Security Optimization of Exposure Region-based Beamforming with a Uniform Circular Array


Published in:
IEEE Transactions on Communications

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal

Publisher rights
© 2017 IEEE
This work is made available online in accordance with the publisher's policies. Please refer to any applicable terms of use of the publisher.

General rights
Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.
Security Optimization of Exposure Region-based Beamforming with a Uniform Circular Array

Yuanrui Zhang, Roger Woods, Senior Member, IEEE, Youngwook Ko, Alan Marshall, Senior Member, IEEE, and Junqing Zhang

Abstract — This paper investigates the impact of a uniform circular array (UCA) in the context of wireless security via exposure region (ER)-based beamforming. An improvement is demonstrated for the security metric proposed in our previous work, namely, the spatial secrecy outage probability (SSOP), by optimizing the configuration of the UCA. Our previous work focused on formalizing the SSOP concept and exploring its applicability using a uniform linear array example. This paper proposes the UCA as a superior candidate because it is more robust against the effects of mutual coupling. The UCA's SSOP configuration is explored and a special expression is derived from the general expression for the first time, and a closed-form upper bound is then generated to facilitate analysis. By carefully designing the UCA structure particularly the radius, an SSOP optimization algorithm is derived and explored for mutual coupling. It is shown that the information leakage to eavesdroppers is reduced while the legitimate user's received signal quality is enhanced due to the use of beamforming.

Index Terms — Physical layer security, beamforming, exposure region, spatial secrecy outage probability, uniform circular array.

I. INTRODUCTION

Wireless communication is vulnerable to passive eavesdropping due to its broadcast nature. Physical layer security exploits the unique and unpredictable features of wireless channels such as fading and has shown a great potential to secure future wireless technologies [1], [2]. This technique dates back to Wyner's seminal work on the wiretap channel model [3], which has triggered much fruitful research and has been extended to various channel models, such as fading channels and multiple antenna channels [4]–[7].

In the physical layer security scenario with legitimate users wishing to carry out secure communication with eavesdroppers observing the transmissions, the channel of the legitimate user in Wyner's wiretap channel model is required to be better than that of the eavesdroppers, at least for a fraction of realizations in the case of fading channels [4]. When the legitimate transmitter is equipped with multiple antennas or an antenna array, beamforming is an effective technique to enlarge the difference of the legitimate users' and eavesdroppers' channels.

This work was supported by the US-Ireland R&D Partnership USI033 WiPhyLoc8 grant involving Rice University (USA), University College Dublin (Ireland) and Queen’s University Belfast (Northern Ireland).

Y. Zhang, R. Woods, Y. Ko, and J. Zhang are with the School of Electronics, Electrical Engineering and Computer Science, Queen’s University Belfast, Belfast, BT9 5AH, U.K. (email: {yzhang31, r.woods, y.ko, j.zhao10}@qub.ac.uk)

A. Marshall is with Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, U.K. (email: Alan.Marshall@liverpool.ac.uk)

Beamforming can be used to create physical regions within which any user can correctly receive the message [10]–[13]; the area was defined as an ‘exposure region’ (ER) in [10]. However, these regions were not based on information-theoretic parameters, such as secrecy capacity or secrecy outage probability (SOP) [4], and thus lacked a quantitative measure of the security level. On the other hand, some information theoretical based methods lacked of the analysis from a physical perspective, for example, the aspect of antenna arrays [14]–[18]. In our previous work [19], we proposed an ER-based beamforming approach which led to the derivation of the spatial secrecy outage probability (SSOP) from an information-theoretic perspective and links with the antenna array configuration. Fig. 1 illustrates a transmitter (Alice) with an antenna array that communicates to a legitimate user (Bob) in the presence of eavesdroppers (Eves) with their location distribution following a Poisson point process (PPP); this hints towards the utilization of location in the Wyner’s channel model. The ER is defined by the physical region where any PPP distributed Eve causes secrecy outage to the legitimate transmission in the Rician fading channel. In [19], the secrecy outage caused by PPP distributed Es is quantitatively measured by the SSOP that is derived from the ER. The general expression of the SSOP for any type of array is derived and the uniform linear array (ULA) is used as an example to explore the properties of the array parameters.

Based on the knowledge of the previous work, we advance knowledge in this paper by optimizing the array parameters. The uniform circular array (UCA) is chosen rather than the ULA because of practical considerations, namely mutual coupling. Mutual coupling is the electromagnetic interaction between the antenna elements of an array and is always...
associated with multiple antenna techniques [20], [21]. In [22], it has been shown that linear arrays are susceptible to mutual coupling, thus rendering no effective optimum solution for minimizing the SSOP. On the other hand, the UCA is less affected and produces a more symmetric beam pattern around 360° [23]. Thus, it is chosen as the candidate to exhibit the optimization of the array parameters, especially the radius.

We assume that Bob’s location information is available at Alice, which is similar to that used in [9]. For example, Bob could send his own location information to Alice, if he wishes to be served by Alice with additional security features. Alice exploits Bob’s location information to perform the beamforming.

In fading channels, the security performance of the aforementioned system, i.e., Alice using beamforming to enlarge the difference between Bob’s and Eves’ channels, can be expressed in terms of secrecy outage. In [24], the secrecy outage probability (SOP) for a single Eve is given by the probability that Eve’s channel capacity is higher than a certain threshold; this is defined by the difference between the rate of the transmitted codewords and that of the confidential information, conditioned on Bob’s channel capacity being larger than the rate of the transmitted codewords. In other words, the ER is an enclosed area within the boundary where Eve’s channel capacity is just equal to that threshold. As Eve’s channel capacity is random due to fading, the boundary of the ER shifts. In Fig. 1, the dashed curve depicts an ER boundary for a deterministic channel, which resembles the shape of the array pattern.

Intuitively, the smaller the ER is, the less possible that Eves are located inside the ER, and therefore the more secure the transmission will be. The overall secrecy outage caused by PPP distributed Eves, i.e., SSOP, is calculated with the aid of stochastic geometry theory, which links the security performance with the UCA parameters. This paper builds substantially on our previous work [19], [25] by investigating the SSOP with respect to UCA parameters in Rician fading channel and creating an optimization algorithm which minimizes the SSOP by adjusting the radius. In addition, the impact of mutual coupling is examined on the SSOP using numerical data. The optimization algorithm and shows that while the algorithm in general is valid, the optimum value needs to be calculated using numerical data.

The rest of the paper is organized as follows. In Section II, the system model is introduced and the definitions of the ER and the SSOP are presented. In Section III, the closed-form expression of the upper bound is derived and from this the impact of the radius of the UCA is analyzed. In Section IV, the optimization problem is established and analyzed with respect to the UCA array parameters; an algorithm is then created with the aim of decreasing the SSOP. In Section V, simulation and numerical results are given. Section VI concludes the paper.

II. EXPOSURE REGION AND SPATIAL SECRECY OUTAGE PROBABILITY

A. System Model

As the paper builds on [19], the system model is the same except for the UCA aspect. For this reason, the essential symbols, concepts and derivations for the UCA are described briefly to avoid repetition. Let’s assume that Alice is equipped with an antenna array while Bob and Eves have a single antenna. As shown in Fig. 1, Alice is located at the origin point. For convenience, assume that the first element of the UCA is on the positive x-axis. The coordinate is denoted by $d, \theta$. For the ease of subsequent mathematical derivations, let $d = (d, \theta)$, and subscripts $B$ and $E_i$ are used to represent Bob and the $i^{th}$ Eve respectively, $\forall i \in \mathbb{N}^+$. A general user’s location is referred to by $z$ when no subscript is specified. Eves are assumed to be non-colluding and distributed by a homogeneous PPP, $\Phi_e$ with density $\lambda_e$ [27].

On the transmitter side, the UCA has $N$ elements and radius $R$, and the array vector of UCA is $s(\theta) = [e^{-j\phi_1(\theta)}, ..., e^{-j\phi_k(\theta)}, ..., e^{-j\phi_N(\theta)}]^T$, $\theta \in [0, 2\pi]$, where $\phi_i(\theta) = kR\cos(\theta - \psi_i)$, and $\psi_i = 2\pi(i - 1)/N$ is the angular location of the $i^{th}$ element [28] and $k = 2\pi/\lambda$, where $\lambda$ is the wavelength of the carrier signal. $P_t$ is the transmit power. Given Bob’s location information, $\theta_B$, the beamforming weight vector can be set as $w = s(\theta_B)/\sqrt{N}$.

Assume a Rician channel with factor $K$. The channel gain vector is given by

$$h(z) = d^{-\beta/2} \left( \sqrt{\frac{K}{K+1}} s(\theta) + \sqrt{\frac{1}{K+1}} g \right),$$

where $d^{-\beta/2}$ denotes the large-scale path loss with the path loss exponent $\beta$ of typical values between 2 and 6. The line-of-sight (LOS) component is $\sqrt{\frac{K}{K+1}} s(\theta)$; the non-LOS component is $\sqrt{\frac{1}{K+1}} g$, where $g = [g_1, ..., g_N]^T$, $g_i \sim \mathcal{CN}(0, 1)$, and the elements of $g$ are independent. Thus, the received signal at $z$ is the sum of the beamforming weighted signals and noise, which can be expressed by

$$r(z) = \sqrt{P_t} h^T(z) w^* x + n_W,$$

where $x$ is the modulated symbol with unit power and $n_W$ is the additive white Gaussian noise with zero mean and variance $\sigma_w^2$.

For the ease of subsequent mathematical derivations, let $\tilde{h}$ be an equivalent channel factor, i.e.,

$$\tilde{h} = h^T(z) w = \sqrt{\frac{K}{K+1}} G(\theta, \theta_B) + \sqrt{\frac{1}{K+1}} g.$$
where \( G(\theta, \theta_B) = s(\theta)^* (\theta_B)/\sqrt{N} \) is an array factor for any array type and \( g \sim CN(0, 1) \). According to (2), \(|\tilde{h}|^2\) can be decomposed as follows:
\[
|\tilde{h}|^2 = \frac{KG^2(\theta, \theta_B)}{K + 1} + \frac{g_{Re}^2 + g_{Im}^2}{K + 1} + \frac{2\sqrt{K}G(\theta, \theta_B)}{K + 1} g_{Re},
\]
(3)
where \( g_{Re} \) and \( g_{Im} \) are the real and imaginary part of \( g \), so \( g_{Re,Im} \sim N(0, 1/2) \). For the UCA, the array factor was derived in [28] and is given by
\[
G(\theta, \theta_B) = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} e^{j k R(\cos(\theta_B-\psi_i)-\cos(\theta-\psi_i))}.
\]
(4)
The channel capacity, denoted by \( C(z) \), is given by
\[
C(z) = \log_2 \left( 1 + \frac{P_t |\tilde{h}|^2}{\sigma_n^2 d^3} \right).
\]
(5)
For convenience, let \( C_B = C(z_B) \) and \( C_{Ei} = C(z_{Ei}) \) denote the channel capacities of Bob and the \( i^{th} \) Eve hereafter. Due to the fact that \(|\tilde{h}|^2\) scales with \( G(\theta, \theta_B) \), a proper design of \( G(\theta, \theta_B) \) can improve \( C_B \) while decreasing \( C_{Ei} \).

### B. Definitions for ER and SSOP for UCA
As in [24], let \( R_B \) and \( R_s \) be the rate of the transmitted codewords and the rate of the confidential information, respectively. A secrecy outage event occurs when Eve’s channel capacity is higher than the difference \( R_B - R_s \) conditioned on \( C_B \geq R_B \), and the probability of such an event is the SOP. Note that here two cases are differentiated, i.e., secrecy outage caused by any Eve conditioned on \( C_B \geq R_B \) and data outage given by \( C_B < R_B \). In the latter case, it is typical outage with no secrecy and thus no secrecy outage. Therefore, the data outage is not part of the secrecy outage and is beyond the scope of this paper. In practice, Bob can transmit a one bit feedback to Alice indicating whether the condition \( C_B \geq R_B \) is satisfied.

The ER, denoted by \( \Theta \), is defined by the geometric region only where Eves cause the secrecy outage event, i.e., \( C_{Ei} > R_B - R_s, \exists z_{Ei} \in \Theta \) conditioned on \( C_B \geq R_B \). The boundary of ER can be derived from \( C(z) > R_B - R_s \) and is given by \( D(\theta) = (c_0 P_t |\tilde{h}|^2)^{1/\beta} \), where \( c_0 = \frac{\sigma_n^2 (2R_B-R_s-1)}{\beta} \) is deterministic and is assumed to be constant in this paper. Thus, \( D(\theta) \) is random as \(|\tilde{h}|^2\) varies. When the channel is deterministic, \( D(\theta) \) is also deterministic, as shown by the dashed curve in Fig. 1.

Let \( A \) denote the size of \( \Theta \). For PPP-distributed Eves, the probability of \( m \) Eves being inside \( D(\theta) \) can be given by [27]
\[
\text{Prob}\{m \text{ Eves in } \Theta\} = \left( \frac{\lambda_c A}{m!} \right)^m e^{-\lambda_c A}.
\]
(6)
Thus, the SSOP, denoted by \( p \), can be defined by the probability that any Eve is located inside \( D(\theta) \).
\[
p = 1 - \text{Prob}\{0 \text{ Eve in } \Theta\} = 1 - e^{-\lambda_c A}.
\]
(7)
Note that \( p \) is computed by the complementary of the probability that no Eve is inside \( \Theta \). In polar coordinates, (7) can be derived by
\[
p = 1 - \exp\left[ -\frac{\lambda_c}{2} \frac{1}{c_0 P_t} \int_0^{2\pi} (|\tilde{h}|^2)^{\frac{1}{\beta}} d\theta \right].
\]
(8)
The smaller \( p \) is, the more secure the transmission to Bob is. Due to the fact that \( \tilde{h} \) is random channel fading, it is more interesting to study the expectation of \( p \) in (8), which reflects the averaged SSOP \( \bar{p} \).
\[
\bar{p} = \mathbb{E}[|\tilde{h}|^2].
\]
(9)
The term \( \bar{p} \) in (9) can be expressed by
\[
\bar{p} = 1 - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \exp\left\{ -\frac{\lambda_c}{2} \frac{1}{c_0 P_t} \left[ \frac{KG^2(\theta, \theta_B)}{K + 1} + \frac{x^2 + y^2}{K + 1} \right]^{\frac{1}{\beta}} d\theta \right\} e^{-(x^2 + y^2)/\pi} dx dy,
\]
(10)
Notice that \( G(\theta, \theta_B) \) is a general array factor expression. For the UCA, \( p \) and \( \bar{p} \) are obtained by substituting (4) into (8) and (10).

### C. An Optimization Problem
The focus of this paper is to increase the security level of the transmission from Alice to Bob, i.e., reducing \( p \). To this end, \( \bar{p} \) is first analyzed against the factors in (10). Assume that the noise variance \( \sigma_n^2 \), channel factors \( \beta \) and \( K \), the security related parameters \( R_B \) and \( R_s \) and the density of Eves \( \lambda_c \) are fixed. The remaining factors are the transmit power \( P_t \), the array factor \( G(\theta, \theta_B) \) and Bob’s location \( (d_B, \theta_B) \). Thus, an optimization problem can be expressed by
\[
\min \bar{p} \text{ s.t. for all } d_B, \theta_B
\]
(11)
To minimize \( \bar{p} \), the interrelationship between parameters related to Alice, i.e., \( P_t \) and \( G(\theta, \theta_B) \), and Bob’s location \( (d_B, \theta_B) \) should be analyzed. Note that \( d_B \) does not appear in (10) and \( P_t \) has a monotonic relationship with \( \bar{p} \). In addition, the impact of \( P_t \) and \( G(\theta, \theta_B) \) on \( \bar{p} \) are independent according to (10). In this paper, when studying the impact of \( G(\theta, \theta_B) \), \( P_t \) and \( d_B \) will be not be included.

\( G(\theta, \theta_B) \) in (4) depends on the array parameters \( N \) and \( R \) as well as Bob’s angle \( \theta_B \). As the number of antennas \( N \) is normally fixed for a certain UCA, the impact of \( R \) will be mainly discussed against \( \theta_B \). Due to the reflection and rotation symmetry of the UCA, the shape of \( G(\theta, \theta_B) \) also has reflection and rotation symmetry regarding \( \theta_B \). An example of \( G(\theta, \theta_B) \) with \( \theta_B = 0, \pi/4 \) and \( N = 8 \) is shown in Fig. 2. As the first element of the UCA lies on the positive x-axis, the shape of \( G(\theta, \theta_B) \) for \( \theta_B = \pi/4 \) can be obtained by shifting the shape for \( \theta_B = 0 \) by \( \pi/4 \), and vice versa. At the same time, the two shapes are symmetric regarding to \( \theta_B = \pi/2 \). In general, \( G(\theta, \theta_B) \) at \( \pm(\theta_B \pm 2\pi/4) \) are of the same shape. Therefore, it suffices to study \( G(\theta, \theta_B) \) only in \( \theta_B \in [0, \pi/2] \) instead of \( [0, 2\pi] \).
The expression of $\bar{p}$ in (10) is complex and can be calculated numerically. However, it is not tractable to obtain in closed-form expression, except for the deterministic channel when $\beta = 2$. Therefore, an upper bound expression for $\bar{p}$, denoted by $\bar{p}_{up}$, should be derived in closed-form for UCA in order to facilitate detailed theoretical analysis. Notice that for other array types, the method of analyzing $\bar{p}$ via closed-from expression of $\bar{p}_{up}$ still works. If closed-form expressions of $\bar{p}_{up}$ do not exist, appropriate approximations or numerical results can be used based on the particular form of given $G(\theta, \theta_B)$.

III. CLOSED-FORM EXPRESSION FOR THE UPPER BOUND FOR SSOP

A. Derivation of the Upper Bound for UCA

Firstly, a general upper bound is briefly introduced as follows, based on which the particular upper bound for UCA can be derived. For a given $\lambda_c$ and $K$, $\bar{p}_{up}$ can be derived using Jensen’s inequality.

$$\bar{p}_{up} = 1 - \exp\left\{ -\lambda_c \pi \left[ e_0 P_0 \frac{K A_0 + 2 \pi \theta^2}{2 \pi (K + 1)} \right] \right\}, \quad (12)$$

where $A_0$ denotes the pattern area and is given by.

$$A_0 = \int_0^{2\pi} G^2(\theta, \theta_B) \, d\theta. \quad (13)$$

The derivation is described in [19]. According to (12), $\bar{p}_{up}$ is monotonically increasing with $A_0$ for any $K$ and $\beta$. Therefore, $\bar{p}_{up}$ can be analyzed via $A_0$.

Notice that the expression of $A_0$ in (13) contains $G(\theta, \theta_B)$ which is a general expression. To obtain the particular expression for the UCA, the expression of $A_0$ needs to be determined. We can isolate $\theta$ to solve the integral in (4).

$$G^2(\theta, \theta_B) = \frac{1}{N} \sum_{i,j} e^{jkR[\cos(\theta_B - \psi_i) - \cos(\theta_B - \psi_j)]} \cdot e^{-jkR[\cos(\theta - \psi_i) - \cos(\theta - \psi_j)]}, \quad (14)$$

where $\sum_{i,j}$ represents $\sum_{i=1}^{N} \sum_{j=1}^{N}$ and $\cos(\theta - \psi_i) - \cos(\theta - \psi_j)$ can be further derived by

$$\cos(\theta - \psi_i) - \cos(\theta - \psi_j) = 2 \sin(\theta - \frac{i + j - 2}{N} \pi) \sin(\frac{i - j}{N} \pi).$$

(15)

Let $W_{i,j} = 2 \sin(\frac{i-j}{N} \pi)$ and $Z_{i,j} = \frac{i+j-2}{2} \pi$. Substituting (15) into (14), $G^2(\theta, \theta_B)$ can be derived as

$$\frac{1}{N} \sum_{i,j} e^{jkRW_{i,j}} \sin(\theta_B - Z_{i,j}), \quad (16)$$

According to $J_n(x) = \frac{1}{\pi} \int_{-\pi}^{\pi} e^{in(\tau - x \sin \tau)} d\tau$, where $J_n(x)$ is the Bessel function of the first kind with order $n$, the following integration can be derived.

$$\int_0^{2\pi} e^{-jkRW_{i,j}} \sin(\theta_B - Z_{i,j}) \, d\theta = \int_{-\pi}^{\pi} e^{jkRW_{i,j}} \sin(\theta + Z_{i,j}) \, d\tau = 2\pi J_0(kRW_{i,j}). \quad (17)$$

Note that in the second step, the upper and lower limits can be transformed to $\pi$ and $-\pi$, because $\sin \tau$ is a periodic function with a period of $2\pi$.

Combining (16) and (17), $A_0$ in (13) can be written as

$$A_0 = \frac{2\pi}{N} \sum_{i,j} J_0(kRW_{i,j}) e^{jkRW_{i,j}} \sin(\theta_B - Z_{i,j}). \quad (18)$$

The double summation of Bessel functions in (18) is intractable to analyze. In the following, $A_0$ will be further simplified. Let $A_{0,i,j}$ denote each summation term in (18).

$$A_{0,i,j} = \frac{2\pi}{N} J_0(kRW_{i,j}) e^{jkRW_{i,j}} \sin(\theta_B - Z_{i,j}). \quad (19)$$

It is deduced that $W_{i,j} = -W_{j,i}$ and $Z_{i,j} = Z_{j,i}$. Considering that $J_n(-x) = (-1)^n J_n(x)$ and $J_0(x)$ is a real number, it can be deduced that $A_{0,i,j} = A_{0,j,i}$. In addition, it can be shown from the expression of $W_{i,j}$ and $Z_{i,j}$ that $W_{i,j+N} = -W_{i,j}$. Similarly, $\sin(\theta_B - Z_{i,j+N}) = -\sin(\theta_B - Z_{i,j})$. Thus, it can be determined found that $A_{0,i,j} = A_{0,i,j+N}$.

A table of $A_{0,i,j}$ is shown in Fig. 3 to illustrate how to use the previous properties to simplify the summation of $A_0$ in (18). For $N = 4$, the table is extended to $j = 8$. As $A_{0,i,j} = A_{0,i,j+N}$, the blue region is equivalent to the green region. Instead of adding $A_{0,i,j}$ for $i$ from 1 to $N$, the summation can now be executed diagonally. For convenience, let $n = i-j$. Then, $W_n = W_{i,j} = 2 \sin(\frac{n \pi}{N})$. The terms $A_{0,i,j}$ on the red diagonal lines in the table have the same $W_n$. In the table, $\frac{N}{2} Z_{i,j}$ is allocated according to their indices $i$ and $j$. Given $n = i-j$, it can be derived that

$$Z_{n,i} = Z_{i,j} = \frac{i + j - 2}{N} \pi = \frac{2i - n - 2}{N} \pi. \quad (20)$$

Thus, it can be derived that

$$A_{0,n,i} = A_{0,i,j} = \frac{2\pi}{N} J_0(kRW_n) e^{jkRW_n} \sin(\theta_B - Z_{n,i}), \quad (21)$$

which is a general expression.
Thus, it can be derived that
\[ e_{i,j} \in Z \]
(23) at the top of the following page.

\[ i > j \]

\[ n \]

A. \textbf{Impact of } R \textbf{ on } A_0

As discussed in Section II-C, the impact of \( R \) will be used as a starting point to formulate the optimization problem. In the low region of \( x \), the Bessel function \( J_N(x) \) in (26) is negligible for high order \( LN \), i.e., \( LN \gg 1 \). Let \( x_0 \) denote the upper limit of the range \( x \in [0, x_0] \) where \( J_N(x) \) is negligible for certain \( LN \). Then, the specific value \( x_0 \) depends on the order \( LN \). As the order \( LN \) increases, \( x_0 \) increases and eventually exceeds the value of \( 2kR \), which is the upper limit of \( x = KRW_n \) in (26) for a fixed \( R \). Once \( x_0 \) becomes larger than \( 2kR \), all \( J_N(x) \) for \( l \geq 1 \) are negligible in the range \( (0, 2kR] \). Thus, for sufficiently large \( N \), \( A_0 \) in (26) can be approximated by

\[ A_0 \approx 2\pi \sum_{n=0}^{N-1} J_N^2(kRW_n). \]  (27)

The asymptotic behavior of \( A_0 \) versus \( R \) can be analyzed through (27). As shown in the upper plot in Fig. 4, when \( n = 0 \), \( J_0(kRW_0) = 1 \), because \( W_0 = 0 \) and \( J_0(0) = 1 \) is a constant that is irrelevant to \( R \). When \( n \neq 0 \), \( J_0(kRW_n) \) gradually decreases with some fluctuation as \( R \) increases, which is determined by the nature of \( J_0(\cdot) \). Notice that in the asymptotic expression in (27), the \( \theta_B \) is neglected. When \( N \) is not large enough, the term \( J_N(kRW_n)e^{JN\theta_B} \) also needs to be considered. As \( J_N(x) \) decreases and approaches zero with different convergence speed, the summation of a series of Bessel functions, i.e., \( A_0 \), in general decreases and approaches a certain value as \( R \) increases. Due to the difference in the converging speed of \( J_l(kRW_n) \), there are some fluctuations.

An example of \( A_0 \) versus \( R \) is shown in the lower plot in Fig. 4 where \( N = 8 \) and \( \theta_B = 0^\circ \). It can be seen that \( A_0 \) fluctuates as \( R \) increases, because the curve is a superposition of \( J_N(kRW_n) \) with different orders \( LN \). Thus, in a local region, e.g., \( R < 2\lambda \), the minimum value does not necessarily correspond to a large or small \( R \), which leads to the optimization problem for \( R \).

IV. \textbf{Optimization Algorithm}

A. \textbf{Refined Optimization Problem}

As mentioned in Section III-B, \( R \) can be properly designed according to \( \theta_B \) to achieve a local minimum value in a certain range of \( R \). According to Section II-C, \( d_B \) is not involved in the expression of \( \tilde{p} \). Thus, the optimization problem can be solved by optimizing \( R \) according to \( \theta_B \).

It is worth noticing that although the closed-form expression of \( \tilde{p}_{up} \) provides an asymptotic analysis on the impact of \( R \), it does not provide accurate results for the optimum value for \( R \). As it is intractable to analyze the expression of \( \tilde{p} \) in (10), we will use numerical results to determine this.

Examples of \( \tilde{p} \) versus \( R \) for different \( \theta_B \) are shown in Fig. 5 where \( N = 8 \). For simplicity, let \( K \rightarrow \infty \) and \( \beta = 2 \), i.e., the

\[
\begin{align*}
\text{Table for } Z_{i,j}, N = 4. \\
\end{align*}
\]

<table>
<thead>
<tr>
<th>( i-j )</th>
<th>( n=0 )</th>
<th>( n=-1 )</th>
<th>( n=-2 )</th>
<th>( n=-3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 1 )</td>
<td>( 1 )</td>
<td>( 2 )</td>
<td>( 3 )</td>
<td>( 4 )</td>
</tr>
<tr>
<td>( 2 )</td>
<td>( 2 )</td>
<td>( 3 )</td>
<td>( 4 )</td>
<td>( 5 )</td>
</tr>
<tr>
<td>( 3 )</td>
<td>( 3 )</td>
<td>( 4 )</td>
<td>( 5 )</td>
<td>( 6 )</td>
</tr>
<tr>
<td>( 4 )</td>
<td>( 4 )</td>
<td>( 5 )</td>
<td>( 6 )</td>
<td>( 7 )</td>
</tr>
<tr>
<td>( 5 )</td>
<td>( 5 )</td>
<td>( 6 )</td>
<td>( 7 )</td>
<td>( 8 )</td>
</tr>
<tr>
<td>( 6 )</td>
<td>( 6 )</td>
<td>( 7 )</td>
<td>( 8 )</td>
<td>( 9 )</td>
</tr>
</tbody>
</table>

Substituting (26) in (13), the closed-form expression for \( \tilde{p}_{up} \) in (12) can be obtained. Compared to (13), the expression of \( A_0 \) in (26) consists of a finite summation of \( J_0(\cdot) \) and an infinite summation of \( J_N(\cdot) \), which can provide asymptotic analysis.
\[ A_0 = \frac{2\pi}{N} \sum_{n=0}^{-(N-1)} J_0(kRW_n) \sum_{m=-\infty}^{\infty} J_m(kRW_n) e^{jm(\theta_B - Z_{n,i})} \]
\[ = \frac{2\pi}{N} \sum_{n=0}^{-(N-1)} J_0(kRW_n) \sum_{m=-\infty}^{\infty} J_m(kRW_n) e^{jm\theta_B} \sum_{i=1}^{N} e^{-jmZ_{n,i}} \]
\[ = \frac{2\pi}{N} \sum_{n=0}^{-(N-1)} J_0(kRW_n) \sum_{m=-\infty}^{\infty} J_m(kRW_n) e^{jm\theta_B} e^{j\pi p/(n+2)} \sum_{i=1}^{N} e^{-j2\pi i \frac{p}{N}}. \quad (23) \]

Fig. 4. Upper plot: Examples of \( J_0(kRW_n) \) versus \( R \). Lower plot: \( A_0 \) versus \( R \). \( N = 8, \theta_B = 0^\circ \).

channel is degraded to a free-space channel. More results for Rician fading channel will be provided in Section V-A. For the purpose of MATLAB simulation, the value of \( R \) is taken by a step of 1 cm in the range \([0.4\lambda, 2\lambda]\). Typical values of \( \theta_B \), i.e., \( \theta_B = 0^\circ, 10^\circ, 20^\circ \), are taken for the UCA with \( N = 8 \). Fig. 5 depicts the fluctuating behavior of \( \bar{p} \) with respect to \( R \) for different values of \( \theta_B \). It can be seen that the curves for different \( \theta_B \) vary. Therefore, for each \( \theta_B \), the local minimum of \( \bar{p} \) in the range \( R \in [0.4\lambda, 2\lambda] \) is given by a different value of \( \theta_B \). This suggests that by varying \( \theta_B \), a different \( R \) should be chosen in order to achieve a minimum \( \bar{p} \). However, this is not practical because \( R \) is usually predefined for an existing UCA.

Since \( R \) can only be a particular value, the optimum value \( R_{\text{opt}} \) needs to be found. To this end, the minimum mean error is used to find \( R_{\text{opt}} \) in a certain range of \( R \) that produces the minimum \( \bar{p} \) for all possible \( \theta_B \sim U(0, 2\pi) \). To establish the cost function, imagine that \( R \) is adjustable, which provides the hypothetical function of \( \bar{p}_{\text{min}} \) with respect to \( \theta_B \). Notice that the value of \( \bar{p}_{\text{min}} \) for each \( \theta_B \) is, in fact, given by a different value of \( R \). To find \( R_{\text{opt}} \), let the mean error, denoted by \( \text{err}(R) \), be the mean value of the difference between \( \bar{p} \) and \( \bar{p}_{\text{min}} \) over the range \( \theta_B \in [0, 2\pi] \),
\[ \text{err}(R) = \mathbb{E}_{\theta_B} [\bar{p} - \bar{p}_{\text{min}}]. \quad (28) \]

Note that the mean error is used instead of the mean square error because \( \bar{p} - \bar{p}_{\text{min}} \) is always non-negative. Thus, \( R_{\text{opt}} \) can be found by
\[ R_{\text{opt}} = \arg \min_R \text{err}(R). \quad (29) \]
(29) can be converted into the following expression, the derivation of which is in Appendix A.
\[ R_{\text{opt}} = \arg \min_R \bar{p}, \quad (30) \]
where \( \bar{p} \) is the averaged \( \bar{p} \) over Bob’s angles and is defined by
\[ \bar{p} = \frac{1}{2\pi} \int_0^{2\pi} \bar{p} \, d\theta_B. \quad (31) \]

B. Analysis and Implementation of Optimization Algorithm

Substituting the expression of \( \bar{p} \) in (10) into (31), the expression of \( \bar{p} \) can be obtained,
\[ \bar{p} = 1 - \frac{1}{2\pi} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \int_0^{2\pi} \exp \left\{ -\frac{\lambda_c}{2} (c_0 P_t)^{\frac{3}{2}} \right\} \]
\[ \left\{ \int_0^{2\pi} \left[ K G_C(\theta, \theta_B) \right] \frac{x^2 + y^2}{K + 1} + \frac{2\sqrt{K G_C(\theta, \theta_B)}}{K + 1} \right\} \]
\[ e^{-\left( x^2 + y^2 \right)} \frac{1}{\pi} \, d\theta_B \, d\theta \, dy. \quad (32) \]
Although (32) can be numerically calculated, it is intractable to analyze. Thus, the upper bound, denoted by \( \bar{p}_{\text{up}} \), is required for theoretical analysis.
Theorem 1:
\[
\bar{p}_{up} = 1 - \exp\left\{-\lambda_c \left[ \frac{c_0}{2\pi(K+1)} + \frac{c_0}{K+1} \right]^2 \right\}, \tag{33}
\]
where \( \bar{A}_0 \) is the expectation of \( A_0 \) over \( \theta_B \) and is given by
\[
\bar{A}_0 = \frac{1}{2\pi} \int_0^{2\pi} A_0 d\theta_B = 2\pi \sum_{n=0}^{N-1} J_0^2(kRW_n). \tag{34}
\]
The proof of Theorem 1 is given in Appendix B. It can be seen that (34) has a similar composition to \( A_0 \) in (26). Therefore, \( A_0 \) in general decreases with some fluctuations as \( R \) increases. Due to the monotonically increasing relationship between \( \bar{p}_{up} \) and \( A_0 \), it can be deduced that \( \bar{p} \) decreases in general with some fluctuations as \( R \) increases.

Because \( \bar{p} \) fluctuates in a certain range of \( R \), there must exist at least one local minimum. Numerical results are used to find \( R_{opt} \) in (30). For example, choosing \( N = 8 \) and \( R \in [0.4\lambda, 2\lambda] \), the results of \( \bar{p} \) shown in Fig. 6 are obtained where the channel is chosen as a free-space channel. It can be seen that there is more than one local minimum. In the range \( R \in [0.4\lambda, 2\lambda] \), \( R_{opt} = 1.76\lambda \) gives the minimum \( \bar{p} \) as \( 2.4 \times 10^{-3} \). Compared to the maximum value of \( \bar{p} \) that is \( 3.6 \times 10^{-3} \) in the same range, there is a \( 33\% \) reduction in the value of \( \bar{p} \). This indicates that by choosing an appropriate value of \( R \), the averaged SSOP can be dramatically reduced.

The numerical implementation of the algorithm is shown in Algorithm 1. The continuous ranges of \( R, \theta_B, \theta \) are discretized with steps of \( \Delta R, \Delta \theta_B \) and \( \Delta \theta \), respectively. In addition, a limit value \( Q \) is used when calculating integral from \( -\infty \) to \( \infty \) in (32). For a normal distribution, a realistic value is set for \( Q \), namely 3. Let \( N_R, N_{\theta_B}, N_{\theta} \) and \( N_Q \) be the number of samples for \( R, \theta_B, \theta \) and the integration range \( Q \) respectively, which determines the iteration numbers.

There are two main steps in the optimization algorithm. The first step is from line 3 to 15, where \( \bar{p} \) for a range of discretized \( R \) is calculated. Notice that the integrals in (32) are implemented via iterated summation from line 6 to 15. The second step section is from line 16 to 21, where the minimum value \( \bar{p}_{\text{min}} \) in the vector \( \bar{p} \) is searched to find \( R_{opt} \) which is the output of the optimization algorithm.

V. SIMULATION AND NUMERICAL RESULTS

In this section, we first provide simulation results for \( \bar{p} \) in (10) and then numerical results for \( \bar{p} \) in (32) over the Rician channel with a wider range of values of \( K \) and \( \beta \). Next, the numerical results of the upper bounds \( \bar{p}_{up} \) and \( \bar{p}_{up} \) are shown in comparison with \( \bar{p} \) and \( \bar{p} \) to demonstrate the validity of the upper bounds. In the end, we investigate a common problem in antenna array, i.e., the mutual coupling and its effect on \( \bar{p} \).

A. More Results for Rician Fading Channels

In Section IV-B, numerical results are used to show the properties of \( \bar{p} \) versus \( R \). Firstly, the simulation results are provided to validate the expressions of \( \bar{p} \) in (10) that is derived from the expression in (9) which contains Gaussian random variables via \( |\hat{h}|^2 \) according to (3). We choose \( K = 10 \) and \( \beta = 3 \) as an example to compare the numerical results based on the expression in (10) and the simulation results based on the expression in (9). We ran Monte Carlo simulations to generate \( 1 \times 10^4 \) samples of \( g_{hc} \) and \( g_{tm} \) in (3). As stated in Section II-C, the noise variance \( \sigma_n^2 \), channel factors \( \beta \) and...
K, the security related parameters $R_B$ and $R_s$ and the density of Eves $\lambda_e$ are assumed to be constant; the transmit power $P_t$ does not affect the impact of the array parameters to the SSOP. In this section, $P_t$ and $\sigma_n^2$ are set to $-65$ dBm and $-80$ dBm, respectively. The rate of the transmitted codewords $R_B$ is set to $3.4594$ bps/Hz which corresponds to a received SNR of $10$ dB for Bob. The rate of the confidential information $R_s$ is set to be smaller than $R_B$, e.g., $1$ bps/Hz as used in [18]. The density of Eves is set to $1 \times 10^{-4}$ which means 100 Eves in $1000 \times 1000$ m$^2$. Finally, the radius of the UCA is set to $[0.4\lambda, 2\lambda]$ which corresponds to $[5, 25]$ cm for $2.4$ GHz frequency. For comparison, a commercial uniform circular array FCI-3710 developed by Fidelity Comtech has $15.24$ cm radius [29]. The simulation and numerical results plotted in Fig. 7 show a good match between them, which verifies the validity of the expressions in (10).

Secondly, a wider range of $K$ and $\beta$ for Rician channel will be examined. We choose typical value of $\beta = 3, 5$ and $K = 1, 10$. The results of $\bar{p}$ is calculated according to (32). As shown in Fig. 8, all curves exhibit similar trend with regard to $R$ to the curve in Fig. 6 where $K \rightarrow \infty$ and $\beta = 2$. In addition, for both curves in Fig. 8, the optimum value $R_{opt}$ in the range $R \in [0.4\lambda, 2\lambda]$ is $1.76\lambda$. It means that the optimum value of $R$ in a certain range is valid for Rician channels with different $K$ and $\beta$.

B. Numerical Results of the Upper Bounds

Next, closed-form expressions of $\bar{p}_{up}$ and $\tilde{p}_{up}$ are derived in Section III-A and Section IV-B, respectively, in order to facilitate analysis. Here, some numerical results are shown to demonstrate that the upper bounds can reflect the fluctuating behavior of $\bar{p}$ and $\tilde{p}$ against $R$.

In Fig. 9, the results for $\bar{p}$ and $\tilde{p}_{up}$ versus $R$ are shown for typical values of $\beta = 3$ and $K = 1, 10$. It can be seen that the curves of $\tilde{p}_{up}$ have a similar shape to the curves of $\bar{p}$, and the value of $\tilde{p}_{up}$ is close to $\bar{p}_{up}$. This suggests that the upper bound can very well reflect the property of $\bar{p}$.

In Fig. 10, the results for $\bar{p}$ and $\tilde{p}_{up}$ versus $R$ are shown for typical values of $\beta = 3$ and $K = 1, 10$. It can be seen that the curves for $\bar{p}$ and $\tilde{p}_{up}$ have a similar shape, and the values of $\bar{p}$ and $\tilde{p}_{up}$ are close to each other, which means that $\tilde{p}_{up}$ is a good upper bound.

C. Impact of Mutual Coupling

The mutual coupling is caused by energy absorption between proximate antennas and causes distortion to the array factor $G(\theta, \theta_B)$, and thus affects $\bar{p}$ and the optimization algorithm. In this paper, we choose the NEC tool [26] to build a numerical model as an example to examine the impact of the mutual coupling, although any analytical model will apply. The NEC tool serves as a numerical method to calculate array patterns that include the mutual coupling effect, and its results are well accepted in the literature [30], [31].

An example shown in Fig. 11 illustrates the difference caused by the mutual coupling for system configurations with $N = 8$, $R = 0.8\lambda$, $\theta_B = 0^\circ$. The array pattern with the mutual
patterns is calculated and the results are shown in Fig. 12. It can be seen that $\rho$ is generally above 0.8 in the range of $R = [0.4\lambda, 2\lambda]$, except for $R = 0.48\lambda$. This shows that the mutual coupling does not cause a significant distortion to the pattern of UCA. The high correlation between the theoretical and NEC patterns indicates that the optimization algorithm, which is based on empirical results on the theoretical patterns, can still work when considering the mutual coupling.

On the other hand, there exists some differences between the theoretical and NEC patterns, which means that when calculating $R_{\text{opt}}$ in the numerical implementation of the optimization algorithm, the NEC simulation data instead of the theoretical data should be used. To compare with Fig. 5, the same array parameters are adopted, i.e., $N = 8$ and $R \in [0.4\lambda, 2\lambda]$, and $\bar{p}$ with the mutual coupling is calculated based on the NEC simulation data. The results are shown in the upper plot in Fig. 13. Compared to Fig. 5, it is not hard to notice the similarity between the theoretical and NEC simulated curves for the same $\theta_B$, which can be explained by the high correlation between them, as shown in Fig. 12.

Because of the differences between the theoretical and NEC simulated results, $\bar{p}$ in Fig. 6 needs to be re-calculated based on the NEC simulation data, in order to find $R_{\text{opt}}$. The lower plot in Fig. 13 shows $\bar{p}$ based on the NEC simulation data in comparison with the theoretical curve. It can be seen that the optimum value for the NEC simulation data is $R_{\text{opt}} = 1.6\lambda$ compared to $R_{\text{opt}} = 1.76\lambda$ for the theoretical result. By choosing $R_{\text{opt}} = 1.6\lambda$, the value of $\bar{p}$ is reduced dramatically by about 59% compared to the maximum value of $\bar{p}$ at $R = 0.4\lambda$.

VI. Conclusions

This paper investigated the security performance of ER-based beamforming system with the UCA in the presence of PPP distributed Eves in Rician fading channel. With the aid of the expression of the averaged SSOP and the closed-form
expression of its upper bound, an optimization algorithm with regard to the radius was developed to minimize the SSOP. This paper provides a mathematical relationship which allows the radius to be optimized for a given UCA with a certain number of elements. The optimization algorithm is still valid for mutual coupling in practice, however, the optimum value needs to be calculated based on the NEC simulation data. In this work, it is assumed that Bob’s location is known by Alice beforehand. In practice, there could be inaccuracy in Bob’s location information at Alice, whether Bob sends his location to Alice or Alice estimates Bob’s location. In future work, it can be extended to include the impact of error in Bob’s location when optimizing the array parameters in practice. We will also extend our work considering random locations of Bob.

**APPENDIX A**

**CONVERSION OF OPTIMIZATION PROBLEM**

Because $\theta_B \sim \mathcal{U}(0, 2\pi)$, $\text{err}(R)$ can be calculated by

$$\text{err}(R) = \frac{1}{2\pi} \int_0^{2\pi} (\tilde{p} - \bar{p}_{\text{min}}) \, d\theta_B. \quad (36)$$

To find the minimum value of $\text{err}(R)$, the zeros of the partial derivative of $\text{err}(R)$ with respect to $R$ are calculated,

$$\frac{\partial}{\partial R} \text{err}(R) = 0 \Rightarrow \frac{1}{2\pi} \int_0^{2\pi} (\tilde{p} - \bar{p}_{\text{min}}) \, d\theta_B = 0 \Rightarrow \frac{1}{2\pi} \int_0^{2\pi} \left( \frac{\partial}{\partial R} \tilde{p} - \frac{\partial}{\partial R} \bar{p}_{\text{min}} \right) \, d\theta_B = 0. \quad (39)$$

Because $\bar{p}_{\text{min}}$ is a fixed value for certain $\theta_B$ and only depends on $\theta_B$, the partial derivative $\frac{\partial}{\partial R} \bar{p}_{\text{min}} = 0$. Thus, it can be derived that

$$\frac{\partial}{\partial R} \text{err}(R) = 0 \Rightarrow \frac{1}{2\pi} \int_0^{2\pi} (\tilde{p} - \bar{p}_{\text{min}}) \, d\theta_B = 0 \Rightarrow \frac{1}{2\pi} \int_0^{2\pi} \left( \frac{\partial}{\partial R} \tilde{p} + \frac{\partial}{\partial R} \bar{p}_{\text{min}} \right) \, d\theta_B = 0. \quad (39)$$

Using (46) and (47), it can be derived that

$$1 - \mathbb{E}_{\theta_B} \left[ \exp \left\{ -\lambda_c \pi \left[ \frac{c_0 K}{2\pi (K+1)} A_0 \right]^{\frac{\theta}{2}} \right\} \right] \leq \mathbb{E}_{\theta_B} \left[ \exp \left\{ -\lambda_c \pi \left[ \frac{c_0 K}{2\pi (K+1)} A_0 \right]^{\frac{\theta}{2}} \right\} \right]. \quad (48)$$

Using (46) and (47), it can be derived that

$$1 - \mathbb{E}_{\theta_B} \left[ \exp \left\{ -\lambda_c \pi \left[ \frac{c_0 K}{2\pi (K+1)} A_0 \right]^{\frac{\theta}{2}} \right\} \right] \leq \mathbb{E}_{\theta_B} \left[ \exp \left\{ -\lambda_c \pi \left[ \frac{c_0 K}{2\pi (K+1)} A_0 \right]^{\frac{\theta}{2}} \right\} \right]. \quad (49)$$

The equality in (50) does not hold because $\theta_B$ is random in this case. Then, $\bar{p}_{up}$ can be obtained by

$$\bar{p}_{up} = 1 - \exp \left\{ -\lambda_c \pi \left[ \frac{c_0 K A_0}{2\pi (K+1)} + \frac{c_0}{K+1} \right]^{\frac{\theta}{2}} \right\}. \quad (52)$$

where $A_0$ is the expectation of $A_0$ over $\theta_B$ and is given by

$$A_0 = \mathbb{E}_{\theta_B} [A_0] = \frac{1}{2\pi} \int_0^{2\pi} A_0 \, d\theta_B. \quad (53)$$
The above equation can be calculated from (26) by directly solving the integral. Because

\[
\int_{0}^{2\pi} e^{jN\theta} d\theta = 0, \quad \text{for } l \neq 0 \tag{54}
\]

it can be obtained that

\[
\bar{A}_0 = 2\pi \sum_{n=0}^{N-1} J_0^2(2kR\sin\left(\frac{n}{N}\pi\right)). \tag{55}
\]

REFERENCES