Private Uplink Communication in C-RAN with Untrusted Radios

Omid Taghizadeh, *Member, IEEE*, Tianyu Yang, *Student Member, IEEE*, and Rudolf Mathar, *Senior Member, IEEE*

***Abstract*—In this work, we study the uplink (UL) of a cloud radio access network (C-RAN), where the central processing unit (CU) utilizes remote radio units (RU)s belonging to the same operator, i.e., the trusted RUs, as well as the RUs belonging to other operators or private owners, i.e., the untrusted RUs. In order to preserve information privacy against the untrusted RUs, the trusted RUs are enabled with full-duplex (FD) capability and transmit a jamming signal towards the exotic RUs, while receiving and forwarding UL signal to the CU. Note that the transmitted jamming signal degrades the decoding capability at the untrusted RUs, however, it can be later subtracted from the UL communication as it is apriori known by the CU. An optimization problem is then formulated to maximize the sum uplink private information rate by jointly designing the fronthaul compression, as well as the information and jamming transmission strategies. Due to the intractability of the resulting mathematical problem, an iterative solution is proposed with convergence to a point satisfying the Karush-Kuhn-Tucker (KKT) optimality conditions. Numerical simulations illustrate a notable gain obtained via the proposed sharing mechanism under the consideration of information privacy.**

***Keywords*—Information privacy, full-duplex, MIMO, C-RAN, physical layer security, friendly jamming.**

I. Introduction

Network and spectrum sharing have been introduced as effective methods to improve efficiency, flexibility, and to enable distributed ownership of the communication infrastructure [1], [2]. In particular, in a C-RAN where radio interface is relegated to distant RUs, usually with limited availability and fronthaul capacity, an efficient use of the available infrastructure is crucial. However, an inter-operator cooperation leads to an inherent loss of information privacy, if not properly controlled. In [3], a physical layer approach[1] is proposed for the downlink of a C-RAN system with untrusted RUs, and later extended for multi-operator system under privacy constraints [6] and with the joint inter-operator quantization approach in [7]. The idea is to utilize the downlink fronthaul quantization, jointly shaped at the CU for all RUs, as an artificially generated noise in order to reduce the decoding capability at the untrusted RUs. However, the proposed method may not be implemented in the UL to ensure information provacy against the untrusted RU nodes, due to the lack of quantization or transmit coordination in the UL user-RU communication.

In this paper, we propose a physical-layer privacy preserving method for the uplink of C-RANs, where RUs belonging to the same operator, i.e., the trusted RUs, as well as the RUs belonging to other operators, i.e., the untrusted RUs, can be utilized by the CU. This is in contrast to the works focusing on the information secrecy against untrusted third-party receivers, e.g., [8], the proposed privacy preserving methods for the downlink [3], [6], as well as the known cryptographic approaches reviewed in [4]. In particular, the untrusted RUs are viewed as potential eavesdropper nodes which constructively participate in the UL communication process. To facilitate this, the trusted RUs are enabled with full-duplex (FD) capability and transmit a jamming signal directed at the untrusted nodes [5]. Note that the jamming signal sent by the trusted RUs is a priori known to the CU, as they belong to the same operator. As a result, it and can be later estimated and subtracted from the UL communication at the CU, while degrading the decoding capability at the untrusted RUs. An optimization problem is then formulated to maximize the sum uplink private rate by jointly designing the quantization, as well as the information and jamming transmission strategies. Due to the intractability of the resulting mathematical problem, an iterative solution is proposed with convergence to a KKT solution. Numerical simulations illustrate a notable gain obtained via the proposed sharing mechanism, under the consideration of information privacy.

A. Mathematical Notation:

Column vectors and matrices are denoted as lower-case and upper-case bold letters, respectively. The trace, Hermitian transpose, and determinant of a matrix are respectively denoted by $\text{tr}(\cdot)$, $(\cdot)^H$, and $|\cdot|$, respectively. The Kronecker product is denoted by $\otimes$. $\lfloor \mathbf{A}_i \rfloor_{i\in\mathbb{F}}$ denotes a tall matrix, obtained by stacking the matrices $\mathbf{A}_i,\ i \in \mathbb{F}$. Similarly, $\langle \mathbf{A}_i \rangle_{i\in\mathbb{F}}$ constructs a block-diagonal matrix with the blocks $\mathbf{A}_i$. $\mathbb{E}\{\cdot\}$ denotes mathematical expectation. $\{a_k\}$ denotes the set of all values of $a_k, \forall k$. The set $\mathcal{A} \setminus \mathcal{B}$ includes all elements of $\mathcal{A}$, excluding those elements in $\mathcal{B}$. $\perp$ indicates statistical independence.

II. System Model

We consider the uplink of a C-RAN where a CU is connected to multiple-antenna users with the help of multiple RUs,

O. Taghizadeh is with the Network Information Theory Group (NetIT) and T. Yang is with the Communications and Information Theory Group (CommIT), TU Berlin, D-10587 Berlin, Germany. R. Mathar is with the Institute for Theoretical Information Technology (TI), RWTH Aachen University, Aachen, 52074, Germany. Main part of this research is conducted when all authors were with TI, RWTH Aachen University. This work has been supported by Deutsche Forschungsgemeinschaft (DFG), under the Grant No. MA 1184/38 − 1. (e-mail: {tianyu.yang, taghizadehmotlagh}@tu-berlin.de, mathar@ti.rwth-aachen.de).

[1] Unlike cryptographic approaches which rely on the limited computational power of the untrusted nodes, physical layer security employs an information theoretic approach, obtaining perfect secrecy [4], [5]. Moreover, it reduces the challenges regarding the distribution and management of secret keys, specially for systems with distributed architecture.

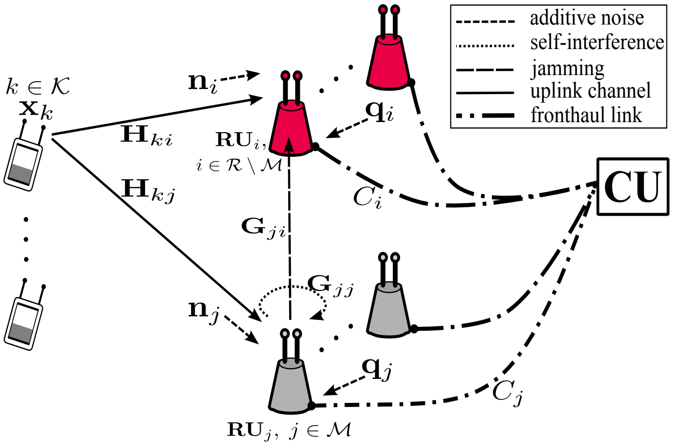

Fig. 1. The studied uplink C-RAN system where the untrusted (red) RUs participate in the communication process. RUs are connected to the CU via limited capacity fronthaul links. In order to provide information privacy the trusted RUs transmit jamming signal towards untrusted RUs, see Section II for details.

see Fig. 1. In particular, the system takes advantage of both the trusted RUs, which belong to the same operator and are capable of FD operation[2], as well as a set of untrusted RUs belonging to other operators or private owners. The index set of UL users, the trusted RUs, and all RUs are denoted as $\mathcal{K}, \mathcal{M}, \mathcal{R}$, respectively. The number of Tx (Rx) antennas at the RUs, and the Tx antennas at the UL users are respectively denoted as $N_{\text{R},m}$ ($M_{\text{R},m}$) and $N_{\text{U},k}$, $\forall k \in \mathcal{K}$ and $m \in \mathcal{R}$. Each RU is connected to the CU via a limited capacity fronthaul, i.e., $C_l, l \in \mathcal{R}$. The complex matrices $\mathbf{H}_{kl} \in \mathbb{C}^{M_{\text{R},l} \times N_{\text{U},k}}$ and $\mathbf{G}_{lm} \in \mathbb{C}^{M_{\text{R},m} \times N_{\text{R},l}}$, $k \in \mathcal{K}, l, m \in \mathcal{R}$, respectively denote the flat-fading user-RU and RU-RU channels.

The received signal at the RUs can be expressed as

$$\mathbf{y} = \mathbf{n} + \boldsymbol{\nu} + \sum_{k \in \mathcal{K}} \mathbf{H}_k \mathbf{x}_k, \tag{1}$$

where $\mathbf{x}_k \sim \mathcal{CN}(\mathbf{0}, \mathbf{X}_k)$, and $\mathbf{H}_k = \lfloor \mathbf{H}_{kl} \rfloor_{l \in \mathcal{R}}$ is the stacked uplink channel. Similarly, we use stacked signal notations $\mathbf{y} = \lfloor \mathbf{y}_l \rfloor_{l \in \mathcal{R}}$, $\boldsymbol{\nu} := \lfloor \boldsymbol{\nu}_l \rfloor_{l \in \mathcal{R}} \sim \mathcal{CN}(\mathbf{0}, \boldsymbol{\Psi})$ and $\mathbf{n} := \lfloor \mathbf{n}_l \rfloor_{l \in \mathcal{R}} \sim \mathcal{CN}(\mathbf{0}, \mathbf{N})$, where $\mathbf{n}_l$, $\boldsymbol{\nu}_l$ and $\mathbf{y}_l$ respectively represent the thermal noise, received self-jamming and the combined received signal at the l-th RU.

The quantized version of $\mathbf{y}$, i.e., $\mathbf{y}_{\text{q}} = \mathbf{y} + \mathbf{q}$, is then received at the CU, where $\mathbf{q} := \lfloor \mathbf{q}_l \rfloor_{l \in \mathcal{R}}$, such that $\mathbf{q}_l \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q}_l)$ is the quantization noise. The limited capacity constraint on the fronthaul links is hence imposed as

$$\log \left| \mathbf{S}_m \left(\mathbf{N} + \boldsymbol{\Psi} + \sum_{k \in \mathcal{K}} \mathbf{H}_k \mathbf{X}_k \mathbf{H}_k^H \right) \mathbf{S}_m^H + \mathbf{Q}_m \right| - \log |\mathbf{Q}_m| \leq C_m / B, \quad m \in \mathcal{R}, \tag{2}$$

where B is the bandwidth, and $\mathbf{S}_m$ is the selection matrix such that $\mathbf{y}_m = \mathbf{S}_m \mathbf{y}$, see [9, Eq. (1)]. The transmit power constraint at the UL users is expressed as

$$\operatorname{tr}(\mathbf{X}_k) \leq P_{\text{U},k}, \quad k \in \mathcal{K}. \tag{3}$$

A. Coordinated Jamming

Due to the SIC capability, the trusted FD-RUs may transmit friendly jamming signal $\mathbf{w} := \lfloor \mathbf{w}_m \rfloor_{m \in \mathcal{R}} \sim \mathcal{CN}(\mathbf{0}, \mathbf{W})$ while receiving UL information[3]. The received jamming covariance, including the impact of residual self-interference at the RUs is characterized as

$$\begin{aligned} &\boldsymbol{\nu} = \boldsymbol{\nu}_{\text{RR}} + \boldsymbol{\nu}_{\text{SI}}, \; \boldsymbol{\nu}_{\text{RR}} = \mathbf{G}_0 \mathbf{w}, \\ &\boldsymbol{\Psi} = \underbrace{\mathbf{G}_0 \mathbf{W} \mathbf{G}_0^H}_{\boldsymbol{\Psi}_{\text{RR}}} + \underbrace{\kappa \mathbf{G} \operatorname{diag}(\mathbf{W}) \mathbf{G}^H + \beta \operatorname{diag}\left(\mathbf{G} \mathbf{W} \mathbf{G}^H\right)}_{\boldsymbol{\Psi}_{\text{SI}}}, \end{aligned} \tag{4}$$

where $\mathbf{G} := \left(\lfloor (\lfloor \mathbf{G}_{ij} \rfloor_{j \in \mathcal{R}})^T \rfloor_{i \in \mathcal{R}} \right)^T$, and $\mathbf{G}_0$ is obtained similar to $\mathbf{G}$, but by replacing the matrices $\mathbf{G}_{ij}, i, j \in \mathcal{M}$ with zeroes[4]. In the above expression, $\boldsymbol{\nu}_{\text{RR}}$ ($\boldsymbol{\Psi}_{\text{RR}}$) indicates the inter-RU interference signal (covariance), whereas $\boldsymbol{\nu}_{\text{SI}}$ ($\boldsymbol{\Psi}_{\text{SI}}$) represents the residual self-interference signal (covariance), with $0 < \kappa, \beta \ll 1$ respectively denote the transmit and receive distortion coefficients, see [10, Section II]. The transmit power constraint at the RUs is consequently expressed as

$$\operatorname{tr}\left(\mathbf{S}_m \mathbf{W} \mathbf{S}_m^H\right) \leq P_{\text{R},m}, \quad m \in \mathcal{R}, \tag{5}$$

where $P_{\text{R},m} = 0, m \in \mathcal{R} \backslash \mathcal{M}$, in order to impose zero jamming transmission from the non FD RUs.

B. Uplink Sum Private Information Rate

Since CU is aware of the transmitted jamming signal and the corresponding channel information, an interference-reduced version of the received signal at the CU is obtained as

$$\begin{aligned} \tilde{\mathbf{y}}_{\text{q}} &= \mathbf{y} - \mathbf{G}_0 \mathbf{w} \\ &= \mathbf{H}_k \mathbf{x}_k + \underbrace{\mathbf{n} + \mathbf{q} + \boldsymbol{\nu}_{\text{SI}} + \sum_{j \in \mathcal{K} \backslash k} \mathbf{H}_j \mathbf{x}_j}_{=: \mathbf{i}_k} . \end{aligned}$$

By utilizing the Gaussian distribution as well as the statistical independence properties for all noise and signal elements, the achievable communication information rate for the k-th UL user to the CU is obtained as

$$\begin{aligned} R_k &= \log \left| \mathbf{I} + \mathbf{H}_k \mathbf{X}_k \mathbf{H}_k^H \left(\mathbb{E}\{\mathbf{i}_k \mathbf{i}_k^H\} \right)^{-1} \right| \\ &= \log \left| \sum_{j \in \mathcal{K}} \mathbf{H}_j \mathbf{X}_j \mathbf{H}_j^H + \mathbf{N} + \boldsymbol{\Psi}_{\text{SI}} + \mathbf{Q} \right| \\ &\quad - \log \left| \sum_{j \in \mathcal{K} \backslash k} \mathbf{H}_j \mathbf{X}_j \mathbf{H}_j^H + \mathbf{N} + \boldsymbol{\Psi}_{\text{SI}} + \mathbf{Q} \right|, \end{aligned} \tag{6}$$

[2] Due to self-interference cancellation capability, FD RUs can send jamming signal while receiving information [5].

[3] For notational simplicity, the jamming signal is defined for all trusted and untrusted RUs. However, the condition $\mathbf{w}_m = \mathbf{0}, \forall m \in \mathcal{R} \setminus \mathcal{M}$ is later enforced via (5).

[4] This follows from the fact that the CU, and by extension, the trusted RUs are aware of the transmitted jamming codebook, and the received jamming at the trusted RUs can be subtracted before it is sent to CU.

where $\mathbf{Q} = \langle \mathbf{Q}_m \rangle_{m\in\mathcal{R}}$. Moreover, the information leakage from the k-th uplink user to the m-th RU is obtained as

$$L_{km} = \log \left|\mathbf{S}_m \left(\mathbf{H}_k \mathbf{X}_k \mathbf{H}_k^H + \mathbf{N} + \mathbf{\Psi}\right) \mathbf{S}_m^H\right| \\ - \log \left|\mathbf{S}_m \left(\mathbf{\Psi} + \mathbf{N}\right) \mathbf{S}_m^H\right|, \quad (7)$$

provisioning a successive interference cancellation/subtraction capability at the untrusted RUs[5], representing the wost-case scenario [11]. Please note that unlike the CU where the inter-RU jamming signal could be subtracted, the received jamming signal will remain at the untrusted RU and prevent it from decoding the UL data. The achievable individual, and sum UL private information rates are hence formulated as [12]

$$R_{\text{prv},k} = \min_{m\in\mathcal{R}\setminus\mathcal{M}} \left\{R_k - L_{km}\right\}^+, \ R_{\text{sum}} = \sum_{k\in\mathcal{K}} R_{\text{prv},k}, \quad (8)$$

where R_{sum} indicates the total amount of information from all UL users that can be privately delivered to CU, i.e., without being decoded by the untrusted RUs. Please note that the positive operator $\{\}^+$ indicates that the secured information rate may not be negative, and it is lower-bounded by zero.

III. Joint Transmission and Compression Optimization

In this part, we seek optimized transmission and fronthaul quantization strategies, characterized by the covariance matrices $\{\mathbf{X}_k\}, \{\mathbf{Q}_k\}, \mathbf{W}$, in order to maximize R_{sum} under the operational system constraints. This is expressed as

$$\begin{aligned} \max_{\{\mathbf{X}_k\},\{\mathbf{Q}_m\},\mathbf{W}} \quad & R_{\text{sum}} && (12a) \\ \text{s.t.} \quad & (2), (3), (5), && (12b) \\ & \mathbf{X}_k, \mathbf{Q}_m, \mathbf{W} \succeq \mathbf{0}, \forall k\in\mathcal{K}, m\in\mathcal{R}. && (12c) \end{aligned}$$

Note that the above problem is intractable due to the non-differentiable and non-concave objective, as well as the non-convexity of the feasible set corresponding to (2). In order to transform the problem into a tractable form, firstly, we relax the non-smooth $\{\}^+$ operator[6], resulting in a smooth optimization problem. The epigraph form of the relaxed problem is formulated as

$$\begin{aligned} \max_{\{\gamma_k\},\{\zeta_k\},\mathcal{V}} \quad & \sum_{k\in\mathcal{K}} \zeta_k - \gamma_k && (13a) \\ \text{s.t.} \quad & (2), (3), (5), (12c), && (13b) \\ & \zeta_k \leq R_k, \ \ \gamma_k \geq L_{km}, \ \ \forall m \in \mathcal{R}\setminus\mathcal{M}, \ k\in\mathcal{K}, && (13c) \end{aligned}$$

where $\mathcal{V} := \{\{\mathbf{X}_k\}, \{\mathbf{Q}_m\}, \mathbf{W}\}$ and γ_k, ζ_k are auxiliary variables. The above problem is still intractable, due to the non-convex constraints (13c). However, it is amenable to the successive general inner approximation (GIA) framework [13], [14], due to the smooth difference-of-convex nature of R_k, L_{km}, as well as the fronthaul constraint (2). The idea is to implement an iterative update, where in each iteration a convex-approximate of the original problem (12) is solved. By applying the first-order Taylor approximation

$$\log|\mathbf{X}| \leq f\left(\mathbf{X}, \mathbf{Y}\right) := \log|\mathbf{Y}| + \text{tr}\left(\mathbf{Y}^{-1}\left(\mathbf{X}-\mathbf{Y}\right)\right)/\ln(2), \quad (14)$$

where $\ln(.)$ denotes the natural logarithm. The problem (12) is approximated in the i-th iteration as

$$\begin{aligned} \max_{\{\gamma_k^{[i]}\},\{\zeta_k^{[i]}\},\mathcal{V}^{[i]}} \quad & \sum_{k\in\mathcal{K}} \zeta_k - \gamma_k && (15a) \\ \text{s.t.} \quad & (3), (5), (12c), && (15b) \\ & \tilde{C}_m\left(\mathcal{V}^{[i]}, \mathcal{V}^{[i-1]}\right) \leq C_m, \ \forall m\in\mathcal{R}, && (15c) \\ & \zeta_k \leq \tilde{R}_k\left(\mathcal{V}^{[i]}, \mathcal{V}^{[i-1]}\right), \ \gamma_k \geq \tilde{L}_{km}\left(\mathcal{V}^{[i]}, \mathcal{V}^{[i-1]}\right), \\ & \qquad \forall m\in\mathcal{R}\setminus\mathcal{M}, \ k\in\mathcal{K}, && (15d) \end{aligned}$$

where the upper-index represents the iteration instance, and the approximations $\tilde{R}_k, \tilde{L}_{km}$ and $\tilde{C}_m$ are given in (9)-(11). The problem (15) is a convex optimization problem and can be solved via state of the art numerical solvers. In particular, the problem (15) can be efficiently implemented as an extended semi-definite-program via the MAX-DET algorithm [15]. The sequence of subproblems (15) are solved until a stable point is achieved. The detailed procedure is given in Algorithm 1.

A. Convergence

The Algorithm 1 converges to a solution satisfying the KKT optimality conditions. In order to observe this, we recall that (14) is obtained as the Taylor's approximation on a smooth concave function. As a result, it satisfies the properties: *i)* $\log\left(\mathbf{X}\right) = f\left(\mathbf{X}, \mathbf{X}\right)$, *ii)* $\log\left(\mathbf{X}\right) \leq f\left(\mathbf{X}, \mathbf{Y}\right), \ \ \forall \mathbf{Y}$, and *iii)* $\partial \log\left(\mathbf{X}\right)/\partial\mathbf{X} = \partial f\left(\mathbf{X}, \mathbf{Y}\right)/\partial\mathbf{X}\big|_{\mathbf{Y}=\mathbf{X}}$. Consequently, the constructed approximations in (9)-(11) also satisfy the properties stated in [13, Theorem 1]. This concludes the convergence of the sequence of $\mathcal{V}^{[i]}$ to a KKT point of (13).

Algorithm 1 GIA-based algorithm for (12). ϵ determines the stability threshold.

```
1: Initialize $\mathcal{V}^{[0]}, \ i \leftarrow 0$,
2: repeat
3:     $i \leftarrow i+1$,
4:     $\mathcal{V}^{[i]} \leftarrow$ solve (15),
5: until $R_{\text{sum}}^{[i]} - R_{\text{sum}}^{[i-1]} \leq \epsilon R_{\text{sum}}^{[i]}$
6: return $\left\{\{\mathbf{X}_k^\star\}, \{\mathbf{Q}_m^\star\}, \mathbf{W}^\star\right\} \leftarrow \mathcal{V}^{[i]}$
7: UL (RU) transmit covariance can be implemented by choosing the matrix square root as the UL (RU) transmit precoders: $\mathbf{x}_k = \left(\mathbf{X}_k^\star\right)^{\frac{1}{2}} \mathbf{s}_k, \forall k$ and $\mathbf{w} = \left(\mathbf{W}^\star\right)^{\frac{1}{2}} \mathbf{z}$, where $\mathbf{s}_k \sim \mathcal{CN}\left(\mathbf{0}, \mathbf{I}\right)$ and $\mathbf{z} \sim \mathcal{CN}\left(\mathbf{0}, \mathbf{I}\right)$ are the UL data symbols and the artificial noise sequence used for jamming.
```

B. Alternative jamming strategies

The proposed jamming strategy obtained via Algorithm 1 utilizes the coordination among the trusted RUs to enable a secure infrastructure sharing. This requires a successful distribution of an a priori-known psedu-random sequence among

[5] A linear transmit/receive strategy is assumed for the communication process. However, the untrusted RUs may employ a non-linear processing, facilitating successive interference decoding and cancellation. As a result, the inter-UL user interference is eliminated in the calculation of the worst-case leakage rate, as it may not be considered as a reliable interference (i.e., may be decoded).

[6] Since $\mathbf{X}_k = \mathbf{0}$ is always a feasible solution, the difference $R_k - L_{km}$ will be never negative at the optimality [5], i.e., the relaxed problem shares the same optimum as (12).

$$\begin{aligned} R_k\left(\mathcal{V}^{[i]}\right) \geq \tilde{R}_k\left(\mathcal{V}^{[i]}, \mathcal{V}^{[i-1]}\right) := \log\left| \sum_{j\in\mathcal{K}} \mathbf{H}_j \mathbf{X}_j^{[i]} \mathbf{H}_j^H + \mathbf{N} + \mathbf{\Psi}_{\text{SI}}^{[i]} + \mathbf{Q}^{[i]} \right| \\ - f\Bigg(\sum_{j\in\mathcal{K}\backslash k} \mathbf{H}_j \mathbf{X}_j^{[i]} \mathbf{H}_j^H + \mathbf{N} + \mathbf{\Psi}_{\text{SI}}^{[i]} + \mathbf{Q}^{[i]}, \sum_{j\in\mathcal{K}\backslash k} \mathbf{H}_j \mathbf{X}_j^{[i-1]} \mathbf{H}_j^H + \mathbf{N} + \mathbf{\Psi}_{\text{SI}}^{[i-1]} + \mathbf{Q}^{[i-1]} \Bigg), \end{aligned} \tag{9}$$

$$\begin{aligned} L_{km}\left(\mathcal{V}^{[i]}\right) \leq \tilde{L}_{km}\left(\mathcal{V}^{[i]}, \mathcal{V}^{[i-1]}\right) := -\log\left|\mathbf{S}_m\left(\mathbf{\Psi}^{[i]} + \mathbf{N}\right)\mathbf{S}_m^H\right| \\ + f\left(\mathbf{S}_m\left(\mathbf{H}_k \mathbf{X}_k^{[i]} \mathbf{H}_k^H + \mathbf{N} + \mathbf{\Psi}^{[i]}\right)\mathbf{S}_m^H,\ \mathbf{S}_m\left(\mathbf{H}_k \mathbf{X}_k^{[i-1]} \mathbf{H}_k^H + \mathbf{N} + \mathbf{\Psi}^{[i-1]}\right)\mathbf{S}_m^H\right) \end{aligned} \tag{10}$$

$$\begin{aligned} \tilde{C}_m\left(\mathcal{V}^{[i]}, \mathcal{V}^{[i-1]}\right) := -\log\left|\mathbf{Q}_m^{[i]}\right| \\ + f\left(\mathbf{S}_m\left(\mathbf{N} + \mathbf{\Psi}^{[i]} + \sum_{k\in\mathcal{K}} \mathbf{H}_k \mathbf{X}_k^{[i]} \mathbf{H}_k^H\right)\mathbf{S}_m^H + \mathbf{Q}_m^{[i]},\ \mathbf{S}_m\left(\mathbf{N} + \mathbf{\Psi}^{[i-1]} + \sum_{k\in\mathcal{K}} \mathbf{H}_k \mathbf{X}_k^{[i-1]} \mathbf{H}_k^H\right)\mathbf{S}_m^H + \mathbf{Q}_m^{[i-1]}\right) \end{aligned} \tag{11}$$

the trusted RUs, in order to act as the jamming signal, as well as the coordinated transmission of the jamming signal at the trusted RUs. Moreover, the trusted RUs must operate in FD mode in order to enable the joint jamming and the reception of the transmitted signal from the UL users. In the following, we offer variations of the proposed jamming strategy with the intention of relaxing the aforementioned requirements, however, at the expense of a slight performance degradation.

1) Separate/independent Jamming: In this strategy, the trusted RUs utilize separate and statistically independent psedu-random sequences for jamming, i.e., $\mathbf{w}_l \perp \mathbf{w}_m$, $\forall l \neq m$, $\mathbf{w}_m \sim \mathcal{CN}\left(\mathbf{0}, \mathbf{W}_m\right)$, see [5], [16]–[18] for similar strategies. As a result, the transmit jamming signal covariance, see (4) and (5), is restricted to a block-diagonal structure as

$$\mathbf{W} = \left\langle \mathbf{W}_m \right\rangle_{m\in\mathcal{R}}. \tag{16}$$

The corresponding design can be consequently expressed as

$$\max_{\{\mathbf{X}_k\},\{\mathbf{Q}_m\},\{\mathbf{W}_m\},\mathbf{W}} \quad R_{\text{sum}} \quad \text{s.t. } (2), (3), (5), (12\text{c}), (16), \tag{17}$$

which differs from (5) only in the additional linear constraint (16) and can be hence solved via the same procedure as proposed by Algorithm 1. Please note that the abovementioned strategy reduces the need for sharing the same jamming sequence among the trusted RUs and thereby reduces the risk of revealing the used codebook to the untrusted nodes.

2) Half-duplex (HD) Jamming: In this scenario, the jammer is not capable of FD operation [17], [19]. As a result, the trusted RUs must choose between participating in the UL communication process, or transmitting jamming signal towards untrusted entities. This scenario, as well as the corresponding design, is similar to the case where chain accuracy is not sufficient for FD operation, i.e., when κ is large.

3) Uniform Jamming: In order to further simplify the jamming strategy, following a similar strategy as in [20], [21], the trusted RUs may transmit a jamming signal uniformly to all directions, i.e., $\mathbf{W}_m = p_m \mathbf{I}$, $p_m \geq 0$, which reduces the design of the jamming strategy to a power allocation problem at the trusted RUs. Please note that in addition to simplicity, this strategy is useful to provide information security in all directions, e.g., considering additional eavesdropper nodes with unknown channel or location, or when the direction of the untrusted RUs may not be revealed to the other parties. The performance of the aforementioned jamming strategies is evaluated via numerical simulations in Section IV.

IV. Simulation Results

In this section, we evaluate the proposed privacy-preserving sharing mechanism via numerical simulations. We assume that the UL users are uniformly distributed in a squared area of 100 meters length. 4 RUs are positioned each at the center of 4 equally divided squares with length 50 meters, wherein 2 trusted RUs are on one diagonal and 2 untrusted RUs are on another diagonal. Similarly as in [6], the channel between two different transceivers (one UL user and one RU or two RUs) with the distance d is modeled as $\mathbf{H} = \sqrt{\rho}\tilde{\mathbf{H}}$, where $\rho = 1/(1 + (d/50)^3)$ represents the path-loss and vec $\left(\tilde{\mathbf{H}}\right) \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$. The self-interference channels are modeled similar to [22] as

$$\mathbf{G}_{ii} \sim \mathcal{CN}\left(\sqrt{\frac{\rho_{\text{si}} K_R}{1 + K_R}}\mathbf{H}_0, \frac{\rho_{\text{si}}}{1 + K_R}\mathbf{I}_{M_{\text{R},i}} \otimes \mathbf{I}_{N_{\text{R},i}}\right), \forall i \in \mathcal{M},$$

where ρ_{si} is the self-interference channel strength, $\mathbf{H}_0$ is a deterministic term indicating the dominant interference path[7], and $K_R = 10$ is the Rician coefficient. Unless otherwise is stated, the following are set as the default system parameters: $|\mathcal{R}| = 4$, $|\mathcal{M}| = 2$, $|\mathcal{K}| = 2$, $\rho_{\text{si}} = 1$, $N_{\text{U},k} = 2$, $N_{\text{R},m} = M_{\text{R},m} = 2$, $C_m = 100$ Mbit/s, $B = 10$ MHz, $P_{\text{bud}} = P_{\text{U},k} = P_{\text{R},m}$, $\forall k \in \mathcal{K}, m \in \mathcal{M}$. The resulting system performance is then averaged over 1000 channel realizations.

In Fig. 2, the average convergence behavior of Algorithm 1, as well as the optimality gap, is observed for different values of chain accuracy (κ). Note that due its iterative nature, the convergence behavior of Algorithm 1 is important as a measure of the required computational efforts, as well as to verify the expected monotonic improvement. The optimum strategy is obtained by running an exhaustive search over the KKT solutions, by repeating Algorithm 1 for 1000 different initializations. It is observed that the algorithm converges within 100 iterations. Moreover, a narrow gap with the optimum

[7] For simplicity, we choose $\mathbf{H}_0$ as a matrix of all-1 elements

solution, specially for the high chain accuracy, indicates that the resulting performance of Algorithm 1 can be regarded as a close-to-optimum benchmark.

In Fig. 3, the achievable system sum rate is observed under the information privacy requirement. In particular, we compare four scenarios which differ in the usage of the proposed jamming and sharing strategies, evaluated under different levels of power budget P_{bud} and transceiver accuracy $\kappa = \beta$. The first scenario, denoted as ”nSh-nJ”, represents a setup that the untrusted RUs do not participate in the communication process, while the proposed jamming strategy is also turned off. It is observed that when the information privacy is guaranteed in the physical layer, the achievable performance is saturated as the transmit power increases, since the higher transmit power also enhances the received signal quality for the untrusted RU. However, the aforementioned shortcoming is effectively resolved in the second scenario, denoted as ”nSH-J”, by enabling the jamming strategy defined in Subsection II-A. Moreover, it is observed that the obtained jamming gain is highly dependent on the transceiver accuracy, since a higher hardware distortion leads to a stronger residual self-interference, see (4). The third and fourth scenarios represent a system where the untrusted RUs also participate in the UL communication, without and with utilizing FD jamming, respectively, denoted as ”Sh-nJ” and ”Sh-J”. A promising improvement is observed via the participation of the untrusted RUs in the UL communication process, when the proposed jammig strategy is enabled at a system with a high hardware accuracy.

In Fig. 4, the performance of the different jamming strategies in Subsection III-B is evaluated and compared for different values of power budjet, as well as hardware accuracy. In particular, the proposed coordinated jamming strategy is compared with the methods proposed in Subsection III-B. It is observed that the proposed coordinated jamming results in a superior performance, compared to all other (simplified) strategies. However, when the hardware accuracy is sufficient, the separate or uniform jamming strategies, lead to only a marginal performance degradation. The coordination gain is particularly high for a system with a larger κ, as it enables a better management of self-interference signal as well as the transmission power resources. However, it is observed that the HD strategy leads to a severe degradation, indicating that FD capability is a key enabling technology to provide information privacy in the studied CRAN system.

In Fig. 5, the achievable sum secrecy rate is evaluated for different levels of the available jamming power which is specified as a portion of the power budjet at the trusted RU nodes, i.e., $P_{\text{R},m} = P_{\text{bud}}/2^{\zeta_{\text{bud}}}, m \in \mathcal{M}$, where $1/2^{\zeta_{\text{bud}}}$ represent the ratio of the available power dedicated for jamming. It is observed that the achievable performance is sensitive to the portion of the available power dedicated for jamming, as it leads to significantly different performance gains as P_{bud} increases. On the other hand, it is observed that even dedcating a small portion of the P_{bud} for jamming, e.g., with $\zeta_{\text{bud}} = 4$ or 6, the resulting performance benefits significantly from the proposed jamming strategy, for a large or medium levels of P_{bud}. Conversly, it is observed that the performance is almost saturated after dedicating 25% of P_{bud} for jamming. The aforemenetioned behaviour is promising, as it indicates a meaningful improvement even when the jamming power expenditure is a small portion of the available power.

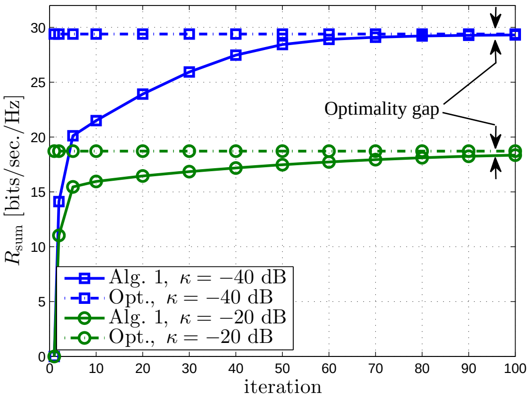

Fig. 2. Achievable sum private rate vs. number of iterations for Algorithm 1.

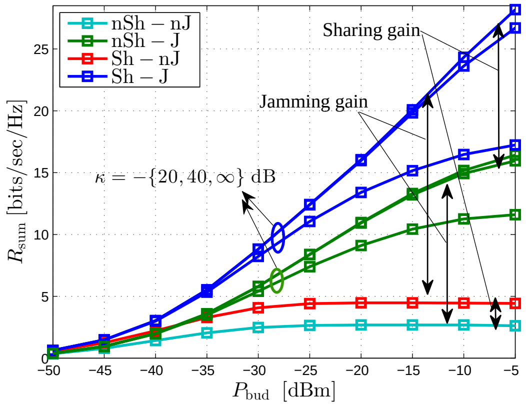

Fig. 3. Achievable sum private rate vs. $P_{\text{bud}} = P_{\text{U},k} = P_{\text{R},m}$. The performance gain due to sharing, and the proposed jamming strategy is observed for different levels of $\kappa = \beta$.

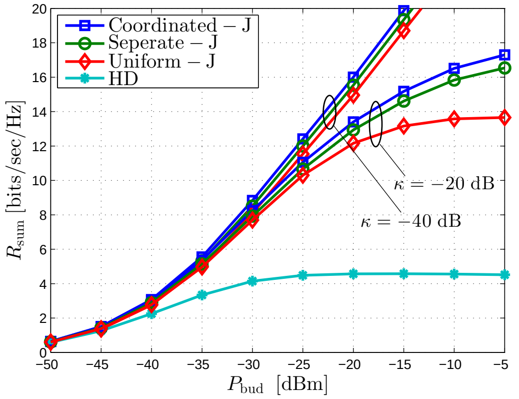

Fig. 4. Achievable sum private rate vs. $P_{\text{bud}} = P_{\text{U},k} = P_{\text{R},m}$ for different jamming strategies.

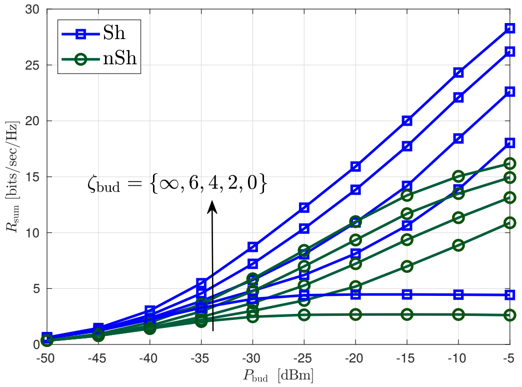

Fig. 5. Achievable sum private rate for different levels of the available jaming power, $P_{\mathrm{R},m} = P_{\mathrm{bud}}/2^{\zeta_{\mathrm{bud}}}, m \in \mathcal{M}$.

V. Conclusion

In this work, we have proposed a coordinated jamming strategy to enable the use of untrusted RU resources in the UL of a C-RAN, while preserving information privacy. We summarize the main take-aways of this work as following. Firstly, for a traditional system without a jamming strategy, it is observed that guaranteeing information privacy in physical layer leads to a sever performance loss and resource inefficiency. Secondly, a significant gain is observed via the application of the proposed jamming, however, the jamming gain is highly influenced by the accuracy of the FD transceivers, due to the degrading impact of residual self-interference. Thirdly, a promising gain can be obtained in the achievable UL private rate via the participation of the external RUs, i.e., sharing gain, when the proposed jamming strategy is implemented in a system with a high transceiver dynamic range.

References

[1] K. Samdanis, X. Costa-Perez, and V. Sciancalepore, "From network sharing to multi-tenancy: The 5g network slice broker," *IEEE Communications Magazine*, vol. 54, no. 7, pp. 32–39, July 2016.

[2] E. A. Jorswieck, L. Badia, T. Fahldieck, E. Karipidis, and J. Luo, "Spectrum sharing improves the network efficiency for cellular operators," *IEEE Communications Magazine*, vol. 52, no. 3, pp. 129–136, March 2014.

[3] S.-H. Park, O. Simeone, and S. Shamai, "Fronthaul quantization as artificial noise for enhanced secret communication in c-ran," *arXiv preprint arXiv:1705.00474*, 2017.

[4] F. Tian, P. Zhang, and Z. Yan, "A survey on c-ran security," *IEEE Access*, vol. 5, pp. 13 372–13 386, 2017.

[5] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4962–4974, Oct 2013.

[6] S. Park, O. Simeone, and S. Shamai, "Multi-tenant c-ran with spectrum pooling: Downlink optimization under privacy constraints," *IEEE Transactions on Vehicular Technology*, pp. 1–1, 2018.

[7] J. Kim, D. Yu, S.H. Park, O. Simeone, and S. Shamai, "Inter-Tenant Cooperative Reception for C-RAN Systems With Spectrum Pooling," *arXiv preprint arXiv:2001.10305*, 2020.

[8] L. Wang, K. Wong, M. Elkashlan, A. Nallanathan and S. Lambotharan, "Secrecy and Energy Efficiency in Massive MIMO Aided Heterogeneous C-RAN: A New Look at Interference," in *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1375-1389, Dec. 2016.

[9] Y. Jeon, S. Park, C. Song, J. Moon, S. Maeng, and I. Lee, "Joint designs of fronthaul compression and precoding for full-duplex cloud radio access networks," *IEEE Wireless Communications Letters*, vol. 5, no. 6, pp. 632–635, Dec 2016.

[10] B. P. Day, A. R. Margetts, D. W. Bliss, and P. Schniter, "Full-duplex bidirectional mimo: Achievable rates under limited dynamic range," *IEEE Transactions on Signal Processing*, vol. 60, no. 7, pp. 3702–3713, July 2012.

[11] J. Zhu, D. W. K. Ng, N. Wang, R. Schober, and V. K. Bhargava, "Analysis and design of secure massive mimo systems in the presence of hardware impairments," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 2001–2016, March 2017.

[12] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wiretap channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, p. 5, 2009.

[13] B. R. Marks and G. P. Wright, "A general inner approximation algorithm for nonconvex mathematical programs," *Operations research*, vol. 26, no. 4, pp. 681–683, 1978.

[14] A. C. Cirik, O. Taghizadeh, L. Lampe, and R. Mathar, "Fronthaul compression and precoding design for mimo full-duplex cognitive radio networks," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, April 2018, pp. 1–6.

[15] L. Vandenberghe, S. Boyd, and S.-P. Wu, "Determinant maximization with linear matrix inequality constraints," *SIAM journal on matrix analysis and applications*, vol. 19, no. 2, pp. 499–533, 1998.

[16] Y. Sun, D. W. K. Ng, J. Zhu, and R. Schober, "Robust and secure resource allocation for full-duplex miso multicarrier noma systems," *IEEE Transactions on Communications*, vol. 66, no. 9, pp. 4119–4137, Sep. 2018.

[17] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[18] O. Taghizadeh, P. Neuhaus, R. Mathar, and G. Fettweis, "Secrecy energy efficiency of mimome wiretap channels with full-duplex jamming," *IEEE Transactions on Communications*, pp. 1–1, 2019.

[19] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the mimo gaussian wiretap channel with a cooperative jammer," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 5013–5022, Oct 2011.

[20] R. Sohrabi and Y. Hua, "A new look at secrecy capacity of mimome using artificial noise from alice and bob without knowledge of eve's csi," in *2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, Nov 2018, pp. 1291–1295.

[21] S. Liu, Y. Hong, and E. Viterbo, "Practical secrecy using artificial noise," *IEEE Communications Letters*, vol. 17, no. 7, pp. 1483–1486, 2013.

[22] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven characterization of full-duplex wireless systems," *IEEE Transactions on Wireless Communications*, vol. 11, no. 12, pp. 4296–4307, December 2012.