Secrecy Zone Achieved by Directional Modulation With Random Frequency Diverse Array

Shuaiyu Wang, Graduate Student Member, IEEE, Shihao Yan¹, Member, IEEE, Jia Zhang, Member, IEEE, Nan Yang, Senior Member, IEEE, Riqing Chen¹, Member, IEEE, and Feng Shu, Member, IEEE

Abstract—This work analyzes the impact of the transceivers’ relative locations on the security achieved by directional modulation with a random frequency diverse array (DM-RFDA). Based on the adopted path loss model, we first derive the probability of non-zero secrecy capacity, denoted by \( p_m \), achieved at a legitimate receiver for an eavesdropper with a fixed location. We then examine how far we need to push the eavesdropper away from the transmitter in order to guarantee \( p_m \geq \delta \), where \( \delta \) is a given value determining a certain level of security. The results reveal that the DM-RFDA system ensures a high level of security (e.g., \( \delta = 0.95 \)) for the legitimate user who is significantly further away from the transmitter than the eavesdropper. Furthermore, the results demonstrate that it is easier to guarantee the required level of security when there are more resources (e.g., higher bandwidth and a larger number of transmit antennas) in the DM-RFDA system.

Index Terms—Physical layer security, directional modulation, random frequency diverse array, path loss.

I. INTRODUCTION

Directional modulation (DM) has the capability of projecting wireless signals into a predetermined and desirable spatial direction, while simultaneously distorting the constellation of these signals in all other directions [1], [2]. Due to this capability, DM is desirable for conducting secure wireless communications [3], [4]. For example, [5] developed a novel and robust DM synthesis method for enhancing the system secrecy performance, where both artificial noise and angle estimation error were considered. Moreover, the secrecy rate achieved by DM with the aid of multiple techniques was examined in [6], where the wiretap region was clarified. Furthermore, [7] proposed a hybrid multiple-input multiple-output (MIMO) phase array (PA) time-modulated DM scheme for achieving physical layer security.

In the aforementioned studies [5]–[7], DM was used on PA antennas and the drawback of this DM-PA system lies in the fact that it can only ensure secure transmission in the angle dimension, i.e., the DM-PA system cannot guarantee a high level of secrecy if an eavesdropper (Eve) is on the same angle relative to a transmitter (Alice) as a legitimate receiver (Bob). Against this background, [8] proposed a novel DM scheme based on random frequency diverse array (RFDA) [9], [10], which randomly allocates varying frequencies to different transmit antennas and thus achieves 2-dimensional (i.e., angle and distance) secure transmission.

Due to its high potential in achieving communication security and privacy, the DM-RFDA system has been considered in various application scenarios, including unmanned aerial vehicle (UAV) networks [11] and wireless broadcasting systems [12]. Specifically, the frequency offsets, beamforming vector, and the artificial-noise projection matrix were optimized for a multi-beam DM-RFDA system in [13] to maximize the system secrecy capacity. In [14], an SVM-aided range-angle dependent DM scheme based on symmetrical multi-carrier FDA was proposed to achieve physical layer security and its performance and complexity priories relative to zero-forcing were examined. Furthermore, [15] and [16] analyzed the secrecy performance of FDA-based DM systems over Rayleigh fading channels and Nakagami-\( \eta \) fading channels [17], respectively. In addition, a DM-RFDA system was also used in unmanned aerial vehicle (UAV) networks to achieve simultaneous wireless information and power transfer [11].

Meanwhile, the concept of secrecy zone has been considered in the literature of physical layer security to characterize the secrecy performance of a system without Eve’s exact location information (e.g., [18]–[22]). In general, the analysis of the secrecy zone can benefit the system design in twofold, as follows: i) For a given boundary around Alice where Eve cannot locate inside, the analysis of the secrecy zone can help determine the maximum achievable secrecy performance of the system. ii) In order to guarantee a certain level of communication secrecy from Alice to Bob, the analysis of the secrecy zone can help identify the area (e.g., determined a minimum distance from Bob) that should be physically protected to avoid Eve moving inside. We note that a physical secrecy zone can be achieved by building fences around Alice in military scenarios, or surveillance conducted by scouts or using telescopes around Alice. Detailed analysis of the secrecy zone was presented in, e.g., [18]–[21]. For example, [18] established a secrecy zone by using traditional beamforming, which can guarantee secure transmission between transceivers (regardless whether they are inside or outside of the secrecy zone), as long as an eavesdropper is not located inside the secrecy zone. Moreover, [19] proposed to steer the information by beamforming and determine the size of the protected zone in resource-constrained scenarios to improve the security. Furthermore, [20] investigated how to enhance physical-layer security in random wireless networks with a secrecy protected zone surrounding the transmitter and an interference protected zone surrounding the legitimate receivers. In addition, [21] tackled additional secrecy enhancement with the secrecy protected zone in the presence of eavesdroppers and interferers with unknown locations.

It is noted that the path loss model (e.g., [23]) has never been considered in the context of physical layer security achieved by DM-RFDA systems, which leads to that the secrecy zone achieved by DM-RFDA systems has never been examined. Thus, the impact of the geometric
locations of Alice, Bob, and Eve on the achievable security has not been identified. As an initial step to characterize this impact, a question arises: “How far we need to push Eve away from Alice in order to guarantee a certain level of security on the wireless transmission from Alice to Bob?” To answer this question, in this work we first derive the probability of non-zero secrecy capacity, denoted by $p_n$, and the secrecy outage probability, denoted by $p_o$, achieved by a DM-RFDA system for a given location of Eve, based on which we evaluate the secrecy level of the transmission from Alice to Bob. Then, we determine the minimum distance from Alice to Eve in order to ensure $p_n \geq \delta$ or $p_o \leq \epsilon$ in the considered DM-RFDA system, where $\delta$ and $\epsilon$ are predetermined values to set the required secrecy level for the transmission from Alice to Bob. Our results show that the minimum distance can be significantly less than the distance from Alice to Bob (even for a high $\delta$, e.g., 0.95). This implies that by using a DM-RFDA system, it is feasible to transmit confidential information to a legitimate receiver who is further away from the transmitter than the eavesdropper. In addition, our results show that the minimum distance decreases when the number of transmit antennas and the available bandwidth increase.

II. SYSTEM MODEL

A. Random Frequency Diverse Array

We consider a system where the base station is equipped with a RFDA and uses random frequency across its antenna elements, as shown in Fig. 1. The frequency allocated to the $n$-th antenna element is given by

$$f_n = f_c + k_n \Delta f, \quad n = 0, 1, \ldots, N - 1,$$

(1)

where $f_c$ is the central carrier frequency, $\Delta f$ is the frequency increment, and $k_n$ is a random variable which determines the distribution of the frequency allocated to different antenna elements. We note that the values of $k_n$ are independent and identically distributed (i.i.d.). In this work, we consider a uniform linear array (ULA) at the transmitter and set the reference antenna element at the geometric center of the ULA. Then, the distance from the $n$-th antenna element to a receiver is denoted by $d_n$. In this work, we assume that Bob’s location is precisely known at Alice, while Eve’s location is unknown. We also assume that Eve cannot be in the vicinity of Bob, e.g., Eve is a few meters away from Bob [24]. Otherwise, she can be found by Bob and secure transmission is thus suspended. Under this assumption, Eve’s received signals are not enhanced by the DM-RFDA system. We note that when the receiver is far from the antenna array, $d_n$ is approximated as

$$d_n = d - b_n l \cos \theta, \quad n = 0, 1, \ldots, N - 1,$$

(2)

where $\theta$ and $d$ are the angle and distance from the geometric center of the ULA to the receiver, respectively, $l$ denotes the element space at the ULA, and $b_n$ is given by

$$b_n = n - \frac{N - 1}{2}.$$

(3)

The phase of the received signal from the $n$-th antenna element of the ULA is given by

$$\psi_n (\theta, d) = 2 \pi f_n \frac{d_n}{c} = \frac{2 \pi}{c} (f_c d - b_n f_c l \cos \theta + k_n \Delta f d - b_n k_n \Delta f l \cos \theta).$$

(4)

Then, the phase shift of the signal received from the $n$-th element relative to the signal received from the reference element is given by

$$\Psi_n (\theta, d) = \psi_n (\theta, d) - \psi_0 (\theta, d) = \frac{2 \pi}{c} (-b_n f_c l \cos \theta + k_n \Delta f d - b_n k_n \Delta f l \cos \theta).$$

(5)

We note that the term $k_n \Delta f d/c$ in (5) is of great importance, since it explicitly shows that the radiation pattern of the signal depends on both the distance and the frequency increment. Normally, the relationship between the frequency increment and the central carrier frequency can guarantee $N \Delta f \ll f_c$, and element spacing $l$ is close to the wavelength $\lambda$ (e.g., $l = \lambda/2$). As such, the last term in (5) is negligible and the phase shift defined in (5) is approximated as

$$\Psi_n (\theta, d) \approx \frac{2 \pi}{c} (-b_n f_c l \cos \theta + k_n \Delta f d).$$

(6)

Using the simplified path loss model, the steering vector of RFDA relative to a specific location $(\theta, d)$ is expressed as

$$h (\theta, d) = \sqrt{\frac{K (\frac{\gamma}{\gamma'})}{N}} [e^{j \psi_0 (\theta, d)}, e^{j \psi_1 (\theta, d)}, \ldots, e^{j \psi_{N-1} (\theta, d)}]^T,$$

(7)

where $K$ is a unitless constant that depends on the antenna characteristics and the average channel attenuation, $d_0$ is a reference distance for the far-field antenna, $\gamma$ is the path loss exponent, $[\cdot]^T$ denotes the transpose. In the following, we define $\rho (d) = K (\frac{\gamma}{\gamma'})$ for the sake of better presentation.

B. Directional Modulation

In the considered system, we assume that Bob’s location, denoted by $(\theta_B, d_B)$, is available at Alice, while Eve’s location, denoted by $(\theta_E, d_E)$, is unavailable at Alice. Considering transmit beamforming, the transmit signal is given by

$$s = \sqrt{P_s} x,$$

(8)

where $x$ is a symbol chosen from the complex signal constellation with an average power constraint, i.e., $\mathbb{E}[|x|^2] = 1$ and $\mathbb{E}[\cdot]$ denotes the expectation, $P_s$ is the transmit power at Alice, and $\nu$ is the normalized beamforming vector of the useful signal for expected users.
The effect of Eve’s location, in order to maximize the SNR at Bob, \( v \) is given by
\[
\nu = \frac{h(\theta_B, d_B)}{\sqrt{\rho(d_B)}},
\]  
where \( h(\theta_B, d_B) \) is the steering vector of the RFDA at Alice to Bob, which can be obtained by replacing \((\theta, d)\) with \((\theta_B, d_B)\) in (7). Following (8) and (9), the received signal at Bob is given by
\[
y(\theta_B, d_B) = h^H(\theta_B, d_B)s + n_B = \sqrt{\rho(d_B)}x + n_B,
\]  
where \( n_B \) is the additive white Gaussian noise (AWGN), i.e., \( n_B \sim \mathcal{CN}(0, \sigma^2_B) \), and \( h^H \) denotes Hermitian transpose. As shown in (10), Bob can restore the original signal \( x \) from Alice without knowing the random mapping rule (i.e., the values of \( n_B \)). Following (10), the signal-to-noise ratio (SNR) at Bob is given by
\[
\gamma_B = \frac{\rho(\theta_B)}{\sigma^2_B}.
\]  
Similarly, the received signal at Eve is expressed as
\[
y(\theta_E, d_E) = h^H(\theta_E, d_E)s + n_E = \sqrt{\rho(\theta_E, d_E)}h(\theta_E, d_E)x + n_E,
\]  
where \( n_E \) is the AWGN at Eve with \( n_E \sim \mathcal{CN}(0, \sigma^2_E) \) and \( h(\theta_E, d_E) \) is the steering vector of the RFDA at Alice to Eve, which can be obtained by replacing \((\theta, d)\) with \((\theta_E, d_E)\) in (7). We note that Eve does not know the random mapping rule (i.e., the values of \( n_E \)), which is the same as Bob. Therefore, we know that the item \( \sqrt{\rho(\theta_E, d_E)}h(\theta_E, d_E) \) distorts the amplitude and phase of the received signals at Eve. Then, following (12), the signal-to-interference-plus-noise ratio (SINR) at Eve is given by
\[
\gamma_E = \frac{\rho(\theta_E, d_E)h(\theta_E, d_E)^2}{\rho(\theta_E, d_E)^2}.
\]  

III. Minimum Distance to Eve for Guaranteeing a Certain Level of Secrecy

In this section, we first derive the probability of non-zero secrecy capacity considering fixed Eve’s location (i.e., for given \( \theta_E \) and \( d_E \)). We then determine the minimum \( d_E \) to guarantee this probability being no less than a certain value. This minimum \( d_E \) allows us to find how far Eve needs to be forced away from Alice such that a certain level of security for the transmission from Alice to Bob is guaranteed.

A. Secrecy Performance With Fixed Eve’s Location

As Alice selects her beamforming vector as per her channel to Bob, the SINR at Eve given in (13) is a random variable (even for fixed \( d_E \)) due to the use of the random diverse array (i.e., the randomness in \( k_n \)). Following (7), \( h^H(\theta_E, d_E)h(\theta_B, d_B) \) is explicitly given by
\[
h^H(\theta_E, d_E)h(\theta_B, d_B) = \lambda \sum_{n=0}^{N-1} e^{j2\pi(n-(N-1)/2)\eta} e^{-j2\pi k_n p},
\]  
where \( \lambda \equiv \sqrt{\rho(d_B)} \rho(d_B) \), and
\[
p \equiv \Delta f / c (d_E - d_B), \quad q \equiv \frac{f\lambda}{c} (\cos \theta_E - \cos \theta_B).
\]  
Considering the randomness of \( k_n \) and following (13), we note that \( h^H(\theta_E, d_E)h(\theta_B, d_B) \) is the sum of \( N \) random variables. Following the central limit theorem and [9], in this work we approximate it as a Gaussian random variable and thus \( \gamma_E \) can be approximated as an exponential random variable. Then, in the following lemma we derive the probability of non-zero secrecy capacity, which is the probability of having \( \gamma_E \geq \gamma_E \) for a fixed \( d_E \). We note that, as per the central limit theorem, the distribution of \( \gamma_E \) is not very sensitive to the specific distribution of \( k_n \) and thus similar results can be obtained by considering other distributions (e.g., discrete uniform distribution, truncated normal distribution) for \( k_n \).

**Lemma 1:** Considering directional modulation with a random diverse array, the probability of non-zero secrecy capacity for given \( d_E \) and \( \gamma_E \) is given by
\[
p_n = \Pr(\gamma_E \geq \gamma_E) = 1 - e^{-\frac{\mu}{\gamma_E}},
\]  
where \( \mu = \mathbb{E}[\gamma_E] \). We further derive \( \mu \) as
\[
\mu = \frac{P \rho(\theta_E)}{\sigma^2_E} \left( 1 + 2 \sum_{n=0}^{N-2} \sum_{u=0}^{n-1} \frac{ec_1 + ec_2 - ec_3}{(2\pi M)^2} \right),
\]  
with \( c_1 = \cos(\omega) \), \( c_2 = \cos(\omega - 2\pi M) \), \( c_3 = \cos(\omega + 2\pi M) \), and \( \omega = 2\pi(n-u) \).

**Proof:** As we approximate \( \gamma_E \) as an exponential random variable, we next derive its mean to determine its probability density function (pdf). Following (13) and (14), we obtain
\[
\gamma_E = \eta \left[ \left( \sum_{n=0}^{N-1} a_n \right)^2 + \left( \sum_{n=0}^{N-1} b_n \right)^2 \right] = \left( N + 2 \sum_{n=0}^{N-2} \sum_{u=0}^{n-1} \cos(\omega[(n-u)q + (k_u - k_n)p]) \right),
\]  
where \( \eta \triangleq P \rho(\theta_E) / \sigma^2_E \), \( a_n \triangleq \cos(\omega[(n-(N-1)/2)q - k_n p]) \), and \( b_n \triangleq \sin(2\pi((n-(N-1)/2)q - k_n p)) \). For fixed \( d_E \), we note from (18) that the random variables involved in \( \gamma_E \) are \( k_n \) and \( k_u \). We also note that the central limit theorem is valid for arbitrary distributions of \( k_n \). Thus, in this subsection, we consider a continuous uniform distribution for \( k_n \), i.e., \( k_n \sim U(-\frac{M}{2}, \frac{M}{2}) \). Since \( k_u \) and \( k_n \) are i.i.d., the pdf of \( (k_u - k_n) \) is obtained as
\[
f_{k_u - k_n}(x) = \begin{cases} \frac{x+M}{M}, & -M \leq x < 0, \\ \frac{M-x}{M}, & 0 \leq x \leq M, \\ 0, & \text{otherwise}. \end{cases}
\]  
Then, the mean of \( \gamma_E \) can be obtained as \( \mathbb{E}[\gamma_E] = \int_{-M}^{M} \gamma_E f_{k_u - k_n}(x) dx \), where \( \gamma_E \) is a function of \( x \), as given in (17). After algebraic manipulations, we obtain \( \mu = \mathbb{E}[\gamma_E] \) given in (17), which completes the proof.

Following Lemma 1, we note that the probability of non-zero secrecy capacity, i.e., \( p_n \), is derived for a deterministic location of Eve. Specifically, \( p_n \) increases with \( d_E \), i.e., the probability to achieve a positive secrecy capacity increases as Eve moves away from Alice. We also note that in some scenarios, we may not know Eve’s exact location, but can establish a secrecy zone around Alice to guarantee a lower bound on \( p_n \), which represents a certain level of secrecy. As such, based on our analysis in Lemma 1, we next determine the minimum \( d_E \) (i.e., how far we need to push Eve away from Alice) in order to guarantee \( p_n \geq \delta \), where \( \delta \) is a given value to ensure a certain level of secrecy.
In the literature of physical layer security (e.g., [25]), in addition to the probability of non-zero secrecy capacity, the secrecy outage probability is also a widely used performance metric in the systems with unknown secrecy capacity. This is indeed the system model considered in this work, since the capacity of the eavesdropper’s channel is unknown. For the same reason, the secrecy capacity is hard to be used as a secrecy performance metric of our considered system model.

The secrecy outage probability is defined as the probability of the secrecy capacity \( C_s \) being less than a specific transmission rate \( R_o \) (bits/channel-use). In the wiretap channel, \( C_s \) is given by

\[
C_s = \begin{cases} 
C_B - C_E, & \gamma B > \gamma E, \\
0, & \gamma B \leq \gamma E,
\end{cases}
\]  

(20)

where \( C_B = \log_2(1 + \gamma_B) \) is the capacity of the main channel, and \( C_E = \log_2(1 + \gamma_E) \) is the capacity of the eavesdropper’s channel. Noting that the instantaneous value of \( C_B \) is known and the codeword rate is set as \( R_o = C_B \) and following a similar approach as detailed in Lemma 1, the secrecy outage probability for a given \( R_o \) is derived as

\[
p_o(R_o) = P_e(C_s < R_o) = P_e \left[ \log_2(1 + \gamma_B) - \log_2(1 + \gamma_E) < R_o \right] = P_e \left[ \gamma B > \frac{1 + \gamma_B}{2R_o} - 1 \right] = 1 - P_e \left[ \gamma B \leq \frac{1 + \gamma_B}{2R_o} - 1 \right] = e^{-\frac{\gamma B}{2R_o} - 1}.
\]  

(21)

Comparing (16) with (21), we note that the probability of non-zero secrecy capacity \( p_n \) can be written as a function of the secrecy outage probability \( p_o(R_o) \) as \( p_o = 1 - p_n(0) \). In addition, we note that \( p_o(R_o) \) for a fixed \( R_o \) decreases with \( d_E \), i.e., the secrecy outage probability decreases as Eve moves away from Alice. As such, a secrecy zone around Alice (which determines a minimum value of \( d_E \)) establishes an upper bound on the secrecy outage probability, i.e., \( p_o(R_o) \leq \epsilon \), where \( \epsilon \) is a predetermined value to represent a similar certain level of security. Therefore, in the following subsection we tackle the minimum value of \( d_E \) in order to guarantee \( p_o \geq \delta \).

B. Minimum Distance

In practical scenarios, we may not be able to know Eve’s exact location. As such, we derive the minimum distance from Alice to Eve (i.e., how far we need to push Eve away from Alice) in the following theorem. This minimum distance guarantees the probability of non-zero secrecy capacity from Alice to Bob being no less than a specific value (i.e., \( p_o \geq \delta \)).

**Theorem 1:** In the considered system, \( p_o \geq \delta \) can be guaranteed by ensuring \( d_E \geq d_{E_o} \), where \( d_{E_o} \) satisfies the following fixed-point equation

\[
\alpha^2 \frac{d_{E_o}}{d_B} = -\ln \left( 1 - \delta \right) \left( 1 + \frac{(N - 1) \sqrt{1 + \alpha^2}}{2(\pi M p)^2} \right).
\]  

(22)

For a sufficiently large bandwidth (i.e., \( M \Delta f \)), \( d_{E_o} \) can be approximated as

\[
d_{E_o} \approx \left( -\ln \left( 1 - \delta \right) \right)^\frac{1}{\alpha} d_B,
\]  

(23)

where \( \alpha \equiv \sin(2\pi M p) \) and \( \beta \equiv \alpha^2 / \beta_2 \).

**Proof:** We note that the probability of non-zero secrecy capacity \( p_n \) depends on Eve’s location (i.e., both \( \theta_E \) and \( d_E \)). In order to derive the approximated \( d_{E_o} \) for guaranteeing \( p_o \geq \delta \), in the following we first determine the minimum \( p_o \) by varying \( \theta_E \) for a given \( d_E \). Following Lemma 1, we know that minimizing \( p_o \) is equivalent to maximizing \( \mu \). Following (17) and using \( e_2 - e_3 = 2 \sin(\omega) \sin(2\pi M p) = 2 \alpha \sin(\omega) \) which is achieved with the aid of trigonometric functions, \( \mu \) can be rewritten as

\[
\mu = \frac{P_s \rho \left( d_E \right)}{N \sigma_E^2} \left( 1 + \frac{2}{N} \sum_{n=0}^{N-2} \sum_{u=n+1}^{N-1} \frac{2e_1 + 2 \alpha \sin(\omega)}{(2\pi M p)^2} \right),
\]  

(24)

As per Lemma 1 and (15), we note that \( \mu \) depends on \( \theta_E \) through \( \omega \). Due to the complexity of (24), the exact maximum value of \( \mu \) achieved by varying \( \theta_E \) cannot be analytically obtained. Here, we consider the worst-case scenario where the maximum value of \( \cos(\omega) + \alpha \sin(\omega) \) can be achieved for each pair of \( n \) and \( u \), which is \( \cos(\theta_1) + \alpha \sin(\theta_1) \) with \( \theta_1 = \arctan(\alpha) \). Then, in this worst-case scenario the maximum value of \( \mu \) is given by

\[
\mu_{\text{max}} = \frac{P_s \rho \left( d_E \right)}{N \sigma_E^2} \left( 1 + \frac{1}{N} \sum_{n=0}^{N-2} \sum_{u=n+1}^{N-1} \cos(\theta_1) + \alpha \sin(\theta_1) \right) \frac{N}{(\pi M p)^2},
\]  

(25)

where \( \mu_{\text{max}} \) is achieved by using

\[
\cos(\arctan(x)) = \frac{1}{\sqrt{1 + x^2}}
\]  

and

\[
\sin(\arctan(x)) = \frac{x}{\sqrt{1 + x^2}}.
\]

Following Lemma 1, if we can ensure \( 1 - e^{-\frac{\gamma B}{2R_o}} \geq \delta \), we can then guarantee \( p_o \geq \delta \). By setting \( 1 - e^{-\frac{\gamma B}{2R_o}} = \delta \) and considering that \( p_o \) monotonically increases with \( d_E \), we obtain \( d_{E_o} \) as a solution to (22). When the bandwidth (i.e., \( M \Delta f \)) increases sufficiently large, following (15) we note that the right hand side of (22) converges to \( -\ln(1 - \delta) \). This leads to the result given in (23) and completes the proof.

Following Theorem 1, we note that for fixed \( d_{B} \), the minimum distance between Alice and Eve to guarantee a certain level of security (i.e., \( p_o \geq \delta \)) monotonically decreases with \( N \). This means that when \( N \) increases, the region around Alice which we need to physically protect and prevent Eve from entering, shrinks. This explicitly shows that the ability of DM-RFDA to guarantee security increases with more antennas. Furthermore, Theorem 1 shows that \( d_{E_o} \) increases when \( \delta \) increases but decreases when \( \beta \) increases (i.e., the noise power ratio from Eve to Bob). We note that \( \theta_E = \theta_B \) does not maximize the SNR at Eve when \( d_E \neq d_{B} \), since the beamforming vector at Alice given in (9) depends on both \( \theta_E \) and \( \delta_{B} \) in the DM-RFDA system.

Based on Theorem 1, we derive the minimum \( d_{E_o} \) to ensure \( p_o(R_o) \leq \epsilon \) in the following corollary.
For a sufficiently large bandwidth (i.e., $M \Delta f$), $\overline{d}_E$ can be approximated as

$$
\overline{d}_E = \left( -\frac{2^{R_s} P_s K d_B^2 \ln \epsilon}{N \beta^2 \left( P_s K \left( \frac{d_B}{M} \right) + \sigma_E^2 (1 - 2^{R_s}) \right) } \right) ^{1/2}.
$$

**IV. NUMERICAL RESULTS**

Unless stated otherwise, our simulation settings are as follows: The central carrier frequency $f_c$ is set to 1 GHz (i.e., $f_c = 1$ GHz), the frequency increment is set to 3 MHz (i.e., $\Delta f = 3$ MHz), the element spacing is half of the wavelength (i.e., $l = c/2 f_c$), the path loss exponent is set to 2 (i.e., $\gamma = 2$), and $\beta = 1$ (i.e., $\sigma_E^2 = \sigma_B^2$).

In Fig. 2, we plot the probability of non-zero secrecy capacity, $p_n$, against the number of transmit antenna, $N$, for different distances from Alice to Eve with a fixed distance to Alice to Bob. In this figure, the markers represent the simulated $p_n$, and the curves represent the theoretical $p_n$ obtained in Lemma 1. We clarify that the simulated $p_n$ is achieved by numerically evaluating $\gamma_E$ through Monte Carlo simulations without any approximation. In this figure, we first observe that the theoretic $p_n$ precisely matches the simulated $p_n$ (especially when $N$ is large), which confirms the high accuracy of approximating $|H(\theta_E, d_B)|h(\theta_B, d_B)$ as a Gaussian random variable.

In Fig. 3, we plot the minimum distance from Alice to Eve for guaranteeing $p_n \geq \delta$, $d_E$, against the bandwidth, $M \Delta f$, for different distances from Alice to Bob, $d_B$. From this figure, we first observe that $d_E$ monotonically decreases (i.e., the size of the region around Alice to be physically protected decreases) and then approaches the approximation given in (23) when $M \Delta f$ increases. Intuitively, this is due to the fact that, as the available bandwidth increases, Alice has more freedom to randomly choose the frequencies to conduct secure transmission. The decrease in the protect region is at the cost of the increase in the required bandwidth. The existence of the performance floor, characterized by the approximation given in (23), can be explained by the fact that the number of transmit antennas becomes the performance limiting factor when the available bandwidth is sufficiently large. In addition, we observe from this figure that $d_E$ is much less than $d_B$. Meanwhile, we also present the minimum value of $d_E$ achieved by DM with a PA (i.e., phase array) for $d_B = 1$ km as a benchmark. We can observe that, the minimum value of $d_E$ is larger than $d_B$ for the DM-PA scheme. This means that, in order to guarantee a positive probability of non-zero secrecy capacity, Eve should be further away from Alice than Bob in the DM-PA scheme. This explicitly shows the benefit of using DM-RFDA for secure transmission.

**V. CONCLUSION**

In this work, we examined the physical layer security achieved by the DM-RFDA system where the path loss model was considered and the impact of the relative locations of Alice, Bob, and Eve was investigated. By using the probability of non-zero secrecy capacity (i.e., $p_n$) as the performance metric, we determined the minimum distance from Alice to Eve in order to guarantee a certain level of security for the communication from Alice to Bob. Our results demonstrated that this minimum distance can be significantly less than the distance from Alice to Bob, and decreases when the number of transmit antennas and the available bandwidth increase.

**REFERENCES**


