Physical Communication 46 (2021) 101319

Contents lists available at ScienceDirect

Physical Communication

journal homepage: www.elsevier.com/locate/phycom

Full length article

Hybrid beamforming strategies for secure multicell multiuser mmWave MIMO communications

Berna Özbek [a,*], Oğulcan Erdoğan [a], Sherif A. Busari [b], Jonathan Gonzalez [b]

[a] Department of Electrical and Electronics Eng., Izmir Institute of Technology, Turkey
[b] GS-Lda, Águeda, Portugal

ARTICLE INFO

Article history:
Received 30 August 2020
Received in revised form 14 February 2021
Accepted 3 March 2021
Available online 20 March 2021

Keywords:
Physical layer security
mmWave communications
Massive MIMO
Hybrid beamforming
AN beamforming

ABSTRACT

Over the last decade, many advancements have been made in the field of wireless communications. Among the major technology enablers being explored for the beyond fifth-generation (B5G) networks at the physical layer (PHY), a great deal of attention has been focused on millimeter-wave (mmWave) communications, massive multiple-input multiple-output (MIMO) antenna systems and beamforming techniques. These enablers bring to the forefront great opportunities for enhancing the performance of B5G networks, concerning spectral efficiency, energy efficiency, latency, and reliability. The wireless communication is prone to information leakage to the unintended nodes due to its open nature. Hence, the secure communication is becoming more critical in the wireless networks. To address this challenge, the concept of Physical Layer Security (PLS) is explored in the literature. In this paper, we examine the mmWave transmission through linear beamforming techniques for PLS based systems. We propose the secure multiuser (MU) MIMO mmWave communications by employing hybrid beamforming at the base stations (BSs), legitimate users and eavesdroppers. Using three Dimensional (3D) mmWave channel model for each node, we utilize the artificial noise (AN) beamforming to jam the transmission of eavesdropper and to enhance the secrecy rate. The secrecy performance on multicell mmWave MU-MIMO downlink communications is demonstrated to reveal the key points directly related to the system security for B5G wireless systems.

1. Introduction

For wireless networks, one of the key technological enablers is the usage of millimeter-wave (mmWave) frequencies to provide ultra high data rate transmission and very low latency [1]. Besides, the mmWave makes also possible to use smaller antennas due to its smaller wavelength. Hence, large antenna arrays can be formed to exploit the spatial degree of freedom.

In the multiple-input multiple-output (MIMO) systems, the transmitter can simultaneously communicate to multiple receivers by forming their signals to the intended direction via beamforming [2]. For the mmWave perspective and using large antenna arrays, the narrow beam can be constructed. However, the large antenna arrays can consume more power than the conventional systems. The hybrid scheme combining analog and digital beamforming has been presented to ensure the power efficiency on such a large arrays [3–5]. Thus, the hybrid beamforming is the inevitable part of MIMO systems.

Besides many advantages of mmWave and hybrid MIMO, the security becomes an important issue for the B5G communication systems. By supporting the massive number of devices in B5G networks, the conventional cryptographic techniques including key generation and distribution become more challenging tasks. To address this challenge, the concept of Physical Layer Security (PLS) has been introduced and explored for the wireless communication systems as a complement solution of cryptographic techniques [6–8].

The aim of PLS is to completely eliminate or reduce the effects of eavesdropping attacks through unauthorized receivers or transmitters [9]. In the literature, there are two types of eavesdropping attacks namely active and passive. The active eavesdropper behaves as a transmitter and attempts to jam the legitimate user's transmission. Conversely, the passive eavesdropper hides its presence from the transmitter and listens the legitimate user's channel. In this paper, we consider only the passive eavesdropper attacks which often occur in the practical applications.

The authors in [10–12] have considered the PLS for the sub-6GHz channel. The robust beamforming has been given in [10] by solving the resource allocation problem for the multiuser multiple-input single-output (MISO) and power transfer system. In [11], the artificial noise (AN) and Maximum Ratio Transmission (MRT) precoders have been studied for the multicell MU-MIMO

* Corresponding author.
E-mail address: bernaozbek@iyte.edu.tr (B. Özbek).

https://doi.org/10.1016/j.phycom.2021.101319
1874-4907/

through the secrecy rate and the secrecy outage probability. In [12], the multiuser (MU)-MIMO communication with different precoders as Zero-Forcing (ZF) and Minimum Mean Squared Error (MMSE) techniques have been considered in the presence of a passive eavesdropper under the imperfect channel state information (CSI).

While the PLS with beamforming techniques have been extensively examined in the literature for sub 6GHz wireless systems [13], there are limited number of PLS studies for the mmWave MIMO systems. In [14], the PLS for the mmWave channels has been studied for the multiuser MISO systems while the MU-MIMO with relaying has been studied in [15,16]. In [17], the PLC of mmWave systems with different secure on–off transmission strategies including capacity threshold-based and secrecy guard zone based schemes has been investigated in the presence of randomly distributed eavesdroppers. [18–20] examined efficient secure hybrid beamformer design algorithms for single cell scenarios.

In this paper, we focus on the multicell systems where the interference between the cells is taken into account for the secure MU-MIMO mmWave communications when the eavesdropper's CSI is not known. We employ hybrid beamforming techniques and apply the AN to enhance the secrecy of the system for the B5G applications. We also assume that the legitimate users' CSI is perfectly available. Under imperfect CSI, the misalignment beamforming on the desired direction causes a noise leakage to the legitimate users' channel which reduces the secrecy rate.

Our contributions can be summarized as followings:

1. Based on the three dimension (3D) mmWave channel model, we present a multicell scenario for a secure MU-MIMO by employing hybrid beamforming at the BSs, legitimate users, and eavesdropper.
2. We design the AN and both the analog and digital beamformers for the secure multicell MU-MIMO mmWave communications. For the beamforming designs, we employ the signal to leakage plus noise ratio (SLNR) based precoder for cooperative multicell processing (CoMP) case whereas MRT, ZF, and random beamformer (RB) precoders for non-CoMP case.
3. We demonstrate the performance of the proposed secure multicell mmWave MU-MIMO communications system based on the secrecy rate and the secrecy outage probability and provide the computational complexity of different beamforming techniques.

The remainder of the paper is organized as follows. The system model covering with the mmWave channel model is given in Section 2. The proposed scheme for the secure multicell mmWave multiuser MIMO communications is described in detail in Section 3. The performance evaluations are provided in Section 4, followed by conclusions in Section 5.

Notations. We use the following notations throughout the paper. The uppercase bold letter $\mathbf{A}$ is matrix, the lowercase bold letter $\mathbf{a}$ is vector and the lowercase letter a is scalar. $\|\cdot\|_F$ represents the Frobenius norm while $|\cdot|$ indicates the determinant. $(\cdot)^{-1}$, $(\cdot)^T$ and $(\cdot)^H$ denotes the inverse, transpose and conjugate transpose operator, respectively.

2. System model

The system model whose the frequency reuse factor is equal to 1 is depicted in Fig. 1 including J BSs in total. Each BS is equipped with N_T antennas and N_{RF} radyo frequency (RF) chains. There are totally K legitimate users with G legitimate users in each cell where $G = K/J$. Each user is equipped with N_R antennas and M_{RF} RF chains that satisfies $N_{RF} \gg M_{RF}$ for practicable scenario. All BSs and legitimate users employ hybrid beamforming scheme which is highly suitable and efficient for the large antenna system scenarios and mmWave communications. The eavesdropper having multiple antennas attempts to obtain information from the legitimate users under the assumption that the eavesdropper share some angle of departure (AoDs) of the legitimate users' channel.

2.1. mmWave channel model

The 3D statistical spatial channel model (SSCM) for the mmWave MIMO system is considered [21]. Since the mmWave channel is known as sparse channel where the propagation tends to be *line-of-sight* (LoS), there are only limited number of resolvable paths including LoS and highly correlated *non-line-of-sight* (nLoS). Besides there is a strong attenuation in the mmWave frequencies due to high path loss compared to sub-6GHz frequencies [22]. From the LoS dominant point of view, the mmWave channel model is defined by [23],

$$\mathbf{H} = \mathbf{H}_{LoS} + \mathbf{H}_{nLoS} \tag{1}$$

where $\mathbf{H}_{LoS}$ denotes the LoS component:

$$\mathbf{H}_{LoS} = \rho_{LoS} \cdot \alpha_{LoS} \cdot \mathbf{a}(\varphi_{LoS}^{Rx}, \theta_{LoS}^{Rx}) \cdot \mathbf{a}^H(\varphi_{LoS}^{Tx}, \theta_{LoS}^{Tx}) \tag{2}$$

$\mathbf{H}_{nLoS}$ is the nLoS component:

$$\mathbf{H}_{nLoS} = \frac{1}{\sqrt{\sum_{c=1}^{C} S_c}} \sum_{c=1}^{C} \sum_{s=1}^{S_c} \rho_c \cdot \alpha_{c,s} \cdot \mathbf{a}(\varphi_{c,s}^{Rx}, \theta_{c,s}^{Rx}) \cdot \mathbf{a}^H(\varphi_{c,s}^{Tx}, \theta_{c,s}^{Tx}) \tag{3}$$

Here, C and S_c denotes the number of clusters and the number of subpaths in each cluster, respectively. ρ is the power of portion while the instantaneous complex coefficient of each subpath is represented by α. Moreover, φ and θ indicate the azimuth angles and the elevation angles and $\mathbf{a}(\varphi, \theta)$ denotes angle of arrival (AoA) or angle of departure (AoD) array responses which correspond to the receiver and the transmitter, respectively [23].

The probability of a link being in LoS condition is given by [21],

$$P_{\text{LoS}}(d) = \left[\min\left(\frac{27}{d}, 1\right)\left(1 - e^{-\frac{d}{71}}\right) + e^{-\frac{d}{71}}\right]^2 \tag{4}$$

where d is the distance between the transmitter and receiver. In this case, when the distance between the transmitter and receiver is less than 27 m, LoS definitely occurs except that there is no blockage in the environment.

In the MIMO system, both the uniform linear array (ULA) and the uniform planar array (UPA) configuration can be used by considering array factor $\mathbf{a}(\varphi, \theta)$. Although the ULA is simpler and more practical, the UPA must be taken into account for the large scale antenna arrays especially square and rectangular ones. Since we consider only UPA, the antenna array response is defined by [23],

$$\mathbf{a}(\varphi, \theta) = \frac{1}{\sqrt{MN}}[1 \ldots, e^{j[(m-1)\Psi_1 + (n-1)\Psi_2]}, \ldots, e^{j[(M-1)\Psi_1 + (N-1)\Psi_2]}]^T \tag{5}$$

where Ψ_1 and Ψ_2 are defined as,

$$\begin{aligned} \Psi_1 &= \frac{2\pi}{\lambda} d_x \cos(\varphi)\sin(\theta) \\ \Psi_2 &= \frac{2\pi}{\lambda} d_y \sin(\varphi)\sin(\theta) \end{aligned} \tag{6}$$

where M and N are the number of antennas in the horizontal axis and in vertical axis, respectively. λ is the wavelength which

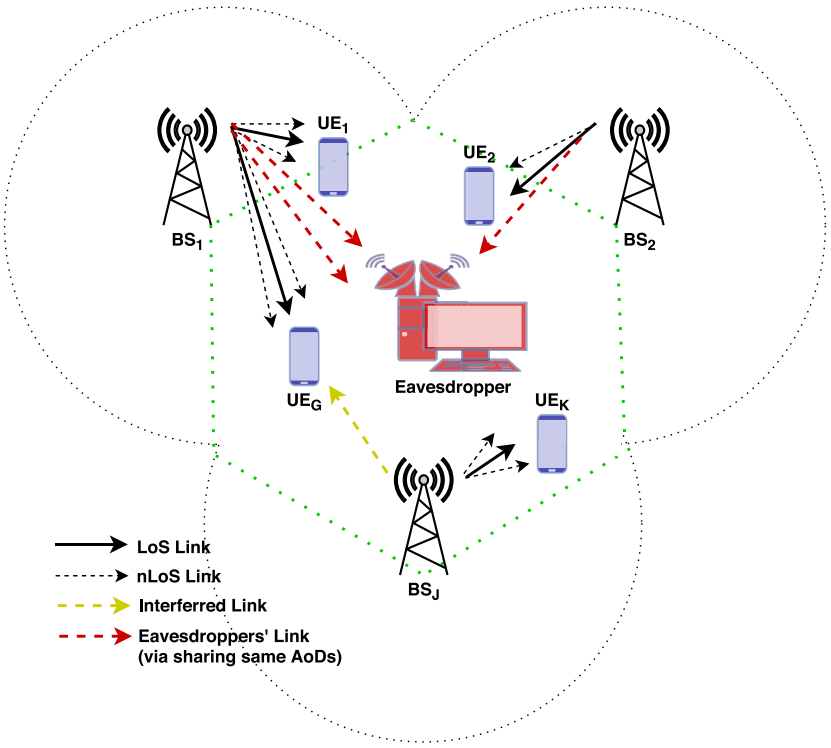


Fig. 1. Secure mmWave multicell MU-MIMO downlink communications.

is defined by $\lambda = c/f$ where f is the operating frequency. The inter-element spacing between two adjacent antenna elements for both the horizontal axis and vertical axis are indicated by d_x and d_y, respectively.

3. The proposed secure multicell mmWave MU-MIMO scheme

We propose a secure multicell multiuser MIMO mmWave system employing hybrid beamforming as shown in Fig. 2. The digital precoder at the jth BS is defined by $\mathbf{F}^j_{DB} \in \mathbb{C}^{N_{RF}\times N_s}$ while the analog precoder is defined by $\mathbf{F}^j_{AB} \in \mathbb{C}^{N_T\times N_{RF}}$ where N_s indicate the total number of streams sent from the BS to the legitimate users. On the other side, the digital combiner and the analog combiner for the gth legitimate user in the jth BS are defined by $\mathbf{W}^j_{DB,g} \in \mathbb{C}^{M_{RF}\times n_s}$ and $\mathbf{W}^j_{AB,g} \in \mathbb{C}^{N_R\times M_{RF}}$, respectively. The number of data stream per user is denoted by n_s.

Using hybrid architecture, the transmit signal $\widetilde{\mathbf{x}}^j \in \mathbb{C}^{N_T\times 1}$ at the jth BS can be defined as,

$$\widetilde{\mathbf{x}}^j = \sqrt{\phi^j}\mathbf{F}^j_{AB}\mathbf{F}^j_{DB}\mathbf{s}^j + \sqrt{1-\phi^j}\mathbf{F}^j_{AN}\mathbf{z}^j \tag{7}$$

where $\mathbf{F}^j_{AB} = \left[\mathbf{F}^j_{AB,1},\ldots,\mathbf{F}^j_{AB,g},\ldots,\mathbf{F}^j_{AB,G}\right]$ and $\mathbf{F}^j_{DB} = \left[\mathbf{F}^j_{DB,1},\ldots,\mathbf{F}^j_{DB,g},\ldots,\mathbf{F}^j_{DB,G}\right]$ are the concatenated analog and digital precoders, respectively. ϕ^j is denoted as the power allocation factor between the precoders of legitimate users and AN precoder.

Furthermore, the received signal by the kth legitimate user out of K legitimate users from the jth BS out of J BSs can be given:

$$\begin{aligned}\mathbf{y}^j_k &= \sqrt{\phi^j P^j_k}(\mathbf{W}^j_{DB,k})^H(\mathbf{W}^j_{AB,k})^H\mathbf{H}^j_k\mathbf{F}^j_{AB,k}\mathbf{F}^j_{DB,k}\mathbf{s}^j_k \\ &+ \sum_{\substack{g\neq k\\ g=1}}^{G}\sqrt{\phi^j P^j_k}(\mathbf{W}^j_{DB,k})^H(\mathbf{W}^j_{AB,k})^H\mathbf{H}^j_k\mathbf{F}^j_{AB,g}\mathbf{F}^j_{DB,g}\mathbf{s}^j_g \\ &+ \sum_{\substack{i\neq j\\ i=1}}^{J}\sum_{n=1}^{G}\sqrt{\phi^i P^i_n}(\mathbf{W}^j_{DB,k})^H(\mathbf{W}^j_{AB,k})^H\mathbf{H}^i_k\mathbf{F}^i_{AB,n}\mathbf{F}^i_{DB,n}\mathbf{s}^i_n \\ &+ \sqrt{(1-\phi^j)P^j_k}(\mathbf{W}^j_{DB,k})^H(\mathbf{W}^j_{AB,k})^H\mathbf{H}^j_k\mathbf{F}^j_{AN}\mathbf{z}^j \\ &+ (\mathbf{W}^j_{DB,k})^H(\mathbf{W}^j_{AB,k})^H\mathbf{n}^j_k\end{aligned} \tag{8}$$

where P^j_k is the received power for the kth user at the jth BS. The first line is the desired signal, the second and the third line denote the intra-cell interference and the inter-cell interference, respectively. While the fourth line indicates the AN beamforming, the fifth line indicates the noise. The channel matrix for the kth legitimate user in the jth BS is denoted by $\mathbf{H}^j_k \in \mathbb{C}^{N_R\times N_T}$ and it can be obtained by using the Eq. (1). $\mathbf{n}^j_k$ is the complex Additive White Gaussian Noise (AWGN) whose elements are zero mean and σ^2_k variance, $\mathcal{CN}(0,\sigma^2_k)$. Nevertheless, the received signal by the corresponding eavesdropper is defined as,

$$\begin{aligned}\mathbf{y}^j_{e,k} &= \sqrt{\phi^j P^j_k}(\mathbf{W}^j_{DB,e,k})^H(\mathbf{W}^j_{AB,e,k})^H\mathbf{H}^j_{e,k}\mathbf{F}^j_{AB,k}\mathbf{F}^j_{DB,k}\mathbf{s}^j_k \\ &+ \sqrt{(1-\phi^j)P^j_k}(\mathbf{W}^j_{DB,e,k})^H(\mathbf{W}^j_{AB,e,k})^H\mathbf{H}^j_{e,k}\mathbf{F}^j_{AN}\mathbf{z}^j \\ &+ (\mathbf{W}^j_{DB,e,k})^H(\mathbf{W}^j_{AB,e,k})^H\mathbf{n}^j_{e,k}\end{aligned} \tag{9}$$

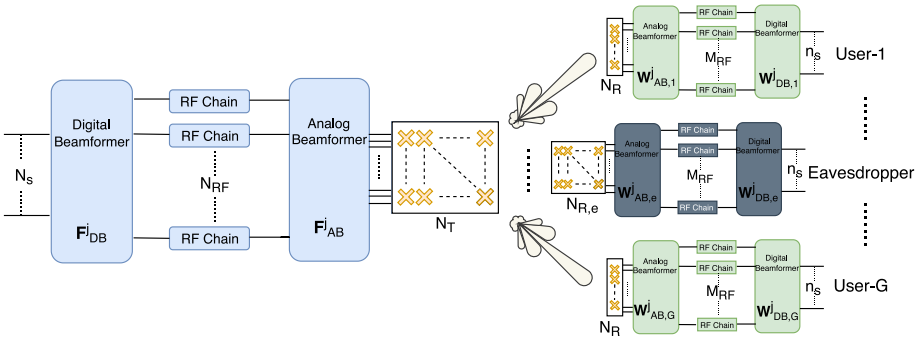


Fig. 2. Hybrid scheme at BS, legitimate users, and eavesdroppers in the jth cell.

where the first row is the intended signal transmitting to the desired legitimate user. The second row is the AN signal that provides to disrupt the eavesdropper channel. The last row indicates the noise. We assume that the eavesdropper can only receive the message signal and AN signal since it is able to cancel out the interfered signals as distinct from the received signals by the legitimate users given in Eq. (9).

In both Eqs. (8) and (9), the analog precoder ($\mathbf{F}^j_{AB,k}$) and combiner ($\mathbf{W}^j_{AB,k}$) matrices for the each legitimate user and the corresponding eavesdropper in the jth BS can be obtained from Algorithm 1 in [24]. Here after, the effective channel matrix for the kth legitimate user in the jth BS is calculated as,

$$\mathbf{H}^j_{eff,k} = (\mathbf{W}^j_{AB,k})^H \mathbf{H}^j_k \mathbf{F}^j_{AB,k} \tag{10}$$

After defining the effective channel, the next step is to design the digital precoders using the effective channel matrix for each legitimate user. The digital combiner for the kth legitimate user in the jth BS, $\mathbf{W}^j_{DB,k}$ are chosen as maximum ratio combiner (MRC) that can be obtained by,

$$\mathbf{W}^j_{DB,k} = \frac{\mathbf{H}^j_{eff,k}\mathbf{F}^j_{DB,k}}{\|\mathbf{H}^j_{eff,k}\mathbf{F}^j_{DB,k}\|_F} \tag{11}$$

Furthermore, the digital combiner for the corresponding eavesdropper, $\mathbf{W}^j_{DB,e,k}$ can be calculated as,

$$\mathbf{W}^j_{DB,e,k} = \frac{(\mathbf{W}^j_{AB,e,k})^H \mathbf{H}^j_{e,k}\mathbf{F}^j_{AB,k}\mathbf{F}^j_{DB,k}}{\|(\mathbf{W}^j_{AB,e,k})^H \mathbf{H}^j_{e,k}\mathbf{F}^j_{AB,k}\mathbf{F}^j_{DB,k}\|_F} \tag{12}$$

Before introducing the multicell digital precoding techniques, we define the SINR of each legitimate user and corresponding eavesdropper as,

$$\boldsymbol{\gamma}^j_k = (\mathbf{D}^j_k + \mathbf{D}^j_{AN,k} + \mathbf{R}^j_{kk})^{-1} \Big[\phi^j P^j_k (\mathbf{W}^j_{DB,k})^H (\mathbf{W}^j_{AB,k})^H \mathbf{H}^j_k \mathbf{F}^j_{AB,k} \mathbf{F}^j_{DB,k} (\mathbf{F}^j_{DB,k})^H (\mathbf{F}^j_{AB,k})^H (\mathbf{H}^j_k)^H \mathbf{W}^j_{AB,k} \mathbf{W}^j_{DB,k}\Big] \tag{13}$$

where $\boldsymbol{\gamma}^j_k$ stands for the SINR of the kth legitimate user in the jth BS and $\mathbf{D}^j_k$ is the interference matrix for the kth legitimate user at the jth BS that is defined as,

$$\mathbf{D}^j_k = (\mathbf{W}^j_{DB,k})^H (\mathbf{W}^j_{AB,k})^H \left(\sum_{\substack{g\neq k \\ g=1}}^{G} \phi^j P^j_k \mathbf{H}^j_k \mathbf{F}^j_{AB,g} \mathbf{F}^j_{DB,g} (\mathbf{F}^j_{DB,g})^H (\mathbf{F}^j_{AB,g})^H (\mathbf{H}^j_k)^H + \sum_{\substack{i\neq j \\ i=1}}^{J} \sum_{n=1}^{G} \phi^i P^i_n \mathbf{H}^i_k \mathbf{F}^i_{AB,n} \mathbf{F}^i_{DB,n} (\mathbf{F}^i_{DB,n})^H (\mathbf{F}^i_{AB,n})^H (\mathbf{H}^i_k)^H \right) \mathbf{W}^j_{AB,k} \mathbf{W}^j_{DB,k} \tag{14}$$

where $\mathbf{D}^j_{AN,k}$ in the Eq. (13) is the AN precoder which propagates from the jth BS for the kth legitimate user can be defined as,

$$\mathbf{D}^j_{AN,k} = (1-\phi^j) P^j_k (\mathbf{W}^j_{DB,k})^H (\mathbf{W}^j_{AB,k})^H \mathbf{H}^j_k \mathbf{F}^j_{AN} (\mathbf{F}^j_{AN})^H (\mathbf{H}^j_k)^H \mathbf{W}^j_{AB,k} \mathbf{W}^j_{DB,k} \tag{15}$$

and where $\mathbf{R}^j_{kk}$ in the Eq. (13) is the noise covariance matrix for the kth legitimate user in the jth BS is evaluated as,

$$\mathbf{R}^j_{kk} = (\mathbf{W}^j_{DB,k})^H (\mathbf{W}^j_{AB,k})^H \mathbf{W}^j_{AB,k} \mathbf{W}^j_{DB,k} \tag{16}$$

Similarly, the SINR of corresponding eavesdropper for the kth legitimate user in the jth BS can be obtained by using Eq. (12) as,

$$\boldsymbol{\gamma}^j_{e,k} = (\mathbf{D}^j_{AN,e,k} + \mathbf{R}^j_{ee,kk})^{-1} \Big[\phi^j P^j_k (\mathbf{W}^j_{DB,e,k})^H (\mathbf{W}^j_{AB,e,k})^H \mathbf{H}^j_{e,k} \mathbf{F}^j_{AB,k} \mathbf{F}^j_{DB,k} (\mathbf{F}^j_{DB,k})^H (\mathbf{F}^j_{AB,k})^H (\mathbf{H}^j_{e,k})^H \mathbf{W}^j_{AB,e,k} \mathbf{W}^j_{DB,e,k}\Big] \tag{17}$$

where $\mathbf{D}^j_{AN,k}$ is the AN precoder which propagates from the jth BS through the eavesdropper is defined as,

$$\mathbf{D}^j_{AN,e,k} = (1-\phi^j) P^j_k (\mathbf{W}^j_{DB,e,k})^H (\mathbf{W}^j_{AB,e,k})^H \mathbf{H}^j_{e,k} \mathbf{F}^j_{AN} (\mathbf{F}^j_{AN})^H (\mathbf{H}^j_{e,k})^H \mathbf{W}^j_{AB,e,k} \mathbf{W}^j_{DB,e,k} \tag{18}$$

and where $\mathbf{R}^j_{ee,kk}$ in the Eq. (17) is the noise covariance matrix of corresponding eavesdropper for the kth legitimate user in the jth BS defined by,

$$\mathbf{R}^j_{ee,kk} = (\mathbf{W}^j_{DB,e,k})^H (\mathbf{W}^j_{AB,e,k})^H \mathbf{W}^j_{AB,e,k} \mathbf{W}^j_{DB,e,k} \tag{19}$$

After that, the data rate of the kth legitimate user in the jth BS can be calculated as,

$$R^j_k = \log_2 \left| \mathbf{I}_{n_s} + \boldsymbol{\gamma}^j_k \right| \tag{20}$$

The corresponding eavesdropper's data rate can be given as,

$$R^j_{e,k} = \log_2 \left| \mathbf{I}_{n_s} + \boldsymbol{\gamma}^j_{e,k} \right| \tag{21}$$

Finally, the average secrecy rate for the kth legitimate user in the jth BS is defined by,

$$R^j_{s,k} = \mathbb{E}\{[R^j_k - R^j_{e,k}]^+\} \tag{22}$$

where $R^j_{s,k}$ is the average secrecy rate of the kth legitimate user in the jth BS and $[x]^+ \triangleq \max\{0, x\}$. The average secrecy sum rate in the multicell is given as,

$$R_s = \sum_{j=1}^{J} \sum_{g=1}^{G} R^j_{s,g} \tag{23}$$

Another metric for measuring to system security is the secrecy outage probability. An outage probability for the kth legitimate user at the jth BS given with threshold secrecy rate (R_{th}) is calculated as,

$$\mathrm{P}_{s,out} = \mathrm{P}(R^j_{s,k} < R_{th}) \tag{24}$$

3.1. The AN design for hybrid beamforming

In this paper, for the multicell MU-MIMO by employing hybrid beamforming at the BSs, legitimate users, and eavesdropper, we propose to generate the AN precoder at the BS at the null-space of both analog and digital precoders.

Then, the AN precoder at the jth BS is the singular value decomposition of the combined precoder matrix such that

$$\bar{\mathbf{U}}\bar{\Sigma}\bar{\mathbf{V}}^H = \bar{\mathbf{F}}^j \tag{25}$$

where $\bar{\mathbf{F}}^j = [(\mathbf{F}^j_{AB,1}\mathbf{F}^j_{DB,1})\dots(\mathbf{F}^j_{AB,G}\mathbf{F}^j_{DB,G})]$. Then, the proposed AN precoder, $\mathbf{F}^j_{AN} \in \mathbb{C}^{N_T \times (N_{RF} - GM_{RF})}$ for the jth BS can be obtained as,

$$\mathbf{F}^j_{AN} = \bar{\mathbf{U}}_{(:,GM_{RF}+1:N_{RF})} \tag{26}$$

3.2. Multicell MIMO precoding techniques

Since we consider the multiple streams and MU-MIMO communication, an appropriate precoding methods are selected to serve multiple users with multiple streams simultaneously. The SLNR based precoding [25] is considered for the CoMP case while the MRT, ZF, and the RB [26–28] precoders are employed for the non-CoMP case.

We select the number of RF chains at users (M_{RF}) is equal to as the number of data streams per user (n_s) for the sake of simplicity. Since we select $n_s = M_{RF}$, we just need M_{RF} RF chains out of N_{RF} RF chains at the BSs for each user. Similarly, we only need n_s streams out of N_s streams at the BSs for each user. Thus, the analog and digital precoder for the kth user in the jth BS should be at the dimensions of $N_T \times M_{RF}$ and $M_{RF} \times n_s$, respectively.

3.2.1. SLNR based precoding (CoMP)

In this case, we assume that there is coordination among the BSs to mitigate the inter-cell and interuser interference while selecting the best beamformer matrix for each user at each cell. Then, $\mathbf{W}^i_{AB,m}$, $\mathbf{H}^i_m$ and $\mathbf{F}^j_{AB,k}$ for $i, j = 1, \dots, J$ and $m, k = 1, \dots, G$ are available at each BS.

For the SLNR based precoder, we first define a new effective channel matrix regarding to leakage for the kth user in the jth BS such that

$$\mathbf{H}^{i,j}_{eff,m,k} = \mathbf{W}^i_{AB,m}\mathbf{H}^i_m\mathbf{F}^j_{AB,k} \tag{27}$$

where $i = 1, \dots, J$ with $(i \neq j)$, and $m = 1, \dots, G$ with $(m \neq k)$.

Then, the leakage matrix $(K-1)M_{RF} \times M_{RF}$ for the kth user in the jth BS can be derived as [25],

$$\dot{\mathbf{H}}^j_k = [(\mathbf{H}^{1,j}_{eff,1,k})^T, \dots, (\mathbf{H}^{i,j}_{eff,m-1,k})^T, (\mathbf{H}^{i,j}_{eff,m+1,k})^T, \dots, (\mathbf{H}^{J,j}_{eff,(K-1),k})^T]^T \tag{28}$$

Since $\mathbb{E}[\mathbf{s}^j_k(\mathbf{s}^j_k)^H] = \mathbf{I}_{n_s}$ and $\mathbb{E}[\mathbf{n}^j_k(\mathbf{n}^j_k)^H] = \sigma^2_k\mathbf{I}_{N_R}$, the normalization factor ζ can be given as [25],

$$\zeta = \frac{\sigma^2_k}{P^j_k}\mathrm{tr}(\mathbf{W}^j_{AB,k}(\mathbf{W}^j_{AB,k})^H) \tag{29}$$

Finally, the digital precoder for the kth user in the jth BS can be calculated by using Eq.(10) and (28) [29] as,

$$\bar{\bar{\mathbf{U}}}\bar{\bar{\Sigma}}\bar{\bar{\mathbf{V}}}^* = \left(\zeta\mathbf{I}_{M_{RF}} + (\dot{\mathbf{H}}^j_k)^H\dot{\mathbf{H}}^j_k\right)^{-1}(\mathbf{H}^j_{eff,k})^H\mathbf{H}^j_{eff,k} \tag{30}$$

$$\mathbf{F}^j_{DB,k} = \bar{\bar{\mathbf{V}}}_{(:,1:n_s)} \tag{31}$$

where $\mathbf{F}^j_{DB,k}$ and the digital precoder of each user should be normalized by its analog counterpart to satisfy the transmit power constraint, $\|\mathbf{F}^j_{AB,k}\mathbf{F}^j_{DB,k}\|^2_F = 1$, such as,

$$\mathbf{F}^j_{DB,k} = \frac{\mathbf{F}^j_{DB,k}}{\|\mathbf{F}^j_{AB,k}\mathbf{F}^j_{DB,k}\|_F} \tag{32}$$

3.2.2. MRT precoding (non-CoMP)

For the MRT scheme, each BS selects its precoding matrix separately without considering intercell and interuser interference. Then, $\mathbf{H}^j_k$ for $k = 1, \dots, G$ are available at each BS j.

Firstly, we define $GM_{RF} \times M_{RF}$ concatenated effective channel matrix for the jth BS as [25],

$$\bar{\mathbf{H}}_j = [(\mathbf{H}^j_{eff,1})^T, \dots, (\mathbf{H}^j_{eff,k})^T, \dots, (\mathbf{H}^j_{eff,G})^T]^T \tag{33}$$

Then, the $M_{RF} \times GM_{RF}$ generalized MRT precoding matrix for the jth BS can be obtained as [25],

$$\mathbf{F}^j_{DB} = \bar{\mathbf{H}}^H_j \tag{34}$$

where $\mathbf{F}^j_{DB} = [\mathbf{F}^j_{DB,1} \dots \mathbf{F}^j_{DB,k} \dots \mathbf{F}^j_{DB,G}]$. Equivalently, MRT precoder of the each user can be obtained by,

$$\mathbf{F}^j_{DB,k} = (\mathbf{H}^j_{eff,k})^H \tag{35}$$

Finally, the MRT precoder for each user must satisfy the transmit power constraint by using Eq. (32).

3.2.3. ZF precoding (non-CoMP)

For the ZF scheme, each BS selects its precoding matrix separately without considering intercell interference. Then, $\mathbf{H}^j_k$ for $k = 1, \dots, G$ are available at each BS j.

Using Eq. (33), the $M_{RF} \times GM_{RF}$ ZF precoding for the jth BS can be defined as,

$$\mathbf{F}^j_{DB} = \bar{\mathbf{H}}^H_j(\bar{\mathbf{H}}_j\bar{\mathbf{H}}^H_j)^{-1} \tag{36}$$

The ZF precoder for each user must satisfy the transmit power constraint so that Eq. (32) should be used.

3.2.4. RB precoding (non-CoMP)

The random beamforming method has been examined by Chung in [26] for the MIMO communications. The main idea is to find the most suitable precoder by using random beamformer generator that maximize the effective SNR (ESNR) of users. In [27] the orthogonal random beamforming and beam selection strategies has been examined for the MIMO communications. Moreover, the random beamforming has been studied for the sparse mmWave channels in [28]. Using random precoders can provide more effective transmission at the BS side because all streams that belongs to each user can be well constructed.

We assume that each BS is able to generate its beamformers randomly and has its own storage or memory to keep them and $\mathbf{H}^j_k$ for $k = 1, \dots, G$ are available at each BS jth.

Firstly, we define a set of N_{pre} candidate precoding vectors is given as,

$$\mathbf{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_{N_{pre}}\} \tag{37}$$

where each precoder, $\mathbf{b}_r$ is a normally distributed complex vector with zero mean and σ^2_r variance with the dimension of $M_{RF} \times 1$. We select the most suitable n_s precoding vectors that maximize the norm of the corresponding effective channel matrix of each user through exhaustive searching on the set of available precoders.

Table 1
Computational Complexity of Beamforming Methods.

Beamforming	Operation	*flops*	$K = 100$ $n_s = 2$ $N_{pre} = 5Kn_s$
ZF	$(\bar{\mathbf{H}}_k^j)^H(\bar{\mathbf{H}}_k^j(\bar{\mathbf{H}}_k^j)^H)^{-1}$	$J[16(Gn_s)^3 - 10(Gn_s)^2 + 8(Gn_s)^2 n_s + 8(Gn_s)n_s^2 + 2(Gn_s) - 2(Gn_s)n_s]$	13.8×10^6
SLNR-CoMP	$svd[(\zeta \mathbf{I}_{n_s} + (\dot{\mathbf{H}}_k^j)^H \dot{\mathbf{H}}_k^j)^{-1}(\mathbf{H}_{eff,k}^j)^H \mathbf{H}_{eff,k}^j]$	$K[16(Ln_s)^3 - 10(Ln_s)^2 + 8(Ln_s)^2 n_s + 8(Ln_s)n_s^2 + 4(Ln_s)] + 8K[21(n_s)^3]$	12.4×10^9
RB	$\arg \max_{n_s} \max_{r=1,\ldots,N_{pre}} \|\|\mathbf{H}_{eff,k}^j \mathbf{b}_r^*\|\|^2$	$J[Gn_s N_{pre}(2n_s^2 + 2n_s)]$	2.4×10^6

Table 2
Simulation parameters.

Parameter	Description	Value
f	Operating frequency	73 GHz SSCM in [21]
N_T	Number of antennas at BSs	256
N_R	Number of antennas at Legitimate Users	16
$N_{R,e}$	Number of antennas at Eavesdroppers	64
J	Total number of BSs	3
K	Total number of users	[45,90]
G	Number of users in each BS	K/J
N_{pre}	Number of available random precoders	$5Kn_s$
n_s	Number of data streams for each user	[1,2]
N_s	Number of data streams for BS	Gn_s
M_{RF}	Number of RF chains at users	n_s
N_{RF}	Number of RF chains at BSs	64

Then, for $n = 1, \ldots, n_s$, the precoder is selected by,

$$\mathbf{b}_n^* = \max_{r=1,\ldots,N_{pre}} \|\mathbf{H}_{eff,k}^j \mathbf{b}_r\|^2 \tag{38}$$

For the kth user in the jth BS, the digital precoder can be obtained as,

$$\mathbf{F}_{DB,k}^j = \left[\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_{n_s}^*\right] \tag{39}$$

where $\mathbf{F}_{DB,k}^j$ should be normalized by Eq. (32) to satisfy the transmit power constraint.

3.2.5. Complexity analysis

The computational complexity is a crucial metric for many real-time applications. Thus, we take into account the complexity of the different beamforming methods considered in this work. To determine computational complexity, we use *flops* which is floating point defined in [30]. The flops calculation for the ZF precoder and the SVD computation are described in [12]. We further extend it for flops computation of SLNR based precoder and also compute the flops computation of the RB based on the norm calculation determined in [31].

The required flops calculation for the different precoder techniques are given in Table 1 where $L = (K-1)/(J/3)$. As listed in Table 1, the CoMP based precoder has higher computational complexity than non-CoMP precoders.

Nonetheless, the CoMP based SLNR precoder is getting more computationally heavy when the system becomes large. In other words, when the users requires higher number of streams or the number of BSs and/or users is increased, SLNR based precoder becomes inefficient in terms of computational complexity. Furthermore, the ZF precoder is also computationally complex since it needs an inverse operation on the concatenated effective channel matrix. On the other side, the MRT is the simplest one however it cannot mitigate the interference. Thus, the RB precoder can be selected as a good alternative in terms of computational complexity.

3.3. The proposed algorithm

In the secure multicell MU-MIMO mmWave communications, we design for both analog and digital beamforming matrices and apply the AN beamforming to enhance the secrecy of the system. In the considered system, there is only one eavesdropper having multiple antennas, and the eavesdropper behaves as a passive receiver that hides its presence and its CSI. We employ different linear beamforming techniques including both CoMP and non-CoMP cases under the assumption that the eavesdropper' CSI is not known and the legitimate users' CSI is perfectly available. The proposed secure scheme is summarized in Algorithm 1.

Algorithm 1 The Secure Multicell mmWave MU-MIMO Algorithm

1: Inputs: The channel state information, $\mathbf{H}_k^j$.
2: Obtain the analog precoder and combiner, $\mathbf{F}_{AB,k}^j$ and $\mathbf{W}_{AB,k}^j$ for the legitimate users and $\mathbf{W}_{AB,e,k}^j$ for the eavesdropper via Algorithm 1 in [24].
3: Calculate the effective channel, $\mathbf{H}_{eff,k}^j$ in Eq. (10) for non-CoMP case and Eq. (27) for CoMP case.
4: Find the digital precoder, $\mathbf{F}_{DB,k}^j$
- Use Eqs. (30) and (31) for the SLNR.
- Use Eq. (35) for the MRT.
- Use Eq. (36) for the ZF.
- Use Eqs. (38) and (39) for the RB.

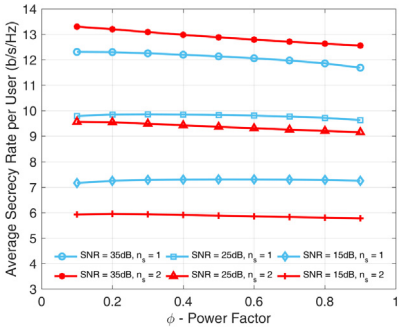
5: Normalize the digital precoder to satisfy transmit power constraint as in Eq. (32).
6: Find the digital combiners $\mathbf{W}_{DB,k}^j$ in Eq. (11) and $\mathbf{W}_{DB,e,k}^j$ in Eq. (12).
7: Determine the AN precoder $\mathbf{F}_{AN}^j$ in Eqs. (25) and (26).

4. Performance evaluations

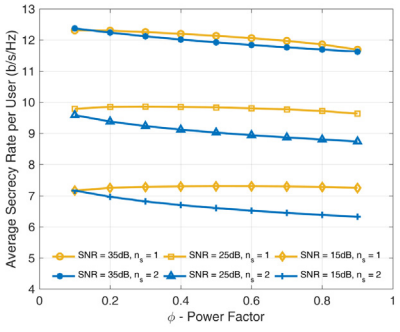
We provide the simulation results to illustrate the system performance in terms of the sum data rate, the secrecy sum rate and the secrecy outage probability. The simulation parameters are given in Table 2. We assume that the RB precoders for each BS are initially generated and stored in a memory to reduce computational complexity. Finally, the performance evaluations are provided through the Monte Carlo simulations.

In Fig. 3, the power allocation factor between the legitimate users precoder and the AN is shown for different beamforming and $K = 90$. The power allocation value is determined for each precoder uniquely and it can be further obtained for different number of legitimate users by similar way. Nevertheless, the SLNR gives better performance when $n_s = 2$ at high SNR regime. It is also noted that giving less power to the MRT and more power to the AN can enhance the secrecy since the MRT improves the data rate performance especially in the low SNR region.

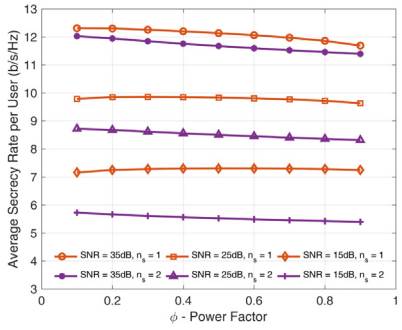
In Fig. 4, the average sum data rate is shown for the comparison of different beamforming techniques both for $K = 45$



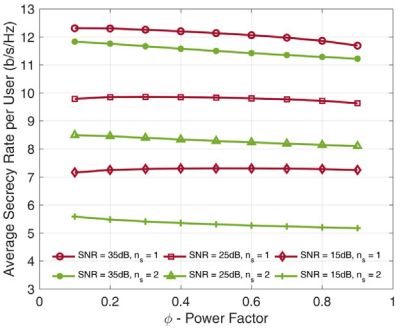
(a) Average secrecy rate per user vs ϕ for SLNR.



(b) Average secrecy rate per user vs ϕ for MRT.



(c) Average secrecy rate per user vs ϕ for ZF.



(d) Average secrecy rate per user vs ϕ for RB.

Fig. 3. Average secrecy rate per user vs ϕ for different precoders with K = 90.

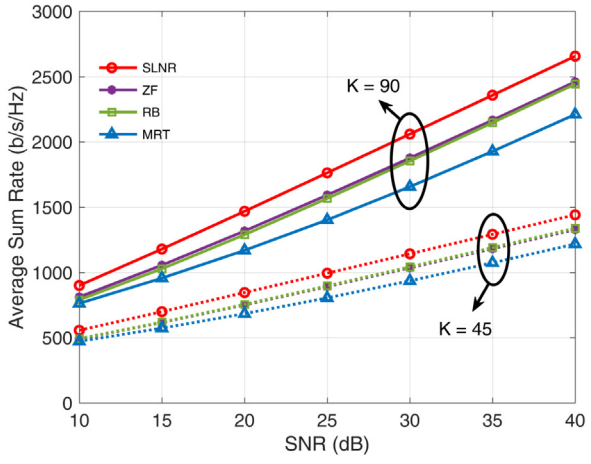


Fig. 4. Average sum rate vs SNR for $n_s = 2$.

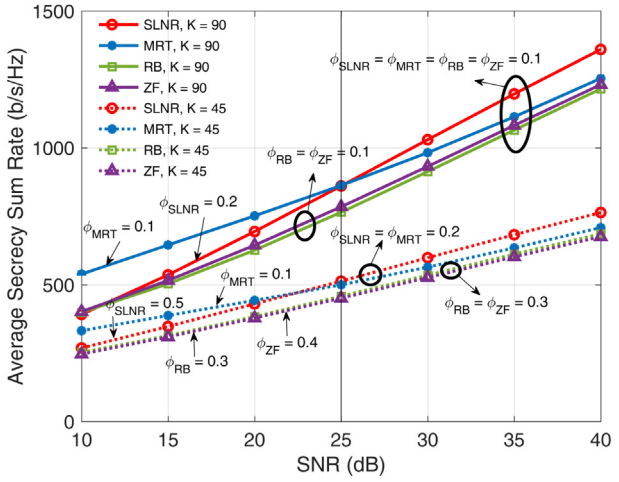


Fig. 5. Average secrecy sum rate vs SNR for different precoders with optimum ϕ.

and $K = 90$ legitimate users using $n_s = 2$ without considering secrecy. The SLNR precoder gives the best sum data rate performance while the MRT provides the worst one. The CoMP based SLNR utilizes the coordination of BSs to prevent information leakage. However, the MRT cannot mitigate this leakage. It is also worth noting that the RB precoders outperform the MRT and give the same results as the ZF precoder.

In Fig. 5, the average secrecy sum rate is given for different precoding techniques with their optimum power allocation values.The secrecy sum rate enhances as the number of users increases. While the SINR performs the best secrecy sum rate at the high SNR region, the MRT gives the best performance at the low SNR region. For LoS dominant small-cell mmWave communication with large antenna arrays at the BSs, the MRT precoder can be selected to satisfy the secrecy requirements. Even though the RB gives the same secrecy rate as the ZF precoder, the performance of ZF precoder is getting better than the RB precoder when the user densities becomes larger.

Figs. 6 and 7 provides the secrecy outage probability for two different threshold rates and different precoders considering their optimal power allocation values determined by Fig. 3. The MRT

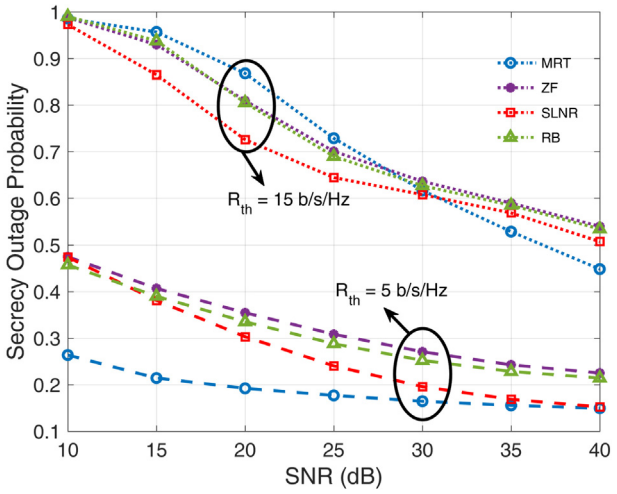


Fig. 6. Secrecy outage probability vs SNR for $K = 45$ and $n_s = 2$ with $\phi = 0.2$.

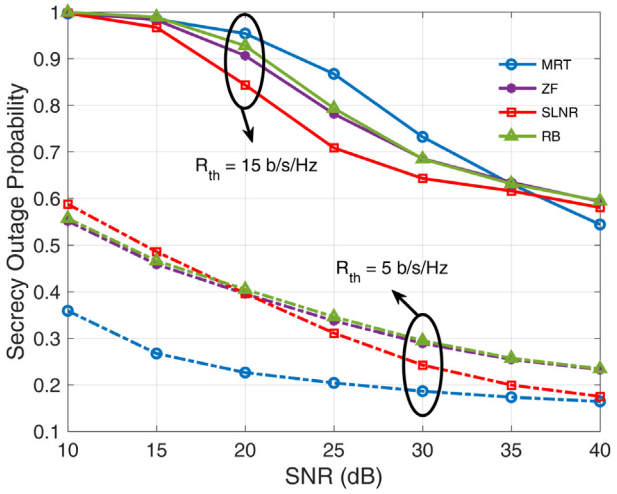


Fig. 7. Secrecy outage probability vs SNR for K = 90 and $n_s = 2$ with $\phi = 0.1$.

precoder improves secrecy outage at low threshold rates however its performance is getting worse at high threshold rates since the interference becomes dominant. Moreover, the SLNR precoder gives the best performance at higher threshold rates.

For each precoder technique, the computational complexity is given in Fig. 8. The SLNR has the highest computational complexity while it gives the best performance in terms of data rate and secrecy rate. On the other side, the computational complexity of the ZF precoder is getting high when the number of users increases. Hence, the RB provides almost the same performance as the ZF precoder while having less complexity for the MU-MIMO mmWave communication systems.

5. Conclusion

In this paper, we have proposed different beamforming strategies for the physical layer security in the mmWave MU-MIMO networks considering multiple streams transmission. We have considered the hybrid scheme at both the BS and the legitimate users to design power-efficient system without compromising the number of antennas and the directivity. In the considered framework, we have proposed to obtain the AN precoder from the null-space of jointly designed digital and analog precoders. It has been demonstrated that the overall system performance highly

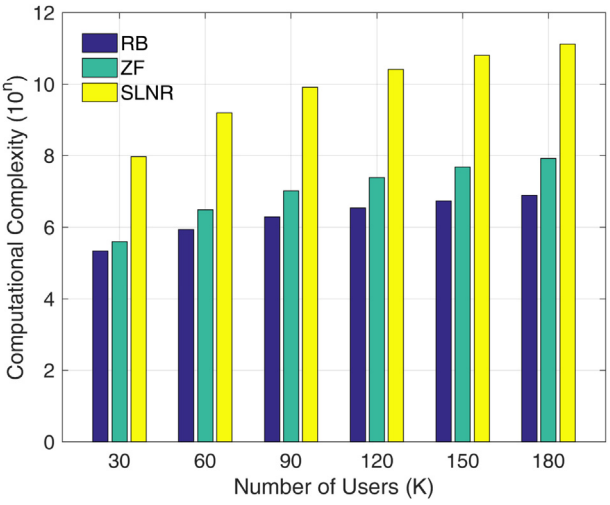


Fig. 8. Complexity vs K for different precoders with $J = 3$ and $n_s = 2$.

depends on the number of streams and the power allocation factor which is between the legitimate users precoder and AN precoder.

Considering the multiple streams, the SLNR gives the best secrecy sum-rate performance since it utilizes the coordination among the BSs, while the MRT gives the best secrecy outage performance for low threshold rates at low SNR regimes. On the other hand, the ZF and the RB precoding give almost the same performance for both the secrecy sum rate and the secrecy outage probability. Although the coordination among BSs plays a huge impact on the performance of the system, the computational complexity is getting high when both the number of users and streams increases. For higher number of users, it can be more wisely to choose the RB precoder while improving the secrecy with moderate computational complexity.

As future work, the proposed framework can be extended to the non-orthogonal multiple access (NOMA) based MU-MIMO in mmWave communications.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work has been funded by the European Union Horizon 2020. RISE 2018 scheme (H2020-MSCA-RISE-2018) under the Marie Skłodowska-Curie grant agreement No. 823903 (RECENT).

References

[1] T.S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G.N. Wong, J.K. Schulz, M. Samimi, F. Gutierrez, Millimeter wave mobile communications for 5G cellular: It will work!, IEEE Access 1 (2013) 335–349.

[2] A. Alkhateeb, J. Mo, N. Gonzalez-Prelcic, R.W. Heath, MIMO precoding and combining solutions for millimeter-wave systems, IEEE Commun. Mag. 52 (12) (2014) 122–131.

[3] F. Sohrabi, W. Yu, Hybrid digital and analog beamforming design for large-scale antenna arrays, IEEE J. Sel. Top. Sign. Proces. 10 (3) (2016) 501–513.

[4] A.F. Molisch, V.V. Ratnam, S. Han, Z. Li, S.L.H. Nguyen, L. Li, K. Haneda, Hybrid beamforming for massive MIMO: A survey, IEEE Commun. Mag. 55 (9) (2017) 134–141.

[5] I. Ahmed, H. Khammari, A. Shahid, A. Musa, K.S. Kim, E. De Poorter, I. Moerman, A survey on hybrid beamforming techniques in 5G: Architecture and system model perspectives, IEEE Commun. Surv. Tutor. 20 (4) (2018) 3060–3097.
[6] A. Khisti, G.W. Wornell, Secure transmission with multiple antennas part I: The MISOME wiretap channel, IEEE Trans. Inform. Theory 56 (7) (2010) 3088–3104.
[7] A. Khisti, G.W. Wornell, Secure transmission with multiple antennas part II: The MIMOME wiretap channel, IEEE Trans. Inform. Theory 56 (11) (2010) 5515–5532.
[8] A. Mukherjee, S.A.A. Fakoorian, J. Huang, A.L. Swindlehurst, Principles of physical layer security in multiuser wireless networks: A survey, IEEE Commun. Surv. Tutor. 16 (3) (2014) 1550–1573.
[9] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, X. Gao, A survey of physical layer security techniques for 5G wireless networks and challenges ahead, IEEE J. Sel. Areas Commun. 36 (4) (2018) 679–695.
[10] D.W.K. Ng, E.S. Lo, R. Schober, Robust beamforming for secure communication in systems with wireless information and power transfer, IEEE Trans. Wireless Commun. 13 (8) (2014) 4599–4615.
[11] J. Zhu, R. Schober, V.K. Bhargava, Secure transmission in multicell massive MIMO systems, IEEE Trans. Wireless Commun. 13 (9) (2014) 4766–4781.
[12] M. Sadeghzadeh, M. Maleki, M. Salehi, H.R. Bahrami, Large-scale analysis of physical-layer security in multi-user wireless networks, IEEE Trans. Commun. 66 (12) (2018) 6450–6462.
[13] D. Wang, B. Bai, W. Zhao, Z. Han, A survey of optimization approaches for wireless physical layer security, IEEE Commun. Surv. Tutor. 21 (2) (2018) 1878–1911.
[14] Y. Ju, H.-M. Wang, T.-X. Zheng, Q. Yin, Secure transmissions in millimeter wave systems, IEEE Trans. Commun. 65 (5) (2017) 2114–2127.
[15] S. Wang, X. Xu, K. Huang, X. Ji, Y. Chen, L. Jin, Artificial noise aided hybrid analog-digital beamforming for secure transmission in MIMO millimeter wave relay systems, IEEE Access 7 (2019) 28597–28606.
[16] R. Ma, W. Yang, X. Sun, L. Tao, T. Zhang, Secure communication in millimeter wave relaying networks, IEEE Access 7 (2019) 31218–31232.
[17] W. Yang, L. Tao, X. Sun, R. Ma, Y. Cai, T. Zhang, Secure on-off transmission in mmWave systems with randomly distributed eavesdroppers, IEEE Access 7 (2019) 32681–32692.
[18] X. Tian, Q. Liu, Z. Wang, M. Li, Secure hybrid beamformers design in mmWave MIMO wiretap systems, IEEE Syst. J. 14 (1) (2020) 548–559.
[19] S. Huang, Y. Ye, M. Xiao, Hybrid beamforming for millimeter wave multi-user MIMO systems using learning machine, IEEE Wirel. Commun. Lett. 9 (11) (2020) 1914–1918, http://dx.doi.org/10.1109/LWC.2020.3007990.
[20] O. Erdoğan, B. Özbek, S.A. Busari, J. Gonzalez, Hybrid beamforming for secure multiuser mmWave MIMO communications, in: 2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications, 2020, pp. 1–6.
[21] M.K. Samimi, T.S. Rappaport, 3-D millimeter-wave statistical channel model for 5G wireless system design, IEEE Trans. Microw. Theory Tech. 64 (7) (2016) 2207–2225.
[22] A.L. Swindlehurst, E. Ayanoglu, P. Heydari, F. Capolino, Millimeter-wave massive MIMO: The next wireless revolution? IEEE Commun. Mag. 52 (9) (2014) 56–62.
[23] I.A. Hemadeh, K. Satyanarayana, M. El-Hajjar, L. Hanzo, Millimeter-wave communications: Physical channel models, design considerations, antenna constructions, and link-budget, IEEE Commun. Surv. Tutor. 20 (2) (2017) 870–913.
[24] O. El Ayach, S. Rajagopal, S. Abu-Surra, Z. Pi, R.W. Heath, Spatially sparse precoding in millimeter wave MIMO systems, IEEE Trans. Wirel. Commun. 13 (3) (2014) 1499–1513.
[25] S. Sun, T.S. Rappaport, M. Shaft, Hybrid beamforming for 5G millimeter-wave multi-cell networks, in: IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS, IEEE, 2018, pp. 589–596.
[26] J. Chung, C.-S. Hwang, K. Kim, Y.K. Kim, A random beamforming technique in MIMO systems exploiting multiuser diversity, IEEE J. Sel. Areas Commun. 21 (5) (2003) 848–855.
[27] J.L. Vicario, R. Bosisio, C. Anton-Haro, U. Spagnolini, Beam selection strategies for orthogonal random beamforming in sparse networks, IEEE Trans. Wireless Commun. 7 (9) (2008) 3385–3396.
[28] G. Lee, Y. Sung, M. Kountouris, On the performance of random beamforming in sparse millimeter wave channels, IEEE J. Sel. Top. Sign. Proces. 10 (3) (2016) 560–575.
[29] M. Sadek, A. Tarighat, A.H. Sayed, A leakage-based precoding scheme for downlink multi-user MIMO channels, IEEE Trans. Wirel. Commun. 6 (5) (2007) 1711–1721.
[30] G.H. Golub, C.F. Van Loan, Matrix Computations, Vol. 3, JHU Press, 2012.
[31] Z. Shen, R. Chen, J.G. Andrews, R.W. Heath, B.L. Evans, Low complexity user selection algorithms for multiuser MIMO systems with block diagonalization, IEEE Trans. Signal Process. 54 (9) (2006) 3658–3663.

Berna Özbek is an Associate Professor in Telecommunication field at the Electrical and Electronics Engineering Department of İzmir Institute of Technology, Turkey and is working in the field of wireless communication systems for more than 15 years. She has been awarded as a Marie-Curie Intra-European (EIF) Fellow by European Commission for two years in the project entitled Interference Management Techniques for Multicell Networks on 2010. She has coordinated 1 international and 4 national projects, served as a consultant for 3 Eureka-Celtic projects and 2 national industry driven projects. Under her supervision, 13 master thesis and 2 doctoral dissertations have been completed. Currently, she is supervising 2 Ph.D. and 2 master students and conducting one international project under Horizon2020-MC-RISE programme from 2018 to 2022. She has published more than 90 peer-reviewed papers, 1 book, 1 book chapter and 2 patents. She is serving as a referee for several international journals, on numerous TPCs for IEEE sponsored conferences, European Commission, Turkish Republic of Ministry of Trade and Industry and The Scientific and Technological Research Council of Turkey. Her research interests are interference management, resource allocation, limited feedback links, device-to-device communications, physical layer security, massive MIMO systems, mmWave communications.

Ogulcan Erdogan received the MSc. degree in electrical and electronics engineering from the Izmir Institute of Technology, Izmir, Turkey, in 2020, and he is currently pursuing his Ph.D. degree in the same university. His research interests are the communication theory based on information theory and signal processing perspectives, the large scale complex networks, and methodologies for the next-generation communication systems.

Sherif A. Busari received the B.Eng. and M.Eng. degrees in electrical and electronics engineering from the Federal University of Technology Akure (FUTA), Nigeria, in 2011 and 2015, respectively, and an industry-driven Ph.D. degree in telecommunications engineering from the Universidade de Aveiro, Portugal, in 2020. His research interests focus on technology enablers and system level simulation methodologies for 5G and beyond-5G networks.

Jonathan Gonzalez received the M.Sc. and Ph.D. degrees in telecommunications from the University of Surrey, U.K., in 1999 and 2004, respectively. He then became a Senior Researcher with the University of Surrey, where he was responsible for project development and research on mobile systems. He became an Honorary Senior Researcher with the University of Bradford in 2019. In 2011, he founded GS-Lda, Portugal, targeting R&I on next generation mobile platforms. He has more than 15 years Research and Development experience in mobile communications and practical experimentation. His research interests include simulation methodologies and radio resource management.