2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications: Track 1 - PHY and Fundamentals

Hybrid Beamforming for Secure Multiuser mmWave MIMO Communications

Oğulcan Erdoğan*, Berna Özbek*, Sherif A. Busari‡, and Jonathan Gonzalez‡
*Department of Electrical and Electronics Engineering, Izmir Institute of Technology, Izmir, Turkey
‡GS-Lda, Portugal
{ogulcanerdogan, bernaozbek}@iyte.edu.tr; {sbusari, jonathan}@gs-lda.com

***Abstract*—Secure communication is critical in wireless networks as the networks are prone to eavesdropping from unintended nodes. To address this challenge, physical layer security (PLS) is being employed to combat information leakage. In this paper, we present the performance evaluations based on the secrecy rate and the secrecy outage probability for multiuser multiple-input multiple-output (MIMO) millimeter-wave (mmWave) communications by employing hybrid beamforming (HBF) at the base station, legitimate users and eavesdropper. Using a 3-dimensional mmWave channel model and uniform planar antenna arrays (UPA), we employ artificial noise (AN) beamforming to jam the channels of eavesdropper and to enhance the secrecy rate. The transmitter uses the minimum mean square error (MMSE) precoder to mitigate multiuser interference for the secure MIMO mmWave systems. It is shown that the overall system performance highly depends on the power allocation factor between AN and the signal of legitimate users.**

***Index Terms*—Physical layer security, mmWave communications, hybrid beamforming, MIMO systems.**

I. Introduction

Over the last decade, many advancements have been made in the field of wireless communications. Among the major technology enablers being explored for wireless networks at the physical layer (PHY), a great deal of attention has been focused on mmWave communications, massive MIMO antenna systems and beamforming techniques [1]. These enablers bring to the forefront great opportunities for enhancing the performance of beyond-5G (B5G) networks, with respect to throughput, spectral efficiency, energy efficiency, latency and reliability.

Due to its open nature, wireless communication is prone to information leakage to unintended users. To address this challenge, the concept of PLS is being introduced and explored for wireless communication systems. Along this line, the studies such as [2], [3] have shown that the secrecy of a wireless communication system can be enhanced by PLS methods, in contrast to the conventional cryptographic methods that are more computationally complex.

The PLS via beamforming techniques is being explored for mmWave MIMO systems while they are largely limited to single user (SU) MIMO systems or multiuser (MU) multiple-input single-output (MISO) systems [4]–[7]. To the best of our knowledge, an extension to the multiuser (MU) MIMO case for mmWave communications has not been studied in the open literature. This work, therefore, presents the secure multiuser MIMO systems with multiple streams per user in the mmWave communications.

978-1-7281-4490-0/20/$31.00 © 2020 IEEE

The remainder of this paper is organized as follows. The mmWave channel model is described in Section II. The proposed scenario for the secure multiuser MIMO mmWave communications is given in detail in Section III. The simulation results are provided in Section IV, followed by conclusions in Section V.

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.

II. Millimeter-Wave Channel Model

We consider a three-dimensional (3D) statistical spatial channel model (SSCM) [8] for the mmWave MIMO system. The mmWave channel model composed of the *line-of-sight* (LOS) and the *non-LOS* (NLOS) components is given by [9],

$$\mathbf{H} = \mathbf{H}_{LOS} + \mathbf{H}_{NLOS} \tag{1}$$

where $\mathbf{H}_{LOS}$ denotes the LOS component of the mmWave channel defined as,

$$\begin{aligned}\mathbf{H}_{LOS} =& \sqrt{\rho_{LOS}} \cdot \alpha_{LOS} \cdot \mathbf{a}(\varphi_{LOS}^{Rx}, \theta_{LOS}^{Rx}) \\ & \cdot \mathbf{a}^H(\varphi_{LOS}^{Tx}, \theta_{LOS}^{Tx})\end{aligned} \tag{2}$$

Another component of the mmWave channel in Eq.(1) is the NLOS component, $\mathbf{H}_{NLOS}$ defined as,

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

where C and S_c denote the number of clusters and the number of subpaths in each cluster, respectively. ρ denotes the power portion of each cluster, α represents the instantaneous complex coefficient for each subpath. Moreover, φ and θ indicate the azimuth angles and the elevation angles, respectively. The array factor is denoted by $\mathbf{a}$ which corresponds to either the angle of arrival (AoA) at the receiver or angle of departure (AoD) at the transmitter, respectively.

978-1-7281-4490-0/20/$31.00 ©2020 IEEE

For the MIMO system, the UPA antenna configuration is considered at both transmitter and receiver sides. For the UPA, the array response can be evaluated as [9],

$$\mathbf{a}(\varphi,\theta) = \frac{1}{\sqrt{MN}}[1\ldots, e^{j[(m-1)\Psi_1+(n-1)\Psi_2]}, \ldots, e^{j[(M-1)\Psi_1+(N-1)\Psi_2]}]^T \tag{4}$$

where Ψ_1 and Ψ_2 are defined as,

$$\begin{cases} \Psi_1 = \frac{2\pi}{\lambda} d_x \cos(\varphi)\sin(\theta) \\ \Psi_2 = \frac{2\pi}{\lambda} d_y \sin(\varphi)\sin(\theta) \end{cases} \tag{5}$$

where M and N are the number of antennas in the horizontal axis and vertical axis, respectively. The wavelength is denoted as λ and the inter-element spacing between two adjacent antenna elements both for the horizontal axis and vertical axis are indicated by d_x and d_y, respectively.

III. Proposed Scenario

We propose a small cell (pico, Femto, etc.) MU-MIMO mmWave communication system. In the proposed scenario, we consider a single cell downlink communication system that has only one base station (BS) equipped with N_T antennas serving to K number of legitimate users equipped with N_R antennas. This scenario where each legitimate user communicates with BS over both LOS and NLOS links is a highly proper scenario for small cell networks. Since we assume that there is only one passive eavesdropper assigned to each legitimate user, it tries to gain information from each channel of legitimate users. To hold this assumption, each legitimate user and eavesdropper can share some of their AoDs shown in Figure 1. In addition to that, in this scenario, each node in the cell (BS, legitimate users, and eavesdropper) employs the HBF architecture shown in Figure 2.

Since HBF is considered both at the transmitter and receiver sides, the digital precoder is given as $\overline{\mathbf{F}_{DB}} \in \mathbb{C}^{N_{RF}\times N_s}$ while the analog precoder is given as $\overline{\mathbf{F}_{AB}} \in \mathbb{C}^{N_T\times N_{RF}}$ where N_{RF} and N_s are the number of RF chains and the number of data streams at the transmitter, respectively.

It is assumed that the channel state information (CSI) of eavesdropper is not known at the BS since the eavesdropper is a passive node that wants to hide its presence from the BS. In this case, we utilize AN beamforming to jam the channel of eavesdropper. Then, the transmit signal including AN precoder is given by,

$$\mathbf{x} = \sqrt{\phi}\overline{\mathbf{F}_{AB}\mathbf{F}_{DB}}\mathbf{s} + \sqrt{1-\phi}\mathbf{F}_{AN}\mathbf{z} \tag{7}$$

where $\mathbf{F}_{AN}$ is the AN precoder, $\mathbf{s} \in \mathbb{C}^{N_s\times 1}$ is the transmit symbol such that $\mathbb{E}\{\mathbf{s}\mathbf{s}^H\} = \mathbf{I}_{N_s}$, $\mathbf{z}$ is the artificial noise generated by $\mathcal{CN}(0,1)$ and ϕ is the power allocation factor between $\mathbf{s}$ and $\mathbf{z}$.

Following transmit HBF, we consider HBF scheme at the receiver side as in Figure 2 such that the analog combiner is $\mathbf{W}_{AB} \in \mathbb{C}^{N_R\times M_{RF}}$ and the digital combiner is $\mathbf{W}_{DB} \in \mathbb{C}^{M_{RF}\times n_s}$ where M_{RF} and n_s are the number of RF chains and the number of data streams at the receiver, respectively.

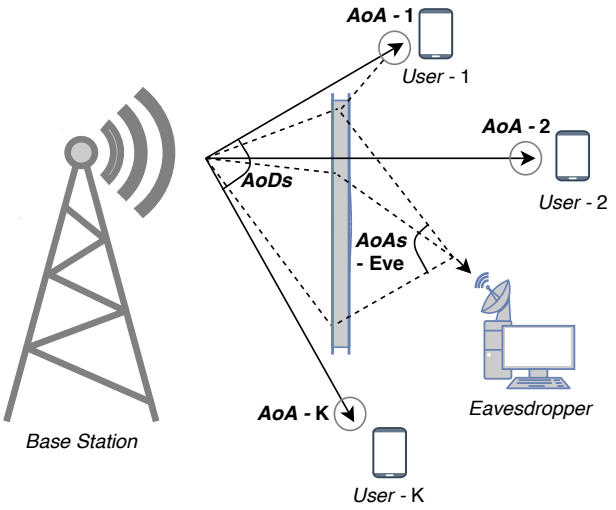

Fig. 1. Single cell donwlink MU-MIMO mmWave communications scenario

For the kth legitimate user, the received signal is given by [10],

$$\begin{aligned} \mathbf{y}_k =& \sqrt{\phi P_k}\mathbf{W}_{DB,k}^H\mathbf{W}_{AB,k}^H\mathbf{H}_k\mathbf{F}_{AB,k}\mathbf{F}_{DB,k}\mathbf{s}_k \\ &+ \sum_{\substack{j=1\\(j\neq k)}}^{K} \sqrt{\phi P_k}\mathbf{W}_{DB,k}^H\mathbf{W}_{AB,k}^H\mathbf{H}_k\mathbf{F}_{AB,j}\mathbf{F}_{DB,j}\mathbf{s}_j \\ &+ \sqrt{(1-\phi)P_k}\mathbf{W}_{DB,k}^H\mathbf{W}_{AB,k}^H\mathbf{H}_k\mathbf{F}_{AN}\mathbf{z} \\ &+ \mathbf{W}_{DB,k}^H\mathbf{W}_{AB,k}^H\mathbf{n}_k \end{aligned} \tag{8}$$

where P_k is the received power, $\mathbf{H}_k \in \mathbb{C}^{N_R\times N_T}$ is the channel between BS and kth legitimate user and $\mathbf{n}_k$ is the complex additive white Gaussian noise (AWGN) with zero mean and σ_k^2 variance. The $\mathbf{W}_{DB,k}$ and $\mathbf{W}_{AB,k}$ are the $M_{RF}\times n_s$ digital combiner and $N_R\times M_{RF}$ analog combiner for the kth legitimate user, respectively.

The proposed scenario, the generalized $N_T\times N_{RF}$ analog precoder and $N_{RF}\times N_s$ digital precoder are denoted by $\overline{\mathbf{F}_{AB}}$ and $\overline{\mathbf{F}_{DB}}$ while $\mathbf{F}_{AB,k}$ and $\mathbf{F}_{DB,k}$ indicate the $N_T\times M_{RF}$ analog precoder and $M_{RF}\times n_s$ digital precoder for the kth legitimate user (where M_{RF} and n_s are selected from N_{RF} and N_s for the corresponding kth legitimate user), respectively. We note that, a reliable communication is performed under the constraint of $KM_{RF} \leq N_{RF}$.

Considering the worst case scenario, it is assumed the eavesdropper has an ability to eliminate the interference among the users. Hence the received signal by the eavesdropper for the kth legitimate user is given as,

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

For the HBF scheme, the first consideration is to find the analog precoder and combiner in such a way that maximizes

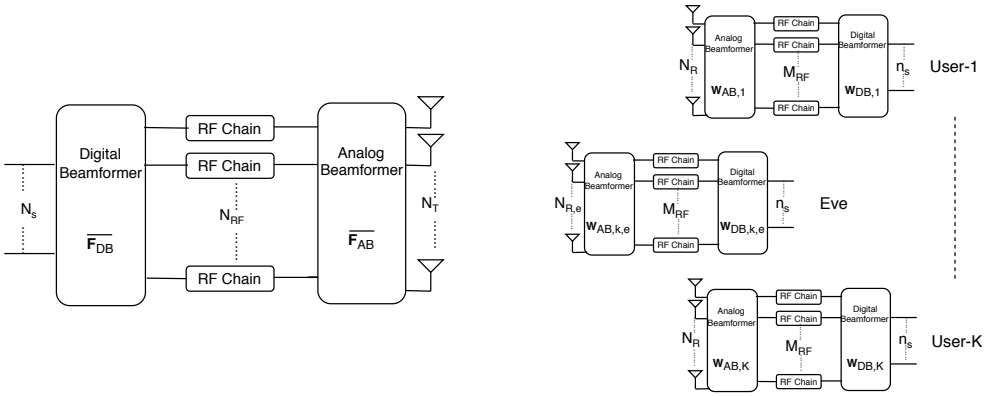

Fig. 2. Hybrid beamforming architecture at the BS, the legitimate users and the eavesdropper

the effective channel by [11],

$$\max ||\mathbf{H}_{eff,k}||_F^2 = \max ||\mathbf{W}_{AB,k}^H \mathbf{H}_k \mathbf{F}_{AB,k}||_F^2 \tag{10}$$

This optimization problem is non-convex and computationally complex for the optimal search of the analog precoder and combiner [12]. In order to convert this problem to a convex problem, a codebook based analog beamformer design can be used. Using codebook based design, $\mathbf{F}_{AB,k}$ and $\mathbf{W}_{AB,k}$ are chosen from corresponding AoDs and AoAs, respectively. In this work, we construct the analog precoders and combiners according to Algorithm 1 as given in [13].

After finding the analog beamformers, the next step is to design the digital beamformers, $\mathbf{F}_{DB,k}$ and $\mathbf{W}_{DB,k}$ for each legitimate user. For the digital precoder, we utilize the MMSE precoder to mitigate the interference among users and streams.

Firstly, the generalized effective channel including the effective channel of each legitimate user is given as,

$$\widetilde{\mathbf{H}} = [\mathbf{H}_{eff,1}^T, \mathbf{H}_{eff,2}^T, \ldots, \mathbf{H}_{eff,K}^T]^T \tag{11}$$

where $\widetilde{\mathbf{H}}$ is concatenated effective channel matrix [10] with dimension of $KM_{RF} \times M_{RF}$. Secondly, the $M_{RF} \times KM_{RF}$ MMSE precoder is defined as,

$$\overline{\mathbf{F}_{DB}} = \widetilde{\mathbf{H}}^H (\widetilde{\mathbf{H}}\widetilde{\mathbf{H}}^H + \beta \mathbf{I}_{KM_{RF}})^{-1} \tag{12}$$

where $\overline{\mathbf{F}_{DB}} = [\mathbf{F}_{DB,1}\, \mathbf{F}_{DB,2} \ldots \mathbf{F}_{DB,K}]$ consists of K legitimate user precoders and β is the regularization factor which is $\frac{1}{\sigma^2}$. In order to satisfy the transmit power constraint such that $||\mathbf{F}_{AB,k}\mathbf{F}_{DB,k}||_F^2 = 1$, each legitimate user precoder should be normalized by,

$$\mathbf{F}_{DB,k} = \frac{\mathbf{F}_{DB,k}}{||\mathbf{F}_{AB,k}\mathbf{F}_{DB,k}||_F} \tag{13}$$

Considering the HBF scheme, we propose to find AN precoder from the null-space of combined with analog and digital precoders of each legitimate user by using singular value decomposition as,

$$\bar{\mathbf{U}}\bar{\mathbf{\Sigma}}\bar{\mathbf{V}}^H = \overline{\mathbf{F}} \tag{14}$$

where $\overline{\mathbf{F}} = [(\mathbf{F}_{AB,1}\mathbf{F}_{DB,1}) \ldots (\mathbf{F}_{AB,K}\mathbf{F}_{DB,K})]$ and the AN precoder can be given as,

$$\mathbf{F}_{AN} = \bar{\mathbf{U}}_{(:,KM_{RF}+1:N_{RF})} \tag{15}$$

It is important to note that we set $M_{RF} = n_s$ to reduce the required time and computation. After finding the digital precoders and AN precoder, the digital combiner for the *k*th legitimate user can be given by,

$$\mathbf{W}_{DB,k} = \frac{\mathbf{H}_{eff,k}\mathbf{F}_{DB,k}}{||\mathbf{H}_{eff,k}\mathbf{F}_{DB,k}||_F} \tag{16}$$

The corresponding digital combiner of eavesdropper can be obtained as,

$$\mathbf{W}_{DB,e,k} = \frac{\mathbf{W}_{AB,e,k}^H \mathbf{H}_{e,k}\mathbf{F}_{AB,k}\mathbf{F}_{DB,k}}{||\mathbf{W}_{AB,e,k}^H \mathbf{H}_{e,k}\mathbf{F}_{AB,k}\mathbf{F}_{DB,k}||_F} \tag{17}$$

where $\mathbf{W}_{AB,e,k}$ is determined by using Eq.(10) based on the channel of eavesdropper.

It is important to note that the Eq.(17) is also the worst case in terms of the secrecy since it is assumed that the eavesdropper knows all the precoding matrices belonging to the legitimate users.

Following all matrices, the signal to interference plus noise ratio (SINR) is evaluated for the *k*th legitimate user in Eq.(18) and the corresponding eavesdropper in Eq.(19) as the top of next page.

Then, the data rate can be calculated for the *k*th legitimate user as,

$$R_k = \log_2 |\mathbf{I}_{n_s} + \boldsymbol{\gamma}_k| \tag{20}$$

and the data rate of corresponding eavesdropper can be given as,

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

Finally, the average secrecy rate is defined by,

$$R_k^s = \mathbb{E}\{[R_k - R_{e,k}]^+\}, \qquad k = 1, \ldots, K \tag{22}$$

where R_k^s is the average secrecy rate of the *k*th legitimate user and $[x]^+ \triangleq \max\{0, x\}$.

The average secrecy sum rate is also given as,

$$R_s = \sum_{k=1}^{K} R_k^s \tag{23}$$

$$\gamma_k = \frac{\phi P_k \mathbf{W}_{DB,k}^H \mathbf{W}_{AB,k}^H \mathbf{H}_k \mathbf{F}_{AB,k} \mathbf{F}_{DB,k} \mathbf{F}_{DB,k}^H \mathbf{F}_{AB,k}^H \mathbf{H}_k^H \mathbf{W}_{AB,k} \mathbf{W}_{DB,k}}{\mathbf{W}_{DB,k}^H \mathbf{W}_{AB,k}^H \left(P_k \mathbf{H}_k \left(\phi \sum_{\substack{j=1 \\ (j \neq k)}}^{K} \mathbf{F}_{AB,j} \mathbf{F}_{DB,j} \mathbf{F}_{DB,j}^H \mathbf{F}_{AB,j}^H + (1-\phi) \mathbf{F}_{AN} \mathbf{F}_{AN}^H \right) \mathbf{H}_k^H + \sigma_k^2 \mathbf{I}_{N_R} \right) \mathbf{W}_{AB,k} \mathbf{W}_{DB,k}} \tag{18}$$

$$\gamma_{e,k} = \frac{\phi P_k \mathbf{W}_{DB,e,k}^H \mathbf{W}_{AB,e,k}^H \mathbf{H}_{e,k} \mathbf{F}_{AB,k} \mathbf{F}_{DB,k} \mathbf{F}_{DB,k}^H \mathbf{F}_{AB,k}^H \mathbf{H}_{e,k}^H \mathbf{W}_{AB,e,k} \mathbf{W}_{DB,e,k}}{\mathbf{W}_{DB,e,k}^H \mathbf{W}_{AB,e,k}^H \left((1-\phi) P_k \mathbf{H}_{e,k} \mathbf{F}_{AN} \mathbf{F}_{AN}^H \mathbf{H}_{e,k}^H + \sigma_{e,k}^2 \mathbf{I}_{N_R} \right) \mathbf{W}_{AB,e,k} \mathbf{W}_{DB,e,k}} \tag{19}$$

Another important metric for measuring the secrecy is the outage probability. A secrecy outage probability for the kth legitimate user is calculated as,

$$\mathrm{P}(R_k^s < R_{th}) \tag{24}$$

where R_{th} is the given threshold secrecy rate.

IV. Simulation Results

We illustrate the simulation results in terms of the secrecy rate and the secrecy outage probability. The average signal-to-noise-ratio (SNR) of the kth legitimate user is $\mathrm{SNR} = \frac{P_k}{\sigma_k^2}$. The key simulation parameters are given in Table I.

TABLE I
Simulation Parameters

Parameter	Description	Value
f_c	Operating frequency	73 GHz SSCM in [8]
K	Legitimate users	[5,10,15,20,30]
N_T	BS antennas	128
N_R	User antennas	8
$N_{R,e}$	Eavesdropper antennas	256
N_{RF}	BS RF chains	32
M_{RF}	User RF chains	n_s $(KM_{RF} \leq N_{RF})$
n_s	Data stream for each user	[1,2]
N_s	Data stream for BS	Kn_s

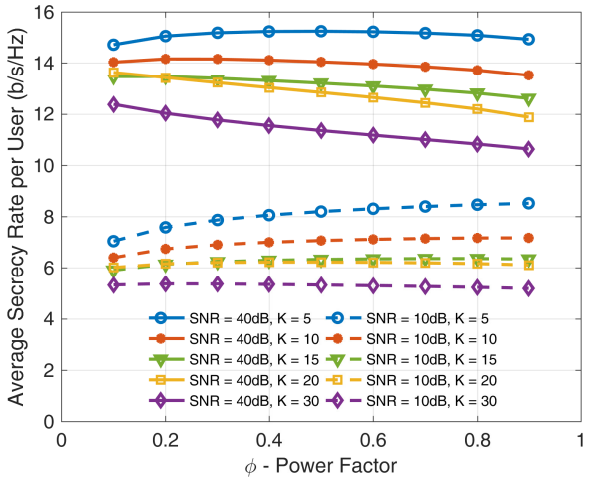

Fig. 3. Average secrecy rate per user vs ϕ for single stream case

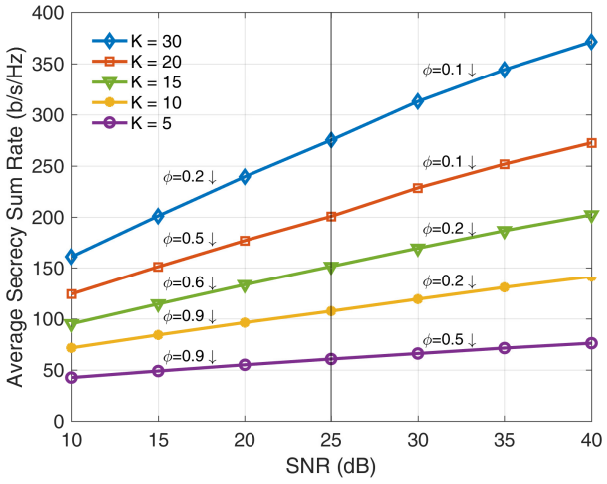

Fig. 4. Average secrecy sum rate vs SNR with the optimum ϕ values in single stream case

In the Figures 3 and 4, only one stream is assigned to each legitimate user as $M_{RF} = n_s = 1$. Since there is only one RF chain at the legitimate users and eavesdropper side, only analog beamforming can be considered instead of the hybrid structure for the case of single stream.

For the Figure 3, the average secrecy rate is shown through different optimum power factor for the different number of users and SNR values. It is observed that the power factor has great importance on the average secrecy rate per user. Therefore, the optimum power factor is nearly chosen as $\phi = 0.9$ for low number of users and low SNR (noise-limited) regime. On the other hand, the power factor of AN signal becomes more important for the low SNR regime when the user density becomes high. Besides, in the high SNR regime, the power of AN signal needs to be increased to reach higher secrecy rates especially when the number of users is high. Since adding the AN signal to the system causes a leakage to the legitimate users, it can compensate at the high SNR (interference-limited) regime.

In the Figure 4, the performance of the average secrecy sum rate is shown for the different number of users with

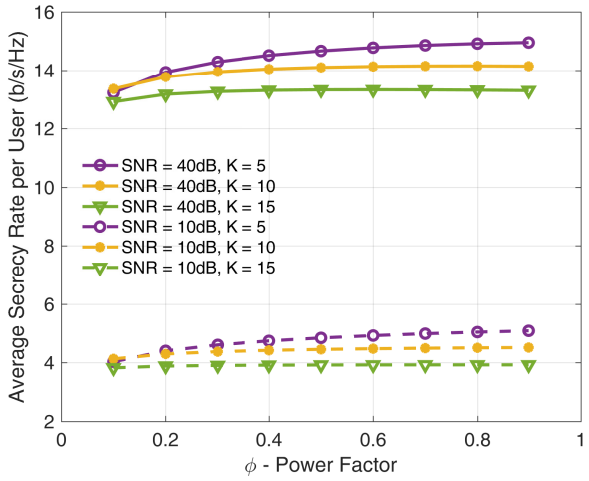

Fig. 5. Average secrecy rate per user vs ϕ for multiple streams ($n_s = 2$) case

their optimal power factors. The performance results show that the average secrecy sum rate is improved significantly when the number of users is increased in the MU-MIMO mmWave communications.

In the Figure 5, the effect of power factor for multiple streams case is observed in different SNR regimes. In the 2-streams case, the power factor is determined adaptively. For the mmWave communications system with 15 legitimate users, the optimum power factor is set as 0.3 for the high SNR regime while it is determined as 0.9 for the low SNR regime. When the number of streams increases, more power for the legitimate users is required to improve secrecy performance.

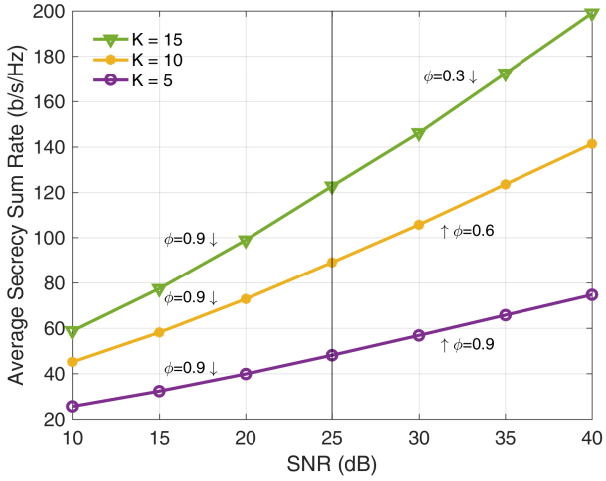

Fig. 6. Average secrecy sum rate vs SNR with the optimum ϕ values in multiple streams ($n_s = 2$) case

Figure 6 gives the simulation results based on the secrecy sum rate for different number of users with their optimum power allocation values. It is shown that the secrecy sum rate is improved when the number of user increases for the case of 2-streams.

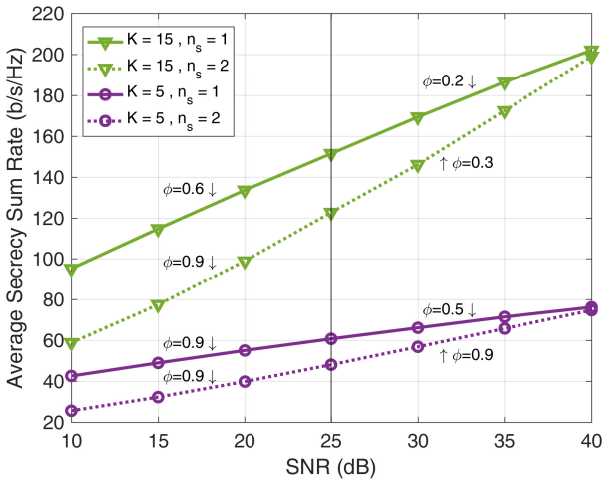

Fig. 7. Average secrecy sum rate vs SNR with the optimum ϕ values in different number of streams

In the Figure 7, the effect of the number of data streams on the average secrecy sum rate is shown by setting the optimum power factors. The performance results indicate that as the number of streams increases, the average secrecy sum rate decreases. It is based on the assumption that the eavesdropper can receive messages from the AoDs of legitimate users but not from the LOS link, increasing data streams makes possible the information leakage from legitimate users to eavesdropper. As a result, the eavesdropper can gain more mutual information about the channel of each legitimate user when the number of streams is high.

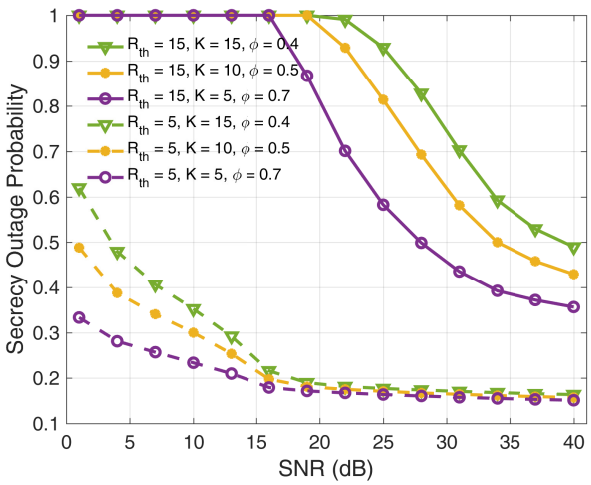

Fig. 8. Secrecy outage probability vs SNR with the optimum ϕ values in single stream case

Figure 8 and 9 draw the secrecy outage probability with respect to SNR for different number of streams considering the power allocation values determined in the Figures 3 and

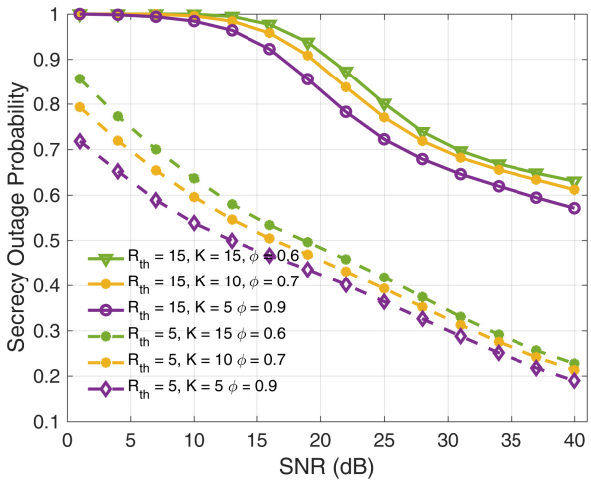

Fig. 9. Secrecy outage probability vs SNR with the optimum ϕ values in multiple streams ($n_s = 2$) case

5. It is observed that the secrecy outage probability is getting poor when the number of streams and users increases.

V. Conclusions

We have provided the performance evaluations based on the secrecy rate and secrecy outage probability for the single-cell MU-MIMO with multiple streams downlink mmWave communication system. On one hand, the hybrid beamforming scheme is applied for all nodes in the cell and MMSE precoder is used to mitigate the interference between legitimate users. On the other hand, the AN precoder is designed to increase the secrecy rate. We have provided extensive simulation results for the different number of users and streams. It has been shown that the secrecy of the overall system is improved by adjusting the power allocation factor depending on the number of streams and the SNR region. As future work, the scenario will be extended to a multicell scenario for ultra-dense networks.

Acknowledgment

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] S. A. Busari, K. M. S. Huq, S. Mumtaz, L. Dai, and J. Rodriguez, "Millimeter-Wave Massive MIMO Communication for Future Wireless Systems: A Survey," *IEEE Communications Surveys Tutorials*, vol. 20, no. 2, pp. 836-869, Secondquarter 2018.

[2] A. Khisti and G. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088-3104, Jul. 2010.

[3] A. Khisti and G. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515-5532, Nov. 2010.

[4] Y. W. P. Hong, P. C. Lan, and C. C. J. Kuo, "Enhancing physical-layer secrecy in multi-antenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29-40, Sep. 2013.

[5] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550-1573, Mar. 2014.

[6] N. Yang et al., "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20-27, Apr. 2015.

[7] Y. Ju, H. M. Wang, T. X. Zheng, and Q. Yin, "Secure transmissions in millimeter wave systems," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2114-2127, May 2017.

[8] M. K. Samimi and T. S. Rappaport, "3-D millimeter-wave statistical channel model for 5G wireless system design," *IEEE Trans. Microw. Theory Techn.*, vol. 64, no. 7, pp. 2207-2225, Jul. 2016.

[9] I. A. Hemadeh, K. Satyanarayana, M. El-Hajjar and L. Hanzo, "Millimeter-Wave Communications: Physical Channel Models, Design Considerations, Antenna Constructions, and Link-Budget," *IEEE Communications Surveys & Tutorials*, vol. 20, pp. 870–913, May 2018.

[10] S. Sun, T. S. Rappaport, and M. Shafi, "Hybrid beamforming for 5G millimeter-wave multi-cell networks," in *Proc. IEEE Conf. Comput. Commun. Workshops*, 2018, pp. 589–596

[11] F. Sohrabi and W. Yu, "Hybrid digital and analog beamforming design for large-scale antenna arrays," *IEEE J. Sel. Topics Signal Process.*,vol. 10, no. 3, pp. 501–513, Apr. 2016.

[12] A. F. Molisch et al., "Hybrid beamforming for massive MIMO: A survey," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 134–141, Sep. 2017.

[13] O. ElAyach,S. Rajagopal,S. Abu-Surra,Z. Pi,and R.Heath,"Spatially sparse precoding in millimeter wave MIMO systems," *IIEEE Transactions on Wireless Communications*, vol. 13, no. 3, pp. 1499–1513, Mar. 2014.