Location-Based Beamforming for Rician Wiretap Channels

Chenxi Liu and Robert Malaney
School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, Australia
Email: chenxi.liu@student.unsw.edu.au, r.malaney@unsw.edu.au

Abstract—We propose a location-based beamforming scheme for wiretap channels, where a source communicates with a legitimate receiver in the presence of an eavesdropper. We assume that the source and the eavesdropper are equipped with multiple antennas, while the legitimate receiver is equipped with a single antenna. We also assume that all channels are in a Rician fading environment, the channel state information from the legitimate receiver is perfectly known at the source, and that the only information on the eavesdropper available at the source is her location. We first describe how the beamforming vector that minimizes the secrecy outage probability of the system is obtained, illustrating its dependence on the eavesdropper’s location. We then derive an easy-to-compute expression for the secrecy outage probability when our proposed location-based beamforming is adopted. Finally, we investigate the impact location uncertainty has on the secrecy outage probability, showing how our proposed solution can still allow for secrecy even when the source has limited information on the eavesdropper’s location.

I. INTRODUCTION

Physical layer security has attracted significant research attention recently. Compared to the traditional upper-layer cryptographic techniques using secret keys, physical layer security safeguards wireless communications by directly exploiting the randomness offered by wireless channels without using secret keys, and thus has been recognized as an alternative for cryptographic techniques [1]. The principle of physical layer security was first studied in [2] assuming single-input single-output systems. It was shown that secrecy can only exist when the wiretap channel between the source and the eavesdropper is a degraded version of the main channel between the source and the legitimate receiver. Subsequently, this result was generalized to the case where the main channel and the wiretap channel are independent [3].

Most recently, implementing multi-input multi-output (MIMO) techniques at the source/legitimate receiver has been shown to significantly improve the physical layer security of wiretap channels [4–14]. In terms of MIMO techniques, beamforming [4–9], artificial noise (AN) [10–12], and transmit antenna selection [13, 14] are just a few techniques that can be utilized to boost the physical layer security of wiretap channels. In [4–14], it is assumed that the channel state information (CSI) from the eavesdropper is perfectly or statistically known at the source. This assumption, however, is unlikely to be valid in practice - especially when the eavesdropper is not an authorized component of the communication system.

In this paper we propose a location-based beamforming scheme that does not require any form of CSI be passed by the eavesdropper back to the source. Rather, we will assume that some a priori known location information of the eavesdropper is available to the source. Such a scenario can occur in many circumstances, such as those detailed in [15]. In our scheme, we assume that all of the communication channels are in a Rician fading environment. That is, the channel between the source and the legitimate receiver and the channel between the source and the eavesdropper are a combination of a line-of-sight (LOS) component and a random scattered component. We also assume that the CSI from the legitimate receiver is perfectly known at the source, while the only information on the eavesdropper available at the source is her location. Our key goal is to determine the beamforming vector at the source that minimizes the secrecy outage probability of the system, given the CSI of the main channel and the eavesdropper’s location.

Perhaps the most relevant work to ours is that of [15] in which the secrecy outage probability in Rician wiretap channels was investigated, largely for the case where the location of the eavesdropper was available at the source but where the CSI of the main channel was unavailable. Compared to [15], our work is different in the following main aspects: (i) We derive a simpler expression of the secrecy outage probability when the eavesdropper’s location and the CSI of the main channel are known. We highlight that our expression is valid for arbitrary values of average signal-to-noise ratios (SNR) and Rician $K$ factors in the main channel and the wiretap channel. (ii) Based on this new expression we develop a much more efficient search algorithm for the determination of the optimal beamforming scheme that minimizes the secrecy outage probability when the CSI of the main channel and the eavesdropper’s location are available at the source. We highlight that our new search algorithm invokes a one-dimensional search, as opposed to the multi-dimensional searches required previously, thereby greatly reducing the computational complexity (important for in-field deployments). (iii) We examine the impact of location uncertainty on the secrecy outage probability, showing how secrecy can still exist when only a noisy estimate of the eavesdropper’s location is available at the source.

II. SYSTEM MODEL

We consider a wiretap channel with Rician fading, as depicted in Fig. 1, where Alice communicates with Bob in the presence of Eve (the eavesdropper). In this channel, Alice and Eve are equipped with uniform linear arrays (ULA) with $N_A$
and $N_E$ antennas, respectively, while Bob is equipped with a single antenna. We adopt the polar coordinate system. As such, the locations of Alice, Bob, and Eve are denoted by $(0, 0)$, $(d_B, \theta_B)$, and $(d_E, \theta_E)$, respectively. We consider that the main channel between Alice and Bob and the eavesdropper’s channel between Alice and Eve are subject to quasi-static independent and identically distributed (i.i.d) Rician K-factors. We also consider that a $K$-factor map ($K$ as a function of location) is known in the vicinity of Alice via some a priori measurement campaign. We assume that the CSI of the main channel is known to Alice, while the only available information on Eve is her location. This assumption is reasonable in some military application scenarios where Alice can obtain Eve’s location through some a priori surveillance.

We denote $h$ as the $1 \times N_A$ channel vector from Alice to Bob, which is given by

$$h = \sqrt{\frac{K_B}{1 + K_B}} h_o + \sqrt{\frac{1}{1 + K_B}} h_r,$$  

(1)

where $K_B$ denotes the Rician $K$-factor of the main channel, $h_o$ denotes the LOS component, and $h_r$ denotes the scattered component - the elements of which are assumed to be i.i.d complex Gaussian random variables with zero mean and unit variance, i.e., $h_o \sim \mathcal{CN}(0_{N_A}, I_{N_A})$. In (1), $h_o$ is expressed as [16]

$$h_o = \left[1, \cdots, \exp(j2\pi(N_A - 1)\delta_A \cos \theta_B)\right],$$  

(2)

where $\delta_A$ denotes the constant spacing, in wavelengths, between adjacent antennas of the ULA at Alice. We also denote $G$ as the $N_E \times N_A$ channel matrix from Alice to Eve, which is given by

$$G = \sqrt{\frac{K_E}{1 + K_E}} G_o + \sqrt{\frac{1}{1 + K_E}} G_r,$$  

(3)

where $K_E$ denotes the Rician $K$-factor of the eavesdropper’s channel, $G_o$ denotes the LOS component, and $G_r$ denotes the scattered component - the elements of which are assumed to be i.i.d complex Gaussian random variables with zero mean and unit variance, i.e., $G_r \sim \mathcal{CN}(0_{N_E}, I_{N_E})$. In (3), $G_o$ is expressed as [17]

$$G_o = r_o^T g_o,$$  

(4)

where $r_o$ denotes the array responses at Eve, which is given by

$$r_o = \left[1, \cdots, \exp\left(-j2\pi(N_E - 1)\delta_E \cos \phi_E\right)\right],$$  

(5)

where $\delta_E$ denotes the constant spacing, in wavelengths, between adjacent antennas of the ULA at Eve, and $\phi_E$ denotes the angle of arrival from Eve to Alice (see Fig. 1), and $g_o$ denotes the array response at Alice, which is given by

$$g_o = \left[1, \cdots, \exp\left(j2\pi(N_A - 1)\delta_A \cos \theta_E\right)\right].$$  

(6)

According to (1)–(6), we express the received signal at Bob as

$$y_B = \sqrt{P_A d_B^\eta} h x_A + n_B,$$  

(7)

where $P_A$ denotes the transmit power at Alice, $\eta$ denotes the path loss component, $x_A$ denotes the transmitted signal by Alice, and $n_B$ denotes the thermal noise at Bob - which is assumed to be a complex Gaussian random variable with zero mean and variance $\sigma_B^2$, i.e., $n_B \sim \mathcal{CN}(0, \sigma_B^2)$. In (7), $x_A$ is expressed as

$$x_A = w t_A,$$  

(8)

where $w$ denotes the $1 \times N_A$ beamforming matrix, and $t_A$ is a scalar, which denotes the information signal transmitted by Alice. We assume that $\|w\|^2 = 1$ and $\mathbb{E}[t_A^2] = 1$. We then express the received signal at Eve as

$$y_E = \sqrt{P_A d_E^\eta} G x_A + n_E,$$  

(9)

where $n_E$ denotes the thermal noise vector at Eve - the elements of which are assumed to be i.i.d complex Gaussian random variables with zero mean and variance $\sigma_E^2$, i.e., $n_E \sim (0_{N_E}, I_{N_E})$. As such, we express the received SNR at Bob as

$$\gamma_B = \gamma_B | hw |^2,$$  

(10)

where $\gamma_B = P_A d_B^\eta / \sigma_B^2$. Note, we assume that Eve adopts maximal ratio combining (MRC) [19] to process her received signal (maximizing her SNR). As per the rules of MRC, the received SNR at Eve is expressed as

$$\gamma_E = \gamma_E \|Gw\|^2,$$  

(11)

where $\gamma_E = P_A d_E^\eta / \sigma_E^2$.
III. LOCATION-BASED BEAMFORMING SCHEME

We first describe in detail how the optimal beamforming scheme that minimizes the secrecy outage probability is obtained by utilizing Bob’s CSI and Eve’s location. We then derive an easy-to-compute expression for the secrecy outage probability when the proposed location-based beamforming scheme is applied.

Based on (10) and (11), the achievable secrecy rate in the wiretap channel is expressed as [18]

\[
C_S = \begin{cases} C_B - C_E, & \gamma_B > \gamma_E \\ 0, & \gamma_B \leq \gamma_E, \end{cases}
\]  
(12)

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. In this wiretap channel, if \( C_S \geq R_S \), where \( R_S \) denotes a given secrecy transmission rate, the perfect secrecy is guaranteed. If \( C_S < R_S \), information on the transmitted signal is leaked to Eve, and the secrecy is compromised. In order to evaluate the secrecy performance, we adopt the secrecy outage probability as the performance metric - defined as the probability that the achievable secrecy rate is less than a given secrecy transmission rate conditioned on \( \gamma_B \). Mathematically, this is formulated as

\[
P_{\text{out}} (R_S) = \Pr (C_S < R_S | \gamma_B). \]  
(13)

Our goal is to find the optimal beamforming vector that minimizes the secrecy outage probability. That is, we wish to find

\[
w^* = \arg \min_{w, ||w||^2 = 1} P_{\text{out}} (R_S). \]  
(14)

In order to solve (14), we present the following proposition.

**Proposition 1:** Given \( \tau \in [0, 1] \), the optimal beamforming vector \( w^* \) that minimizes the secrecy outage probability is a member of the following family of beamformer solutions,

\[
w (\tau) = \sqrt{\tau}w_{ZF} + \sqrt{1 - \tau}w_{ZF}^\perp. \]  
(15)

Here, \( w_{ZF} = \frac{\Psi_{G_o, h_o}^H h}{||\Psi_{G_o, h_o}^H||} \), where \( \Psi_{G_o, h_o} = I_{N_A} - G_o^H (G_o G_o^H)^{-1} G_o \); and \( w_{ZF}^\perp = \frac{\Psi_{G_o, h_o}^H}{||\Psi_{G_o, h_o}^H||} \), where \( \Psi_{G_o} = G_o^H (G_o G_o^H)^{-1} G_o \).

**Proof:** Suppose that \( \{w_{ZF}, w_{ZF}^\perp, w_3, \ldots, w_{N_A}\} \) denotes an orthonormal basis in the complex space \( \mathbb{C}^{N_A} \). As such, any beamforming vector at Alice can be expressed as [20]

\[
w = \lambda_1 w_{ZF} + \lambda_2 w_{ZF}^\perp + \sum_{i=3}^{N_A} \lambda_i w_i, \]  
(16)

where \( \lambda = [\lambda_1, \lambda_2, \ldots, \lambda_{N_A}] \) are complex and \( ||\lambda||^2 = 1 \). We first note that the achievable secrecy rate \( C_S \) is a function of \( w \). We then note that beamforming into \( w \) has no impact on the capacity of the main channel \( C_B \). This is due to the fact that \( w \) are orthogonal to the plane spanned by \( \{w_{ZF}, w_{ZF}^\perp\} \) and the main channel lies in this plane. We also find that beamforming into \( w \), on the other hand, may increase the capacity of the eavesdropper’s channel \( C_E \) unless the eavesdropper’s channel \( G \) also lies in the plane spanned by \( \{w_{ZF}, w_{ZF}^\perp\} \).

Based on the above analysis, we see that beamforming into \( w \) decreases \( C_S \) or has no impact on \( C_S \). As such, we confirm that the optimal beamforming vector has the following structure, given by

\[
w (\tau) = \sqrt{\tau} \exp (j\theta_a) w_{ZF} + \sqrt{1 - \tau} \exp (j\theta_b) w_{ZF}^\perp. \]  
(17)

We note that \( (\theta_a) \) and \( (\theta_b) \) in (17) are general phases have no impact on \( C_S \), thus without loss of generality we can set \( \theta_a = \theta_b = 0 \). Substituting \( \theta_a = \theta_b = 0 \) into (17) we obtain the desired result in (15), which completes the proof.

With the aid of Proposition 1, we note that the optimal beamforming vector \( w^* \) that solves (14) can be obtained by finding the optimal \( \tau^* \) that minimizes the secrecy outage probability. As such, we re-express (14) as

\[
\tau^* = \arg \min_{0 \leq \tau \leq 1} \gamma (N_E m_E, 2^{-N_A (1 + \gamma_B) - 1}) \]  
(18)

where \( \gamma (\cdot, \cdot) \) is the lower incomplete gamma function, defined as [21, Eq. (8.350)],

\[
\gamma (\mu, \nu) = \int_0^\nu \exp (-t) t^{\mu-1} dt, \]  
(20)

\[
m_E = \left( \frac{K_E + 1}{2K_E + 1} \right)^2, \]  
(21)

where \( K_E = |g_o w (\tau)|^2 K_E \),

\[
\tilde{\gamma}_E = E [\gamma_E] = \frac{(K_E |g_o w (\tau)|^2 + 1) \gamma_E}{1 + K_E}, \]  
(22)

and \( \Gamma (\cdot) \) is the Gamma function, defined as [21, Eq. (8.310)],

\[
\Gamma (z) = \int_0^\infty \exp (-t) t^{z-1} dt. \]  
(23)
Proof: We focus on the probability density function (PDF) of $\gamma_E$ when $w(\tau)$ is adopted as the beamforming vector, which is expressed as [15]

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

(24)

The cumulative distribution function (CDF) of $\gamma_E$ is then obtained as

$$F_{\gamma_E}(\gamma) = \frac{\gamma^{N_E\hat{m}_E, \frac{m}{\gamma_E}}}{\Gamma(N_E\hat{m}_E)}. \quad (25)$$

As such, we re-express $P_{\text{out}}(R_S)$ in (13) as

$$P_{\text{out}}(R_S) = \Pr (C_B - C_E < R_S | \gamma_B)$$

$$= \Pr (C_E > C_B - R_S | \gamma_B)$$

$$= \Pr (\gamma_E > 2^{-R_S} (1 + \gamma_B) - 1)$$

$$= 1 - F_{\gamma_E}(2^{-R_S} (1 + \gamma_B) - 1). \quad (26)$$

Substituting (25) into (26), we obtain the desired result in Theorem 1. The proof is completed.

Note, in Theorem 1 Eve’s location is explicitly expressed in the expressions for $\hat{m}_E$, $\hat{F}_E$, and $\gamma_E$. Note also, that our derived expression is valid for arbitrary values of average SNRs and Rician $K$ factors in the main channel and the wiretap channel. Based on Proposition 1 and Theorem 1, we see that the optimal $\tau^*$ that minimizes $P_{\text{out}}(R_S)$ can be easily obtained through a one-dimensional numerical search.

We point out that $\phi_E$ disappears in the expression for the secrecy outage probability in Theorem 1. As an aside, it is perhaps interesting to show why this is so. To this end, we re-express $\gamma_E$ in (11) as

$$\gamma_E = \gamma_E \sum_{i=1}^{N_E} |g_{r,i}(\tau)|^2, \quad (27)$$

where $g_i$ is the $1 \times N_A$ channel vector between Alice and $i$-th Eve’s antenna, given by

$$g_i = \sqrt{\frac{K_E}{1 + K_E}} r_{o,i} g_o + \sqrt{\frac{1}{1 + K_E}} g_{r,i}, \quad (28)$$

where $r_{o,i}$ is the $i$-th element of $r_o$, given by $r_{o,i} = \exp(-2\pi (i-1) \theta_E \cos \phi_E)$ and $g_{r,i}$ is the $i$-th row of $G_r$. Based on (28), we express $g_i(\tau)$ as

$$g_i(\tau) = \sqrt{\frac{K_E}{1 + K_E}} r_{o,i} g_o(\tau) + \sqrt{\frac{1}{1 + K_E}} g_{r,i}(\tau). \quad (29)$$

We note that $|r_{o,i} g_o(\tau)|^2 = |g_{r,i}(\tau)|^2$ for any $r_{o,i}$. As such, we confirm that the value of $\phi_E$ has no impact on the secrecy outage probability. This reveals that our analysis reported here is also applicable for antenna arrays other than ULA at Eve.

IV. IMPACT OF EAVESDROPPER’S LOCATION UNCERTAINTY

Thus far, we have assumed that Eve’s location is perfectly available at Alice. In this section, we examine the impact of Eve’s location uncertainty on the secrecy performance of our proposed location-based beamforming scheme. To this end, we first characterize the uncertainty in Eve’s location.

We assume that Eve’s location, available at Alice, is obtained through some estimation. This estimation of Eve’s location can be made by using received signal strength (RSS), angle of arrival (AOA), time of arrival (TOA), and/or time difference of arrival (TDOA). In addition, we note that there will be errors in the estimated Eve’s location due to noise in the RSS and timing information measurements. To provide focus, we assume the use of the TDOA scheme, e.g. [22, 23], as the positioning algorithm. Providing such algorithms are close to optimal, we can directly utilize in our analysis a probability distribution of estimated positions derived from the Fisher matrix of the TDOA scheme.

We now detail the Fisher matrix of the TDOA scheme [24]. For the sake of generality, we assume there exist $N$ anchor points in our system that cooperate to localize Eve. We denote Eve’s true location and the location of the $n$th anchor point in a 2-D plane by $\xi_0 = [x_0, y_0]$ and $\xi_n = [x_n, y_n]$, respectively. We denote the time difference relative to that measured by anchor point 1 and the $n$th anchor point as $\phi_n$, then we obtain the logarithm of the distribution of $\phi_n$ as

$$-\ln f(\phi_n) = \frac{(\phi_n - \frac{d_n - d_0}{c})^2}{4\sigma_c^2}, \quad (30)$$

where $c$ denotes the speed of light, $\sigma_c^2$ in the variance of the timings, and $d_n$ denotes the distance between the $n$th anchor point and Eve, expressed as

$$d_n = \sqrt{(x_n - x_0)^2 + (y_n - y_0)^2}. \quad (31)$$

According to (30), we can introduce a variable as $\theta_n = \arctan \frac{y_n - y_0}{x_n - x_0}$, then we express the Fisher matrix of the TDOA scheme as

$$J(\phi_n) = \begin{bmatrix} J(\phi_n)_{11} & J(\phi_n)_{12} \\ J(\phi_n)_{21} & J(\phi_n)_{22} \end{bmatrix}, \quad (32)$$

where

$$J(\phi_n)_{11} = \frac{1}{2c^2\sigma_c^2} \sum_{n=2}^{N} (\cos \theta_n - \cos \theta_1)^2, \quad (33)$$

$$J(\phi_n)_{22} = \frac{1}{2c^2\sigma_c^2} \sum_{n=2}^{N} (\sin \theta_n - \sin \theta_1)^2, \quad (34)$$

and

$$J(\phi_n)_{12} = J(\phi_n, \varphi_n)_{21} = \frac{1}{2c^2\sigma_c^2} \sum_{n=2}^{N} (\sin \theta_n - \sin \theta_1) (\cos \theta_n - \cos \theta_1). \quad (35)$$
Based on (32), we express the covariance matrix of the true Eve’s location as $V = J^{-1}$. We further define $V$ as

$$V = \begin{bmatrix} \sigma_x^2 & \sigma_{xy} \\ \sigma_{yx} & \sigma_y^2 \end{bmatrix},$$

where $\sigma_{xy} = \sigma_{yx}$. We denote the estimated Eve’s location by $\xi_E = [x_E, y_E]$, and the correlation coefficient by $\rho = \sigma_{xy}/(\sigma_x \sigma_y)$. As such, the distribution of the estimated Eve’s location can be expressed as

$$P(\xi_E) = \frac{1}{2\pi \sqrt{1 - \rho^2} \sigma_x \sigma_y} \exp \left\{ -\frac{1}{2 (1 - \rho^2)} \left( \frac{(x_E - x_0)^2}{\sigma_x^2} + \frac{(y_E - y_0)^2}{\sigma_y^2} - \frac{2 \rho (x_E - x_0)(y_E - y_0)}{\sigma_x \sigma_y} \right) \right\}. \quad (37)$$

In order to examine the impact of the uncertainty in Eve’s location, we adopt an “average” measure of $P_{out}(R_S)$, which is given by

$$\overline{P_{out}}(R_s) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} P_{out}(R_s) P(\xi_E) \, dx_E \, dy_E. \quad (38)$$

We note that a closed-form expression for $\overline{P_{out}}(R_s)$ in (38) is not attainable. As such, we will numerically evaluate the impact of Eve’s location uncertainty on the secrecy outage probability in Section V. Specifically, such an evaluation will be performed through the following steps: (1) Obtain Eve’s estimated location by randomly selecting a position $\xi_E = [x_E, y_E]$ from the distribution given in (37). (2) Based on this estimated location, obtain the distance between Alice and Eve’s location $d_E$, and the angle from Alice to the estimated Eve’s location $\theta_E$ (see Fig. 1). (3) Substitute $d_E$ and $\theta_E$ into (19), and obtain $P_{out}(R_S)$. (4) Repeat (1)-(3) and utilize all derived $P_{out}(R_S)$ in (38), thereby obtaining $\overline{P_{out}}(R_s)$.

V. NUMERICAL RESULTS

In this section we present numerical results to validate our analysis. Specifically, we first demonstrate the effectiveness of the proposed location-based beamforming scheme. We then examine in detail the impact of the uncertainty in Eve’s location on the secrecy performance of our proposed scheme.

In Fig. 2, we plot $P_{out}(R_S)$ versus $\tau$ for different values of $N_A$ with $N_E = 2$, $K_B = 10$ dB, $K_E = 5$ dB, $\tau_B = \tau_E = 10$ dB, $\theta_B = \pi/3$, $\theta_E = \pi/4$, and $R_S = 1$ bits/s/Hz. We first observe that the analytical curves, generated from Proposition 1 and Theorem 1, precisely match the simulation points marked by black dots, thereby demonstrating the correctness of our analysis for $P_{out}(R_S)$ in Theorem 1. Second, we see that there exists a unique $\tau^*$ that minimizes $P_{out}(R_S)$ for each $N_A$. Third, we see that the minimal $P_{out}(R_S)$, denoted by $P^*(R_S)$, decreases significantly as $N_A$ increases. Furthermore, we observe that the optimal $\tau^*$ that achieves $P^*(R_S)$ approaches 1 as $N_A$ increases. This reveals that the optimal beamforming vector $w^*$ that minimizes $P_{out}(R_S)$ approaches $w_{ZF}$ as $N_A$ increases.

In Fig. 3, we plot $P^*_B(R_S)$ versus $\tau_B$ for different values of $N_A$ with $N_E = 2$, $K_B = 10$ dB, $K_E = 5$ dB, $\tau_B = \tau_E = 10$ dB, $\theta_B = \pi/3$, $\theta_E = \pi/4$, and $R_S = 1$ bits/s/Hz.
Alice uses a higher power to transmit.

In Fig. 4, we plot $P_{out}(R_S)$ versus $\tau$ for different levels of $c\sigma_t$ with $N_A = 4$, $N_E = 2$, $K_B = 10$ dB, $K_E = 5$ dB, $\theta_B = \pi/4$, and $R_S = 1$ bits/s/Hz.

![Graph](image-url)

Fig. 4: $P_{out}(R_S)$ versus $\tau$ for different values of $c\sigma_t$ with $N_A = 4$, $N_E = 2$, $K_B = 10$ dB, $K_E = 5$ dB, $\theta_B = \pi/4$, and $R_S = 1$ bits/s/Hz.

VI. CONCLUSION

In this work we have proposed a new location-based beamforming solution for Rician wiretap channels, in which a multi-antenna source communicates with a single-antenna receiver in the presence of a multi-antenna eavesdropper. In our scheme, we assumed that the CSI from the legitimate receiver is known at the source, while the only available information on the eavesdropper is her location. We showed how the beamforming vector that minimizes the secrecy outage probability of our scheme can be obtained via our simplified analytical expression for the secrecy outage probability. We also examined the impact of the eavesdropper’s location uncertainty on the secrecy performance, showing that secrecy can still exist over a wide range of (anticipated) location inaccuracies. The results presented here are of importance to a range of realistic wiretap channels in which the only information known on an eavesdropper is a noisy estimate of her location.

REFERENCES

[1] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, “Safeguarding 5G wireless communication networks using physical layer security,” IEEE Commun. Mag., vol. 53, no. 4, pp. 20–27, Apr. 2015.
[2] A. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[3] I. Csiszár and J. Körner, “Broadcast channels with confidential messages,” IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348, May 1978.
[4] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas I: The MISO wiretap channel,” IEEE Trans. Inf. Theory, vol. 56, no. 6, pp. 3088–3104, Jul. 2010.
[5] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas II: The MIMO wiretap channel,” IEEE Trans. Inf. Theory, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
[6] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, “Secrecy outage in MIMO wiretap channels: Beamforming with imperfect CSI,” in Proc. IEEE ICC 2014, Sydney, Australia, Jun. 2014.
[7] S. Yan and R. Malaney, “Optimal transmission with artificial noise in MIMO multiuser networks,” IEEE Trans. Commun., vol. 62, no. 7, pp. 2515–2530, Jul. 2014.
[8] J. Li, and A. P. Petropulu, “Ergodic secrecy rate for multiple-antenna wiretap cahnnels with Rician fading,” IEEE Trans. Inf. Foren. Sec., vol. 6, no. 3, pp. 861–867, Sep. 2011.
[9] X. Zhang, X. Zhou, and M. R. McKay, “On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels,” IEEE Trans. Veh. Technol., vol. 62, no. 5, pp. 2170–2181, Jun. 2013.
[10] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, “Artificial noise: Transmission optimization in multi-input single-output wiretap channels,” IEEE Trans. Commun., vol. 63, no. 5, pp. 1771–1783, May 2015.
[11] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, “Optimal transmission with artificial noise in MISO wiretap channels,” IEEE Trans. Veh. Technol., accepted to appear.
[12] 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.
[13] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, “MIMO wiretap channels: A secure transmission using transmit antenna selection and receive generalized selection combining,” IEEE Commun. Lett., vol. 17, no. 9, pp. 1754–1757, Sep. 2013.
[14] S. Yan and R. Malaney, “Secrecy performance analysis of location-based beamforming in Rician wiretap channels,” arXiv:1412.6882.
[15] J. -A. Tsai, R. Buehrer, and B. D. Woerner, “BER performance of a uniformly 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.
[16] 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.
[17] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” IEEE Trans. Inf. Theory, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
[18] P. A. Dighe, R. K. Mallik, and S. S. Jammul, “Analysis of transmitreceive diversity in Rayleigh fading,” IEEE Trans. Commun., vol. 51, no. 4, pp. 694–703, Apr. 2003.
[19] G. Taricco, C. Schenker, and E. A. Jorswieck, “Secrecy outage in MISO systems with partial channel information,” IEEE Trans. Inf. Foren. Sec., vol. 7, no. 2, pp. 704–716, Apr. 2012.
[20] I. S. Gradshteyn and I. M. Ryzhik, Table of Integrals, Series, and Products, 7th edition. Academic Press, 2007.
[21] Y.-T. Chan and K. Ho, “A simple and efficient estimator for hyperbolic location,” IEEE Trans. Signal Process., vol. 42, no. 8, pp. 1905-1915, Aug. 1994.
[22] Y.-T. Chan, H. Yau Chin Hang, and P.-C. Ching, “Exact and approximate maximum likelihood localization algorithms,” IEEE Trans. Veh. Technol., vol. 55, no. 1, pp. 10-16, Jan. 2006.
[23] 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.