SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •
Special Focus on Mobile Network Virtualization

April 2017, Vol. 60 040303:1–040303:17
doi: 10.1007/s11432-016-9013-0

Towards win-win: weighted-Voronoi-diagram based channel quantization for security enhancement in downlink cloud-RAN with limited CSI feedback

Dongyang XU[1,2], Pinyi REN[1,2]*, Qinghe DU[1,2], Li SUN[1,2] & Yichen WANG[1,2]

[1]*School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an* 710049*, China;*
[2]*Shaanxi Smart Networks and Ubiquitous Access Research Center, Xi'an* 710049*, China*

Received December 17, 2016; accepted January 22, 2017; published online March 17, 2017

Abstract Physical layer (PHY) security is recently proved to enable improving the security of wireless communication networks. In downlink frequency division duplex (FDD) cloud radio access network (C-RAN), the performance of PHY security highly relies on the channel state information (CSI) which is usually acquired through the codebook-quantization-based technique at the transceiver. However, the conventional quantization method aggravates the leakage of privacy information in C-RAN under the eavesdropping environment. In this paper, a novel channel quantization method is investigated to improve the secrecy-rate performance of C-RAN by exploiting the high-dimension space geometry. Based on this method, it is proved that when the statistical distribution of the channel matrices of both the legitimate user and the eavesdropper is exploited, a win-win situation can be created where secrecy-rate gains are improved without sacrificing beamforming gains from the point of view of ergodic rate. Particularly, a secrecy-oriented criterion is devised to implement the proposed method for generating codebooks. Then a weighted Voronoi diagram (WVD) is formulated on the complex Grassmann manifold and finally, a vector quantization based algorithm is proposed to build up novel quantization codebooks iteratively. Simulation results further validate the superiority of our proposed codebooks over conventional codebooks in C-RAN systems.

Keywords C-RAN, virtualization, physical layer security, Grassmann manifold, channel quantization

Citation Xu D Y, Ren P Y, Du Q H, et al. Towards win-win: weighted-Voronoi-diagram based channel quantization for security enhancement in downlink cloud-RAN with limited CSI feedback. Sci China Inf Sci, 2017, 60(4): 040303, doi: 10.1007/s11432-016-9013-0

1 Introduction

Recently, virtualization has drawn great attentions in many areas such as data storage, virtual desktop and access network. Virtualization mainly involves abstraction and sharing of resources among different parties. With virtualization, logically isolated networks can be fused into abstracted physical networks which can be shared in a flexible and dynamic way [1]. Though deployed in various applications for many years, virtualization technology is now developing vigorously in the area of wireless communications [2], especially under the stringent needs of 5G technology. As an example of wireless network virtualization,

* Corresponding author (email: pyren@mail.xjtu.edu.cn)

software-defined networking (SDN)-based C-RAN architecture [3, 4] can integrate multiple wireless networks, e.g. Long Term Evolution (LTE), Wi-Fi conveniently and efficiently. Communication resources can be integrated, shared and reciprocated in a flexible manner, including channel state information (CSI) of each base station-mobile station (BS-MS) link, traffic data, and control information of mobile services among cooperating BSs. The information is usually delivered among virtualized baseband units (BBUs) in clouds, remote radio heads (RRHs) and backhaul links [5].

In C-RAN, the security provision is a key functionality that guarantees the precise resource control and sharing [6]. In despite of inherent security benefits brought by the decoupling of physical and logical planes, C-RAN virtualization is also threatened by conventional security risks due to the inevitable difficulties in secret key distribution and management [7] when using cryptographic methods in the upper layers. Actually, the security achieved by cryptographic methods highly relies on the computational hardness of decrypting the message when the secret key is not available [8]. This mechanism may no longer hold true as the power of computation increases, e.g., with the development of quantum computers, in which encryption keys can become more easily compromised and many current cryptosystems can be broken down. In this context, physical layer security in C-RAN increasingly arouses great interests of researchers by exploiting the unique characteristics of wireless physical channels [9]. The fundamental principle of physical layer security theoretically originates from the conventional point-to-point network [10–12]. The related work in practical systems (e.g., limited-feedback FDD multiple-input multiple-output (MIMO) systems) has also been investigated extensively in [13, 14]. The most eye-catching feature is that the security performance with only quantized CSI is unfavorable unless at a great cost such as a large amount of feedback overheads and power budgets [14].

One important feature for the physical security in C-RAN is that CSIs, including which from the RRH to the legitimate user as well as from the RRH to the eavesdropper, cannot be perfectly known by BBUs. Particularly, downlink CSIs in C-RAN using FDD air interface are usually acquired by using quantization techniques and uplink feedback mechanism [15, 16]. The quantization is originally designed to reduce uplink feedback overheads while providing suitable sum-rate gains in conventional point-to-point systems. However, it highly relies on the degree of codebook-quantization precision which is significantly decreased when various large-scale fading is also quantized [17], especially in C-RAN systems. Besides, conventional quantization methods ignore the secrecy consideration and cannot satisfy secrecy requirements of limited feedback C-RAN systems. To our best knowledge, the quantization codebook design for C-RAN has not been studied in the eavesdropping environment, which motivates our current work.

We in this paper first propose using the concept of WVD method [18] to improve the precision of the wireless channel quantization in the physical layer of C-RAN with limited CSI feedback. By exploiting this method, system secrecy rate can be improved and inter-user interference can be simultaneously reduced. Our contributions are detailed below:

1. We simplify the C-RAN model subjected to eavesdropping behaviors into an easy-to-represent model in which security-oriented quantization codebooks can be designed effectively and extended to C-RAN system naturally. Based on this model the concept of quantization loss of ergodic non-zero secrecy rate (QES) is firstly proposed to serve as an efficient codebook design criterion and its upper bound is then derived. The effectiveness of proposed criterion on reducing interference to other co-scheduled users is verified for C-RAN systems when the suitable codeword is selected at the legitimate users.

2. To further design quantization codebooks according to the above criterion, a concept of weighted Voronoi diagram (WVD) on the complex Grassmann manifold of one-dimensional subspaces is formulated by minimizing the upper bound of QES. To implement the derived WVD, a vector-quantization WVD (V-WVD) algorithm is proposed in which conventional codebooks serve as the initial codebooks and iteratively searching for the optimum Voronoi partition is operated on the manifold. To guarantee the convergence property of proposed algorithms, new codeword updating mechanism is devised, based on which new codeword selection criterion is then derived.

3. To theoretically verify the effectiveness of V-WVD based codebook framework on secrecy improvement, two single-integral expressions of the upper bound of QES are derived analytically. A comparison between those two analytical curves and simulated curves of ergodic secrecy rate loss further verifies

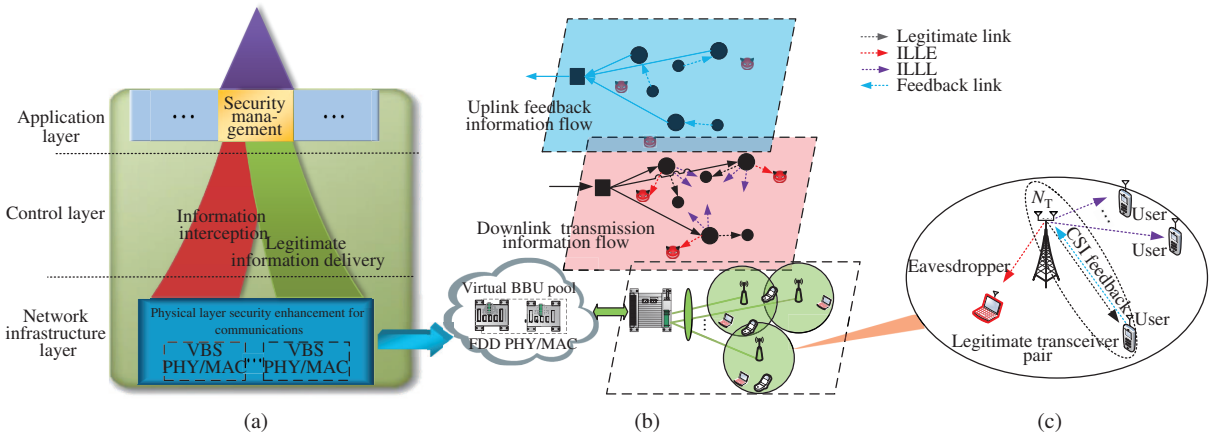

Figure 1 (Color online) (a) Illustration of SDN based C-RAN system with security management; (b) illustration of eavesdropping issues in the physical layer of C-RAN with limited CSI feedback; (c) illustration of QCF model considering both of security and interference issues.

the fact that: for the legitimate user, V-WVD codebooks together with the suitable codeword selection criterion can position the channel vector of eavesdropper to be around the quantization cell [17] created by the orthogonal vector of the suitably selected codeword vector.

4. Simulation results show that the beamforming gain and secrecy rate gain of proposed codebooks, relative to conventional codebooks, can be both acquired from the point of view of ergodic rate with no extra overheads. Therefore, proposed codebooks can be substituted universally for conventional codebooks while no dedicated detection and handover related technologies are operated between proposed codebooks and conventional codebooks. Hence, we can say that our method does not increase the overheads on virtualization of C-RAN while improving the target performance. Furthermore, robust secrecy performance of proposed codebooks can be retained well even when the signal-to-noise ratio (SNR) at the eavesdropper is 10 dB higher than that at the legitimate receiver.

The remainder of this paper is organized as follows. Section 2 introduces the system model. Design framework for quantization codebook in C-RAN is proposed in Section 3 and simulation results are presented in Section 4. Finally, we conclude our work in Section 5.

Notation: Boldface is used for matrixes $\boldsymbol{A}$. $\boldsymbol{A}^{\mathrm{H}}$ respectively denotes the conjugate transpose of matrix $\boldsymbol{A}$. $\|\cdot\|$ denotes the Euclidean norm of a vector or a matrix. $\mathrm{E}\{\cdot\}$ is the expectation operator. $[\cdot]^+$ represents $\max(0,\cdot)$.

2 System model

Consider an SDN based C-RAN system in Figure 1(a) where the system security is enhanced via physical layer techniques, e. g., virtual BS (VBS), to reduce the amount of confidential information intercepted and improve the delivery efficiency of legitimate information. Particularly, a downlink C-RAN system adopting FDD pattern, as shown in Figure 1(b), is researched in which RRHs with N_{T} antennas are connected with virtual BBU pools via fiber front-hauls. Moreover, large-scale single-antenna legitimate users and single-antenna eavesdroppers coexist in the network. Those eavesdroppers are mutually independent and unknown, and each of them overhears the downlink secrecy information intended for the user of interest. We denote $\sqrt{\beta_{k,n}}\boldsymbol{h}_{k,n}$ as the legitimate channel between the nth RRH and the kth legitimate user, and $\sqrt{\alpha_{k,n}}\boldsymbol{g}_{k,n}$ as the channel from the nth RRH to the eavesdropper overhearing the kth user. $\beta_{k,n}$ and $\alpha_{k,n}$ obey the large scale fading which is caused by, e.g., path loss and shadow fading. We assume that the small scale fading vectors (i.e., $\boldsymbol{h}_{k,n}$ and $\boldsymbol{g}_{k,n}$) satisfy $\boldsymbol{h}_{k,n} \sim \mathcal{CN}(\boldsymbol{0},\boldsymbol{I})$ and $\boldsymbol{g}_{k,n} \sim \mathcal{CN}(\boldsymbol{0},\boldsymbol{I})$. Furthermore, each legitimate user is served by one sole RRH. The beamforming vector between the nth RRH and its serving user (i.e., user k) is given as $\boldsymbol{w}_n$. In general, $\boldsymbol{w}_n$ is generated based on the quantized CSI which is derived at user k from the quantization codebook and then conveyed back to RRH

n through limited-feedback channels. For simplicity, we denote the RRH set and user set in C-RAN as $\mathcal{M} = \{1, \ldots, M\}$, $\mathcal{K} = \{1, 2, \ldots, K\}$ respectively. Thus, the received information at arbitrary legitimate user k and its eavesdropper in the network can be given respectively as

$$y_k = \sqrt{P_{\rm s}\beta_{k,n}}\boldsymbol{h}_{k,n}\boldsymbol{w}_n x_n + \underbrace{\sqrt{P_{\rm s}}\sum\nolimits_{m\neq n, m\in\mathcal{M}}\sqrt{\beta_{k,m}}\boldsymbol{h}_{k,m}\boldsymbol{w}_m x_m}_{\text{inter}-\text{RRH interference}} + n_k, \quad k \in K, \tag{1}$$

and

$$y_{{\rm E},k} = \sqrt{P_{\rm s}\alpha_{k,n}}\boldsymbol{g}_{k,n}\boldsymbol{w}_n x_n + \sqrt{P_{\rm s}}\sum\nolimits_{m\neq n, m\in\mathcal{M}}\sqrt{\alpha_{k,m}}\boldsymbol{g}_{k,m}\boldsymbol{w}_m x_m + n_{{\rm E},k}, \quad k \in \mathcal{K}, \tag{2}$$

where x_k is the transmitted symbol for the kth user. $P_{\rm s}$ is the power budget at each RRH. n_k and $n_{{\rm E},k}$ is respectively the additive white Gaussian noise (AWGN) with σ_k^2 variance at the kth user and $\sigma_{{\rm E},k}^2$ variance at its eavesdropper.

2.1 Eavesdropping and secrecy sum-rate model

We assume that each eavesdropper can acquire perfect CSIs between all activated RRHs and itself. It is however noted that this is a quite pessimistic assumption because limited downlink pilot resources make it difficult for the eavesdropper to perform accurate estimation for so many channels simultaneously. As a worst case, the eavesdropper is also able to cancel the received signals except the signal intended for the user of interest, e. g. user k. Since the transmitter uses independent wiretap codebooks for each user, an achievable secrecy sum rate in C-RAN with M RRHs can be given by [19]

$$R_{\rm s} = \sum_{k=1}^{M} R_{{\rm s},k} = \sum_{k=1}^{M}\left[\log_2\left(1+\mathrm{SINR}_k\right) - \log_2\left(1+\mathrm{SINR}_{{\rm E},k}\right)\right]^+, \tag{3}$$

where SINR_k and $\mathrm{SINR}_{{\rm E},k}$ respectively denote the signal to interference plus noise ratios (SINR) for message x_k at the user k and its eavesdropper, which are given by

$$\mathrm{SINR}_k = \frac{(\beta_{k,n}P_{\rm s}/\sigma_k^2)\boldsymbol{w}_n^{\rm H}\boldsymbol{h}_{k,n}^{\rm H}\boldsymbol{h}_{k,n}\boldsymbol{w}_n}{1+P_{\rm s}/\sigma_k^2(\sum_{m\neq n, m\in\mathcal{M}}\boldsymbol{w}_m^{\rm H}\beta_{k,m}\boldsymbol{h}_{k,m}^{\rm H}\boldsymbol{h}_{k,m}\boldsymbol{w}_m)}, \quad \mathrm{SINR}_{{\rm E},k} = \left(P_{\rm s}\alpha_{k,n}/\sigma_{{\rm E},n}^2\right)\|\boldsymbol{g}_{k,n}\boldsymbol{w}_n\|^2. \tag{4}$$

It is noted that the wiretap codebook used herein is not our quantization codebook to be designed. Actually, the two types of codebooks are totally different.

2.2 Scheduling and CSI feedback model

In C-RAN, the joint scheduling of users and RRHs is an essential task for reducing the co-channel interference. We, in this paper, adopt the scheduling framework proposed in [15]. When the scheduling operation for RRHs and legitimate users is completed, each legitimate user will be served by only one anchor RRH. The set $\mathcal{M}$ and $\mathcal{K}$ is assumed to be determined before we conduct any type of codebook design. Note that our newly-designed codebook can be applied to any scheduling algorithm in FDD C-RAN systems.

As to the CSI estimation, the large-scale fading factor is a long term statistic and can be extracted from the uplink reference signal by exploiting its reciprocity. We assume that C-RAN has the knowledge of all large-scale fading factors between each RRH and each legitimate user. In terms of the small-scale fading, each of scheduled legitimate users is assumed to have perfect downlink fading channel information, based on which its channel direction is then quantized as an unit-norm vector from a predefined codebook of unit-norm row vectors: $\mathcal{V} = \{\boldsymbol{c}_1, \ldots \boldsymbol{c}_N\}, N = 2^B$. In particular, when $\boldsymbol{c}_{\rm opt}$ is finally chosen from the codebook $\mathcal{V}$ at user k, the beamforming vector $\boldsymbol{w}_n$ satisfies $\boldsymbol{w}_n = \boldsymbol{c}_{\rm opt}$.

As to the CSI feedback pattern, since RRHs and users are randomly distributed, it is more reasonable to adopt the disjoint feedback mechanism [15] in which each user just quantizes downlink channels from RRHs in RRH cluster to itself as codewords and delivers its codeword indexes back to its anchor RRH.

2.3 Quantization codebook generation model

In this subsection, a clustering communication model is provided as a guideline for quantization codebook generation, which can be then extended naturally to C-RAN systems. We propose to cluster RRHs and users so that each cluster includes one RRH, one target legitimate user and one eavesdropper. This operation is also exploited in [19–21] and considered as a worst case for performance analysis in a cellular communication system subjected to non-colluding eavesdropping behaviors. Based on those models, we consider a more practical scenario where RRH in each cluster also has to leak its information to nodes belonging to other surrounding active clusters. We define this type of cluster as a reference scenario where a Quantized-CSI-feedback (QCF) based communications model is formulated and shown in Figure 1(c). Specifically, the link between the RRH and its eavesdropper is defined as the information leakage link to eavesdropper (ILLE) and the legitimate link between the RRH and other legitimate users is denoted as the information leakage link to legitimate (ILLL) users.

In the following, we will give detailed backgrounds and physical motivations for developing QCF model. In general, two vital points need to be considered for C-RAN in terms of CSI quantization.

1. Cooperative RRHs engender great difficulties for the downlink CSI quantization and induce significant quantization errors. Particularly, the combination of channels between users and cooperative RRHs (even with two cooperative RRHs) can generate a complicate, unmeasurable and unpredictable high-dimension space. Take a two-RRH cluster for example. The channel magnitude and phase of the composite channel at user k, denoted as $\left[\ \sqrt{\beta_{k,1}}\boldsymbol{h}_{k,1}\ \ \sqrt{\beta_{k,2}}\boldsymbol{h}_{k,2}\ \right]$, can vary significantly with large-scale factors $\beta_{k,1}, \beta_{k,2}$ which are usually determined by user behaviors.

2. The ubiquitous interference induced by surrounding RRHs is hard to estimate and eliminate, thus impeding the precise and deterministic quantization for downlink channels through an unique codebook.

Fortunately, our proposed QCF model has the following benefits:

1. Codebook generation is based on a sole wireless channel between the anchor RRH and its serving user, thus facilitating the channel quantization.

2. Information leakage at the transmitter can be controlled by redesigning the waveform directly during the process of quantization codebook design.

3. The generated codebook can be generalized to cooperative scenarios supporting user and RRH scheduling functionality, despite the fact that QCF model is solely designed for codebook design rather than user scheduling.

Under QCF model, the received signals at the legitimate user and its eavesdropper at ILLE can be given as

$$y_k = \sqrt{P_{\mathrm{s}}\beta_{k,n}}\boldsymbol{h}_{k,n}\boldsymbol{w}_n x_n + z_k \ \text{ and } \ y_{\mathrm{E},k} = \sqrt{P_{\mathrm{s}}\alpha_{k,n}}\boldsymbol{g}_{k,n}\boldsymbol{w}_n x_n + n_{\mathrm{E},k}, \quad k \in \mathcal{K},\ n \in \mathcal{M}, \tag{5}$$

where $z_k = \sqrt{P_{\mathrm{s}}}\sum_{m\neq n, m\in\mathcal{M}}\sqrt{\beta_{k,m}}\boldsymbol{h}_{k,m}\boldsymbol{w}_m x_m + n_k$ is equivalent noise with its power defined as $\sigma^2_{k,\mathrm{equ}}$. $y_{\mathrm{E},k}$ is obtained by assuming the worst case described in Subsection 2.1. To measure the level of information leakage at ILLL, the concept of signal-to-leakage-and-noise ratio (SLNR) is considered in this paper. Recall that SLNR is defined as the ratio of received signal power at the desired user to received signal power at the other terminals (the leakage) plus noise power. For an arbitrary RRH n, its SLNR is defined as

$$\mathrm{SLNR}_n = \frac{\frac{P_{\mathrm{s}}}{\sigma^2_{k,\mathrm{equ}}}\beta_{k,n}\boldsymbol{w}_n^{\mathrm{H}}\boldsymbol{h}_{k,n}^{\mathrm{H}}\boldsymbol{h}_{k,n}\boldsymbol{w}_n}{1+\frac{P_{\mathrm{s}}}{\sigma^2_{k,\mathrm{equ}}}\boldsymbol{w}_n^{\mathrm{H}}(\sum_{i\neq k, i\in\mathcal{K}}\beta_{i,n}\boldsymbol{h}_{i,n}^{\mathrm{H}}\boldsymbol{h}_{i,n})\boldsymbol{w}_n} \overset{\mathrm{def}}{=} \frac{\frac{P_{\mathrm{s}}}{\sigma^2_{k,\mathrm{equ}}}\beta_{k,n}\boldsymbol{w}_n^{\mathrm{H}}\boldsymbol{h}_{k,n}^{\mathrm{H}}\boldsymbol{h}_{k,n}\boldsymbol{w}_n}{1+\gamma_{\mathrm{equ},n}\boldsymbol{w}_n^{\mathrm{H}}\boldsymbol{h}^{\mathrm{H}}\boldsymbol{h}\boldsymbol{w}_n}, \tag{6}$$

where $\boldsymbol{h}$ has the same statistical distribution as $\boldsymbol{h}_{k,n}$ and $\gamma_{\mathrm{equ},n}$ is a constant of limited value, influenced by the interference level.

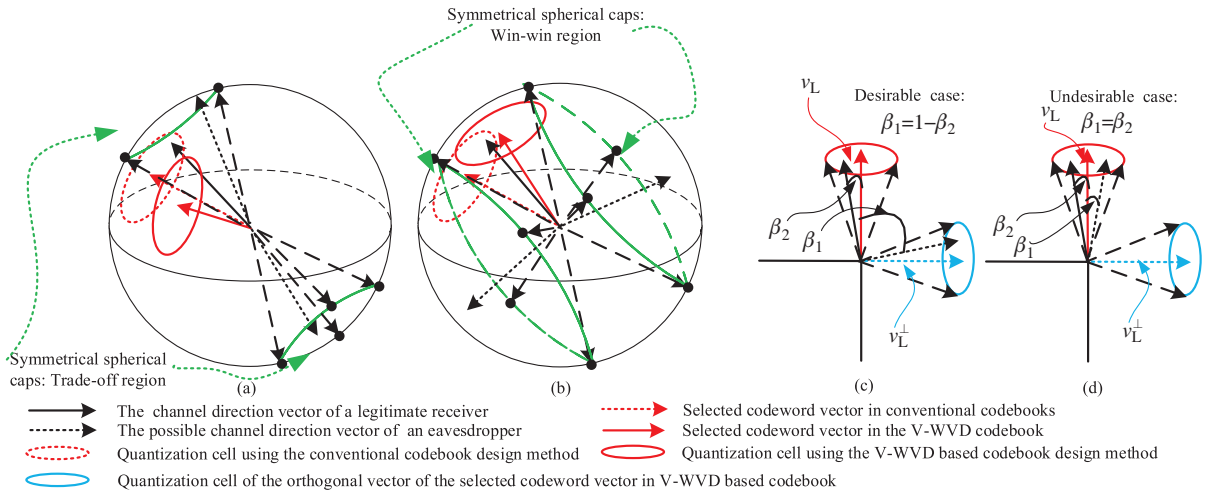

Figure 2 (Color online) (a)(b) A geometric interpretation for quantized codeword vectors, channel direction vectors and corresponding win-win and tradeoff regions. Especially, an eavesdropper's channel direction vector is distributed randomly in the whole space composed of win-win and tradeoff regions. Those two kinds of regions are complementary. Quantization cell of a codeword functions to quantize a channel direction vector located in the cell as the codeword; (c)(d) the relationship of novel codewords in V-WVD codebooks with the eavesdropper's channel direction vector.

3 Design framework for quantization codebook in C-RAN

3.1 Advanced channel quantization method for QCF model

3.1.1 *Rethinking conventional channel quantization method*

Problem 1. Conventional channel quantization focuses on the point-to-point or single-user channel and its performance optimization, e.g., maximizing minimum distance which is defined in a Grassmannian line packing problem [22] or minimizing the quantization loss of capacity. However, in the wireless multiuser environment with large-scale communication nodes (i.e., legitimate users and eavesdroppers), the information leakage of each node manifests inevitably in the form of interference to other nodes and/or via the patterns of secrecy loss. The conventional quantization method is thus no longer suitable for proposed QCF model. Furthermore, as the channel dimension increases, the information transmission efficiency is further deteriorated by the limited-precision codewords and the level of information leakage is reinforced unexpectedly, thus incurring serious interference and security problems.

3.1.2 *Novel quantization method towards two users: exploiting the statistical distribution of the legitimate user's channel and eavesdropper's channel simultaneously*

To explain the consideration, we focus on the one-time random channel realization, analyse the possible phenomenon, give the corresponding interpretation and then extend the result to the codebook design under ergodic realization.

As is shown in Figure 2 (a) and (b), the effect of eavesdropping behaviors on the codeword generation is interpreted geometrically. When the eavesdropping behavior happens, codeword vectors selected from conventional codebooks will actuate secrecy information leakage. The leakage level is influenced by the location of the eavesdropper's channel vector in the space. To reduce the leakage by using new codewords, the adaptive revision of the codewords is necessary and determined by the region that the eavesdropper's channel vector is located in. Generally, perfect positioning and precise tracking for the CSI of an eavesdropper is impossible for the legitimate transceiver pair. However, when considering the traditional ergodic fading scenario, an interesting division for the space experienced by eavesdropper's channel vectors can be formulated and the whole space can be divided into two regions, namely tradeoff region and win-win region respectively. These space partitions can help us find a valuable quantization method. The sizes of these partitions are determined by several factors, e.g. the size of quantization cell,

the relative location between legitimate user's channel vector and eavesdropper's channel vector.

The tradeoff region. This region can be seen as a Voronoi region of a spherical cap. When falling into this region, the channel vector of an eavesdropper is in close proximity to that of a legitimate user. However, it is impossible that a desirable codeword attempting to obtain secrecy rate gain can be generated via improving beamforming gain. There are two reasons: the first is that more beamforming gain is hard to obtain due to quantization errors. The second is that the improvement of beamforming gain can extremely benefit the eavesdropper as well. Thus the ultimate result for the adaptive revision of a new codword is that it will compel systems to sacrifice bemaforming gain for secrecy rate gain.

The win-win region. This region is a complementary space of the trade-off region. When the eavesdropper's channel vector is located in this region, the new codeword can not only be closer to the orthogonal vector of the eavesdropper's channel vector but also be nearer to the channel vector of the legitimate user, which means that both improving beamforming gain and secrecy rate gain can be achieved in this context.

Based on the two regions, we consider the ergodic fading situation and have:

Proposition 1. Given that ergodic fast Rayleigh fading channels are experienced, novel codewords could be generated both with better measure of the legitimate user's channel and improved secrecy from the point of view of ergodic rate.

According to the random matrix theory, the random Gaussian channel matrix is bi-unitarily invariant and its channel vector is uniformly distributed over the manifold. Based on the geometry method, the quantization cell of conventional codebooks affects and restricts the relative location of channel vectors due to the influence of quantization errors. By comparing the angles between two channel vectors, it can be easily calculated and outlined that the win-win region in high-dimension space is more dominant to be experienced than the tradeoff region for the ergodic fading environment.

3.2 Novel quantization codebook design

3.2.1 *Secrecy-oriented criterion for quantization codebook design*

In this subsection, we provide a formulized solution for the criterion design by adopting an optimum secure beamforming method. With the beamforming vector quantized, a design criterion of quantization codebook can be then derived.

Remark 1. In the optimum secure beamforming method, perfect CSIs for legitimate users and eavesdroppers are assumed to formulate the criterion under an information-theoretic framework. This theoretical framework provides a guideline for the practical criterion implementation which is based on the offline training approach shown in Subsection 3.2.4. All the channels in the training are both unknown except their statistical distribution and both selected from a common dictionary satisfying the statistical distribution. Specifically, we define the dictionary as $\mathcal{P} = \{\boldsymbol{G}_i\}_{i=1}^{T}$, where T is the number of channel samples. $\boldsymbol{G}_i$ is the random and memoryless channel realization under the statistical distribution (e.g., ergodic fast Rayleigh fading). For simplicity, we let $P_{\mathrm{s}}\beta_{k,n}/\sigma_{k,\mathrm{equ}}^2 \overset{\mathrm{def}}{=} \gamma_{\mathrm{L}}$, $P_{\mathrm{s}}\alpha_{k,n}/\sigma_{\mathrm{E},k}^2 \overset{\mathrm{def}}{=} \gamma_{\mathrm{E}}$, $\boldsymbol{w} = \{\boldsymbol{w}_n | n \in \mathcal{M}\}$, $\boldsymbol{G} = [\boldsymbol{h}_{k,n}^{\mathrm{H}}, \boldsymbol{g}_{k,n}^{\mathrm{H}}]^{\mathrm{H}}$, and $\boldsymbol{\Sigma}_{\mathrm{L}}\boldsymbol{G} = \{\boldsymbol{h}_{k,n} | k \in \mathcal{K}, n \in \mathcal{M}\}$, $\boldsymbol{\Sigma}_{\mathrm{E}}\boldsymbol{G} = \{\boldsymbol{g}_{k,n} | k \in \mathcal{K}, n \in \mathcal{M}\}$, $\boldsymbol{\Sigma}_{\mathrm{L}} = [\,1\ 0\,], \boldsymbol{\Sigma}_{\mathrm{E}} = [\,0\ 1\,]$ According to [12], the achievable secrecy rate for (5) with beamforming can be written as

$$R_{\mathrm{S}}^{\mathrm{BF}} = \left[\max_{\boldsymbol{w}:\|\boldsymbol{w}\|^2=1} \log_2 \left(\frac{1+\gamma_{\mathrm{L}}\boldsymbol{w}^{\mathrm{H}}\boldsymbol{G}^{\mathrm{H}}\boldsymbol{\Sigma}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{\Sigma}_{\mathrm{L}}\boldsymbol{G}\boldsymbol{w}}{1+\gamma_{\mathrm{E}}\boldsymbol{w}^{\mathrm{H}}\boldsymbol{G}^{\mathrm{H}}\boldsymbol{\Sigma}_{\mathrm{E}}^{\mathrm{H}}\boldsymbol{\Sigma}_{\mathrm{E}}\boldsymbol{G}\boldsymbol{w}} \right) \right]^{+}. \tag{7}$$

Under the power constraint P, the maximum achievable secrecy rate can be determined as

$$R_{\mathrm{S}}^{\mathrm{BF}} = \left[\log_2 \lambda_{\max} \left(\boldsymbol{A}\left(\boldsymbol{G}, \gamma_{\mathrm{L}}\right), \boldsymbol{B}\left(\boldsymbol{G}, \gamma_{\mathrm{E}}\right) \right) \right]^{+}, \tag{8}$$

and the corresponding optimal beamforming vector is given by

$$\boldsymbol{w}_{\mathrm{opt}} = \varphi_{\max} \left(\boldsymbol{A}\left(\boldsymbol{G}, \gamma_{\mathrm{L}}\right), \boldsymbol{B}\left(\boldsymbol{G}, \gamma_{\mathrm{E}}\right) \right), \tag{9}$$

where $\boldsymbol{A}(\boldsymbol{G},\gamma_{\mathrm{L}}) = \boldsymbol{I}_{N_{\mathrm{T}}} + \gamma_{\mathrm{L}}\boldsymbol{G}^{\mathrm{H}}\boldsymbol{\Sigma}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{\Sigma}_{\mathrm{L}}\boldsymbol{G}$ and $\boldsymbol{B}(\boldsymbol{G},\gamma_{\mathrm{E}}) = \boldsymbol{I}_{N_{\mathrm{T}}} + \gamma_{\mathrm{E}}\boldsymbol{G}^{\mathrm{H}}\boldsymbol{\Sigma}_{\mathrm{E}}^{\mathrm{H}}\boldsymbol{\Sigma}_{\mathrm{E}}\boldsymbol{G}$. $\lambda_{\max}(\boldsymbol{A},\boldsymbol{B})$ is the maximum eigenvalue of $\boldsymbol{B}^{-1}\boldsymbol{A}$. $\varphi_{\max}(\boldsymbol{A},\boldsymbol{B})$ is the generalized eigenvector corresponding to $\lambda_{\max}(\boldsymbol{A},\boldsymbol{B})$. The ergodic secrecy rate adopting (9) is derived as follows:

$$R_{\mathrm{S}}^{\mathrm{Erg}} = \mathrm{E}\left\{\left[\log_2\lambda_{\max}\left(\boldsymbol{A}(\boldsymbol{G},\gamma_{\mathrm{L}}),\boldsymbol{B}(\boldsymbol{G},\gamma_{\mathrm{E}})\right)\right]^{+}\right\}. \tag{10}$$

Remark 2. By assuming that in each channel realization the optimal beamforming vector is adopted, ergodic secrecy rate is obtained, which actually serves as an upper bound rate for limited-feedback systems and acts as a benchmark for the following calculation of the loss of ergodic secrecy rate due to the channel quantization.

Generally, a quantization version of $\boldsymbol{w}_{\mathrm{opt}}$ can be given by $\boldsymbol{v}_{\mathrm{L}} = \mathcal{Q}(\boldsymbol{w}_{\mathrm{opt}})$ where $\mathcal{Q}$ is the quantization function. The ergodic secrecy rate under this quantized beamformer is further represented by

$$R_{\mathrm{S}}^{\mathrm{Erg,Q}} = \mathrm{E}\left\{\left[\log_2\left(\frac{1+\gamma_{\mathrm{L}}\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{G}^{\mathrm{H}}\boldsymbol{\Sigma}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{\Sigma}_{\mathrm{L}}\boldsymbol{G}\boldsymbol{v}_{\mathrm{L}}}{1+\gamma_{\mathrm{E}}\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{G}^{\mathrm{H}}\boldsymbol{\Sigma}_{\mathrm{E}}^{\mathrm{H}}\boldsymbol{\Sigma}_{\mathrm{E}}\boldsymbol{G}\boldsymbol{v}_{\mathrm{L}}}\right)\right]^{+}\right\}. \tag{11}$$

Therefore, ergodic secrecy rate loss due to the beamforming quantization is denotes as

$$R_{\mathrm{S}}^{\mathrm{Q,loss}} = R_{\mathrm{S}}^{\mathrm{Erg}} - R_{\mathrm{S}}^{\mathrm{Erg,Q}}. \tag{12}$$

Intuitively, it is difficult to obtain a specific criterion for designing codebooks. In the following, we provide an efficient methodology for further simplification and formulate the concept of QES. For simplicity, we let $\boldsymbol{A} = \boldsymbol{A}(\boldsymbol{G},\gamma_{\mathrm{L}}), \boldsymbol{B} = \boldsymbol{B}(\boldsymbol{G},\gamma_{\mathrm{E}})$ and $\boldsymbol{C} = \lambda_{\max}(\boldsymbol{A}(\boldsymbol{G},\gamma_{\mathrm{L}}))\boldsymbol{B}(\boldsymbol{G},\gamma_{\mathrm{E}})$.

Definition 1. Based on (12), the QES criterion tailored for V-WVD codebook design can be given by

$$R^{\mathrm{QES}} = \mathrm{E}\left\{\log_2\left(\lambda_{\max}(\boldsymbol{A},\boldsymbol{B})\frac{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{B}\boldsymbol{v}_{\mathrm{L}}}{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{A}\boldsymbol{v}_{\mathrm{L}}}\right)\right\}. \tag{13}$$

Proof. We firstly focus on the first term of $R_{\mathrm{S}}^{\mathrm{Q,loss}}$ in (12). If $\lambda_{\max}(\boldsymbol{A},\boldsymbol{B}) > 1$, the first term will be $\mathrm{E}\{\log_2\lambda_{\max}(\boldsymbol{A},\boldsymbol{B})\}$, otherwise zero. Secondly, we denote an arbitrary rayleigh entropy as $Z = \frac{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{A}\boldsymbol{v}_{\mathrm{L}}}{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{B}\boldsymbol{v}_{\mathrm{L}}}$. According to the property of rayleigh entropy, there exists $\lambda_{\min}(\boldsymbol{A},\boldsymbol{B}) \leqslant Z \leqslant \lambda_{\max}(\boldsymbol{A},\boldsymbol{B})$. Therefore, if there exists $\lambda_{\max}(\boldsymbol{A},\boldsymbol{B}) > 1, \lambda_{\min}(\boldsymbol{A},\boldsymbol{B}) > 1$, $R_{\mathrm{S}}^{\mathrm{Q,loss}}$ is equal to $\mathrm{E}\{\log_2(\lambda_{\max}(\boldsymbol{A},\boldsymbol{B})\frac{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{B}\boldsymbol{v}_{\mathrm{L}}}{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{A}\boldsymbol{v}_{\mathrm{L}}})\}$. Or if $\lambda_{\max}(\boldsymbol{A},\boldsymbol{B}) > 1$, $\lambda_{\min}(\boldsymbol{A},\boldsymbol{B}) < 1$, then $R_{\mathrm{S}}^{\mathrm{Q,loss}}$ will be $\mathrm{E}\{\log_2(\lambda_{\max}(\boldsymbol{A},\boldsymbol{B}))\} - \mathrm{E}\{[\log_2(\frac{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{A}\boldsymbol{v}_{\mathrm{L}}}{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{B}\boldsymbol{v}_{\mathrm{L}}})]^{+}\}$. However, in each channel realization our focus is the loss of the non-zero secrecy rate which means $\frac{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{A}\boldsymbol{v}_{\mathrm{L}}}{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{B}\boldsymbol{v}_{\mathrm{L}}} > 1$, thus QES will be equal to $\mathrm{E}\{\log_2(\lambda_{\max}(\boldsymbol{A},\boldsymbol{B})\frac{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{B}\boldsymbol{v}_{\mathrm{L}}}{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{A}\boldsymbol{v}_{\mathrm{L}}})\}$. Moreover, if $\lambda_{\max}(\boldsymbol{A},\boldsymbol{B}) < 1$ the second part will be zero, which means that the secrecy rate is zero and is not our focus. Note that the number of channel realizations satisfying $R_{\mathrm{S}}^{\mathrm{Erg,Q}} > 0$ is much larger than that satisfying that $R_{\mathrm{S}}^{\mathrm{Erg,Q}} = 0$, if we exploit the suitable codeword selection criterion [17]. This property means that the term of secrecy rate equal to zero can be ignored and $\mathrm{E}\{\log_2(\lambda_{\max}(\boldsymbol{A},\boldsymbol{B})\frac{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{B}\boldsymbol{v}_{\mathrm{L}}}{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{A}\boldsymbol{v}_{\mathrm{L}}})\}$ is a reasonable criterion for QES. Then the proof is completed.

Lemma 1. Under the fixed power constrain at the transmitter, for the Hermitian matrices $\boldsymbol{A}$ and $\boldsymbol{B}$, there exists

$$\lambda_{\max}(\boldsymbol{A},\boldsymbol{B}) \leqslant \lambda_{\max}\left(\boldsymbol{B}^{-1}\right)\lambda_{\max}(\boldsymbol{A}). \tag{14}$$

Proof. For an arbitrary matrix $\boldsymbol{A}$, $\lambda_{\max}(\boldsymbol{A})$ can be seen an induced norm such as $\|\boldsymbol{A}\|_{\alpha}$ with $\alpha = 2$ which is usually seen as L2-induced norm. Generally, for arbitrary induced norm, there exists the following inequalities [23]:

$$\|\boldsymbol{B}^{-1}\boldsymbol{A}\|_{\alpha} = \max_{x\neq 0}\frac{\|\boldsymbol{B}^{-1}\boldsymbol{A}\boldsymbol{x}\|_{\alpha}}{\|\boldsymbol{x}\|_{\alpha}} \leqslant \max_{x\neq 0}\frac{\|\boldsymbol{B}^{-1}(\boldsymbol{A}\boldsymbol{x})\|_{\alpha}}{\|\boldsymbol{A}\boldsymbol{x}\|_{\alpha}}\max_{x\neq 0}\frac{\|\boldsymbol{A}\boldsymbol{x}\|_{\alpha}}{\|\boldsymbol{x}\|_{\alpha}} = \|\boldsymbol{B}^{-1}\|_{\alpha}\|\boldsymbol{A}\|_{\alpha}. \tag{15}$$

When $\alpha = 2$, we can easily transform the above inequality into $\lambda_{\max}\left(\boldsymbol{B}^{-1}\boldsymbol{A}\right) \leqslant \lambda_{\max}\left(\boldsymbol{B}^{-1}\right)\lambda_{\max}(\boldsymbol{A})$. It has been proved in [24] that $\lambda_{\max}\left(\boldsymbol{B}^{-1}\boldsymbol{A}\right)$ is approximately $\lambda_{\max}\left(\boldsymbol{B}^{-1}\right)\lambda_{\max}(\boldsymbol{A})$ when the eigenvectors of two matrixes $\boldsymbol{B}^{-1}$ and $\boldsymbol{A}$ vary slowly.

Remark 3. When the eigenvectors of two matrixes $\boldsymbol{B}^{-1}$ and $\boldsymbol{A}$ vary slowly, it means that the CSI of the eavesdropper is approximately equal to that of the legitimate user. Actually, it can be seen as a case where an eavesdropper is located around the legitimate user and has similar wireless propagation conditions with the legitimate user. Therefore, this upper bound can be achieved and further used for criterion simplification.

Theorem 1. According to the above lemma, under the fixed power constrain at the transmitter, the upper bound of QES in (13) will be given by

$$R^{\mathrm{QES}} \leqslant R^{\mathrm{QES}}_{\mathrm{upper}} = \mathbb{E}\left[\log_2\left(\frac{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{C}\boldsymbol{v}_{\mathrm{L}}}{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{A}\boldsymbol{v}_{\mathrm{L}}}\right)\right]. \tag{16}$$

Proof. Since the matrix $\boldsymbol{B}$ is a positive definite Hermitian matrix with the largest eigenvalue $1+\gamma_{\mathrm{E}}\boldsymbol{\Sigma}_{\mathrm{E}}\boldsymbol{G}\boldsymbol{G}^{\mathrm{H}}\boldsymbol{\Sigma}_{\mathrm{E}}^{\mathrm{H}}$ and smallest eigenvalue 1, $\boldsymbol{B}^{-1}$ has the largest eigenvalue satisfying $\lambda_{\max}(\boldsymbol{B}^{-1})=1$ and smallest eigenvalue satisfying $\lambda_{\min}(\boldsymbol{B}^{-1})=\frac{1}{1+\gamma_{\mathrm{E}}\boldsymbol{\Sigma}_{\mathrm{E}}\boldsymbol{G}\boldsymbol{G}^{\mathrm{H}}\boldsymbol{\Sigma}_{\mathrm{E}}^{\mathrm{H}}}$. Therefore, we can derive the upper bound of $\lambda_{\max}(\boldsymbol{A},\boldsymbol{B})$ in (13) as $\lambda_{\max}(\boldsymbol{A})$ according to the lemma 1. Because of the convex property of log function, an upper bound of (13) is obtained as (16). The proof is completed.

When further simplifying the upper bound in (16), we have:

$$R^{\mathrm{QES}}_{\mathrm{upper}} = -\mathrm{E}\left[\log_2\left(1-\left(1-\frac{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{A}\boldsymbol{v}_{\mathrm{L}}}{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{C}\boldsymbol{v}_{\mathrm{L}}}\right)\right)\right] \overset{\text{(a)}}{\approx} \frac{1}{\ln 2}\mathrm{E}\left(1-\frac{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{A}\boldsymbol{v}_{\mathrm{L}}}{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{C}\boldsymbol{v}_{\mathrm{L}}}\right), \tag{17}$$

where (a) is obtain by taking the first order approximation using $\ln(1-x)\approx -x$. The approximation is important as it provide an efficient design guideline for codebook design method and is well justified in the high power and high resolution regime (large N). To minimize $R^{\mathrm{QES}}_{\mathrm{upper}}$ in (17), we design a quantizer $\mathcal{Q}\left(\mathcal{Q}:\mathbb{C}^{N_{\mathrm{T}}}\to\mathcal{V}\right)$ satisfying:

$$\max_{\mathcal{Q}(\bullet)} \mathrm{E}\left[\frac{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{A}\boldsymbol{v}_{\mathrm{L}}}{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{C}\boldsymbol{v}_{\mathrm{L}}}\right]. \tag{18}$$

Secrecy-quality measure. We define $S(\boldsymbol{v}_{\mathrm{L}})=\frac{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{A}\boldsymbol{v}_{\mathrm{L}}}{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{C}\boldsymbol{v}_{\mathrm{L}}}$ as a secrecy-quality measure. Then the secrecy-oriented criterion is equivalent to maximize the average secrecy-quality measure.

3.2.2 *Achieve interference reduction by reconsidering the structure of secrecy-oriented criterion*

In this subsection, we show how the secrecy-oriented criterion can bring interference reduction gains.

Proposition 2. The offline training-based optimization for (18) under high SNR can be equivalent to maximizing the SLNR subjected to quantized beamforming $\boldsymbol{v}_{\mathrm{L}}$.

We denote the expansion of (18) as $\max\limits_{\mathcal{Q}(\bullet)}\mathrm{E}\left[\frac{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{h}_{k,n}^{\mathrm{H}}\boldsymbol{h}_{k,n}\boldsymbol{v}_{\mathrm{L}}}{1+P_{\mathrm{s}}\alpha_{k,n}/\sigma_{\mathrm{E},k}^2\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{g}_{k,n}^{\mathrm{H}}\boldsymbol{g}_{k,n}\boldsymbol{v}_{\mathrm{L}}}\right]$. To optimize the criterion, we adopt the training-based approach which can be detailed in Subsection 3.2.4. Based on this approach, $\boldsymbol{g}_{k,n}$ and $\boldsymbol{h}_{k,n}$ in the expectation item are both selected from the dictionary to approximate the expectation operator. As shown in Section 2, eavesdroppers have the same channel distribution as the legitimate users, which means that all types of channels can share a common dictionary. Thus, optimizing $\boldsymbol{g}_{k,n}$ from $\mathcal{P}$ in the denominator of the expectation item can be deemed equivalently as optimizing a legitimate channel vector sampled from $\mathcal{P}$, that is to say,

$$\max_{\mathcal{Q}(\bullet)}\mathrm{E}\left[\frac{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{h}_{k,n}^{\mathrm{H}}\boldsymbol{h}_{k,n}\boldsymbol{v}_{\mathrm{L}}}{1+P_{\mathrm{s}}\alpha_{k,n}/\sigma_{\mathrm{E},k}^2\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{g}_{k,n}^{\mathrm{H}}\boldsymbol{g}_{k,n}\boldsymbol{v}_{\mathrm{L}}}\right] \overset{\text{Equivalent}}{\longleftrightarrow} \max_{\mathcal{Q}(\bullet)}\mathrm{E}\left[\frac{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{h}_{k,n}^{\mathrm{H}}\boldsymbol{h}_{k,n}\boldsymbol{v}_{\mathrm{L}}}{1+P_{\mathrm{s}}\alpha_{k,n}/\sigma_{\mathrm{E},k}^2\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{h}^{\mathrm{H}}\boldsymbol{h}\boldsymbol{v}_{\mathrm{L}}}\right], \tag{19}$$

where $\boldsymbol{h}$ is shown in (6) and can be the channel sample selected from $\mathcal{P}$. Based on the above interpretation, the original secrecy-oriented design criterion can be interpreted as the maximum of the expectation of SLNR, thus reducing its information leakage to eavesdroppers and interference to other co-channel users simultaneously.

3.2.3 *Constructing WVD based on secrecy-oriented criterion*

According to the criterion (18), an optimum partition (Voronoi Region) for the ith codeword vector in the kth partition can be defined as

$$\mathcal{R}_{(k),i} = \left\{ \widehat{\boldsymbol{h}}_{\mathrm{L}}^{\mathrm{H}} \middle| \frac{\boldsymbol{v}_{(k-1),\mathrm{L},i}^{\mathrm{H}} \boldsymbol{A} \boldsymbol{v}_{(k-1),\mathrm{L},i}}{\boldsymbol{v}_{(k-1),\mathrm{L},i}^{\mathrm{H}} \boldsymbol{C} \boldsymbol{v}_{(k-1),\mathrm{L},i}} \geqslant \frac{\boldsymbol{v}_{(k-1),\mathrm{L},j}^{\mathrm{H}} \boldsymbol{A} \boldsymbol{v}_{(k-1),\mathrm{L},j}}{\boldsymbol{v}_{(k-1),\mathrm{L},j}^{\mathrm{H}} \boldsymbol{C} \boldsymbol{v}_{(k-1),\mathrm{L},j}} \right\}. \tag{20}$$

The partition that is optimum for $\mathcal{V}$ is constructed by mapping each $\widehat{\boldsymbol{h}}_{\mathrm{L}}^{\mathrm{H}}$ into $\boldsymbol{v}_{(k-1),\mathrm{L},i}, i = 1, \ldots, N$ maximizing the secrecy-quality measure, that is, by choosing the maximum secrecy-quality measure or farthest-neighbor codeword vector for each random channel vector. To further characterize the Voronoi diagram, a distance measure between the codeword vector and the channel direction vector is defined as

$$d_{\mathrm{o}}\left(\boldsymbol{v}_{(k-1),\mathrm{L},i}, \widehat{\boldsymbol{h}}_{\mathrm{L}}^{\mathrm{H}}\right) = \left| \boldsymbol{v}_{(k-1),\mathrm{L},i}^{\mathrm{H}} \widehat{\boldsymbol{h}}_{\mathrm{L}}^{\mathrm{H}} \right|^2 = \cos\left(\boldsymbol{v}_{(k-1),\mathrm{L},i}, \widehat{\boldsymbol{h}}_{\mathrm{L}}^{\mathrm{H}}\right), \tag{21}$$

where $\widehat{\boldsymbol{h}}_{\mathrm{L}}^{\mathrm{H}} = \boldsymbol{h}_{\mathrm{L}} / \|\boldsymbol{h}_{\mathrm{L}}\|$. This measure is usually used for generating Voronoi diagram on the Grassmann manifold $\mathcal{G}(N_{\mathrm{T}}, 1)$ which is a set of one-dimensional subspaces [22].

Theorem 2. The overall partition (20) constitute a compoundly weighted Voronoi diagram on $\mathcal{G}(N_{\mathrm{T}}, 1)$ with multiplicative and additive weights. The corresponding Voronoi region of ith codeword vector satisfies

$$\mathcal{R}_{(k),i}\left(\mathcal{W}_{(k-1)}\right) = \left\{ \widehat{\boldsymbol{h}}_{\mathrm{L}}^{\mathrm{H}} \middle| d\left(\boldsymbol{v}_{(k-1),\mathrm{L},i}, \widehat{\boldsymbol{h}}_{\mathrm{L}}^{\mathrm{H}}\right) \geqslant d\left(\boldsymbol{v}_{(k-1),\mathrm{L},j}, \widehat{\boldsymbol{h}}_{\mathrm{L}}^{\mathrm{H}}\right) \right\}, \quad \forall j \neq i, j = 1, \ldots, N. \tag{22}$$

The weight set $\mathcal{W}_{(k-1)} = \{w_{(k-1),1} \ldots w_{(k-1),N_{\mathrm{T}}}\}$ is dynamically updated and each element of this set satisfies $w_{(k-1),i} = \frac{1}{1+\gamma_{\mathrm{E}} \boldsymbol{v}_{(k-1),\mathrm{L},i}^{\mathrm{H}} \boldsymbol{h}_{\mathrm{E}}^{\mathrm{H}} \boldsymbol{h}_{\mathrm{E}} \boldsymbol{v}_{(k-1),\mathrm{L},i}}$, $\boldsymbol{h}_{\mathrm{E}}^{\mathrm{H}} \in \mathbb{C}^{N_{\mathrm{T}} \times 1}$. $d(\boldsymbol{v}_{(k-1),\mathrm{L},i}, \widehat{\boldsymbol{h}}_{\mathrm{L}}^{\mathrm{H}})$ is a weighted distance measure satisfying:

$$d\left(\boldsymbol{v}_{(k-1),\mathrm{L},i}, \widehat{\boldsymbol{h}}_{\mathrm{L}}^{\mathrm{H}}\right) = w_{(k-1),i} + f\left(w_{(k-1),i}\right) d_{\mathrm{o}}\left(\boldsymbol{v}_{(k-1),\mathrm{L},i}, \widehat{\boldsymbol{h}}_{\mathrm{L}}^{\mathrm{H}}\right), \tag{23}$$

where $\widehat{\boldsymbol{h}}_{\mathrm{L}}^{\mathrm{H}} \in \mathcal{G}(N_{\mathrm{T}}1)$. $f(x)$ is a non-decreasing function with $f(x) = x\gamma_{\mathrm{L}} \|\boldsymbol{h}_{\mathrm{L}}\|^2$. Intuitively, codeword vectors that benefit eavesdroppers (small weight) tend to increase the distances $d_{\mathrm{o}}(\boldsymbol{v}_{(k-1),\mathrm{L},i}, \widehat{\boldsymbol{h}}_{\mathrm{L}}^{\mathrm{H}})$; vice versa, codeword vectors (large weight) tend to decrease the distances. Product $f(w_{(k-1),i}) d_{\mathrm{o}}(\boldsymbol{v}_{(k-1),\mathrm{L},i}, \widehat{\boldsymbol{h}}_{\mathrm{L}}^{\mathrm{H}})$ can be viewed as an operator which "attracts" (increases overall distance measure) vectors $\boldsymbol{h}_{\mathrm{L}}^{\mathrm{H}}$ that are far away from $\boldsymbol{v}_{(k-1),\mathrm{L},i}$ or the corresponding weight $w_{(k-1),i}$ is large. Likewise, they "repels" (decreases overall distance measure) such vectors $\boldsymbol{h}_{\mathrm{L}}^{\mathrm{H}}$ that are close to $\boldsymbol{v}_{(k-1),\mathrm{L},i}$ or are quantized with small $w_{(k-1),i}$. Using addition operation of weight for distance measure has the same intuitive interpretation shown above.

3.2.4 *Codebook generation algorithm*

In this subsection, we first propose to extend the VQ method to WVD and formulate a V-WVD framework for novel codebook generation. To facilitate the offline operation, plentiful channels $\boldsymbol{G}$ are selected ergodically from the dictionary $\mathcal{P}$, which provides sufficient channel samples and accommodates the requirements of statistical properties during the criterion optimization. Codewords for beamforming are iteratively generated and improved, and a quantization codebook can be constructed ultimately. The procedure is given as follows:

I. Initializing Codebooks: Select a conventional codebook as an initial codebook $\mathcal{V}$ satisfying $\mathcal{V}_{(0)} = \left\{\boldsymbol{v}_{(0),\mathrm{L},1}, \boldsymbol{v}_{(0),\mathrm{L},2}, \ldots, \boldsymbol{v}_{(0),\mathrm{L},N}\right\}$ with $N = 2^B$. Each codeword vector $\boldsymbol{v}_{(0),\mathrm{L},i} \in \mathbb{C}^{N_{\mathrm{T}} \times 1}, i = 1, \ldots, N$ has unit norm. At first, the number of iterations k is set to be $k = 1$.

II. Generating V-WVD Based Codebooks:

Step 1. Nearest neighborhood condition (NNC): The above partition in (22), a kind of farthest-point WVD, is adopted as a extension of NNC [25] to the maximum operation.

Step 2. Centroid condition (CC): The codebook $\mathcal{V}$ is updated in this step by optimizing each $\boldsymbol{v}_{(k),\mathrm{L},i}$. For a partition $\mathcal{R}_{(k),i}, 1 \leqslant i \leqslant N$, the new codeword vector satisfies

$$\boldsymbol{v}_{(k),\mathrm{L},i} = \arg \max_{\|\boldsymbol{v}_\mathrm{L}\|=1} \left\{ \mathrm{E}\left[\frac{\boldsymbol{v}_\mathrm{L}^\mathrm{H} \boldsymbol{A} \boldsymbol{v}_\mathrm{L}}{\boldsymbol{v}_\mathrm{L}^\mathrm{H} \boldsymbol{C} \boldsymbol{v}_\mathrm{L}} \right] \middle| \widehat{\boldsymbol{h}}_\mathrm{L}^\mathrm{H} \in \mathcal{R}_{(k),i}\left(\mathcal{W}_{(k-1)}\right) \right\}. \tag{24}$$

The centroid condition exploited above is to estimate optimal vectors constrained by the "hidden" variable $\boldsymbol{G}$ obeying a certain distribution. This can be solved by the Expectation Maximization (EM) method proposed in [26]. In particular, we want to maximize the function expectation on the channel samples which follows a certain unknown distribution. We can construct a lower-bound to the expectation operation, whereas the CC step optimizes the bound, thereby improving the estimate for vectors located in the certain distribution space.

Proposition 3. To determine the corresponding suboptimal codeword vector within each space partition, we derive a lower bound of the function $\mathrm{E}\left[\frac{\boldsymbol{v}_\mathrm{L}^\mathrm{H} \boldsymbol{A} \boldsymbol{v}_\mathrm{L}}{\boldsymbol{v}_\mathrm{L}^\mathrm{H} \boldsymbol{C} \boldsymbol{v}_\mathrm{L}}\right]$ on the variables of channel vectors located in the partition as the following:

$$\mathrm{E}\left[\frac{\boldsymbol{v}_\mathrm{L}^\mathrm{H} \boldsymbol{A} \boldsymbol{v}_\mathrm{L}}{\boldsymbol{v}_\mathrm{L}^\mathrm{H} \boldsymbol{C} \boldsymbol{v}_\mathrm{L}} \right] \geqslant \frac{\boldsymbol{v}_\mathrm{L}^\mathrm{H} \boldsymbol{A}_* \boldsymbol{v}_\mathrm{L}}{\boldsymbol{v}_\mathrm{L}^\mathrm{H} \boldsymbol{B}_* \boldsymbol{v}_\mathrm{L}}, \tag{25}$$

where $\boldsymbol{B}_* = \boldsymbol{I}_{N_\mathrm{T}} + \mathrm{E}\left(\gamma_\mathrm{E} \boldsymbol{G}^\mathrm{H} \boldsymbol{\Sigma}_\mathrm{E}^\mathrm{H} \boldsymbol{\Sigma}_\mathrm{E} \boldsymbol{G}\right)$ and $\boldsymbol{A}_* = \mathrm{E}\left[\frac{\boldsymbol{I}_{N_\mathrm{T}} + \gamma_\mathrm{L} \boldsymbol{G}^\mathrm{H} \boldsymbol{\Sigma}_\mathrm{L}^\mathrm{H} \boldsymbol{\Sigma}_\mathrm{L} \boldsymbol{G}}{\left(1+\gamma_\mathrm{L} \boldsymbol{\Sigma}_\mathrm{L} \boldsymbol{G} \boldsymbol{G}^\mathrm{H} \boldsymbol{\Sigma}_\mathrm{L}^\mathrm{H}\right)}\right]$.

Proof. We define $m = \boldsymbol{v}_\mathrm{L}^\mathrm{H} \frac{\boldsymbol{I} + \gamma_\mathrm{L} \boldsymbol{G}^\mathrm{H} \boldsymbol{\Sigma}_\mathrm{L}^\mathrm{H} \boldsymbol{\Sigma}_\mathrm{L} \boldsymbol{G}}{\left(1+\gamma_\mathrm{L} \boldsymbol{\Sigma}_\mathrm{L} \boldsymbol{G} \boldsymbol{G}^\mathrm{H} \boldsymbol{\Sigma}_\mathrm{L}^\mathrm{H}\right)} \boldsymbol{v}_\mathrm{L}$ and $z = \gamma_\mathrm{E} \boldsymbol{v}_\mathrm{L}^\mathrm{H} \boldsymbol{G}^\mathrm{H} \boldsymbol{\Sigma}_\mathrm{E}^\mathrm{H} \boldsymbol{\Sigma}_\mathrm{E} \boldsymbol{G} \boldsymbol{v}_\mathrm{L}$, then the expectation item in (24) will be transformed into $\mathrm{E}_{m,z}(\frac{m}{1+z})$. The variable m and z can respectively be transformed into $m = \frac{1+\gamma_\mathrm{L} \|\boldsymbol{G}^\mathrm{H} \boldsymbol{\Sigma}_\mathrm{L}^\mathrm{H}\|^2 \beta_2}{\left(1+\gamma_\mathrm{L} \boldsymbol{\Sigma}_\mathrm{L} \boldsymbol{G} \boldsymbol{G}^\mathrm{H} \boldsymbol{\Sigma}_\mathrm{L}^\mathrm{H}\right)}$ and $z = \gamma_\mathrm{E} \|\boldsymbol{G}^\mathrm{H} \boldsymbol{\Sigma}_\mathrm{E}^\mathrm{H}\|^2 \beta_1$. For an arbitrary channel model $\boldsymbol{h}$ satisfying $\boldsymbol{h} \sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{I}_{N_\mathrm{T}})$, the channel amplitude $\|\boldsymbol{h}\|$ is independent of the channel direction $\boldsymbol{h}/\|\boldsymbol{h}\|$. Thus $\left\|\boldsymbol{G}^\mathrm{H} \boldsymbol{\Sigma}_\mathrm{L}^\mathrm{H}\right\|^2, \beta_2$ are mutual independent while $\left\|\boldsymbol{G}^\mathrm{H} \boldsymbol{\Sigma}_\mathrm{E}^\mathrm{H}\right\|^2, \beta_1$ are also mutual independent. Then we can obtain that $\left\|\boldsymbol{G}^\mathrm{H} \boldsymbol{\Sigma}_\mathrm{L}^\mathrm{H}\right\|^2, \left\|\boldsymbol{G}^\mathrm{H} \boldsymbol{\Sigma}_\mathrm{E}^\mathrm{H}\right\|^2, \beta_1, \beta_2$ are mutual independent, which means that the variable m is independent of the variable z. Therefore, we have

$$\mathrm{E}\left[\frac{\boldsymbol{v}_\mathrm{L}^\mathrm{H} \boldsymbol{A} \boldsymbol{v}_\mathrm{L}}{\boldsymbol{v}_\mathrm{L}^\mathrm{H} \boldsymbol{C} \boldsymbol{v}_\mathrm{L}} \right] = \mathrm{E}_{m,z}\left(\frac{m}{1+z} \right) \overset{\text{(b)}}{\geqslant} \mathrm{E}_m\left(\frac{m}{1+\mathrm{E}\left(z\right)} \right) = \frac{\boldsymbol{v}_\mathrm{L}^\mathrm{H} \mathrm{E}[\frac{\boldsymbol{I}_{N_\mathrm{T}} + \gamma_\mathrm{L} \boldsymbol{G}^\mathrm{H} \boldsymbol{\Sigma}_\mathrm{L}^\mathrm{H} \boldsymbol{\Sigma}_\mathrm{L} \boldsymbol{G}}{\left(1+\gamma_\mathrm{L} \boldsymbol{\Sigma}_\mathrm{L} \boldsymbol{G} \boldsymbol{G}^\mathrm{H} \boldsymbol{\Sigma}_\mathrm{L}^\mathrm{H}\right)}] \boldsymbol{v}_\mathrm{L}}{\boldsymbol{v}_\mathrm{L}^\mathrm{H} [\boldsymbol{I}_{N_\mathrm{T}} + \gamma_\mathrm{E} \mathrm{E}(\boldsymbol{\Sigma}_\mathrm{L} \boldsymbol{G} \boldsymbol{G}^\mathrm{H} \boldsymbol{\Sigma}_\mathrm{E}^\mathrm{H})] \boldsymbol{v}_\mathrm{L}}. \tag{26}$$

(b) is obtained according to Jensen's inequality for the convex function. The proof is then completed.

The lower bound can be interpreted as a worst and practical case where the eavesdropper has higher SNR level than the legitimate user or the case where the generated codebook has high resolution N. Then, we simplify (24) as the following:

$$\boldsymbol{v}_{(k),\mathrm{L},i} = \arg \min_{\|\boldsymbol{v}_\mathrm{L}\|=1} \left(\frac{\boldsymbol{v}_\mathrm{L}^\mathrm{H} \boldsymbol{B}_* \boldsymbol{v}_\mathrm{L}}{\boldsymbol{v}_\mathrm{L}^\mathrm{H} \boldsymbol{A}_* \boldsymbol{v}_\mathrm{L}} \middle| \widehat{\boldsymbol{h}}_\mathrm{L}^\mathrm{H} \in \mathcal{R}_{(k),i}\left(\mathcal{W}_{(k-1)}\right) \right). \tag{27}$$

We use GEVD (Generalized Eigenvalue Decomposition) to solve the above minimization problem and obtain the suboptimal codeword vector in kth iteration as follows:

$$\boldsymbol{v}_{(k),\mathrm{L},i} = \varphi_{\max}\left(\boldsymbol{B}_*, \boldsymbol{A}_*\right), \quad i = 1, \ldots, N. \tag{28}$$

Remark 4. The rayleigh entropy as shown in (27) guarantees the algorithm has a monotonic convergence property. Moreover, during the implementation of the algorithm, the statistical matrix $\boldsymbol{B}_*$ and $\boldsymbol{A}_*$ can be estimated with an experimental expectation from the training channel vectors belonging to $\mathcal{R}_{(k),i}$.

Step 3. Updating codebook and weight: Codebook $\mathcal{V}_{(k-1)}$ is updated by substituting codeword vectors in (28) for those in the previous iteration process. Moreover, updating the weight set is performed as $\mathcal{W}_{(k-1)} = \mathcal{W}_{(k)}$ after obtaining new weights $w_{(k),i},\ i = 1, \ldots, N$.

The above three procedures are iterated until the convergence.

3.2.5 *Codeword selection mechanism*

Since the legitimate user can only know its own perfect CSI, the suitable selection of codeword vector for the legitimate user is defined below: $\boldsymbol{v}_{\mathrm{L}}^{\mathrm{opt}} = \arg\max_{\boldsymbol{v}_{\mathrm{L},i}\in\mathcal{V}} \frac{1+\gamma_{\mathrm{L}}\boldsymbol{v}_{\mathrm{L},i}^{\mathrm{H}}\boldsymbol{G}^{\mathrm{H}}\boldsymbol{\Sigma}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{\Sigma}_{\mathrm{L}}\boldsymbol{G}\boldsymbol{v}_{\mathrm{L},i}}{1+\gamma_{\mathrm{L}}\boldsymbol{\Sigma}_{\mathrm{L}}\boldsymbol{G}\boldsymbol{G}^{\mathrm{H}}\boldsymbol{\Sigma}_{\mathrm{L}}^{\mathrm{H}}}$, where $\mathcal{V}$ is the V-WVD based codebook obtained in the previous subsection. The strategy suggests that a legitimate user should pay more attention to its channel direction in high-SNR and high-resolution situation when there exists an eavesdropper.

3.3 Secrecy-quantization loss analysis for codebook generation

In this subsection, we give the analytical expressions for the upper bound of QES. Take the QCF model with RRH n for example. According to (17), we firstly obtain

$$\mathrm{E}\left\{\log_2\left[\frac{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{C}\boldsymbol{v}_{\mathrm{L}}}{\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\boldsymbol{A}\boldsymbol{v}_{\mathrm{L}}}\right]\right\} = \mathrm{E}_{\|\boldsymbol{g}_{k,n}\|^2,\beta_1}\left\{\log_2\left(1+\gamma_{\mathrm{E}}\|\boldsymbol{g}_{k,n}\|^2\beta_1\right)\right\} + \mathrm{E}_{\|\boldsymbol{h}_{k,n}\|^2,\beta_2}\left\{\log_2\frac{1+\gamma_{\mathrm{L}}\|\boldsymbol{h}_{k,n}\|^2}{1+\gamma_{\mathrm{L}}\|\boldsymbol{h}_{k,n}\|^2\beta_2}\right\}, \quad (29)$$

where $\beta_1=\left|\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\frac{\boldsymbol{g}_{k,n}^{\mathrm{H}}}{\|\boldsymbol{g}_{\mathrm{k,n}}\|}\right|^2$ and $\beta_2=\left|\boldsymbol{v}_{\mathrm{L}}^{\mathrm{H}}\frac{\boldsymbol{h}_{k,n}^{\mathrm{H}}}{\|\boldsymbol{h}_{k,n}\|}\right|^2$. To further give a theoretical expression of (29), we adopt the Voronoi region approximation method [17] to characterise the pdf of β_1 and β_2 in which an approximate pdf yielding a performance upper bound can be achieved. Specifically, the statistical characterization of β_2 can be given as [17]

$$f_{\beta_2}(x) = 2^B(N_{\mathrm{T}}-1)(1-x)^{N_{\mathrm{T}}-2}, \quad \zeta < x < 1, \quad (30)$$

where $\zeta = 1-2^{-B/(N_{\mathrm{T}}-1)}$. β_2 denotes the level of similarity between the selected codeword vector and the channel vector of the legitimate user. However, due to the randomness of the eavesdropper's channel, it is a difficult task to evaluate β_1 which represents the level of similarity between the selected codeword vector and the eavesdropper's channel vector. We consider two cases as shown in Figure 2 (c) and (d): the desirable case where β_1 has the same pdf as $1-\beta_2$ and the undesirable case in which β_1 has the same pdf as β_2. The two cases are defined for better measuring the ability of codebook to compel eavesdropper's channel direction vector to stay far away from the selected codeword vector. The former shows that the eavesdropper's channel vector is located in the region of quantization cell of the orthogonal vector of the selected codeword vector for the legitimate user and the latter demonstrates that the eavesdropper's channel vector is located in the quantization cell of the selected codeword vector. It is noted that only one of two cases is encountered in one channel realization. However, for the ergodic channel realizations, two cases may alternately appear, thus incurring difficult performance analysis. As two extreme examples, only the desirable or undesirable case occurs during overall channel realizations, which produces two kinds of upper bound of QES. Two corresponding analytical integral-form expressions are shown in (31), (32) and (33), respectively.

$$R_{\mathrm{upper,undesirable}}^{\mathrm{QES}} = 2^B(N_{\mathrm{T}}-1)\log_2\mathrm{e}\sum_{j=0}^{N_{\mathrm{T}}-1}\gamma_{\mathrm{E}}^{-j}\int_{\zeta}^{1}(1-x)^{N_{\mathrm{T}}-2}x^{-j}\mathrm{e}^{1/(\gamma_{\mathrm{E}}x)}\Gamma\left(-j,\frac{1}{\gamma_{\mathrm{E}}x}\right)\mathrm{d}x+\eta, \quad (31)$$

$$R_{\mathrm{upper,desirable}}^{\mathrm{QES}} = 2^B(N_{\mathrm{T}}-1)\log_2\mathrm{e}\sum_{j=0}^{N_{\mathrm{T}}-1}\gamma_{\mathrm{E}}^{-j}\int_{0}^{1-\zeta}x^{N_{\mathrm{T}}-j-2}\mathrm{e}^{1/(\gamma_{\mathrm{E}}x)}\Gamma\left(-j,\frac{1}{\gamma_{\mathrm{E}}x}\right)\mathrm{d}x+\eta, \quad (32)$$

$$\eta = \frac{(N_{\mathrm{T}}-1)}{\ln 2}\sum_{k=1}^{\infty}\frac{2^{-Bk/(N_{\mathrm{T}}-1)}}{k(k+N_{\mathrm{T}}-1)}\frac{\Gamma(k+N_{\mathrm{T}})}{\Gamma(N_{\mathrm{T}})}\gamma_{\mathrm{L}}^{k}{}_2F_0(k+N_{\mathrm{T}},k;;-\gamma_{\mathrm{L}}). \quad (33)$$

4 Simulation results

In this section, we simulate the performance of the proposed codebook framework in QCF model and describe the emulation when it is extended to the C-RAN scenario in which ILLL and ILLE are more

Table 1 Simulation configuration for applying V-WVD based codebooks to C-RAN systems

Parameter	Value
Path-loss model $L\left(d_{k,n}\right)$	$148.1+37.6\log 10(d_{k,n})$ (dB)
Standard deviation of log-norm shadowing $s_{k,n}$	8 dB
Noise power (10 MHz bandwidth)	-102 dBm
Maximum transmission power of each RRH	25 dBm
Power gain of transmission antennas $\psi_{k,n}$	9 dBi
Number of transmission antennas N_{T}	4
Covering radius R of C-RAN	2 km
Distribution of RRHs and users	uniform distribution
Scheduling algorithm and transmission strategy	JDCUS, CB [15]
Number of RRHs in each RRH cluster	2

prevalent. To give the specific simulation configuration, we firstly classify the required configurations as two categories: codebook training configuration, codebook application configuration.

Codebook training configuration. In this configuration, we consider the conventional codebooks as the initial codebooks, including Grassmannian codebook, random vector quantization (RVQ) codebook and discrete fourier transform (DFT) codebook. For simplicity, they are respectively denoted as codebook I, II and III. To improve the secrecy rate with low feedback overheads, the size of codebooks $N = 2^B$ is configured with $B = 4$ for every codebook. The number of transmit antennas N_{T} is set to 4. During each codebook realization, the SNR of legitimate user is assumed to be identical with that of the eavesdropper.

Codebook application configuration. For the QCF model, in Figure 3 (a)–(d) and Figure 4(a), we let $\gamma_{\mathrm{E}} = \gamma_{\mathrm{L}}$, while we let $\gamma_{\mathrm{E}} \neq \gamma_{\mathrm{L}}$ in Figure 4(b) to verify that our codebooks generated at $\gamma_{\mathrm{E}} = \gamma_{\mathrm{L}}$ have robust performance with no information of SNR at the eavesdropper. The SNR differences between the legitimate users and eavesdroppers can further reflect the unpredictability of interference level in C-RAN. The large-scale fading factors are given as $\beta_{k,n}, \alpha_{k,n} \sim \{10^{-L(d_{k,n})/20}\sqrt{\psi_{k,n}s_{k,n}}, \forall k, n\}$, and the related parameters are defined in Table 1. In general, multiple drops should be simulated due to the inevitable effect of the large-scale fading. Therefore, our simulation runs consist of 100 user and RRH drops, during each of which K users and M RRHs are respectively dropped into a circular region with radius R. During each drop, we further perform 1000 independent Rayleigh fading channel realizations to calculate average sum-rate.

4.1 Advantages of V-WVD framework in QCF model

In this subsection, we compare the numerical results of both V-WVD based codebooks and conventional codebooks in the respect of average secrecy rate and transmission rate.

In Figure 3(a), we compare the convergence of the codebook generation under V-WVD framework with $T = 10000$ channel samples. Based on (27), we define the measure for the kth iteration as follows:

$$S\left(\boldsymbol{v}_{(k),\mathrm{L}}\right) = \frac{1}{T}\sum_{i=1}^{N}\sum_{j=1}^{\left|R_{(k),i}\right|}\frac{\boldsymbol{v}_{(k-1),\mathrm{L},i}^{\mathrm{H}}\boldsymbol{B}_{*}\left(\boldsymbol{G}_{j}\right)\boldsymbol{v}_{(k-1),\mathrm{L},i}}{\boldsymbol{v}_{(k-1),\mathrm{L},i}^{\mathrm{H}}\boldsymbol{A}_{*}\left(\boldsymbol{G}_{j}\right)\boldsymbol{v}_{(k-1),\mathrm{L},i}}.$$

The iteration is terminated when $\{S(\boldsymbol{v}_{(k-1),\mathrm{L}}) - S(\boldsymbol{v}_{(k),\mathrm{L}})\}/S(\boldsymbol{v}_{(k),\mathrm{L}}) \leqslant 0.0005$. Obviously, the algorithm converges in fewer than 50 iterations, verifying the convergence property of V-WVD based codebooks.

Average secrecy rate gain. Figure 3 (b) and (c) compare the average secrecy rates of various codebooks. Observe that V-WVD based codebooks can bring higher average secrecy-rate gains compared with all the corresponding conventional codebooks. The reason is that codeword vectors in V-WVD based codebooks, relatively to that in conventional codebooks, can reshape the transmitted beams and direct them into a suitable region with higher average secrecy rate gain. We respectively plot the analytical curves of the QES upper bounds and the simulated curve of the ergodic secrecy rate loss in Figure 3(d).

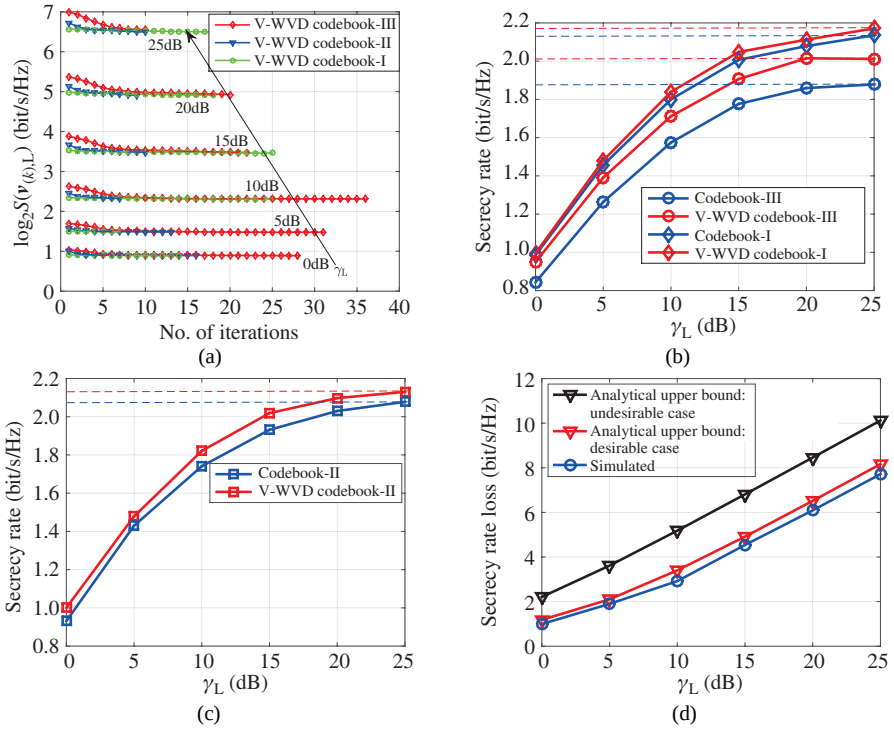

Figure 3 (Color online) Performance comparison between V-WVD based codebooks and conventional codebooks. (a) Convergence history of the V-WVD based codebook generation algorithm under different $\gamma_{\rm L}$; (b) and (c) secrecy rate versus $\gamma_{\rm L}$ for various V-WVD based codebooks; (d) two upper bounds of QES versus $\gamma_{\rm L}$ and simulated ergodic secrecy rate loss.

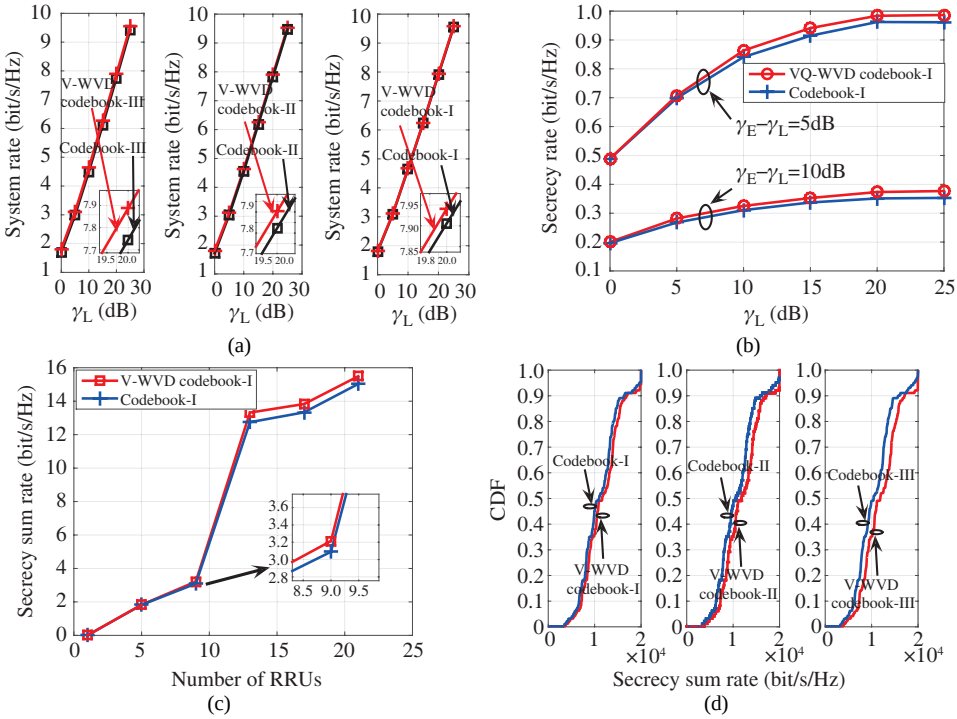

Figure 4 (Color online) Performance comparison between V-WVD based codebooks and conventional codebooks, respectively in QCF model and C-RAN. (a) Transmission rate versus $\gamma_{\rm L}$ even with no eavesdropping in QCF model; (b) secrecy rate versus $\gamma_{\rm L}$ under different $\gamma_{\rm E}$ in QCF model; (c) secrecy sum-rate versus the number of RRHs in C-RAN; (d) cumulative distribution function of secrecy sum-rate in C-RAN.

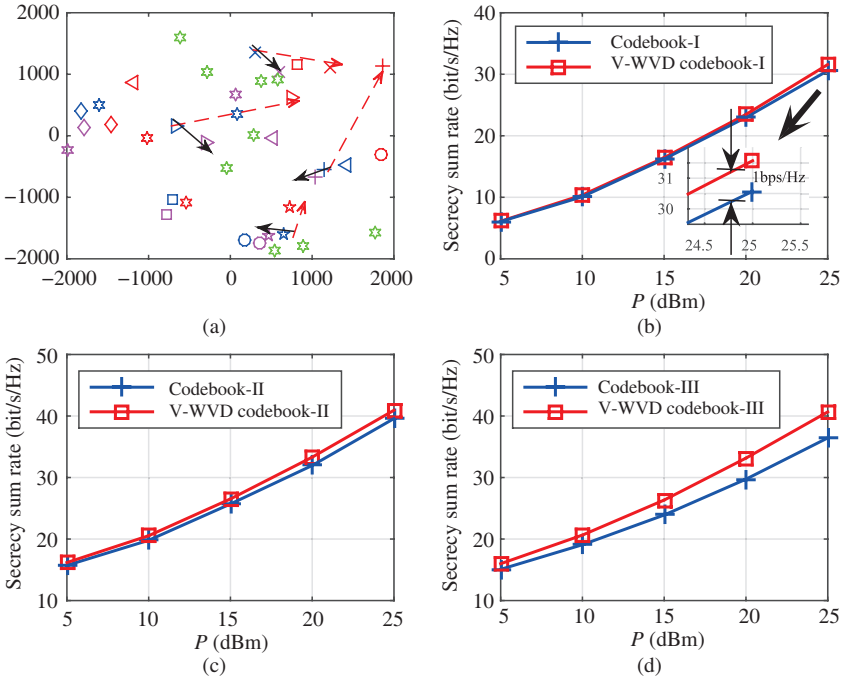

Figure 5 (Color online) Performance of proposed codebooks in C-RAN deployment I. (a) Topological graph for communication nodes; (b) secrecy sum-rate of codebook I versus transmit power; (c) secrecy sum-rate of codebook II versus transmit power; (d) secrecy sum-rate of codebook III versus transmit power.

Obviously, the analytical upper bound curve in the desirable case is closer to the simulated ergodic secrecy rate loss than that in the undesirable case. This phenomenon verifies that the desirable case is more likely encountered in the use of V-WVD based codebooks. That is to say, codewords in V-WVD based codebooks can better position the eavesdropper's channel vector to be around the quantization cell created by the orthogonal vector of a codeword vector, if being suitably selected by the legitimate user, which can be shown in Figure 2 (c) and (d).

Average beamforming gain. Figure 4(a) shows the performance of V-WVD based codebooks in scenes without considering security. It is remarkable that this example determines whether the transceiver pair needs the secrecy leakage detection for judging which codebook deserves being employed: V-WVD based codebooks or conventional codebooks. As we expect, V-WVD codebooks perform a bit better than the corresponding conventional codebooks. The simulation results verify our analysis in Proposition 2.

Figure 4(b) shows the robust performance of V-WVD based codebooks which are generated under $\gamma_{\mathrm{E}} = \gamma_{\mathrm{L}}$. Its superiority over conventional codebooks is maintained well during the information transmission even though γ_{E} is 10 dB higher than γ_{L}. This result is reasonable because the matching degree between channel vectors and codeword vectors have more influence on the ergodic rate loss than the discrepancy of magnitude within a certain range, e.g. 10 dB-difference in SNR. This results coincides with the related conclusion in Subsection 3.2.5.

4.2 Advantages of V-WVD framework in C-RAN

In this subsection, we compare the performance of V-WVD based codebooks with that of conventional codebooks in C-RAN systems. The performance includes two aspects: secrecy sum-rate gain, beamforming gain or sum-rate gain.

Figure 4(c) shows the secrecy sum-rate gains of different quantization codebooks versus the number of RRHs at $P_{\mathrm{s}} = 20$ mdB. The number of RRHs are respectively given as 1, 5, 9, 13, 17, 21, while the selected user are correspondingly restricted to 1, 3, 5, 10, 10, 10. As we can see, the secrecy sum-rate increases with the number of RRHs in all codebooks. Moreover, the V-WVD based Grassmannian codebook induces better gains compared with Grassmannian codebook, about 0.5 bit/s/Hz at $M = 21$.

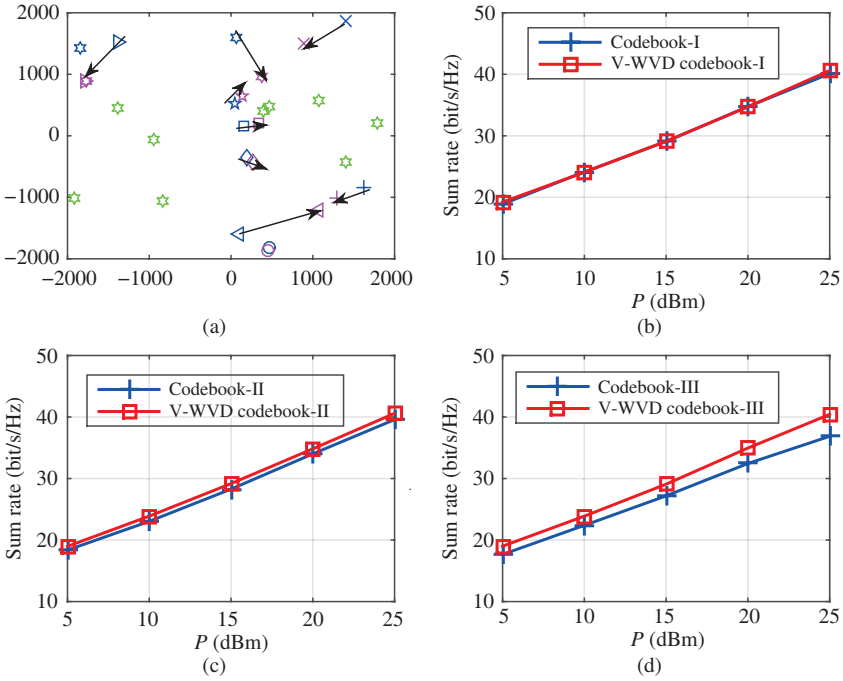

Figure 6 (Color online) Performance of proposed codebooks in C-RAN deployment II. (a) Topological graph for communication nodes; (b) sum rate of codebook I versus transmit power; (c) sum rate of codebook II versus transmit power; (d) sum rate of codebook III versus transmit power.

Figure 4(d) shows the CDF of secrecy sum-rate under 100 simulation drops with $P_{\mathrm{s}} = 25$ mdB and $M = 19$. The number of selected users is up to 10. As we can see, the V-WVD based Grassmannian codebook brings better gains compared with Grassmannian codebook.

Figure 5 describes the secrecy sum-rate versus the transmission power. The topological graph reflects the distribution of the users, eavesdroppers and RRHs in one drop. In this sense, the secrecy sum-rate is a kind of average rate under this topological graph. Specifically, the blue, mauve, red and green nodes respectively represent the active of scheduled RRHs, legitimate users, eavesdroppers and sleeping RRHs. Each eavesdropper only overhears one anchor RRH of interest in the simulation no matter how the clustering is performed. As shown in the figure, all of V-WVD BASED codebooks obtain the secrecy sumrate gains which is respectively 1, 1.5 and 4 bit/s/Hz at SNR = 25 dB.

Figure 6 presents how V-WVD based framework can bring beamforming gains than conventional codebooks in the uncertain environment with varied large-scale fading and interference. It is shown that two curves that respectively denote V-WVD based Grassmannian codebook and Grassmannian codebook almost coincide. As to the RVQ and DFT codebooks, the sumrate gain brought by V-WVD framework is visible in which the former has 1 bit/s/Hz gain and the latter has 3.6 bit/s/Hz gain respectively at SNR = 25 dB. This is because novel codebooks can effectively reduce the information leakage and improve the beamforming gain even under the unpredicted information leakage for each user. This result accords with what is shown in Figure 4(b).

5 Conclusion

In this paper, we proposed a novel quantization codebook framework to improve the physical layer security of C-RAN system from the aspect of channel acquirement. By simplifying the C-RAN systems under the eavesdropping environment, we redesigned security-oriented quantization codebooks effectively and accommodated them with C-RAN systems. It is shown that beamforming gains and secrecy rate gains can be both obtained in the proposed framework, with no extra feedback overheads and no increase in the number of antennas from the point of view of ergodic rate. This framework can get rid of the burden

of leakage detection techniques for secrecy information in the physical layer and does not increase the overheads on virtualization of C-RAN while improving the performance needed.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 61431011), National High-Tech R&D Program of China (863) (Grant No. 2014AA01A707), National Science and Technology Major Project (Grant No. 2016ZX03001016-005), and Fundamental Research Funds for the Central Universities.

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Blenk A, Basta A, Reisslein M, et al. Virtualization: survey on network virtualization hypervisors for software defined networking. IEEE Commun Surv Tut, 2016, 18: 655–685
2 Liang C C, Yu F R. Wireless network virtualization: a survey, some research issues and challenges. IEEE Commun Surv Tut, 2015, 17: 358–380
3 Arslan M Y, Sundaresan K, Rangarajan S. Software-defined networking in cellular radio access networks: potential and challenges. IEEE Commun Mag, 2015, 53: 150–156
4 Xu D Y, Ren P Y, Du Q H, et al. Hybrid secure beamforming and vehicle selection using hierarchical agglomerative clustering for C-RAN-based vehicle-to-infrastructure communications in vehicular cyber-physical systems. Int J Distrib Sens Netw, 2016, 12, doi: 10.1177/1550147716662783
5 Checko A, Christiansen H L, Yan Y, et al. Cloud RAN for mobile networks—a technology overview. IEEE Commun Surv Tut, 2015, 17: 405–426
6 Peng M G, Wang C G, Lau, V, et al. Fronthaul-constrained cloud radio access networks: insights and challenges. IEEE Wirel Commun, 2015, 22: 152–160
7 Chen M, Qian Y F, Mao S W, et al. Software-defined mobile networks security. Mob Netw Appl, 2016, 21: 729–743
8 Mukherjee A, Fakoorian S A A, Huang J, et al. Principles of physical layer security in multiuser wireless networks: a survey. IEEE Commun Surv Tut, 2014, 16: 1550–1573
9 You J, Zhong Z D, Wang G P, et al. Security and reliability performance analysis for cloud radio access networks with channel estimation errors. IEEE Access, 2014, 2: 1348–1358
10 Diffie W, Hellman M. New directions in cryptography. IEEE Trans Inform Theory, 1976, 22: 644–654
11 Wyner A D. The wire-tap channel. Bell Syst Tech J, 1975, 54: 1355–1387
12 Khisti A, Wornell G W. Secure transmission with multiple antennas I: the MISOME wiretap channel. IEEE Trans Inform Theory, 2010, 56: 3088–3104
13 Bashar S, Ding Z, Li G Y. On secrecy of codebook-based transmission beamforming under receiver limited feedback. IEEE Trans Wirel Commun, 2011, 10: 1212–1223
14 Lin C H, Tsai S H, Lin Y P. On quantization for masked beamforming secrecy systems. IEEE Trans Wirel Commun, 2015, 14: 5618–5628
15 Xu D Y, Ren P Y, Du Q H, et al. Joint dynamic clustering and user scheduling for downlink cloud radio access network with limited feedback. China Commun, 2015, 12: 147–159
16 Xu D Y, Du Q H, Ren P Y, et al. AF-based CSI feedback for user selection in multi-user MIMO systems. In: Proceedings of IEEE Global Communications Conference (GLOBECOM), San Diego, 2015. 1–6
17 Yoo T, Jindal N, Goldsmith A. Multi-antenna downlink channels with limited feedback and user selection. IEEE J Sel Areas Commun, 2007, 25: 1478–1491
18 Aurenhammer F. Voronoi diagrams—a survey of a fundamental geometric data structure. ACM Comput Surv, 1991, 23: 345–405
19 Krikidis I, Ottersten B. Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling. IEEE Signal Process Lett, 2013, 20: 141–144
20 Zhou X Y, Ganti R K, Andrews J G. Secure wireless network connectivity with multi-antenna transmission. IEEE Trans Wirel Commun, 2011, 10: 425–430
21 Geraci G, Singh S, Andrews J G, et al. Secrecy rates in broadcast channels with confidential messages and external eavesdroppers. IEEE Trans Wirel Commun, 2014, 13: 2931–2943
22 Love D J, Heath R W, Strohmer T. Grassmannian beamforming for multiple-input multiple-output wireless systems. IEEE Trans Inform Theory, 2003, 49: 2735–2747
23 Cohen J E, Friedland S, Kato T, et al. Eigenvalue inequalities for products of matrix exponentials. Linear Algebra Appl, 1982, 45: 55–95
24 Johnson C R, Bru R. The spectral radius of a product of nonnegative matrices. Linear Algebra Appl, 1990, 141: 227–240
25 Roh J C, Rao B D. Transmit beamforming in multiple-antenna systems with finite rate feedback: a VQ-based approach. IEEE Trans Inform Theory, 2006, 52: 1101–1112
26 Moon T K. The expectation-maximlization algorithm. IEEE Signal Process Mag, 1996, 13: 47–60