Fronthaul Quantization as Artificial Noise for Enhanced Secret Communication in C-RAN

[1]Seok-Hwan Park, [2]Osvaldo Simeone and [3]Shlomo Shamai (Shitz)
[1]Division of Electronic Engineering, Chonbuk National University, Jeonju-si, Jeollabuk-do, 54896 Korea
[2]CWiP, New Jersey Institute of Technology, 07102 Newark, New Jersey, USA
[3]Department of Electrical Engineering, Technion, Haifa, 32000, Israel
Email: seokhwan@jbnu.ac.kr, osvaldo.simeone@njit.edu, sshlomo@ee.technion.ac.il

***Abstract*—This work considers the downlink of a cloud radio access network (C-RAN), in which a control unit (CU) encodes confidential messages, each of which is intended for a user equipment (UE) and is to be kept secret from all the other UEs. As per the C-RAN architecture, the encoded baseband signals are quantized and compressed prior to the transfer to distributed radio units (RUs) that are connected to the CU via finite-capacity fronthaul links. This work argues that the quantization noise introduced by fronthaul quantization can be leveraged to act as "artificial" noise in order to enhance the rates achievable under secrecy constraints. To this end, it is proposed to control the statistics of the quantization noise by applying multivariate, or joint, fronthaul quantization/compression at the CU across all outgoing fronthaul links. Assuming wiretap coding, the problem of jointly optimizing the precoding and multivariate compression strategies, along with the covariance matrices of artificial noise signals generated by RUs, is formulated with the goal of maximizing the weighted sum of achievable secrecy rates while satisfying per-RU fronthaul capacity and power constraints. After showing that the artificial noise covariance matrices can be set to zero without loss of optimaliy, an iterative optimization algorithm is derived based on the concave convex procedure (CCCP), and some numerical results are provided to highlight the advantages of leveraging quantization noise as artificial noise.**

***Index Terms*—C-RAN, physical-layer security, fronthaul quantization, beamforming.**

I. INTRODUCTION

Motivated by the original works on the wiretap channel [1][2], physical-layer security techniques have been extensively studied as effective means of protecting data secrecy for communications over wireless channels in a variety of scenarios [3][4]. One of the key techniques that have been devised for enhancing the rates at which information can be transmitted securely is the addition of artificial noise at the transmitter [5]-[10]. This strategy finds its theoretical justification in the prefix channel approach that was shown in [2] to achieve the secrecy capacity of a general wiretap channel.

In this work, we study physical-layer secure communication in the context of the downlink of cloud radio access networks (C-RANs). In a C-RAN, a control unit (CU) performs joint encoding of the messages intended for all the user equipments (UEs) located in the geographical area covered by the radio units (RUs) connected to the CU. The encoded baseband signals are then transferred to the RUs on the fronthaul link in analog or digital format. For digital fronthauling, the CU quantizes and compresses the encoded baseband signals prior to the transfer to the RUs due to the limited bit rate of the fronthaul links [11][12].

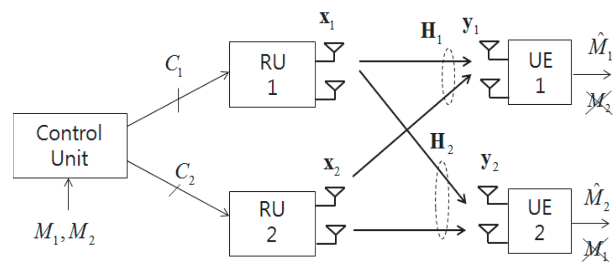

Figure 1. Illustration of the downlink of a C-RAN system with confidential messages for $N_R = 2$ RUs, $N_U = 2$ UEs, $n_{R,i} = 2$ RU antennas and $n_{U,k} = 2$ UE antennas.

In this work, we argue that the quantization noise introduced by fronthaul quantization can be leveraged to act as artificial noise in order to enhance the rates achievable under secrecy constraints. To this end, as an extension of the work [11], we propose to apply multivariate, or joint, fronthaul quantization/compression [13] at the CU for all outgoing fronthaul links in order to control the statistics of the quantization noise. Multivariate quantization/compression was recently shown in [11] to improve the performance of C-RANs without secrecy constraints with respect to standard per-fronthaul link point-to-point quantization/compression.

In the rest of this paper, we first formulate the problem of jointly optimizing precoding, multivariate compression and the covariance matrices of artificial noise signals generated by RUs, with the goal of maximizing the weighted sum of achievable secrecy rates of the intended UEs subject to per-RU fronthaul capacity and power constraints (Sec. III). We show that the artificial noise covariance matrices can be set to zero with no loss of optimality and hence focus on the joint optimization of precoding and multivariate compression.

The work of S.-H. Park was supported by the NRF Korea funded by the Ministry of Science, ICT & Future Planning (MSIP) through grant 2015R1C1A1A01051825. The work of O. Simeone was partially supported by the U.S. NSF through grant 1525629. The work of S. Shamai has been supported by the European Union's Horizon 2020 Research And Innovation Programme, grant agreement no. 694630.

An iterative optimization algorithm is then derived based on the concave convex procedure (CCCP) (Sec. III), and numerical evidence is provided to highlight the advantages of the proposed schemes (Sec. IV).

II. System Model

We consider the downlink of a C-RAN in which a single CU controls N_R RUs. The CU communicates with the ith RU through a fronthaul link of capacity C_i bits/s/Hz where the normalization is with respect to the downlink bandwidth. The N_R RUs transmit signals to N_U UEs located in the union of the coverage areas of the RUs. We define the sets $\mathcal{N}_R \triangleq \{1, \ldots, N_R\}$ and $\mathcal{N}_U \triangleq \{1, \ldots, N_U\}$ of the RUs and the UEs, and denote the numbers of antennas of RU i and UE k as $n_{R,i}$ and $n_{U,k}$, respectively. An illustration is shown in Fig. 1.

The signal $\mathbf{y}_k \in \mathbb{C}^{n_{U,k}\times 1}$ received by UE k is given by

$$\mathbf{y}_k = \sum_{i\in\mathcal{N}_R} \mathbf{H}_{k,i}\mathbf{x}_i + \mathbf{z}_k, \tag{1}$$

where $\mathbf{H}_{k,i} \in \mathbb{C}^{n_{U,k}\times n_{R,i}}$ represents the channel response matrix from RU i to UE k; $\mathbf{x}_i \in \mathbb{C}^{n_{R,i}\times 1}$ indicates the signal transmitted by RU i; and $\mathbf{z}_k \in \mathbb{C}^{n_{U,k}\times 1}$ is the additive noise at UE k distributed as $\mathbf{z}_k \sim \mathcal{CN}(\mathbf{0}, \mathbf{\Sigma}_{\mathbf{z}_k})$. Each RU i is subject to the power constraint $\mathbb{E}\left\|\mathbf{x}_i\right\|^2 \leq P_i$.

The information messages $M_k \in \{1, \ldots, 2^{nR_k}\}$, each of rate R_k bits/s/Hz, are encoded within a block of n channel uses, where n is large enough to justify the use of information-theoretic limits. The message M_k is intended for UE $k \in \mathcal{N}_U$ and is required to be kept secret from the other UEs. Specifically, we impose that the UEs $l \in \mathcal{N}_U \setminus \{k\}$ be unable to decode the message M_k even in the worst-case scenario where they cooperate since the CU cannot control the activities of the UEs (see [1]). The messages $\{M_k\}_{k\in\mathcal{N}_U}$ are processed by the CU in the two steps described in the following subsections before being transferred to the RUs.

A. Linear Precoding

The CU first encodes each message M_k using a wiretap code [1] and obtaining an encoded signal $\mathbf{s}_k \in \mathbb{C}^{d_k\times 1}$, which is distributed as $\mathbf{s}_k \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$. We assume that the number d_k of data streams satisfies the condition $d_k \leq \min\{n_R, n_{U,k}\}$ with the notation $n_R \triangleq \sum_{i\in\mathcal{N}_R} n_{R,i}$. In order to enable the management of the inter-UE interference and to enhance secrecy, the CU performs linear precoding, or beamforming, with a precoding matrix $\mathbf{A} \in \mathbb{C}^{n_R\times d}$, yielding the precoded signal $\tilde{\mathbf{x}} = [\tilde{\mathbf{x}}_1; \ldots; \tilde{\mathbf{x}}_{N_R}] \in \mathbb{C}^{n_R\times 1}$ with

$$\tilde{\mathbf{x}} = \mathbf{A}\mathbf{s}, \tag{2}$$

where $\tilde{\mathbf{x}}_i \in \mathbb{C}^{n_{R,i}\times 1}$ is the signal to be communicated to RU i; $\mathbf{s} \triangleq [\mathbf{s}_1; \ldots; \mathbf{s}_{N_U}]$ is the vector of the signals encoded for the UEs; and we have defined the notation $d \triangleq \sum_{k\in\mathcal{N}_U} d_k$. We note that the discussion can be easily extended to systems, in which the CU performs non-linear secrecy dirty-paper coding (S-DPC) precoding proposed in [10].

B. Fronthaul Compression

The precoded baseband signal $\tilde{\mathbf{x}}_i$ needs to be compressed prior to transmission to the RU, since the CU communicates to RU i through a fronthaul link of capacity C_i bits/s/Hz. Using standard rate-distortion considerations, we model the impact of compression by adding a quantization noise $\mathbf{q}_i$ to the compression input signal $\tilde{\mathbf{x}}_i$ so that the compression output signal $\hat{\mathbf{x}}_i$ is given as

$$\hat{\mathbf{x}}_i = \tilde{\mathbf{x}}_i + \mathbf{q}_i, \tag{3}$$

where the quantization noise $\mathbf{q}_i$ is independent of the signal $\tilde{\mathbf{x}}_i$ and is distributed as $\mathbf{q}_i \sim \mathcal{CN}(\mathbf{0}, \mathbf{\Omega}_{i,i})$. Each RU i decompresses the baseband signal $\hat{\mathbf{x}}_i$ based on the bit stream received on the fronthaul link. We emphasize that, as done in, e.g., [11], quantization is not designed so as to minimize the (e.g., quadratic) distortion between the precoded signals $\tilde{\mathbf{x}}_i$ and the compressed signals $\hat{\mathbf{x}}_i$, but rather with the aim of maximizing the weighted sum of achievable secrecy rates, which will be defined in Sec. II-D.

In the standard point-to-point compression approach [14], in which the precoded signals $\tilde{\mathbf{x}}_i$ and $\tilde{\mathbf{x}}_j$ for different RUs $i \neq j$ are separately compressed, the quantization noises $\mathbf{q}_i$ and $\mathbf{q}_j$ are independent, i.e., $\mathbf{\Omega}_{i,j} = \mathbf{0}$ for $i \neq j$. Instead, multivariate, or joint, compression [13, Ch. 9] allows the CU to correlate the quantization noises $\mathbf{q}_1, \ldots, \mathbf{q}_{N_R}$ by jointly compressing the signals $\tilde{\mathbf{x}}_1, \ldots, \tilde{\mathbf{x}}_{N_R}$. This adds a further degree of freedom to the system design, which will be leveraged here to enhance physical-layer security. It was shown in [11, Sec. IV-D] that multivariate compression can be implemented with no loss of optimality using a low-complexity sequential processing architecture.

Specifically, in this work, we propose to shape the quantization noise signals in order to enhance the secrecy performance by controlling the correlation matrix $\mathbf{\Omega}$ of the quantization noise vector $\mathbf{q} \triangleq [\mathbf{q}_1; \ldots; \mathbf{q}_{N_R}]$, where the covariance matrix $\mathbf{\Omega} \triangleq \mathbb{E}[\mathbf{q}\mathbf{q}^\dagger]$ is given as a block matrix whose (i,j)th block is $\mathbf{\Omega}_{i,j} \triangleq \mathbb{E}[\mathbf{q}_i\mathbf{q}_j^\dagger]$. As mentioned, this control can be realized by means of multivariate compression, which was recently demonstrated in [11] to achieve performance gains in terms of non-secrecy information rates.

It is a classic result in network information theory that the quantized signals (3) with the given quantization noise covariance $\mathbf{\Omega}$ can be recovered by the RUs if the conditions

$$\begin{aligned} g_{\mathcal{S}}(\mathbf{A}, \mathbf{\Omega}) &\triangleq \sum_{i\in\mathcal{S}} h(\mathbf{x}_i) - h(\hat{\mathbf{x}}_{\mathcal{S}}|\tilde{\mathbf{x}}) \\ &= \sum_{i\in\mathcal{S}} \log_2\det\left(\mathbf{E}_i^\dagger(\mathbf{A}\mathbf{A}^\dagger + \mathbf{\Omega})\mathbf{E}_i\right) \\ &\quad - \log_2\det\left(\mathbf{E}_{\mathcal{S}}^\dagger\mathbf{\Omega}\mathbf{E}_{\mathcal{S}}\right) \leq \sum_{i\in\mathcal{S}} C_i \end{aligned} \tag{4}$$

are satisfied for all subsets $\mathcal{S} \subseteq \mathcal{N}_R$, where we have defined the set $\hat{\mathbf{x}}_{\mathcal{S}} \triangleq \{\hat{\mathbf{x}}_i\}_{i\in\mathcal{S}}$ and the matrix $\mathbf{E}_{\mathcal{S}}$ obtained by stacking the matrices $\mathbf{E}_i$ for $i \in \mathcal{S}$ horizontally with the matrices $\mathbf{E}_i \in \mathbb{C}^{n_R\times n_{R,i}}$ having all-zero elements except for the rows from

$(\sum_{j=1}^{i-1} n_{R,j}+1)$ to $(\sum_{j=1}^{i} n_{R,j})$ being the identity matrix of size $n_{R,i}$ [13, Ch. 9].

C. Artificial Noise

Based on the decompressed baseband signal $\hat{\mathbf{x}}_i$, each RU i creates the signal $\mathbf{x}_i$ to be transmitted in the downlink as

$$\mathbf{x}_i = \hat{\mathbf{x}}_i + \mathbf{n}_i, \tag{5}$$

where $\mathbf{n}_i$ represents the artificial noise signal generated by RU i and is distributed as $\mathbf{n}_i \sim \mathcal{CN}(\mathbf{0}, \mathbf{\Phi}_i)$. The artificial noise signals $\mathbf{n}_i$ are independent across the index i since each signal $\mathbf{n}_i$ is locally produced by the corresponding RU. As for the quantization noise signal $\mathbf{q}_i$, we need to carefully design the covariance matrix $\mathbf{\Phi}_i$ based on the channel matrices in order to enhance secrecy.

D. Achievable Secrecy Rates

The signal $\mathbf{y}_k$ in (1) received by UE k can be written as

$$\mathbf{y}_k = \mathbf{H}_k\mathbf{A}_k\mathbf{s}_k + \sum_{l\in\mathcal{N}_U\setminus\{k\}} \mathbf{H}_k\mathbf{A}_l\mathbf{s}_l + \mathbf{H}_k(\mathbf{q}+\mathbf{n}) + \mathbf{z}_k, \tag{6}$$

where we defined the channel matrix $\mathbf{H}_k \triangleq [\mathbf{H}_{k,1} \ldots \mathbf{H}_{k,N_R}]$ from all the RUs to UE k, the aggregate vector $\mathbf{n} \triangleq [\mathbf{n}_1; \ldots; \mathbf{n}_{N_R}]$ of the artificial noise signals and the submatrix $\mathbf{A}_k \in \mathbb{C}^{n_R\times d_k}$ of $\mathbf{A}$ multiplied to the signal $\mathbf{s}_k$ encoded for UE k. The first term in (6) indicates the desired signal to be decoded by the receiving UE k, the second term represents the inter-UE interference signals, which encode the unintended messages, and the third and last terms are channelized quantization noise and antenna additive noise signals, respectively. Eq. (6) suggests that a joint design of $\mathbf{A}$ and $\mathbf{\Omega}$ has the potential to jointly "shape" the useful signals and the quantization noise signals to enhance the secrecy rate.

Assuming that each UE k decodes the message M_k based on the signal $\mathbf{y}_k$ in (6) while treating the interference signals as noise, it was shown in [1] that the rate

$$R_k = [f_k(\mathbf{A}, \mathbf{\Omega}, \mathbf{\Phi})]^+ \tag{7}$$

is achievable for UE k ensuring that the other UEs cannot decode the message M_k, where we defined the function

$$\begin{aligned} f_k(\mathbf{A}, \mathbf{\Omega}, \mathbf{\Phi}) &\triangleq I(\mathbf{s}_k; \mathbf{y}_k) - I(\mathbf{s}_k; \mathbf{y}_{\bar{k}}) \qquad (8)\\ &= \phi\left(\mathbf{H}_k\mathbf{R}_l\mathbf{H}_k^\dagger, \sum_{l\in\mathcal{N}_U\setminus\{k\}} \mathbf{H}_k\mathbf{R}_l\mathbf{H}_k^\dagger + \mathbf{H}_k(\mathbf{\Omega}+\mathbf{\Phi})\mathbf{H}_k^\dagger + \mathbf{\Sigma}_{\mathbf{z}_k}\right) \\ &- \phi\left(\mathbf{H}_{\bar{k}}\mathbf{R}_k\mathbf{H}_{\bar{k}}^\dagger, \sum_{l\in\mathcal{N}_U\setminus\{k\}} \mathbf{H}_{\bar{k}}\mathbf{R}_l\mathbf{H}_{\bar{k}}^\dagger + \mathbf{H}_{\bar{k}}(\mathbf{\Omega}+\mathbf{\Phi})\mathbf{H}_{\bar{k}}^\dagger + \mathbf{\Sigma}_{\mathbf{z}_{\bar{k}}}\right), \end{aligned}$$

with the functions $\phi(\mathbf{A}, \mathbf{B}) \triangleq \log_2\det(\mathbf{A}+\mathbf{B}) - \log_2\det(\mathbf{B})$ and $[x]^+ = \max(0, x)$ and the notations $\mathbf{\Phi} \triangleq \mathrm{diag}(\{\mathbf{\Phi}_i\}_{i\in\mathcal{N}_R})$ and $\mathbf{R}_k \triangleq \mathbf{A}_k\mathbf{A}_k^\dagger$. The vector $\mathbf{y}_{\bar{k}}$, defined as

$$\mathbf{y}_{\bar{k}} \triangleq [\mathbf{y}_1; \ldots; \mathbf{y}_{k-1}; \mathbf{y}_{k+1}; \ldots; \mathbf{y}_{N_U}] = \mathbf{H}_{\bar{k}}\mathbf{x} + \mathbf{z}_{\bar{k}}, \tag{9}$$

represents the vector obtained by stacking the signals $\mathbf{y}_l$ received by the malicious UEs $l \in \mathcal{N}_U \setminus \{k\}$, where we have defined the notations $\mathbf{H}_{\bar{k}} \triangleq [\mathbf{H}_1^\dagger \ldots \mathbf{H}_{k-1}^\dagger \mathbf{H}_{k+1}^\dagger \ldots \mathbf{H}_{N_U}^\dagger]^\dagger$ and $\mathbf{z}_{\bar{k}} \triangleq [\mathbf{z}_1^\dagger \ldots \mathbf{z}_{k-1}^\dagger \mathbf{z}_{k+1}^\dagger \ldots \mathbf{z}_{N_U}^\dagger]^\dagger$. The maximization of the secrecy sum-rate over the quantization noise covariance matrix $\mathbf{\Omega}$ entails that the rate loss induced by the quantization noise is minimized at the intended UE while it is maximized at the unintended UEs.

III. Problem Definition and Optimization

We aim at optimizing the precoding matrix $\mathbf{A}$, the quantization noise covariance matrix $\mathbf{\Omega}$ and the artificial noise covariance matrix $\mathbf{\Phi}$ with the goal of maximizing the weighted sum of secrecy rates subject to the per-RU power and the fronthaul capacity constraints. The problem is stated as

$$\begin{aligned} \underset{\mathbf{A}, \{\mathbf{\Omega},\mathbf{\Phi}\succeq\mathbf{0}\}}{\text{maximize}} \; & \sum_{k\in\mathcal{N}_U} w_k [f_k(\mathbf{A}, \mathbf{\Omega}, \mathbf{\Phi})]^+ && (10a)\\ \text{s.t. } & g_{\mathcal{S}}(\mathbf{A}, \mathbf{\Omega}) \le \sum_{i\in\mathcal{S}} C_i, \text{ for all } \mathcal{S} \subseteq \mathcal{N}_R, && (10b)\\ & \mathrm{tr}\left(\mathbf{E}_i^\dagger\mathbf{A}\mathbf{A}^\dagger\mathbf{E}_i + \mathbf{\Omega}_{i,i} + \mathbf{\Phi}_i\right) \\ & \quad \le P_i, \text{ for all } i \in \mathcal{N}_R. && (10c) \end{aligned}$$

The following lemma shows that we can reduce the optimization domain without loss of optimality.

Lemma 1. *Setting $\mathbf{\Phi} = \mathbf{0}$ in the problem (10), which corresponds to adding no artificial noise at the RUs, does not cause any loss of optimality.*

Proof. Suppose that an optimal solution $(\mathbf{A}^*, \mathbf{\Omega}^*, \mathbf{\Phi}^*)$ exists with $\mathbf{\Omega}^* \neq \mathbf{0}$. We can then define another solution given by $(\mathbf{A}^*, \mathbf{\Omega}^* + \mathbf{\Phi}^*, \mathbf{0})$ that achieves exactly the same objective (10a) without violating any of the constraints. This is because the left-hand side of the fronthaul capacity constraint (4) is non-increasing with respect to the covariance matrix $\mathbf{\Omega}$, that is, adding quantization noise can only alleviate the fronthaul overhead and hence any artificial noise added by the RUs can be directly added to the quantization noise without loss of optimality. □

From Lem. 1, we set $\mathbf{\Phi} = \mathbf{0}$ without loss of optimality. However, it is still not easy to solve the problem (10) due to the non-smoothness (and non-convexity) of the objective function. In order to make the problem more tractable, we propose to solve an alternative problem obtained by replacing the objective function with a smooth function

$$\sum_{k\in\mathcal{N}_U} w_k f_k(\mathbf{A}, \mathbf{\Omega}), \tag{11}$$

where we remove the dependence on the covariance $\mathbf{\Phi} = \mathbf{0}$. Then, solving the obtained problem with respect to the variables $\mathbf{R} \triangleq \{\mathbf{R}_k\}_{k\in\mathcal{N}_U}$ and $\mathbf{\Omega}$ is a difference-of-convex (DC) program, and we can adopt an iterative algorithm based on the CCCP as in [11]. The detailed algorithm is described in Algorithm I, where we defined the functions $\tilde{f}_k(\{\mathbf{R}^{(t+1)},\mathbf{\Omega}^{(t+1)}\},\{\mathbf{R}^{(t)},\mathbf{\Omega}^{(t)}\})$ and $\tilde{g}_{\mathcal{S}}(\{\mathbf{R}^{(t+1)},\mathbf{\Omega}^{(t+1)}\},\{\mathbf{R}^{(t)},\mathbf{\Omega}^{(t)}\})$ as

$$\begin{aligned}
&\tilde{f}_k\left(\{\mathbf{R}^{(t+1)},\mathbf{\Omega}^{(t+1)}\},\{\mathbf{R}^{(t)},\mathbf{\Omega}^{(t)}\}\right) \qquad (12)\\
&\triangleq \log_2\det\left(\sum_{l\in\mathcal{N}_U}\mathbf{H}_k\mathbf{R}_l^{(t+1)}\mathbf{H}_k^\dagger+\mathbf{H}_k\mathbf{\Omega}^{(t+1)}\mathbf{H}_k^\dagger+\mathbf{\Sigma}_{\mathbf{z}_k}\right)\\
&-\log_2\det\left(\sum_{l\in\mathcal{N}_U\setminus\{k\}}\mathbf{H}_k\mathbf{R}_l^{(t)}\mathbf{H}_k^\dagger+\mathbf{H}_k\mathbf{\Omega}^{(t)}\mathbf{H}_k^\dagger+\mathbf{\Sigma}_{\mathbf{z}_k}\right)\\
&-\log_2\det\left(\sum_{l\in\mathcal{N}_U}\mathbf{H}_{\bar{k}}\mathbf{R}_l^{(t)}\mathbf{H}_{\bar{k}}^\dagger+\mathbf{H}_{\bar{k}}\mathbf{\Omega}^{(t)}\mathbf{H}_{\bar{k}}^\dagger+\mathbf{\Sigma}_{\mathbf{z}_{\bar{k}}}\right)\\
&+\log_2\det\left(\sum_{l\in\mathcal{N}_U\setminus\{k\}}\mathbf{H}_{\bar{k}}\mathbf{R}_l^{(t+1)}\mathbf{H}_{\bar{k}}^\dagger+\mathbf{H}_{\bar{k}}\mathbf{\Omega}^{(t+1)}\mathbf{H}_{\bar{k}}^\dagger+\mathbf{\Sigma}_{\mathbf{z}_{\bar{k}}}\right)\\
&-\varphi\left(\begin{array}{c}\sum_{l\in\mathcal{N}_U\setminus\{k\}}\mathbf{H}_k\mathbf{R}_l^{(t+1)}\mathbf{H}_k^\dagger+\mathbf{H}_k\mathbf{\Omega}^{(t+1)}\mathbf{H}_k^\dagger+\mathbf{\Sigma}_{\mathbf{z}_k},\\ \sum_{l\in\mathcal{N}_U\setminus\{k\}}\mathbf{H}_k\mathbf{R}_l^{(t)}\mathbf{H}_k^\dagger+\mathbf{H}_k\mathbf{\Omega}^{(t)}\mathbf{H}_k^\dagger+\mathbf{\Sigma}_{\mathbf{z}_k}\end{array}\right)\\
&-\varphi\left(\begin{array}{c}\sum_{l\in\mathcal{N}_U}\mathbf{H}_{\bar{k}}\mathbf{R}_l^{(t+1)}\mathbf{H}_{\bar{k}}^\dagger+\mathbf{H}_{\bar{k}}\mathbf{\Omega}^{(t+1)}\mathbf{H}_{\bar{k}}^\dagger+\mathbf{\Sigma}_{\mathbf{z}_{\bar{k}}},\\ \sum_{l\in\mathcal{N}_U}\mathbf{H}_{\bar{k}}\mathbf{R}_l^{(t)}\mathbf{H}_{\bar{k}}^\dagger+\mathbf{H}_{\bar{k}}\mathbf{\Omega}^{(t)}\mathbf{H}_{\bar{k}}^\dagger+\mathbf{\Sigma}_{\mathbf{z}_{\bar{k}}}\end{array}\right),
\end{aligned}$$

and

$$\begin{aligned}
&\tilde{g}_{\mathcal{S}}\left(\{\mathbf{R}^{(t+1)},\mathbf{\Omega}^{(t+1)}\},\{\mathbf{R}^{(t)},\mathbf{\Omega}^{(t)}\}\right) \qquad (13)\\
&\triangleq\sum_{i\in\mathcal{S}}\log_2\det\left(\mathbf{E}_i^\dagger(\sum_{k\in\mathcal{N}_U}\mathbf{R}_k^{(t)}+\mathbf{\Omega}^{(t)})\mathbf{E}_i\right)\\
&\quad-\log_2\det\left(\mathbf{E}_{\mathcal{S}}^\dagger\mathbf{\Omega}^{(t+1)}\mathbf{E}_{\mathcal{S}}\right)\\
&\quad+\sum_{i\in\mathcal{S}}\varphi\left(\begin{array}{c}\sum_{k\in\mathcal{N}_U}\mathbf{E}_i^\dagger\mathbf{R}_k^{(t+1)}\mathbf{E}_i+\mathbf{E}_i^\dagger\mathbf{\Omega}^{(t+1)}\mathbf{E}_i,\\ \sum_{k\in\mathcal{N}_U}\mathbf{E}_i^\dagger\mathbf{R}_k^{(t)}\mathbf{E}_i+\mathbf{E}_i^\dagger\mathbf{\Omega}^{(t)}\mathbf{E}_i\end{array}\right)
\end{aligned}$$

with the definition $\varphi(\mathbf{X},\mathbf{Y})\triangleq\log\det(\mathbf{Y})+\mathrm{tr}(\mathbf{Y}^{-1}(\mathbf{X}-\mathbf{Y}))/\ln 2$.

After convergence of Algorithm 1, the actual precoding matrix $\mathbf{A}_k$ for UE k is obtained via rank reduction as $\mathbf{A}_k\leftarrow\mathbf{V}_k\mathbf{D}_k^{1/2}$, where $\mathbf{D}_k$ is a diagonal matrix whose diagonal elements are the d_k leading eigenvalues of $\mathbf{R}_k^{(t+1)}$ and the columns of $\mathbf{V}_k$ are the corresponding eigenvectors. This transformation from $\mathbf{R}_k^{(t+1)}$ to $\mathbf{A}_k$ may cause suboptimality (in terms of local optima) when the rank of the matrix $\mathbf{R}_k^{(t+1)}$ is larger than d_k. However, note that the obtained precoding matrices $\{\mathbf{A}_k\}_{k\in\mathcal{N}_U}$ together with $\mathbf{\Omega}^{(t+1)}$ are feasible in that they satisfy the conditions (10b) and (10c), since the matrices $\{\mathbf{R}_k^{(t+1)}\}_{k\in\mathcal{N}_U}$ satisfy (10b) and (10c) at each iteration. We also mention that, when the matrices $\mathbf{A}$ and $\mathbf{\Omega}$ are optimized upon as per problem (10), we necessarily have that $f_k(\mathbf{A},\mathbf{\Omega})\geq 0$. The reason is that it is always possible to obtain $f_k(\mathbf{A},\mathbf{\Omega})=0$ by setting $\mathbf{A}_k=\mathbf{0}$ in order to satisfy the constraints (10b) and (10c).

IV. Numerical Results

In this section, we present numerical results to validate the effectiveness of the proposed secure design based on multivariate compression. We compare four different strategies,

Algorithm 1 DC programming algorithm for problem (10)

1. Initialize the matrices $\mathbf{R}^{(1)}$ and $\mathbf{\Omega}^{(1)}$ to arbitrary feasible positive semidefinite matrices for problem (10) and set $t=1$.
2. Update the matrices $\mathbf{R}^{(t+1)}$ and $\mathbf{\Omega}^{(t+1)}$ as a solution of the convex problem

$$\begin{aligned}
&\underset{\mathbf{R}^{(t+1)},\mathbf{\Omega}^{(t+1)}\succeq\mathbf{0}}{\text{maximize}}\ \sum_{k\in\mathcal{N}_U}w_k\tilde{f}_k\left(\{\mathbf{R}^{(t+1)},\mathbf{\Omega}^{(t+1)}\},\{\mathbf{R}^{(t)},\mathbf{\Omega}^{(t)}\}\right)\\
&\quad\text{s.t. }\tilde{g}_{\mathcal{S}}\left(\{\mathbf{R}^{(t+1)},\mathbf{\Omega}^{(t+1)}\},\{\mathbf{R}^{(t)},\mathbf{\Omega}^{(t)}\}\right)\\
&\qquad\leq\sum_{i\in\mathcal{S}}C_i,\ \text{for all }\mathcal{S}\subseteq\mathcal{N}_R,\\
&\qquad\sum_{k\in\mathcal{N}_U}\mathrm{tr}\left(\mathbf{E}_i^\dagger\mathbf{R}_k^{(t+1)}\mathbf{E}_i\right)+\mathrm{tr}(\mathbf{\Omega}_{i,i}^{(t+1)})\\
&\qquad\leq P_i,\ \text{for all }i\in\mathcal{N}_R.
\end{aligned}$$

3. Stop if a convergence criterion is satisfied. Otherwise, set $t\leftarrow t+1$ and go back to Step 2.

i.e., non-secure and secure design based on point-to-point and multivariate fronthaul compression strategies. For the non-secure design, the problem (10) is tackled without taking into account the second term in (8) that represents the penalty for guaranteeing the security. The so-obtained precoding and quantization noise covariance matrices are then used in (7) to evaluate the secrecy sum-rate. Unless stated otherwise, we focus on evaluating the average secrecy sum-rate performance given in (10a). We assume that the locations of RUs and UEs are sampled from a uniform distribution within a square area of side length 500m, and the channel matrices $\mathbf{H}_{k,i}$ are modeled as $\mathbf{H}_{k,i}=\sqrt{\gamma_{k,i}}\mathbf{H}_{k,i}^w$, where the path-loss $\gamma_{k,i}$ is obtained as $\gamma_{k,i}=1/(1+(d_{k,i}/d_0)^\alpha)$ with α, $d_{k,i}$ and d_0 being the path-loss exponent, the distance between RU i and UE k and the reference distance, respectively, and the elements of the channel matrices $\mathbf{H}_{k,i}^w$ are independent and identically distributed (i.i.d.) as $\mathcal{CN}(0,1)$. We also assume that $P_i=P$, $C_i=C$ and $\mathbf{\Sigma}_{\mathbf{z}_k}=\mathbf{I}$ for all $i\in\mathcal{N}_R$ and $k\in\mathcal{N}_U$, and $\alpha=3$ and $d_0=50$m.

In Fig. 2, we plot the average secrecy sum-rate versus the transmission power P for the downlink of a C-RAN system with $N_R=2$, $N_U=3$, $n_{U,k}=1$ and $C=2$ bits/s/Hz. It is seen that the secure design significantly outperforms the non-secure design. Also, it is observed that multivariate compression yields a significant performance gain that is increasing with the transmission power P. This is because the impact of the quantization noise $\mathbf{H}_k\mathbf{q}$ in (6) compared to the additive noise $\mathbf{z}_k$ is more significant when the SNR is large at the UE side. It is noted that the secrecy sum-rate of the secure design saturates to a finite level at high-SNR, since, in this regime, the performance is limited by the power of the quantization noise that does not decrease with the SNR. Moreover, the performance of the non-secure design is degraded in the high-SNR regime due to the enhanced decodability of the messages of the unintended UEs. We also observe that, comparing the curves with $(n_{R,i},n_{U,k})=(1,1)$ and $(n_{R,i},n_{U,k})=(2,1)$

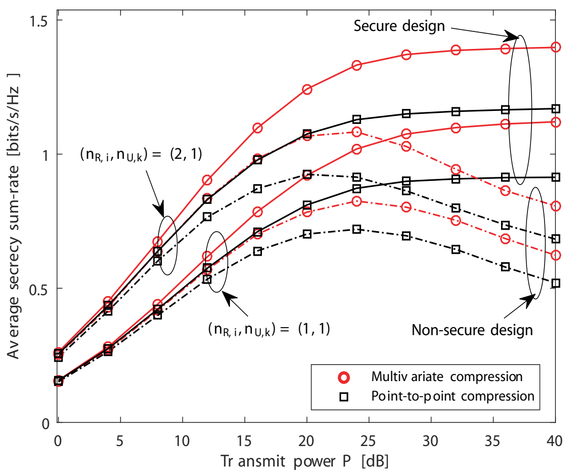

Figure 2. Average secrecy sum-rate versus the transmission power P for the downlink of a C-RAN with $N_R = 2$, $N_U = 3$, $n_{U,k} = 1$ and $C = 2$ bits/s/Hz.

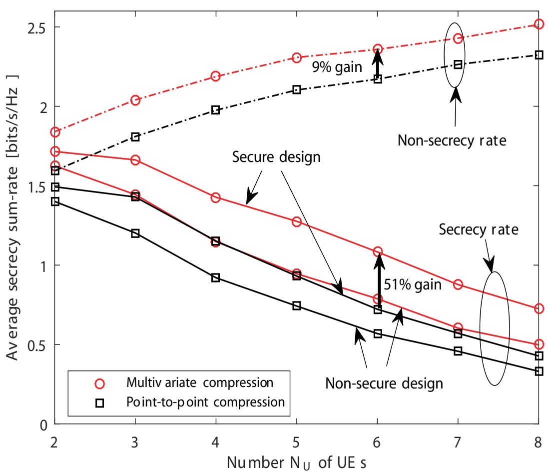

Figure 3. Average secrecy sum-rate and non-secrecy sum-rate versus the number N_U of UEs for the downlink of a C-RAN with $N_R = 3$, $n_{R,i} = n_{U,k} = 1$, $P = 20$ dB and $C = 1$ bits/s/Hz.

suggests that increasing the number of RU antennas results in improved performance since the additional excessive antennas can be leveraged to obtain beamforming gains.

Fig. 3 plots the average secrecy sum-rate, along with the standard "non-secrecy" sum-rate obtained without imposing secrecy constraints, versus the number N_U of UEs for the downlink of C-RAN with $N_R = 3$, $n_{R,i} = n_{U,k} = 1$, $P = 20$ dB and $C = 1$ bits/s/Hz. The "non-secrecy" rates are obtained by plugging the precoding and quantization noise covariance matrices of the non-secure design into the weighted sum $\sum_{k\in\mathcal{N}_U} w_k R'_k$ of rates $R'_k = I(\mathbf{s}_k; \mathbf{y}_k)$ that are achievable without secrecy constraints [11, Eq. (13)]. We observe that, unlike the non-secrecy rate, as the number N_U of UEs increases, the secrecy rate of all schemes becomes worse due to the increased number $N_U - 1$ of eavesdroppers on each message M_k. However, the proposed secure design based on multivariate compression provides a significant benefit in mitigating the impairments from the eavesdroppers compared to the other schemes. In particular, for $N_U = 6$, multivariate compression yields a 51% sum-rate gain under the secrecy constraint while about 9% is gained without secrecy constraint. This demonstrates the additional role of artificial noise that quantization noise shaping plays under secrecy constraint.

V. Conclusions

This work has proposed to leverage the quantization noise that is inevitably added by fronthaul compression in a C-RAN downlink as "artificial" noise for enhancing the rate achievable under secrecy constraints. To this end, we have investigated the application of multivariate fronthaul quantization/compression at the CU in order to control the statistics of the quantization noise across all the outgoing fronthaul links. We have formulated the joint optimization problem of the precoding and quantization noise covariance matrices for maximizing the weighted sum of secrecy rates of the UEs subject to the per-RU fronthaul capacity and power constraints. Numerical results were provided to verify the effectiveness of multivariate compression in enhancing secret communication.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell System Tech. Journ.*, vol. 54, pp. 1355-1387, 1975.

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339-348, May 1978.

[3] Y. Liang, H. V. Poor and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Comm. and Inf. Theory*, vol. 5, no. 4-5, pp. 355-580, Jun. 2009.

[4] M. Bloch and J. Barros, *Physical-layer security*, Cambridge University Press, Nov. 2011.

[5] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Comm.*, vol. 7, no. 6, pp. 2180-2189, Jun. 2008.

[6] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735-2751, Jun. 2008.

[7] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831-3842, Oct. 2010.

[8] W. Li, M. Ghogho, B. Chen and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Comm. Letters*, vol. 16, no. 10, pp. 1628-1631, Oct. 2012.

[9] T. Tsiligkaridis, "Secure MIMO communications under quantized channel feedback in the presence of jamming," *IEEE Trans. Sig. Processing*, vol. 62, no. 23, pp. 6265-6275, Dec. 2014.

[10] R. Liu, T. Liu, H. V. Poor and S. Shamai (Shitz), "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215-4227, Sep. 2010.

[11] S.-H. Park, O. Simeone, O. Sahin and S. Shamai (Shitz), "Joint precoding and multivariate backhaul compression for the downlink of cloud radio access networks," *IEEE Trans. Sig. Processing*, vol. 61, no. 22, pp. 5646-5658, Nov. 2013.

[12] O. Simeone, A. Maeder, M. Peng, O. Sahin and W. Yu, "Cloud radio access network: Virtualizing wireless access for dense heterogeneous systems," *Journ. Comm. Networks*, vol. 18, no. 2, pp. 135-149, Apr. 2016.

[13] A. E. Gamal and Y.-H. Kim, *Network information theory*, Cambridge University Press, 2011.

[14] O. Simeone, O. Somekh, H. V. Poor and S. Shamai (Shitz), "Downlink multicell processing with limited backhaul capacity," *EURASIP Journal on Advances in Signal Processing*, 2009.