Secrecy Rate Analysis for Millimeter-wave Lens Antenna Array Transmission

Kai Wu, Wei Ni, *Senior Member, IEEE*, J. Andrew Zhang, *Senior Member, IEEE*, Ren Ping Liu, *Senior Member, IEEE*, and Y. Jay Guo, *Fellow, IEEE*

***Abstract*—Physical layer security is vital to millimeter-wave communications enabled by large-scale arrays, particularly the energy-efficient lens antenna arrays (LAAs). However, the broad application of LAAs can be hindered by the lack of a proper understanding of the secrecy performance. This letter derives an asymptotic closed-form expression for the secrecy rate of LAA, despite the critical challenges including the coupling of unknown lens beam responses. With the new secrecy rate analysis, the optimal power assignment for the legitimate transmission is achieved, leading to the maximization of LAA secrecy. This power assignment is unprecedentedly studied in LAA due to the previous absence of an analytical secrecy rate. Simulations validate the accuracy of the analysis over wide ranges of system parameters.**

***Index Terms*—Physical layer security, lens antenna array (LAA), secrecy rate, power assignment.**

I. Introduction

Physical layer security, as an effective supplement to upper-layer security techniques, has attracted increasing attention in millimeter-wave (mmWave) communications. [1]–[5]. MmWave large-scale antenna arrays can provide rich spatial degrees-of-freedom (DoFs) to interfere the potential eavesdroppers, greatly increasing difficulties for eavesdropping [5]. Due to the high energy efficiency, lens antenna array (LAA) has attracted huge interest in mmWave applications, including mobile communication, tracking and localization, and wireless power transfer [6]–[10]. However, there is very limited work on physical layer security for LAAs. In a pioneering work [4], a Rotman Fourier LAA-enabled secure transmission scheme (LAA-STS) was developed, where a single lens beam is selected for legitimate transmission, and the remaining beams are for artificial noise injection. Extensive simulations and prototype experiments were conducted in [4], while the analytical secrecy performance of LAA-STS has not been studied yet.

In a different yet relevant context, secrecy analysis has been well established for discrete antenna arrays (DAAs) which inject artificial noises towards potential eavesdroppers [1]–[3]. By weighting the transmitted signals with constant-modulus antenna weights, the central limit theorem (CLT) was invoked in [1]–[3] to approximate the artificial noises as Gaussian-distributed random variables (GRV). By evaluating the variance and mean of the GRV, the power of the artificial noise and information leakage (and hence the secrecy rate) was readily achieved; and was found to be independent of the angle-of-departure (AoD) of an eavesdropper.

The secrecy analysis can be more challenging for LAAs than for DAAs. Unlike for DAAs employing the uniform constant-modulus antenna weights, CLT cannot be applied in LAAs which weight the transmitted signals by non-uniform spatial responses of different beams [11]. As a consequence, the distribution of the LAA-injected artificial noises is hard to predict. With no prior known distribution of the artificial noise and the AoD of an eavesdropper, the power of the information leakage and the eavesdropped signal needs to be averaged over an AoD region. Moreover, the coupling of the unknown lens beam responses makes the averaging over AoDs (and further the secrecy analysis) in LAAs very challenging.

This letter provides a secrecy analysis for LAA-STS by addressing the above critical challenges. (In contrast, the state-of-the-art benchmark [4] only used simulation/prototype validation.) A key contribution of the letter is a new asymptotic closed-form expression for the secrecy rate, which is derived by exploiting the properties of the discrete Fourier transform (DFT), such as symmetry and Parseval's Theorem [12]. Another contribution of the letter is the newly unveiled impact of the allocation of legitimate transmission power on the secrecy rate of LAAs. The impact has not been captured by the previous LAA-related works due to lack of analytical expressions for the secrecy rate. As a result, an asymptotically optimal power assignment is derived to maximize the secrecy rate. Simulations validate the accuracy of our analysis. In particular, the gap between the simulated and analytical secrecy rates is less than 0.5% at the low signal-to-noise ratio (SNR) of -10 dB when the LAA dimension is larger than 16.

The rest of the letter is arranged as follows. Section II presents the system architecture of LAA-STS and the signal models for both the legitimate user and eavesdropper. Section III derives the secrecy rate and the optimal power assignment. Simulation results are provided in Section IV, followed by conclusions in Section V.

II. System Architecture and Signal Model

A. LAA-Enabled Secure Transmission Scheme

Fig. 1 illustrates the LAA-STS [4] consisting of a transmitter (Alice), a legitimate receiver (Bob) and an eavesdropper (Eave). Alice is equipped with a LAA that transmits the signal $s(k)$ to Bob via the $n^\star$-th DFT beam at symbol k,

K. Wu, J. A. Zhang, R. P. Liu and Y. J. Guo are with the Global Big Data Technologies Centre, University of Technology Sydney, Sydney, NSW 2007, Australia (e-mail: kai.wu@uts.edu.au; andrew.zhang@uts.edu.au; renping.liu@uts.edu.au; jay.guo@uts.edu.au).
W. Ni is with DATA61, CSIRO, Sydney, NSW 2122, Australia (e-mail: wei.ni@csiro.au).

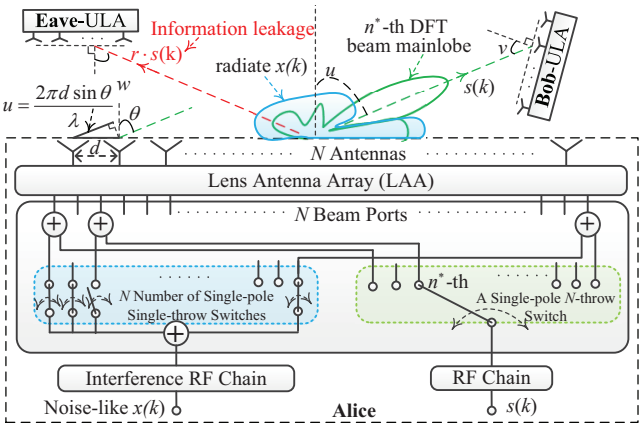

Fig. 1. The schematic diagram of the LAA-STS, where the $n^\star$-th beam is selected at Alice to send $s(k)$ to Bob, the remaining beams send $x(k)$ to the sidelobe region of the $n^\star$-th beam.

and transmits simultaneously an artificial noise $x(k)$ via the remaining DFT beams. The radio frequency (RF) chain used for transmitting $x(k)$ is referred to as "noise RF chain"; see Fig. 1. As assumed in existing studies [1]–[3], we consider that (i) a two-ray channel exists between Alice and Bob, and between Alice and Eave; (ii) the uniform linear arrays (ULAs) with M and $\tilde{M}$ antennas are installed at Bob and Eave, respectively, both performing the spatial matched filter beamforming towards their line-of-sight (LoS) paths; and (iii) Alice knows the AoD of Bob (denoted by u) but does not know the AoD of Eave (denoted by $\tilde{u}$), and Bob and Eave know the angles-of-arrival (AoAs) of the LoS paths (denoted by v and w, respectively). Here, u, $\tilde{u}$, v and w are in the beamspace domain. Taking u in Fig. 1 for an illustration, we have $u = \frac{2\pi d \sin\theta}{\lambda}$, where θ is the spatial-domain AoD, λ is the wavelength and d is the antenna spacing.

B. Signal Model

Let $\mathbb{E}\{|s(k)|^2\} = 1$ and $\mathbb{E}\{|x(k)|^2\} = 1$, and $P_{\rm T} = P + \tilde{P}$ denote the total transmission power at Alice, where P is the power of $s(k)$, and $\tilde{P}$ is the power of $x(k)$. The Rotman Fourier LAA can be represented by an $N \times N$ DFT matrix [4], denoted by $\mathbf{U}$. Thus, the precoder of Bob is $\mathbf{Ub}$, where $\mathbf{b}$ denotes the $N \times 1$ Boolean beam selection vector with $[\mathbf{b}]_{n^\star} = 1$ and $[\mathbf{b}]_n = 0, \forall n \neq n^\star$. Similarly, the precoder of Eave is $\mathbf{U}\tilde{\mathbf{b}}$, where $\tilde{\mathbf{b}} = \frac{\mathbf{1}_N - \mathbf{b}}{\sqrt{N-1}}$, $\mathbf{1}_N$ is the all-one vector, and $\frac{1}{\sqrt{N-1}}$ is due to the power splitting at the noise RF chain; see Fig. 1.

The signal received by Bob is given by $y(k) = \sqrt{P}\mathbf{w}^{\rm H}\mathbf{HUb}s(k) + \sqrt{\tilde{P}}\mathbf{w}^{\rm H}\mathbf{HU}\tilde{\mathbf{b}}x(k) + z(k)$, where $\mathbf{H} \in \mathbb{C}^{M\times N}$ is the channel matrix between Alice and Bob, $\mathbf{w} \in \mathbb{C}^{M\times 1}$ is the spatial matched filter at Bob, and $z(k)$ denotes an additive white Gaussian noise (AWGN). The two-ray channel model is given by $\mathbf{H} = \beta\mathbf{a}(v)\mathbf{a}^{\rm H}(u)$ where $\beta = \sqrt{10^{\frac{\beta_{\rm PL}}{10}}} \times \frac{1}{\sqrt{2}}\left(1 - e^{j\frac{2\pi}{\lambda}\frac{2H_{\rm T}H_{\rm R}}{D}}\right)$ is the path gain [3], [13]; $\mathbf{a}(v) \in \mathbb{C}^{M\times 1}$ is the array response vector at Bob; and $\mathbf{a}(u) \in \mathbb{C}^{N\times 1}$ is the steering vector at Alice. $\beta_{\rm PL} = \alpha + 10n\log_{10} D$ (dB) accounts for the path loss, α accounts for system losses, n is path loss exponent, and D is the distance between a transmitter-receiver pair; and $H_{\rm T}$ and $H_{\rm R}$ are the transmitter and receiver heights, respectively [3].

The spatial matched filter at Bob leads to $\mathbf{w} = \frac{1}{\sqrt{M}}\mathbf{a}(v)$, and further $\mathbf{w}^{\rm H}\mathbf{H} = \frac{\beta}{\sqrt{M}}\mathbf{a}^{\rm H}(v)\mathbf{a}(v)\mathbf{a}^{\rm H}(u) = \beta\sqrt{M}\mathbf{a}^{\rm H}(u)$. Substituting $\mathbf{w}^{\rm H}\mathbf{H}$ into $y(k)$ leads to (1), where $g(n,u) = \sum_{n'=0}^{N-1}\frac{e^{-jn'(u-\frac{2\pi n}{N})}}{\sqrt{N}}$ is the spatial response of the n-th DFT beam at u, as given by (2). $g(n^\star,u)$ is obtained by plugging $n = n^\star$ in (2). $f(\overline{n^\star},u) = \sum_{n=0,n\neq n^\star}^{N-1}\frac{g(n,u)}{\sqrt{N-1}}$ provides the sum of the spatial responses of the remaining $(N-1)$ DFT beams at u.

$$y(k) = \underbrace{\beta\sqrt{PM}g(n^\star,u)s(k)}_{y_s(k)} + \underbrace{\beta\sqrt{\tilde{P}M}f(\overline{n^\star},u)x(k)}_{y_x(k)} + z(k) \tag{1}$$

$$g(n,u) = e^{-j\frac{N-1}{2}(u-\frac{2\pi n}{N})}\frac{\sin\left[\frac{N}{2}(u-\frac{2\pi n}{N})\right]}{\sqrt{N}\sin\left[\frac{1}{2}(u-\frac{2\pi n}{N})\right]} \tag{2}$$

With reference to (1), the received signal at Eave, denoted by $\tilde{y}(k)$, is given by $\tilde{y}(k) = \tilde{y}_s(k) + \tilde{y}_x(k) + \tilde{z}(k)$, where $\tilde{y}_s(k)$ and $\tilde{y}_x(k)$ are obtained by replacing β, M and u in $y_s(k)$ and $y_x(k)$ with $\tilde{\beta}$, $\tilde{M}$ and $\tilde{u}$, respectively. Like β, we have $\tilde{\beta} = \sqrt{\frac{10^{\frac{\alpha}{10}+\tilde{D}^n}}{2}}\left(1 - e^{j\frac{2\pi}{\lambda}\frac{2H_{\rm T}\tilde{H}_{\rm R}}{\tilde{D}}}\right)$, where $\tilde{D}$ is the Alice-Eave distance and $\tilde{H}_{\rm R}$ is the receiver height of Eave.

III. Secrecy Analysis

In this section, the secrecy analysis of LAA-STS [4] is performed by first deriving the secrecy rate and then optimizing the power assignment between P and $\tilde{P}$. The secrecy rate is defined as $\mathcal{R} = \max\{\log_2(1+\gamma) - \log_2(1+\tilde{\gamma}), 0\}$ [2], where γ and $\tilde{\gamma}$ are the signal-to-interference-plus-noise ratios (SINRs) at Bob and Eave, respectively. To obtain $\mathcal{R}$, we need to derive γ and $\tilde{\gamma}$ from $y(k)$ and $\tilde{y}(k)$, respectively. In the following, Lemma 1 derives γ; and Lemmas 2 and 3 derive the power of $\tilde{y}_s(k)$ and $\tilde{y}_x(k)$, respectively. For analytical tractability, the asymptotic condition $N \to \infty$ is considered in the following derivations. This is practical, because N is typically large in mmWave communications, e.g., tens to hundreds [6], [14].

Lemma 1: *The SINR at Bob is $\gamma = PMN\gamma_0$, where $\gamma_0 = \frac{\mathbb{E}\{|\beta|^2\}}{\sigma^2}$ is referred to as the channel quality at Bob, and σ^2 is the power of $z(k)$ in (1).*

Proof: Based on (1), we can obtain

$$\gamma = \frac{\mathbb{E}\{|\beta s(k) g(n^\star,u)|^2 PM\}}{\mathbb{E}\{|z(k)|^2\} + \mathbb{E}\{|\beta\sqrt{\tilde{P}M}f(\overline{n^\star},u)x(k)|^2\}}, \tag{3}$$

where $\mathbb{E}\{|s(k)|^2\} = \mathbb{E}\{|x(k)|^2\} = 1$ and $\mathbb{E}\{|z(k)|^2\} = \sigma^2$. As considered in the original LAA-STS work [4], $u = \frac{2\pi(n^\star-1)}{N}$ is taken for Bob, leading to the following spatial orthogonality: $\left|g\left(n^\star, \frac{2\pi(n^\star-1)}{N}\right)\right|^2 = N$ and $\left|f\left(\overline{n^\star}, \frac{2\pi(n^\star-1)}{N}\right)\right|^2 = \left|\sum_{\substack{n=0\\n\neq n^\star}}^{N-1}\frac{g\left(n, \frac{2\pi(n^\star-1)}{N}\right)}{\sqrt{N-1}}\right|^2 = 0$. This is readily verified by substituting $u = \frac{2\pi(n^\star-1)}{N}$ into (2). By plugging the two results in (3), $\gamma = PMN\gamma_0$ is obtained. ■

We see from $\tilde{y}(k)$ that, to obtain $\tilde{\gamma}$, the power of $\tilde{y}_s(k)$ and $\tilde{y}_x(k)$ have to be evaluated first. As discussed in Section

I, CLT, a commonly applied technique, cannot be employed here due to the non-uniform weights of $s(k)$ and $x(k)$, i.e., $g(n,\tilde{u}),\ n\in[0,N-1]$. Moreover, given the uniformly distributed $\tilde{u}$ in the sidelobe regions of $g(n,\tilde{u})$, the analytical probability density function (PDF) of $|g(n,\tilde{u})|^2$ is mathematically intractable, since the one-to-one inverse mapping from $|g(n,\tilde{u})|^2$ to $\tilde{u}$ is unavailable. Here, we propose to calculate the average power of $\tilde{y}_s(k)$ and $\tilde{y}_x(k)$ over u using the methods presented in Lemmas 2 and 3.

Lemma 2: *Suppose that $\tilde{u}$ is randomly and uniformly distributed in the sidelobe region of the $n^\star$ DFT beam, the average power of $\tilde{y}_s(k)$ is $\tilde{P}_s=\mathbb{E}\{|\tilde{y}_s(k)|^2\}=\mathcal{K}P\tilde{M}\tilde{\sigma}_\beta^2$, where $\tilde{\sigma}_\beta^2=\mathbb{E}\{|\tilde{\beta}|^2\}$, $\mathcal{K}\cong 1-\frac{2}{\pi}\mathrm{Si}(2\pi)$, and $\mathrm{Si}(a)=\int_0^a\frac{\sin t}{t}\mathrm{d}t$.*

Proof: We see from $\tilde{y}_s(k)$, a key step of calculating $\tilde{P}_s$ is the calculation of $\mathbb{E}_{\tilde{u}}\{g(n^\star,\tilde{u})\}$, where $\mathbb{E}_{\tilde{u}}\{\cdot\}$ denotes the expectation w.r.t. $\tilde{u}$. By exploiting the properties of DFT beams (symmetry, Parseval's theorem, rotational invariance, etc. [12]), the calculation of $\mathbb{E}_{\tilde{u}}\{g(n^\star,\tilde{u})\}$ can be much simplified; see Appendix A for details. ∎

Lemma 3: *The average power of $\tilde{y}_x(k)$ can be approximated by $\tilde{P}_x=\mathbb{E}\{|\tilde{y}_x(k)|^2\}\approxeq\tilde{P}\tilde{M}\tilde{\sigma}_\beta^2$.*

Proof: See Appendix B. ∎

Despite the inapplicability of the common analysis technique, e.g., CLT, we have achieved estimation of the average power of the information leakage and eavesdropper signal in Lemmas 2 and 3, respectively. Although we consider the uniformly distributed $\tilde{u}$ in the whole sidelobe region of the $n^\star$-th DFT beam for legitimate transmission, the derivation techniques developed in Appendices A and B can be readily applied to any region of $\tilde{u}$ by altering the integral bounds in (7). Next, the above lemmas are used to derive the secrecy rate of LAA-STS.

Theorem 1: *Given a large N, the secrecy rate of LAA-STS is given by*

$$\mathcal{R}\approxeq\max\Bigg\{\underbrace{\log_2\frac{1+PMN\gamma_0}{1+\frac{\mathcal{K}P}{\tilde{P}}}}_{\bar{\mathcal{R}}},0\Bigg\}. \tag{4}$$

Proof: Based on Lemmas 2 and 3, the SINR at Eave can be given by $\tilde{\gamma}=\frac{\tilde{P}_s}{\tilde{P}_x+\tilde{\sigma}^2}\approxeq\frac{\mathcal{K}P\tilde{M}\tilde{\sigma}_\beta^2}{\tilde{P}\tilde{M}\tilde{\sigma}_\beta^2+\tilde{\sigma}^2}\approxeq\frac{\mathcal{K}P}{\tilde{P}}$, where $\tilde{\sigma}^2$ is the power of the AWGN $\tilde{z}(k)$ at Eave; and the second approximation is obtained due to $\frac{\tilde{\sigma}^2}{\tilde{M}\tilde{\sigma}_\beta^2}\approx 0$ given a large $\tilde{M}$. Plugging Lemma 1 and $\tilde{\gamma}$ into $\mathcal{R}$ leads to (4). ∎

The secrecy rate of LAA-STS is analyzed under the assumption of large N, yet the result also applies to a moderate N, as will be validated in Section IV. Also, Theorem 1 indicates that $\bar{\mathcal{R}}$ monotonically increases with respect to (w.r.t.) N, M and γ_0; however, the three parameters cannot be directly adjusted in practice. N and M are fixed once hardware is manufactured, and γ_0 relies on a specific communication scenario. On the other hand, Theorem 1 implies a strong dependence between the secrecy rate and the power assignment between Bob and Eave, which leads to Theorem 2.

Theorem 2: *If $\gamma_0>\frac{\mathcal{K}}{MNP_\mathrm{T}}$, $\bar{\mathcal{R}}(P)$ is a concave function of P, and its maximum can be achieved at $P^\star$, as given in (5), where $\bar{\mathcal{R}}(P)$ shows the explicit dependence of the secrecy rate w.r.t. P given the fixed N, M and P_T.*

$$P^\star=\frac{2P_\mathrm{T}-2\sqrt{\frac{P_\mathrm{T}\mathcal{K}(1-\mathcal{K})}{MN\gamma_0}+\mathcal{K}P_\mathrm{T}^2}}{2(1-\mathcal{K})}\overset{MN\gamma_0}{\underset{\approxeq}{\to\infty}}\frac{1-\sqrt{\mathcal{K}}}{1-\mathcal{K}}P_\mathrm{T} \tag{5}$$

Proof: Instead of directly examining the signs of the first and second derivatives of $\bar{\mathcal{R}}(P)$ (which can be mathematically intractable due to the nested functions of P in $\bar{\mathcal{R}}(P)$), we divide $\bar{\mathcal{R}}(P)$ into two sub-functions and evaluate their monotonicity. See Appendix C for details. ∎

We note that $\gamma_0>\frac{\mathcal{K}}{MNP_\mathrm{T}}$ is generally satisfied in practice, because $\frac{\mathcal{K}}{MNP_\mathrm{T}}$ is very small in mmWave communications. Taking the settings of [2] for example, $M=16$, $N=32$, $P_\mathrm{T}=37$ dBm, and hence $\frac{\mathcal{K}}{MNP_\mathrm{T}}$ is about -44.225 dB.

Our analysis can be extended to the scenarios with multiple eavesdroppers. The SINR at Bob, i.e., γ derived in Lemma 1, is unaffected by the number of eavesdroppers due to the spatial orthogonality of DFT beams [4]. Provided that the AoDs of the eavesdroppers are independently and uniformly distributed in the sidelobes of the $n^\star$-th DFT beam (selected for Bob), the derivations in Lemmas 2 and 3 are applicable to derive the power of the signal and artificial noise overheard at each eavesdropper. The SINR at any eavesdropper l, denoted by $\tilde{\gamma}_l$, is equal to $\tilde{\gamma}$, since the approximation $\frac{\tilde{\sigma}_l^2}{\tilde{M}_l\tilde{\sigma}_{\beta,l}^2}\approx 0$ holds $\forall l$, where $l\in[1,L]$ denotes the index for the eavesdropper. L is the number of eavesdroppers, and the subscript $(\cdot)_l$ denotes the corresponding variables for the l-th eavesdropper. With reference to (4), the secrecy rate in the L-eavesdropper case is $\mathcal{R}_L\approxeq\max\{\bar{\mathcal{R}}_L,0\}$, where $\bar{\mathcal{R}}_L=\log_2\frac{1+PMN\gamma_0}{\left(1+\frac{\mathcal{K}P}{\tilde{P}}\right)^L}$.

The secrecy outage probability (SOP) is another interesting secrecy performance measure, particularly when Alice has no information of Eave [15]. For LAA-STS, SOP can be readily evaluated based on the results in Lemmas 1-3. With reference to [15, eq. 14], the SOP of LAA-STS, denoted by $\mathcal{P}$, can be calculated via $\mathcal{P}=\mathbb{P}\{\bar{\mathcal{R}}(\tilde{u})<\mathcal{R}_\mathrm{T}\}$, where $\mathbb{P}\{\cdot\}$ stands for probability, $\bar{\mathcal{R}}(\tilde{u})$ is the instantaneous secrecy rate given $\tilde{u}$ (c.f., the averaged $\bar{\mathcal{R}}$ in (4)), and $\mathcal{R}_\mathrm{T}$ is the target secrecy rate. Based on Lemmas 1-3, we have $\mathcal{R}(\tilde{u})=\log_2\frac{1+\gamma}{1+\frac{\tilde{P}_s(\tilde{u})}{\tilde{P}_x+\tilde{\sigma}^2}}=\log_2\frac{1+\gamma}{1+\frac{P\tilde{M}\tilde{\sigma}_\beta^2|g(n^\star,\tilde{u})|^2}{\tilde{P}_x+\tilde{\sigma}^2}}$, where γ is provided in Lemma 1, $\tilde{P}_s(\tilde{u})=P\tilde{M}\tilde{\sigma}_\beta^2|g(n^\star,\tilde{u})|^2$ is obtained based on Lemma 2 without taking the average over $\tilde{u}$, and $\tilde{P}_x$ is proved in Lemma 3 to be spatially identical. Substituting $\mathcal{R}(\tilde{u})$ into $\mathcal{P}$ and collecting terms, we obtain

$$\mathcal{P}=\mathbb{P}\left\{|g(n^\star,\tilde{u})|^2>\frac{\left(\frac{1+\gamma}{2^{\mathcal{R}_\mathrm{T}}}-1\right)\left(\tilde{P}_x+\tilde{\sigma}^2\right)}{P\tilde{M}\tilde{\sigma}_\beta^2}\right\}. \tag{6}$$

Since the one-to-one mapping from $|g(n^\star,\tilde{u})|^2$ to $\tilde{u}$ is unavailable, deriving the analytical expression for $\mathcal{P}$ becomes mathematically intractable. Nevertheless, in Section IV, we evaluate $\mathcal{P}$ numerically to validate its accuracy in depicting the SOP of LAA-STS under practical parameter settings.

IV. Simulation Results

In this section, simulations are performed to validate the above analysis. The simulation parameters are set based on the mmWave vehicular communication scenario in [2]. In specific, $N=32$, $M=16$, $\tilde{M}=100$, $f_c=60$ GHz, $B=50$ MHz,

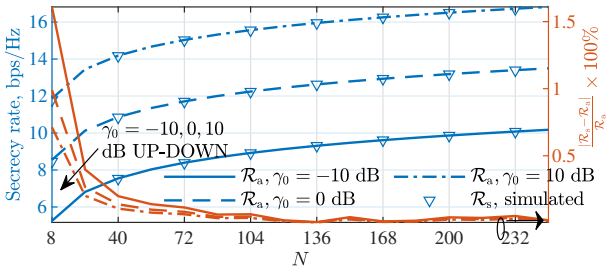

Fig. 2. Secrecy rate vs N, where $\mathcal{R}_{\rm s}$ is obtained by the scheme [4] and $\mathcal{R}_{\rm a}$ is the analytical secrecy rate given by Theorem 1.

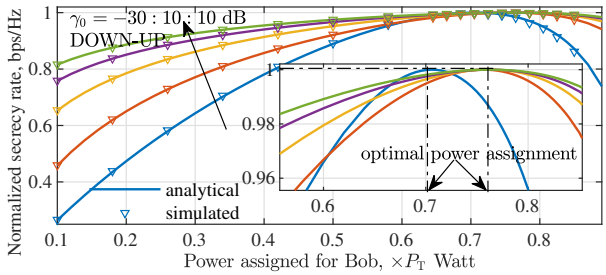

Fig. 3. Secrecy rate vs P with each curve normalized by its own maximum, where the simulated and analytical results are obtained by the scheme [4] and Theorem 2, respectively.

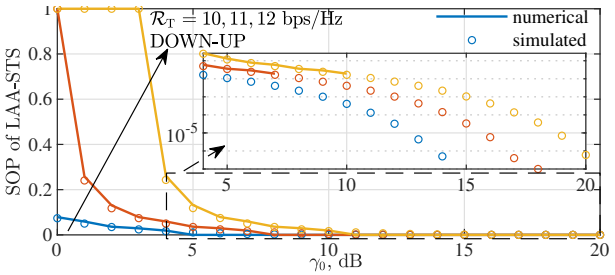

Fig. 4. SOP vs γ_0, where the analytical $\mathcal{P}$ is obtained by numerically evaluating (6) and the simulated SOP is obtained by the scheme [4].

$P_{\rm T}=37$ dBm, $H_{\rm T}=H_{\rm R}=1.5$ m, $D=50\sim500$ m, $\tilde{D}=10$ m, $u=\frac{2\pi(N-1)}{N}=6.0868$ rad, $\tilde{u}\in\mathcal{U}_{[0,\frac{2\pi(N-2)}{N}]}$, and $\tilde{\beta}\sim\mathcal{CN}(0,1)$[1]; unless otherwise specified.

Fig. 2 plots the simulated and analytical secrecy rate of LAA-STS [4], as N increases. We see that the analytical secrecy rate is able to accurately depict the performance of LAA-STS [4]. Although the analytical secrecy rate is derived under the large N assumption, we see that it also suits a moderate N, e.g., 16. As expected, we also see that the approximation error under a small N can be slightly larger due to the approximation errors in Theorem 1. Nevertheless, with a small γ_0 of -10 dB, the relative approximation error between the analytical and simulated secrecy rates is smaller than 0.5% for $N>16$.

Fig. 3 plots the normalized secrecy rate against the power assigned for Bob, i.e., P. Given the simulation parameters, we can obtain $\frac{\mathcal{K}}{MNP_{\rm T}}<-30$, and according to Theorem 2 the secrecy rate should be a concave function of P. We see that Fig. 3 validates Theorem 2 via the first increasing and then decreasing secrecy rate, as P increases from $0.1P_{\rm T}$ to $0.9P_{\rm T}$. This can be seen more clearly in the zoomed-in sub-figure, where denser power values are taken around the maximum to validate the concavity of the secrecy rate against P. Moreover, the optimal power assignment maximizing the secrecy rate is also marked in sub-figure. We see that the maximum secrecy rate is achieved at $P=0.76P_{\rm T}$ when $\gamma_0\geq-20$ dB. This is consistent with the result of Theorem 2, i.e., (5). In the case of $\gamma_0=-30$ dB, we see that the optimal power moves away from (5) slightly. This is because a very low SNR value can invalidate the asymptotic condition for (5). Figs. 2 and 3 validate the applicability and accuracy of Theorems 1 and 2 over wide ranges of N and γ_0.

Fig. 4 plots SOP against γ_0, where 10^7 independent trials are performed for both the numerical analysis of (6) and the simulation of SOP using the scheme developed in [4]. We see that the analytical SOP in (6) can accurately depict the simulated SOP of LAA-STS. We also see that SOP increases with $\mathcal{R}_{\rm T}$, but decreases as γ_0 increases, which is consistent with (6). Given its accuracy, the SOP (6) can be used to predict the secrecy performance of LAA-STS systems in practice.

Given their accuracy (as confirmed by Figs. 2-4), the new expressions for the asymptotic secrecy rate (4) and SOP (6), and the optimal power assignment (5) can be used to design parameters of LAA-STS to ensure the secrecy performance. For example, to achieve a secrecy rate of 14 bps/Hz under $P_{\rm T}=37$ dBm and $M=16$, we can use (4) and (5) to design the number of antennas at Alice to be $N\geq40$; see Fig. 2. Likewise, to achieve an SOP of less than 0.1 under $N=32$, $M=16$ and $\mathcal{R}_{\rm T}=10$ bps/Hz, we can apply (5) and (6) to design the overall transmission power of Alice to be $P_{\rm T}\geq37$ dBm; see Fig. 4.

V. Conclusions

This letter discloses the analytical secrecy performance for LAA-STS. This is achieved by deriving an analytical secrecy rate in an asymptotic closed-form expression. Is is also accomplished by unprecedentedly optimizing the power assignment between legitimate and artificial noise transmissions, hence maximizing the LAA secrecy. Simulations validate the accuracy of our analysis, e.g., less than 5% relative error between simulated and analytical secrecy rates, across wide ranges of LAA dimensions and SNRs.

In our future work, the analytical secrecy rate will be exploited to help with mmWave transceiver designs. In particular, when multiple LAAs form a larger hybrid array [16], we will study how to holistically design the array parameters to optimize the secrecy performance. We will also exploit our secrecy rate analysis to perform a comparison between LAAs and DAAs with the power consumption taken into account.

Appendix

A. Proof of Lemma 2

The average power leakage at Eave is given by $\mathbb{E}\{|\tilde{y}_s(k)|^2\}=\mathbb{E}\{|\tilde{\beta}\sqrt{P\tilde{M}}s(k)g(n^\star,\tilde{u})|^2\}=P\tilde{M}\tilde{\sigma}_\beta^2\cdot\mathbb{E}_{\tilde{u}}\{|g(n^\star,\tilde{u})|^2\}$, where $\mathbb{E}\{|s(k)|^2\}=1$ is used, and the subscript of $\mathbb{E}_{\tilde{u}}$ indicates that the expectation is taken w.r.t.

[1]The two-ray channel model adopted in this paper can be adapted for different mmWave frequencies by altering the parameters, α and n in (1), [2], [3].

$\tilde{u}$. Provided the uniformly distributed $\tilde{u}$ in the sidelobe region of the $n^\star$-th DFT beam, $\mathbb{E}_{\tilde{u}}\{|g(n^\star,\tilde{u})|^2\}$ is identical $\forall n^\star$ due to the rotational invariance of DFT beams [12]. Without loss of generality, we can take $n^\star=0$ and simplify the calculation of $\mathbb{E}_{\tilde{u}}\{|g(n^\star,\tilde{u})|^2\}$ as

$$\mathbb{E}_{\tilde{u}}\{|g(n^\star,\tilde{u})|^2\}=\underbrace{\frac{N}{2\pi(N-2)}\int_0^{2\pi}|g(0,u)|^2\mathrm{d}u}_{\mathcal{E}_1}-\underbrace{\frac{N}{2\pi(N-2)}\cdot 2\times\int_0^{\frac{2\pi}{N}}|g(0,u)|^2\mathrm{d}u}_{\mathcal{E}_2}\overset{N}{\underset{\to\infty}{\approx}}1-\frac{2}{\pi}\mathrm{Si}(2\pi) \quad (7)$$

where $\mathcal{E}_1 \overset{N\to\infty}{\approx} 1$ can be derived based on the Parseval's Theorem [17, Appendix D]; and $\mathcal{E}_2$ can be calculated as

$$\begin{aligned}\mathcal{E}_2 &\overset{N}{\underset{\to\infty}{\approx}}\frac{1}{\pi}\int_0^{\frac{2\pi}{N}}\frac{\sin^2\frac{Nu}{2}}{N\sin^2\frac{u}{2}}\mathrm{d}u\approxeq\frac{1}{\pi}\int_0^{\frac{2\pi}{N}}\frac{\sin^2\frac{Nu}{2}}{N(\frac{u}{2})^2}\mathrm{d}u\\&=\frac{2}{\pi}\int_{u=0}^{\frac{2\pi}{N}}\frac{\sin^2\frac{Nu}{2}}{(\frac{Nu}{2})^2}\mathrm{d}\frac{Nu}{2}\overset{t:=\frac{Nu}{2}}{=\!=}\frac{2}{\pi}\int_0^{\pi}\frac{\sin^2 t}{t^2}\mathrm{d}t=\frac{2}{\pi}\mathrm{Si}(2\pi),\end{aligned} \quad (8)$$

where the last equality is due to $\int_0^x(\frac{\sin t}{t})^2\mathrm{d}t=\mathrm{Si}(2x)-\frac{\sin^2 x}{x}$ [18] and $\sin\pi=0$. This concludes the proof.

B. Proof of Lemma 3

The average power of $\tilde{y}_x(k)$ is $\mathbb{E}\{|\tilde{y}_x(k)|^2\}=\mathbb{E}\left\{\left|\tilde{\beta}\sqrt{\tilde{P}\tilde{M}}f(\overline{n^\star},\tilde{u})x(k)\right|^2\right\}=\tilde{P}\tilde{M}\times\tilde{\sigma}_\beta^2\times\mathbb{E}_{\tilde{u}}\{|f(\overline{n^\star},\tilde{u})|^2\}$. Based on (2), we have $\lim_{N\to\infty}\mathbb{E}_{\tilde{u}}\{|f(\overline{n^\star},\tilde{u})|^2\}=\lim_{N\to\infty}\frac{|g(\tilde{n}^\star,\tilde{u})|^2}{N-1}=\lim_{N\to\infty}\frac{N}{N-1}=1$, since $\lim_{N\to\infty}|g(\tilde{n}^\star,\tilde{u})|^2=N$ and $\lim_{\substack{N\to\infty\\ n\neq\tilde{n}^\star}}g(n,\tilde{u})=0$ given $\lim_{N\to\infty}\tilde{u}=\frac{2\pi\tilde{n}^\star}{N}$ $(\forall\tilde{n}^\star\in[0,N-1],\ \tilde{n}^\star\neq n^\star)$. This leads to $\tilde{P}_x$ in Lemma 3, and concludes the proof.

C. Proof of Theorem 2

The proof can be established by analyzing the monotonicity of $\bar{\mathcal{R}}(P)$ w.r.t. P. From (4), $\bar{\mathcal{R}}(P)=\mathcal{R}_1(P)-\mathcal{R}_2(P)$, where $\mathcal{R}_1(P)=\log_2(1+PMN\gamma_0)$ and $\mathcal{R}_2(P)=\log_2(1+\frac{\mathcal{K}P}{\bar{P}})$. The first derivatives of $\mathcal{R}_1(P)$ and $\mathcal{R}_2(P)$ w.r.t. P can be given by

$$\mathcal{R}_1'(P)=\frac{\mathrm{d}\mathcal{R}_1(P)}{\mathrm{d}P}=\frac{MN\gamma_0}{(1+PMN\gamma_0)\ln 2}; \quad (9a)$$

$$\mathcal{R}_2'(P)=\frac{\mathrm{d}\mathcal{R}_2(P)}{\mathrm{d}P}=\frac{\mathcal{K}P_\mathrm{T}}{(P_\mathrm{T}-P+\mathcal{K}P)(P_\mathrm{T}-P)\ln 2}. \quad (9b)$$

From (9), we obtain (10) and (11), where "$\uparrow$" and "$\downarrow$" denote "monotonically increasing" and "monotonically decreasing", respectively.

$$P\uparrow\Longrightarrow\ \mathcal{R}_1'(P)\downarrow\ \text{and}\ \mathcal{R}_2'(P)\uparrow\Longrightarrow\ \bar{\mathcal{R}}'(P)\downarrow \quad (10)$$

$$\mathcal{R}_2'(P)\to\infty\ \text{as}\ P\to P_\mathrm{T} \quad (11)$$

From (10), the second derivative of $\bar{\mathcal{R}}(P)$ w.r.t. P, denoted by $\bar{\mathcal{R}}''(P)$, satisfies $\bar{\mathcal{R}}''(P)<0$. By applying the second order condition of concave functions, we confirm that $\bar{\mathcal{R}}(P)$ is a concave function of P. The maximum of $\bar{\mathcal{R}}(P)$ can be achieved in two different cases.

(i) In the case of $\mathcal{R}_1'(0)\leq\mathcal{R}_2'(0)$, $\bar{\mathcal{R}}(P)$ decreases, as P becomes larger. This is because $\bar{\mathcal{R}}'(P)<\mathcal{R}_1'(0)-\mathcal{R}_2'(0)\leq 0$, according to (10). By substituting $P=0$ into (9), $\mathcal{R}_1'(0)\leq\mathcal{R}_2'(0)$ and then $\gamma_0\leq\frac{\mathcal{K}}{MNP_\mathrm{T}}$.

(ii) In the case of $\mathcal{R}_1'(0)>\mathcal{R}_2'(0)$, i.e., $\gamma_0>\frac{\mathcal{K}}{MNP_\mathrm{T}}$, we have $\bar{\mathcal{R}}'(0)=\mathcal{R}_1'(0)-\mathcal{R}_2'(0)>0$; and $\bar{\mathcal{R}}'(P_\mathrm{T})=\mathcal{R}_1'(P_\mathrm{T})-\mathcal{R}_2'(P_\mathrm{T})<0$, since $\mathcal{R}_1'(P_\mathrm{T})$ is a limited value based on (9a) whereas $\mathcal{R}_2'(P_\mathrm{T})\to\infty$; see (10). Combining with (10), we know that there exists such a $P^\star$ that $\bar{\mathcal{R}}'(P^\star)=0$. Based on (9), $P^\star$ can be solved, leading to (5). The proof is concluded.

REFERENCES

[1] N. Valliappan, A. Lozano, and R. W. Heath, "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3231–3245, August 2013.

[2] M. E. Eltayeb *et al.*, "Enhancing secrecy with multiantenna transmission in millimeter wave vehicular communication systems," *IEEE Trans. Veh. Techn.*, vol. 66, no. 9, pp. 8139–8151, Sep. 2017.

[3] Y. Hong, X. Jing, and H. Gao, "Programmable weight phased-array transmission for secure millimeter-wave wireless communications," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 2, pp. 399–413, May 2018.

[4] Y. Zhang, Y. Ding, and V. Fusco, "Sidelobe modulation scrambling transmitter using Fourier Rotman lens," *IEEE Trans. Antennas Propag.*, vol. 61, no. 7, pp. 3900–3904, July 2013.

[5] X. Chen *et al.*, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, Secondquarter 2017.

[6] X. Gao, L. Dai, and A. M. Sayeed, "Low RF-complexity technologies to enable millimeter-wave MIMO with large antenna array for 5G wireless communications," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 211–217, April 2018.

[7] A. Shahmansoori *et al.*, "Tracking position and orientation through millimeter wave lens MIMO in 5G systems," *CoRR*, vol. abs/1809.06343, 2018. [Online]. Available: http://arxiv.org/abs/1809.06343

[8] S. A. Shaikh and A. M. Tonello, "Localization based on angle of arrival in EM lens-focusing massive MIMO," in *2016 IEEE 6th ICCE-Berlin*, Sep. 2016, pp. 124–128.

[9] K. Wu *et al.*, "Efficient Angle-of-Arrival estimation of lens antenna arrays for wireless information and power transfer," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 1, pp. 116–130, Jan 2019.

[10] K. Wu *et al.*, "Exploiting spatial-wideband effect for fast AoA estimation at lens antenna array," *IEEE J. Sel. Topics Signal Process.*, pp. 1–1, 2019.

[11] W. Feller, *An introduction to probability theory and its applications*. John Wiley & Sons, 2008, vol. 2, ch. 5. Variable Distributions.

[12] A. V. Oppenheim, *Discrete-time signal processing*. Pearson Education India, 1999.

[13] M. R. Akdeniz, Y. Liu, M. K. Samimi, S. Sun, S. Rangan, T. S. Rappaport, and E. Erkip, "Millimeter wave channel modeling and cellular capacity evaluation," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1164–1179, June 2014.

[14] J. A. Zhang *et al.*, "Massive hybrid antenna array for millimeter-wave cellular communications," *IEEE Wireless Commun.*, vol. 22, no. 1, pp. 79–87, 2015.

[15] H. Lei *et al.*, "Performance analysis of physical layer security over generalized-K fading channels using a mixture Gamma distribution," *IEEE Commun. Lett.*, vol. 20, no. 2, pp. 408–411, Feb 2016.

[16] K. Wu *et al.*, "Expeditious estimation of angle-of-arrival for hybrid Butler matrix arrays," *IEEE Trans. Wireless Commun.*, vol. 18, no. 4, pp. 2170–2185, April 2019.

[17] K. Wu *et al.*, "Fast and accurate estimation of angle-of-arrival for satellite-borne wideband communication system," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 2, pp. 314–326, Feb 2018.

[18] (2011, Dec.) Sinc-squared function. [Online]. Available: https://calculus.subwiki.org/wiki/Sinc-squared_function