1, 2, \ldots, I$.
2: Calculate $\mathcal{O}(R_s)$ for each $\psi_i$ by utilizing (25), and denote the value of $\mathcal{O}(R_s)$ for $\psi_i$ as $\mathcal{O}_i(R_s)$.
3: Find the minimum value among all $\mathcal{O}(R_s)$, denoted as $\mathcal{O}^*(R_s)$.
4: Determine the value $\psi_i$ that achieves $\mathcal{O}^*(R_s)$, which is denoted as $\psi^*$.
5: Set $\psi = \psi^*$ in (39) to obtain the optimal beamformer $\mathbf{b}^*$.
```

We note ψ^* obtained through Algorithm 1 approaches the true optimal value of ψ as N, L, and I increase. Using Algorithm 1 we find a solution is obtained well below 1 second on an average processor for $N = 50$, $L = 50$, and $I = 1000$. For all intents and purposes this solution is optimal. We would like to highlight that ψ^* can be analytically determined in some special cases as detailed in the following corollary.

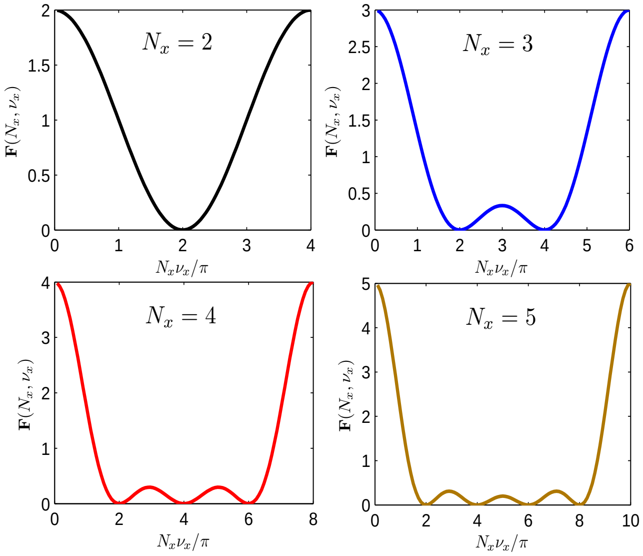

Fig. 2. $\mathbf{F}(N_x,\nu_x)$ versus $N_x\nu_x/\pi$ for different values of N_x.

Corollary 3: For $K_E > 0$, the (multiple) solution to (40) is $\psi^* = \arccos\left(\cos\theta_E + \frac{2n_A\pi}{N_A\tau_A}\right)$, $n_A = 1,\ldots,N_A-1$, in the following cases: (i) when $\overline{\gamma}_E \to \infty$ for finite $\overline{\gamma}_B$, (ii) when $K_B = 0$, or (iii) when θ_B is unavailable at Alice.

Proof: For all the cases in the corollary, γ_B is of little impact on the secrecy outage probability or it is out of control of $\mathbf{b}$. As such, $\mathbf{b}$ is to minimize γ_E for these cases. To this end, ψ^* is to minimize $|\mathbf{g}_o\mathbf{b}|^2$ due to the expression of γ_E given in (17). Denoting $\nu_E = \tau_A(\cos\theta_E - \cos\psi)$, as per (6) and (39), for $\nu_E \neq 0$ we have

$$\begin{aligned}\mathbf{g}_o\mathbf{b} &= \frac{1}{\sqrt{N_A}}\frac{\exp\left(jN_t\nu_E\right)-1}{\exp\left(j\nu_E\right)-1}\\ &= \frac{1}{\sqrt{N_A}}\frac{-e^{jN_A\nu_E/2}\left(-e^{-jN_A\nu_E/2}-e^{jN_A\nu_E/2}\right)}{-e^{j\nu_E/2}\left(-e^{-j\nu_E/2}-e^{j\nu_E/2}\right)}\\ &= \frac{1}{\sqrt{N_A}}\frac{\sin\left(\frac{1}{2}N_A\nu_E\right)}{\sin\left(\frac{1}{2}\nu_E\right)}e^{j\nu_E(N_A-1)/2}.\end{aligned} \tag{41}$$

For $\nu_E = 0$, we have $\mathbf{g}_o\mathbf{b} = \sqrt{N_A}$. Then, following (41) we have

$$|\mathbf{g}_o\mathbf{b}|^2 = \mathbf{F}(N_A,\nu_E), \tag{42}$$

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

$$\mathbf{F}(N_x,\nu_x) = \begin{cases} N_x, & \nu_x = 0,\\ \frac{1}{N_x}\left(\frac{\sin\left(\frac{1}{2}N_x\nu_x\right)}{\sin\left(\frac{1}{2}\nu_x\right)}\right)^2, & 0 \leq \nu_x < 2\pi.\end{cases} \tag{43}$$

It can be proved that the minimum value of $\mathbf{F}(N_x,\nu_x)$ is achieved when $\nu_x = 2n_x\pi$ for $n_x = 1,\ldots,N_x-1$, which is also confirmed by Fig. 2. As such, $|\mathbf{g}_o\mathbf{b}|^2$ is minimized

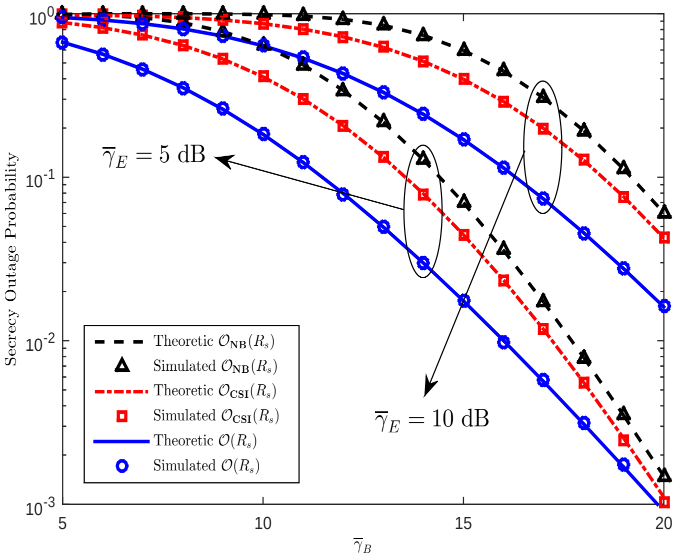

Fig. 3. Secrecy outage probabilities under Nakagami channels versus different values of $\overline{\gamma}_B$, where $m_B = 1.35, m_E = 1.33, \overline{\lambda}_0 = 0.85, N_A = 3, N_E = 2$, and $R_s = 1$.

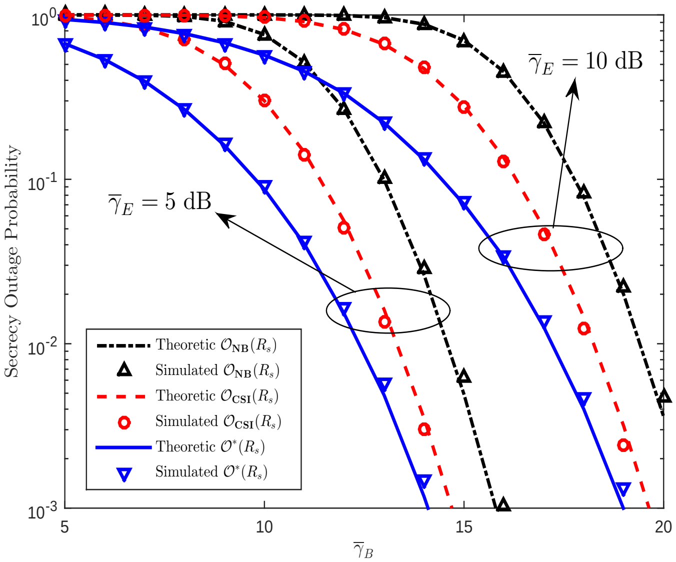

Fig. 4. Secrecy outage probabilities under Rician channels versus different values of $\overline{\gamma}_B$, where $N_A = 3, N_E = 2, K_B = 10$ dB, $K_E = 5$ dB, $\theta_B = \pi/3, \theta_E = \pi/4$, and $R_s = 1$.

when $\nu_E = 2n_A\pi$ for $n_A = 1, \ldots, N_A - 1$, and thus we obtain Corollary 3. ■

Intuitively, the solution to (40) is $\psi^* = \theta_B$ for $K_B > 0$ in the following cases: (i) when $\overline{\gamma}_B \to \infty$ for finite $\overline{\gamma}_E$, (ii) when $K_E = 0$, or (iii) when θ_E is unavailable at Alice. This is due to the fact that the best Alice can do is to enhance the main channel quality when γ_E of little impact on the secrecy outage probability or out of control of $\mathbf{b}$. 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 $\widetilde{K}_B = N_A K_B$ and $\widetilde{\overline{\gamma}}_B = (N_A K_B + 1)\overline{\gamma}_B/(1 + K_B)$.

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, $\overline{\gamma}_B$, and $\overline{\gamma}_E$) on the LBB scheme. To better illustrate the gains obtained by our LBB scheme, we will also present simulations of the secrecy performances of the NB (non-beamforming) scheme and the full-CSI scheme. The NB scheme represents the case when an isotropic beamforming pattern is produced by Alice (see Appendix A for an analytical analysis of this scheme). The full-CSI scheme represents the case when the maximum ratio transmission based on the CSI of the main channel is adopted by Alice (see Appendix B for an analytical analysis of this scheme). To conduct simulations, we deploy Bob and Eve at specific locations and then map such locations into $\overline{\gamma}_B$ and $\overline{\gamma}_E$, 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 $\overline{\gamma}_B$ and $\overline{\gamma}_E$ 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. We also note that only the following Fig. 3 (in which we pick an arbitrary beamformer $\mathbf{b}$) is generated under Nakagami fading channels. This is done simply to verify our theoretical analysis provided in Theorem 1. As such, Fig. 3 will not be used to draw any insights on the performance of different schemes. All other figures are generated under Rician fading channels.

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 $\widetilde{m}_B = 2m_B$, $\widetilde{m}_E = m_E$, $\widetilde{\overline{\gamma}}_B = 3\overline{\gamma}_B$, and $\widetilde{\overline{\gamma}}_E = \overline{\gamma}_E$, where $m_B = (K_B + 1)^2/(2K_B + 1)$ and $m_E = (K_E + 1)^2/(2K_E + 1)$. The theoretic secrecy outage probability of the LBB scheme, $\mathcal{O}(R_s)$, the secrecy outage probability of the NB scheme, denoted as $\mathcal{O}_{\mathbf{NB}}(R_s)$, and the secrecy outage probability of the full-CSI scheme, denoted as $\mathcal{O}_{\mathbf{CSI}}(R_s)$, are obtained through (25), (49), (50), respectively, where relevant infinite series are truncated approximately at 30. In this figure, we observe that the theoretic $\mathcal{O}(R_s)$, $\mathcal{O}_{\mathbf{NB}}(R_s)$, and $\mathcal{O}_{\mathbf{CSI}}(R_s)$ precisely match the simulated $\mathcal{O}(R_s)$, $\mathcal{O}_{\mathbf{NB}}(R_s)$, and $\mathcal{O}_{\mathbf{CSI}}(R_s)$, 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 plot the secrecy outage probabilities of the LBB, NB, and full-CSI schemes, for specific Rician fading channels. Note, in the full-CSI scheme Eve's location is unknown to Alice. In this figure, we observe that the simulated minimum secrecy outage probability of the LBB scheme, $\mathcal{O}^*(R_s)$, the secrecy outage probability of the NB scheme, $\mathcal{O}_{\mathbf{NB}}(R_s)$, and the secrecy outage probability of the full-CSI scheme, $\mathcal{O}_{\mathbf{CSI}}(R_s)$, match well the theoretic $\mathcal{O}^*(R_s)$, $\mathcal{O}_{\mathbf{NB}}(R_s)$, and $\mathcal{O}_{\mathbf{CSI}}(R_s)$, respectively, thus confirming the validity of our channel approximation. We note that we have set θ_E 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 $\mathcal{O}_{\mathbf{NB}}(R_s)$ can even be larger when θ_E is not so close to θ_B. We also observe that $\mathcal{O}^*(R_s)$ is

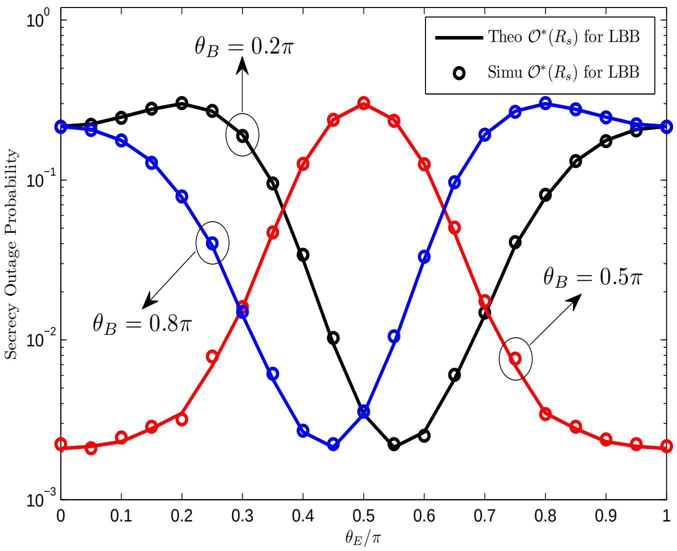

Fig. 5. Minimum secrecy outage probability of the LBB scheme versus different values of θ_E, where $N_A = 2, N_E = 2, K_B = 10$ dB, $K_E = 10$ dB, $\overline{\gamma}_B = 10$ dB, $\overline{\gamma}_E = 10$ dB, and $R_s = 1$.

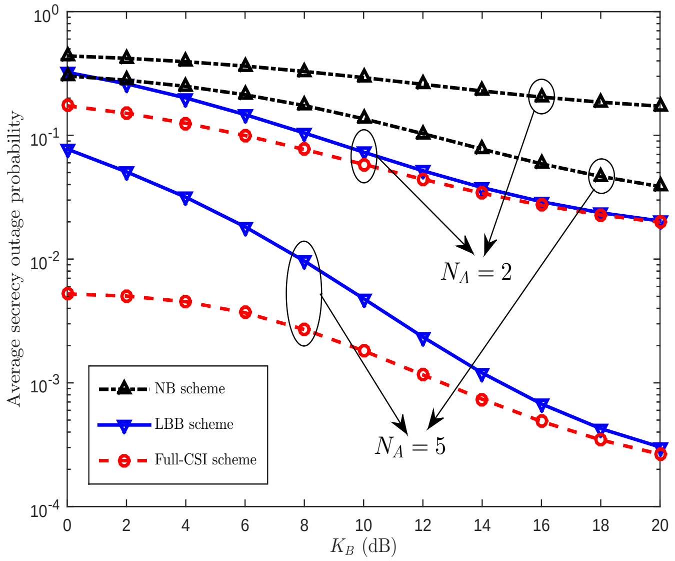

Fig. 6. Average secrecy outage probabilities without Eve's location versus different values of K_B, where $N_E = 3, K_E = 5$ dB, $\overline{\gamma}_B = 10$ dB, $\overline{\gamma}_E = 1$ dB$\theta_B = \pi/3$, and $R_s = 1$.

lower than $\mathcal{O}_{\mathbf{CSI}}(R_s)$, which indicates that the LBB scheme outperforms the full-CSI scheme. This is related to the fact that Alice knows Eve's location in the LBB scheme only (i.e., Alice does not know Eve's location in the NB and full-CSI scheme). However, we highlight that this comparison result is only valid for these specific system settings. Perhaps a more fairer comparison between the LBB and full-CSI schemes is provided in Fig. 6, where we adopt a modified LBB scheme, referred to as LBB$_u$, in which Eve's location is unknown to Alice.

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$_u$ scheme relative to the NB and full-CSI schemes. Here, we assume a uniform distribution of θ_E, i.e. $\theta_E \sim \mathcal{U}[0, 2\pi]$, and we then average the secrecy outage probability for all θ_E to obtain the average secrecy outage probability for each scheme. As expected, we observe that the average secrecy outage probability of the LBB$_u$ scheme is lower than that of the NB scheme, and higher than that of the full-CSI scheme. In addition, we observe that the performance gap between the LBB$_u$ scheme and the NB scheme increases as K_B increases, and the performance gap between the LBB$_u$ scheme and the full-CSI scheme decreases as K_B increases. These two observations can be explained by the fact that Bob's location provides more information on the main channel as K_B increases (e.g., as $K_B \to \infty$, knowing Bob's location is equivalent to knowing the CSI of the main channel). Based on these observations, we can conclude that the LBB$_u$ scheme is preferable when the Rician K-factor is large.

We note that the performance gain of the full-CSI scheme relative to the LBB$_u$ scheme is achieved at the cost of high implementation complexities. In comparison, the LBB$_u$ scheme only requires Bob's location. Taking the feedback overhead as an example, the full-CSI scheme requires N_A complex numbers to be fed back, while feeding back Bob's location only requires two real numbers. As we can see from Fig. 6, the performance gap between the LBB$_u$ scheme and the full-CSI scheme increases as N_A increases. This demonstrates the tradeoff between the system performance and the system complexity.

V. Discussions

It is worth mentioning how relaxation of some assumptions we have made impacts our results. 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.

We have assumed that Alice, Bob, and Eve are static. However, we note that our proposed LBB scheme can be deployed in mobile environments. Our analysis holds in such environments as long as Bob and Eve are exposed to a reasonable sample of the possible channel realizations. This requires the coherence time of the channel to be much shorter than the timescale associated with the receiver mobility. This timescale is set by the spatial distance over which the channel changes significantly divided by the relative velocity of the transceivers. This requirement is met for most application scenarios of wireless communications [34, 35].

We note that in this work we focus on a 3-node scenario, which serves as the basis of a networking scenario. For example, in the networking scenario Alice can serve several Bob's by utilizing time division multiple access (TDMA) techniques (e.g., Alice serves one Bob at each time slot), and thus the networking scenario can be treated as a 3-node scenario for each time slot. We would also like to highlight that we consider multiple antennas at Eve while assuming that Eve applies MRC to combine the received signals at different antennas. This latter consideration basically captures a practical networking scenario with multiple cooperating single-antenna eavesdroppers. A more detailed exploration of the many-node networking scenario beyond TDMA schemes could be considered in future works.

Although the adopted Rician fading channel model is more general than the Rayleigh fading channel model, in practice real wireless channels may be more complex again than Rician fading channels. For example, a wireless channel may consist of multiple deterministic components and scattered components. As long as these deterministic components are known, we can incorporate them into $\mathbf{h}_o$ and $\mathbf{G}_o$ in (1) and (3), respectively. Based on our analysis presented in Section III-A, we know that the pdfs of γ_B and γ_E derived in (16) and (22), respectively, are still valid when we replace the LOS component with multiple known deterministic components in the channel model. This is due to the fact that this replacement only changes the values of the effective Rician K-factor and average SNR (e.g., $\widetilde{K}_B$, $\widetilde{\overline{\gamma}}_B$). As such, our derived secrecy outage probability of the LBB scheme given in (25) is still valid for such a replacement.

VI. 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 being available at Alice. We derived the secrecy outage probability of the LBB scheme in an easy-to-evaluate expression valid for arbitrary real 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
Secrecy 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 $P\mathbf{I}_{N_A}/N_A$) [36, 37]. Then, the SNR at Bob is given by [36, 37]

$$\gamma_B^{\mathbf{NB}} = \frac{\overline{\gamma}_B ||\mathbf{h}||^2}{N_A}. \tag{44}$$

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

$$f_{\gamma_B^{\mathbf{NB}}}(\gamma) = \frac{m_B^{N_A m_B} \gamma^{N_A m_B - 1} e^{-\frac{N_A m_B \gamma}{\overline{\gamma}_B}}}{\Gamma(N_A m_B)(\overline{\gamma}_B/N_A)^{N_A m_B}}. \tag{45}$$

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

$$\gamma_E^{\mathbf{NB}} = \frac{\overline{\gamma}_E ||\mathbf{s}_0^\dagger \mathbf{G}||^2}{N_A} = \frac{\overline{\gamma}_E \lambda_0^2}{N_A}, \tag{46}$$

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 [38]. 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 [39]. As such, the pdf of $\gamma_E^{\mathbf{NB}}$ can be approximated by

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

where $\overline{\lambda}_0$ is the mean of the per-branch largest eigenvalue (i.e., $\overline{\lambda}_0 = \mathbb{E}[\lambda_0]/N_A N_E$). The value of $\overline{\lambda}_0$ can be approximated by [39]

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

We note that we have $\overline{\lambda}_0 = 1$ for arbitrary real 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

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

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 $\overline{\gamma}_B$ and $\overline{\gamma}_E$, which are dependent on d_B and d_E, respectively.

Appendix B
Secrecy Performance of the Full-CSI Scheme

In the full-CSI scheme Alice knows the CSI of the main channel, but does not know the CSI or location of Eve. Then, Alice adopts $\mathbf{h}^{\dagger}/\|\mathbf{h}\|$ as the beamformer $\mathbf{b}$ to maximize the SNR of the main channel [37, 40] in order to minimize the secrecy outage probability.

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

$$\begin{aligned}\mathcal{O}_{\mathbf{CSI}}(R_s) &= \int_0^{\infty} f_{\gamma_E^{\mathbf{CSI}}}(\gamma_E)\left[\int_0^{2^{R_s}(1+\gamma_E)-1} f_{\gamma_B^{\mathbf{CSI}}}(\gamma_B)d\gamma_B\right]d\gamma_E \\ &= \frac{m_B^{N_A m_B}\ddot{m}_E^{N_E\ddot{m}_E}2^{N_A m_B R_s}}{\Gamma(N_E\ddot{m}_E)\overline{\gamma}_B^{-N_E\ddot{m}_E}\ddot{\overline{\gamma}}_E^{-N_A m_B}}\times \\ &\sum_{n=0}^{+\infty}\frac{2^{nR_s}\exp\left(-\frac{m_B\left(2^{R_s}-1\right)}{\overline{\gamma}_B}\right)}{m_B^{-n}\ddot{\overline{\gamma}}_E^{-n}\Gamma(N_A m_B+n+1)}\times \\ &\sum_{l=0}^{+\infty}\frac{\binom{N_A m_B+n}{l}\left(2^{R_s}-1\right)^l\Gamma_G(N_A m_B+N_E\ddot{m}_E+n-l)}{\left(\overline{\gamma}_B\ddot{\overline{\gamma}}_E\right)^l 2^{lR_s}\left(2^{R_s}m_B\ddot{\overline{\gamma}}_E+\ddot{m}_E\overline{\gamma}_B\right)^{N_A m_B+N_E\ddot{m}_E+n-l}},\end{aligned} \tag{50}$$

where $\ddot{m}_E = (\ddot{K}_E+1)^2/(2\ddot{K}_E+1)$,

$$\ddot{K}_E = \frac{K_B K_E|\mathbf{g}_o\mathbf{h}_o^{\dagger}|^2}{N_A(K_B+K_E+1)}, \tag{51}$$

and

$$\ddot{\overline{\gamma}}_E = \frac{K_B K_E|\mathbf{g}_o\mathbf{h}_o^{\dagger}|^2+N_A(K_B+K_E+1)}{\overline{\gamma}_E^{-1}N_A(K_B+1)(K_E+1)}. \tag{52}$$

Acknowledgments

This work was funded by Australian Research Council Grants DP120102607 and DP150103905. We thank the Editor and the anonymous referees for their valuable comments.

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. Elkashlan, 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] C. Zhang, H. Gao, T. lv, Y. Lu, and X. Su, "Beamforming to secure two-way relay networks with physical layer network coding," in *Proc. IEEE GlobeCOM*, Dec. 2014, pp. 1734–1739.

[11] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Selec. Areas Commun.*, vol. 33, no. 6, pp. 1154–1170, Jun. 2015.

[12] J. Zhou, R. Cao, H. Gao, C. Zhang, and T. Lv, "Secure beamforming and artificial noise design in interference networks with imperfect ECSI", in *Proc. IEEE ICCW on Physical Layer Security*, Jun. 2015, pp. 423–428.

[13] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," *IEEE Trans. Commun.*, vol. 63, no. 8, pp. 2959–2971, Aug. 2015.

[14] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.

[15] 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 Proces. Mag.*, vol. 30, no. 1, pp. 40–46, Jan. 2013.

[16] 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.

[17] 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.

[18] H. Yin, D. Gesbert, M. Filippou, and Y. Liu, "A coordinated approach to channel estimation in large-scale multipleantenna systems," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 2, pp. 264–273, Feb. 2013.

[19] 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.

[20] C. Liu, N. Yang, J. Yuan, and R. Malaney, "Location-based secure transmission for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 7, pp. 1458–1470, Jul. 2015.

[21] 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.

[22] 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.

[23] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1802–1814, Aug. 2013.

[24] C. Wang and H. Wang, "On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1814–1827, Sep. 2014.

[25] 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 Comm.*, vol. 3, no. 3, pp. 695–700, May 2004.

[26] 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.

[27] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[28] 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.

[29] 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.

[30] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 7th ed., Academic, San Diego, CA, 2007.

[31] N. M. Temme, "Computational aspects of incomplete gamma functions with large complex parameters," *Intl. Ser. Numer. Math.*, vol. 119, pp. 551–562, 1994.

[32] N. Yang, H. A. Suraweera, R. Schober, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Forensics Security*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[33] F. S. AL-Qahtani, C. Zhong, and H. Alnuweiri, “Opportunistic relay selection for secrecy enhancement in cooperative networks,” *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1756–1770, May 2015.

[34] B. Sklar, “Rayleigh fading channels in mobile digital communication systems part I: Characterization,” *IEEE Communications Magazine*, vol. 35, no. 7, pp. 90–100, Jul. 1997.

[35] L. Cheng, B. Henty, D. Stancil, F. Bai, and P. Mudalige, “Mobile vehicle-to-vehicle narrowband channel measurement and characterization of the 5.9-GHz dedicated short range communication (DSRC) frequency band,” *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1501–1516, Oct. 2007.

[36] E. Telatar, “Capacity of multi-antenna gaussian channels,” *Eur. Trans. Telecommun.*, vol. 10, no. 6, pp. 585–596, Nov. 1999.

[37] 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.

[38] M. Kang, and M.-S. Alouini, “Largest eigenvalue of complex Wishart matrices and performance analysis of MIMO MRC systems,” *IEEE J. Selec. Areas Commun.*, vol. 21, no. 3, pp.418–426, Apr. 2003.

[39] 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.

[40] 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.

Shihao Yan (M’15) received the Ph.D degree in Electrical Engineering from The University of New South Wales, Sydney, Australia, in 2015. He received the B.S. in Communication Engineering and the M.S. in Communication and Information Systems from Shandong University, Jinan, China, in 2009 and 2012, respectively. He was a visiting Ph.D student at The University of South Australia, Adelaide, Australia, in 2014. He is currently a Postdoctoral Research Fellow in the Research School of Engineering, The Australia National University, Canberra, Australia. His current research interests are in the areas of wireless communications and statistical signal processing, including physical layer security, location verification, and localization algorithms.

Robert Malaney (M’03) received the B.S. degree in physics from the University of Glasgow, Glasgow, U.K., and the Ph.D. degree in physics from the University of St. Andrews, St. Andrews, U.K. He is currently an Associate Professor at the School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, Australia. He is a former Principal Research Scientist at the Commonwealth Scientific and Industrial Research Organization (CSIRO) and a former Project Leader at the National Information and Communications Technology Australia (NICTA). He has previously held research positions at Caltech, UC Berkeley, and the University of Toronto. He has over 100 publications.