On Physical-Layer Security of FDA Communications Over Rayleigh Fading Channels

Shilong Ji, Wen-Qin Wang, *Senior Member, IEEE*, Hui Chen, and Shunsheng Zhang

***Abstract*—In this paper, we investigate frequency diverse array (FDA) antenna for physical-layer security and analyze the system performance (i.e., average secrecy capacity and secrecy outage performance) over independent but not necessarily identical distributed Rayleigh fading channels. A single-antenna multiple-channel receiver structure is proposed to address the time-variance property of FDA antenna. The transmitter allocates part of its power to send artificial noise (AN) so as to ensure the security of communications, such that the channels other than the desired receiver's are degraded. Specifically, we derive the closed-form expressions for average secrecy capacity, probability of nonzero secrecy capacity, and secrecy outage probability, respectively. The correctness of the proposed analysis is corroborated via simulations. Furthermore, the corresponding asymptotic expressions for average secrecy capacity and secrecy outage probability in high signal-to-interference-plus-noise ratio (SINR) regime are also provided, respectively, to have deep insights into the performance of the considered system. Numerical results show that the FDA communications significantly outperforms the phased-array (PA) scheme in range dimension for secure communication.**

***Index Terms*—Secure communication, frequency diverse array (FDA), physical-layer security, FDA communications, Rayleigh fading, secrecy capacity, secrecy outage probability.**

I. Introduction

PHYSICAL-LAYER security plays an important role in wireless communications [1]–[10], due to the fact that the secure transmission is provided by exploiting the characteristic of wireless channels rather than the traditional security that was regarded as an independent issue beyond the physical layer and was studied through designing and implementing cryptographic algorithms. A secure transmission protocol was developed in [11] based on one-way communications over quasi-static wireless channels, the authors shown that the security is available even in a more realistic scenario where only imperfect channel state information (CSI) can be obtained. Gopala *et al.* [12] and Liang *et al.* [13] derived the ergodic secrecy capacity of fading channels independently and presented the power and rate allocation strategies at the same time. Later, the multiple desired receiver scenario was studied by Khisti *et al.* [14] over fading channels and the secrecy capacity was analyzed on the basis of outage probability in delay-limit situation.

The recent interest of physical-layer security turns to multiple-input multiple-output (MIMO) scenarios, where the eavesdropper's channel may be further deteriorated by exploiting the spatial degrees-of-freedom (DOFs). Taking the resource-constrained nature of the backscatter system into consideration, [15] proposed a noise-injection precoding strategy to safeguard the physical layer security of a multiple-input multiple-output (MIMO) radio frequency identification (RFID) system. In [16], power allocation schemes for relay-aided large-scale MIMO systems are proposed to address the joint power and time allocation issue for secure communications in massive multiple-input multiple-output (M-MIMO) relaying system. Further, for large-scale MIMO systems, the secrecy outage probability and interception probability are investigated in [17] with Rayleigh fading scenario consideration for emerging cyber-physical systems (CPSs) and Internet of Things. A multiple-antenna wiretap-channel under multiple cooperative jammers was investigated in [18] and the secure DOFs were established for all possible values of the number of antennas. Zhu *et al.* [19] designed robust beamforming to guarantee the physical layer security for a multiuser beam division multiple access (BDMA) massive MIMO system, when the channel estimation errors are taken into consideration. Another meaningful approach that widely being used in physical-layer security is artificial noise [19]–[25]. In AN-aided approaches, the transmitter should allocate part of its power to send the artificially generated noise to interfere potential eavesdroppers. With multiple randomly located jammers, Wu *et al.* [25] investigated the secrecy rate maximization problem in AN-aided multiple-input single-output (MISO) wiretap channel.

More recently, array antenna has been received great attention in communication community. Specially, phased-array antenna, which is composed of lots of radiating elements each with a phase shifter. Beams are formed by shifting the phase of the signal emitted from each radiating element, to provide constructive/destructive interference so as

Manuscript received September 14, 2018; revised January 1, 2019; accepted February 27, 2019. Date of publication March 22, 2019; date of current version September 9, 2019. This work was supported by National Natural Science Foundation of China under grant 61571081, Young top-notch talent of the national Ten Thousand Talent Program, and Sichuan Science and Technology Program under grant 2018RZ0141. The associate editor coordinating the review of this paper and approving it for publication was D. Niyato. *(Corresponding author: Wen-Qin Wang.)*

S. Ji, W.-Q. Wang, and H. Chen are with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: slji14430@yeah.net; wqwang@uestc.edu.cn; huichen0929@uestc.edu.cn).

S. Zhang is with the Research Institute of Electronic Science and Technology, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: zhangss@uestc.edu.cn).

Digital Object Identifier 10.1109/TCCN.2019.2906896

to steer the beams in the desired direction, thus high gain can be achieved. Several phased-array-based schemes have been proposed in [26]–[29]; however, phased-array antenna can only produce angle-dependent beampattern in a far-field point, which implies only the security in angle dimension can be achieved. Later, Frequency diverse array antenna emerges as a new form of antenna to overcome this problem. FDA uses a small frequency offset across the array elements to make its steering direction change as a function of the angle, range, and even the frequency offset [30], which is different from the range-independent phased-array antenna, enables the array beam to scan without the need of phase shifters or mechanical steering, and provides both angle and range dependent beampattern. These properties make FDA potentially useful in many promising applications [31]–[36]. Although current FDA related investigations focus on radar applications [37]–[40], it also can provide potential two-dimension secure transmission for physical layer security rather than one-dimension security of phased-array antenna. Therefore, in this paper, we utilize FDA antenna for physical-layer security communication.

Exploiting FDA antenna for secure communication has been reported in [41]–[44]. Ding *et al.* [41] established an orthogonal frequency-division multiplexing (OFDM) transmitter based on FDA to enhance physical-layer security. Directional modulation and FDA were jointly utilized in [42] for point-to-point secure communication. Aided with AN, a random FDA secure transmission scheme was proposed in [43]; however, only the instantaneous time was considered and thus ignored the time-variance property, a fundamental problem of FDA antenna. Very recently, Lin *et al.* [44] investigated the physical layer security for highly correlated channels between the desired receiver and eavesdropper by utilizing an FDA beamforming approach.

However, all the aforementioned works in [41]–[44] are limited to Gaussian channels. In practical wireless environment, the amplitude variation of a received radio signal can be modeled as a product of path loss and fading [45]. Several models exist for characterizing path loss, including the variants of Okumura-Hata and Walfisch-Ikegami formulas [46]. Fading may be either due to multipath propagation, which is referred to as small-scale multipath fading, or due to the shadowing from obstacles affecting the wave propagation, which is usually referred to as shadowing. As fading is one of the two fundamental aspects (the other one is interference) of wireless communications, which has been necessarily considered in various communication systems [47], [48]. Thus, it is of great interest to investigate FDA based secure communication over fading channels. To the best of our knowledge, until now, there has been no literature on FDA-based secure communication over fading channels available.

Motivated by the observations above, in this paper, we take Rayleigh fading scenario for consideration and concentrate on analyzing the secure performance provided by artificial-noise aided secure communication using FDA antenna. Our main contributions are listed as follows:

(i) Different from the conventional phased-array, time-variance property is a thorny problem for the application of FDA antenna, which is difficult to cope with, and has not been well handled in the literature. In this paper, we propose a single-antenna multiple-channel signal processing structure to address the time-variant property and can effectively process the received signal, which is completely different from the existing works [41]–[44] and significantly facilitates the analysis. This form of multiple-channel receive signal processing structure is applied to all the receivers of the considered system.

(ii) Based on the multiple-channel structure proposed, we firstly derive an approximate SINR for the eavesdropper's channel, which greatly simplifies our derivations for achieving a closed-form expression of average secrecy capacity over Rayleigh fading channels, and then, the optimal power allocation problem is studied accordingly. Moreover, by employing an approximate approach, the asymptotic expression for average secrecy capacity in high SINR regime is also derived as an upper bound to have a deep insight into system performance.

(iii) The secrecy outage performance including probability of nonzero secrecy capacity and secrecy outage probability are investigated over Rayleigh fading channels, together with the approximate closed-form expressions derived. In addition, the impacts incurred by the eavesdropper's locations on secrecy outage performance are examined. Furthermore, the asymptotic expression for secrecy outage probability in high SINR regime are also achieved as a lower bound, which provide us a convenient way to evaluate the outage performance of the proposed communication scheme.

(iv) The conventional phased-array schemes [26]–[28] and the existing FDA schemes [41]–[44] are all focused on Gaussian channels. All of theses works lose to study the random property of fading channels on the system performance. With Rayleigh fading scenario considered in this paper, we investigate FDA scheme and the conventional phased-array scheme over both Gaussian and Rayleigh fading channels. Moreover, the worst performance case that the desired receiver and eavesdropper locate very close are studied.

The rest of this paper is organized as follows. In Section II, we present the proposed single-antenna receiver structure and the FDA communications system model over Rayleigh fading channels. In Section III, the closed-form expression of average secrecy capacity is derived, together with its performance analysis. In Section IV, the secrecy outage performance of the proposed FDA communication system are analyzed according to the derived closed-form expressions. Finally, numerical results and discussions are provided in Section V, and conclusions are drawn in Section VI.

Notations: Boldface lowercase and uppercase letters, e.g., $\mathbf{a}$ and $\mathbf{A}$, are used to denote vectors and matrices, respectively. Italic letters denote scalars. For a complex number, $|\cdot|$, $(\cdot)^*$, and $\|\cdot\|$ represent the modulus, the conjugate operator and the Eulcidean norm, respectively. Pr$[\cdot]$ denotes the probability. For a vector or matrix, $(\cdot)^T$ and $(\cdot)^H$ denote the transpose and Hermitian transpose, respectively. The $N \times N$ identity matrix is given by $\mathbf{I}_N$ and the expectation is denoted by $\mathbb{E}[\cdot]$.

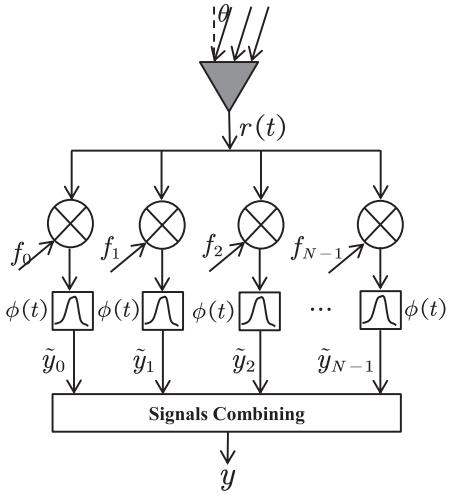

Fig. 1. Single-antenna multiple-channel receiver structure.

II. System and Channel Model

A. FDA Communications Receiver

The basic FDA uses a small frequency offset across its array elements. That is, the radiation frequency from the *n*th element is given by

$$f_n = f_0 + n\Delta f,\ \ n = 0, 1, \ldots, N-1, \tag{1}$$

where f_0, Δf, and N are the carrier frequency, the frequency offset, and the number of array element, respectively.

For a communication receiver located in a far-field point (θ, R) (θ and R are the azimuth and range from the receiver to the first transmitting element, respectively), the distance between the receiver and the *n*th transmitting element is approximated as $R_n \approx R - nd\sin\theta$, with d being the uniform linear inter-element spacing. Let $\phi(t)$ be the transmitted baseband complex waveform with unit energy, i.e., $\int_T \phi(t)\phi^*(t)dt = 1$, where T is the pulse duration. The superimposed signals arriving at the communication receiver can be written as

$$r(t) = hx\sum_{n=0}^{N-1} \Pi_n \phi(t-\tau_n) e^{j2\pi f_n(t-\tau_n)}, \tag{2}$$

where h is the channel coefficient, x is the transmitted complex digital modulation symbol, Π_n is the weight of *n*th transmit element, $\tau_n = R_n/c$ denotes the signal propagation delay from the *n*th element to the receiver, with c being the speed of light. Following the narrow-band assumption, it holds $\phi(t-\tau_n) \approx \phi(t-\tau)$ with $\tau = R/c$. Then, (2) can be rewritten as

$$\begin{aligned} r(t) &\approx \phi(t-\tau)hxe^{j2\pi f_0\left(t-\frac{R}{c}\right)}\sum_{n=0}^{N-1}\Pi_n e^{j2\pi n\Phi(t)} \\ &= hxe^{j2\pi f_0\left(t-\frac{R}{c}\right)}\mathbf{\Pi}^H\mathbf{u}(t;\theta,R)\phi(t-\tau), \end{aligned} \tag{3}$$

where $\Phi(t) = \Delta f t - \frac{\Delta f R}{c} + \frac{f_0 d\sin\theta}{c}$, $\mathbf{u}(t;\theta,R) = [1, e^{j2\pi\Phi(t)}, \ldots, e^{j2\pi(N-1)\Phi(t)}]^T$ is the transmit steering vector, and $\mathbf{\Pi} = [\Pi_0, \Pi_1, \ldots, \Pi_{N-1}]^T$ denotes the transmit weight vector.

Then, at the communication receiver, we adopt a single-antenna multiple-channel approach to deal with the received signals, whose structure is shown in Fig. 1. In the single-antenna receiver model, the multiple carriers, denoted by $f_0, f_1, f_2, \ldots, f_{M-1}$, are adopted to demodulate the received signals, then followed by matched filters, the outputs of all the filters are finally combined. By exploiting this approach, the received radio frequency (RF) signal in (3) is first down-converted to the following baseband signal

$$\begin{aligned} r'(t) &= hxe^{j2\pi f_0\left(t-\frac{R}{c}\right)}e^{-j2\pi f_0\left(t-\frac{R}{c}\right)}\mathbf{\Pi}^H\mathbf{u}(t;\theta,R)\phi(t-\tau) \\ &= hx\mathbf{\Pi}^H\mathbf{u}(t;\theta,R)\phi(t-\tau), \end{aligned} \tag{4}$$

by using a signal down-conversion operation. Then, matched-filtering the obtained baseband signal in (4) and making the assumption that the waveform satisfies the following orthogonality condition

$$\int_T \phi(t)\phi^*(t-\tau)e^{j2\pi m\Delta f t}dt = \delta(m),\ \forall\tau, \tag{5}$$

where $\delta(\cdot)$ is the Kronecker delta function. Consider all one weight vector, i.e., $\mathbf{\Pi} = [1, 1, \ldots, 1]^T$, we obtain the noise-free signal of the *n*th filter output

$$\begin{aligned} \tilde{y}_n(t) &= \left[r'(t) \times e^{-j2\pi n\Delta f t}\right] \circledast \phi(t) \\ &= hxe^{j\frac{2\pi n}{c}(-\Delta f R + f_0 d\sin\theta)}, \end{aligned} \tag{6}$$

where $\circledast$ is the convolution operator. Further, we have

$$\tilde{\mathbf{y}} = [\tilde{y}_0, \tilde{y}_1, \ldots, \tilde{y}_{N-1}]^T = hx\mathbf{u}(\theta,R), \tag{7}$$

with $\mathbf{u}(\theta,R) = [1, e^{j2\pi\Phi(0)}, \ldots, e^{j2\pi(N-1)\Phi(0)}]^T$.

Let $\mathbf{a}(\theta,R) = \mathbf{u}(\theta,R)/\sqrt{N}$ be the normalized transmit steering vector. Then, we combine all the filters' outputs, and the final combined noise-free signal at the receiver is given by

$$y = h\mathbf{a}^H(\theta,R)\mathbf{s}, \tag{8}$$

where $\mathbf{s} = x[1, 1, \ldots, 1]^T$ is the $N \times 1$ transmitted symbol vector.

In this paper, this form of single-antenna approach will be applied to all the receivers of the considered system.

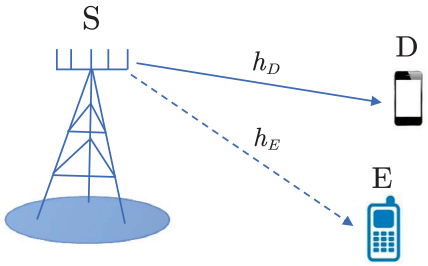

Fig. 2. System model.

B. System Model Formation

As illustrated in Fig. 2, we consider a MISO wiretap-channel consisting of one source transmitter S, a desired receiver D, and a potential passive eavesdropper E. The transmitter S intends to send its message to D, while E attempts to decode this message from its received signal through the eavesdropper channel. The transmitter S uses an N-element FDA antenna, while the desired receiver and eavesdropper

adopt single antenna. In addition, we assume both the main channel (S $\rightarrow$ D) and eavesdropper channel (S $\rightarrow$ E) experience ergodic block quasi-static fading, where the channel coefficients remain constants during a block period and vary independently from block to block. We also consider that the coefficients from the transmitter S to the desired receiver D and to eavesdropper E are ideally estimated in D and E, respectively. In cases of active eavesdropper, E is capable of estimating its corresponding channel as D does, whereas in other cases, it needs to eavesdrop the characteristics of the channel estimation process (e.g., the transmitter's pilots signals).

In the study of physical-layer security, beamforming with AN is widely used in the literature because of the robustness and desirable secrecy performance [49]–[52]. Hence, in this paper, AN-aided secure transmission is adopted in the FDA scheme and the transmitted baseband signal can be given by

$$\mathbf{s} = \sqrt{\alpha P_S}\mathbf{v}x + \sqrt{\beta P_S}\mathbf{w}, \tag{9}$$

where x is the transmitted symbol at S with average power constraint, i.e., $\mathbb{E}[|x|^2] = 1$. P_S is the fixed average transmit power of S. α and β are the parameters that determine the power allocation for the useful signal and artificial noise, respectively, satisfying $\alpha + \beta = 1$, and $\mathbf{v}$ is a beamforming vector designed by S to implement coherent combining at the desired receiver, so as to maximize the receive SINR of D. Note that, the artificial noise should satisfy $\mathbf{a}^H(\theta_D, R_D)\mathbf{w} = 0$, which projects AN to the null space of $\mathbf{a}(\theta_D, R_D)$. Thus, the artificial noise vector $\mathbf{w}$ can be expressed by [43]

$$\mathbf{w} = \frac{\big(\mathbf{I}_N - \mathbf{a}(\theta_D, R_D)\mathbf{a}^H(\theta_D, R_D)\big)\mathbf{z}}{\big\|\big(\mathbf{I}_N - \mathbf{a}(\theta_D, R_D)\mathbf{a}^H(\theta_D, R_D)\big)\mathbf{z}\big\|}, \tag{10}$$

where $\mathbf{z}\sim\mathcal{CN}(0, \mathbf{I}_N)$.

Then, according to (8), when the baseband signal in (9) is transmitted, the received signals at the desired receiver D and eavesdropper E can be expressed as

$$\begin{aligned} y_D &= h_D\mathbf{a}^H(\theta_D, R_D)\mathbf{s} + n_D \\ &= \sqrt{\alpha P_S}h_D x + n_D, \end{aligned} \tag{11}$$

and

$$\begin{aligned} y_E &= h_E\mathbf{a}^H(\theta_E, R_E)\mathbf{s} + n_E \\ &= \sqrt{\alpha P_S}h_E\mathbf{a}^H(\theta_E, R_E)\mathbf{v}x \\ &\quad + \sqrt{\beta P_S}h_E\mathbf{a}^H(\theta_E, R_E)\mathbf{w} + n_E, \end{aligned} \tag{12}$$

respectively, where h_i, $i \in \{D, E\}$ is the complex channel coefficient of the link S $\rightarrow$ i and n_i is the complex additive white Gaussian noise (AWGN) with zero mean and variance σ_i^2, i.e., $n_i \sim \mathcal{CN}(0, \sigma_i^2)$. Note that, the received signal is coherent combined at D by exploiting the beamforming scheme mentioned above. However, for the eavesdropper E, the item $\mathbf{a}^H(\theta_E, R_E)\mathbf{v}$ distorts the amplitude and phase of the signal received at E. Also, the randomly change of artificial noise vector $\mathbf{w}$ and the nonzero of $\mathbf{a}(\theta_E, R_E)$ make the item $\mathbf{a}^H(\theta_E, R_E)\mathbf{w}$ distort the receive signal seriously.

The corresponding output SINR at D and E can be expressed as

$$\gamma_D = \frac{\alpha P_S|h_D|^2}{\sigma_D^2} = |h_D|^2\alpha\mu_D, \tag{13}$$

and

$$\begin{aligned} \gamma_E &= \frac{\alpha P_S\big|\mathbf{a}^H(\theta_E, R_E)\mathbf{a}(\theta_D, R_D)\big|^2|h_E|^2}{\beta P_S\big|\mathbf{a}^H(\theta_E, R_E)\mathbf{w}\big|^2|h_E|^2 + \sigma_E^2} \\ &= \frac{\alpha\mu_D\big|\mathbf{a}^H(\theta_E, R_E)\mathbf{a}(\theta_D, R_D)\big|^2|h_E|^2}{\beta\mu_D\big|\mathbf{a}^H(\theta_E, R_E)\mathbf{w}\big|^2|h_E|^2 + \kappa}, \end{aligned} \tag{14}$$

respectively, where $\mu_D = P_S/\sigma_D^2$ and $\kappa = \sigma_E^2/\sigma_D^2$. Herein, we assume the complex channel coefficient h_i, $i \in \{D, E\}$ undergoes independent but not necessarily identical distributed Rayleigh fading, which implies that the channel gains $|h_i|^2$ follows an exponential distribution, with $\mathbb{E}[|h_i|^2] = \Omega_i, i \in \{D, E\}$.

Although the quasi-static h_i is random but it remains constant for each realization, it is reasonable to view the main and eavesdropper channels (with fading) as complex AWGN channels. Thus, according to [53], the instantaneous secrecy capacity for one realization (γ_D, γ_E) in quasi-static complex fading wiretap-channel is given by

$$C_s(\gamma_D, \gamma_E) = \max\{C_D - C_E,\ 0\}, \tag{15}$$

where

$$C_D = \ln(1 + \gamma_D), \tag{16}$$

and

$$C_E = \ln(1 + \gamma_E), \tag{17}$$

are the channel capacities at D and E, respectively. In this scenario, the optimal power allocation parameter α for useful signal that maximizes $C_s(\gamma_D, \gamma_E)$ can be obtained through

$$\alpha^*_{\text{AWGN}} = \underset{0\le\alpha\le1}{\operatorname{argmax}}\, C_s(\gamma_D, \gamma_E). \tag{18}$$

Suppose perfect CSI of the eavesdropper's channel is available to the transmitter, the coding scheme can be adapted to every realization of the fading coefficients. The average secrecy capacity can then be calculated by [53]

$$\begin{aligned} \bar{C}_s(\gamma_D, \gamma_E) &= \mathbb{E}[C_s(\gamma_D, \gamma_E)] \\ &= \int_0^\infty\int_0^\infty C_s(\gamma_D, \gamma_E)f(\gamma_D, \gamma_E)\,d\gamma_D\,d\gamma_E, \end{aligned} \tag{19}$$

where $f(\gamma_D, \gamma_E)$ is the joint probability density function (PDF) of γ_D and γ_E.

III. Secrecy Capacity Analysis

Although (15) gives the instantaneous secrecy capacity, it just depicts the secrecy capacity for one realization (γ_D, γ_E) of the wiretap-channel. In this section, we analyze the average secrecy capacity over Rayleigh fading channels.

A. Preliminary

To facilitate the analysis, we need to derive the PDFs of γ_D and γ_E, respectively, first.

Since the random variable $|h_D|^2$ follows an exponential distribution with mean Ω_D and (13) reveals that the instantaneous SINR is $\gamma_D \propto |h_D|^2$, γ_D also should be exponentially distributed with mean $\bar{\gamma}_D = \mathbb{E}[\gamma_D] = \alpha\mu_D\Omega_D$, specifically

$$f(\gamma_D) = \frac{1}{\alpha\mu_D\Omega_D} e^{-\frac{\gamma_D}{\alpha\mu_D\Omega_D}},\ \gamma_D > 0. \tag{20}$$

The following theorem provides a tight upper bound for the instantaneous SINR of the eavesdropper channel, so as to obtain the approximate PDF of γ_E.

Theorem 1: According to the SINR of γ_E in (14), a tight upper bound SINR for γ_E can be approximated given as follows:

$$\gamma_E \overset{(\bigstar)}{\leq} \gamma_E^{\mathrm{up}} = \alpha\left|\mathbf{a}^H(\theta_E, R_E)\mathbf{a}(\theta_D, R_D)\right|^2 \times \min\left\{\frac{1}{\beta\left|\mathbf{a}^H(\theta_E, R_E)\mathbf{w}\right|^2}, \frac{\mu_D}{\kappa}|h_E|^2\right\}. \tag{21}$$

Proof: The upper bound γ_E^{up} can be derived straightforwardly as follows:

$$\begin{aligned}\frac{1}{\gamma_E} &= \frac{\beta\mu_D\left|\mathbf{a}^H(\theta_E, R_E)\mathbf{w}\right|^2|h_E|^2 + \kappa}{\alpha\mu_D\left|\mathbf{a}^H(\theta_E, R_E)\mathbf{a}(\theta_D, R_D)\right|^2|h_E|^2} \\ &= \frac{\beta\left|\mathbf{a}^H(\theta_E, R_E)\mathbf{w}\right|^2}{\alpha\left|\mathbf{a}^H(\theta_E, R_E)\mathbf{a}(\theta_D, R_D)\right|^2} + \frac{\kappa}{\alpha\mu_D\left|\mathbf{a}^H(\theta_E, R_E)\mathbf{a}(\theta_D, R_D)\right|^2|h_E|^2} \\ &\geq \frac{1}{\alpha\left|\mathbf{a}^H(\theta_E, R_E)\mathbf{a}(\theta_D, R_D)\right|^2} \times \max\left\{\beta\left|\mathbf{a}^H(\theta_E, R_E)\mathbf{w}\right|^2, \frac{\kappa}{\mu_D|h_E|^2}\right\}.\end{aligned} \tag{22}$$

Taking the reciprocal of (22) on both sides, we can obtain the upper bound γ_E^{up}, which completes the proof. ∎

It is important to point out that the step $(\bigstar)$ in (21) obtaining γ_E^{up} arises as a tight upper bound approximation of γ_E, which will be validated through numerical results in Section V. This tight upper bound approximation implies that the PDF of γ_E can be approximately obtained by deriving the PDF of γ_E^{up}.

Next, we present a method to calculate the cumulative distribution function (CDF) of the approximate SINR γ_E^{up} in the following theorem.

Theorem 2: The CDF of the approximate SINR γ_E^{up} for the eavesdropper channel is given by

$$F_{\gamma_{\mathrm{E}}^{\mathrm{up}}}(\gamma) = F_{|h_E|^2}\left(\frac{\kappa}{\alpha\mu_D Y}\gamma\right),\ \gamma > 0, \tag{23}$$

where $Y \triangleq |\mathbf{a}^H(\theta_E, R_E)\mathbf{a}(\theta_D, R_D)|^2$, and $F_X(\cdot)$ denotes the CDF of a random variable X.

Proof: The proof is presented in the Appendix. ∎

Theorem 2 demonstrates that, the CDF of γ_E^{up} is closely related to the CDF of $|h_E|^2$. With the assumption that h_E undergoes Rayleigh fading, the CDF of γ_E^{up} then can be derived as

$$F_{\gamma_{\mathrm{E}}^{\mathrm{up}}}(\gamma) = 1 - e^{-\frac{\kappa}{\alpha\mu_D Y\Omega_E}\gamma},\ \gamma > 0. \tag{24}$$

Note that γ_E^{up} follows an exponential distribution with mean $\bar{\gamma}_E^{\mathrm{up}} = \mathbb{E}[\gamma_E^{\mathrm{up}}] = \alpha\mu_D Y\Omega_E/\kappa$. Therefore, the PDF of γ_E^{up} can be easily obtained as

$$f\left(\gamma_E^{\mathrm{up}}\right) = \frac{\kappa}{\alpha\mu_D Y\Omega_E} e^{-\frac{\kappa}{\alpha\mu_D Y\Omega_E}\gamma_E^{\mathrm{up}}},\ \gamma_E^{\mathrm{up}} > 0. \tag{25}$$

B. Closed-Form Analysis

Here, we aim to derive a tight lower bound closed-form expression for the average secrecy capacity over Rayleigh fading channels. Since γ_E^{up} in (21) is a tight upper bound approximation of γ_E, by plugging (21) to (19), we can get the following extended approximate expression

$$\begin{aligned}\bar{C}_s(\gamma_D, \gamma_E) &\geq \bar{C}_{LB}(\gamma_D, \gamma_E) \\ &= \int_0^\infty\int_0^\infty C_s\left(\gamma_D, \gamma_E^{\mathrm{up}}\right) f(\gamma_D) f\left(\gamma_E^{\mathrm{up}}\right) d\gamma_E^{\mathrm{up}} d\gamma_D.\end{aligned} \tag{26}$$

Similar to (18), the optimal power allocation parameter α that maximizes the lower bound average secrecy capacity, $\bar{C}_{LB}(\gamma_D, \gamma_E)$, can be obtained by

$$\alpha_{LB}^* = \underset{0\leq\alpha\leq 1}{\operatorname{argmax}}\ \bar{C}_{LB}(\gamma_D, \gamma_E). \tag{27}$$

Changing the order of integral in (26), we obtain

$$\bar{C}_{LB}(\gamma_D, \gamma_E) = \int_0^\infty \underbrace{\left[\int_0^\infty C_s\left(\gamma_D, \gamma_E^{\mathrm{up}}\right) f\left(\gamma_E^{\mathrm{up}}\right) d\gamma_E^{\mathrm{up}}\right]}_{\mathcal{L}} f(\gamma_D) d\gamma_D, \tag{28}$$

where

$$\mathcal{L} = \int_0^{\gamma_D} \left(\ln(1+\gamma_D) - \ln\left(1+\gamma_E^{\mathrm{up}}\right)\right) f\left(\gamma_E^{\mathrm{up}}\right) d\gamma_E^{\mathrm{up}}. \tag{29}$$

By exploiting the integration by parts and applying some algebraic manipulations, we derive (29) as

$$\begin{aligned}\mathcal{L} &= \int_0^{\gamma_D} (\ln(1+\gamma_D) - \ln(1+\gamma_E^{\mathrm{up}})) f(\gamma_E^{\mathrm{up}}) d\gamma_E^{\mathrm{up}} \\ &= \int_0^{\gamma_D} \ln(1+\gamma_D) f(\gamma_E^{\mathrm{up}}) d\gamma_E^{\mathrm{up}} - \int_0^{\gamma_D} \ln(1+\gamma_E^{\mathrm{up}}) f(\gamma_E^{\mathrm{up}}) d\gamma_E^{\mathrm{up}} \\ &= \ln(1+\gamma_D) F_{\gamma_E^{\mathrm{up}}}(\gamma_D) - \int_0^{\gamma_D} \ln(1+\gamma_E^{\mathrm{up}}) f(\gamma_E^{\mathrm{up}}) d\gamma_E^{\mathrm{up}} \\ &= \ln(1+\gamma_D) F_{\gamma_E^{\mathrm{up}}}(\gamma_D) \\ &\quad - \left[\ln(1+\gamma_D) F_{\gamma_E^{\mathrm{up}}}(\gamma_D) - \int_0^{\gamma_D} \frac{F_{\gamma_E^{\mathrm{up}}}(\gamma_E^{\mathrm{up}})}{1+\gamma_E^{\mathrm{up}}} d\gamma_E^{\mathrm{up}}\right] \\ &= \int_0^{\gamma_D} \frac{F_{\gamma_E^{\mathrm{up}}}(\gamma_E^{\mathrm{up}})}{1+\gamma_E^{\mathrm{up}}} d\gamma_E^{\mathrm{up}}.\end{aligned} \tag{30}$$

Substituting (30) and (28) into (26), we rewrite the average secrecy capacity as

$$\begin{aligned}\bar{C}_s(\gamma_D,\gamma_E) &\geq \bar{C}_{LB}(\gamma_D,\gamma_E)\\ &= \int_0^{\infty}\left[\int_0^{\gamma_D}\frac{F_{\gamma_E^{\mathrm{up}}}\left(\gamma_E^{\mathrm{up}}\right)}{1+\gamma_E^{\mathrm{up}}}d\gamma_E^{\mathrm{up}}\right]f(\gamma_D)d\gamma_D. \quad (31)\end{aligned}$$

By changing the order of the integral in (31), we have

$$\begin{aligned}\bar{C}_s(\gamma_D,\gamma_E) &\geq \bar{C}_{LB}(\gamma_D,\gamma_E)\\ &= \int_0^{\infty}\frac{F_{\gamma_E^{\mathrm{up}}}\left(\gamma_E^{\mathrm{up}}\right)}{1+\gamma_E^{\mathrm{up}}}\left[\int_{\gamma_E^{\mathrm{up}}}^{\infty}f(\gamma_D)d\gamma_D\right]d\gamma_E^{\mathrm{up}}\\ &= \int_0^{\infty}\frac{F_{\gamma_E^{\mathrm{up}}}\left(\gamma_E^{\mathrm{up}}\right)}{1+\gamma_E^{\mathrm{up}}}\left[1-F_{\gamma_D}\left(\gamma_E^{\mathrm{up}}\right)\right]d\gamma_E^{\mathrm{up}}. \quad (32)\end{aligned}$$

Observe that (32) depends on the statistics of the main channel and the eavesdropper's channel. Based on (20) and the Rayleigh fading assumption, we can easily obtain

$$F_{\gamma_D}(\gamma)=1-e^{-\frac{\gamma}{\alpha\mu_D\Omega_D}},\ \gamma>0. \quad (33)$$

By substituting (24) and (33) to (32), and applying some algebraic manipulations, we obtain

$$\begin{aligned}\bar{C}_s(\gamma_D,\gamma_E) &\geq \bar{C}_{LB}(\gamma_D,\gamma_E)\\ &= \int_0^{\infty}\frac{e^{-\frac{1}{\alpha\mu_D\Omega_D}\gamma_E^{\mathrm{up}}}}{1+\gamma_E^{\mathrm{up}}}d\gamma_E^{\mathrm{up}}\\ &\quad-\int_0^{\infty}\frac{e^{-\frac{\kappa\Omega_D+Y\Omega_E}{\alpha\mu_D Y\Omega_D\Omega_E}\gamma_E^{\mathrm{up}}}}{1+\gamma_E^{\mathrm{up}}}d\gamma_E^{\mathrm{up}}. \quad (34)\end{aligned}$$

Note that, the two integrals in (34) have the same form

$$\int_0^{\infty}\frac{e^{-\mu x}}{1+x}dx. \quad (35)$$

By utilizing integration by parts, the integral in (35) can be transformed as follows

$$\int_0^{\infty}\frac{e^{-\mu x}}{1+x}dx=\mu\int_0^{\infty}e^{-\mu x}\ln(1+x)dx. \quad (36)$$

Further, from [54, eq. (4.337.2)], the following relationship exists

$$\int_0^{\infty}e^{-\mu x}\ln(1+x)dx=\frac{1}{\mu}e^{\mu}\mathrm{E}_1(\mu). \quad (37)$$

where $\mathrm{E}_1(x)=\int_x^{\infty}\frac{e^{-t}}{t}dt$ is the exponential-integral function.

Then, by applying (36) and (37) to (34), the average secrecy capacity in closed-form is finally given as follows

$$\begin{aligned}\bar{C}_s(\gamma_D,\gamma_E) &\geq \bar{C}_{LB}(\gamma_D,\gamma_E)\\ &= e^{\frac{1}{\alpha\mu_D\Omega_D}}\mathrm{E}_1\left(\frac{1}{\alpha\mu_D\Omega_D}\right)\\ &\quad-e^{\frac{\kappa\Omega_D+Y\Omega_E}{\alpha\mu_D Y\Omega_D\Omega_E}}\mathrm{E}_1\left(\frac{\kappa\Omega_D+Y\Omega_E}{\alpha\mu_D Y\Omega_D\Omega_E}\right). \quad (38)\end{aligned}$$

It is seen that this approximate closed-formed expression for average secrecy capacity given in (38) involves the products of exponential and the exponential integral function.

C. Asymptotic Analysis

In this part, we aim to derive an asymptotic expression for the average secrecy capacity to have a deep insight into the system performance. To achieve this goal, we firstly examine the following inequality [55]

$$\underbrace{\frac{1}{2}e^{-x}\ln\left(1+\frac{2}{x}\right)}_{L(x)}<\mathrm{E}_1(x)<\underbrace{e^{-x}\ln\left(1+\frac{1}{x}\right)}_{U(x)},\ x>0, \quad (39)$$

where $L(x)$ and $U(x)$ denote a lower and upper boundary-value for the exponential integral function $\mathrm{E}_1(x)$, respectively.

Now, we analyze the following limit in order to evaluate the relationship between $L(x)$ and $U(x)$

$$\lim_{x\to\infty}\frac{U(x)}{L(x)}. \quad (40)$$

From the inequality in (39) we know, the ratio of $U(x)$ and $L(x)$ is the indeterminate form $\frac{0}{0}$, which implies the limit in (40) can be evaluated by applying the L'Hôspital's rule. Thus, according to L'Hôspital's rule, this limit can be calculated as follows

$$\begin{aligned}\lim_{x\to\infty}\frac{U(x)}{L(x)} &= \lim_{x\to\infty}\frac{e^{-x}\ln\left(1+\frac{1}{x}\right)}{\frac{1}{2}e^{-x}\ln\left(1+\frac{2}{x}\right)}\\ &= 2\lim_{x\to\infty}\frac{\frac{1}{1+\frac{1}{x}}\left(1+\frac{1}{x}\right)'}{\frac{1}{1+\frac{2}{x}}\left(1+\frac{2}{x}\right)'}\\ &= \lim_{x\to\infty}\frac{x+2}{x+1}=1, \quad (41)\end{aligned}$$

where $(\cdot)'$ denotes the first-order derivative operator. The result in (41) implies, when $x\to\infty$, we have

$$L(x)\approx U(x) \quad (42)$$

Therefore, from (39) and (42), we have the following approximation

$$\mathrm{E}_1(x)\approx e^{-x}\ln\left(1+\frac{1}{x}\right),\ x>0. \quad (43)$$

In addition, Fig. 3 plots the upper ($U(x)$) and lower ($L(x)$) boundary-value curves of $\mathrm{E}_1(x)$ function. It is seen that $L(x)$ tightly converges to $U(x)$, and both of them become coincident to $\mathrm{E}_1(x)$ when x is large enough, which validates the correctness of the aforementioned analysis and the existence of the approximation in (43).

By plugging (43) into (38), we derive the approximate expression of the lower bound average secrecy capacity, given as

$$\begin{aligned}\bar{C}_{LB}(\gamma_D,\gamma_E) &\approx \ln(1+\alpha\mu_D\Omega_D)-\ln\left(1+\frac{\alpha\mu_D Y\Omega_D\Omega_E}{Y\Omega_E+\kappa\Omega_D}\right)\\ &= \ln\left(\frac{(1+\alpha\mu_D\Omega_D)(Y\Omega_E+\kappa\Omega_D)}{(1+\alpha\mu_D\Omega_D)Y\Omega_E+\kappa\Omega_D}\right). \quad (44)\end{aligned}$$

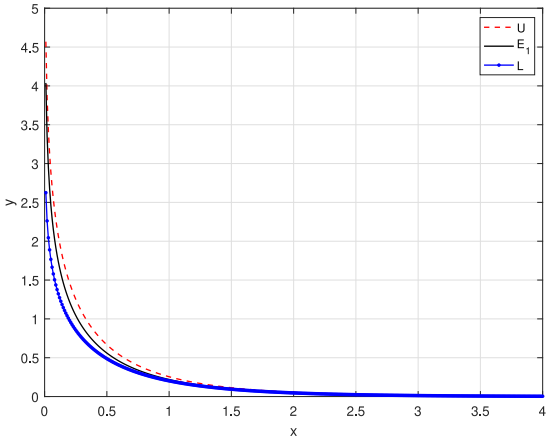

Fig. 3. Bracketing of E_1 by U and L.

Further, for $\forall z > 0$, when $z \gg 1$, the following approximation exists [56]

$$\ln(1+z) \to \ln(z). \tag{45}$$

Thus, by applying (45) to (44), the asymptotic expression of $\bar{C}_{LB}(\gamma_D, \gamma_E)$ for extreme high SINR can then be expressed as

$$\bar{C}_{LB}(\gamma_D, \gamma_E) \overset{\mu_D \to \infty}{\approx} \ln\left(1 + \frac{\kappa \Omega_D}{Y \Omega_E}\right). \tag{46}$$

IV. Secrecy Outage Performance Analysis

In this section, the secrecy outage performance is analyzed over Rayleigh fading channels. Firstly, we present the probability of nonzero secrecy capacity and secrecy outage probability, and then, the corresponding asymptotic analysis for secrecy outage probability are provided to have deep insights into the secrecy outage performance.

A. Probability of Nonzero Secrecy Capacity

When the main and eavesdropper channels experience independent Rayleigh fading, the probability of nonzero secrecy capacity is

$$\begin{aligned}
\Pr(C_s(\gamma_D, \gamma_E) > 0) &= \Pr(\gamma_D > \gamma_E) \\
&\geq \Pr\left(\gamma_D > \gamma_E^{\mathrm{up}}\right) \\
&= \int_0^{\infty} \int_0^{\gamma_D} f\left(\gamma_D, \gamma_E^{\mathrm{up}}\right) d\gamma_E^{\mathrm{up}} d\gamma_D \\
&= 1 - \int_0^{\infty} e^{-\frac{\kappa}{\alpha \mu_D \Omega_E Y} \gamma_D} f(\gamma_D) d\gamma_D \\
&= \frac{\kappa \Omega_D}{\kappa \Omega_D + Y \Omega_E}.
\end{aligned} \tag{47}$$

Since

$$\mathbf{a}^H(\theta_E, R_E)\mathbf{a}(\theta_D, R_D) = \frac{1}{N} \sum_{n=1}^{N} e^{j2\pi(n-1)\Delta\Phi(0)}, \tag{48}$$

and

$$\mathbf{a}^H(\theta_D, R_D)\mathbf{a}(\theta_E, R_E) = \frac{1}{N} \sum_{n=1}^{N} e^{-j2\pi(n-1)\Delta\Phi(0)}, \tag{49}$$

with

$$\Delta\Phi(0) = \frac{\Delta f(R_E - R_D)}{c} - \frac{1}{2}(\sin\theta_E - \sin\theta_D). \tag{50}$$

Then, we have

$$\begin{aligned}
Y &= \left|\mathbf{a}^H(\theta_E, R_E)\mathbf{a}(\theta_D, R_D)\right|^2 \\
&= \frac{1}{N} \sum_{n=1}^{N} e^{j2\pi(n-1)\Delta\Phi(0)} \cdot \frac{1}{N} \sum_{n=1}^{N} e^{j2\pi(n-1)\Delta\Phi(0)}.
\end{aligned} \tag{51}$$

To ascertain the range of Y, we examine the null points of array pattern along the distance dimension and direction dimension, respectively. We study the following expression

$$\begin{aligned}
\mathcal{J} &= \sum_{n=1}^{N} e^{-j2\pi(n-1)\Delta\Phi(0)} \\
&= \underbrace{\sum_{n=1}^{N} e^{-j2\pi(n-1)\frac{\Delta f(R_E - R_D)}{c}}}_{\mathcal{A}} \underbrace{\sum_{n=1}^{N} e^{j2\pi(n-1)\frac{1}{2}(\sin\theta_E - \sin\theta_D)}}_{\mathcal{B}}.
\end{aligned} \tag{52}$$

For distance dimension, we examine the part $\mathcal{A}$ of (52) as follows [57]

$$\begin{aligned}
\mathcal{A} &= \sum_{n=1}^{N} e^{-j2\pi\frac{\Delta f(R_E - R_D)}{c}(n-1)} \\
&= e^{-j\pi(N-1)\frac{\Delta f(R_E - R_D)}{c}} \frac{\sin\left(\pi N \frac{\Delta f(R_E - R_D)}{c}\right)}{\sin\left(\pi \frac{\Delta f(R_E - R_D)}{c}\right)}.
\end{aligned} \tag{53}$$

When $\mathcal{A} = 0$, which yields

$$\pi N \frac{\Delta f(R_E - R_D)}{c} = \pm K\pi, \ K \neq mN, \ m = 1, 2, 3, \ldots. \tag{54}$$

In the same manner, for the direction dimension, we evaluate the $\mathcal{B}$ part as

$$\begin{aligned}
\mathcal{B} &= \sum_{n=1}^{N} e^{j\pi(n-1)(\sin\theta_E - \sin\theta_D)} \\
&= e^{j\frac{\pi(N-1)(\sin\theta_E - \sin\theta_D)}{2}} \frac{\sin\left(\frac{\pi N(\sin\theta_E - \sin\theta_D)}{2}\right)}{\sin\left(\frac{\pi(\sin\theta_E - \sin\theta_D)}{2}\right)}.
\end{aligned} \tag{55}$$

By taking $\mathcal{B} = 0$, we have

$$\frac{\pi N(\sin\theta_E - \sin\theta_D)}{2} = \pm K\pi, \ K \neq mN, \ m = 1, 2, 3, \ldots. \tag{56}$$

From (54) and (56), we will get the first-null position with the assumption $K = 1$, as follows

$$R_E = R_D \pm \frac{c}{N\Delta f}, \tag{57}$$

$$\theta_E = \arcsin\left(\sin\theta_D \pm \frac{2}{N}\right). \tag{58}$$

In addition, when eavesdropper locates at the desired position, Y achieves the maximum value one. Therefore, we have the range of Y

$$0 \le Y = \left|\mathbf{a}^H(\theta_E, R_E)\mathbf{a}(\theta_D, R_D)\right|^2 \le 1. \tag{59}$$

Accordingly, the range for probability of nonzero secrecy capacity caused by eavesdropper's location is given by

$$\frac{\kappa\Omega_D}{\kappa\Omega_D + \Omega_E} \le \Pr(C_s(\gamma_D, \gamma_E) > 0) \le 1. \tag{60}$$

Note that, the minimum value in (60) occurs when the eavesdropper locates in $(\theta_D,\ R_D)$, whereas the probability one occurs when eavesdropper in the null points $(\arcsin(\sin\theta_D \pm \frac{2K}{N}),\ R_D \pm \frac{Kc}{N\Delta f})$, $K \neq mN$, $m = 1, 2, \ldots$

Next, we examine the frequency offset as it is a vital parameter in FDA related research. Since Δf should satisfy the constraint $\Delta f \ll f_0$, we consider the following case only.

When $\Delta f \to 0$, we have

$$\begin{aligned} Y &\to \frac{1}{N^2}\sum_{n=1}^{N} e^{j2\pi(n-1)\Delta\Phi_{\mathrm{PA}}(0)} \sum_{n=1}^{N} e^{j2\pi(n-1)\Delta\Phi_{\mathrm{PA}}(0)} \\ &\triangleq Y_{\mathrm{PA}}, \end{aligned} \tag{61}$$

where

$$\Delta\Phi_{\mathrm{PA}}(0) = \frac{1}{2}(\sin\theta_D - \sin\theta_E). \tag{62}$$

Comparing (50) with (62), the range-dependence property is lost, FDA scheme degenerates into the conventional phased-array scheme. It is worth noting that, this phased-array scheme corresponds to the FDA scheme when $R_E = R_D$. From (47), we have

$$\Pr(C_s(\gamma_D, \gamma_E) > 0) \to \frac{\kappa\Omega_D}{\kappa\Omega_D + Y_{\mathrm{PA}}\Omega_E}. \tag{63}$$

Note that, the minimum and maximum probability in (63) are achieved in directions $\theta_E = \theta_D$ and $\theta_E = \arcsin(\sin\theta_D \pm \frac{2K}{N})$, $K \neq mN$, $m = 1, 2, \cdots$, respectively.

Furthermore, since $Y\Omega_E/(\kappa\Omega_D) = \bar{\gamma}_E^{\mathrm{up}}/\bar{\gamma}_D$, (47) can be rewritten as

$$\Pr(C_s(\gamma_D, \gamma_E) > 0) \ge \frac{\bar{\gamma}_D}{\bar{\gamma}_E^{\mathrm{up}} + \bar{\gamma}_D}. \tag{64}$$

Remark: From (60) and (64) we know: When $\Omega_D \gg \Omega_E$ (i.e., $\bar{\gamma}_D \gg \bar{\gamma}_E^{\mathrm{up}}$), $\Pr(C_s(\gamma_D, \gamma_E) > 0) \approx 1$. Conversely, when $\Omega_D \ll \Omega_E$ (i.e., $\bar{\gamma}_D \ll \bar{\gamma}_E^{\mathrm{up}}$), $\Pr(C_s(\gamma_D, \gamma_E) > 0) \approx 0$. This means, the better the channel quality of link S $\to$ D is, the higher secrecy capacity can be obtained, and the more secure transmission can be guaranteed for the proposed FDA communications system.

B. Secrecy Outage Probability

Now, we are to derive the closed-form expression for secrecy outage probability, which is defined as the probability that the instantaneous secrecy capacity is less than a target secrecy capacity threshold C_{th} ($C_{\mathrm{th}} > 0$), which is given by [11]

$$\begin{aligned} P_{\mathrm{out}}(C_{\mathrm{th}}) &= \Pr(C_s(\gamma_D, \gamma_E) < C_{\mathrm{th}}) \\ &= \Pr\left(\frac{1+\gamma_D}{1+\gamma_E} < e^{C_{\mathrm{th}}}\right) \\ &= \Pr(\gamma_D < \gamma_E\lambda + \lambda - 1), \end{aligned} \tag{65}$$

where $\lambda = e^{C_{\mathrm{th}}}$.

When the main and eavesdropper channels experience Rayleigh fading, the secrecy outage probability is calculated as

$$\begin{aligned} P_{\mathrm{out}}(C_{\mathrm{th}}) &= \Pr(\gamma_D < \gamma_E\lambda + \lambda - 1) \\ &\le \int_0^{\infty} f\left(\gamma_E^{\mathrm{up}}\right) \int_0^{\gamma_E^{\mathrm{up}}\lambda+\lambda-1} f(\gamma_D)\, d\gamma_D\, d\gamma_E^{\mathrm{up}} \\ &= 1 - e^{-\frac{\lambda-1}{\alpha\mu_D\Omega_D}} \int_0^{\infty} e^{-\frac{\lambda}{\alpha\mu_D\Omega_D}\gamma_E^{\mathrm{up}}} f\left(\gamma_E^{\mathrm{up}}\right) d\gamma_E^{\mathrm{up}} \\ &= 1 - e^{-\frac{\lambda-1}{\alpha\mu_D\Omega_D}} \frac{\kappa\Omega_D}{\kappa\Omega_D + \lambda Y\Omega_E}. \end{aligned} \tag{66}$$

Similar to the analysis for probability of nonzero secrecy capacity, with $Y \in [0, 1]$, secrecy outage probability will vary in a range, and the maximum and minimum value can be obtained when the eavesdropper locates in $(\theta_D,\ R_D)$ and $(\arcsin(\sin\theta_D \pm \frac{2K}{N}),\ R_D \pm \frac{Kc}{N\Delta f})$, $K \neq mN$, $m = 1, 2, \ldots$, respectively. When it comes to the case $\Delta f \to 0$, the analysis is almost the same as Section IV-A.

C. Asymptotic Analysis

Here, we consider some asymptotic cases of the secrecy outage probability. It is illustrative to examine the asymptotic behavior of the secrecy outage probability for extreme high SINR μ_D. When $\mu_D \to \infty$, (66) will simplify into

$$P_{\mathrm{out}}(C_{\mathrm{th}}) \overset{\mu_D\to\infty}{\approx} \frac{\lambda Y\Omega_E}{\kappa\Omega_D + \lambda Y\Omega_E}. \tag{67}$$

Finally, we examine the asymptotic behavior of the secrecy outage probability for extreme average SINRs of the main and the eavesdropper channels. Since $Y \in [0, 1]$, when $\bar{\gamma}_D \gg \bar{\gamma}_E^{\mathrm{up}}$ (i.e., $\Omega_D \gg \Omega_E$), (66) becomes

$$P_{\mathrm{out}}(C_{\mathrm{th}}) \approx 1 - e^{-\frac{\lambda-1}{\alpha\mu_D\Omega_D}}. \tag{68}$$

Now, we intend to evaluate the secrecy outage performance in high SINR ($\mu_D \to \infty$) regime. It is well known that, when $x \to 0$, we have $1 - e^{-x} \to x$. From (68), we know that, when $\mu_D \to \infty$, $\frac{\lambda-1}{\alpha\mu_D\Omega_D} \to 0$. Therefore, we obtain the secrecy outage probability in high SINR regime, which is given as follows

$$P_{\mathrm{out}}(C_{\mathrm{th}}) \overset{\mu_D\to\infty}{\approx} \frac{\lambda - 1}{\alpha\mu_D\Omega_D}. \tag{69}$$

The outage decays as $1/\mu_D$. Conversely, when $\bar{\gamma}_D \ll \bar{\gamma}_E^{\mathrm{up}}$ (i.e., $\Omega_D \ll \Omega_E$), $P_{\mathrm{out}}(C_{\mathrm{th}}) \to 1$, and the secure transmission becomes impossible.

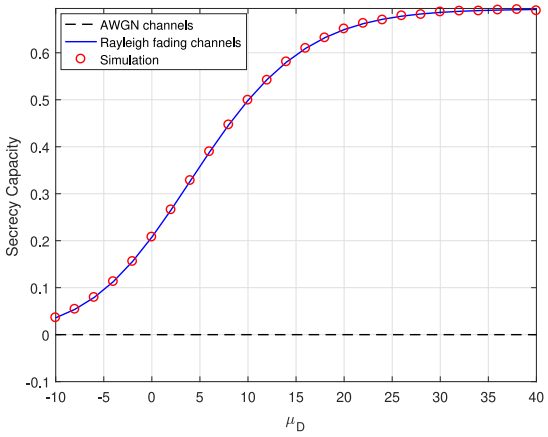

Fig. 4. Secrecy capacity comparison between AWGN and Rayleigh fading channels with D and E in (20°, 2km), where $N = 100$, $\Delta f = 10$kHz, and $\alpha = 0.8$.

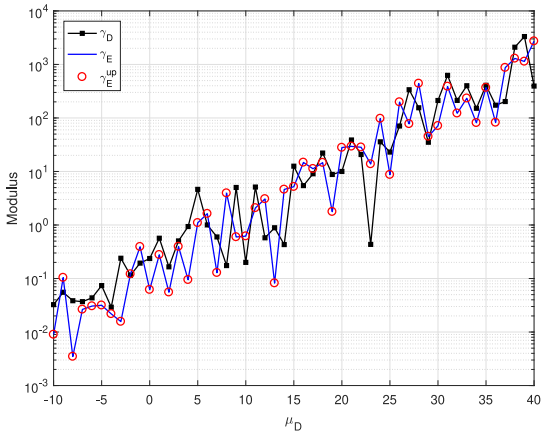

Fig. 5. Random simulation results of γ_D, γ_E and γ_E^{up}, where $N = 100$, $\Delta f = 10$kHz, $\alpha = 0.2$, and both D and E are in (20°, 2km).

V. Numerical Results and Discussions

In this section, we provide numerical results to validate the proposed analysis of the secrecy capacity and secrecy outage performance (including the probability of nonzero secrecy capacity and secrecy outage probability) for the proposed FDA communications over Rayleigh fading channels. Without loss of generality, the parameters are set to $\sigma_D^2 = \sigma_E^2 = 1$, $\Omega_D = \Omega_E = 1$, the carrier frequency is $f_0 = 10$ GHz, and the inter-element spacing is $d = c/(2f_0)$.

A. Average Secrecy Capacity Analysis

Here, we give several examples to evaluate the secrecy capacity of the proposed analysis. Fig. 4 shows the secrecy capacity versus SINR μ_D for AWGN and Rayleigh fading channels. It is observed that the simulation result matches our analytical result very well, validating the accuracy of our methodology. As anticipated, it is seen that when E is in the same location with D the secrecy capacity becomes zero under AWGN channels, while in Rayleigh fading scenario the average secrecy capacity is nonzero and increases as μ_D increases. This is because, γ_D in (13) and γ_E in (14) become the same ascending linear function of μ_D with E in D's location in AWGN channels. However, in Rayleigh fading channels, as shown in Fig. 5, they are random functions and accordingly, the secrecy capacity is nonzero.

In Fig. 6, we analyze the average secrecy capacity for two cases, being given as: (i) Case 1: E and D are in the same locations; and (ii) Case 2: E and D are in different locations. In both cases the desired receiver D is located at (20°, 2km), while E's locations are (20°, 2km) and (40°, 2km), respectively. Fig. 6 shows that our analytical results (from (38)) match the simulations very well. It is seen that the average secrecy capacity in Case 2 greatly outperforms that of Case 1 due to the fact that, in Case 2 the amplitude of useful signal received by E is lowered by the item $\mathbf{a}^H(\theta_E, R_E)\mathbf{v}$ and the artificial noise item $\mathbf{a}^H(\theta_E, R_E)\mathbf{w}$ further distorts the received signal at E, leading to a large channel capacity difference between S $\rightarrow$ D and S $\rightarrow$ E channels and, therefore, a better secure transmission for the proposed system can be achieved. In addition, the asymptotic results (from (46)) in high SINR

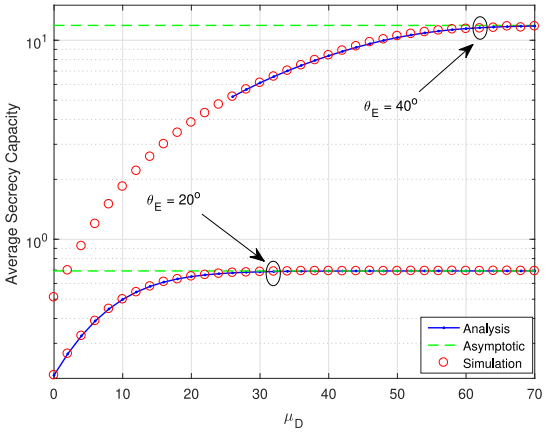

Fig. 6. Average secrecy capacity comparison versus μ_D for different angles, where $N = 100$, $\Delta f = 10$kHz, and $\alpha = 0.8$.

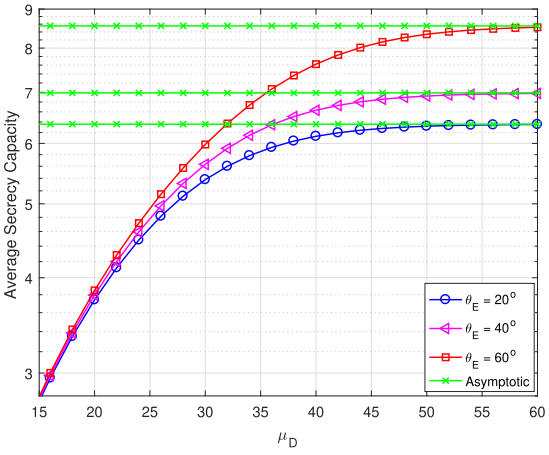

Fig. 7. Average secrecy capacity versus μ_D for different directions, where $N = 100$, $\Delta f = 10$kHz, $\alpha = 0.8$, $R_E = 3$km, and D's location is (20°, 1km).

regime, (i.e., $\mu_D \rightarrow \infty$), are also provided as upper bounds of the analysis. Note that, the asymptotic curves tightly converge to the simulations and the analytical ones in high SINR, which validates the accuracy of our analysis.

Fig. 7 (from (38) and (46)) illustrates how angles influence the average secrecy capacity in physical-layer security when D

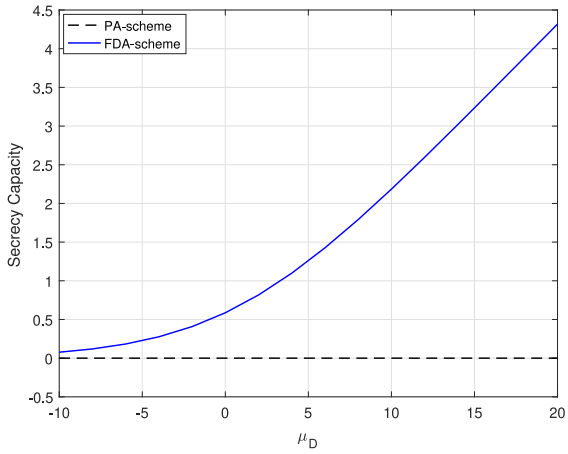

Fig. 8. Secrecy capacity versus μ_D for different schemes, where $N = 100$, $\alpha = 0.8$, D and E's locations are (20°, 2km) and (20°, 4km), respectively.

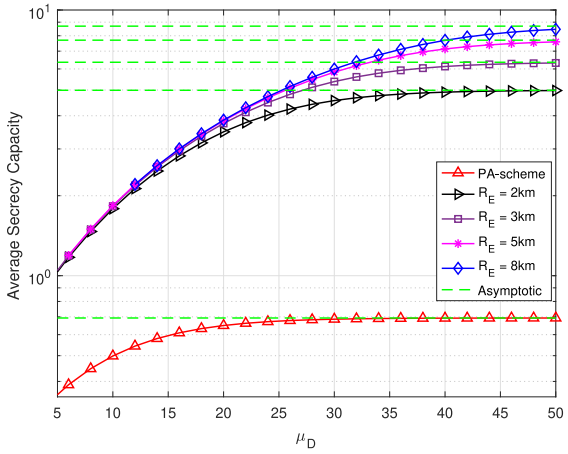

Fig. 9. Average secrecy capacity versus μ_D for different ranges, where $N = 100$, $\Delta f = 10$kHz, $\theta_D = \theta_E = 20°$, $R_D = 1$km, and $\alpha = 0.8$.

and E have different ranges with respect to the transmitter S. It is seen that, when $\theta_E = 20°$, D and E are in the same direction, the eavesdropper can obtain more useful signal, which makes the system secure performance worse than other directions. More exactly, (12) can explain the phenomenon. The scenario where D and E locate in the same direction but different ranges are examined in Figs. 8 and 9. As can be observed in Fig. 8, for the secrecy capacity analysis in AWGN, when D and E are in the same direction, the secrecy capacity for PA scheme ($\Delta f = 0$) is zero, while the FDA scheme ($\Delta f = 10$kHz) can obtain secrecy capacity and greatly outperforms that of PA scheme. This is because PA is only angle dependent and the range does not work, while FDA is dependent in both angle and range, providing a potential two-dimension security. With the assumption that D and E have the same angles $\theta_D = \theta_E = 20°$, Fig. 9 (from (38) and (46)) shows the impacts of ranges on the average secrecy capacity, where the PA scheme is also provided for comparison. It is seen that the FDA scheme outperforms the PA scheme significantly. The average secrecy capacity of PA scheme is not influenced by the varying R_E, whereas for FDA scheme, the average secrecy capacity increases along with the increasing R_E due to its range dependence property. Further, to have deep insights into the impacts of ranges on the system performance, Fig. 10 plots the average secrecy capacity versus range (R_E) with different frequency offsets. It is seen that, when the eavesdropper has the same range as the desired receiver ($R_D = 2500$m), the worst system performance appears. This worst performance corresponds to the performance of the phased-array scheme. Whereas beyond the desired receiver's point, high secure performance can be obtained, the larger the range differences between the desired receiver and the eavesdropper are, the higher secure performance will be, which significantly outperforms the phased-array scheme. As is known, it is the frequency offsets that make FDA differ from the phased-array. It is seen that, for a certain range (R_E), the system performance gets better with the increasing frequency offset. In addition, an upper bound for average secrecy capacity is provided.

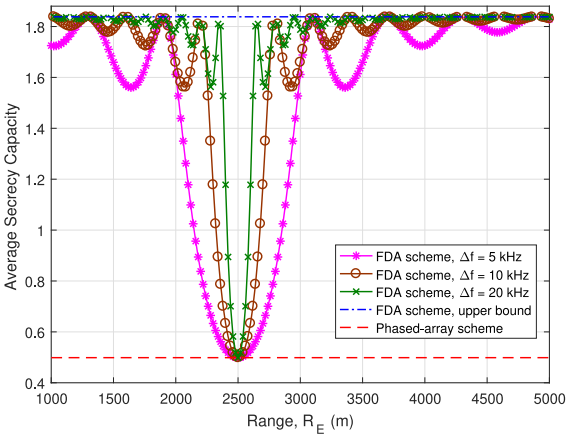

Fig. 10. Average secrecy capacity versus eavesdropper's range for different Δf, where $N = 100$, $\mu_D = 10$dB, $\theta_D = \theta_E = 20°$, and $\alpha = 0.8$.

Figs. 11 and 12 (from (38)) illustrate the average secrecy capacity versus the power allocation parameter α. The locations of D and E are set to (0°, 2km) and (5°, 200m), respectively. We observe that the average secrecy capacity in Rayleigh fading channels (the red dash line) increases with the increasing α, and the maximum secrecy capacity can be obtained when the power allocation parameter equals to one. In addition, the average secrecy capacity in AWGN channels outperforms the Rayleigh fading channels. In Fig. 11, we observe that more average secrecy capacity can be achieved for larger N because of the array gain. Moreover, the optimal α in AWGN channel increases with increasing N, which implies that the optimal power allocation parameter for AWGN channel will be achieved with the maximum N. Fig. 12 shows that the increasing μ_D brings better secrecy capacity performance to the considered system, which indicates that S can increase the total transmit power to enhance the physical-layer security. However, the optimal power allocation parameter α in AWGN decreases along with the increasing μ_D. This means that S can allocate more power to the useful signal when the total transmit power is very low.

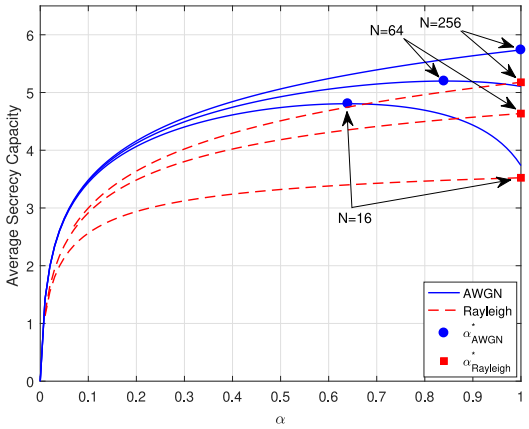

Fig. 11. Average secrecy capacity versus α for different number of array elements, where $\Delta f = 5$kHz and $\mu_D = 25$dB.

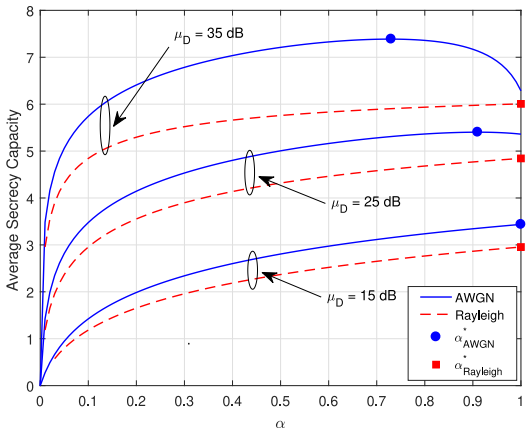

Fig. 12. Average secrecy capacity versus α for different SINR μ_D, where $\Delta f = 5$kHz and $N = 100$.

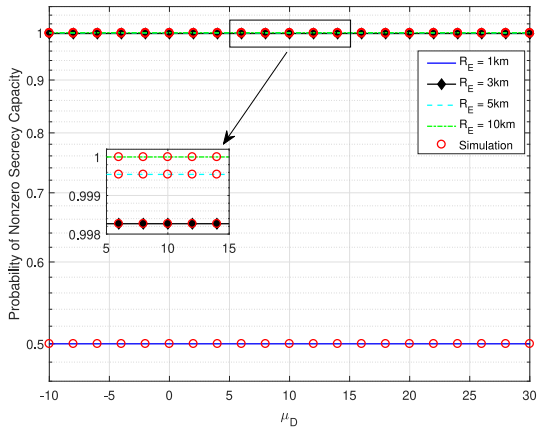

Fig. 13. Probability of nonzero secrecy capacity versus μ_D for different ranges, where $\Delta f = 10$kHz and $\alpha = 0.8$.

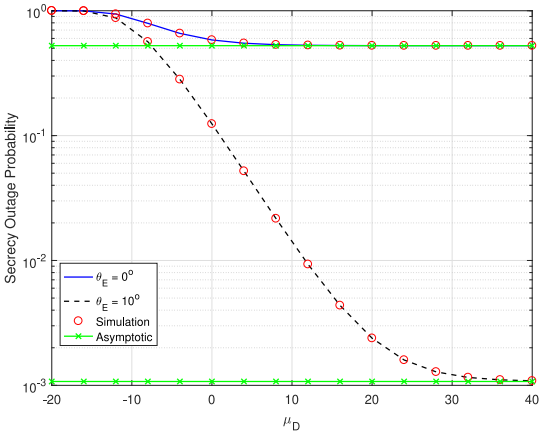

Fig. 14. Secrecy outage probability versus μ_D for different locations, where $\Delta f = 10$kHz, $R_D = R_E = 2$km, $\theta_D = 0^\circ$, $\alpha = 0.8$, and $C_{\rm th} = 0.1$.

B. Secrecy Outage Performance Analysis

Here, we provide numerical results to verify our analysis of Section IV over Rayleigh fading channels. Unless state otherwise, $N = 100$ is assumed in all simulations.

Firstly, we examine the probability of nonzero secrecy capacity. Suppose $R_D = 1$km and $\theta_D = \theta_E = 20^\circ$, the results are given in Fig. 13 (from (47)). Simulation results tightly match with the analytical ones. The probability increases along with the increasing R_E due to its range-dependent channels. When $R_E = 1$km, D and E locate in the same position, E can obtain more useful signal, thus degrading the system performance, and the minimum probability is obtained, just as being analyzed in Section IV-A. However, in other scenarios (i.e., $R_E = 3$km, 5km, 10km), the probabilities are very high but with minor differences. Note that, the large gap between the scenario $R_E = 1$km and other scenarios is mainly caused by serious distortion of useful signal received by E in the latter.

Next, we evaluate the secrecy outage probability. As expected in Fig. 14 (from (66)), when $\theta_E = 0^\circ$, D and E are in the same position and the secrecy outage probability is very high, whereas the outage probability is lower when they are in different directions. The big gap between two curves can be explained as the same reason as Fig. 6. Note that, when μ_D is large enough, the outage probability will be saturated, this phenomenon is referred to as "outage floor". The appearance of outage floor is mainly due to the constraint of the relationship between Ω_D and Ω_E, which will be further simulated in subsequent Fig. 19. In addition, the asymptotic result (from (67)) for high SINR, i.e., $\mu_D \to \infty$, is also provided in the figure as a lower bound, which is also called "floor value", of the outage probability. The floor values tightly converge to the analytical results in high SINR regime, which indicate the minimum secrecy outage probabilities can be obtained.

As FDA is dependent in both angle and range parameters, so in Fig. 15 (from (66) and (67)), we evaluate how ranges influence the secrecy outage probability. The asymptotic results are also given as the "outage floor" values to have deep insights into the range effects on the secrecy outage performance. It is seen that the outage probability decreases as R_E gets bigger and secure transmission is guaranteed, whereas the decrement is reduced along with the increasing ranges. The FDA scheme outperforms the PA scheme evidently with a large performance gap due to the range dependence.

The effects of frequency offset on the secrecy outage probability are studied in Fig. 16 (from (66) and (67)), where D and E are located at (10°, 1km) and (0°, 3km), respectively. As expected, the secrecy outage probability decreases with the increasing Δf, but the decrement is reduced as Δf gets

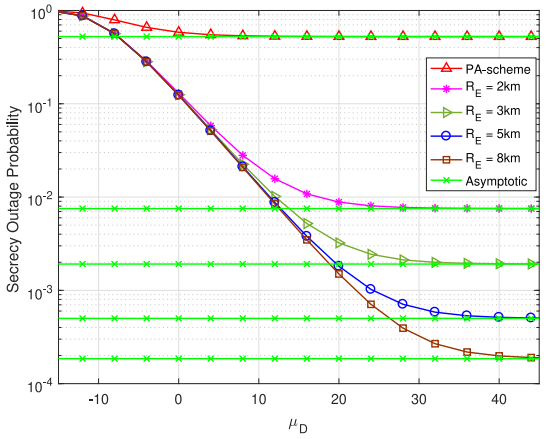

Fig. 15. Secrecy outage probability versus μ_D for different ranges, where $\Delta f = 10$kHz, $R_D = 1$km, $\theta_D = \theta_E = 20°$, $\alpha = 0.8$, and $C_{\rm th} = 0.1$.

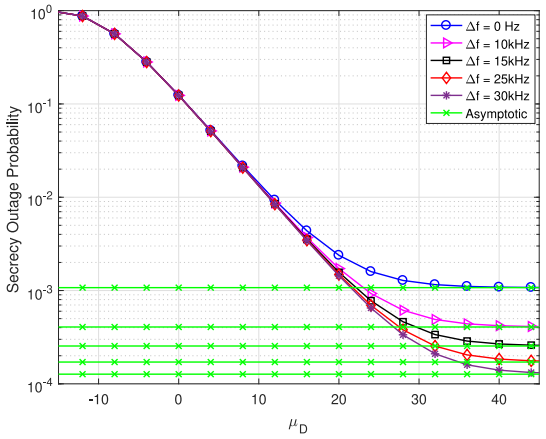

Fig. 16. Effects of frequency increment Δf on secrecy outage probability, where $\alpha = 0.8$ and $C_{\rm th} = 0.1$.

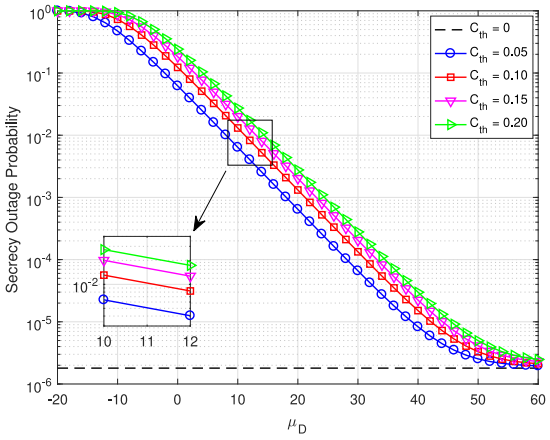

Fig. 17. Effects of secrecy capacity theshold $C_{\rm th}$ on secrecy outage probability, where $\alpha = 0.8$ and $\Delta f = 10$kHz.

bigger. When $\Delta f = 0$, the FDA scheme deteriorates into conventional PA scheme, which results in the large gap between the scenario $\Delta f = 0$ and the scenario $\Delta f = 10$kHz. This phenomenon validates again that the FDA scheme outperforms the PA scheme significantly.

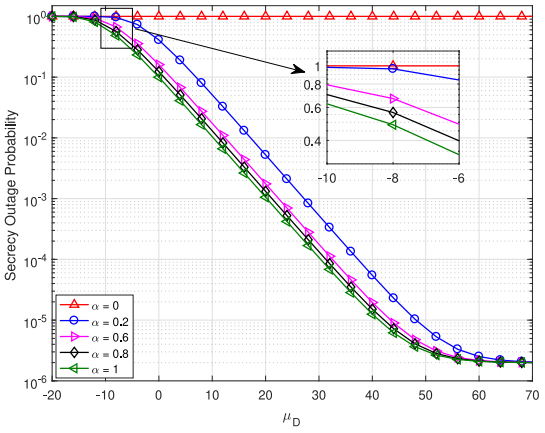

Fig. 18. Effects of power allocation parameter α on secrecy outage probability, where $C_{\rm th} = 0.1$ and $\Delta f = 10$kHz.

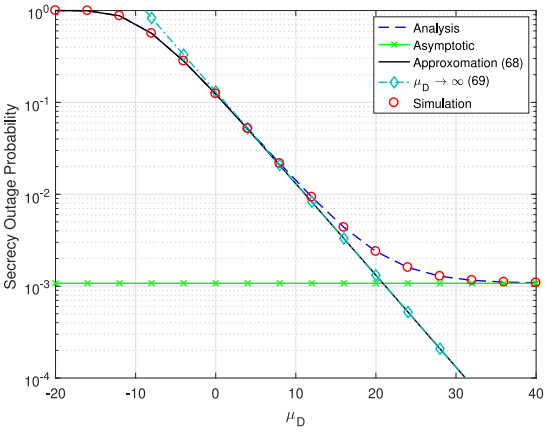

Fig. 19. Secrecy outage probability versus μ_D when $\bar{\gamma}_D \gg \bar{\gamma}_E^{\rm up}$, where $\Delta f = 10$kHz and $\alpha = 0.8$.

In Figs. 17 and 18 (from (66)), the effects of secrecy capacity threshold and power allocation parameter α on the secrecy outage probability are examined, respectively. The locations of D and E are set to (10°, 1km) and (0°, 2km), respectively. Five cases are provided in Fig. 17. The secrecy outage probability increases as the threshold $C_{\rm th}$ becomes larger, but they have the same outage floor value. The minimum outage probability is obtained at $C_{\rm th} = 0$. Fig. 18 shows that the outage probability decreases along with the increasing α. This implies that, for a fixed SINR, lower secrecy outage probability can be achieved by allocating a large fraction of its transmit power to the useful signal.

Finally, Fig. 19 provides an example to evaluate the relationship between $\bar{\gamma}_D$ and $\bar{\gamma}_E^{\rm up}$. Similar to Figs. 17 and 18, the locations of D and E are set to (10°, 1km) and (0°, 2km), respectively. It is seen that, the outage probability decays as $1/\mu_D$ and the outage floor will disappear when $\bar{\gamma}_D \gg \bar{\gamma}_E^{\rm up}$ (i.e., $\Omega_D \gg \Omega_E$) (see (68)). In this case, the channel quality of link S $\rightarrow$ D outperforms the link S $\rightarrow$ E significantly. In addition, the result of (68) in high SINR, namely, (69), is also presented as a benchmark for comparison. Obviously, in high SINR regime, the simulation result tightly converges to

$$
\begin{aligned}
F_{\gamma_{\mathrm{E}}^{\mathrm{up}}}(\gamma) &= \Pr\left(\gamma_E^{\mathrm{up}} < \gamma\right) \\
&= \Pr\left(\min\left\{\frac{\alpha Y}{\beta\left|\mathbf{a}^H(\theta_E, R_E)\mathbf{w}\right|^2}, \ \frac{\alpha\mu_D Y}{\kappa}|h_E|^2\right\} < \gamma\right) \\
&= 1 - \Pr\left(\min\left\{\frac{\alpha Y}{\beta\left|\mathbf{a}^H(\theta_E, R_E)\mathbf{w}\right|^2}, \ \frac{\alpha\mu_D Y}{\kappa}|h_E|^2\right\} > \gamma\right) \\
&= 1 - \Pr\left(\frac{\alpha Y}{\beta\left|\mathbf{a}^H(\theta_E, R_E)\mathbf{w}\right|^2} > \gamma\right)\Pr\left(\frac{\alpha\mu_D Y}{\kappa}|h_E|^2 > \gamma\right), \ \gamma > 0
\end{aligned} \tag{70}
$$

the approximate one. Therefore, we can conclude that confidential communication transmission can be achieved when $\bar{\gamma}_D \gg \bar{\gamma}_E^{\mathrm{up}}$.

VI. Conclusion

In this paper, we have investigated the physical-layer security of artificial noise aided FDA communications over Rayleigh fading channels based on the single-antenna receiver structure proposed to address the time-variance property of FDA antenna. The secrecy capacity and secrecy outage performance (including probability of nonzero secrecy capacity and secrecy outage probability) are analyzed with the derived closed-form approximate expressions. Moreover, asymptotic results are also provided to further analyze the promising FDA communication performance. All theoretical analysis are verified by extensive simulation results. Numerical results show that the range-dependence property of FDA indeed provides promising application potentials for physical-layer security communications. Future work will further investigate the physical-layer security of promising FDA communications in more complex scenarios so as to excavate the potential application of FDA antenna.

Appendix
Proof of Theorem 2

Let $Y \triangleq |\mathbf{a}^H(\theta_E, R_E)\mathbf{a}(\theta_D, R_D)|^2$. Recall the derived tight upper bound of instantaneous SINR in (21), the CDF of $\gamma_{\mathrm{E}}^{\mathrm{up}}$ can then be directly calculated by (70), which is shown at the top of this page.

For $\forall\gamma > 0$, the calculation of CDF $F_{\gamma_{\mathrm{E}}^{\mathrm{up}}}(\gamma)$ can be classified as the following two scenarios:

1) When $\frac{\alpha Y}{\beta|\mathbf{a}^H(\theta_E,R_E)\mathbf{w}|^2} < \frac{\alpha\mu_D Y}{\kappa}|h_E|^2$, i.e., $|h_E|^2 > \frac{\kappa}{\beta\mu_D|\mathbf{a}^H(\theta_E,R_E)\mathbf{w}|^2}$. There are following two possible events.
   a) If $\frac{\alpha Y}{\beta|\mathbf{a}^H(\theta_E,R_E)\mathbf{w}|^2} > \gamma$, we have $\frac{\alpha\mu_D Y}{\kappa}|h_E|^2 > \gamma$, and the following two identities can be easily obtained from the last line of (70)

$$\Pr\left(\frac{\alpha\mu_D Y}{\kappa}|h_E|^2 > \gamma\right) = 1, \tag{71}$$

$$\Pr\left(\frac{\alpha Y}{\beta\left|\mathbf{a}^H(\theta_E, R_E)\mathbf{w}\right|^2} > \gamma\right) = 1. \tag{72}$$

   By plugging (71) and (72) into (70), we then have

$$F_{\gamma_{\mathrm{E}}^{\mathrm{up}}}(\gamma) = 0. \tag{73}$$

   b) If $\frac{\alpha Y}{\beta|\mathbf{a}^H(\theta_E,R_E)\mathbf{w}|^2} \leq \gamma$, we have the following identity

$$\Pr\left(\frac{\alpha Y}{\beta\left|\mathbf{a}^H(\theta_E, R_E)\mathbf{w}\right|^2} > \gamma\right) = 0. \tag{74}$$

   By plugging (74) into (70), we have

$$F_{\gamma_{\mathrm{E}}^{\mathrm{up}}}(\gamma) = 1. \tag{75}$$

   It is worth noting that, in this scenario, the CDF derived in (73) means the eavesdropper cannot receive any information, which is impractical in a secrecy communication system due to the omnidirectional antenna elements used in the transmit array. While the result obtained in (75) implies that the system secrecy capacity is zero, and secure transmission is impossible, which is meaningless. Therefore, this scenario will not be considered in this paper.

2) When $\frac{\alpha Y}{\beta|\mathbf{a}^H(\theta_E,R_E)\mathbf{w}|^2} \geq \frac{\alpha\mu_D Y}{\kappa}|h_E|^2$, i.e., $|h_E|^2 \leq \frac{\kappa}{\beta\mu_D|\mathbf{a}^H(\theta_E,R_E)\mathbf{w}|^2}$. The following two events exist.
   a) If $\frac{\alpha Y}{\beta|\mathbf{a}^H(\theta_E,R_E)\mathbf{w}|^2} > \gamma$, we have the following identity

$$\Pr\left(\frac{\alpha Y}{\beta\left|\mathbf{a}^H(\theta_E, R_E)\mathbf{w}\right|^2} > \gamma\right) = 1. \tag{76}$$

   Substituting (76) into (70), we obtain

$$
\begin{aligned}
F_{\gamma_{\mathrm{E}}^{\mathrm{up}}}(\gamma) &= 1 - \Pr\left(\frac{\alpha\mu_D Y}{\kappa}|h_E|^2 > \gamma\right) \\
&= \Pr\left(|h_E|^2 < \frac{\kappa}{\alpha\mu_D Y}\gamma\right), \ \gamma > 0.
\end{aligned} \tag{77}
$$

   Note that, the result in (77) is conditioned under the following two constraints

$$\begin{cases} |h_E|^2 \leq \frac{\kappa}{\beta\mu_D|\mathbf{a}^H(\theta_E,R_E)\mathbf{w}|^2} \\ \gamma < \frac{\alpha Y}{\beta|\mathbf{a}^H(\theta_E,R_E)\mathbf{w}|^2}. \end{cases} \tag{78}$$

   From (77) and (78), we know $|h_E|^2$ is constrained by two upper limit values, i.e., $\frac{\kappa}{\alpha\mu_D Y}\gamma$ and $\frac{\kappa}{\beta\mu_D|\mathbf{a}^H(\theta_E,R_E)\mathbf{w}|^2}$. To further ascertain $F_{\gamma_{\mathrm{E}}^{\mathrm{up}}}(\gamma)$, we examine the relationship of $\frac{\kappa}{\alpha\mu_D Y}\gamma$ and $\frac{\kappa}{\beta\mu_D|\mathbf{a}^H(\theta_E,R_E)\mathbf{w}|^2}$. The ratio of these two parts are

calculated as follows:

$$\begin{aligned}\frac{\frac{\kappa}{\alpha\mu_D Y}\gamma}{\frac{\kappa}{\beta\mu_D|\mathbf{a}^H(\theta_E,R_E)\mathbf{w}|^2}} &= \frac{\beta\left|\mathbf{a}^H(\theta_E,R_E)\mathbf{w}\right|^2}{\alpha Y}\cdot\gamma \\ &< \frac{\beta\left|\mathbf{a}^H(\theta_E,R_E)\mathbf{w}\right|^2}{\alpha Y} \\ &\quad\times\frac{\alpha Y}{\beta\left|\mathbf{a}^H(\theta_E,R_E)\mathbf{w}\right|^2} \\ &= 1. \end{aligned} \tag{79}$$

The result in (79) demonstrates that $\frac{\kappa}{\alpha\mu_D Y}\gamma < \frac{\kappa}{\beta\mu_D|\mathbf{a}^H(\theta_E,R_E)\mathbf{w}|^2}$, which implies

$$F_{\gamma_{\mathrm{E}}^{\mathrm{up}}}(\gamma) = F_{|h_E|^2}\left(\frac{\kappa}{\alpha\mu_D Y}\gamma\right),\ \gamma>0 \tag{80}$$

Conversely, if (80) is established, we can easily get $\frac{\kappa}{\alpha\mu_D Y}\gamma < \frac{\kappa}{\beta\mu_D|\mathbf{a}^H(\theta_E,R_E)\mathbf{w}|^2}$, therefore, we write the range of γ as $\gamma>0$.

b) If $\frac{\alpha Y}{\beta|\mathbf{a}^H(\theta_E,R_E)\mathbf{w}|^2} \le \gamma$, we have the following identity

$$\Pr\left(\frac{\alpha Y}{\beta\left|\mathbf{a}^H(\theta_E,R_E)\mathbf{w}\right|^2}>\gamma\right)=0. \tag{81}$$

By plugging (81) into (70), we have

$$F_{\gamma_{\mathrm{E}}^{\mathrm{up}}}(\gamma)=1. \tag{82}$$

Similar to (75), the CDF obtained in (82) is also out of consideration in this paper.

Therefore, the CDF of $\gamma_{\mathrm{E}}^{\mathrm{up}}$ is finally given as

$$F_{\gamma_{\mathrm{E}}^{\mathrm{up}}}(\gamma) = F_{|h_E|^2}\left(\frac{\kappa}{\alpha\mu_D Y}\gamma\right),\ \gamma>0. \tag{83}$$

Here, the proof for this theorem is completed.

REFERENCES

[1] H. Fang, L. Xu, and X. Wang, "Coordinated multiple-relays based physical-layer security improvement: A single-leader multiple-followers Stackelberg game scheme," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 197–209, Jan. 2018.

[2] J. Choi, "Physical layer security for channel-aware random access with opportunistic jamming," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2699–2711, Nov. 2017.

[3] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.

[4] T. Xiong, W. Lou, J. Zhang, and H. Tan, "MIO: Enhancing wireless communications security through physical layer multiple inter-symbol obfuscation," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 8, pp. 1678–1691, Aug. 2015.

[5] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

[6] H. Moosavi and F. M. Bui, "Delay-aware optimization of physical layer security in multi-hop wireless body area networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 1928–1939, Sep. 2016.

[7] M. Zhang and Y. Liu, "Energy harvesting for physical-layer security in OFDMA networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 154–162, Jan. 2016.

[8] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 247–258, Feb. 2014.

[9] N. H. Mahmood, I. S. Ansari, P. Popovski, P. Mogensen, and K. A. Qaraqe, "Physical-layer security with full-duplex transceivers and multiuser receiver at Eve," *IEEE Trans. Commun.*, vol. 65, no. 10, pp. 4392–4405, Oct. 2017.

[10] Y. Deng, L. Wang, M. Elkashlan, A. Nallanathan, and R. K. Mallik, "Physical layer security in three-tier wireless sensor networks: A stochastic geometry approach," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1128–1138, Jun. 2016.

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

[12] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[13] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[14] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.

[15] Q. Yang, H.-M. Wang, Y. Zhang, and Z. Han, "Physical layer security in MIMO backscatter wireless systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7547–7560, Nov. 2016.

[16] J. Chen, X. Chen, W. H. Gerstacker, and D. W. K. Ng, "Resource allocation for a massive MIMO relay aided secure communication," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1700–1711, Aug. 2016.

[17] D. B. Rawat, T. White, M. S. Parwez, C. Bajracharya, and M. Song, "Evaluating secrecy outage of physical layer security in large-scale MIMO wireless communications for cyber-physical systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1987–1993, Dec. 2017.

[18] M. Nafea and A. Yener, "Secure degrees of freedom for the MIMO wiretap channel with a multi-antenna cooperative jammer," *IEEE Trans. Inf. Theory*, vol. 63, no. 11, pp. 7420–7441, Nov. 2017.

[19] F. Zhu *et al.*, "Robust beamforming for physical layer security in BDMA massive MIMO," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 775–787, Apr. 2018.

[20] H.-M. Wang, C. Wang, and D. W. K. Ng, "Artificial noise assisted secure transmission under training and feedback," *IEEE Trans. Signal Process.*, vol. 63, no. 23, pp. 6285–6298, Dec. 2015.

[21] H.-M. Wang, C. Wang, D. W. K. Ng, M. H. Lee, and J. Xiao, "Artificial noise assisted secure transmission for distributed antenna systems," *IEEE Trans. Signal Process.*, vol. 64, no. 15, pp. 4050–4064, Aug. 2016.

[22] Y. Deng, L. Wang, S. A. R. Zaidi, J. Yuan, and M. Elkashlan, "Artificial-noise aided secure transmission in large scale spectrum sharing networks," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 2116–2129, May 2016.

[23] Y. Liu, H.-W. Chen, and L. Wang, "Secrecy capacity analysis of artificial noisy MIMO channels—An approach based on ordered eigenvalues of Wishart matrices," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 617–630, Mar. 2017.

[24] W. Wang, K. C. Teh, and K. H. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1470–1482, Jun. 2017.

[25] H. Wu, X. Tao, Z. Han, N. Li, and J. Xu, "Secure transmission in MISOME wiretap channel with multiple assisting jammers: Maximum secrecy rate and optimal power allocation," *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 775–789, Feb. 2017.

[26] M. P. Daly and J. T. Bernhard, "Directional modulation technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, pp. 2633–2640, Sep. 2009.

[27] M. P. Daly, E. L. Daly, and J. T. Bernhard, "Demonstration of directional modulation using a phased array," *IEEE Trans. Antennas Propag.*, vol. 58, no. 5, pp. 1545–1550, May 2010.

[28] Y. Ding and V. F. Fusco, "A vector approach for the analysis and synthesis of directional modulation transmitters," *IEEE Trans. Antennas Propag.*, vol. 62, no. 1, pp. 361–370, Jan. 2014.

[29] W.-Q. Wang and Z. Zheng, "Hybrid MIMO and phased-array directional modulation for physical layer security in mmWave wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1383–1396, Jul. 2018.

[30] W.-Q. Wang, "Frequency diverse array antenna: New opportunities," *IEEE Antennas Propag. Mag.*, vol. 57, no. 2, pp. 145–152, Apr. 2015.

[31] W.-Q. Wang, H. C. So, and A. Farina, "An overview on time/frequency modulated array processing," *IEEE J. Sel. Topics Signal Process.*, vol. 11, no. 2, pp. 228–246, Mar. 2017.

[32] J. Xu, G. Liao, S. Zhu, L. Huang, and H. C. So, "Joint range and angle estimation using MIMO radar with frequency diverse array," *IEEE Trans. Signal Process.*, vol. 63, no. 13, pp. 3396–3410, Jul. 2015.
[33] R. Gui, W.-Q. Wang, C. Cui, and H. C. So, "Coherent pulsed-FDA radar receiver design with time-variance consideration: SINR and CRB analysis," *IEEE Trans. Signal Process.*, vol. 66, no. 1, pp. 200–214, Jan. 2018.
[34] Y. Liu, H. Ruan, L. Wang, and A. Nehorai, "The random frequency diverse array: A new antenna structure for uncoupled direction-range indication in active sensing," *IEEE J. Sel. Topics Signal Process.*, vol. 11, no. 2, pp. 295–308, Mar. 2017.
[35] Q. Li, L. Huang, H. C. So, H. Xue, and P. Zhang, "Beampattern synthesis for frequency diverse array via reweighted ℓ_1 iterative phase compensation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 54, no. 1, pp. 467–475, Feb. 2018.
[36] S. Qin, Y. D. Zhang, M. G. Amin, and F. Gini, "Frequency diverse coprime arrays with coprime frequency offsets for multitarget localization," *IEEE J. Sel. Topics Signal Process.*, vol. 11, no. 2, pp. 321–335, Mar. 2017.
[37] W.-Q. Wang and H. C. So, "Transmit subaperturing for range and angle estimation in frequency diverse array radar," *IEEE Trans. Signal Process.*, vol. 62, no. 8, pp. 2000–2011, Apr. 2014.
[38] W.-Q. Wang, "Moving-target tracking by cognitive RF stealth radar using frequency diverse array antenna," *IEEE Trans. Geosci. Remote Sens.*, vol. 54, no. 7, pp. 3764–3773, Jul. 2016.
[39] B. Chen, X. Chen, Y. Huang, and J. Guan, "Transmit beampattern synthesis for the FDA radar," *IEEE Antennas Wireless Propag. Lett.*, vol. 17, no. 1, pp. 98–101, Jan. 2018.
[40] J. Li, H. Li, and S. Ouyang, "Identifying unambiguous frequency pattern for target localisation using frequency diverse array," *Electron. Lett.*, vol. 53, no. 19, pp. 1331–1333, Nov. 2017.
[41] Y. Ding, J. Zhang, and V. Fusco, "Frequency diverse array OFDM transmitter for secure wireless communication," *Electron. Lett.*, vol. 51, no. 17, pp. 1374–1376, Aug. 2015.
[42] W.-Q. Wang, "DM using FDA antenna for secure transmission," *IET Microw. Antennas Propag.*, vol. 11, no. 3, pp. 336–345, Apr. 2017.
[43] J. Hu *et al.*, "Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays," *IEEE Access*, vol. 5, pp. 1658–1667, 2017.
[44] J. Lin, Q. Li, J. Yang, H. Shao, and W.-Q. Wang, "Physical-layer security for proximal legitimate user and eavesdropper: A frequency diverse array beamforming approach," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 3, pp. 671–684, Mar. 2018.
[45] M. Patzold, *Mobile Radio Channels*, 2nd ed. Hoboken, NJ, USA: Wiley, 2012.
[46] C. Haslett, *Essentials of Radio Wave Propagation*. Cambridge, U.K.: Cambridge Univ. Press, 2008.
[47] P.-H. Lin and E. Jorswieck, "On the fast fading Gaussian wiretap channel with statistical channel state information at the transmitter," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 46–58, Jan. 2016.
[48] M. Ozmen and M. C. Gursoy, "Secure transmission of delay-sensitive data over wireless fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 9, pp. 2036–2051, Sep. 2017.
[49] N. Yang *et al.*, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1771–1783, May 2015.
[50] Y. Lu, K. Xiong, P. Fan, Z. Zhong, and K. B. Letaief, "Coordinated beamforming with artificial noise for secure SWIPT under non-linear EH model: Centralized and distributed designs," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1544–1563, Jul. 2018.
[51] F. Zhou, Z. Chu, H. Sun, R. Q. Hu, and L. Hanzo, "Artificial noise aided secure cognitive beamforming for cooperative MISO-NOMA using SWIPT," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 918–931, Apr. 2018.
[52] A. Al-Nahari, G. Geraci, M. Al-Jamali, M. H. Ahmed, and N. Yang, "Beamforming with artificial noise for secure MISOME cognitive radio transmissions," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 1875–1889, Aug. 2018.
[53] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.
[54] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 8th ed. Amsterdam, The Netherlands: Academic, 2015.
[55] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables*. New York, NY, USA: U.S. Dept. Commerce, 1964.
[56] D. Tse and P. Viswanath, *Fundamentals of Wireless Communications*. New York, NY, USA: Cambridge Univ. Press, 2005.
[57] J. D. Kraus and R. J. Marhefka, *Antennas: For All Applications*. New York, NY, USA: McGraw-Hill, 2002.

Shilong Ji received the M.S. degree in communication and information systems from the School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo, China, in 2016. He is currently pursuing the Ph.D. degree with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu, China. His research interests include radar communication and physical layer security.

Wen-Qin Wang (M'08–SM'16) received the B.E. degree in electrical engineering from Shandong University, Shandong, China, in 2002, and the M.E. and Ph.D. degrees in information and communication engineering from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2005 and 2010, respectively.

From 2005 to 2007, he was with the National Key Laboratory of Microwave Imaging Technology, Chinese Academy of Sciences, Beijing, China. Since 2007, he has been with the School of Information and Communication Engineering, UESTC, where he is currently a Professor and the Director. From 2011 to 2012, he was a Visiting Scholar with the Stevens Institute of Technology, NJ, USA. From 2012 to 2013, he was a Hong Kong Scholar with the City University of Hong Kong, Hong Kong. From 2014 to 2016, he was a Marie Curie Fellow with Imperial College London, U.K. His research interests span the area of array signal processing and circuit systems for radar, communications, and microwave remote sensing.

Hui Chen received the B.S. degree in electronics information engineering from Southwest University for Nationalities, Chengdu, China, in 2007, and the Ph.D. degree from the Department of Electronic Engineering, University of Electronic Science and Technology of China (UESTC), Chengdu, in 2013. Since 2014, she has been with the School of Communication and Information Engineering, UESTC, where she is currently an Associate Professor. From 2011 to 2013, she was a Visiting Scholar with Columbia University, NY, USA. Her research interests include array signal processing, wireless communication, compressive sensing, and convex optimization.

Shunsheng Zhang was born in Anhui, China, in 1980. He received the Ph.D. degree in signal and information processing from the Beijing Institute of Technology in 2007.

In 2007, he joined the Research Institute of Electronic Science and Technology, University of Electronic Science and Technology of China, where he became an Associate Professor in 2009. From 2014 to 2015, he was a Visiting Scholar with the Department of Electrical and Computer Engineering, National University of Singapore. His major research interests include radar imaging (SAR/ISAR) and the application of frequency diverse array technology.