Confidential Communication in C-RAN Systems with Infrastructure Sharing

Michael Zeide, Osvaldo Simeone, and Shlomo Shamai (Shitz)

***Abstract*—This work considers a Cloud Radio Access Network (C-RAN) architecture in which the Radio Units (RUs) are shared among multiple operators or are managed by a separate infrastructure provider, while mobile users and cloud processor belong to the given service provider. In order to account for the resulting privacy concerns, the strict constraint is imposed that the RUs should only be able to infer a fraction of the information about the mobiles' messages that vanishes with the transmission blocklength. The largest achievable rate under this constraint, or secrecy capacity, is characterized for a two-cell Gaussian model and for a multi-cell circular Wyner model.**

I. Introduction

MODERN cellular communication systems can leverage the sharing of spectral and infrastructure resources in order to reduce deployment costs and capital expenditures (see [1] and references therein). An architecture that is particularly well suited for infrastructure sharing is Cloud Radio Access Network (C-RAN), in which a dense deployment of Radio Units (RUs) by an infrastructure provider may be leveraged by multiple service providers in order to serve their subscribers. The RUs are connected to a proprietary or shared cloud platform in which baseband processing takes place. While there is a vast literature on the analysis of C-RAN, systems with shared infrastructure have received far less attention.

The information-theoretic performance of C-RAN has been carried out in a larger number of works, which are reviewed in [2]. These works implicitly assume that all RUs and the cloud processor belong to the same service provider in that no constraints are imposed on the confidentiality of the users' information that traverses the radio interface and the fronthaul links connecting RUs to cloud.

In contrast, this work considers a C-RAN architecture in which the RUs are shared among multiple operators or are managed by a separate infrastructure provider, while mobile users and cloud processor belong to the given service provider. In order to account for the resulting privacy concerns, the strict constraint is imposed that the RUs should only be able to infer a fraction of the information about the mobiles' messages that vanishes with the transmission blocklength. The largest achievable rate under this constraint, or secrecy capacity [4], is characterized for a two-cell Gaussian model and for a multi-cell circular Wyner model.

This work follows a long line of research on the derivation of performance bounds on the achievable rates in the presence of secrecy constraints. Basic models, such as the multiple access channel, the broadcast channel, and the interference channel were considered in [6]-[10]. This paper is mostly related to the activity on relay channels with untrusted relays

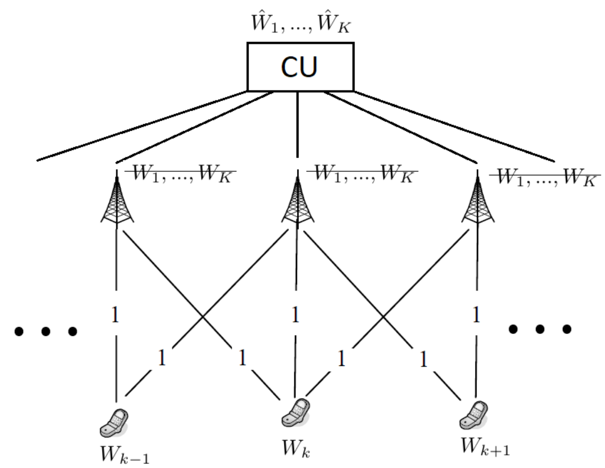

Fig. 1: Multi-cell C-RAN model with untrusted radio-units (RUs).

[3] and it distinguishes itself by considering relays, the RUs that operate out-of-band. Full proofs can be found on [15].

II. System Model

In order to investigate the secrecy capacity in the presence of untrusted RUs in C-RAN systems, we consider two system models of increasing complexity. First, we study a simple Cloud-RAN system, where each cell contains a single user a RU. Each RU receives the transmission of the same-cell user with interference from the adjacent cell's user and additive white Gaussian noise. The received signal at the jth RU for an arbitrary time index reads

$$\begin{aligned} Y_1 &= X_1 + X_2 + Z_1 \\ Y_2 &= X_1 + X_2 + Z_2, \end{aligned} \tag{1}$$

where the additive noise is $Z_j \sim \mathcal{N}(0,1)$, and the transmission power of each user is bounded by P.

Then, we consider a multi-cell Cloud-RAN system modeled as a circular variant of the Wyner model [4]. As seen in Fig. 1, this model includes an array of K cell-sites, indexed by $j = 1, ..., K$. Each cell contains a single user and a RU. Each RU receives the transmission of the same-cell user with interference from the users of the adjacent cells and additive white Gaussian noise. The received signal at the jth RU for an arbitrary time index reads

$$Y_j = X_{[j-1]_K} + X_j + X_{[j+1]_K} + Z_j, \tag{2}$$

where $[j]_K = \big(j-1 \text{ mod } K\big)+1$, the additive noise is $Z_j \sim \mathcal{N}(0,1)$, and the transmission power of each user is bounded by P. Model (2) assumes a circular geometry in which cell 1 interferes with cell K.

We consider a conservative set-up in which each user wishes to guarantee secrecy with respect to all RUs. An $\big(2^{nR},n\big)$ code for this model consists of the following: (a) A message set $\mathcal{W}=\{1,2,...,2^{nR}\}$, from which independent and uniformly distributed messages W_1,...,W_K are generated for the K users; (b) K stochastic encoders, f_k: $\mathcal{W}\rightarrow\mathbb{R}^n$, which map each message $w_k\in\mathcal{W}$ to a codeword $x_k^n\in\mathbb{R}^n$, for $k=1,...,K$; (c) A "cloud" decoder g: $\mathbb{R}^n\times...\times\mathbb{R}^n\rightarrow\mathcal{W}^K$, which maps received sequences $y_1^n,...,y_K^n$ to an estimated message pair $(\hat{w}_1,...,\hat{w}_K)\in\mathcal{W}^K$. For a given code, we define the average probability of block error as

$$P_e^n=\frac{1}{2^{KnR}}\sum_{(w_1,...,w_K)\in\mathcal{W}^K}\mathbb{P}\{(\hat{W}_1,...,\hat{W}_K)\neq(w_1,...,w_K)\}. \tag{3}$$

A rate is said to be *achievable* if there exists a sequence of $(2^{nR},n)$ codes with average error probability satisfying $P_e^n\rightarrow 0$ as n goes to infinity, and ensuring the equivocation conditions

$$KR\leq\frac{1}{n}H(W_1,...,W_K|Y_k^n) \tag{4}$$

for $k=1,...,K$, and for sufficiently large n. Condition (4) guarantees secrecy with respect to each RUk. The secrecy per-user capacity C is the supremum of the set of achievable rates.

III. Main Results

In this section, we derive our main results.

A. Two-Cell Model

For the two-cell model, we first derive an achievable rate and then characterize the secrecy capacity. The first rate is obtained by using orthogonal transmission, whereby each transmitter transmits for half of the time with double power, while the other is silent. The capacity achieving scheme uses non-orthogonal transmission, whereby the two transmitters transmit simultaneously. The proofs follow by using the same technique in [11].

Proposition 1: The secrecy capacity under the two-cell model is given by

$$C=\tfrac{1}{4}\log\big(1+4P\big)-\tfrac{1}{4}\log\big(1+2P\big), \tag{5}$$

and is achieved by non-orthogonal transmission.

Remark 1: The number of achievable degrees of freedom (DoF) is defined as

$$\text{DoF}=\lim_{P\rightarrow\infty}\frac{C}{\frac{1}{2}\log P}. \tag{6}$$

In the case of no secrecy constraints, it is well known that we have DoF $=1$ (see, e.g [13]). In contrast, as shown in Proposition 1, as a result of the secrecy constraints against untrusted RUs, we have DoF $=0$.

B. Multi-Cell Wyner Model

As in the two-cell case, in this section, we first derive an achievable rate and then characterize the secrecy capacity.

Lemma 3: Orthogonal transmission yields the following lower bound on the secrecy capacity for the case of multi-cell Wyner model

$$C\geq\frac{1}{6}\log\big(1+9P\big)-\frac{1}{6}\log\big(1+3P\big). \tag{7}$$

Proposition 2: For $K\geq 5$, the secrecy capacity for the multi-cell Wyner model is given by

$$\begin{aligned}C&\\ &=\tfrac{1}{2K}\sum_{k=0}^{K-1}\log\left(1+3P+4P\cos\Big(2\pi\frac{k}{K}\Big)+2P\cos\Big(2\pi\frac{2k}{K}\Big)\right)\\ &-\tfrac{1}{2K}\log\big(1+3P\big),\end{aligned} \tag{8}$$

and is achieved by non-orthogonal transmission.

Proof: The achievability follows in a manner similar to [11] and a sketch of the converse proof is given in Appendix A.

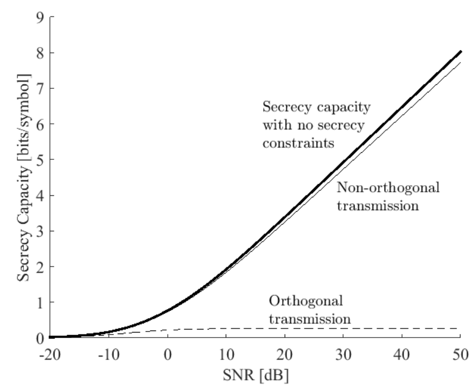

Fig. 2: Secrecy capacity for the multi-cell Wyner model versus the SNR for $K=30$.

Remark 2: Under no secrecy constraints, the DoF tends to 1 for large K [14, Section 3.1.2]. From Proposition 2, when adding secrecy constraints, the DoF still tends to 1 for large K. By comparison with the two-cell case in Remark 1, this result shows the important role played by the limited inter-cell interference span in ensuring confidential communication. Fig. 2 shows the capacity sum-rate versus the signal-to-noise ratio P, confirming the scaling revealed by the discussed DoF result.

IV. Conclusions and Outlook

Ensuring secrecy in shared cellular infrastructures is an important problem and this work has addressed a simple set-up that reveals the roles of centralized decoding in C-RAN. Further work is needed in order to address more realistic system models.

Appendix A

From Fano's inequality, we have

$$H(W_1,...,W_K|Y_1^n,...,Y_K^n)\leq n\epsilon_n, \tag{9}$$

where $\lim_{n\to\infty} \epsilon_n = 0$. Then for each k

$$\begin{aligned}
& KnR \\
& \overset{(a)}{\leq} H(W_1, ..., W_K|Y_k^n) \\
& \overset{(b)}{\leq} H(W_1, ..., W_K|Y_k^n) \\
& -H(W_1, ..., W_K|Y_1^n, ..., Y_K^n) + n\epsilon_n \\
& = I(W_1, ..., W_K; Y_1^n, ..., Y_{k-1}^n, Y_{k+1}^n, ..., Y_K^n|Y_k^n) + n\epsilon_n \\
& \overset{(c)}{\leq} I(X_1^n, ..., X_K^n; Y_1^n, ..., Y_{k-1}^n, Y_{k+1}^n, ..., Y_K^n|Y_k^n) + n\epsilon_n \\
& \overset{(d)}{\leq} \sum_{i=1}^{n} I(X_{1,i}, ..., X_{K,i}; \\
& Y_{1,i}, ..., Y_{k-1,i}, Y_{k+1,i}, ..., Y_{K,i}|Y_{k,i}) + n\epsilon_n,
\end{aligned} \tag{10}$$

where (a) follows from the secrecy constraint (4); (b) follows from Fano's inequality; (c) follows from the following Markov chain $W_1, ..., W_K \rightarrow X_1^n, ..., X_K^n \rightarrow Y_1^n, ..., Y_K^n$; and ($d$) follows from Appendix B. Then for all i we obtain

$$\begin{aligned}
& I(X_{1,i}, ..., X_{K,i}; Y_{1,i}, ..., Y_{[k-1]_K,i}, Y_{[k+1]_K,i}, ..., Y_{K,i}|Y_{k,i}) \\
& = h(Y_{1,i}, ..., Y_{[k-1]_K,i}, Y_{[k+1]_K,i}, ..., Y_{K,i}|Y_{k,i}) \\
& -h(Y_{1,i}, ..., Y_{K,i}|X_{1,i}, ..., X_{K,i}) \\
& +h(Y_{k,i}|X_{1,i}, ..., X_{K,i}).
\end{aligned} \tag{11}$$

For $K \geq 5$, we obtain the following upper bound for the first term above

$$\begin{aligned}
& h(Y_{1,i}, ..., Y_{[k-1]_K,i}, Y_{[k+1]_K,i}, ..., Y_{K,i}|Y_{k,i}) \\
& = h(Y_{1,i}, ..., Y_{[k-2]_K,i} - sY_{k,i}, Y_{[k-1]_K,i} - tY_{k,i}, \\
& Y_{[k+1]_K,i} - tY_{k,i}, Y_{[k+2]_K,i} - sY_{k,i}, ..., Y_{K,i}|Y_{k,i}) \\
& \leq h(Y_{1,i}, ..., Y_{[k-2]_K,i} - sY_{k,i}, Y_{[k-1]_K,i} - tY_{k,i}, \\
& Y_{[k+1]_K,i} - tY_{k,i}, Y_{[k+2]_K,i} - sY_{k,i}, ..., Y_{K,i}) \triangleq h(\tilde{\mathbf{Y}}_{k,i}),
\end{aligned} \tag{12}$$

where

$$\tilde{\mathbf{Y}}_{k,i} = \mathbf{H}_k \mathbf{X}_i + \mathbf{G}_k \mathbf{Z}_i, \tag{13}$$

where the $K \times 1$ vectors $\mathbf{X}_i$ and $\mathbf{Z}_i$ are defined as $\mathbf{X}_i = \left[X_{1,i}, ..., X_{K,i}\right]^T$ and $\mathbf{Z}_i = \left[Z_{1,i}, ..., Z_{K,i}\right]^T$.

Define the $K-1 \times K$ matrix $\mathbf{U}_k$ from an identity matrix $\mathbf{I}_{K\times K}$ by removing the kth row. The product $\mathbf{U}_k\mathbf{A}$, where $\mathbf{A}$ is an arbitrary $K \times K$ size matrix, hence removes the kth row of $\mathbf{A}$, while the product of $\mathbf{A}\mathbf{U}_k^\dagger$ removes the kth column of $\mathbf{A}$. The $K-1 \times K$ size matrices $\mathbf{H}_k$ and $\mathbf{G}_k$ in (13) are then defined as

$$\begin{aligned}
\mathbf{H}_k &= \mathbf{U}_k \mathbf{Q}_k \mathbf{H}, \\
\mathbf{G}_k &= \mathbf{U}_k \mathbf{Q}_k,
\end{aligned} \tag{14}$$

where

$$\left(\mathbf{Q}_k\right)_{i,j} = \begin{cases} 1 & \text{if } i = j \\ -t & \text{if } i = [k \pm 1]_K, j = k \\ -s & \text{if } i = [k \pm 2]_K, j = k \\ 0 & \text{otherwise.} \end{cases} \tag{15}$$

The entropy of $\tilde{\mathbf{Y}}_{k,i}$ can be bounded as

$$\begin{aligned}
& h(\tilde{\mathbf{Y}}_{k,i}) \\
& \leq \tfrac{1}{2}\log\left((2\pi e)^{K-1}|P\mathbf{H}_k\mathbf{H}_k^\dagger + \mathbf{G}_k\mathbf{G}_k^\dagger|\right) \\
& = \tfrac{1}{2}\log\left((2\pi e)^{K-1}\right. \\
& \left.\cdot|P\mathbf{U}_k\mathbf{Q}_k\mathbf{H}\mathbf{H}^\dagger\mathbf{Q}_k^\dagger\mathbf{U}_k^\dagger + \mathbf{U}_k\mathbf{Q}_k\mathbf{Q}_k^\dagger\mathbf{U}_k^\dagger|\right) \\
& = \tfrac{1}{2}\log\left((2\pi e)^{K-1} \cdot |\mathbf{U}_k\mathbf{Q}_k\left(\mathbf{I} + P\mathbf{H}\mathbf{H}^\dagger\right)\mathbf{Q}_k^\dagger\mathbf{U}_k^\dagger|\right),
\end{aligned} \tag{16}$$

where in the inequality we have used the independence of signals transmitted by different users. We define the matrix $\mathbf{J}_k$ as

$$\mathbf{J}_k \triangleq \mathbf{Q}_k\left(\mathbf{I} + P\mathbf{H}\mathbf{H}^\dagger\right)\mathbf{Q}_k^\dagger \tag{17}$$

By the definition of matrix $\mathbf{U}_k$ the product $\mathbf{U}_k\mathbf{J}_k\mathbf{U}_k^\dagger$ is the (k,k)'s minor of matrix $\mathbf{J}_k$, i.e. $\mathbf{M}_{k,k}(\mathbf{J}_k) = \mathbf{U}_k\mathbf{J}_k\mathbf{U}_k^\dagger$. Furthermore, the elements in the kth row of matrix $\mathbf{J}_k$ where $\mathbf{M}_{k,k}(\mathbf{J}_k)$ is the (k,k)'s minor of $\mathbf{J}_k$. From the other hand, from $\mathbf{Q}_k$ and $\mathbf{H}$ definitions, the elements in matrix $\mathbf{J}_k$ kth row are equal to

$$\left(\mathbf{J}_k\right)_{k,j} = \begin{cases} 1 + 3P & \text{if } j = k \\ 2P - (1+3P)t & \text{if } j = [k \pm 1]_K \\ P - (1+3P)s & \text{if } j = [k \pm 2]_K \\ 0 & \text{otherwise.} \end{cases} \tag{18}$$

Substituting $t = \frac{2P}{1+3P}$ and $s = \frac{P}{1+3P}$ yields that there is only one element in the kth row of $\mathbf{J}_k$ that is different from zero, and its position is (k,k). Hence, the determinant of $\mathbf{J}_k$ equals to

$$|\mathbf{J}_k| = (1+3P)|\mathbf{M}_{k,k}(\mathbf{J}_k))|. \tag{19}$$

Finally, since $|\mathbf{Q}_k| = 1$, the determinant of matrix $\mathbf{J}_k$ is given by

$$|\mathbf{J}_k| = |\mathbf{Q}_k(\mathbf{I} + P\mathbf{H}\mathbf{H}^\dagger)\mathbf{Q}_k^\dagger| = |\mathbf{I} + P\mathbf{H}\mathbf{H}^\dagger|. \tag{20}$$

Hence by combining eq. (19) and (20) we obtain

$$\begin{aligned}
& |\mathbf{U}_k\mathbf{Q}_k\left(\mathbf{I} + P\mathbf{H}\mathbf{H}^\dagger\right)\mathbf{Q}_k^\dagger\mathbf{U}_k^\dagger| \\
& = |\mathbf{M}_{k,k}(\mathbf{J}_k)| \\
& = \frac{|\mathbf{I} + P\mathbf{H}\mathbf{H}^\dagger|}{1+3P},
\end{aligned} \tag{21}$$

and we have

$$\begin{aligned}
& h(\tilde{\mathbf{Y}}_i) \\
& \leq \tfrac{1}{2}\log\left((2\pi e)^{K-1} \cdot |\mathbf{U}_k\mathbf{Q}_k\left(\mathbf{I} + P\mathbf{H}\mathbf{H}^\dagger\right)\mathbf{Q}_k^\dagger\mathbf{U}_k^\dagger|\right) \\
& = \tfrac{1}{2}\log\left[(2\pi e)^{K-1}\frac{|\mathbf{I} + P\mathbf{H}\mathbf{H}^\dagger|}{1+3P}\right].
\end{aligned} \tag{22}$$

The other terms in (11) can be expressed as

$$\begin{aligned}
& -h(Y_{1,i}, ..., Y_{K,i}|X_{1,i}, ..., X_{K,i}) \\
& +h(Y_{k,i}|X_{1,i}, ..., X_{K,i}) \\
& = -\tfrac{1}{2}\log\left(2\pi e\right)^{K-1}.
\end{aligned} \tag{23}$$

Since matrix $\mathbf{I} + P\mathbf{H}\mathbf{H}^\dagger$ is circulant, its eigenvalues can be computed as in [14], obtaining

$$\lambda_k = 1 + 3P + 4P\cos\left(2\pi\tfrac{k}{K}\right) + 2P\cos\left(2\pi\tfrac{2k}{K}\right). \tag{24}$$

for $k = 1, ..., K$. Since the determinant of a matrix is equal to the product of its eigenvalues, we can write

$$\begin{aligned}
& \log|\mathbf{I} + P\mathbf{H}\mathbf{H}^\dagger| \\
& = \sum_{k=0}^{K-1} \log\left(1 + 3P + 4P\cos\left(2\pi\frac{k}{K}\right) + 2P\cos\left(2\pi\frac{2k}{K}\right)\right).
\end{aligned} \tag{25}$$

Substituting (22) and (23) into (11), and then into (10) and using (25), we obtain

$$R \leq \frac{1}{2K}\sum_{k=0}^{K-1}\log\left(1+3P+4P\cos\left(2\pi\frac{k}{K}\right)+2P\cos\left(2\pi\frac{2k}{K}\right)\right) -\frac{1}{2K}\log\left(1+3P\right). \quad (26)$$

This concludes the proof. □

Appendix B

Proof: For any $k=1,...,K$ we obtain

$$\begin{aligned} &I(X_1^n,...,X_K^n;Y_1^n,...,Y_{k-1}^n,Y_{k+1}^n,...,Y_K^n|Y_k^n)\\ &=h(Y_1^n,...,Y_{k-1}^n,Y_{k+1}^n,...,Y_K^n|Y_k^n)\\ &-h(Y_1^n,...,Y_{k-1}^n,Y_{k+1}^n,...,Y_K^n|X_1^n,...,X_K^n,Y_k^n)\\ &=h(Y_1^n,...,Y_{k-1}^n,Y_{k+1}^n,...,Y_K^n|Y_k^n)\\ &+h(Y_k^n|X_1^n,...,X_K^n)-h(Y_1^n,...,Y_K^n|X_1^n,...,X_K^n). \end{aligned} \quad (27)$$

For the first term we obtain

$$\begin{aligned} &h(Y_1^n,...,Y_{k-1}^n,Y_{k+1}^n,...,Y_K^n|Y_k^n)\\ &=\sum_{\substack{j=1\\ j\neq k}}^{K} h(Y_j^n|Y_1^n,...,Y_{j-1}^n,Y_k^n)\\ &=\sum_{\substack{j=1\\ j\neq k}}^{K}\sum_{i=1}^{n} h(Y_{j,i}|Y_j^{i-1},Y_1^n,...,Y_{j-1}^n,Y_k^n)\\ &\overset{(a)}{\leq}\sum_{i=1}^{n}\sum_{j=1,j\neq k}^{K} h(Y_{j,i}|Y_{1,i},...,Y_{j-1,i},Y_{k,i})\\ &=\sum_{i=1}^{n} h(Y_{1,i},...,Y_{k-1,i},Y_{k+1,i},...,Y_{K,i}|Y_{k,i}) \end{aligned} \quad (28)$$

where *(a)* follows from entropy increasing due to conditioning removal. Now for the second term we obtain

$$\begin{aligned} &h(Y_k^n|X_1^n,...,X_K^n)\\ &=\sum_{i=1}^{n} h(Y_{k,i}|Y_k^{i-1},X_1^n,...,X_K^n)\\ &\overset{(a)}{\leq}\sum_{i=1}^{n} h(Y_{k,i}|X_{1,i},...,X_{K,i}) \end{aligned} \quad (29)$$

where *(a)* follows from entropy increasing due to conditioning removal. Now for the third term we obtain

$$\begin{aligned} &h(Y_1^n,...,Y_K^n|X_1^n,...,X_K^n)\\ &=h(Z_1^n,...,Z_K^n|X_1^n,...,X_K^n)\\ &\overset{(a)}{=}h(Z_1^n,...,Z_K^n)\\ &\overset{(b)}{=}\sum_{i=1}^{n} h(Z_{1,i},...,Z_{K,i})\\ &=\sum_{i=1}^{n} h(Z_{1,i},...,Z_{K,i}|X_{1,i},...,X_{K,i})\\ &=\sum_{i=1}^{n} h(Y_{1,i},...,Y_{K,i}|X_{1,i},...,X_{K,i}), \end{aligned} \quad (30)$$

where *(a)* follows from the noise components independence of the transmitted signals' components; *(b)* follows from the fact that the noise components are iid. Hence combining (28), (29) and (30) yields

$$\begin{aligned} &I(X_1^n,...,X_K^n;Y_1^n,...,Y_{k-1}^n,Y_{k+1}^n,...,Y_K^n|Y_k^n)\\ &\leq\sum_{i=1}^{n} I(X_{1,i},...,X_{K,i};Y_{1,i},...,Y_{k-1,i},Y_{k+1,i},...,Y_{K,i}|Y_{k,i}) \end{aligned} \quad (31)$$

Acknowledgment

This work has been supported by the European Research Council (ERC) under the European Unions Horizon 2020 Research and Innovation Programme (Grant Agreement Nos. 694630 and 725731).

References

[1] Park SH, Simeone O, Shamai S., "Multi-Tenant C-RAN With Spectrum Pooling: Downlink Optimization Under Privacy Constraints," arXiv preprint arXiv:1710.06094. 2017 Oct 17.

[2] S.H. Park, O. Simeone, O. Sahin, and S.S. Shitz, "Fronthaul compression for cloud radio access networks: Signalprocessing advances inspired by network information theory," IEEE Signal Process. Magazine, vol. 31, no. 6, pp. 6979, Nov. 2014.

[3] Bassily, Raef, et al. "Cooperative security at the physical layer: A summary of recent advances." IEEE Signal Processing Magazine 30.5 (2013): 16-28.

[4] A.D. Wyner, "Shannon-Theoretic Approach to a Gaussian Cellular Multiple-Access Channel," IEEE Transactions on Information Theory, vol. 40, no. 6, Nov. 1994.

[5] S.K. Leung-Yan-Cheong and M.E. Hellman, "The Gaussian Wiretap Channel," IEEE Transactions on Information Theory, vol. it-24, no. 4, July 1978.

[6] S. Zou, Y. Liang, L. Lai, S. Shamai (Shitz), "Degraded Broadcast Channel: Secrecy Outside of a Bounded Range," IEEE Information Theory Workshop (ITW2015), April 26-May 1, 2015, Jerusalem, Israel.

[7] E. Tekin and A. Yener, "The general Gaussian Multiple Access and Two-Way Wire-Tap Channels" Achievable Rates and Cooperative Jamming," IEEE Transactions on Information Theory, Jan. 2012.

[8] Y. Liang and H.V. Poor, "Multiple-Access Channels With Confidential Messages," IEEE Transactions on Information Theory, vol. 54, no. 3, March 2008

[9] R. Liu, I. Maric, P. Spasojevic and R.D Yates, "Discrete Memoryless Interference and Broadcast Channels with Confidential Messages: Secrecy Rate Regions," IEEE Transactions on Information Theory, vol. 54, no. 6, June 2008

[10] T.M. Cover and J.A. Thomas, "Elements of information theory," New York: Wiley, 1991.

[11] X. Tang, R. Liu, P. Spasojevic and H. Poor, "The Gaussian Wiretap Channel with a Helping Interferer," ISIT 2008, Toronto, Canada.

[12] R.M. Gray, "On the asymptotic eigenvalue distribution of Topeliz matrices," IEEE Trans. Inf. Theory, vol. IT-18, no. 6, pp. 725-730, Nov. 1972.

[13] A.H. Madsen and A. Nosratinia, "The Multiplexing Gain of Wireless Networks," Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.

[14] O. Simeone, N. Levy, A. Sanderovich, O. Somekh, B.M. Zaidel, H.V. Poor and S. Shamai (Shitz), "Cooperative Wireless Cellular Systems: An Information-Theoretic View," Foundations and Trends in Communications and Information Theory: Vol. 8: No. 1-2, pp 1-177. http://dx.doi.org/10.1561/0100000048.

[15] M. Zeide, O. Simeone, and S. Shamai (Shitz), "Confidential Communication in C-RAN Systems with Infrastructure Sharing," available at https://nms.kcl.ac.uk/osvaldo.simeone/Zeide18.pdf.