Article:
Zhang, Yuanrui, Woods, Roger, Ko, Youngwook et al. (2 more authors) (2018) Security optimisation of exposure region-based beamforming with a uniform circular array. IEEE Transactions on Communications. pp. 2630-2641. ISSN 0090-6778

https://doi.org/10.1109/TCOMM.2017.2768516

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' channel quality and can be achieved by exploiting the channel state information (CSI) [8] or the location information [9].

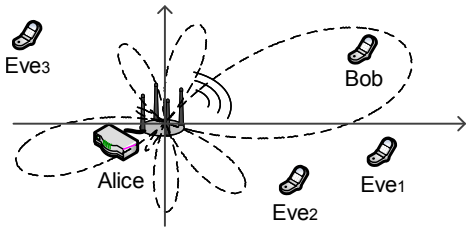

Fig. 1. The enclosed area surrounding Bob illustrates the ER created using a circular antenna array

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 Eves 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

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, jzhang20}@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)

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 a numerical simulation tool, i.e., NEC [26]. In essence, this sets the scene for setting secure regions in wireless networks. The main contributions of this paper are:

- Deriving the expression of the SSOP for the UCA and the closed-form expression of its upper bound for the first time, thus revealing the relationship between the security performance and various parameters, especially the radius of the UCA.
- Based on the expressions of the SSOP for the UCA, the first investigation of the security performance of ER-based beamforming for a Rician fading channel with respect to radius is presented. Simulation and numerical results are covered, which show how the behavior of averaged SSOP varies with the radius.
- An optimization algorithm is derived based on the above analysis, which enhances the security level by optimizing the radius for all of Bob's possible angles. The impact of the mutual coupling with the radius is compared with 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 $z = (d, \theta)$, and subscripts $_B$ and $_{Ei}$ 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, Φ_e with density λ_e [27].

On the transmitter side, the UCA has N elements and radius R, and the array vector of UCA is $\mathbf{s}(\theta) = [e^{-j\phi_1(\theta)}, ..., e^{-j\phi_i(\theta)}, ..., e^{-j\phi_N(\theta)}]^T$, $\theta \in [0, 2\pi]$, 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 λ is the wavelength of the carrier signal. P_t is the transmit power. Given Bob's location information, θ_B, the beamforming weight vector can be set as $\mathbf{w} = \mathbf{s}(\theta_B)/\sqrt{N}$.

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

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

where $d^{-\beta/2}$ denotes the large-scale path loss with the path loss exponent β of typical values between 2 and 6. The line-of-sight (LOS) component is $\sqrt{\frac{K}{K+1}}\mathbf{s}(\theta)$; the non-LOS component is $\sqrt{\frac{1}{K+1}}\mathbf{g}$, where $\mathbf{g} = [g_1, ..., g_i, ..., g_N]^T$, $g_i \sim \mathcal{CN}(0, 1)$, and the elements of $\mathbf{g}$ are independent. Thus, the received signal at z is the sum of the beamforming weighted signals and noise, which can be expressed by $r(z) = \sqrt{P_t}\mathbf{h}^T(z)\mathbf{w}^* x + n_W$, where x is the modulated symbol with unit power and n_W is the additive white Gaussian noise with zero mean and variance σ_n^2.

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

$$\tilde{h} = \mathbf{h}^T(z)\mathbf{w}^* = \sqrt{\frac{K}{K+1}}G(\theta, \theta_B) + \sqrt{\frac{1}{K+1}}g, \qquad (2)$$

where $G(\theta,\theta_B)=\mathbf{s}(\theta)\mathbf{s}^*(\theta_B)/\sqrt{N}$ is an array factor for any array type and $g\sim\mathcal{CN}(0,1)$. According to (2), $|\tilde{h}|^2$ can be decomposed as follows:

$$|\tilde{h}|^2=\frac{KG^2(\theta,\theta_B)}{K+1}+\frac{g_{Re}^2+g_{Im}^2}{K+1}+\frac{2\sqrt{K}G(\theta,\theta_B)}{K+1}g_{Re}, \tag{3}$$

where g_{Re} and g_{Im} are the real and imaginary part of g, so, $g_{Re},g_{Im}\sim\mathcal{N}(0,\frac{1}{2})$. For the UCA, the array factor was derived in [28] and is given by

$$G(\theta,\theta_B)=\frac{1}{\sqrt{N}}\sum_{i=1}^{N}e^{jkR[\cos(\theta_B-\psi_i)-\cos(\theta-\psi_i)]}. \tag{4}$$

The channel capacity, denoted by $C(z)$, is given by

$$C(z)=\log_2\Big(1+\frac{P_t|\tilde{h}|^2}{\sigma_n^2 d^\beta}\Big). \tag{5}$$

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 hereinafter. 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 Θ, 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 $D(\theta)=(c_0P_t|\tilde{h}|^2)^{1/\beta}$, where $c_0=[\sigma_n^2(2^{R_B-R_S}-1)]^{-1}$ 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 Θ. For PPP-distributed Eves, the probability of m Eves being inside $D(\theta)$ can be given by [27]

$$\text{Prob}\{m\text{ Eves in }\Theta\}=\frac{(\lambda_eA)^m}{m!}e^{-\lambda_eA}. \tag{6}$$

Thus, the SSOP, denoted by p, can be defined by the probability that any Eve is located inside $D(\theta)$.

$$p=1-\text{Prob}\{0\text{ Eve in }\Theta\}=1-e^{-\lambda_eA}. \tag{7}$$

Note that p is computed by the complementary of the probability that no Eve is inside Θ. In polar coordinates, (7) can be derived by

$$p=1-\exp\Big[-\frac{\lambda_e}{2}c_0^{\frac{2}{\beta}}P_t^{\frac{2}{\beta}}\int_0^{2\pi}(|\tilde{h}|^2)^{\frac{2}{\beta}}\,\mathrm{d}\theta\Big]. \tag{8}$$

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 $\bar{p}$,

$$\bar{p}=\mathbb{E}_{|\tilde{h}|}[p]. \tag{9}$$

The term $\bar{p}$ in (9) can be expressed by

$$\begin{aligned}\bar{p}=1-\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\exp\Big\{-\frac{\lambda_e}{2}c_0^{\frac{2}{\beta}}P_t^{\frac{2}{\beta}}\int_0^{2\pi}\Big[\frac{KG^2(\theta,\theta_B)}{K+1}\\+\frac{x^2+y^2}{K+1}+\frac{2\sqrt{K}G(\theta,\theta_B)}{K+1}x\Big]^{\frac{2}{\beta}}\,\mathrm{d}\theta\Big\}\frac{e^{-(x^2+y^2)}}{\pi}\,\mathrm{d}x\,\mathrm{d}y,\end{aligned} \tag{10}$$

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 $\bar{p}$. To this end, $\bar{p}$ is first analyzed against the factors in (10). Assume that the noise variance σ_n^2, channel factors β and K, the security related parameters R_B and R_s and the density of Eves λ_e are fixed. The remaining factors are the transmit power P_t, the array factor $G(\theta,\theta_B)$ and Bob's location (d_B,θ_B). Thus, an optimization problem can be expressed by

$$\min\bar{p}\text{ s.t. for all }d_B,\theta_B \tag{11}$$

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,θ_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 θ_B. As the number of antennas N is normally fixed for a certain UCA, the impact of R will be mainly discussed against θ_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 θ_B. An example of $G(\theta,\theta_B)$ with $\theta_B=0,\frac{\pi}{4}$ 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 $\theta_B=\frac{\pi}{4}$ can be obtained by shifting the shape for $\theta_B=0$ $by\frac{\pi}{4}$, and vice versa. At the same time, the two shapes are symmetric regarding to $\theta_B=\frac{\pi}{8}$. In general, $G(\theta,\theta_B)$ at $\pm(\theta_B\pm2\pi/N)$ are of the same shape. Therefore, it suffices to study $G(\theta,\theta_B)$ only in $\theta_B\in[0,\frac{\pi}{N}]$ instead of $[0,2\pi]$.

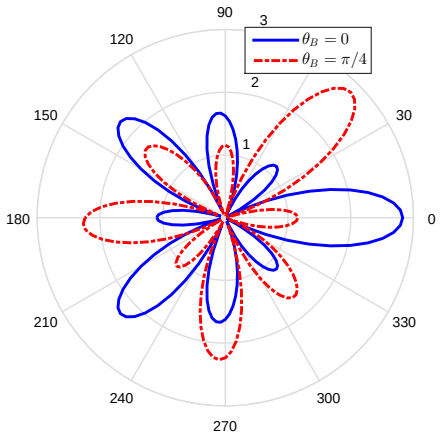

Fig. 2. $G(\theta, \theta_B)$ for $\theta_B = 0$ and $\theta_B = \frac{\pi}{4}$. $N = 8$ and $R = 0.8\lambda$.

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 λ_e and K, $\bar{p}_{up}$ can be derived using Jensen's inequality.

$$\bar{p}_{up} = 1 - \exp\Big\{ -\lambda_e \pi \Big[c_0 P_t \frac{K A_0 + 2\pi}{2\pi(K+1)} \Big]^{\frac{2}{\beta}} \Big\}, \tag{12}$$

where A_0 denotes the pattern area and is given by,

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

The derivation is described in [19]. According to (12), $\bar{p}_{up}$ is monotonically increasing with A_0 for any K and β. 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 θ to solve the integral in (4).

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

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

$$\begin{aligned} &\cos(\theta - \psi_i) - \cos(\theta - \psi_j) \\ =&2 \sin(\theta - \frac{i+j-2}{N}\pi) \sin(\frac{i-j}{N}\pi). \end{aligned} \tag{15}$$

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

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

According to $J_n(x) = \frac{1}{2\pi} \int_{-\pi}^{\pi} e^{j(n\tau - x\sin\tau)} \mathrm{d}\tau$, where $J_n(x)$ is the Bessel function of the first kind with order n, the following integration can be derived.

$$\begin{aligned} &\int_0^{2\pi} e^{-jkRW_{i,j} \sin(\theta - Z_{i,j})}\, \mathrm{d}\theta \\ =&\int_{-Z_{i,j}}^{2\pi - Z_{i,j}} e^{j[0\cdot\tau - kRW_{i,j}\sin\tau]}\, \mathrm{d}(\tau + Z_{i,j}) \\ =&\int_{-\pi}^{\pi} e^{j[0\cdot\theta - kRW_{i,j}\sin\tau]}\, \mathrm{d}\tau \\ =&2\pi J_0(kRW_{i,j}) \end{aligned} \tag{17}$$

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

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

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

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),

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

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 $A_{i,j}$ for i, j from 1 to N, the summation can now be executed diagonally. For convenience, let $n = i - j$. Then, $W_n = W_{i,j} = 2\sin(\frac{n}{N}\pi)$. The terms $A_{0,i,j}$ on the red diagonal lines in the table have the same W_n. In the table, $\frac{N}{\pi} Z_{i,j}$ is allocated according to their indices i and j. Given $n = i - j$, it can be derived that

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

Thus, it can be derived that

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

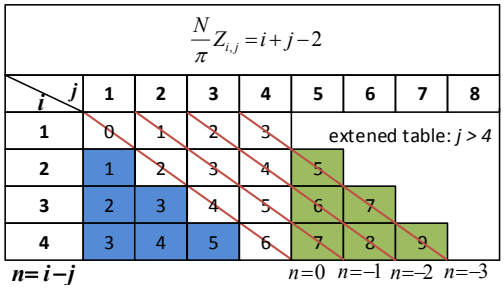

Fig. 3. Table for $Z_{i,j}$, $N = 4$.

A_0 is the summation of all elements in the original table (i.e., $i, j = 1, ..., 4$). Because $A_{0,i,j+N} = A_{0,i,j}$, the calculation of A_0 can be executed by replacing the lower triangle in the original table (i.e., $i > j$) with the lower triangle in the extended table (i.e., $i > j - N$). In the new formation of A_0, which is a parallelogram table, the summation can be carried out along the diagonal lines from $n = 0$ to $n = -(N-1)$. For any n, the summation of $A_{0,n,i}$ includes N terms with $Z_{n,i}$. Thus, (18) can be converted into

$$\begin{aligned} A_0 &= \sum_{i=1}^{N}\sum_{j=1}^{N} A_{0,i,j} = \sum_{n=0}^{-(N-1)}\sum_{i=1}^{N} A_{0,n,i} \\ &= \sum_{n=0}^{-(N-1)}\sum_{i=1}^{N} \frac{2\pi}{N} J_0(kRW_n) e^{jkRW_n \sin(\theta_B - Z_{n,i})} \\ &= \frac{2\pi}{N} \sum_{n=0}^{-(N-1)} J_0(kRW_n) \sum_{i=1}^{N} e^{jkRW_n \sin(\theta_B - Z_{n,i})}. \end{aligned} \quad (22)$$

According to Jacobi-Anger expansion $e^{j\alpha \sin\gamma} = \sum_{m=-\infty}^{\infty} J_m(\alpha) e^{jm\gamma}$, (22) can be further derived by (23) at the top of the following page.

When $m = lN$, $l \in \mathbb{Z}$, $e^{j\pi \frac{m}{N}(n+2)} = e^{jln\pi} e^{j2\pi l} = e^{jln\pi}$ and

$$\sum_{i=1}^{N} e^{-j2\pi \frac{m}{N} i} = \sum_{i=1}^{N} e^{-j2\pi li} = N. \quad (24)$$

When $m \neq lN$,

$$\sum_{i=1}^{N} e^{-j2\pi \frac{m}{N} i} = e^{-j2\pi \frac{m}{N}} \frac{1 - e^{-j2\pi \frac{m}{N} N}}{1 - e^{-j2\pi \frac{m}{N}}} = 0. \quad (25)$$

Thus, it can be derived that

$$\begin{aligned} A_0 &= \frac{2\pi}{N} \sum_{n=0}^{-(N-1)} J_0(kRW_n) \sum_{l=-\infty}^{\infty} J_{lN}(kRW_n) e^{jlN\theta_B} e^{jln\pi} N \\ &= 2\pi \sum_{n=0}^{-(N-1)} J_0(kRW_n) \sum_{l=-\infty}^{\infty} J_{lN}(kRW_n) e^{jlN\theta_B} (-1)^{ln} \\ &= 2\pi \sum_{n=0}^{N-1} J_0(-kRW_n) \sum_{l=-\infty}^{\infty} (-1)^{-ln} J_{lN}(-kRW_n) e^{jlN\theta_B} \\ &= 2\pi \sum_{n=0}^{N-1} J_0(kRW_n) \sum_{l=-\infty}^{\infty} (-1)^{ln+lN} J_{lN}(kRW_n) e^{jlN\theta_B}. \end{aligned} \quad (26)$$

Substituting (26) in (13), the closed-form expression for $\bar{p}_{up}$ 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 $J_{lN}(\cdot)$, which can provide asymptotic analysis.

B. Impact of R 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 $J_{lN}(x)$ 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 $J_{lN}(x)$ 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 $J_{lN}(x)$ for $l \geq 1$ are negligible in the range $(0, 2kR]$. Thus, for sufficiently large N, A_0 in (26) can be approximated by

$$A_0 \approx 2\pi \sum_{n=0}^{N-1} J_0^2(kRW_n). \quad (27)$$

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 $J_0(0)$ 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 angle θ_B is neglected. When N is not large enough, the term $J_{lN}(kRW_n)e^{jlN\theta_B}$ 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 $J_{lN}(kRW_n)$, there are some fluctuations.

An example of A_0 versus R is shown in the lower plot in Fig. 4 where $N = 8$ and $\theta_B = 0°$. It can be seen that A_0 fluctuates as R increases, because the curve is a superposition of $J_{lN}(kRW_n)$ 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. Optimization Algorithm

A. Refined Optimization Problem

As mentioned in Section III-B, R can be properly designed according to θ_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 $\bar{p}$. Thus, the optimization problem can be solved by optimizing R according to θ_B.

It is worth noticing that although the closed-form expression of $\bar{p}_{up}$ 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 $\bar{p}$ in (10), we will use numerical results to determine this.

Examples of $\bar{p}$ versus R for different θ_B are shown in Fig. 5 where $N = 8$. For simplicity, let $K \to \infty$ and $\beta = 2$, i.e., the

$$
\begin{aligned}
A_0 &= \frac{2\pi}{N}\sum_{n=0}^{-(N-1)} J_0(kRW_n)\sum_{i=1}^{N}\sum_{m=-\infty}^{\infty} J_m(kRW_n)e^{jm(\theta_B - Z_{n,i})} \\
&= \frac{2\pi}{N}\sum_{n=0}^{-(N-1)} J_0(kRW_n)\sum_{m=-\infty}^{\infty} J_m(kRW_n)e^{jm\theta_B}\sum_{i=1}^{N} e^{-jmZ_{n,i}} \\
&= \frac{2\pi}{N}\sum_{n=0}^{-(N-1)} J_0(kRW_n)\sum_{m=-\infty}^{\infty} J_m(kRW_n)e^{jm\theta_B}e^{j\pi\frac{m}{N}(n+2)}\sum_{i=1}^{N} e^{-j2\pi\frac{m}{N}i}.
\end{aligned} \tag{23}
$$

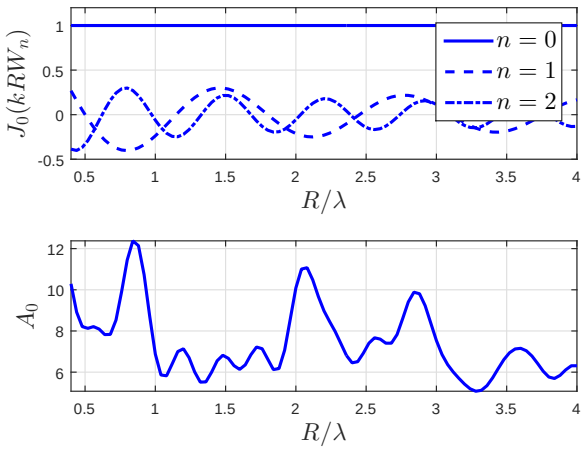

Fig. 4. Upper plot: Examples of $J_0(kRW_n)$ versus R. Lower plot: A_0 versus R. $N = 8$, $\theta_B = 0°$.

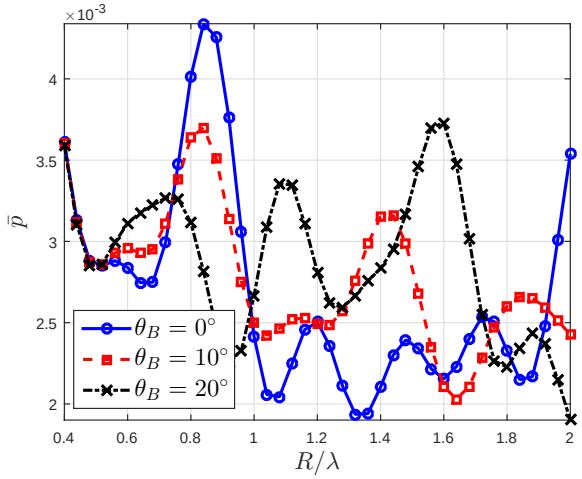

Fig. 5. $\bar{p}$ versus R for different values of θ_B, $N = 8$, $P_t/\sigma_n^2 = 15$ dB, $R_B = 3.4594$ bps/Hz, $R_s = 1$ bps/Hz, $\lambda_e = 1 \times 10^{-4}$.

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 θ_B, i.e., $\theta_B = 0°$, $10°$, $20°$, 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 θ_B. It can be seen that the curves for different θ_B vary. Therefore, for each θ_B, the local minimum of $\bar{p}$ in the range $R \in [0.4\lambda, 2\lambda]$ is given by a different value of R. This suggests that by varying θ_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_{opt} needs to pre-designed. To this end, the minimum mean error is used to find R_{opt} in a certain range of R that produces the minimum $\bar{p}$ for all possible $\theta_B \sim \mathcal{U}(0, 2\pi)$. To establish the cost function, imagine that R is adjustable, which provides the hypothetical function of $\bar{p}_{\min}$ with respect to θ_B. Notice that the value of $\bar{p}_{\min}$ for each θ_B is, in fact, given by a different value of R. To find R_{opt}, let the mean error, denoted by $\mathrm{err}(R)$, be the mean value of the difference between $\bar{p}$ and $\bar{p}_{\min}$ over the range $\theta_B \in [0, 2\pi]$,

$$\mathrm{err}(R) = \mathbb{E}_{\theta_B}[\bar{p} - \bar{p}_{\min}]. \tag{28}$$

Note that the mean error is used instead of the mean square error because $\bar{p} - \bar{p}_{\min}$ is always non-negative. Thus, R_{opt} can be found by

$$R_{opt} = \arg\min_R \mathrm{err}(R). \tag{29}$$

(29) can be converted into the following expression, the derivation of which is in Appendix A.

$$R_{opt} = \arg\min_R \bar{\bar{p}}, \tag{30}$$

where $\bar{\bar{p}}$ is the averaged $\bar{p}$ over Bob's angles and is defined by

$$\bar{\bar{p}} = \frac{1}{2\pi}\int_0^{2\pi} \bar{p}\,\mathrm{d}\theta_B. \tag{31}$$

B. Analysis and Implementation of Optimization Algorithm

Substituting the expression of $\bar{p}$ in (10) into (31), the expression of $\bar{\bar{p}}$ can be obtained,

$$
\begin{aligned}
\bar{\bar{p}} = 1 - \frac{1}{2\pi}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_0^{2\pi} &\exp\Big\{-\frac{\lambda_e}{2}(c_0P_t)^{\frac{2}{\beta}} \\
&\int_0^{2\pi}\Big[\frac{KG_C^2(\theta,\theta_B)}{K+1} + \frac{x^2+y^2}{K+1} + \frac{2\sqrt{K}G_C(\theta,\theta_B)}{K+1}x\Big]^{\frac{2}{\beta}}\mathrm{d}\theta\Big\} \\
&\frac{e^{-(x^2+y^2)}}{\pi}\,\mathrm{d}\theta_B\,\mathrm{d}x\,\mathrm{d}y.
\end{aligned} \tag{32}
$$

Although (32) can be numerically calculated, it is intractable to analyze. Thus, the upper bound, denoted by $\bar{\bar{p}}_{up}$, is required for theoretical analysis.

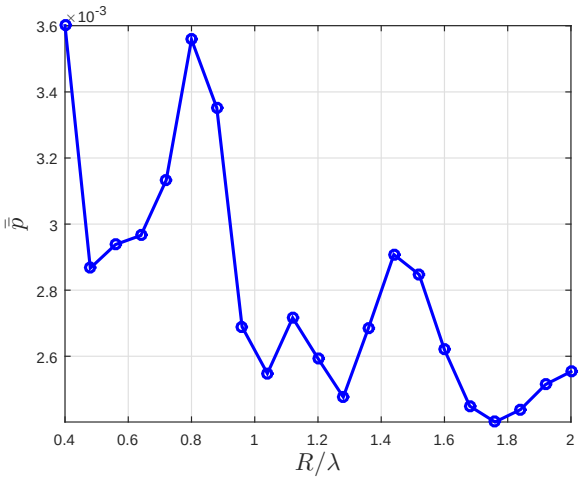

Fig. 6. $\bar{\bar{p}}$ versus R for all θ_B, $N = 8$, $P_t/\sigma_n^2 = 15\,\text{dB}$, $R_B = 3.4594\,\text{bps/Hz}$, $R_s = 1\,\text{bps/Hz}$, $\lambda_e = 1 \times 10^{-4}$.

Theorem 1:

$$\bar{\bar{p}}_{up} = 1 - \exp\Big\{ -\lambda_e \pi \Big[\frac{c_0 K \bar{A}_0}{2\pi(K+1)} + \frac{c_0}{K+1} \Big]^{\frac{2}{\beta}} \Big\}, \quad (33)$$

where $\bar{A}_0$ is the expectation of A_0 over θ_B and is given by

$$\bar{A}_0 = \frac{1}{2\pi} \int_0^{2\pi} A_0 \, \mathrm{d}\theta_B = 2\pi \sum_{n=0}^{N-1} J_0^2(kRW_n). \quad (34)$$

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, $\bar{A}_0$ in general decreases with some fluctuations as R increases. Due to the monotonically increasing relationship between $\bar{\bar{p}}_{up}$ and $\bar{A}_0$, it can be deduced that $\bar{\bar{p}}$ decreases in general with some fluctuations as R increases.

Because $\bar{\bar{p}}$ 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 $\bar{\bar{p}}$ 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 $\bar{\bar{p}}$ as 2.4×10^{-3}. Compared to the maximum value of $\bar{\bar{p}}$ that is 3.6×10^{-3} in the same range, there is a 33% reduction in the value of $\bar{\bar{p}}$. 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, θ_B, θ are discretized with steps of ΔR, $\Delta\theta_B$ and $\Delta\theta$, respectively. In addition, a limit value Q is used when calculating integral from $-\infty$ to ∞ in (32). For a normal distribution, a realistic value is set for Q, namely 3. Let N_R, N_{θ_B}, N_θ and N_Q be the number of samples for R, θ_B, θ 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 $\bar{\bar{p}}$ 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 $\bar{\bar{p}}_{\min}$ in the vector $\bar{\bar{p}}$ is searched to find R_{opt} which is the output of the optimization algorithm.

Algorithm 1 Optimization of R for fixed N

INPUT: σ_n^2, β, K, R_B, R_s, λ_e, λ, P_t, N
INPUT: R_1, R_2, ΔR; θ_{B1}, θ_{B2}, $\Delta\theta_B$; θ_1, θ_2, $\Delta\theta$; Q, ΔQ
OUTPUT: R_{opt}

1: discretize R, θ_B, θ, Q
2: calculate N_R, N_{θ_B}, N_θ, N_Q and c_0
3: create an $1 \times N_R$ empty vector of $\bar{\bar{p}}$ with index idx
4: **for** each value of $R \in [R_1, R_2]$, $\theta_B \in [\theta_{B1}, \theta_{B2}]$ **do**
5: $\quad S_1 = 0$
6: $\quad$ **for** each value of $x, y \in [-Q, Q]$ **do**
7: $\quad\quad S_2 = 0$
8: $\quad\quad$ **for** each value of $\theta \in [\theta_1, \theta_2]$ **do**
9: $\quad\quad\quad S_2 = S_2 +$
10: $\quad\quad\quad \Big[\frac{KG^2(\theta,\theta_B)+x^2+y^2+2\sqrt{K}G(\theta,\theta_B)x}{K+1}\Big]^{\frac{2}{\beta}} \Delta\theta$
11: $\quad\quad$ **end for**
12: $\quad\quad S_1 = S_1 + \exp\{-\frac{\lambda_e}{2}(P_t c_0)^{\frac{2}{\beta}} S_2\} \frac{e^{-(x^2+y^2)}}{\pi} \Delta Q^2$
13: $\quad$ **end for**
14: $\quad \bar{\bar{p}}(idx) = \bar{\bar{p}}(idx) + (1 - S_1)/N_{\theta_B}$
15: **end for**
16: initialization: $R_{opt} = R_1$, $\bar{\bar{p}}_{min} = \bar{\bar{p}}(1)$
17: **for** each value of $R \in [R_1, R_2]$ **do**
18: $\quad$ **if** $\bar{\bar{p}}_{min} > \bar{\bar{p}}(idx)$ **then**
19: $\quad\quad$ reassignment: $R_{opt} = R$, $\bar{\bar{p}}_{min} = \bar{\bar{p}}(idx)$
20: $\quad$ **end if**
21: **end for**

The accuracy of the result increases with number of samples; however, the compuational complexity also increases. The running time of the numerical implementation is approximately $\mathcal{O}(N_R N_{\theta_B} N_Q^2 N_\theta)$. There is no specific restriction on the sampling interval as long as the chosen resolution generates a reasonable value.

V. Simulation and Numerical Results

In this section, we first provide simulation results for $\bar{p}$ in (10) and then numerical results for $\bar{\bar{p}}$ in (32) over the Rician channel with a wider range of values of K and β. Next, the numerical results of the upper bounds $\bar{p}_{up}$ and $\bar{\bar{p}}_{up}$ are shown in comparison with $\bar{p}$ and $\bar{\bar{p}}$ 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 $|\tilde{h}^2|$ 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 1×10^4 samples of g_{Re} and g_{Im} in (3). As stated in Section II-C, the noise variance σ_n^2, channel factors β and

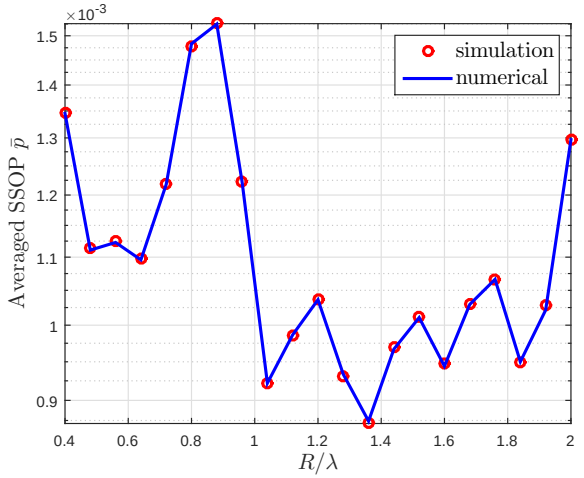

Fig. 7. Simulation and numerical results for $\bar{p}$ versus R; $K = 10$, $\beta = 3$, $\theta_B = 0°$ $P_t/\sigma_n^2 = 15$ dB, $R_B = 3.4594$ bps/Hz, $R_s = 1$ bps/Hz, $\lambda_e = 1 \times 10^{-4}$.

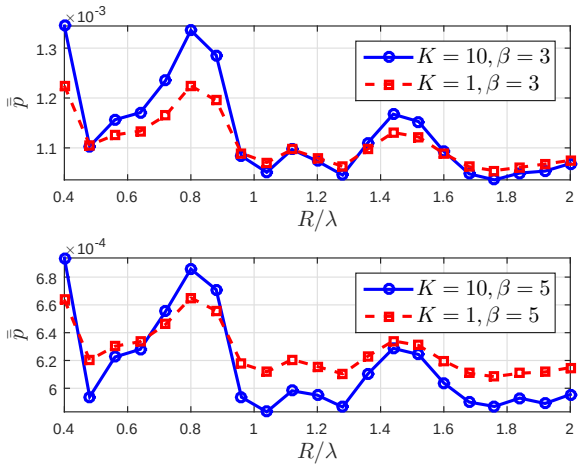

Fig. 8. Numerical results for $\bar{\bar{p}}$ versus R; $P_t/\sigma_n^2 = 15$ dB, $R_B = 3.4594$ bps/Hz, $R_s = 1$ bps/Hz, $\lambda_e = 1 \times 10^{-4}$.

K, the security related parameters R_B and R_s and the density of Eves λ_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 σ_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 1×10^{-4} which means 100 Eves in 1000×1000 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 β for Rician channel will be examined. We choose typical value of $\beta = 3, 5$ and $K = 1, 10$. The results of $\bar{\bar{p}}$ 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 $K \to \infty$ 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 1.76λ. It means that the optimum value of R in a certain range is valid for Rician channels with different K and β.

B. Numerical Results of the Upper Bounds

Next, closed-form expressions of $\bar{p}_{up}$ and $\bar{\bar{p}}_{up}$ 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 $\bar{\bar{p}}$ against R.

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

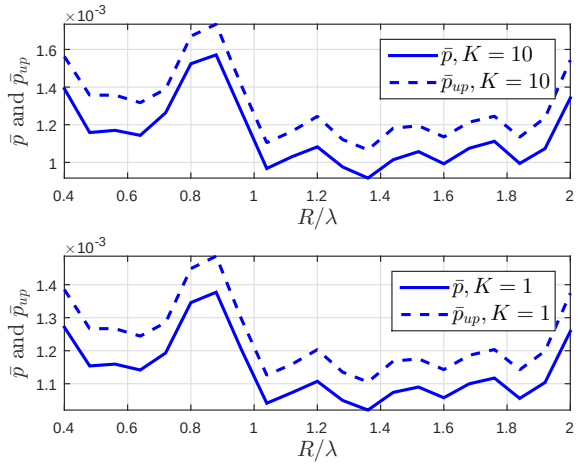

Fig. 9. Numerical results for $\bar{p}$ and $\bar{p}_{up}$ versus R; $\beta = 3$, $P_t/\sigma_n^2 = 15$ dB, $R_B = 3.4594$ bps/Hz, $R_s = 1$ bps/Hz, $\lambda_e = 1 \times 10^{-4}$.

In Fig. 10, the results for $\bar{\bar{p}}$ and $\bar{\bar{p}}_{up}$ versus R are shown for typical values of $\beta = 3$ and $K = 1, 10$. It can be seen that the curves for $\bar{\bar{p}}$ and $\bar{\bar{p}}_{up}$ have a similar shape, and the values of $\bar{\bar{p}}$ and $\bar{\bar{p}}_{up}$ are close to each other, which means that $\bar{\bar{p}}_{up}$ 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 $N = 8$, $R = 0.8\lambda$, $\theta_B = 0°$. The array pattern with the mutual

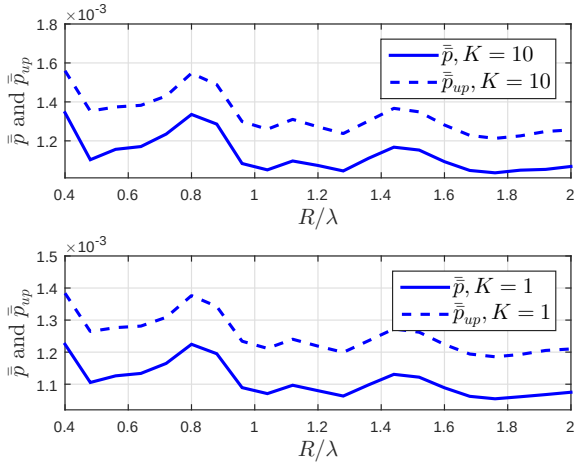

Fig. 10. Numerical results for $\bar{\bar{p}}$ and $\bar{\bar{p}}_{up}$ versus R; $\beta = 3$, $P_t/\sigma_n^2 = 15$ dB, $R_B = 3.4594$ bps/Hz, $R_s = 1$ bps/Hz, $\lambda_e = 1 \times 10^{-4}$.

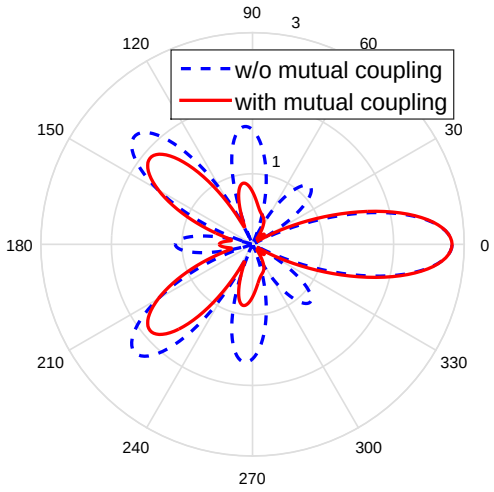

Fig. 11. Example of theoretical and NEC simulated patterns, $N = 8$, $R = 0.8\lambda$, $\theta_B = 0°$.

coupling is calculated by the NEC simulation. It can be seen that there is not much difference in the main beam, but with deviation in the sidelobes.

To measure the array pattern distortion caused by the mutual coupling, Pearson's correlation coefficient, denoted by ρ, is adopted. It measures the correlation between two variables X and Y, as defined by

$$\rho = \frac{cov(X, Y)}{std(X) \cdot std(Y)}, \tag{35}$$

where $cov(\cdot, \cdot)$ stands for the covariance and $std(\cdot)$ the standard deviation. ρ between the theoretical array pattern and the simulated array pattern via NEC tool can be calculated to quantify their similarity. The larger ρ is, the more alike two patterns are.

The patterns of the UCA with a range of radius are simulated in NEC. For $N = 8$, typical values are chosen, i.e., $\theta_B = 0°, 10°, 20°$ in the range $R = [0.4\lambda, 2\lambda]$. The correlation coefficient, ρ, between the theoretical and NEC

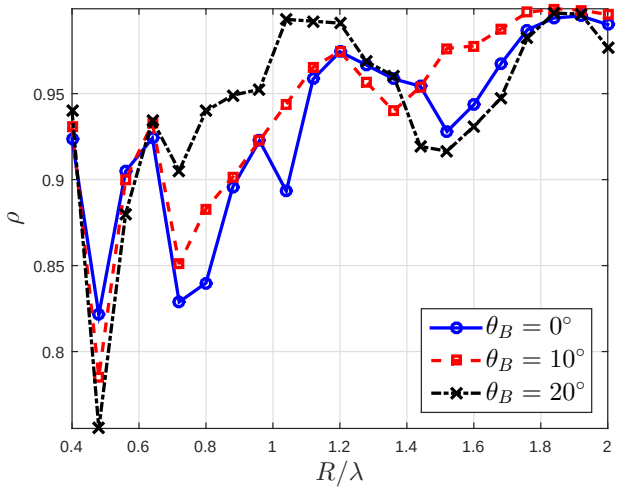

Fig. 12. Correlation coefficients between theoretical and NEC simulated patterns, $N = 8$, $P_t/\sigma_n^2 = 15$ dB, $R_B = 3.4594$ bps/Hz, $R_s = 1$ bps/Hz, $\lambda_e = 1 \times 10^{-4}$.

patterns is calculated and the results are shown in Fig. 12. It can be seen that ρ 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_{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 θ_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, $\bar{\bar{p}}$ in Fig. 6 needs to be re-calculated based on the NEC simulation data, in order to find R_{opt}. The lower plot in Fig. 13 shows $\bar{\bar{p}}$ 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 $R_{opt} = 1.6\lambda$ compared to $R_{opt} = 1.76\lambda$ for the theoretical result. By choosing $R_{opt} = 1.6\lambda$, the value of $\bar{\bar{p}}$ is reduced dramatically by about 59% compared to the maximum value of $\bar{\bar{p}}$ 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

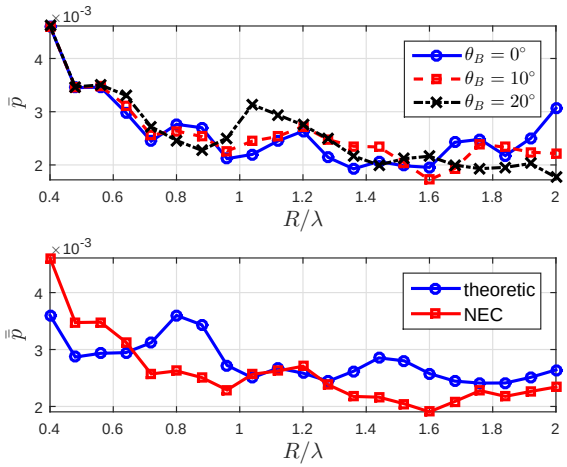

Fig. 13. Upper plot: $\bar{p}$ versus R. Lower plot: $\bar{\bar{p}}$ versus R. $N = 8$, $P_t/\sigma_n^2 = 15\,\text{dB}$, $R_B = 3.4594\,\text{bps/Hz}$, $R_s = 1\,\text{bps/Hz}$, $\lambda_e = 1 \times 10^{-4}$.

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

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

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,

$$\frac{\partial}{\partial R}\text{err}(R) = 0 \tag{37}$$
$$\Rightarrow \frac{\partial}{\partial R}\frac{1}{2\pi}\int_0^{2\pi} (\bar{p} - \bar{p}_{\min})\,\mathrm{d}\theta_B = 0 \tag{38}$$
$$\Rightarrow \frac{1}{2\pi}\int_0^{2\pi} (\frac{\partial}{\partial R}\bar{p} - \frac{\partial}{\partial R}\bar{p}_{\min})\,\mathrm{d}\theta_B = 0. \tag{39}$$

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

$$\frac{\partial}{\partial R}\text{err}(R) = 0 \tag{40}$$
$$\Rightarrow \frac{1}{2\pi}\int_0^{2\pi} \frac{\partial}{\partial R}\bar{p}\,\mathrm{d}\theta_B = 0 \tag{41}$$
$$\Rightarrow \frac{\partial}{\partial R}\frac{1}{2\pi}\int_0^{2\pi} \bar{p}\,\mathrm{d}\theta_B = 0 \tag{42}$$
$$\Rightarrow \frac{\partial}{\partial R}\bar{\bar{p}} = 0, \tag{43}$$

where $\bar{\bar{p}}$ is the averaged SSOP over Bob's angle and is defined by

$$\bar{\bar{p}} = \frac{1}{2\pi}\int_0^{2\pi} \bar{p}\,\mathrm{d}\theta_B. \tag{44}$$

Thus, we can obtain

$$R_{opt} = \arg\min_R \bar{\bar{p}}. \tag{45}$$

Appendix B
Proof of Theorem 1

To obtain the upper bound $\bar{\bar{p}}_{up}$, two instances of Jensen's inequality will be used to derive $\bar{p}_{up}$.

$$\mathbb{E}[e^X] \geq e^{\mathbb{E}[X]}, \tag{46}$$

where X is a random variable. The equality holds if and only if X is a deterministic value. The other one involved is expressed by

$$\mathbb{E}[X^{\frac{2}{\beta}}] \leq (\mathbb{E}[X])^{\frac{2}{\beta}}, \tag{47}$$

where X is a random variable and $\beta \geq 2$. The equality holds when $\beta = 2$ for any X.

The upper bound $\bar{\bar{p}}_{up}$ can be derived based on $\bar{p} \leq \bar{p}_{up}$. Using (12), it can be derived that

$$\begin{aligned}\bar{\bar{p}} &= \mathbb{E}_{\theta_B}[\bar{p}] \leq \mathbb{E}_{\theta_B}[\bar{p}_{up}] \\ &= 1 - \mathbb{E}_{\theta_B}\Big[\exp\Big\{-\lambda_e\pi\Big[\frac{c_0 K}{2\pi(K+1)}A_0 + \frac{c_0}{K+1}\Big]^{\frac{2}{\beta}}\Big\}\Big].\end{aligned} \tag{48}$$

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

$$1 - \mathbb{E}_{\theta_B}\Big[\exp\Big\{-\lambda_e\pi\Big[\frac{c_0 K}{2\pi(K+1)}A_0 + \frac{c_0}{K+1}\Big]^{\frac{2}{\beta}}\Big\}\Big] \tag{49}$$
$$< 1 - \exp\Big\{-\lambda_e\pi\mathbb{E}_{\theta_B}\Big[\Big[\frac{c_0 K}{2\pi(K+1)}A_0 + \frac{c_0}{K+1}\Big]^{\frac{2}{\beta}}\Big]\Big\} \tag{50}$$
$$\leq 1 - \exp\Big\{-\lambda_e\pi\Big[\frac{c_0 K}{2\pi(K+1)}\mathbb{E}_{\theta_B}[A_0] + \frac{c_0}{K+1}\Big]^{\frac{2}{\beta}}\Big\}. \tag{51}$$

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

$$\bar{\bar{p}}_{up} = 1 - \exp\Big\{-\lambda_e\pi\Big[\frac{c_0 K\bar{A}_0}{2\pi(K+1)} + \frac{c_0}{K+1}\Big]^{\frac{2}{\beta}}\Big\}, \tag{52}$$

where $\bar{A}_0$ is the expectation of A_0 over θ_B and is given by

$$\bar{A}_0 = \mathbb{E}_{\theta_B}[A_0] = \frac{1}{2\pi}\int_0^{2\pi} A_0\,\mathrm{d}\theta_B. \tag{53}$$

The above equation can be calculated from (26) by directly solving the integral. Because

$$\int_0^{2\pi} e^{jlN\theta_B}\,\mathrm{d}\theta_B = 0, \text{ for } l \neq 0 \tag{54}$$

it can be obtained that

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

REFERENCES

[1] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Third Quarter 2014.

[2] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347 – 376, First Quarter 2017.

[3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[4] J. Barros and M. R. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. on Inf. Theory*, Seattle, USA, Jul. 2006, pp. 356–360.

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

[6] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. on Inf. Theory*, Nice, France, Jun. 2007, pp. 2466–2470.

[7] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

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

[9] S. Yan and R. Malaney, "Location-based beamforming for enhancing secrecy in rician wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2780–2791, Apr. 2016.

[10] S. Lakshmanan, C. Tsao, and R. Sivakumar, "Aegis: Physical space security for wireless networks with smart antennas," *IEEE/ACM Trans. Netw.*, vol. 18, pp. 1105–1118, Aug. 2010.

[11] A. Sheth, S. Seshan, and D. Wetherall, "Geo-fencing: Confining Wi-Fi coverage to physical boundaries," in *Proc. IEEE 7th Int. Conf. on Pervasive Comput.*, Nara, Japan, May 2009, pp. 274–290.

[12] N. Anand, S.-J. Lee, and E. W. Knightly, "STROBE: Actively securing wireless communications using zero-forcing beamforming," in *Proc. IEEE 31th Annu. Int. Conf. on Comput. Commun.*, Orlando, FL, USA, Mar. 2012, pp. 720–728.

[13] T. Wang and Y. Yang, "Enhancing wireless communication privacy with artificial fading," in *Proc. IEEE 9th Int. Conf. on Mobile Adhoc and Sensor Systems*, Las Vegas, NV, USA, Oct. 2012, pp. 173–181.

[14] H. Li, X. Wang, and W. Hou, "Security enhancement in cooperative jamming using compromised secrecy region minimization," in *Proc. IEEE 13th Canadian Workshop on Inf. Theory*, Toronto, Canada, Jun. 2013, pp. 214–218.

[15] J. Wang, J. Lee, F. Wang, and T. Q. Quek, "Jamming-aided secure communication in massive MIMO Rician channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 6854–6868, Dec. 2015.

[16] S. Sarma, S. Shukla, and J. Kuri, "Joint scheduling & jamming for data secrecy in wireless networks," in *Proc. IEEE 11th Int. Symp. on Modeling & Optimization in Mobile, Ad Hoc & Wireless Networks*, Takezono, Japan, May 2013, pp. 248–255.

[17] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628–1631, Oct. 2012.

[18] T.-X. Zheng, H.-M. Wang, and Q. Yin, "On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers," *IEEE Commun. Lett.*, vol. 18, no. 8, pp. 1299–1302, Aug. 2014.

[19] Y. Zhang, Y. Ko, R. Woods, and A. Marshall, "Defining spatial security outage probability for exposure region based beamforming," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 900 – 912, Feb. 2017.

[20] B. Friedlander and A. J. Weiss, "Direction finding in the presence of mutual coupling," *IEEE Trans. Antennas Propag.*, vol. 39, pp. 273–284, Mar. 1991.

[21] J. Dai, X. Bao, N. Hu, C. Chang, and W. Xu, "A recursive RARE algorithm for DOA estimation with unknown mutual coupling," *IEEE Antennas Wireless Propag. Lett.*, vol. 13, pp. 1593–1596, Aug. 2014.

[22] Y. Zhang, B. Yin, R. Woods, J. Cavallaro, A. Marshall, and Y. Ko, "Investigation of secure wireless regions using configurable beamforming on WARP," in *Proc. IEEE 48th Asilomar Conf. on Signals, Syst. and Comput.*, Asilomar, USA, Nov. 2014, pp. 1979–1983.

[23] B. Allen and M. Ghavami, *Adaptive Array Systems: Fundamentals and Applications*. New Jersey, USA: John Wiley & Sons, 2006.

[24] 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.

[25] Y. Zhang, Y. Ko, R. Woods, A. Marshall, J. Cavallaro, and K. Li, "On spatial security outage probability derivation of exposure region based beamforming with randomly located eavesdroppers," in *Proc. IEEE 50th Asilomar Conf. on Signals, Syst. and Comput.*, Asilomar, USA, Nov. 2016, pp. 689–690.

[26] G. Burke and A. Poggio, "Numerical electromagnetic code (NEC) – Method of moments," Livermore, CA, USA, 1981.

[27] M. Ghogho and A. Swami, "Physical-layer secrecy of MIMO communications in the presence of a poisson random field of eavesdroppers," in *Proc. IEEE Int. Conf. on Commun.*, Kyoto, Japan, Jun. 2011, pp. 1–5.

[28] F. Gross, *Smart Antennas for Wireless Communications with MATLAB*. New York: McGraw-Hill, 2005.

[29] FCI-3710 Phased Array Antenna. Accessed on 25 Oct., 2017. [Online]. Available: http://www.fidelity-comtech.com/wp-content/uploads/SpecSheet_FCI-3710.pdf

[30] K. R. Dandekar, H. Ling, and G. Xu, "Effect of mutual coupling on direction finding in smart antenna applications," *Electron. Lett.*, vol. 36, pp. 1889–1891, Oct. 2000.

[31] H. Singh, H. Sneha, and R. Jha, "Mutual coupling in phased arrays: A review," *International Journal of Antennas and Propagation*, vol. 2013, 2013.