IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 6 February 2023, accepted 19 February 2023, date of publication 3 March 2023, date of current version 9 March 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3252503

RESEARCH ARTICLE

Cooperative Beamforming With Artificial Noise Injection for Physical-Layer Security

GEUNYEONG JANG[1], (Graduate Student Member, IEEE), DONGHYEON KIM[1], (Graduate Student Member, IEEE), IN-HO LEE[2], (Senior Member, IEEE), AND HAEJOON JUNG[1], (Senior Member, IEEE)

[1]Department of Electronics and Information Convergence Engineering, Kyung Hee University, Yongin-si 17104, South Korea
[2]School of Electronic and Electrical Engineering, Hankyong National University, Anseong 17579, South Korea

Corresponding authors: Haejoon Jung (haejoonjung@khu.ac.kr) and In-Ho Lee (ihlee@hknu.ac.kr)

This work was supported in part by the Korean Government [Ministry of Science and ICT (MSIT)] under the National Research Foundation of Korea (NRF) under Grant NRF-2021M1A2A2061357, Grant NRF-2022R1F1A1065367, Grant NRF-2022R1A4A3033401, and Grant NRF-2022R1A2C1003388; and in part by the Information Technology Research Center (ITRC) Support Programs under Grant IITP-2021-0-02046.

ABSTRACT In the sixth-generation (6G) communications, how to deploy and manage massively connected Internet-of-Things (IoT) nodes will be one of the key technical challenges, because 6G is expected to provide 10 times higher connection, compared to 5G. At the same time, due to the sharp growth in connected devices and newly adopted technologies, learning-based attacks and big data breaches are expected to occur more frequently. With the advances of quantum computing in the future, conventional cryptography-based security protocols may be obsolete in the future wireless networks, which makes physical layer security (PLS) an attractive alternative or complement for secure communications. In this context, cooperative beamforming (CB)-based PLS schemes are known to be effective solutions to guarantee high secrecy rate with IoT devices, which have limited power and hardware complexity. However, the existing CB-based PLS algorithms suffer from extremely low secrecy rate, in case that eavesdroppers are close to the intended receiver. To overcome such critical issue, in this paper, we propose a CB-based PLS with artificial noise (AN) injection, which can be realized in a fully distributed manner to minimize the overhead in the IoT networks with a large number of devices. We analyze the array factor using the virtual antenna array (VAA) created by the proposed PLS algorithm. Then, the secrecy rate is derived in a closed-form expression, which can be used to optimize the performance for given system parameters in both the absence and presence of channel state information (CSI) error. The proposed scheme provides considerably higher secrecy rate compared to the conventional CB-based PLS schemes, when an eavesdropper exists near to the intended receiver. Furthermore, through simulation and numerical results, we show that the secrecy rate of the proposed scheme can be maximized by adjusting the ratio between the data beamformer and AN injection beamformer components. As a result, the proposed method shows a performance improvement of up to two times compared to the conventional CB-based PLS schemes, in terms of the secrecy rate. Such performance gain increases as the angular location of Eve becomes closer to that of Bob, which corresponds to the most vulnerable situation of the conventional CB-based PLS algorithms.

INDEX TERMS Physical layer security, distributed beamforming, cooperative beamforming, artificial noise.

I. INTRODUCTION

The sixth-generation (6G) mobile communication systems will seamlessly integrate terrestrial and non-terrestrial networks, which will provide more reliable and faster services to a more number of devices, while satisfying stringent requirements for extremely low latency [1], [2], [3]. However, considering its higher degree of operational flexibility and autonomy to achieve disruptive connectivity, 6G is expected to face unprecedented security challenges [4].

The associate editor coordinating the review of this manuscript and approving it for publication was Chan Hwang See.

Moreover, in addition to traditional security issues, learning-based attacks and big data breaches are incurred more frequently because of the sharp increment in connected devices and newly adopted technologies [5]. Also, with the advances of quantum computing in the future, the conventional cryptography-based security protocols may be obsolete in the future wireless networks [6]. For this reason, physical layer security (PLS), based the inherent randomness of wireless medium, can complement or replace the traditional security solutions in the 6G networks, providing intrinsic contextual and entropic richness [7].

For the 6G visions to better support and activate object-oriented communications, various research are investigating revolutionary transmission techniques, network architectures (e.g., O-RAN, softwarization, and virtualization), and diverse frequency bands [8]. Along these lines, the authors in [9], [10], and [11] present how to exploit 6G key technologies to further enhance PLS and at the same time satisfy 6G key performance indicator (KPI) requirements. For example, intelligent reflecting surface (IRS) technology, which can reconfigure channels in the presence of the significant path attenuation at millimeter wave (mm-Wave) and subterahertz (sub-THz) frequency bands, is combined with PLS to enable highly secure communications, as in [4], [12], and [13]. Moreover, cell-free massive multiple-input-multiple-output (CF-mMIMO) systems, where multiple access points jointly transmit to users using the same wireless resources, are expected to effectively protect against eavesdropping attacks with improved spectral efficiency [14], [15], [16], [17]. In addition, PLS schemes are applied to different frequency bands, all of which are equally important to meet the peak data rate of 1 Tbps envisioned in 6G, including mm-Wave [18], [19], [20], [21], [22], sub-THz [23], [24], [25], [26], and visible light spectra [27], [28], [29].

6G is expected to provide 10 times higher connection, compared to 5G. Therefore, how to deploy and manage massively connected Internet-of-Things (IoT) nodes will be one of the key technical challenges [8], [30]. Massive IoT scenarios targeting for 6G will involve more than 75 billion devices by 2025, according to the Global System for Mobile Communications Association [1]. On the top of that, such IoT devices are typically battery-powered and low-complexity nodes such as sensors and actuators; thus, they inherently suffer from short transmission ranges and limited capabilities to employ sophisticated protocols. For this reason, the conventional cryptography approaches with security key management and distribution are not appropriate for the massive IoT or massive machine-type communications (mMTC) [31].

Therefore, in such networks, PLS can be an effective complement or alternative to the conventional security solutions in the 6G era. It is noted that due to the space and power limitations of IoT nodes, multiple antennas cannot be accommodated, even though the PLS schemes with an antenna array are capable to transmit the desired information only to an intended receiver, while eavesdroppers may suffer from artificial noise (AN), as discussed in [32] and [33]. In this situation, cooperative beamforming, where multiple IoT devices create a virtual antenna array (VAA) together, can be employed to achieve selective information transmissions.

Because of its effectiveness in the massive IoT networks, the authors in [34], [35], and [36] propose a cooperative beamforming (CB), which does not require channel state information (CSI) and precoding vector sharing, because each VAA element can align its phase in a fully distributed manner. Using such CB-based PLS methods, the radiation pattern is randomized, which is observed as a noise-like signal (or AN) to eavesdroppers, at the cost of the slight degradation in the array factor at the main lobe directed to the intended receiver. An open-loop implementation of the CB-based PLS, where each element aligns its phase using its own location and the angular location of the intended receiver, is investigated in [37], where the impact of phase synchronization error on the secrecy rate is also analyzed. Similarly, a cooperative null steering beamformer is proposed in [38] to minimize the information leakage to an eavesdropper. Moreover, in [39], multiple unmanned aerial vehicles (UAVs) construct a VAA together for CB-based PLS, whereas the authors in [40] analyze the secrecy energy efficiency for a group of UAVs, which are randomly changing their locations.

Furthermore, the authors in [41] and [42] propose novel cooperative jamming schemes through power synthesis. The crucial idea is to nullify the synthesis of jamming powers transmitted by multiple friendly jammers at the desired receiver; thus, it can provide high secrecy rate without requiring the CSI of Eve. Moreover, the authors in [43] consider cooperative jamming in a two-tier 5G heterogeneous network and propose three secure transmission algorithms respectively applied in different tiers. In addition, in [44], they analyze various jamming strategies under different assumptions of CSI and show that jamming with multiple jammers is effective to maximize both jamming coverage and jamming efficiency.

Different from [20], [41], [42], [43], and [44], we consider a CB-based PLS, as in [34], [35], [36], [37], [38], [39], and [40], assuming that a single node cannot reach the intended receiver, while CB can significantly extend the transmission range by constructing a VAA. Moreover, our work is distinct from the existing CB-based PLS in [34], [35], [37], [36], [38], [39], and [40], because we propose a combination of data transmission beamformer for the intended receiver and AN injection beamformer for the potential location of Eve. Because nodes are randomly selected for each TTI, it is challenging to collect CSI of all the VAA elements and share the computed precoding weights, which incur prohibitively large overhead. To alleviate such limitations in distributed IoT networks, we propose to utilize the statistical information of the CSI to realize the CB-based AN injection scheme in a fully decentralized manner. Accordingly, the CSI collection and precoding weight shared by a cluster head are not required in our proposed scheme.

In spite of the effectiveness of the conventional CB-based schemes, as revealed in the analytical and simulation results in [34], [35], [36], [37], [38], [39], and [40], they suffers from extremely low secrecy rate when the desired receiver and an eavesdropping node are in close proximity to each other. In particular, in the far-field scenario, where the distance to the intended receiver is significantly longer than the size of the VAA cluster, the secrecy rate becomes almost zero, whenever an eavesdropper is adjacent to the intended receiver in the angular direction. In other words, the existing CB-based PLS in [34], [35], [36], [37], [38], [39], and [40] is highly vulnerable, in case that the angular direction of the main lobe is known to an eavesdropper with mobility, which can move itself to breach the randomized radiations created at the non-receiver directions.

In IoT networks that require huge overhead to share the CSI and precoding vectors of nodes, we propose a fully distributed CB using the statistical properties of the stochastic VAAs, which is distinct from the existing AN-aided PLS schemes. The proposed scheme employs a precoder consisting of a data transmission beamformer and an AN injection beamformer to maximize the secrecy performance by appropriately adjusting the ratio of the two beamformers in highly vulnerable situations, where the eavesdropper is near the intended receiver. In addition, we derive a closed-form expression by analyzing the secrecy rate of the proposed scheme, so that it is possible to maximize the secrecy performance by optimizing the parameters. Furthermore, we investigate the impact of the CSI to reflect the practical implementation of the system. The key contributions of this paper are summarized as follows:

- We first propose a CB-based PLS scheme with AN injection to jam an eavesdropper, which can be realized in a fully distributed fashion. The key idea is to exploit the statistical characteristics of CB links instead of requiring CSI collection by a cluster head and computed precoding weight sharing. Also, the proposed precoder consists of the data transmission beamformer and the AN injection beamformer. We show that by adjusting the ratio of the two (i.e., desired information towards the intended receiver and AN injection to the potential location of the eavesdropper). In this way, the proposed method can considerably enhance the secrecy rate compared to the existing schemes in [34], [35], [36], [37], [38], [39], and [40] for the eavesdropping attacks at angular locations near the desired receiver.
- Considering randomly and uniformly distributed VAA elements at different transmit time intervals (TTIs), we derive the statistical characteristics of the array factor of VAA at an arbitrary location of a receiver, which can be used to characterize the received signal of both intended and unintended receivers.
- The secrecy rate of our proposed scheme is analyzed, by which a closed-form expression is derived. The derived secrecy rate shows the effectiveness of our proposed method to fix the inherent vulnerability of the existing CB-based PLS schemes at the neighboring angles of the intended receiver. Further, based on the excellent correlation of analytical and simulation results, our analysis can provide good design insights to optimize system parameters to maximize the secrecy rate.
- To consider the practical realization of the proposed scheme, we characterize the array factor statistics under the CSI estimation error. Further, the secrecy rate with imperfect CSI is derived, which is subject to the signal-to-noise ratio (SNR) of the phase-locked loop (PLL) for the channel estimation.
- Through simulations, the impacts of key system parameters are investigated such as the angular location of the unintended receiver relative to the intended receiver, the AN injection angle and degree, the number of VAA elements, and the size of the VAA cluster. In particular, the secrecy rate of our proposed method can be optimized by adjusting the degree of AN injection.

The rest of this paper is organized as follows. In Section II, we introduce the system model, whereas in Section III, practical challenges in the CB-based AN injection are identified. In Section IV, we propose a fully distributed PLS scheme with the AN injection using statistical characteristics of the array factor. We analyze the secrecy rate of our proposed scheme with perfect CSI in Section V and further analyze the secrecy rate under imperfect CSI in Section VI. Section VII presents both simulation and numerical results to delve into the impacts of various system parameters. Lastly, this paper is concluded in Section VIII.

Notations: A matrix and a column vector are denoted by boldface upper- and lower-case letters (e.g. $\mathbf{A}$ and $\mathbf{a}$), respectively. In addition, the statistical average and variance are denoted by $\mathbb{E}[\cdot]$ and $\mathbb{V}\text{ar}[\cdot]$, respectively. Furthermore, $\mathbf{a}^T$ is the transpose of $\mathbf{a}$, whereas $\mathbf{a}^H$ is the conjugate transpose. Lastly, $\mathcal{R}\{a\}$ and $\mathcal{I}\{a\}$ denote the real and imaginary components of a complex number a, respectively.

II. SYSTEM MODEL

We consider a cooperative network, where N nodes (i.e., VAA elements) transmit together to the desired receiver (i.e., Bob) using the same frequency at the same time, in the presence of an eavesdropper (i.e., Eve). It is assumed that a single antenna is mounted in all of the nodes (i.e., VAA elements, Bob, and Eve), which is typical in the IoT networks with a limited form factor and computational capability. For these inherent limitations in the IoT nodes, the VAA is created by the collaboration of multiple nodes, which are randomly distributed. In other words, the VAA elements are small IoT devices, which cannot accommodate multi-antenna array, because of the hardware limitations such as space, power, and computational capacity. The VAA can achieve higher diversity gain, as compared to the co-located (or real) antenna array (a single node with multi-antennas), because of macro-diversity gain [45]. As illustrated in Fig. 1, the VAA elements are independent and identically distributed (i.i.d.) according to the two-dimensional (2D) uniform distribution over the

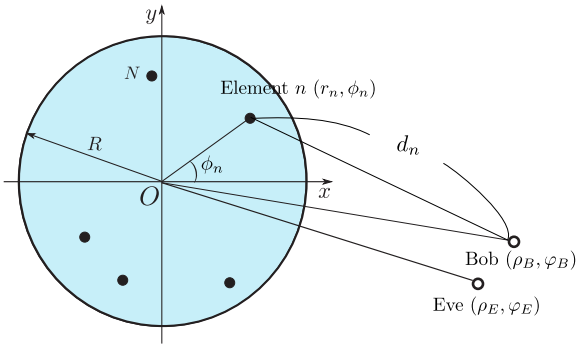


FIGURE 1. Network geometry.

disk centered at the origin O with the radius of R. The location of the nth VAA element is denoted by (r_n, ϕ_n) using the polar coordinates for $n \in \{1, \ldots, N\}$. Following the 2D uniform distribution, the probability density function (PDF) of the radial distance from the origin, r_n, is expressed as

$$f_{r_n}(r) = \frac{2r}{R^2}, \tag{1}$$

where $0 \leq r \leq R$. In addition, the PDF of the azimuth angle with respect to the x-axis, ϕ_n, is

$$f_{\phi_n}(\phi) = \frac{1}{2\pi}, \tag{2}$$

where $0 \leq \phi < 2\pi$. Moreover, as shown in Fig. 1, the locations of Bob and Eve are denoted by (ρ_B, φ_B) and (ρ_E, φ_E), using the polar coordinates, respectively.

The group of nodes (the elements of the VAA) correspond to the source nodes (i.e., Alice), which send data to Bob, while creating AN to the potential directions of Eve, as indicated by the solid line arrows and the dotted line arrows respectively in Fig. 2. As assumed in [34], [35], [36], [37], [38], [39], and [40], we are mainly interested in the far-field scenario, where the distances of Bob and Eve to the center of the VAA are significantly greater than the size of the disk R (i.e., $\rho_B \gg R$ and $\rho_E \gg R$). Therefore, we aim to diminish the information leakage to Eve, while transmitting desired information (data) to Bob by degrading the SNR at Eve. In particular, focusing on the most vulnerable case, in which Eve exists in the proximity to Bob in angular locations, there exists a trade-off between the data transmission to Bob and AN injection to Eve, because the desired information can be overheard by Eve, whereas Bob may suffer from AN targeting Eve, due to the close angular locations of Bob and Eve.

For the kth transmit time interval (TTI), the distance from the nth VAA element to a receiver (either Bob or Eve), which is located at (ρ, φ), is obtained as

$$d_n(\rho, \varphi, k) = \sqrt{r_n^2(k) - 2r_n(k)\rho\cos(\varphi - \phi_n(k)) + \rho^2}. \tag{3}$$

Suppose that $s(k) \in \mathbb{C}$ is the data symbol, where k is the TTI index and $\mathbb{E}[|s(k)|^2] = 1$. Also, $\mathbf{w}(k) = [w_1(k), \ldots, w_N(k)]^T \in \mathbb{C}^{N\times 1}$ is the precoding vector, by which the nth VAA element multiplies the complex weight $w_n(k)$ with $s(k)$. Assuming a narrow-band channel, the signal received at a node located at (ρ, φ) is expressed as

$$y(\rho, \varphi, k) = \sqrt{P}\,\mathbf{h}(\rho, \varphi, k)\,\mathbf{w}(k)s(k) + z(k), \tag{4}$$

where P denotes the transmit power. Further, $z(k)$ represents the additive white Gaussian noise with mean zero and variance σ^2 (i.e., $z(k) \sim \mathcal{CN}(0, \sigma^2)$). Moreover, $\mathbf{h}(\rho, \varphi, k) \in \mathbb{C}^{1\times N}$ is a channel vector between the VAA elements and the receiver at (ρ, φ), the nth element of which is given by

$$h_n(\rho, \varphi, k) = \frac{1}{d_n(\rho, \varphi, k)} e^{j\frac{2\pi}{\lambda}d_n(\rho,\varphi,k)}, \tag{5}$$

where $|h_n(\rho, \varphi, k)|^2 = \frac{1}{d_n^2(\rho,\varphi,k)}$ corresponds to the path loss with the exponent of two. Further, $\angle h_n(\rho, \varphi, k) = \frac{2\pi d_n(\rho,\varphi,k)}{\lambda}$ is the phase rotation to propagate the distance of $d_n(\rho, \varphi, k)$ with the wavelength of λ.

In other words, we assume a line-of-sight (LoS) channel between a VAA element and a receiver (either Bob or Eve), because the secrecy rate with both LoS and non-LoS (NLoS) components are not tractable. If both components exist, the secrecy rate analyzed in this paper can still be used as an upper bound of the achievable secrecy rate in the presence of multi-path fading, as shown in [36] and [38] that assume Rician channels. Further, the results in [36] and [38] show that the analysis with the LoS channel can be a good approximation for the secrecy rate with high Rician factor K. In addition, when it comes to millimeter wave and sub-terahertz frequency bands, which are being considered for 6G systems, the channel is LoS-dominant and widely modeled by a pure LoS channel without NLoS components, as in [19], [20], [21], [46], [47], [48], and [49]. Further, our work in this paper can provide design insight for applications with LoS-dominant channels such as UAV and low-Earth orbit (LEO) satellite networks [50], [51], [52]. Also, future extensions of this work include the secrecy rate analysis with various channel models including multi-path fading and shadowing.

To randomize the radiation pattern, for each TTI, the VAA elements are randomly selected; thus, the channel vector $\mathbf{h}(\rho, \varphi, k)$ also varies randomly. Consequently, the received signal at Eve from the random VAA in (4) is given by

$$\begin{aligned} y(\rho_E, \varphi_E, k) &= \sqrt{P}\sum_{n=1}^{N} h_n(\rho_E, \varphi_E, k)w_n(k)\,s(k) + z(k) \\ &= \underbrace{F(\rho_E, \varphi_E, k)}_{\text{array factor}}\,\underbrace{s(k)}_{\text{message}} + \underbrace{z(k)}_{\text{additive noise}}, \end{aligned} \tag{6}$$

where $F(\rho_E, \varphi_E, k) = \sqrt{P}\sum_{n=1}^{N} h_n(\rho_E, \varphi_E, k)w_n(k)$, which is subject to the stochastic VAA at the kth TTI. Because the VAA elements are randomly selected, the radiation pattern is randomized, which is indicated by the changes in the amplitude and phase of the array factor $F(\rho, \varphi, k)$ (or the received signal), as noted in [18], [19], [20], [21], [22], [34], [35], [36], [37], [38], [39], [40], [46], [48], and [49]. Accordingly, the

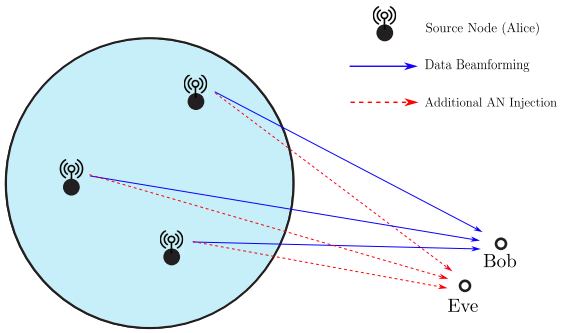


FIGURE 2. Illustration of the combination of data beamformer to Bob and AN injection beamformer to Eve.

received signal at Bob is given by

$$y(\rho_B, \varphi_B, k) = \sqrt{P}\sum_{n=1}^{N} h_n(\rho_B, \varphi_B, k) w_n(k)\, s(k) + z(k)$$
$$= \underbrace{F(\rho_B, \varphi_B, k)}_{\text{array factor}} \underbrace{s(k)}_{\text{message}} + \underbrace{z(k)}_{\text{additive noise}}, \quad (7)$$

where $F(\rho_B, \varphi_B, k) = \sqrt{P}\sum_{n=1}^{N} h_n(\rho_B, \varphi_B, k) w_n(k)$. With our proposed beamformer, the statistical characteristics of the array factor will be analyzed in Sections III and IV. Then, in Section V, we will further analyze the received signal and derive the secrecy rate.

Remark 1 (Practical Implementation Issues of CB): In [53], it is shown that with proper design, CB-based techniques can enhance spectral efficiency and energy efficiency. For this reason, CB is also exploited to secure IoT networks [34], [35], [36], [37], [38], [39], [40]. However, when it comes to the practical implementation of CB, there are some technical issues, as highlighted in [54]. In particular, synchronization across the VAA elements is challenging without wired connections, because they are operated with their own local oscillators. As a result, various synchronization protocols are proposed in the prior studies.

As presented in [54] and [55], the synchronization can be achieved through closed-loop or open-loop approaches. In the closed-loop algorithms, each VAA element synchronizes itself to the beacon sent from the receiver (Bob), which is especially effective in time-division duplex with many VAA elements. In this case, the phase jitter is subject to the SNR of the PLL. The authors in [56] propose a master-slave synchronization protocol with beacon signals, by which the VAA elements are shown to be synchronized.

On the other hand, in the case of the open-loop approaches, the VAA elements can locally adjust their phases using the location information (r_n, ϕ_n) relative to the VAA center and the angular location of the receiver, as in [37]. Obtaining Bob's direction is straightforward, while that of Eve is not available in general. However, there are many circumstances, where the direction of Eve is known to the transmitter (or Alice) in reality, as noted in [38], [57], [58], and [59]. In [60], when Eve is an authorized user with the intention of eavesdropping, they show that the location of Eve can be shared in the network through location-based applications including IEEE 1609.2. In addition, the VAA elements can identify Eve's direction through visual or electronic detection as in military surveillance [57]. Even if Eve is purely passive with infrequent transmissions, various signal processing techniques can help find its location [59].

Both closed-loop and open-loop algorithms are experimentally studied, which shows their feasibility in practical scenarios. For example, in [61], the authors present a fully wireless implementation of CB using software-defined radios (SDRs), where VAA elements are synchronized without wired connections among them. Further, the authors in [62] propose a fast open-loop synchronization protocol for CB. In [63], the authors provide a mathematical framework to model and evaluate the CB protocol, which is verified experimentally using SDRs in a lab. They also demonstrate that CB with VAA constructed by multiple UAVs can achieve more than 80% performance gain compared to that of the ideal CB even under the short coherence time in the UAV applications. In [64], a deep learning-based CB algorithm is proposed for distributed networks under hardware impairments such as the nonlinearity of power amplifiers.

Remark 2 (Cooperative Beamforming Applications): CB can be employed in various IoT applications. For example, in [65], the authors present a novel method to use CB for continuous monitoring wireless sensor networks. Moreover, in [55], CB is adopted to upload video or image data or sensing data collected over several days. On top of that, they consider other interesting applications such as reach-back using low-power radios carried by soldiers on battlefields and collaboration of subscriber nodes for uplink transmission. Also, in disaster or emergency cases, where the existing infrastructure is not properly working, a long-range communication through CB is particularly useful.

In [66], CB is employed in UAV networks to overcome the limitations of the UAV platform such as battery capacity, transmission range (or low coverage), insufficient service time, and security vulnerability. Similarly, UAV swarm sensing can be improved in terms of the secrecy rate and energy efficiency, as discussed in [39] and [40]. A CB algorithm for the distributed multiple-RIS communications is considered in [67]. Further, CB can be employed in distributed sensing or distributed machine learning with ultra-fast wireless data (or machine learning parameters) aggregation through over-the-air computation (AirComp) [68]. In most of the above-mentioned studies except [68], it is assumed that data sharing among the VAA elements can be readily realized as long as the VAA size, which limits the data rate of such location communications, is small enough compared to the distance to the receiver, which typically holds in the far-field scenario.

III. AN INJECTION BEAMFORMER AND PRACTICAL CHALLENGES

In this section, we first consider an AN injection beamformer, as a simple extension of the AN injection beamformer for the

real (or co-located) antenna array, where each VAA element should know the others' CSI. We highlight the practical challenges due to such overhead to realize the AN injection through CB.

We first present a CB precoding as a linear sum of a data precoder, $\mathbf{w}_D$, by which the desired signal $s(k)$ is transmitted to Bob, and an AN injection precoder, $\mathbf{w}_{AN}$, by which noise-like signals are sent to Eve. The nth element of the data transmission beamformer, $\mathbf{w}_D$, by which $s(k)$ is coherently combined at Bob, is given by

$$[\mathbf{w}_D(k)]_n = \frac{1}{\sqrt{N}} \frac{h_n^*(\rho_B, \varphi_B, k)}{|h_n(\rho_B, \varphi_B, k|} = \frac{e^{-j\angle h_n(\rho_B,\varphi_B,k)}}{\sqrt{N}} = \frac{1}{\sqrt{N}} e^{-j\frac{2\pi}{\lambda} d_n(\rho_B,\varphi_B,k)}. \quad (8)$$

In the far field, the distance in (3) is simplified as

$$d_n(\rho, \varphi, k) \approx \rho - r_n(k)\cos(\phi_n(k) - \varphi). \quad (9)$$

Then, in (8), we can approximate the distance from the nth VAA element to Bob as $d_n(\rho_B, \varphi_B, k) \approx \rho_B - r_n(k)\cos(\phi_n(k) - \varphi_B)$. Thus, the data precoder in (8) can be expressed as

$$[\mathbf{w}_D(k)]_n = \frac{e^{-j\frac{2\pi}{\lambda}[\rho_B - r_n(k)\cos(\varphi_B - \phi_n(k))]}}{\sqrt{N}} = \frac{1}{\sqrt{N}}[\mathbf{v}(\varphi_B, k)]_n, \quad (10)$$

where $\mathbf{v}(\varphi, k)$ is the array manifold to the angle of φ at the kth TTI:

$$\mathbf{v}(\varphi, k) = \left[e^{j\frac{2\pi}{\lambda} r_1(k)\cos(\varphi - \phi_1(k))}, \ldots, e^{j\frac{2\pi}{\lambda} r_N(k)\cos(\varphi - \phi_N(k))}\right]^T. \quad (11)$$

Now, we construct the AN injection beamformer, which creates AN to degrade the SNR along the potential angular location of Eve, denoted by the direction of φ_{AN}. First, we define the following projection matrix $\mathbf{P}_B \in \mathbb{C}^{N\times N}$ onto the direction of Bob

$$\mathbf{P}_B = \frac{\mathbf{v}(\varphi_B, k)\,\mathbf{v}^H(\varphi_B, k)}{\mathbf{v}^H(\varphi_B, k)\,\mathbf{v}(\varphi_B, k)} = \frac{\mathbf{v}(\varphi_B, k)\,\mathbf{v}^H(\varphi_B, k)}{N}. \quad (12)$$

When designing the AN injection beamformer, $\mathbf{w}_{AN}$, the AN should not hurt the SNR at Bob; thus, we first create the projection matrix $\mathbf{P}_{B\perp} \in \mathbb{C}^{N\times N}$ as the orthogonal complement of a subspace of $\mathbf{P}_B$ as

$$\mathbf{P}_{B\perp} = \mathbf{I} - \mathbf{P}_B = \mathbf{I} - \frac{\mathbf{v}(\varphi_B, k)\,\mathbf{v}^H(\varphi_B, k)}{N}, \quad (13)$$

where $\mathbf{I}$ is the identity matrix of size $N \times N$. Thus, we design the noise beamformer, $\mathbf{w}_{AN}(k)$, which radiates an AN to the potential angular location of Eve φ_{AN} but does not affect Bob (i.e., orthogonal to $\mathbf{v}(\varphi_B, k)$), as

$$\mathbf{w}_{AN}(k) = \frac{\mathbf{P}_{B\perp}\mathbf{v}(\varphi_{AN}, k)}{\|\mathbf{P}_{B\perp}\mathbf{v}(\varphi_{AN}, k)\|}. \quad (14)$$

Therefore, we can create the beamformer to transmit the desired information to Bob and radiate the AN to Eve, simultaneously, by using the following precoding vector as the mixture of the data beamformer, $\mathbf{w}_D(k)$, and the AN injection beamformer, $\mathbf{w}_{AN}(k)$, as

$$\mathbf{w}(k) = \sqrt{t}\ \mathbf{w}_D(k) + \sqrt{1-t}\ \mathbf{w}_{AN}(k)\epsilon(k) = \frac{\sqrt{t}}{\sqrt{N}}\mathbf{v}(\varphi_B, k) + \sqrt{1-t}\,\frac{\mathbf{P}_{B\perp}\mathbf{v}(\varphi_{AN}, k)}{\|\mathbf{P}_{B\perp}\mathbf{v}(\varphi_{AN}, k)\|}\epsilon(k), \quad (15)$$

where $\epsilon(k)$ is the AN (or jamming signal). We assume that $\epsilon(k) = e^{j\theta(k)}$ with $\theta(k)$ being uniformly distributed between 0 and 2π. Also, t corresponds to the power ratio of the data transmission to the total power allocated for the precoder $\mathbf{w}(k)$, where $0 \le t \le 1$. In contrast, $1 - t$ is the power ratio of the AN to the aggregate power of $\mathbf{w}(k)$.

For example, if $t = 1$ in (15), $\mathbf{w}(k)$ is reduced into the data beamformer without AN injection (i.e., $\mathbf{w}(k) = \mathbf{w}_D(k)$). In other words, the proposed beamformer with $t = 1$ corresponds to the pure CB without the AN injection proposed in [34], [35], and [36]. On the other hand, when $t = 0$, the precoding vector is reduced into the AN injection beamformer (i.e., $\mathbf{w}(k) = \mathbf{w}_{AN}(k)$). When $0 < t < 1$, a certain level of the data signal $s(k)$ is transmitted to Bob, and the AN is also injected to deteriorate Eve's SNR, which can impact Bob's SNR. In other words, there exists a trade-off between the SNRs of Bob and Eve controlled by t. Thus, we can optimize the secrecy throughput by adjusting t, which will be treated in Section V.

Taking advantage of such a trade-off relationship, we can overcome the secrecy rate degradation with the simple data beamformer (i.e., $t = 1$) for Eve close to Bob. To obtain the precoding vector in (15), however, each VAA element should know CSI (or locations) of the other elements. For instance, the nth element of $\mathbf{w}(k)$ in (15) can be obtained by using all the elements of $\mathbf{w}_D(k)$ and $\mathbf{v}(\varphi_B, k)$. However, that may be infeasible in practice, because the VAA elements are selected randomly for different k, which may result in the excessive overhead to compute and share $\mathbf{w}(k)$ in (15) among the VAA elements.

IV. DECENTRALIZED NOISE INJECTION BEAMFORMER

To tackle this issue, we aim at designing a decentralized AN injection precoding algorithm, where VAA elements can adjust their phases and amplitudes in a fully distributed manner. For this reason, we propose a novel AN injection precoder that minimizes the implementation overhead by using the statistical information.

If expanding $\mathbf{w}(k)$ in (15), we obtain

$$\mathbf{w}(k) = \frac{\sqrt{t}}{\sqrt{N}}\mathbf{v}(\varphi_B, k) + \frac{\epsilon(k)\sqrt{1-t}}{\|\mathbf{P}_{B\perp}\mathbf{v}(\varphi_{AN}, k)\|}\left(\mathbf{v}(\varphi_{AN}, k) - \frac{\mathbf{v}(\varphi_B, k)\,\mathbf{v}^H(\varphi_B, k)}{N}\mathbf{v}(\varphi_{AN}, k)\right), \quad (16)$$

which cannot be locally applied, since its nth element is subject to $\mathbf{v}(\varphi_B, k)\,\mathbf{v}^H(\varphi_B, k)\,\mathbf{v}(\varphi_{AN}, k)$ and $\|\mathbf{P}_{B\perp}\mathbf{v}(\varphi_{AN}, k)\|$.

Thus, to realize it in a decentralized way, we first replace $\mathbf{v}^H(\varphi_B, k)\,\mathbf{v}(\varphi_{AN}, k)$ with its statistical average as

$$\begin{aligned}&\mathbb{E}[\mathbf{v}(\varphi_B, k)^H \mathbf{v}(\varphi_{AN}, k)]\\ &= \mathbb{E}[\sum_{n=1}^{N} e^{j\frac{2\pi}{\lambda} r_n(k)[\cos(\varphi_{AN}-\phi_n(k))-\cos(\varphi_B-\phi_n(k))]}]\\ &= N\,\mathbb{E}\left[e^{j\frac{4\pi}{\lambda} r_n(k)\sin\left(\phi_n(k)-\frac{\varphi_B+\varphi_{AN}}{2}\right)\sin(\frac{\varphi_{AN}-\varphi_B}{2})}\right]. \quad (17)\end{aligned}$$

For further simplification, letting $u_n(k) = r_n(k)\sin\left(\phi_n(k) - \frac{\varphi_B+\varphi_{AN}}{2}\right)$, the PDF of which is obtained as

$$f_{u_n(k)}(u) = \frac{2\sqrt{1-u^2}}{\pi}, \quad (18)$$

where $-R \le u \le R$. Therefore, $\mathbb{E}[\mathbf{v}(\varphi_B, k)^H \mathbf{v}(\varphi_{AN}, k)]$ in (17) can be obtained as

$$\begin{aligned}\mathbb{E}[\mathbf{v}(\varphi_B, k)^H \mathbf{v}(\varphi_{AN}, k)] &= N\,\mathbb{E}[e^{j\frac{4\pi}{\lambda}u_n(k)\sin(\frac{\varphi_{AN}-\varphi_B}{2})}]\\ &= N\int_{-R}^{R} e^{j\frac{4\pi}{\lambda}u\sin(\frac{\varphi_{AN}-\varphi_B}{2})} f_{u_n(k)}(u)du\\ &= N\frac{J_1(\frac{4\pi R}{\lambda}\sin(\frac{\varphi_{AN}-\varphi_B}{2}))}{\frac{2\pi R}{\lambda}\sin(\frac{\varphi_{AN}-\varphi_B}{2})}\\ &= N\Upsilon(\Delta\varphi), \quad (19)\end{aligned}$$

where $J_1(\cdot)$ is the first order Bessel function of the first kind. Further, $\Upsilon(x) = 2\frac{J_1(\frac{4\pi R}{\lambda}\sin(\frac{x}{2}))}{\frac{4\pi R}{\lambda}\sin(\frac{x}{2})}$ and $\Delta\varphi = \varphi_{AN} - \varphi_B$.

As a result, the decentralized version of $\mathbf{w}(k)$ in (15), by which each VAA element can locally adjust its phase, is expressed as

$$\begin{aligned}\tilde{\mathbf{w}}(k) &= \frac{\sqrt{t}}{\sqrt{N}}\mathbf{v}(\varphi_B, k)\\ &\quad + \frac{\epsilon(k)\sqrt{1-t}\left(\mathbf{v}(\varphi_{AN}, k) - \Upsilon(\Delta\varphi)\,\mathbf{v}(\varphi_B, k)\right)}{\mathbb{E}[\|\mathbf{v}(\varphi_{AN}, k) - \Upsilon(\Delta\varphi)\,\mathbf{v}(\varphi_B, k)\|]}. \quad (20)\end{aligned}$$

We can compute the expected value in the denominator of (20) through the following steps. First, we derive the squared norm of $\mathbf{v}(\varphi_{AN}, k) - \Upsilon(\Delta\varphi)\,\mathbf{v}(\varphi_B, k)$ as

$$\begin{aligned}&\|\mathbf{v}(\varphi_{AN}, k) - \Upsilon(\Delta\varphi)\,\mathbf{v}(\varphi_B, k)\|^2\\ &= \mathbf{v}^H(\varphi_{AN}, k)\mathbf{v}(\varphi_{AN}, k) - \mathbf{v}^H(\varphi_{AN}, k)\,\mathbf{v}(\varphi_B, k)\Upsilon(\Delta\varphi)\\ &\quad - \Upsilon(\Delta\varphi)\,\mathbf{v}^H(\varphi_B, k)\mathbf{v}(\varphi_{AN}, k) + N\Upsilon^2(\Delta\varphi) \quad (21)\end{aligned}$$

Hence, the expected value of the squared norm in (21) can be obtained as

$$\begin{aligned}&\mathbb{E}[\|\mathbf{v}(\varphi_{AN}, k) - \Upsilon(\Delta\varphi)\,\mathbf{v}(\varphi_B, k)\|^2]\\ &= N - \Upsilon(\Delta\varphi)\,\mathbb{E}[\mathbf{v}^H(\varphi_{AN}, k)\,\mathbf{v}(\varphi_B, k)]\\ &\quad - \Upsilon(\Delta\varphi)\,\mathbb{E}[\mathbf{v}^H(\varphi_B, k)\mathbf{v}(\varphi_{AN}, k)] + N\Upsilon^2(\Delta\varphi)\\ &\overset{(a)}{=} N - 2N\Upsilon^2(\Delta\varphi) + N\Upsilon^2(\Delta\varphi)\\ &= N - N\Upsilon^2(\Delta\varphi), \quad (22)\end{aligned}$$

TABLE 1. Complexity of centralized and decentralized noise injection beamformer.

Algorithm	*Local Communication*	*Vector Normalization*
Centralized AN Injection Beamformer	$2N$	Required
Decentralized AN Injection Beamformer	1	Not required

where (a) follows from $\mathbb{E}[\mathbf{v}^H(\varphi_{AN}, k)\mathbf{v}(\varphi_B, k)] = \mathbb{E}[\mathbf{v}^H(\varphi_B, k)\mathbf{v}(\varphi_{AN}, k)] = N\Upsilon(\Delta\varphi)$ based on (19). Finally, replacing (22) into (20), the decentralized beamformer for simultaneous data transmission to Bob and AN injection to Eve can be derived as

$$\begin{aligned}\tilde{\mathbf{w}}(k) &= \frac{\sqrt{t}}{\sqrt{N}}\mathbf{v}(\varphi_B, k)\\ &\quad + \frac{\epsilon(k)\sqrt{1-t}\left(\mathbf{v}(\varphi_{AN}, k) - \Upsilon(\Delta\varphi)\,\mathbf{v}(\varphi_B, k)\right)}{\sqrt{N - N\Upsilon^2(\Delta\varphi)}}\\ &= \left[\frac{\sqrt{t}}{\sqrt{N}} - \frac{\epsilon(k)\Upsilon(\Delta\varphi)\sqrt{1-t}}{\sqrt{N - N\Upsilon^2(\Delta\varphi)}}\right]\mathbf{v}(\varphi_B, k)\\ &\quad + \frac{\epsilon(k)\sqrt{1-t}}{\sqrt{N - N\Upsilon^2(\Delta\varphi)}}\mathbf{v}(\varphi_{AN}, k). \quad (23)\end{aligned}$$

Since the nth element of $\tilde{\mathbf{w}}(k)$ in (23) is subject to the nth elements of $\mathbf{v}(\varphi_B, k)$ and $\mathbf{v}(\varphi_{AN}, k)$, while the other terms are not subject to the stochastic topology of the VAA, each VAA element can independently apply the precoding. In other words, each VAA element only needs the angular location of Bob and its own location $(r_n(k), \phi_n(k))$ relative to the VAA center for the nth element of $\mathbf{v}(\varphi_B, k)$. Similarly, the nth element of $\mathbf{v}(\varphi_{AN}, k)$ can also be computed with the direction information of the AN injection φ_{AN} and $(r_n(k), \phi_n(k))$. The following proposition shows that it has the unit norm asymptotically, when N is large enough.

Proposition 1: As $N \to \infty$, the norm of the proposed vector $\tilde{\mathbf{w}}(k)$ in (23) converges to unity with probability one as

$$\lim_{N\to\infty} ||\tilde{\mathbf{w}}(k)||^2 \xrightarrow{p1} 1. \quad (24)$$

Proof: It is noted that $\mathbb{E}[|\epsilon(k)|^2] = 1$. Also, the elements of $\mathbf{v}(\varphi_B, k)$ and $\mathbf{v}(\varphi_{AN}, k)$ in (23) are complex exponential functions with purely imaginary exponents, which are functions of i.i.d. random variables depending on the locations of the VAA elements. Thus, by the law of large numbers, we have

$$\lim_{N\to\infty} ||\tilde{\mathbf{w}}(k)||^2 \xrightarrow{p1} t + (1-t) = 1. \quad (25)$$

□

Table 1 shows the overhead and complexity of centralized and decentralized (proposed) AN injection beamformers. As discussed in Section III, the centralized AN injection beamformer needs N local communications to collect the CSI and another N local communications to share the computed precoding weights. Thus, in total $2N$ times of local communications are required. Furthermore, the normalization

using the collected CSI should be performed in the centralized AN injection beamformer, as expressed in (15). On the other hand, in our proposed approach, the decentralized AN injection beamformer, presented in this section, uses the statistical location information. Therefore, each VAA element can locally adjust its phase without intra-cluster coordination (or local communication). Moreover, vector normalization is not required in the decentralized AN injection beamformer, as indicated in (23).

V. SECRECY RATE ANALYSIS

In this section, the secrecy rate (i.e., secrecy throughput) performance of the proposed PLS with AN injection is analyzed. As in [18], [19], [20], [21], [22], [34], [35], [36], [37], [38], [39], [40], [46], [48], [49] the secrecy rate is quantified as the maximum data rate provided that information can be communicated reliably and securely. Then, the secrecy rate can be expressed as

$$\eta = [\log_2(1+\gamma_B) - \log_2(1+\gamma_E)]^+, \tag{26}$$

where γ_B and γ_E are the SNRs at Bob and Eve, respectively, and $[x]^+$ denotes $\max\{0, x\}$.

The array factor, $F(\rho, \varphi, k)$, can be approximated as a complex Gaussian random variable, which has been proven in Lemma 1 of [20] as well as in [46]. In other words, the array factor randomized over multiple TTIs per codeword jams Eve at an undesired direction. Hence, as analyzed in [20], the constant $\mathbb{E}[F(\rho, \varphi, k)]$ is the array factor observed at Eve, whereas the term $(F(\rho, \varphi, k) - \mathbb{E}[F(\rho, \varphi, k)])$ is a zero-mean complex Gaussian random variable that represents the noise at (ρ, φ). Therefore, the array factor over multiple TTIs both at Bob and Eve, which correspond to $(\rho, \varphi) = (\rho_B, \varphi_B)$ and $(\rho, \varphi) = (\rho_E, \varphi_E)$ respectively, follow complex Gaussian random variables; thus, the capacities of Bob and Eve can be obtained by the additive white Gaussian Noise (AWGN) channel capacities, as noted in [20] as well as in [46]. As a result, the SNR at Bob is computed as

$$\gamma_B = \frac{|\mathbb{E}[F(\rho_B, \varphi_B, k)]|^2}{\mathbb{V}\text{ar}[F(\rho_B, \varphi_B, k)] + \sigma^2}. \tag{27}$$

Similarly, the SNR at Eve is obtained as

$$\gamma_E = \frac{|\mathbb{E}[F(\rho_E, \varphi_E, k)]|^2}{\mathbb{V}\text{ar}[F(\rho_E, \varphi_E, k)] + \sigma^2}. \tag{28}$$

As analyzed in [18], [19], [20], [34], [35], [36], [37], [38], [39], [40], and [46], $|\mathbb{E}[F(\rho_B, \varphi_B, k)]|^2$ and $|\mathbb{E}[F(\rho_E, \varphi_E, k)]|^2$ in (27) and (28) corresponds to the power of the desired information. Further, as explained above, the random fluctuations in the received signal correspond to the signal distortion, as noted in [18], [19], [20], [34], [35], [36], [37], [38], [39], [40], and [46]. Therefore, the noise power considering both AN and additive noise $z(k)$ can be computed by the sum of the variance of the array factor and the variance of $z(k)$, which also follows from [18], [19], [20], [34], [35], [36], [37], [38], [39], [40], and [46]. Thus, we need to derive the mean value and variance of the array factor. To this end, from (6), the array factor can be obtained with the proposed precoding in (23) as follows:

$$\begin{aligned}
F(\rho, \varphi, k) &= \sqrt{P}\sum_{n=1}^{N} h_n(\rho, \varphi, k)[\tilde{\mathbf{w}}(k)]_n \\
&= \sqrt{P}\sum_{n=1}^{N}\Bigg(\sqrt{t}\frac{e^{j\frac{2\pi}{\lambda}r_n(k)\cos(\varphi_B-\phi_n(k))}}{\sqrt{N}} \\
&\quad + \frac{\sqrt{1-t}e^{j\frac{2\pi}{\lambda}r_n(k)\cos(\varphi_{AN}-\phi_n(k))}\epsilon(k)}{\sqrt{N-N\Upsilon^2(\Delta\varphi)}} \\
&\quad - \frac{\sqrt{1-t}\Upsilon(\Delta\varphi)e^{j\frac{2\pi}{\lambda}r_n(k)\cos(\varphi_B-\phi_n(k))}\epsilon(k)}{\sqrt{N-N\Upsilon^2(\Delta\varphi)}}\Bigg) \\
&\quad \times \frac{1}{\rho}e^{-j\frac{2\pi}{\lambda}r_n(k)\cos(\varphi-\phi_n(k))} \\
&= \sqrt{P}\sum_{n=1}^{N}\Bigg(\sqrt{t}\frac{e^{j\frac{4\pi}{\lambda}\hat{u}_n(k)\sin(\frac{\varphi_B-\varphi}{2})}}{\rho\sqrt{N}} \\
&\quad + \frac{\sqrt{1-t}e^{j\frac{4\pi}{\lambda}\check{u}_n(k)\sin(\frac{\varphi_{AN}-\varphi}{2})}\epsilon(k)}{\rho\sqrt{N-N\Upsilon^2(\Delta\varphi)}} \\
&\quad - \frac{\sqrt{1-t}\Upsilon(\Delta\varphi)e^{j\frac{4\pi}{\lambda}\hat{u}_n(k)\sin(\frac{\varphi_B-\varphi}{2})}\epsilon(k)}{\rho\sqrt{N-N\Upsilon^2(\Delta\varphi)}}\Bigg) \\
&= \sqrt{P}\sum_{n=1}^{N}\Bigg(\frac{\sqrt{t}}{\rho\sqrt{N}}\Xi_n(k) + \frac{\sqrt{1-t}\Lambda_n(k)\epsilon(k)}{\rho\sqrt{N-N\Upsilon^2(\Delta\varphi)}} \\
&\quad - \frac{\sqrt{1-t}\Upsilon(\Delta\varphi)\Xi_n(k)\epsilon(k)}{\rho\sqrt{N-N\Upsilon^2(\Delta\varphi)}}\Bigg),
\end{aligned} \tag{29}$$

where $\hat{u}_n(k) = r_n(k)\sin(\hat{\phi}_n(k))$ and $\check{u}_n(k) = r_n(k)\sin(\check{\phi}_n(k))$ for $\hat{\phi}_n(k) = \phi_n(k) - \frac{\varphi_B+\varphi}{2}$ and $\check{\phi}_n(k) = \phi_n(k) - \frac{\varphi_{AN}+\varphi}{2}$, respectively. Because specific selections of φ_B, φ_{AN}, and φ do not affect the statistical characteristics of both $\hat{\phi}_n(k)$ and $\check{\phi}_n(k)$, the PDFs of $\hat{u}_n(k)$ and $\check{u}_n(k)$ are the identical as $f_{u_n(k)}(u)$ in (18). Also, it is noted that $\Xi_n(k) = e^{j\frac{4\pi\hat{u}_n(k)}{\lambda}\sin(\frac{\varphi_B-\varphi}{2})}$ and $\Lambda_n(k) = e^{j\frac{4\pi}{\lambda}\check{u}_n(k)\sin(\frac{\varphi_{AN}-\varphi}{2})}$. Thus, following the classification of the received signal into the effective channel gain corresponding to the desired signal, artificial noise, and additive noise components in [20], the received signal at Eve can be written as

$$\begin{aligned}
&y(\rho_E, \varphi_E, k) \\
&= \sqrt{P}\mathbf{h}(\rho_E, \varphi_E, k)\tilde{\mathbf{w}}(k)s(k) + z(k) \\
&= F(\rho_E, \varphi_E, k)s(k) + z(k) \\
&= \sqrt{P}\sum_{n=1}^{N}\Bigg(\frac{\sqrt{t}}{\rho\sqrt{N}}\Xi_n(k) + \frac{\sqrt{1-t}\Lambda_n(k)\epsilon(k)}{\rho\sqrt{N-N\Upsilon^2(\Delta\varphi)}} \\
&\quad - \frac{\sqrt{1-t}\Upsilon(\Delta\varphi)\Xi_n(k)\epsilon(k)}{\rho\sqrt{N-N\Upsilon^2(\Delta\varphi)}}\Bigg)s(k) + z(k) \\
&= \sum_{n=1}^{N}\Bigg(\underbrace{\frac{\sqrt{Pt}}{\rho\sqrt{N}}\Xi_n(k)}_{\text{effective channel gain}}
\end{aligned}$$

$$+\underbrace{\frac{\sqrt{P(1-t)}\epsilon(k)\Big(\Lambda_n(k)-\Upsilon(\Delta\varphi)\Xi_n(k)\Big)}{\rho\sqrt{N-N\Upsilon^2(\Delta\varphi)}}}_{\text{artificial noise}}\Bigg)\underbrace{s(k)}_{\text{message}}$$
$$+\underbrace{z(k)}_{\text{additive noise}}. \tag{30}$$

In contrast, Bob's received signal is expressed as

$$\begin{aligned}
&y(\rho_B,\varphi_B,k)\\
&=\sqrt{P}\,\mathbf{h}(\rho_B,\varphi_B,k)\,\mathbf{w}(k)s(k)+z(k)\\
&=F(\rho_B,\varphi_B,k)s(k)+z(k)\\
&=\sqrt{P}\sum_{n=1}^{N}\Bigg(\frac{\sqrt{t}}{\rho\sqrt{N}}+\frac{\sqrt{1-t}e^{j\frac{4\pi}{\lambda}\check{u}_n(k)\sin(\frac{\varphi_{AN}-\varphi_B}{2})}\epsilon(k)}{\rho\sqrt{N-N\Upsilon^2(\Delta\varphi)}}\\
&\quad-\frac{\sqrt{1-t}\Upsilon(\Delta\varphi)\epsilon(k)}{\rho\sqrt{N-N\Upsilon^2(\Delta\varphi)}}\Bigg)s(k)+z(k).\\
&=\sum_{n=1}^{N}\Bigg(\underbrace{\frac{\sqrt{Pt}}{\rho\sqrt{N}}}_{\text{effective channel gain}}\\
&\quad+\underbrace{\frac{\sqrt{P(1-t)}\epsilon(k)\Big(e^{j\frac{4\pi}{\lambda}\check{u}_n(k)\sin(\frac{\varphi_{AN}-\varphi_B}{2})}-\Upsilon(\Delta\varphi)\Big)}{\rho\sqrt{N-N\Upsilon^2(\Delta\varphi)}}}_{\text{artificial noise}}\Bigg)\underbrace{s(k)}_{\text{message}}\\
&\quad+\underbrace{z(k)}_{\text{additive noise}}.
\end{aligned}\tag{31}$$

The following two lemmas provide the expected value and variance of the array factor observed at an arbitrary location of a receiver located at (ρ,φ), which can be used to derive the secrecy rate by simply exchanging $(\rho,\varphi)=(\rho_B,\varphi_B)$ and $(\rho,\varphi)=(\rho_E,\varphi_E)$, respectively.

Lemma 1: The expected value of the array factor, $F(\rho,\varphi,k)$, with the proposed CB with the AN injection is expressed as

$$\mathbb{E}[F(\rho,\varphi,k)]=\frac{\sqrt{tPN}}{\rho}\Upsilon(\varphi_B-\varphi). \tag{32}$$

Proof: The array factor $F(\rho,\varphi,k)$ in (29) can be rewritten as

$$F(\rho,\varphi,k)=\sqrt{P}\sum_{n=1}^{N}\Big[c_1\,\Xi_n(k)+c_2\Lambda_n(k)\Big], \tag{33}$$

where $c_1=\frac{\sqrt{t}}{\rho\sqrt{N}}-\frac{\sqrt{1-t}\Upsilon(\Delta\varphi)\epsilon(k)}{\rho\sqrt{N-N\Upsilon^2(\Delta\varphi)}}$ and $c_2=\frac{\sqrt{1-t}\epsilon(k)}{\rho\sqrt{N-N\Upsilon^2(\Delta\varphi)}}$. The injected noise term $\epsilon(k)$ follows a standard normal complex Gaussian distribution. Thus, $\mathbb{E}[c_1]=\frac{\sqrt{t}}{\rho\sqrt{N}}$ and $\mathbb{E}[c_2]=0$. In addition, we can find the average values of $\Xi_n(k)$ and $\Lambda_n(k)$ as

$$\begin{aligned}
\mathbb{E}[\Xi_n(k)]&=\mathbb{E}[\mathcal{R}\{\Xi_n(k)\}]+\mathbb{E}[\mathcal{I}\{\Xi_n(k)\}]\\
&=\int_{-1}^{1}\Bigg[\cos\left(\frac{4\pi R}{\lambda}\sin\left(\frac{\varphi_B-\varphi}{2}\right)x\right)\\
&\quad+\sin\left(\frac{4\pi R}{\lambda}\sin\left(\frac{\varphi_B-\varphi}{2}\right)x\right)\Bigg]f_{\check{u}_n(k)}(u)du\\
&=\Upsilon(\varphi_B-\varphi),
\end{aligned}\tag{34}$$

$$\begin{aligned}
\mathbb{E}[\Lambda_n(k)]&=\mathbb{E}[\mathcal{R}\{\Lambda_n(k)\}]+\mathbb{E}[\mathcal{I}\{\Lambda_n(k)\}]\\
&=\int_{-1}^{1}\Bigg[\cos\left(\frac{4\pi R}{\lambda}\sin\left(\frac{\varphi_{AN}-\varphi}{2}\right)x\right)\\
&\quad+\sin\left(\frac{4\pi R}{\lambda}\sin\left(\frac{\varphi_{AN}-\varphi}{2}\right)x\right)\Bigg]f_{\check{u}_n(k)}(u)du\\
&=\Upsilon(\varphi_{AN}-\varphi).
\end{aligned}\tag{35}$$

As a result, we obtain (32) as

$$\begin{aligned}
\mathbb{E}[F(\rho,\varphi,k)]&=\sqrt{PN}\Big(\mathbb{E}[c_1]\,\mathbb{E}[\Xi_n(k)]+\mathbb{E}[c_2]\,\mathbb{E}[\Lambda_n(k)]\Big)\\
&=\frac{\sqrt{tPN}}{\rho}\Upsilon(\varphi_B-\varphi).
\end{aligned}\tag{36}$$

□

Lemma 2: The variance of the array factor $F(\rho,\varphi,k)$ with the proposed CB with the AN injection is

$$\begin{aligned}
&\mathbb{V}\mathrm{ar}[F(\rho,\varphi,k)]\\
&=P\Bigg[\Big(\frac{t}{\rho^2}(1-\Upsilon^2(\varphi_B-\varphi))\Big)\\
&\quad+\frac{1-t}{\rho^2(1-\Upsilon^2(\Delta\varphi))}\Big(N\Upsilon^2(\Delta\varphi)\Upsilon^2(\varphi_B-\varphi)\\
&\quad+\Upsilon^2(\Delta\varphi)(1-\Upsilon^2(\varphi_B-\varphi))+N\Upsilon^2(\varphi_{AN}-\varphi)\\
&\quad+(1-\Upsilon^2(\varphi_{AN}-\varphi))\Big)-2\frac{(1-t)\Upsilon(\Delta\varphi)}{\rho^2(1-\Upsilon^2(\Delta\varphi))}\Big(\Upsilon(\Delta\varphi)\\
&\quad+(N-1)\Upsilon(\varphi_B-\varphi)\Upsilon(\varphi_{AN}-\varphi)\Big)\Bigg].
\end{aligned}\tag{37}$$

Proof: Please refer to Appendix. □

With the array factor statistics derived in Lemmas 1 and 2, we can first obtain the SNR at Bob γ_B in (27) with $(\rho,\varphi)=(\rho_B,\varphi_B)$, which corresponds to (38), as shown at the bottom of the next page. In the same manner, the SNR at Eve γ_E can be derived as (39), shown at the bottom of the next page, with $(\rho,\varphi)=(\rho_E,\varphi_E)$. Consequently, replacing (38) and (39) into (26), the secrecy rate η can be obtained in a closed-form expression in (40), as shown at the bottom of the next page. In the derived expression in (40), the secrecy rate η is a function of various system parameters such as the locations of Bob (ρ_B,φ_B) and Eve (ρ_E,φ_E), the AN injection angle φ_{AN}, the degree of the AN injection t, the number of nodes N, and the radius R of the VAA. Therefore, our analysis can be used to better design and optimize the secrecy rate. In particular, the optimal values of t and φ_{AN} can be readily obtained numerically using the derived secrecy rate in (40), instead of the exhaustive search through simulation with a large number of iterations. We will present simulation results in the next Section to validate our analysis and delve into the impacts of various system parameters.

VI. SECRECY RATE ANALYSIS WITH IMPERFECT CSI

In the previous section, we assume the perfect CSI condition, but it is technically challenging to achieve error-free CSI, when it comes to the implementation of CB in practice. For this reason, in this section, we analyze the secrecy rate degradation caused by CSI error. As indicated in (23), the CSI

between each VAA element and Bob is required to locally adjust the phase, so that the desired signal can be coherently combined through the data beamformer, while the AN is injected into the potential angular location of Eve. However, such CSI can be contaminated by various factors such as low-power beacon signals for the closed-loop CB. For this reason, we consider the phase synchronization error caused by the imperfect CSI and its impact on the secrecy rate.

With imperfect CSI, the data transmission beamformer in (10) is changed into

$$[\mathbf{w}_D^{\dagger}(k)]_n = \frac{e^{-j\frac{2\pi}{\lambda}[\rho_B - r_n(k)\cos(\varphi_B - \phi_n(k))] + \varsigma_n(k)}}{\sqrt{N}} = \frac{1}{\sqrt{N}}[\mathbf{v}^{\dagger}(\varphi_B, k)]_n, \tag{41}$$

where $[\mathbf{v}^{\dagger}(\varphi_B, k)]_n = e^{-j\frac{2\pi}{\lambda}[\rho_B - r_n(k)\cos(\varphi_B - \phi_n(k))] + \varsigma_n(k)}$ and $\varsigma_n(k)$ is the phase error due to the imperfect CSI. As modeled in [36], [39], [54], and [69], $\varsigma_n(k)$ is a random variable that follows a Tikhonov (or von Mises) distribution as

$$f_{\varsigma}(x) = \frac{1}{2\pi}\frac{\exp(\cos(x)\sigma_{\varsigma}^{-2})}{I_0(\sigma_{\varsigma}^{-2})}, \tag{42}$$

where $0 < x < 2\pi$ and σ_{ς}^{-2} is the variance of the phase error ς, which is related to the loop SNR γ_L of the PLL as $\sigma_{\varsigma}^{-2} = \frac{1}{\gamma_L}$. Furthermore, $I_m(\cdot)$ is the modified Bessel function of the first kind with order m. With such phase error term, we can also write the array manifold to the angle of the AN injection φ_{AN} as $[\mathbf{v}^{\dagger}(\varphi_{AN}, k)]_n = e^{-j\frac{2\pi}{\lambda}[\rho_{AN} - r_n(k)\cos(\varphi_{AN} - \phi_n(k))] + \varsigma_n(k)}$. Thus, in the presence of the phase estimation error, the

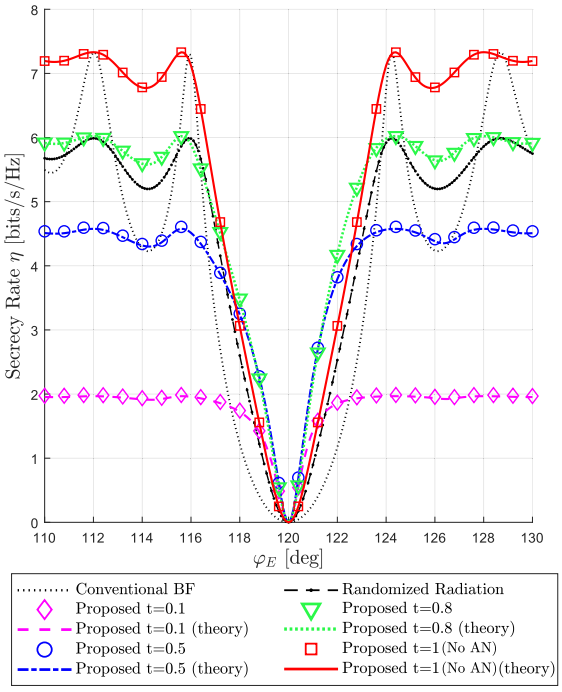


FIGURE 3. Secrecy rate η versus φ_E, when $\varphi_B = 120°$, $\varphi_{AN} = \varphi_B + 2° = 122°$, $N = 32$, $\rho_B = \rho_E = 1$ km, $R = 8\lambda$, t $\in \{0.1, 0.5, 0.8, 1\}$, and $\frac{P}{\rho_B^2\sigma^2} = 5$ dB.

precoding weight in (23) can be rewritten as

$$\tilde{\mathbf{w}}^{\dagger}(k) = \frac{\sqrt{t}}{\sqrt{N}}\mathbf{v}^{\dagger}(\varphi_B, k) + \frac{\epsilon(k)\sqrt{1-t}\left(\mathbf{v}^{\dagger}(\varphi_{AN}, k) - \Upsilon(\Delta\varphi)\,\mathbf{v}^{\dagger}(\varphi_B, k)\right)}{\sqrt{N - N\Upsilon^2(\Delta\varphi)}}$$

$$\gamma_B = \frac{t}{\frac{(1-t)\Upsilon^2(\Delta\varphi)}{1-\Upsilon^2(\Delta\varphi)} + \frac{(1-t)\Upsilon^2(\Delta\varphi)}{1-\Upsilon^2(\Delta\varphi)} + \frac{1-t}{N} - \frac{2(1-t)\Upsilon^2(\Delta\varphi)}{1-\Upsilon^2(\Delta\varphi)} + \frac{\rho_B^2\sigma^2}{NP}}. \tag{38}$$

$$\gamma_E = tN\Upsilon^2(\varphi_B - \varphi_E) \Big/ \Bigg[t(1-\Upsilon^2(\varphi_B - \varphi_E)) + \frac{1-t}{1-\Upsilon^2(\Delta\varphi)}\Big(N\Upsilon^2(\Delta\varphi)\Upsilon^2(\varphi_B - \varphi_E) + \Upsilon^2(\Delta\varphi)(1-\Upsilon^2(\varphi_B - \varphi_E)) + N\Upsilon^2(\varphi_{AN} - \varphi_E) + (1-\Upsilon^2(\varphi_{AN} - \varphi_E))\Big) - 2\frac{(1-t)\Upsilon(\Delta\varphi)}{1-\Upsilon^2(\Delta\varphi)}\Big(\Upsilon(\Delta\varphi) + (N-1)\Upsilon(\varphi_B - \varphi_E)\Upsilon(\varphi_{AN} - \varphi_E)\Big) + \frac{\rho_E^2\sigma^2}{P}\Bigg]. \tag{39}$$

$$\eta = \Bigg[\log_2\left(1 + \frac{t}{\frac{(1-t)\Upsilon^2(\Delta\varphi)}{1-\Upsilon^2(\Delta\varphi)} + \frac{(1-t)\Upsilon^2(\Delta\varphi)}{1-\Upsilon^2(\Delta\varphi)} + \frac{1-t}{N} - \frac{2(1-t)\Upsilon^2(\Delta\varphi)}{1-\Upsilon^2(\Delta\varphi)} + \frac{\rho_B^2\sigma^2}{NP}}\right) - \log_2\Bigg(1 + \Big(tN\Upsilon^2(\varphi_B - \varphi_E) \Big/ \Big[t(1-\Upsilon^2(\varphi_B - \varphi_E)) + \frac{(1-t)N\Upsilon^2(\Delta\varphi)\Upsilon^2(\varphi_B - \varphi_E)}{1-\Upsilon^2(\Delta\varphi)} + \frac{(1-t)\Upsilon^2(\Delta\varphi)(1-\Upsilon^2(\varphi_B - \varphi_E))}{1-\Upsilon^2(\Delta\varphi)} + \frac{(1-t)N\Upsilon^2(\varphi_{AN} - \varphi_E)}{1-\Upsilon^2(\Delta\varphi)} + \frac{(1-t)(1-\Upsilon^2(\varphi_{AN} - \varphi_E))}{1-\Upsilon^2(\Delta\varphi)} - 2\frac{(1-t)\Upsilon(\Delta\varphi)}{1-\Upsilon^2(\Delta\varphi)}\Big(\Upsilon(\Delta\varphi) + (N-1)\Upsilon(\varphi_B - \varphi_E)\Upsilon(\varphi_{AN} - \varphi_E)\Big) + \frac{\rho_E^2\sigma^2}{P}\Big]\Big)\Bigg)\Bigg]^{+}. \tag{40}$$

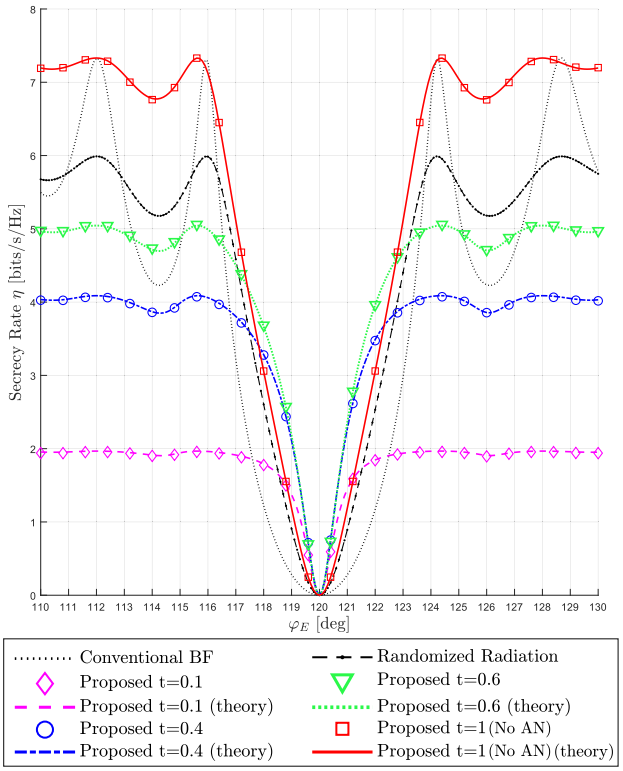


FIGURE 4. Secrecy rate η versus φ_E, when $\varphi_B = 120°$, $\varphi_{AN} = \varphi_B + 1° = 121°$, $N = 32$, $\rho_B = \rho_E = 1$ km, $R = 8\lambda$, t $\in \{0.1, 0.4, 0.6, 1\}$, and $\frac{P}{\rho_B^2 \sigma^2} = 5$ dB.

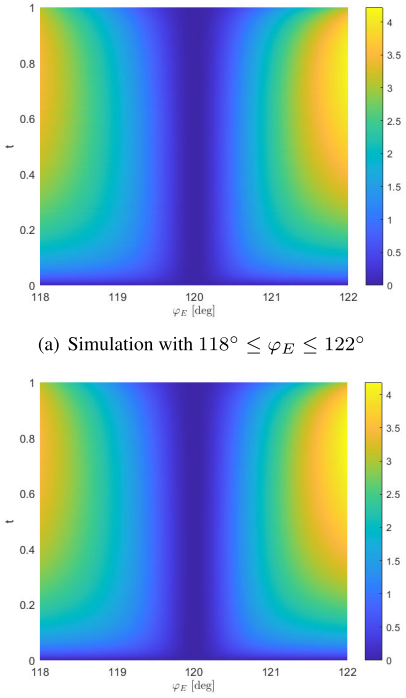
$$= \left[\frac{\sqrt{t}}{\sqrt{N}} - \frac{\epsilon(k)\Upsilon(\Delta\varphi)\sqrt{1-t}}{\sqrt{N - N\Upsilon^2(\Delta\varphi)}} \right] \mathbf{v}^\dagger(\varphi_B, k) + \frac{\epsilon(k)\sqrt{1-t}}{\sqrt{N - N\Upsilon^2(\Delta\varphi)}} \mathbf{v}^\dagger(\varphi_{AN}, k), \tag{43}$$

where $\mathbf{v}^\dagger(\varphi, k)$ is the array manifold with the phase error due to the imperfect CSI. Accordingly, the received signal under the imperfect CSI is derived as

$$\begin{aligned} y^\dagger(\rho, \varphi, k) &= \sqrt{P}\,\mathbf{h}(\rho, \varphi, k)\tilde{\mathbf{w}}^\dagger(k)s(k) + z(k) \\ &= F^\dagger(\rho, \varphi, k)s(k) + z(k), \end{aligned} \tag{44}$$

where $F^\dagger(\rho, \varphi, k)$ is the array factor under the imperfect CSI. It is noted that $(\rho, \varphi) = (\rho_B, \varphi_B)$ and $(\rho, \varphi) = (\rho_E, \varphi_E)$ for Bob and Eve, respectively. Due to the phase error, the array factor with the perfect CSI in (29) becomes

$$\begin{aligned} &F^\dagger(\rho, \varphi, k) \\ &= \sqrt{P}\sum_{n=1}^{N} h_n(\rho, \varphi, k)[\tilde{\mathbf{w}}^\dagger(k)]_n \\ &= \sqrt{P}\sum_{n=1}^{N} \left(\sqrt{t}\frac{e^{j\frac{2\pi}{\lambda}r_n(k)\cos(\varphi_B - \phi_n(k)) + \varsigma_n(k)}}{\sqrt{N}} \right. \\ &\quad \left. + \frac{\sqrt{1-t}e^{j\frac{2\pi}{\lambda}r_n(k)\cos(\varphi_{AN} - \phi_n(k)) + \varsigma_n(k)}\epsilon(k)}{\sqrt{N - N\Upsilon^2(\Delta\varphi)}} \right. \\ &\quad \left. - \frac{\sqrt{1-t}\Upsilon(\Delta\varphi)e^{j\frac{2\pi}{\lambda}r_n(k)\cos(\varphi_B - \phi_n(k)) + \varsigma_n(k)}\epsilon(k)}{\sqrt{N - N\Upsilon^2(\Delta\varphi)}} \right) \\ &\quad \times \frac{1}{\rho} e^{-j\frac{2\pi}{\lambda}r_n(k)\cos(\varphi - \phi_n(k))}. \end{aligned} \tag{45}$$



(a) Simulation with $118° \le \varphi_E \le 122°$

(b) Theory with $118° \le \varphi_E \le 122°$

FIGURE 5. Secrecy rate η versus φ_E and t, when $\varphi_B = 120°$, $\varphi_{AN} = \varphi_B + 2° = 122°$, $N = 32$, $\rho_B = \rho_E = 1$ km, $R = 8\lambda$, and $\frac{P}{\rho_B^2 \sigma^2} = 5$ dB.

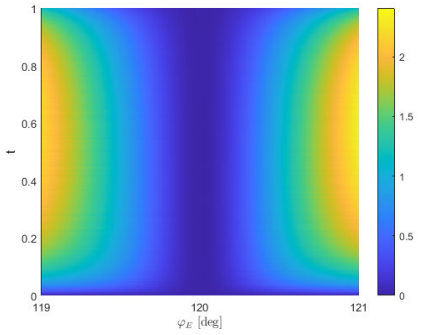
The average and variance of the array factor under the imperfect CSI, $F^\dagger(\rho, \varphi, k)$, can be expressed as

$$\begin{aligned} \mathbb{E}[F^\dagger(\rho, \varphi, k)] &= \mathbb{E}\left[e^{j\varsigma_n(k)}\right]\mathbb{E}[F(\rho, \varphi, k)] \\ &= \frac{I_1(\sigma_\varsigma^{-2})}{I_0(\sigma_\varsigma^{-2})}\mathbb{E}[F(\rho, \varphi, k)], \end{aligned} \tag{46}$$

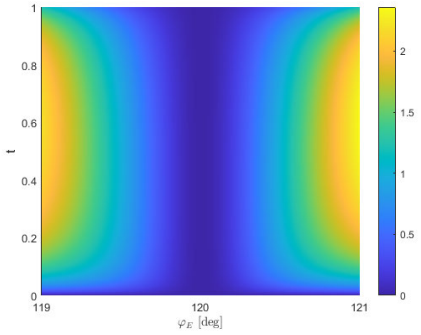
and

$$\begin{aligned} \mathbb{V}\mathrm{ar}[F^\dagger(\rho, \varphi, k)] &= \frac{1}{N}(\mathbb{E}[F(\rho, \varphi, k)])^2\,\mathbb{V}\mathrm{ar}\left[e^{j\varsigma_n(k)}\right] \\ &\quad + \mathbb{V}\mathrm{ar}[F(\rho, \varphi, k)]\left(\mathbb{E}\left[e^{j\varsigma_n(k)}\right]\right)^2 \\ &\quad + \mathbb{V}\mathrm{ar}[F(\rho, \varphi, k)]\,\mathbb{V}\mathrm{ar}\left[e^{j\varsigma_n(k)}\right] \\ &= \frac{(\mathbb{E}[F(\rho, \varphi, k)])^2}{N}\left(1 - \left(\frac{I_1(\sigma_\varsigma^{-2})}{I_0(\sigma_\varsigma^{-2})}\right)^2\right) \\ &\quad + \mathbb{V}\mathrm{ar}[F(\rho, \varphi, k)], \end{aligned} \tag{47}$$

where $F(\rho, \varphi, k)$ is the array factor with perfect CSI. Because the original array factor and the phase errors $\varsigma_n(k)$'s are independent. By the following formula as $\mathbb{E}\left[e^{j\varsigma_n(k)}\right] = \int_{-\pi}^{\pi} e^{j\varsigma} \cdot f_\varsigma(e)de = \frac{I_1(\sigma_\varsigma^{-2})}{I_0(\sigma_\varsigma^{-2})}$ and $\mathbb{V}\mathrm{ar}\left[e^{j\varsigma_n(k)}\right] = \mathbb{V}\mathrm{ar}[\mathcal{R}[e^{j\varsigma_n(k)}] + \mathbb{V}\mathrm{ar}[\mathcal{I}[e^{j\varsigma_n(k)}]] = 1 - \left(\mathbb{E}\left[e^{j\varsigma_n(k)}\right]\right)^2$, we can easily compute



(a) Simulation with $119° \leq \varphi_E \leq 121°$



(b) Theory with $119° \leq \varphi_E \leq 121°$

FIGURE 6. Secrecy rate η versus φ_E and t, when $\varphi_B = 120°$, $\varphi_{AN} = \varphi_B + 1° = 121°$, $N = 32$, $\rho_B = \rho_E = 1$ km, $R = 8\lambda$, and $\frac{P}{\rho_B^2 \sigma^2} = 5$ dB.

(46) and (47) based on the CSI error-free results in (36) and (37). Correspondingly, with (46) and (47), we can calculate γ_B and γ_E in (38) and (39), by simply replacing the array factor $F(\rho, \varphi, k)$ into $F^{\dagger}(\rho, \varphi, k)$. As a result, we can derive the secrecy rate in the presence of the phase estimation error. In Section VII-F, we will validate our analysis by comparing it with simulation results and present how the secrecy rate varies with the loop SNR.

VII. SIMULATION RESULTS

In this section, we evaluate the proposed CB-based PLS with AN injection through simulation and numerical results. For the simulation, the carrier frequency is assumed to be 5GHz, where the wavelength λ is about 0.06m. In addition, the simulation results are made through 10^4 random realizations of the VAA element locations following the 2D uniform distribution. Furthermore, for comparison, we consider the CB without the AN injection in [34], [35], and [36]. Also, we compare our proposed scheme with the conventional analog beamforming (conventional BF) and the randomized radiation scheme in [20], both of which exploit the *co-located* (or real) antenna array.

A. SECRECY RATE WITH DIFFERENT ANGULAR LOCATIONS OF EVE

Figs. 3 and 4 show how the secrecy rate η changes with different angular locations of Eve, φ_E. In the figures, the

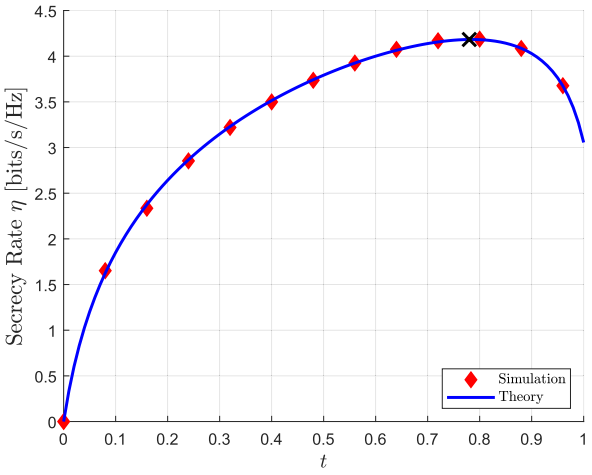


FIGURE 7. Secrecy rate η versus t, when $\varphi_B = 120°$, $\varphi_E = \varphi_{AN} = \varphi_B + 2° = 122°$, $N = 32$, $\rho_B = \rho_E = 1$ km, $R = 8\lambda$, and $\frac{P}{\rho_B^2 \sigma^2} = 5$ dB.

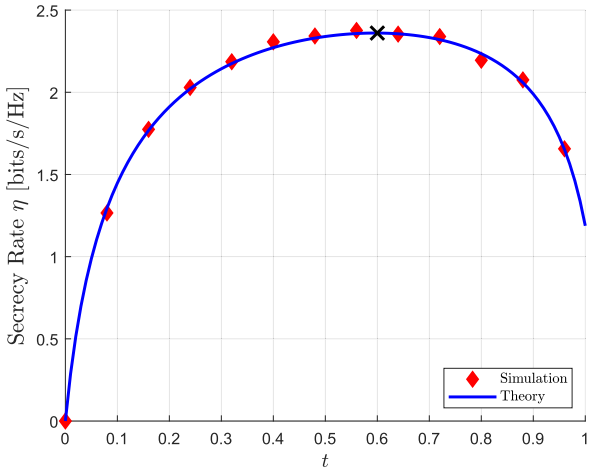
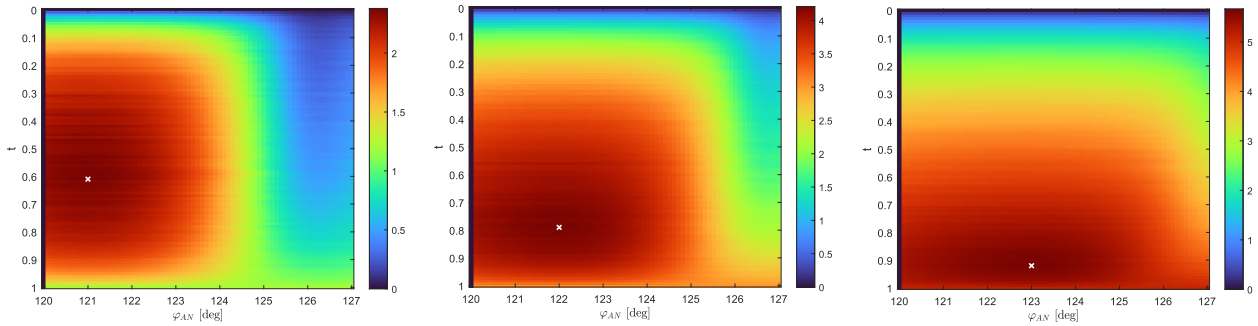


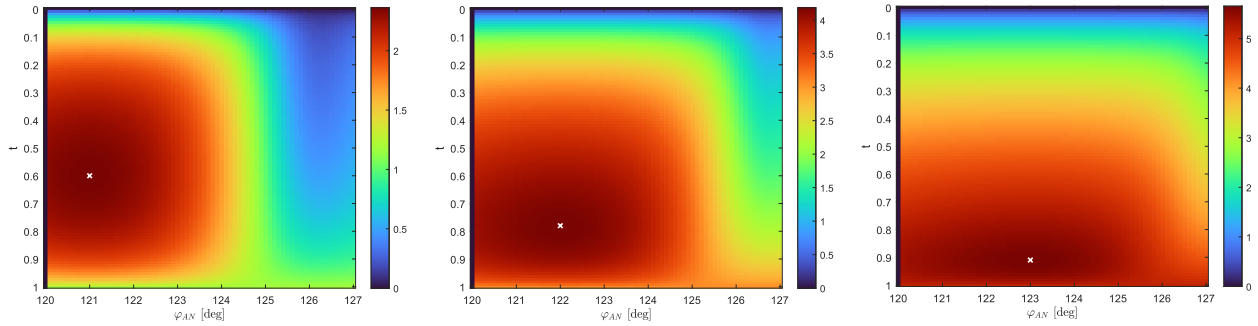
FIGURE 8. Secrecy rate η versus t, when $\varphi_B = 120°$, $\varphi_E = \varphi_{AN} = \varphi_B + 1° = 121°$, $N = 32$, $\rho_B = \rho_E = 1$ km, $R = 8\lambda$, and $\frac{P}{\rho_B^2 \sigma^2} = 5$ dB.

horizontal axis indicates φ_E, while the vertical axis corresponds to η. Further, the different colored curves and markers represent the theoretical and simulation results, respectively, with different degrees of the AN injection, characterized by t. It is noted that the results with $t = 1$ correspond to the pure CB without AN injection proposed in [34], [35], and [36]. We first observe that the theoretical results based on the closed-form expression of the secrecy rate derived in the previous Section are consistent with the corresponding simulation results, which validate our analysis.

In addition, as shown in the figures, the secrecy rate of the original CB without AN injection in [34], [35], and [36] is low when the angular location of Eve is close to Bob (i.e., $|\varphi_E - \varphi_B|$ is small). On the other hand, the results with $0 < t < 1$ show higher secrecy rate compared to that with $t = 1$ (i.e., the CB without AN injection). In addition, for Eve in close proximity to Bob, the proposed scheme provides



(a) Simulation with $\varphi_E = \varphi_B + 2^\circ = 121^\circ$ (b) Simulation with $\varphi_E = \varphi_B + 2^\circ = 122^\circ$ (c) Simulation with $\varphi_E = \varphi_B + 2^\circ = 123^\circ$



(d) Theory with $\varphi_E = \varphi_B + 2^\circ = 121^\circ$ (e) Theory with $\varphi_E = \varphi_B + 2^\circ = 122^\circ$ (f) Theory with $\varphi_E = \varphi_B + 2^\circ = 123^\circ$

FIGURE 9. Secrecy rate η versus φ_{AN} and t, when $\varphi_B = 120°$, $\rho_B = \rho_E = 1$ km, $N = 32$, $R = 8\lambda$, and $\frac{P}{\rho_B^2 \sigma^2} = 5$ dB.

higher secrecy rate compared to the co-located antenna-based schemes (i.e., conventional BF and randomized radiation). Thus, the proposed decentralized AN injection beamformer can be an effective solution to overcome the limited secrecy rate caused by Eve located close to Bob. However, when φ_E is far from φ_B, the original CB without AN injection (i.e., $t = 1$) outperforms the AN injection beamformer (i.e., $0 < t < 1$), because of the loss in the array factor or power at Bob to create AN. Therefore, the degree of the AN injection, t, should be pertinently determined depending on the relative angular locations of Bob and Eve.

B. DEGREE OF AN INJECTION

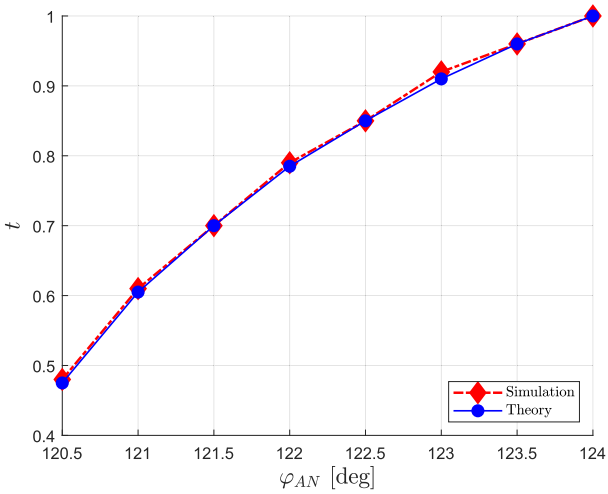
In Figs. 5 and 6, we further investigate the impact of the degree of the AN injection t with different AN injection angles (i.e., $\varphi_{AN} = 122^\circ$ and 121° for Figs. 5 and 6, respectively). In both figures, we show the secrecy rate η with the different angular locations of Eve φ_E and the degree of AN injection t, which correspond to the x-axis and y-axis, respectively. Also, the two sub-figures in Figs. 5 and 6 correspond to the simulation and theoretical analysis, respectively, which show the identical performances. In the figures, we observe that the optimal value of t, which corresponds to the maximum secrecy rate η is subject to the angular location of Eve φ_E.

As expected, in both Figs. 5 and 6, the secrecy rate η becomes zero, when Eve is located along the same angle as Bob (i.e., $\varphi_E = \varphi_B = 120^\circ$). Also, in Fig. 5, when $\varphi_E = 122^\circ$, the secrecy rate is maximized with $t \approx 0.8$. Similarly, in Fig. 6, for $\varphi_E = 121^\circ$, the secrecy rate has its maximum, when $t \approx 0.6$. In both figures, we conclude that the proposed AN injection with pertinent t can provide higher secrecy rate compared to the CB-based PLS without the AN injection in [34], [35],and [36], which corresponds to $t = 1$.

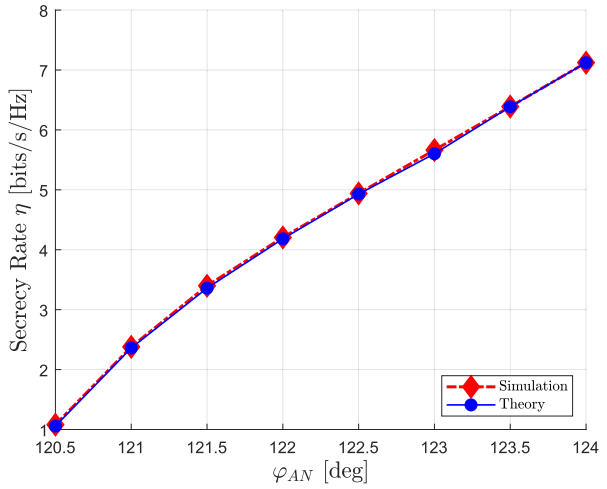
To delve into the impact of t, we plot the cross-sectional view of Fig. 5 with $\varphi_E = 122^\circ$ and $\varphi_E = 121^\circ$ in Figs. 7 and 8, respectively. Fig. 7 shows the secrecy rate η with respect to the value of t at $\varphi_E = \varphi_{AN} = 122^\circ$, where the maximum secrecy rate is achieved when $t = 0.79$, which is indicated by the 'x'-marker in the figure. Similarly, Fig. 8 shows η as a function of t with Eve's location of $\varphi_E = \varphi_{AN} = 121^\circ$, in which we observe the maximum secrecy throughput is obtained with $t = 0.6$. As shown in both Figs. 7 and 8, there is an optimal value of t that corresponds to the maximum secrecy rate. However, the optimal values, indicated by the 'x'-makers are different in the two figures. Therefore, as presented in Figs. 5 and 6, the optimal degree of AN injection t is subject to Eve's angular location φ_E.

C. ARTIFICIAL NOISE INJECTION ANGLE

In Fig. 9, we consider how the secrecy rate η changes with the different angular locations of AN injection φ_{AN} and the degrees of AN injection t, which are indicated by the horizontal and vertical axes, respectively. Figs. 9(a), (b), and (c) show the simulation results with $\varphi_E = 121^\circ$, 122°, and 123°, respectively, whereas Figs. 9(d), (e), and (f) are corresponding theoretical results. From the figures, the simulation results are consistent with the theoretical results.

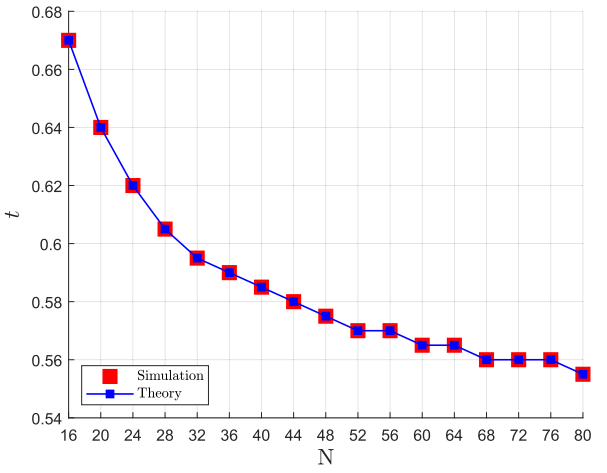


(a) Optimal t

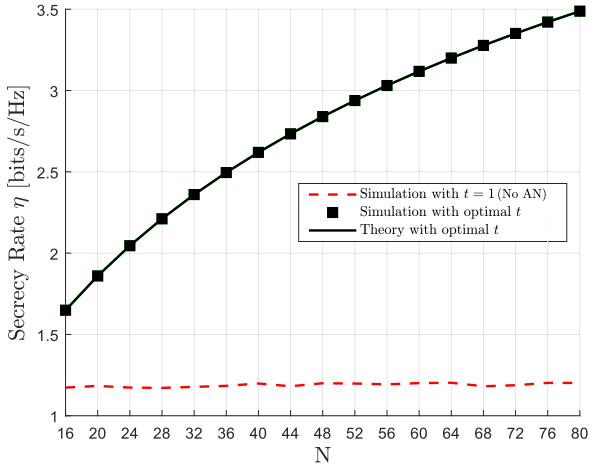


(b) Optimal secrecy rate

FIGURE 10. Optimal t and the corresponding η, when $\varphi_B = 120°$, $\rho_B = \rho_E = 1$ km, $N = 32$, $R = 8\lambda$, and $\frac{P}{\rho_B^2 \sigma^2} = 5$ dB.



(a) Optimal t



(b) Optimal secrecy rate

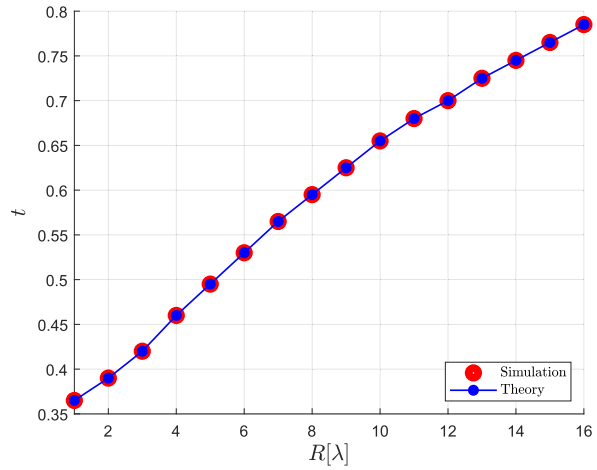
FIGURE 11. Optimal t and the corresponding η with different number of nodes N, when $\varphi_B = 120°$, $\varphi_E = \varphi_{AN} = \varphi_B + 1° = 121°$, $\rho_B = \rho_E = 1$ km, $R = 8\lambda$, and $\frac{P}{\rho_B^2 \sigma^2} = 5$ dB.

Also, in the figures, the 'x'-markers indicate the values of φ_{AN} and t that jointly maximize η. We observe that in all of the figures, the optimal φ_{AN} is the same as φ_E, which means that the maximum η can be achieved by injecting AN towards Eve's angular location. On the other hand, as φ_{AN} becomes more distinct from φ_E, the secrecy rate η decreases. Thus, assuming $\varphi_{AN} = \varphi_E$, the optimal value of t and the corresponding maximum secrecy rate η are shown in Figs. 10(a) and (b), respectively.

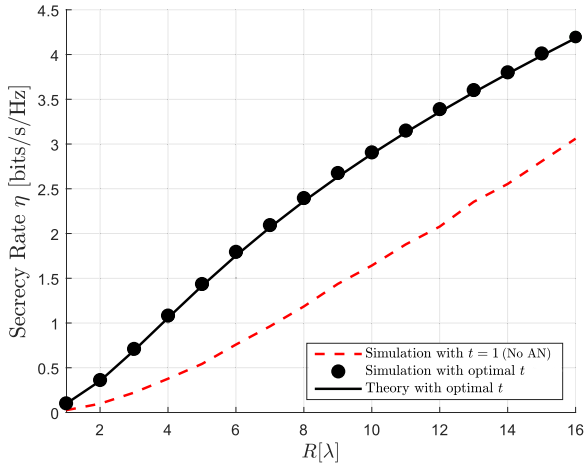
Fig. 10(a) shows the optimal values of t that maximize the secrecy rate η with the varying φ_{AN} for given parameters. The maximum secrecy rate with such adjustment of t corresponds to the optimal secrecy rate in Fig. 10(b). In the simulation, the optimal t is obtained by exhaustive search with the step size of 0.01. In other words, the value of t that provides the maximum secrecy rate η is chosen as the optimal one. In contrast, the theoretical optimum of t is computed numerically using the derived secrecy rate expression in (40) through analysis. As shown in the example result in Figs. 7 and 8, obtaining such best t values is straightforward through analysis. In Fig. 10, it can be confirmed that when the location of Eve, which is the same as the AN injection location ($\varphi_E = \varphi_{AN}$), is 122° and 121°, the results are the same as those in Figs. 7 and 8, respectively. Based on the high correlation between simulation and theoretical results observed in Fig. 10, we can conclude that the secrecy rate expression derived in (40) can be exploited to better operate the proposed PLS scheme for given system parameters. As shown in Fig. 10(a), the optimal t increases as the gap between φ_B and $\varphi_{AN} = \varphi_E$ increases. In other words, a higher degree of the AN injection is required, when the angular locations of Bob and Eve are closer.

D. NUMBER OF VAA ELEMENTS

In Fig. 11, we investigate the impact of the number of the VAA elements N on the optimal t and η. As in the investigation on φ_{AN} in Fig. 10, we compare the simulation and



(a) Optimal t



(b) Optimal secrecy rate

FIGURE 12. Optimal t and the corresponding η with different VAA sizes R, when $\varphi_B = 120°$, $\varphi_E = \varphi_{AN} = \varphi_B + 1° = 121°$, $\rho_B = \rho_E = 1$ km, $N = 32$, and $\frac{P}{\rho_B^2 \sigma^2} = 5$ dB.

theoretical results with different N, which are obtained by exhaustive search and analytical expression in (40). Fig. 11(a) shows the value of t that maximizes the secrecy rate η for the given number of nodes, whereas Fig. 11(b) shows the corresponding optimal (i.e., maximum) secrecy rate η for each number of nodes. In Fig. 11(b), for the conventional CB beamformer without the AN injection (i.e., $t = 1$) in [34], [35], and [36], the number of the VAA elements gives a little impact on the secrecy rate. However, the proposed scheme provides the different optimal secrecy throughput with respect to N, which increases with N. In addition, Fig. 11(a) demonstrates that the optimal t decreases as N rises.

E. VAA SIZE

The size of the VAA, which is characterized by its radius R, affects the secrecy throughput η. Figs. 12(a) and (b) show the optimal degree of the AN injection t and the corresponding secrecy rate η, respectively. In Fig. 12(a), we observe that

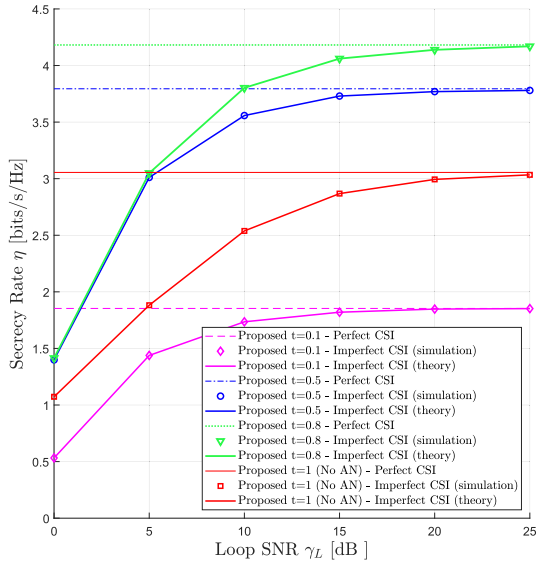


FIGURE 13. Secrecy rate η with the imperfect CSI versus loop SNR γ_L, when $\varphi_B = 120°$, $\varphi_E = \varphi_{AN} = \varphi_B + 2° = 122°$, $N = 32$, $\rho_B = \rho_E = 1$ km, $R = 8\lambda$, $t \in \{0.1, 0.5, 0.8, 1\}$, and $\frac{P}{\rho_B^2 \sigma^2} = 5$ dB.

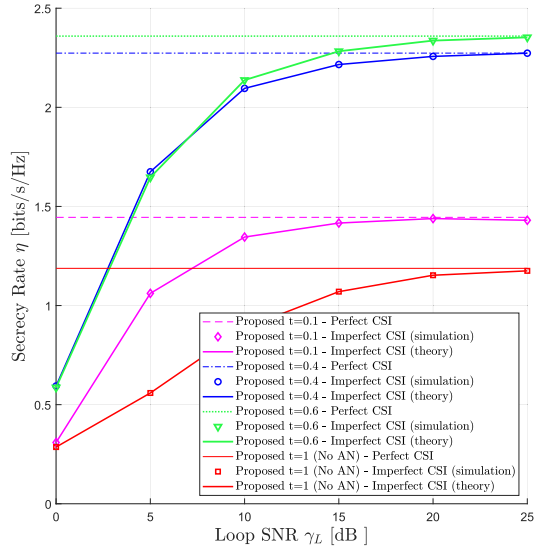


FIGURE 14. Secrecy rate η with the imperfect CSI versus loop SNR γ_L, when $\varphi_B = 120°$, $\varphi_E = \varphi_{AN} = \varphi_B + 1° = 121°$, $N = 32$, $\rho_B = \rho_E = 1$ km, $R = 8\lambda$, $t \in \{0.1, 0.4, 0.6, 1\}$, and $\frac{P}{\rho_B^2 \sigma^2} = 5$ dB.

the optimal t increases, as R grows. Further, in Fig. 12(b), with larger R, η increases for both proposed scheme and CB without the AN injection, because of the larger effective aperture size. However, the proposed scheme provides better η, as compared to the conventional CB without the AN injection (i.e., $t = 1$).

F. IMPERFECT CSI

Figs. 13 and 14 show the performance degradation caused by the CSI error η with $\varphi_E = \varphi_{AN} = 122°$ and $\varphi_E = \varphi_{AN} = 121°$, respectively. In the figures, the vertical axis indicates the secrecy rate η, whereas the horizontal axis represents the loop SNR γ_L in decibel (dB) scale. As discussed in

Section VI, the phase synchronization error increases as the loop SNR γ_L decreases. In both figures, we observe that the simulation results are consistent with the theoretical results, which validate our analysis in Section VI. In Fig. 13, with any γ_L, the proposed scheme with proper AN injection (i.e., $t = 0.5, 0.8$) still outperforms the conventional CB-based PLS without the AN injection (i.e., $t = 1$). Comparing the results in Figs. 13 and 14, the proposed scheme can be more effective, when the angular location of Eve, φ_E, is closer to that of Bob, φ_B. Moreover, in both figures, regardless of any value of the degree of the AN injection t, as the loop SNR is low, the secrecy rate is significantly decreased compared to the perfect CSI case. On the other hand, when the loop SNR is greater than or equal to 25dB, the secrecy rate performance is almost the same as the error-free results. Therefore, we can conclude that achieving accurate CSI is of paramount importance.

VIII. CONCLUSION

In this paper, we have proposed a CB-based PLS scheme with AN injection, which can be realized in a fully distributed manner by using statistical information of the array factor of VAA. The proposed scheme can be a desirable solution for the massive IoT networks with hardware limitations to protect against eavesdropping attacks, when Eve is in close proximity to Bob. In such a case, while the conventional CB-based PLS reveals high vulnerability, our proposed scheme can provide vastly higher secrecy rate by adjusting the degree of the AN injection. We have derived the closed-form expression for the secrecy rate of our proposed scheme in both the absence and presence of the CSI error, which has been confirmed by comparing it with simulation results. Further, we have investigated the impacts of various system parameters such as the number of VAA elements and the size of VAA on the secrecy rate, which provides insights for designing and operating the CB-based PLS systems with the AN injection. Simulation results have indicated that our proposed scheme with the optimized AN injection can provide a performance improvement of up to two times compared to the conventional CB-based PLS schemes, which corresponds to $t = 1$. Moreover, such performance gain increases as the angular location of Eve becomes closer to that of Bob, which corresponds to the most vulnerable situation of the conventional CB-based PLS algorithms.

APPENDIX: PROOF OF LEMMA 2

From (33), the variance of the array factor is expressed as

$$\begin{aligned}
&\mathbb{V}\mathrm{ar}[F(\rho,\varphi,k)] \\
&= P\,\mathbb{V}\mathrm{ar}\Big[\sum_{n=1}^{N}(c_1\Xi_n(k)+c_2\Lambda_n(k))\Big] \\
&= P\Big[\mathbb{V}\mathrm{ar}[\sum_{n=1}^{N}c_1\Xi_n(k)]+\mathbb{V}\mathrm{ar}[\sum_{n=1}^{N}c_2\Lambda_n(k)] \\
&\quad+2\,\mathbb{C}\mathrm{ov}[\sum_{n=1}^{N}c_1\Xi_n(k),\sum_{n=1}^{N}c_2\Lambda_n(k)] \\
&= P\Big[\mathbb{V}\mathrm{ar}[\mathcal{R}\{\sum_{n=1}^{N}c_1\Xi_n(k)\}]+\mathbb{V}\mathrm{ar}[\mathcal{I}\{\sum_{n=1}^{N}c_1\Xi_n(k)\}] \\
&\quad+\mathbb{V}\mathrm{ar}[\mathcal{R}\{\sum_{n=1}^{N}c_2\Lambda_n(k)\}]+\mathbb{V}\mathrm{ar}[\mathcal{I}\{\sum_{n=1}^{N}c_2\Lambda_n(k)\}] \\
&\quad+2\,\mathbb{C}\mathrm{ov}[\mathcal{R}\{\sum_{n=1}^{N}c_1\Xi_n(k)\},\mathcal{R}\{\sum_{n=1}^{N}c_2\Lambda_n(k)\}] \\
&\quad+2\,\mathbb{C}\mathrm{ov}[\mathcal{I}\{\sum_{n=1}^{N}c_1\Xi_n(k)\},\mathcal{I}\{\sum_{n=1}^{N}c_2\Lambda_n(k)\}] \\
&\quad+2\,\mathbb{C}\mathrm{ov}[\mathcal{R}\{\sum_{n=1}^{N}c_1\Xi_n(k)\},\mathcal{I}\{\sum_{n=1}^{N}c_2\Lambda_n(k)\}] \\
&\quad+2\,\mathbb{C}\mathrm{ov}[\mathcal{I}\{\sum_{n=1}^{N}c_1\Xi_n(k)\},\mathcal{R}\{\sum_{n=1}^{N}c_2\Lambda_n(k)\}]\Big]. \qquad (48)
\end{aligned}$$

It is noted that the variances of c_1 and c_2 become

$$\mathbb{V}\mathrm{ar}[c_1] = \frac{(1-t)\Upsilon^2(\Delta\varphi)}{\rho^2(N-N\Upsilon^2(\Delta\varphi))}, \qquad (49)$$

$$\mathbb{V}\mathrm{ar}[c_2] = \frac{1-t}{\rho^2(N-N\Upsilon^2(\Delta\varphi))}, \qquad (50)$$

respectively. Moreover, $\mathbb{V}\mathrm{ar}[\Xi_n(k)]$ and $\mathbb{V}\mathrm{ar}[\Lambda_n(k)]$ can be obtained as

$$\begin{aligned}
\mathbb{V}\mathrm{ar}[\Xi_n(k)] &= \mathbb{V}\mathrm{ar}[\mathcal{R}\{\Xi_n(k)\}]+\mathbb{V}\mathrm{ar}[\mathcal{I}\{\Xi_n(k)\}] \\
&= \int_{-1}^{1}\Big[\cos^2\Big(\frac{4\pi R}{\lambda}\sin\Big(\frac{\varphi_B-\varphi}{2}\Big)x\Big) \\
&\quad+\sin^2\Big(\frac{4\pi R}{\lambda}\sin\Big(\frac{\varphi_B-\varphi}{2}\Big)x\Big)\Big]f_{\hat{u}_n(k)}(u)du \\
&\quad-(\mathbb{E}[\mathcal{R}\{\Xi_n(k)\}])^2-(\mathbb{E}[\mathcal{I}\{\Xi_n(k)\}])^2 \\
&= 1-\Upsilon^2(\varphi_B-\varphi), \qquad (51) \\
\mathbb{V}\mathrm{ar}[\Lambda_n(k)] &= \mathbb{V}\mathrm{ar}[\mathcal{R}\{\Lambda_n(k)\}]+\mathbb{V}\mathrm{ar}[\mathcal{I}\{\Lambda_n(k)\}] \\
&= 1-\Upsilon^2(\varphi_{AN}-\varphi), \qquad (52)
\end{aligned}$$

respectively. Now, we consider each term in (48) as follows:

$$\begin{aligned}
&\mathbb{V}\mathrm{ar}\Big[\mathcal{R}\{\sum_{n=1}^{N}c_1\Xi_n(k)\}\Big] \\
&= \mathbb{V}\mathrm{ar}\Big[\sum_{n=1}^{N}c_{R1}\Xi_{Rn}(k)+\sum_{n=1}^{N}c_{I1}\Xi_{In}(k)\Big] \\
&= \mathbb{V}\mathrm{ar}[\sum_{n=1}^{N}c_{R1}\Xi_{Rn}(k)]+\mathbb{V}\mathrm{ar}[\sum_{n=1}^{N}c_{I1}\Xi_{In}(k)] \\
&\quad+2\,\mathbb{C}\mathrm{ov}[\sum_{n=1}^{N}c_{R1}\Xi_{Rn}(k),\sum_{n=1}^{N}c_{I1}\Xi_{In}(k)], \qquad (53)
\end{aligned}$$

where $c_{R1} = \mathcal{R}\{c_1\}$, $c_{I1} = \mathcal{I}\{c_1\}$, $\Xi_{Rn}(k) = \mathcal{R}\{\Xi_n(k)\}$, and $\Xi_{In}(k) = \mathcal{I}\{\Xi_n(k)\}$. In (53), we have

$$\mathbb{V}\mathrm{ar}[\sum_{n=1}^{N}c_{R1}\Xi_{Rn}(k)] = \mathbb{E}[c_{R1}]^2\,\mathbb{V}\mathrm{ar}[\sum_{n=1}^{N}\Xi_{Rn}(k)]$$

$$+\mathbb{E}[\sum_{n=1}^{N}\Xi_{Rn}(k)]^2\,\mathbb{V}\mathrm{ar}[c_{R1}] + \mathbb{V}\mathrm{ar}[c_{R1}]\,\mathbb{V}\mathrm{ar}[\sum_{n=1}^{N}\Xi_{Rn}(k)], \quad (54)$$

$$\mathbb{V}\mathrm{ar}[\sum_{n=1}^{N}c_{I1}\,\Xi_{In}(k)] = \mathbb{E}[c_{I1}]^2\,\mathbb{V}\mathrm{ar}[\sum_{n=1}^{N}\Xi_{In}(k)] + \mathbb{E}[\sum_{n=1}^{N}\Xi_{In}(k)]^2\,\mathbb{V}\mathrm{ar}[c_{I1}] + \mathbb{V}\mathrm{ar}[c_{I1}]\,\mathbb{V}\mathrm{ar}[\sum_{n=1}^{N}\Xi_{In}(k)]. \quad (55)$$

Because $(\mathbb{E}[c_{R1}])^2 = (\mathbb{E}[c_{I1}])^2 = \frac{1}{2}(\mathbb{E}[c_1])^2$ and $\mathbb{V}\mathrm{ar}[c_{R1}] = \mathbb{V}\mathrm{ar}[c_{I1}] = \frac{1}{2}\mathbb{V}\mathrm{ar}[c_1]$, the sum of (54) and (55), which are present in (53), is simplified as

$$\begin{aligned}
&\mathbb{V}\mathrm{ar}[\sum_{n=1}^{N}c_{R1}\,\Xi_{Rn}(k)] + \mathbb{V}\mathrm{ar}[\sum_{n=1}^{N}c_{I1}\,\Xi_{In}(k)] \\
&= \frac{1}{2}\,\mathbb{E}[c_1]^2\,\mathbb{V}\mathrm{ar}[\sum_{n=1}^{N}\Xi_n(k)] + \frac{1}{2}\,\mathbb{V}\mathrm{ar}[c_1]\,\mathbb{E}[\sum_{n=1}^{N}\Xi_n(k)]^2 \\
&\quad + \frac{1}{2}\,\mathbb{V}\mathrm{ar}[c_1]\,\mathbb{V}\mathrm{ar}[\sum_{n=1}^{N}\Xi_n(k)] \\
&= N\Big(\frac{t}{2\rho^2 N}(1-\Upsilon^2(\varphi_B-\varphi))\Big) \\
&\quad + N^2\Big(\frac{(1-t)\Upsilon^2(\Delta\varphi)}{2\rho^2(N-N\Upsilon^2(\Delta\varphi))}\Upsilon^2(\varphi_B-\varphi)\Big) \\
&\quad + N\Big(\frac{(1-t)\Upsilon^2(\Delta\varphi)}{2\rho^2(N-N\Upsilon^2(\Delta\varphi))}(1-\Upsilon^2(\varphi_B-\varphi))\Big). \quad (56)
\end{aligned}$$

On the other hand, the covariance term in (53) is decomposed as

$$\begin{aligned}
&\mathbb{C}\mathrm{ov}[\sum_{n=1}^{N}c_{R1}\,\Xi_{Rn}(k), \sum_{n=1}^{N}c_{I1}\,\Xi_{In}(k)] \\
&= \mathbb{E}\Big[\sum_{n=1}^{N}c_{R1}\,\Xi_{Rn}(k)\sum_{n=1}^{N}c_{I1}\,\Xi_{In}(k)\Big] \\
&\quad - \mathbb{E}\Big[\sum_{n=1}^{N}c_{R1}\,\Xi_{Rn}(k)\Big]\mathbb{E}\Big[\sum_{n=1}^{N}c_{I1}\,\Xi_{In}(k)\Big] \\
&= \mathbb{E}[c_{R1}]\,\mathbb{E}[c_{I1}]\Big(\mathbb{E}\Big[\sum_{n=1}^{N}\Xi_{Rn}(k)\sum_{n=1}^{N}\Xi_{In}(k)\Big] \\
&\quad - \mathbb{E}\Big[\sum_{n=1}^{N}\Xi_{Rn}(k)\Big]\mathbb{E}\Big[\sum_{n=1}^{N}\Xi_{In}(k)\Big]\Big) \\
&= \frac{t}{2\rho^2 N}\Big(\mathbb{E}\Big[\sum_{n=1}^{N}\Xi_{Rn}(k)\sum_{n=1}^{N}\Xi_{In}(k)\Big] \\
&\quad - \mathbb{E}\Big[\sum_{n=1}^{N}\Xi_{Rn}(k)\Big]\mathbb{E}\Big[\sum_{n=1}^{N}\Xi_{In}(k)\Big]\Big). \quad (57)
\end{aligned}$$

For simplicity, we define four variables as $\mathcal{A}_{\mathcal{R}} = \mathcal{R}\{\sum_{n=1}^{N}\Xi_n(k)\}$, $\mathcal{A}_{\mathcal{I}} = \mathcal{I}\{\sum_{n=1}^{N}\Xi_n(k)\}$, $\mathcal{B}_{\mathcal{R}} = \mathcal{R}\{\sum_{n=1}^{N}\Lambda_n(k)\}$, and $\mathcal{B}_{\mathcal{I}} = \mathcal{I}\{\sum_{n=1}^{N}\Lambda_n(k)\}$. Accordingly, we need to compute $\mathbb{E}[\mathcal{A}_{\mathcal{R}}\,\mathcal{A}_{\mathcal{I}}] - \mathbb{E}[\mathcal{A}_{\mathcal{R}}]\,\mathbb{E}[\mathcal{A}_{\mathcal{I}}]$. First, $\mathbb{E}[\mathcal{A}_{\mathcal{R}}\,\mathcal{A}_{\mathcal{I}}]$ is expressed as

$$\begin{aligned}
&\mathbb{E}\Big[\,\mathcal{A}_{\mathcal{R}}\,\mathcal{A}_{\mathcal{I}}\,\Big] \\
&= \mathbb{E}\Big[\sum_{n=1}^{N}\cos\big(\alpha\hat{u}_n(k)\big)\sin\big(\alpha\hat{u}_n(k)\big)\Big] \\
&\quad + \mathbb{E}\Big[\sum_{n=1}^{N}\sum_{\substack{i=1\\ i\neq n}}^{N}\cos\big(\alpha\hat{u}_n(k)\big)\sin\big(\alpha\hat{u}_i(k)\big)\Big] \\
&= \sum_{n=1}^{N}\mathbb{E}\big[\cos\big(\alpha\hat{u}_n(k)\big)\sin\big(\alpha\hat{u}_n(k)\big)\big] \\
&\quad + \sum_{n=1}^{N}\sum_{\substack{i=1\\ i\neq n}}^{N}\mathbb{E}\big[\cos\big(\alpha\hat{u}_n(k)\big)\big]\,\mathbb{E}\big[\sin\big(\alpha\hat{u}_n(k)\big)\big] \\
&= N\,\mathbb{E}\big[\cos\big(\alpha\hat{u}_n(k)\big)\sin\big(\alpha\hat{u}_n(k)\big)\big] \\
&\quad + N(N-1)\,\mathbb{E}\big[\cos\big(\alpha\hat{u}_n(k)\big)\big]\,\mathbb{E}\big[\sin\big(\alpha\hat{u}_n(k)\big)\big] \\
&= N\,\mathbb{E}\big[\cos\big(\alpha\hat{u}_n(k)\big)\sin\big(\alpha\hat{u}_n(k)\big)\big] \\
&= \frac{N}{2}\,\mathbb{E}\big[\sin(2\alpha\hat{u}_n(k))\big] = 0. \quad (58)
\end{aligned}$$

Then, we can obtain

$$\begin{aligned}
\mathbb{E}\Big[\,\mathcal{A}_{\mathcal{R}}\,\Big]\,\mathbb{E}\Big[\,\mathcal{A}_{\mathcal{I}}\,\Big] &= N^2\,\mathbb{E}\big[\cos\big(\alpha\hat{u}_n(k)\big)\big]\,\mathbb{E}\big[\sin\big(\alpha\hat{u}_n(k)\big)\big] \\
&= 0. \quad (59)
\end{aligned}$$

Consequently, the covariance is

$$\mathbb{C}\mathrm{ov}[\sum_{n=1}^{N}c_{R1}\,\Xi_{Rn}(k), \sum_{n=1}^{N}c_{I1}\,\Xi_{In}(k)] = 0. \quad (60)$$

In accordance with (56) to (60),

$$\begin{aligned}
&\mathbb{V}\mathrm{ar}\Big[\mathcal{R}\{\sum_{n=1}^{N}c_1\,\Xi_n(k)\}\Big] = \\
&= N\Big(\frac{t}{2\rho^2 N}(1-\Upsilon^2(\varphi_B-\varphi))\Big) \\
&\quad + N^2\Big(\frac{(1-t)\Upsilon^2(\Delta\varphi)}{2\rho^2(N-N\Upsilon^2(\Delta\varphi))}\Upsilon^2(\varphi_B-\varphi)\Big) \\
&\quad + N\Big(\frac{(1-t)\Upsilon^2(\Delta\varphi)}{2\rho^2(N-N\Upsilon^2(\Delta\varphi))}(1-\Upsilon^2(\varphi_B-\varphi))\Big). \quad (61)
\end{aligned}$$

The following equation is derived using the method of (54) to (60):

$$\begin{aligned}
&\mathbb{V}\mathrm{ar}\Big[\mathcal{I}\{\sum_{n=1}^{N}c_1\,\Xi_n(k)\}\Big] = \\
&= N\Big(\frac{t}{2\rho^2 N}(1-\Upsilon^2(\varphi_B-\varphi))\Big)
\end{aligned}$$

$$+N^2\Big(\frac{(1-t)\Upsilon^2(\Delta\varphi)}{2\rho^2(N-N\Upsilon^2(\Delta\varphi))}\Upsilon^2(\varphi_B-\varphi)\Big)$$
$$+N\Big(\frac{(1-t)\Upsilon^2(\Delta\varphi)}{2\rho^2(N-N\Upsilon^2(\Delta\varphi))}(1-\Upsilon^2(\varphi_B-\varphi))\Big). \quad (62)$$

As in (61) and (62), we obtain

$$\begin{aligned}&\mathbb{V}\mathrm{ar}\Big[\sum_{n=1}^{N}c_1\,\Xi_n(k)\Big]\\&=\mathbb{V}\mathrm{ar}\Big[\mathcal{R}\{\sum_{n=1}^{N}c_1\,\Xi_n(k)\}\Big]+\mathbb{V}\mathrm{ar}\Big[\mathcal{I}\{\sum_{n=1}^{N}c_1\,\Xi_n(k)\}\Big]\\&=N\Big(\frac{t}{\rho^2N}(1-\Upsilon^2(\varphi_B-\varphi))\Big)\\&\quad+N^2\Big(\frac{(1-t)\Upsilon^2(\Delta\varphi)}{\rho^2(N-N\Upsilon^2(\Delta\varphi))}\Upsilon^2(\varphi_B-\varphi)\Big)\\&\quad+N\Big(\frac{(1-t)\Upsilon^2(\Delta\varphi)}{\rho^2(N-N\Upsilon^2(\Delta\varphi))}(1-\Upsilon^2(\varphi_B-\varphi))\Big). \quad (63)\end{aligned}$$

Likewise, the following equation can be derived by using (54) to (62):

$$\mathbb{V}\mathrm{ar}\Big[\sum_{n=1}^{N}c_2\Lambda_n(k)\Big]=N^2\Big(\frac{(1-t)\Upsilon^2(\varphi_{AN}-\varphi)}{\rho^2(N-N\Upsilon^2(\Delta\varphi))}\Big)+N\Big(\frac{(1-t)(1-\Upsilon^2(\varphi_{AN}-\varphi))}{\rho^2(N-N\Upsilon^2(\Delta\varphi))}\Big), \quad (64)$$

where $\mathbb{E}[c_2]=0$ and the covariance of $\mathbb{V}\mathrm{ar}\Big[\sum_{n=1}^{N}c_2\Lambda_n(k)\Big]$ is zero.

From (48), the following term can be expressed as

$$\begin{aligned}&\mathbb{C}\mathrm{ov}[\mathcal{R}\{\sum_{n=1}^{N}c_1\,\Xi_n(k)\},\mathcal{R}\{\sum_{n=1}^{N}c_2\Lambda_n(k)\}]\\&=\mathbb{E}[c_{R1}c_{R2}\,\mathcal{A}_\mathcal{R}\,\mathcal{B}_\mathcal{R}]+\mathbb{E}[c_{R1}c_{I2}\,\mathcal{A}_\mathcal{R}\,\mathcal{B}_\mathcal{I}]\\&\quad+\mathbb{E}[c_{I1}c_{R2}\,\mathcal{A}_\mathcal{I}\,\mathcal{B}_\mathcal{R}]+\mathbb{E}[c_{I1}c_{I2}\,\mathcal{A}_\mathcal{I}\,\mathcal{B}_\mathcal{I}]\\&\quad-\mathbb{E}[c_{R1}\,\mathcal{A}_\mathcal{R}]\,\mathbb{E}[c_{R2}\,\mathcal{B}_\mathcal{R}]-\mathbb{E}[c_{R1}\,\mathcal{A}_\mathcal{R}]\,\mathbb{E}[c_{I2}\,\mathcal{B}_\mathcal{I}]\\&\quad-\mathbb{E}[c_{I1}\,\mathcal{A}_\mathcal{I}]\,\mathbb{E}[c_{R2}\,\mathcal{B}_\mathcal{R}]-\mathbb{E}[c_{I1}\,\mathcal{A}_\mathcal{I}]\,\mathbb{E}[c_{I2}\,\mathcal{B}_\mathcal{I}]\\&=\mathbb{E}[c_{R1}c_{R2}\,\mathcal{A}_\mathcal{R}\,\mathcal{B}_\mathcal{R}]+\mathbb{E}[c_{R1}c_{I2}\,\mathcal{A}_\mathcal{R}\,\mathcal{B}_\mathcal{I}]\\&\quad+\mathbb{E}[c_{I1}c_{R2}\,\mathcal{A}_\mathcal{I}\,\mathcal{B}_\mathcal{R}]+\mathbb{E}[c_{I1}c_{I2}\,\mathcal{A}_\mathcal{I}\,\mathcal{B}_\mathcal{I}]. \quad (65)\end{aligned}$$

Let $\alpha=\frac{4\pi}{\lambda}\sin(\frac{\varphi_B-\varphi}{2})$ and $\beta=\frac{4\pi}{\lambda}\sin(\frac{\varphi_{AN}-\varphi}{2})$. Then, because $c_1=\frac{\sqrt{t}}{\rho\sqrt{N}}-\frac{\sqrt{1-t}\Upsilon(\Delta\varphi)\epsilon(k)}{\rho\sqrt{N-N\Upsilon^2(\Delta\varphi)}}$ and $c_2=\frac{\sqrt{1-t}\epsilon(k)}{\rho\sqrt{N-N\Upsilon^2(\Delta\varphi)}}$, we can obtain $\mathbb{E}[c_{R1}c_{R2}]=\mathbb{E}[c_{I1}c_{I2}]=\mathbb{E}[c_{I1}c_{R2}]=\mathbb{E}[c_{R1}c_{I2}]=\frac{1}{4}\mathbb{E}[c_1c_2]=-\frac{(1-t)\Upsilon(\Delta\varphi)}{4\rho^2(N-N\Upsilon^2(\Delta\varphi))}$. Thus,

$$\begin{aligned}&\mathbb{E}[c_{R1}c_{R2}\,\mathcal{A}_\mathcal{R}\,\mathcal{B}_\mathcal{R}]+\mathbb{E}[c_{I1}c_{I2}\,\mathcal{A}_\mathcal{I}\,\mathcal{B}_\mathcal{I}]\\&=\mathbb{E}[c_{R1}c_{R2}]\,\mathbb{E}\Big[\sum_{n=1}^{N}\cos\big(\alpha\hat{u}_n(k)\big)\cos\big(\beta\check{u}_n(k)\big)\Big]\\&\quad+\mathbb{E}[c_{R1}c_{R2}]\,\mathbb{E}\Big[\sum_{n=1}^{N}\sum_{\substack{i=1\\i\neq n}}^{N}\cos\big(\alpha\hat{u}_n(k)\big)\cos\big(\beta\check{u}_i(k)\big)\Big]\\&\quad+\mathbb{E}[c_{I1}c_{I2}]\,\mathbb{E}\Big[\sum_{n=1}^{N}\sin\big(\alpha\hat{u}_n(k)\big)\sin\big(\beta\check{u}_n(k)\big)\Big]\\&\quad+\mathbb{E}[c_{I1}c_{I2}]\,\mathbb{E}\Big[\sum_{n=1}^{N}\sum_{\substack{i=1\\i\neq n}}^{N}\sin\big(\alpha\hat{u}_n(k)\big)\sin\big(\beta\check{u}_i(k)\big)\Big]\\&=\frac{1}{2}\,\mathbb{E}[AB]\sum_{n=1}^{N}\mathbb{E}\big[\cos\big(\alpha\hat{u}_n(k)-\beta\check{u}_n(k)\big)\big]\\&\quad+\frac{1}{2}\,\mathbb{E}[AB]\sum_{n=1}^{N}\sum_{\substack{i=1\\i\neq n}}^{N}\mathbb{E}\big[\cos\big(\alpha\hat{u}_n(k)\big)\big]\,\mathbb{E}\big[\cos\big(\beta\check{u}_i(k)\big)\big]\\&\quad+\frac{1}{2}\,\mathbb{E}[AB]\sum_{n=1}^{N}\sum_{\substack{i=1\\i\neq n}}^{N}\mathbb{E}\big[\sin\big(\alpha\hat{u}_n(k)\big)\big]\,\mathbb{E}\big[\sin\big(\beta\check{u}_i(k)\big)\big]\\&=\frac{1}{2}\,\mathbb{E}[AB]N\,\mathbb{E}\Big[\cos\Big(\frac{4\pi}{\lambda}u_n(k)\sin(\frac{\varphi_B-\varphi_{AN}}{2})\Big)\Big]\\&\quad+\frac{1}{2}\,\mathbb{E}[AB]N(N-1)\,(\mathbb{E}[\Xi_n(k)]\,\mathbb{E}[\Lambda_n(k)])\\&=\frac{1}{2}\,\mathbb{E}[AB]N\Big(\mathbb{E}\Big[\cos\Big(\frac{4\pi}{\lambda}u_n(k)\sin(\frac{\varphi_B-\varphi_{AN}}{2})\Big)\Big]\\&\quad+(N-1)\,\mathbb{E}[\Xi_n(k)]\,\mathbb{E}[\Lambda_n(k)]\Big)\\&=-\frac{(1-t)\Upsilon(\Delta\varphi)N}{4\rho^2(N-N\Upsilon^2(\Delta\varphi))}\Big(\Upsilon(\Delta\varphi)\\&\quad+(N-1)\Upsilon(\varphi_B-\varphi)\Upsilon(\varphi_{AN}-\varphi)\Big). \quad (66)\end{aligned}$$

Also, $\mathbb{E}[c_{R1}c_{I2}\,\mathcal{A}_\mathcal{R}\,\mathcal{B}_\mathcal{I}]+\mathbb{E}[c_{I1}c_{R2}\,\mathcal{A}_\mathcal{I}\,\mathcal{B}_\mathcal{R}]$ can be rewritten as

$$\begin{aligned}&\mathbb{E}[c_{R1}c_{I2}\,\mathcal{A}_\mathcal{R}\,\mathcal{B}_\mathcal{I}]+\mathbb{E}[c_{I1}c_{R2}\,\mathcal{A}_\mathcal{I}\,\mathcal{B}_\mathcal{R}]\\&=\frac{1}{2}\,\mathbb{E}[AB]\,\mathbb{E}\Big[\sum_{n=1}^{N}\cos\big(\alpha\hat{u}_n(k)\big)\sin\big(\beta\check{u}_n(k)\big)\Big]\\&\quad+\frac{1}{2}\,\mathbb{E}[AB]\,\mathbb{E}\Big[\sum_{n=1}^{N}\sum_{\substack{i=1\\i\neq n}}^{N}\cos\big(\alpha\hat{u}_n(k)\big)\sin\big(\beta\check{u}_i(k)\big)\Big]\\&\quad+\frac{1}{2}\,\mathbb{E}[AB]\,\mathbb{E}\Big[\sum_{n=1}^{N}\sin\big(\alpha\hat{u}_n(k)\big)\cos\big(\beta\check{u}_n(k)\big)\Big]\\&\quad+\frac{1}{2}\,\mathbb{E}[AB]\,\mathbb{E}\Big[\sum_{n=1}^{N}\sum_{\substack{i=1\\i\neq n}}^{N}\sin\big(\alpha\hat{u}_n(k)\big)\cos\big(\beta\check{u}_i(k)\big)\Big]\\&=\frac{1}{2}\,\mathbb{E}[AB]\sum_{n=1}^{N}\mathbb{E}\big[\sin\big(\alpha\hat{u}_n(k)+\beta\check{u}_n(k)\big)\big]\end{aligned}$$

$$+\frac{1}{2}\mathbb{E}[AB]\sum_{n=1}^{N}\sum_{\substack{i=1\\i\neq n}}^{N}\mathbb{E}[\cos\left(\alpha\hat{u}_n(k)\right)]\,\mathbb{E}[\sin\left(\beta\check{u}_i(k)\right)]$$
$$+\frac{1}{2}\mathbb{E}[AB]\sum_{n=1}^{N}\sum_{\substack{i=1\\i\neq n}}^{N}\mathbb{E}[\sin\left(\alpha\hat{u}_n(k)\right)]\,\mathbb{E}[\cos\left(\beta\check{u}_i(k)\right)]$$
$$=0. \tag{67}$$

Thus, (65) is simplified as

$$\mathbb{C}\mathrm{ov}[\mathcal{R}\{\sum_{n=1}^{N}c_1\Xi_n(k)\},\mathcal{R}\{\sum_{n=1}^{N}c_2\Lambda_n(k)\}]$$
$$=\frac{(t-1)\Upsilon(\Delta\varphi)N}{4\rho^2(N-N\Upsilon^2(\Delta\varphi))}\Big(\Upsilon(\Delta\varphi)$$
$$+(N-1)\Upsilon(\varphi_B-\varphi)\Upsilon(\varphi_{AN}-\varphi)\Big). \tag{68}$$

As we have derived (65), the following covariance can be simplified as

$$\mathbb{C}\mathrm{ov}[\mathcal{R}\{\sum_{n=1}^{N}c_1\Xi_n(k)\},\mathcal{R}\{\sum_{n=1}^{N}c_2\Lambda_n(k)\}]$$
$$=\mathbb{C}\mathrm{ov}[\mathcal{I}\{\sum_{n=1}^{N}c_1\Xi_n(k)\},\mathcal{I}\{\sum_{n=1}^{N}c_2\Lambda_n(k)\}]$$
$$=\mathbb{C}\mathrm{ov}[\mathcal{R}\{\sum_{n=1}^{N}c_1\Xi_n(k)\},\mathcal{I}\{\sum_{n=1}^{N}c_2\Lambda_n(k)\}]$$
$$=\mathbb{C}\mathrm{ov}[\mathcal{I}\{\sum_{n=1}^{N}c_1\Xi_n(k)\},\mathcal{R}\{\sum_{n=1}^{N}c_2\Lambda_n(k)\}]$$
$$=-\frac{(1-t)\Upsilon(\Delta\varphi)N}{4\rho^2(N-N\Upsilon^2(\Delta\varphi))}\Big(\Upsilon(\Delta\varphi)$$
$$+(N-1)\Upsilon(\varphi_B-\varphi)\Upsilon(\varphi_{AN}-\varphi)\Big). \tag{69}$$

Therefore, by using (63), (64) and (69), we can express (48) as

$$\mathbb{V}\mathrm{ar}[F(\rho,\varphi,k)]$$
$$=P\Big[\mathbb{V}\mathrm{ar}[\mathcal{R}\{\sum_{n=1}^{N}c_1\Xi_n(k)\}]+\mathbb{V}\mathrm{ar}[\mathcal{I}\{\sum_{n=1}^{N}c_1\Xi_n(k)\}]$$
$$+\mathbb{V}\mathrm{ar}[\mathcal{R}\{\sum_{n=1}^{N}c_2\Lambda_n(k)\}]+\mathbb{V}\mathrm{ar}[\mathcal{I}\{\sum_{n=1}^{N}c_2\Lambda_n(k)\}]$$
$$+2\,\mathbb{C}\mathrm{ov}[\mathcal{R}\{\sum_{n=1}^{N}c_1\Xi_n(k)\},\mathcal{R}\{\sum_{n=1}^{N}c_2\Lambda_n(k)\}]$$
$$+2\,\mathbb{C}\mathrm{ov}[\mathcal{I}\{\sum_{n=1}^{N}c_1\Xi_n(k)\},\mathcal{I}\{\sum_{n=1}^{N}c_2\Lambda_n(k)\}]$$
$$+2\,\mathbb{C}\mathrm{ov}[\mathcal{R}\{\sum_{n=1}^{N}c_1\Xi_n(k)\},\mathcal{I}\{\sum_{n=1}^{N}c_2\Lambda_n(k)\}]$$
$$+2\,\mathbb{C}\mathrm{ov}[\mathcal{I}\{\sum_{n=1}^{N}c_1\Xi_n(k)\},\mathcal{R}\{\sum_{n=1}^{N}c_2\Lambda_n(k)\}]\Big]$$
$$=P\Big[N\Big(\frac{t}{\rho^2N}(1-\Upsilon^2(\varphi_B-\varphi))\Big)$$
$$+N^2\Big(\frac{(1-t)\Upsilon^2(\Delta\varphi)}{\rho^2(N-N\Upsilon^2(\Delta\varphi))}\Upsilon^2(\varphi_B-\varphi)\Big)$$
$$+N\Big(\frac{(1-t)\Upsilon^2(\Delta\varphi)}{\rho^2(N-N\Upsilon^2(\Delta\varphi))}(1-\Upsilon^2(\varphi_B-\varphi))\Big)$$
$$+N^2\Big(\frac{(1-t)\Upsilon^2(\varphi_{AN}-\varphi)}{\rho^2(N-N\Upsilon^2(\Delta\varphi))}\Big)$$
$$+N\Big(\frac{(1-t)(1-\Upsilon^2(\varphi_{AN}-\varphi))}{\rho^2(N-N\Upsilon^2(\Delta\varphi))}\Big)$$
$$-2\frac{(1-t)\Upsilon(\Delta\varphi)}{\rho^2(N-N\Upsilon^2(\Delta\varphi))}\Big(N\Upsilon(\Delta\varphi)$$
$$+N(N-1)\Upsilon(\varphi_B-\varphi)\Upsilon(\varphi_{AN}-\varphi)\Big)\Big]$$
$$=P\Big[\Big(\frac{t}{\rho^2}(1-\Upsilon^2(\varphi_B-\varphi))\Big)$$
$$+\frac{1-t}{\rho^2(1-\Upsilon^2(\Delta\varphi))}\Big(N\Upsilon^2(\Delta\varphi)\Upsilon^2(\varphi_B-\varphi)$$
$$+\Upsilon^2(\Delta\varphi)(1-\Upsilon^2(\varphi_B-\varphi))+N\Upsilon^2(\varphi_{AN}-\varphi)$$
$$+(1-\Upsilon^2(\varphi_{AN}-\varphi))\Big)-2\frac{(1-t)\Upsilon(\Delta\varphi)}{\rho^2(1-\Upsilon^2(\Delta\varphi))}\Big(\Upsilon(\Delta\varphi)$$
$$+(N-1)\Upsilon(\varphi_B-\varphi)\Upsilon(\varphi_{AN}-\varphi)\Big)\Big]. \tag{70}$$

Finally, we obtain (37) in Lemma 2.

REFERENCES

[1] M. W. Akhtar, S. A. Hassan, R. Ghaffar, H. Jung, S. Garg, and M. S. Hossain, "The shift to 6G communications: Vision and requirements," *Hum.-Centric Comput. Inf. Sci.*, vol. 10, no. 1, Dec. 2020.

[2] S. Talwar, N. Himayat, H. Nikopour, F. Xue, G. Wu, and V. Ilderem, "6G: Connectivity in the era of distributed intelligence," *IEEE Commun. Mag.*, vol. 59, no. 11, pp. 45–50, Nov. 2021.

[3] K. David, A. Al-Dulaimi, H. Haas, and R. Q. Hu, "6G networks: Is this an evolution or a revolution?" *IEEE Veh. Tech. Mag.*, vol. 16, no. 4, pp. 14–15, Dec. 2021.

[4] Z. Zhang, C. Zhang, C. Jiang, F. Jia, J. Ge, and F. Gong, "Improving physical layer security for reconfigurable intelligent surface aided NOMA 6G networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4451–4463, May 2021.

[5] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2384–2428, 4th Quart., 2021.

[6] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3682–3722, 4th Quart., 2019.

[7] L. Mucchi, S. Jayousi, S. Caputo, E. Panayirci, S. Shahabuddin, J. Bechtold, I. Morales, R.-A. Stoica, G. Abreu, and H. Haas, "Physical-layer security in 6G networks," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1901–1914, 2021.

[8] E.-K. Hong, I. Lee, B. Shim, Y.-C. Ko, S.-H. Kim, S. Pack, K. Lee, S. Kim, J.-H. Kim, Y. Shin, Y. Kim, and H. Jung, "6G R&D vision: Requirements and candidate technologies," *J. Commun. Netw.*, vol. 24, no. 2, pp. 232–245, Apr. 2022.

[9] C. Lipps, S. Baradie, M. Noushinfar, J. Herbst, A. Weinand, and H. D. Schotten, "Towards the sixth generation (6G) wireless systems: Thoughts on physical layer security," in *Proc. Mobile Commun. Technol. Appl. 25th ITG-Symp.*, Nov. 2021, pp. 1–6.

[10] K. N. Vaishnavi, S. D. Khorvi, R. Kishore, and S. Gurugopinath, "A survey on jamming techniques in physical layer security and anti-jamming strategies for 6G," in *Proc. 28th Int. Conf. Telecommun. (ICT)*, Jun. 2021, pp. 174–179.

[11] F. Irram, M. Ali, M. Naeem, and S. Mumtaz, "Physical layer security for beyond 5G/6G networks: Emerging technologies and future directions," *J. Netw. Comput. Appl.*, vol. 206, Oct. 2022, Art. no. 103431.

[12] K. Feng, X. Li, Y. Han, S. Jin, and Y. Chen, "Physical layer security enhancement exploiting intelligent reflecting surface," *IEEE Commun. Lett.*, vol. 25, no. 3, pp. 734–738, Mar. 2021.

[13] S. Xu, J. Liu, and Y. Cao, "Intelligent reflecting surface empowered physical-layer security: Signal cancellation or jamming?" *IEEE Internet Things J.*, vol. 9, no. 2, pp. 1265–1275, Jan. 2022.

[14] S. Elhoushy, M. Ibrahim, and W. Hamouda, "Cell-free massive MIMO: A survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 492–523, 1st Quart., 2022.

[15] X. Zhang, T. Liang, K. An, G. Zheng, and S. Chatzinotas, "Secure transmission in cell-free massive MIMO with RF impairments and low-resolution ADCs/DACs," *IEEE Trans. Veh. Technol.*, vol. 70, no. 9, pp. 8937–8949, Sep. 2021.

[16] J. Qiu, K. Xu, X. Xia, Z. Shen, W. Xie, D. Zhang, and M. Wang, "Secure transmission scheme based on fingerprint positioning in cell-free massive MIMO systems," *IEEE Trans. Signal Inf. Process. over Netw.*, vol. 8, pp. 92–105, Aug. 2022.

[17] L. Du, L. Li, H. Q. Ngo, T. C. Mai, and M. Matthaiou, "Cell-free massive MIMO: Joint maximum-ratio and zero-forcing precoder with power control," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 3741–3756, Jun. 2021.

[18] 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.

[19] M. E. Eltayeb and R. W. Heath, "Securing mmWave vehicular communication links with multiple transmit antennas," in *Proc. IEEE ICC*, May 2018, pp. 1–6.

[20] M. E. Eltayeb, J. Choi, T. Y. Al-Naffouri, and R. W. Heath Jr., "Enhancing secrecy with multiantenna transmission in millimeter wave vehicular communication systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8139–8151, Sep. 2017.

[21] B. You, I.-H. Lee, and H. Jung, "Optimal subset size analysis of randomized analog beamforming using uniform planar arrays in mmWave networks," *IEEE Wireless Commun. Lett.*, vol. 10, no. 7, pp. 1414–1418, Jul. 2021.

[22] B. You, I.-H. Lee, and H. Jung, "Exact secrecy rate analysis of antenna subset modulation schemes," *IEEE Syst. J.*, vol. 15, no. 4, pp. 4827–4830, Dec. 2021.

[23] A. Alali and D. B. Rawat, "Combating distance limitation in sub-terahertz frequency band for physical layer security in UAV communications," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, May 2021, pp. 1–6.

[24] A. Alali, D. B. Rawat, and C. Liu, "Trajectory and power optimization in sub-THz band for UAV communications," in *Proc. IEEE Int. Conf. Commun.*, May 2022, pp. 1–6.

[25] Z. Fang, H. Guerboukha, R. Shrestha, M. Hornbuckle, Y. Amarasinghe, and D. M. Mittleman, "Secure communication channels using atmosphere-limited line-of-sight terahertz links," *IEEE Trans. Terahertz Sci. Technol.*, vol. 12, no. 4, pp. 363–369, Jul. 2022.

[26] J. Qiao, C. Zhang, A. Dong, J. Bian, and M.-S. Alouini, "Securing intelligent reflecting surface assisted terahertz systems," *IEEE Trans. Veh. Technol.*, vol. 71, no. 8, pp. 8519–8533, Aug. 2022.

[27] H. Peng, Z. Wang, S. Han, and Y. Jiang, "Physical layer security for MISO NOMA VLC system under eavesdropper collusion," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 6249–6254, Jun. 2021.

[28] M. A. Arfaoui, M. D. Soltani, I. Tavakkolnia, A. Ghrayeb, M. Safari, C. M. Assi, and H. Haas, "Physical layer security for visible light communication systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1887–1908, Sep. 2020.

[29] F. Yang, J. Wang, and Y. Dong, "Physical-layer security for indoor VLC wiretap systems under multipath reflections," *IEEE Trans. Wireless Commun.*, vol. 21, no. 12, pp. 11179–11192, Dec. 2022.

[30] X. Li, Y. Zheng, W. U. Khan, M. Zeng, D. Li, G. K. Ragesh, and L. Li, "Physical layer security of cognitive ambient backscatter communications for green Internet-of-Things," *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 3, pp. 1066–1076, Sep. 2021.

[31] D. P. M. Osorio, E. E. B. Olivo, H. Alves, and M. Latva-Aho, "Safeguarding MTC at the physical layer: Potentials and challenges," *IEEE Access*, vol. 8, pp. 101437–101447, 2020.

[32] P. Angueira, I. Val, J. Montalban, O. Seijo, E. Iradier, P. S. Fontaneda, L. Fanari, and A. Arriola, "A survey of physical layer techniques for secure wireless communications in industry," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 810–838, 2nd Quart., 2022.

[33] A. Chorti, A. N. Barreto, S. Kopsell, M. Zoli, M. Chafii, P. Sehier, G. Fettweis, and H. V. Poor, "Context-aware security for 6G wireless: The role of physical layer security," *IEEE Commun. Standards Mag.*, vol. 6, no. 1, pp. 102–108, Mar. 2022.

[34] H. Jung and I.-H. Lee, "Secrecy rate of analog collaborative beamforming with virtual antenna array following spatial random distributions," *IEEE Wireless Commun. Lett.*, vol. 7, no. 4, pp. 626–629, Aug. 2018.

[35] H. Jung and I.-H. Lee, "Analog cooperative beamforming with spherically-bound random arrays for physical-layer secure communications," *IEEE Commun. Lett.*, vol. 22, no. 3, pp. 546–549, Mar. 2018.

[36] H. Jung and I.-H. Lee, "Secrecy performance analysis of analog cooperative beamforming in three-dimensional Gaussian distributed wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 18, no. 3, pp. 1860–1873, Mar. 2019.

[37] H. Jung and I.-H. Lee, "Secrecy rate analysis of open-loop analog collaborative beamforming under position estimation error of virtual antenna array," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1337–1340, Oct. 2019.

[38] H. Jung and I.-H. Lee, "Distributed null-steering beamformer design for physical layer security enhancement in Internet-of-Things networks," *IEEE Syst. J.*, vol. 15, no. 1, pp. 277–288, Mar. 2021.

[39] H. Jung, S.-W. Ko, and I.-H. Lee, "Secure transmission using linearly distributed virtual antenna array with element position perturbations," *IEEE Trans. Veh. Technol.*, vol. 70, no. 1, pp. 474–489, Jan. 2021.

[40] H. Jung, I.-H. Lee, and J. Joung, "Security energy efficiency analysis of analog collaborative beamforming with stochastic virtual antenna array of UAV swarm," *IEEE Trans. Veh. Technol.*, vol. 71, no. 8, pp. 8381–8397, Aug. 2022.

[41] X. Fan, L. Huang, Y. Huo, C. Hu, Y. Tian, and J. Qian, "Space power synthesis-based cooperative jamming for unknown channel state information," in *Proc. Int. Conf. Wireless Algorithms, Syst., Appl.*, May 2017, pp. 483–495.

[42] L. Huang, X. Fan, Y. Huo, C. Hu, Y. Tian, and J. Qian, "A novel cooperative jamming scheme for wireless social networks without known CSI," *IEEE Access*, vol. 5, pp. 26476–26486, 2017.

[43] Y. Huo, X. Fan, L. Ma, X. Cheng, Z. Tian, and D. Chen, "Secure communications in tiered 5G wireless networks with cooperative jamming," *IEEE Trans. Wireless Commun.*, vol. 18, no. 6, pp. 3265–3280, Jun. 2019.

[44] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 256–266, Jun. 2011.

[45] H. Jung, Y. J. Chang, and M. A. Ingram, "Experimental range extension of concurrent cooperative transmission in indoor environments at 2.4 GHz," in *Proc. MILCOM Mil. Commun. Conf.*, Oct. 2010, pp. 148–153.

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

[47] Y. Hong, X. Jing, H. Gao, H. Huang, N. Gao, and J. Xie, "Programmable weight phased-array transmission for secure millimeter-wave wireless communication," in *Proc. 1st ACM Workshop Millimeter-Wave Netw. Sens. Syst.*, Oct. 2017, pp. 41–46.

[48] B. You, I.-H. Lee, and H. Jung, "Exact secrecy rate analysis of randomized radiation technique with frequency diverse subarrays," *IEEE Wireless Commun. Lett.*, vol. 11, no. 12, pp. 2630–2634, Dec. 2022.

[49] B. You, I.-H. Lee, and H. Jung, "Secrecy rate analysis of randomized radiation for intelligent reflecting surface-aided communication systems," *IEEE Commun. Lett.*, vol. 26, no. 9, pp. 1999–2003, Sep. 2022.

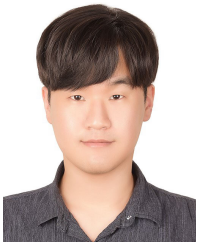
[50] J. Chu and X. Chen, "Robust design for integrated satellite–terrestrial Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 9072–9083, Jun. 2021.

[51] G. Jang, B. You, and H. Jung, "A survey on physical layer security schemes in satellite networks," in *Proc. 13th Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2022, pp. 1213–1215.

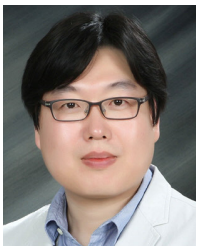
[52] R. Bajracharya, R. Shrestha, S. Kim, and H. Jung, "6G NR-U based wireless infrastructure UAV: Standardization, opportunities, challenges and future scopes," *IEEE Access*, vol. 10, pp. 30536–30555, 2022.

[53] G. Lim and L. J. Cimini, "Energy-efficient cooperative beamforming in clustered wireless networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 3, pp. 1376–1385, Mar. 2013.
[54] H. Ochiai, P. Mitran, H. V. Poor, and V. Tarokh, "Collaborative beamforming for distributed wireless ad hoc sensor networks," *IEEE Trans. Signal Process.*, vol. 53, no. 11, pp. 4110–4124, Nov. 2005.
[55] R. Mudumbai, D. R. B. Iii, U. Madhow, and H. V. Poor, "Distributed transmit beamforming: Challenges and recent progress," *IEEE Commun. Mag.*, vol. 47, no. 2, pp. 102–110, Feb. 2009.
[56] R. Mudumbai, G. Barriac, and U. Madhow, "On the feasibility of distributed beamforming in wireless networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 5, pp. 1754–1763, May 2007.
[57] S. Yan and R. Malaney, "Location-based beamforming for enhancing secrecy in Rician wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2780–2791, Apr. 2016.
[58] C. Liu and R. Malaney, "Location-based beamforming and physical layer security in Rician wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7847–7857, Nov. 2016.
[59] C. Liu, N. Yang, J. Yuan, and R. Malaney, "Location-based secure transmission for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 7, pp. 1458–1470, Jul. 2015.
[60] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.
[61] F. Quitin, U. Madhow, M. M. U. Rahman, and R. Mudumbai, "Demonstrating distributed transmit beamforming with software-defined radios," in *Proc. IEEE Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2012, pp. 1–3.
[62] N. Xie, X. Bao, A. Petropulu, and H. Wang, "Fast open-loop synchronization for cooperative distributed beamforming," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 3441–3446.
[63] S. Hanna and D. Cabric, "Distributed transmit beamforming: Design and demonstration from the lab to UAVs," *IEEE Trans. Wireless Commun.*, vol. 22, no. 2, pp. 778–792, Feb. 2023.
[64] J. Jee, G. Kwon, and H. Park, "Cooperative beamforming with nonlinear power amplifiers: A deep learning approach for distributed networks," *IEEE Trans. Veh. Technol.*, early access, Dec. 5, 2022, doi: 10.1109/TVT.2022.3226799.
[65] A. Kalis, A. Kanatas, and G. Efthymoglou, "A co-operative beamforming solution for eliminating multi-hop communications in wireless sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 28, no. 7, pp. 1055–1062, Sep. 2010.
[66] G. Sun, J. Li, A. Wang, Q. Wu, Z. Sun, Y. Liu, and S. Liang, "Collaborative beamforming for UAV networks exploiting swarm intelligence," *IEEE Wireless Commun.*, vol. 29, no. 4, pp. 10–17, Aug. 2022.
[67] Y. Zhao, W. Xu, X. You, N. Wang, and H. Sun, "Cooperative reflection and synchronization design for distributed multiple-RIS communications," *IEEE J. Sel. Topics Signal Process.*, vol. 16, no. 5, pp. 980–994, Aug. 2022.
[68] H. Jung and S.-W. Ko, "Performance analysis of UAV-enabled over-the-air computation under imperfect channel estimation," *IEEE Wireless Commun. Lett.*, vol. 11, no. 3, pp. 438–442, Mar. 2022.
[69] M. Akcakaya and A. Nehorai, "MIMO radar detection and adaptive design under a phase synchronization mismatch," *IEEE Trans. Signal Process.*, vol. 58, no. 10, pp. 4994–5005, Oct. 2010.

GEUNYEONG JANG (Graduate Student Member, IEEE) received the B.S. degree in information and communication engineering from Incheon National University, South Korea, in 2022. He is currently pursuing the M.S. degree in electronics and information convergence engineering with Kyung Hee University, South Korea. His research interests include physical-layer security and signal processing for 6G.



DONGHYEON KIM (Graduate Student Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Hankyong National University, South Korea, in 2020 and 2022, respectively. He is currently pursuing the Ph.D. degree in electronics and information convergence engineering with Kyung Hee University, South Korea. His current research interests include wireless communications, resource allocation, and deep-learning algorithms.



IN-HO LEE (Senior Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electrical engineering from Hanyang University, Ansan, South Korea, in 2003, 2005, and 2008, respectively. He worked for LTE-advanced standardization with Samsung Electronics Company, from 2008 to 2010. He was a Postdoctoral Fellow with the Department of Electrical Engineering, Hanyang University, from April 2010 to March 2011. Since March 2011, he has been a Professor with the School of Electronic and Electrical Engineering, Hankyong National University, Anseong, South Korea. From February 2017 to February 2018, he was a Visiting Associate Professor with the Department of Electrical and Computer Engineering, The University of British Columbia, Vancouver, Canada. His current research interests include non-orthogonal multiple access, millimeter wave wireless communications, cooperative communications, multi-hop relaying, transmission and reception of multiple-input and multiple-output communications, multicast communications, and deep-learning algorithms.

HAEJOON JUNG (Senior Member, IEEE) received the B.S. degree (Hons.) from Yonsei University, South Korea, in 2008, and the M.S. and Ph.D. degrees from the Georgia Institute of Technology (Georgia Tech), Atlanta, GA, USA, in 2010 and 2014, respectively, all in electrical engineering. From 2014 to 2016, he was a Wireless Systems Engineer with Apple, Cupertino, CA, USA. From 2016 to 2021, he was with Incheon National University, Incheon, South Korea. Since September 2021, he has been with the Department of Electronic Engineering, Kyung Hee University, as an Associate Professor. His research interests include communication theory, wireless communications, wireless power transfer, and statistical signal processing. He was a recipient of the Haedong Young Scholar Award from the Korean Institute of Communications and Information Sciences (KICS), in 2022.