Improved Hybrid Precoder Design for Secure mmWave MIMO Communications

Yasin Kabalci[1, *], Muhammad Ali[1, 2]
[1]*Faculty of Engineering, Electrical and Electronics Engineering,*
Nigde Omer Halisdemir University,
Nigde, Turkey
[2]*Department of Electrical Engineering, Faculty of Engineering,*
University of Azad Jammu and Kashmir,
Muzaffarabad, Pakistan
yasinkabalci@ohu.edu.tr

***Abstract*—Key challenges of emerging mobile communication systems are to provide higher data rates, diverse device connectivity, low latency, higher system capacity, and low energy consumption. The communication systems exploiting the millimeter-wave (mmWave) band are realized to resolve thereof inevitable issues. However, security is considered as one of the challenging issues in mmWave communication in addition to unavoidable problems (e.g., propagation loss, penetration loss, and fading). This study aims to construct efficient secure hybrid precoder with low-resolution phase shifters that can protect legitimate information from eavesdropping by employing coordinated analog precoder and combiner algorithms and improve the secrecy rate. Moreover, in order to further enhance the secrecy rate, hybrid precoder are obtained using an efficient channel. This work compares its results with the recent approach reported in the literature, which indicates that our proposed model outperforms at high signal-to-noise ratio (SNR) values, while our model provides similar performance at low SNR values. Simulation studies also confirm the effectiveness of the proposed hybrid precoder to achieve maximum secrecy rate.**

***Index Terms*—5G; Hybrid precoder; mmWave; Physical layer security; SNR.**

I. Introduction

The millimeter-waves (mmWaves) aim to provide a wide bandwidth around 200 times more than the present mobile communication systems by utilizing the upper part of the electromagnetic spectrum. These waveforms are realized to accommodate the challenging demands of upcoming fifth-generation (5G) mobile communication systems such as higher data rate, diverse device connectivity, low latency, higher system capacity, and low energy consumption [1]. Still, it is very difficult to develop communication systems using mmWave bands owing to unavoidable degradation problems (e.g., penetration loss, propagation loss, and rain fading) [2]. However, shorter wavelengths of mmWaves support the deployment of large-scale antenna array structure to attain promising beamforming gainsthat allows more efficient utilization of spectrum. Since it is inappropriate to integrate radio frequency (RF) chain for each antenna in mmWave communication systems causing cost and energy consumptionissues, it is practicle to exploit digital and analog hybrid multiple-input multiple-output (MIMO) system with an optimal number of RF chains [3], [4]. In addition, definite number of useful propagation paths are achievable by mmWave channels. To cope with this issue, narrow directional beam is achieved from hybrid precoder by utilizing extensive antenna array structure [5]. Despite the promising features offered by hybrid precoder, efficiency of mmWave communication systems is compromised due to analog precoding, which has certain magnitude and phase limitations. It is logical to utilize the low-resolution phase shifters (PSs) to avoid circuit and energy consumptioncomplications.

Security is also an inevitable issue in addition to the aforementioned in mmWave communication systems. The physical layer security (PLS) is realized as promising solution to guarantee secure transmission for the present and next-generation wireless systems [6]. It is obligatory to prevent information from undesired user (eavesdropper, Eve) since wireless communication systems are vulnerable to all the mobile users located in its vicinity due to the broadcast nature of their wireless links. The multi-antennas in mmWave communication systems provide spatial degree of freedom (DoF) that may be used to enhance main channel to desired users and degrade main channel to Eves. In this way, beam direction may be regulated by the transmitter that can provide best signal-to-noise ratio (SNR) for required users, and confirms least information leakage towards Eves [7]. It is very important to note that Eve with multiple antenna can experience significant information leakage [8]. To enhance the secrecy rate that is considered as the minimal discrepancy between the achievable rate of the required and Eve channel [9], transmitter generates and transmits the artificial noise (AN) in all directions excluding required users. Therefore, it is likely possible that Eve will encounter AN along with desired signals that lessens the SNR at Eve, and makes it tough for it to decode the original signals [10].

An effective directional precodingdesign, known as antenna subset modulation (ASM), is firstly given in [11] for

Manuscript received 18 November, 2019; accepted 10 April, 2020.

mmWave communication systems. In this scheme, a protected mmWave link is realized by utilizing the specific subset ofantenna array, which helps to develop tightly identified constellation in the aimed angle while randomized constellation in the rest of sides. The ASM approach faces certain computational and side-lobe complications, which are improved by [12]. Authors in [13] developed an effective scheme for secure transmission where Alice (i.e., transmitter) utilizes hybrid massive MIMO schemes with suitable arbitrary approaches to activate a huge number of dumb antennas. This scheme can overcome the eavesdropping capability of Eve and approve itself as a secure scheme against Eves. However, Eve cannot deploy same number of antennas as Alice in this scheme. In [14], authors investigated secure hybrid beamforming scheme for mmWave communication systems. In this scheme, Eve is also deploying the same number of antennas similar to Alice and modeled hybrid-precoding design with high-resolution PSs, and then they presented a hybrid precoder design exploiting low-resolution PSs in [15]. In addition, they obtained secure analog precoder and combiner by utilizing the proposed algorithm, and then found the digital precoder that helped them to further improve the security. However, at higher SNR values, a notable gap is realized between the algorithm reported in [15] and the full-digital benchmark in the study. This fact motivated us to improve the secrecy rate in high SNR regimes.

To the best of our knowledge, no significant work has been done so far to improve thereof gap in high SNR value for mmWave massive MIMO systems using secure hybrid precoder designs. Inspired from [14] and [15], we have two aims in this study. First, is to design a secure hybrid precoder that ensures secure transmission for the intended user without significant information leakage towards Eve, and the second is to improve the secrecy rate at high SNR values in mmWave MIMO communication systems. The primary objective of this work is to intensely examine the secure hybrid precoding algorithms over broadly used scatterer-sharing channel model [16]. The most popular zero-forcing scheme [17] is applied on Eve channel in order to suppress it at eavesdropper side and attempts to reduce the information leakage towards Eve. Later on, we attained secure analog precoder and combiner using the algorithm proposed in this study and the recent algorithm reported in [15]. Finally, digital precoder and combiner are obtained using singular value decomposition (SVD) in this study. It is verified via extensive simulation studies that our proposed algorithm dominates the recent algorithm reported in [15] at high SNR values, while provides similar secrecy rates at low SNR values.

Notations: The lower case, boldface lower case, and boldface upper case letters denote scalars, column vectors, and matrices, respectively. The set of complex numbers is indicated by $\mathbb{C}$. The transpose and conjugate-transpose operations are represented by $(\cdot)^T$ and $(\cdot)^H$, respectively. An identity matrix with $N_s \times N_s$ dimensions is expressed as $\mathbf{I}_{N_s}$. The operations of absolute value, Euclidean norm, and Frobenius norm are shown by $|\cdot|$, $\|\cdot\|$, and $\|\cdot\|_F$, respectively. The expectation (statistical) function and phase of a complex number are denoted by $\mathbb{E}[\cdot]$ and $angle[\cdot]$. The output of the operation $(\cdot)^+ \triangleq max(0,\cdot)$ will either provide positive value or zero. The transmitter (Alice), receiver (Bob), and eavesdropper (undesired receiver) are represented by the subscripts a, b, and e, respectively.

II. System Model

A mmWave MIMO system consisting of Alice, Bob, and an undesired user (Eve) is shown in Fig. 1. Alice deploys N_a antennas and N_a^{RF} number of RF chains to transmit N_s number of data streams through mmWave MIMO channels in the direction of Bob, which consists of $N_s \le N_a^{RF} < N_a$ and $N_s \le N_b^{RF} < N_b$ conditions to enable multi-stream transmission and decrease limitations of cost and energy consumption. A data stream vector $\mathbf{s} = N_s \times 1$, which justifies $\mathbb{E}\left[\mathbf{ss}^H\right] = 1/N_s \times \mathbf{I}_{N_s}$ condition is first processed by digital precoder ($\mathbf{F}_D \in \mathbb{C}^{N_a^{RF} \times N_s}$), and then passed through analog RF precoder ($\mathbf{F}_A \in \mathbb{C}^{N_a \times N_a^{RF}}$). Finally, the precoder is passed through normalized power constraint denoted by $\|\mathbf{F}_A\mathbf{F}_D\|_F^2 = N_s$.

It is worth noting that $\mathbf{F}_A$ is comprises of PSs whose elements are bound to fulfill constantamplitude. Thus, the transmitted signal $\mathbf{x} \in \mathbb{C}^{N_a \times 1}$ from Alice can be represented as

$$\mathbf{x} = \sqrt{P}\mathbf{Fs} = \sqrt{P}\mathbf{F}_A\mathbf{F}_D\mathbf{s}, \tag{1}$$

where P shows transmitted power while $\mathbf{F} \in \mathbb{C}^{N_a \times N_s}$ indicates hybrid precoder. The transmitted signal is then received at Bob through Alice-to-Bob channel $\mathbf{H}_b \in \mathbb{C}^{N_b \times N_a}$. If there is a noise vector representing independent and identical distribution $\mathcal{CN}\left(0,\sigma_b^2\right)$ denoted by $\mathbf{n}_b \in \mathbb{C}^{N_b \times 1}$, then thesignal received at Bob side is shown as

$$\mathbf{y}_b = \mathbf{H}_b\mathbf{x} + \mathbf{n}_b, \tag{2}$$

where $\mathbf{y}_b$ is handled by hybrid combiner $\mathbf{W}_b = \mathbf{W}_{A,b}\mathbf{W}_{D,b}$. $\mathbf{W}_{A,b}$ and $\mathbf{W}_{D,b}$ show analog and digital combiner, respectively. The last signal at Bob is defined as follows

$$\mathbf{s}_b = \sqrt{P}\mathbf{W}_{D,b}^H\mathbf{W}_{A,b}^H\mathbf{H}_b\mathbf{F}_A\mathbf{F}_D\mathbf{s} + \mathbf{W}_{D,b}^H\mathbf{W}_{A,b}^H\mathbf{n}_b. \tag{3}$$

Since Eve is also involved in the considered wiretap system that employs N_e antennas and N_e^{RF} RF chains, he will also try to obtain information via combiner $\mathbf{W}_e = \mathbf{W}_{A,e}\mathbf{W}_{D,e}$. Thus, the last signal at Eve side is shown similar to (3) as

$$\mathbf{s}_e = \sqrt{P}\mathbf{W}_{D,e}^H \mathbf{W}_{A,e}^H \mathbf{H}_e \mathbf{F}_A \mathbf{F}_D \mathbf{s} + \mathbf{W}_{D,e}^H \mathbf{W}_{A,e}^H \mathbf{n}_e, \qquad (4)$$

where the Alice-to-Eve channel is denoted by $\mathbf{H}_e$.. The Alice exploits angle of departures (AoDs) of the Bob in order to deliver protected information in the direction of Bob. The chances of Eve to leake the information are extremely enhanced due to similar AoDs of Bob and Eve that encouraged to explore the PLS. The Alice-to-Bob channel $\mathbf{H}_b$ can be represented as

$$\mathbf{H}_b = \sqrt{\frac{N_a N_b}{N_{sc} N_{ray}}} \sum_{k=1}^{N_{sc}} \sum_{l=1}^{N_{ray}} \gamma_{kl} \mathbf{a}_b\left(\theta_{kl}^b\right) \mathbf{a}_a^H\left(\phi_{kl}^b\right), \qquad (5)$$

where N_{sc} is the number of scatterers, while N_{ray} denotes propagation paths of each scatterer. γ_{kl} indicates complex gain of the l^{th} propagation path in k^{th} scatterer with Rayleigh distribution. The azimuth AoDs or angle of arrivals (AoAs) of Alice and Bob for the kl^{th} path is represented by θ_{kl}^b and $\phi_{kl}^b \in [0, \pi]$, respectively. The response vectors of antenna array are respectively given as:

$$\mathbf{a}_a\left(\phi_{kl}^b\right) = \frac{1}{N_a}\left[1, e^{j\frac{2\pi}{\lambda} d \sin\left(\phi_{kl}^b\right)}, \dots, e^{j(N_a-1)\frac{2\pi}{\lambda} d \sin\left(\phi_{kl}^b\right)}\right], \qquad (6)$$

$$\mathbf{a}_b\left(\theta_{kl}^b\right) = \frac{1}{N_b}\left[1, e^{j\frac{2\pi}{\lambda} d \sin\left(\theta_{kl}^b\right)}, \dots, e^{j(N_b-1)\frac{2\pi}{\lambda} d \sin\left(\theta_{kl}^b\right)}\right], \qquad (7)$$

where λ is the wavelength and d specifies antenna spacing. In addition, a uniform linear array (ULA) structure is utilized by both Alice and Bob. Similarly, Alice-to-Eve channel $\mathbf{H}_e$ is defined as

$$\mathbf{H}_e = \sqrt{\frac{N_a N_e}{N_{sc} N_{ray}}} \sum_{k=1}^{N_{sc}} \sum_{l=1}^{N_{ray}} \gamma_{kl} \mathbf{a}_e\left(\theta_{kl}^e\right) \mathbf{a}_a^H\left(\phi_{kl}^e\right). \qquad (8)$$

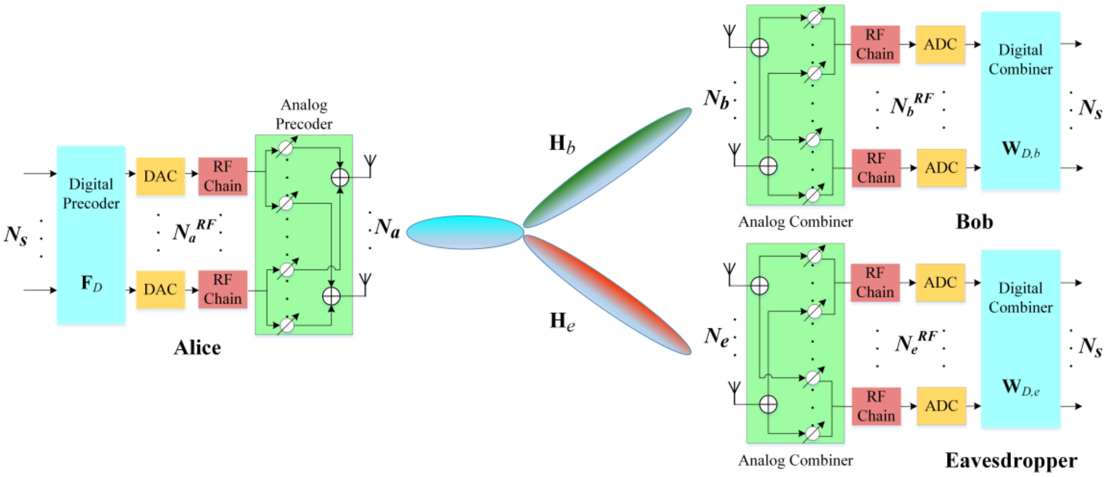

Fig. 1. Block diagram of hybrid precoder and combiner design for mmWave MIMO wiretap systems.

III. SECRECY ANALYSIS AND SECURE HYBRID PRECODER

A. Secrecy Analysis

The secrecy rate using full-digital precoder and combiner structure is examined by the authors in [15]. They established that the generalized eigen decomposition (GED) scheme [18] based on PLS displays comprehensive outcomes than generalized SVD (GSVD) approach [19] in the mmWave communication systems.Farther, they showed that significant information leakage can be realizable by adopting conventional precoding design without PLS effort, which approves the importance of PLS. Therefore, GED-based PLS scheme is adopted as performance criteria all over this paper. The analysis of secrecy rate is usually investigated by exploiting the following PLS performance metric:

$$R_s = \left(\log_2\left|\mathbf{I}_{N_s} + \mathbf{C}_b\right| - \log_2\left|\mathbf{I}_{N_s} + \mathbf{C}_e\right|\right)^+, \qquad (9)$$

$$\mathbf{C}_b \triangleq P/N_s\, \mathbf{R}_{n,b}^{-1}\left(\mathbf{W}_{D,b}\right)^H\left(\mathbf{W}_{A,b}\right)^H \mathbf{H}_b \mathbf{F}_A \mathbf{F}_D \times$$
$$\times \mathbf{F}_D^H \mathbf{F}_A^H \mathbf{H}_b^H \mathbf{W}_{A,b} \mathbf{W}_{D,b}, \qquad (10)$$

$$\mathbf{C}_e \triangleq P/N_s\, \mathbf{R}_{n,e}^{-1}\left(\mathbf{W}_{D,e}\right)^H\left(\mathbf{W}_{A,e}\right)^H \mathbf{H}_e \mathbf{F}_A \mathbf{F}_D \times$$
$$\times \mathbf{F}_D^H \mathbf{F}_A^H \mathbf{H}_e^H \mathbf{W}_{A,e} \mathbf{W}_{D,e}, \qquad (11)$$

$$\mathbf{R}_{n,b} \triangleq \sigma_b^2\left(\mathbf{W}_{D,b}\right)^H\left(\mathbf{W}_{A,b}\right)^H \mathbf{W}_{A,b} \mathbf{W}_{D,b}, \qquad (12)$$

$$\mathbf{R}_{n,e} \triangleq \sigma_e^2\left(\mathbf{W}_{D,e}\right)^H\left(\mathbf{W}_{A,e}\right)^H \mathbf{W}_{A,e} \mathbf{W}_{D,e}, \qquad (13)$$

where the secrecy capacity of Bob and Eve is denoted by $\mathbf{C}_b$ and $\mathbf{C}_e$, respectively While noise covariance matrices for Bob and Eve are indicated by $\mathbf{R}_{n,b}$ and $\mathbf{R}_{n,e}$, respectively.

B. Secure Hybrid Precoder Scheme

The hybrid precoder and combiner design problem based on PLS can be defined as follows:

$$\left\{\mathbf{F}_A, \mathbf{F}_D, \mathbf{W}_{A,b}, \mathbf{W}_{D,b}\right\} = \arg\max R_s,$$
$$s.t.\;\; \mathbf{F}_A(:,k) \in \mathcal{P}, \mathbf{W}_{A,b}(:,k) \in \mathcal{C}, \qquad (14)$$
$$\left\|\mathbf{F}_A \mathbf{F}_D\right\|_F^2 = N_s,\, k = 1,\dots,N_{RF},$$

where $\mathcal{P}$ and $\mathcal{C}$ control the resolution of $\mathbf{F}_A$ and $\mathbf{W}_{A,b}$, respectively, given in (15), where $N_a = N_b = N$

$$\mathcal{P} = \mathcal{C} \triangleq \left\{ \left(1/\sqrt{N}\right) \times e^{j\frac{2\pi i}{2^B}} \middle| i = 1, 2, ...2^B \right\}. \tag{15}$$

It is worth noting that analog precoder and combiner face certain amplitude and phase limitations because of the PSs. However, we presumed that the PSs have constant amplitude and quantized phase that are controlled by *B* number of quantization bits for simplicity. Although analog precoder and combiner can provide enhanced outcomes using larger value of *B*, the energy consumption and circuit complexities cannot be overlooked in mmWave MIMO communication systems. Consequently, it is practical to incorporate PSs with low resolution in mmWave MIMO communication systems. However, it may degrade the performance efficiency. In the context of PLS, a secure channel $\mathbf{H}_s$ is required that can be attained by excluding common AoDs elements of $\mathbf{H}_b$ and $\mathbf{H}_e$ from $\mathbf{H}_b$. However, before doing that, popular zero-forcing scheme [17, eq. (4.10)] is applied on $\mathbf{H}_e$, which helps to suppress the Eve channel and tries to minimize the information leakage towards Eve as

$$\mathbf{H}_e = \mathbf{H}_e \left(\mathbf{H}_e^H \mathbf{H}_e\right)^{-1}. \tag{16}$$

The SVD operation is performed on Eve channel $\mathbf{H}_e$

$$\mathbf{H}_e = \mathbf{U}_e \Sigma_e \mathbf{V}_e^H, \tag{17}$$

where $\mathbf{U}_e$ and $\mathbf{V}_e$ represent unitary matrices comprises of singular vectors related to a diagonal matrix Σ_e. $\mathbf{H}_s$ is obtained as

$$\mathbf{H}_s = \mathbf{H}_b \left(\mathbf{I}\text{-}\mathbf{V}_e \mathbf{V}_e^H\right). \tag{18}$$

Now, Alice can securely transmit by designing her precoder based on $\mathbf{H}_s$. Equation (9) can be reconsidered as:

$$R_s \approx R_{\mathbf{H}_s} = \log_2 \left|\mathbf{C}_s\right|, \tag{19}$$

$$\mathbf{C}_s \triangleq P/N_s \, \mathbf{R}_s^{-1} \left(\mathbf{W}_{D,b}\right)^H \left(\mathbf{W}_{A,b}\right)^H \mathbf{H}_s \mathbf{F}_A \mathbf{F}_D \times$$
$$\times \mathbf{F}_D^H \mathbf{F}_A^H \mathbf{F} \mathbf{H}_s^H \mathbf{W}_{A,b} \mathbf{W}_{D,b}, \tag{20}$$

$$\mathbf{R}_s \triangleq \sigma_b^2 \left(\mathbf{W}_{D,b}\right)^H \left(\mathbf{W}_{A,b}\right)^H \mathbf{W}_{A,b} \mathbf{W}_{D,b}. \tag{21}$$

However, still it is a complex hybrid precoder design problem that is resolved into two stages.In first stage, analog precoder and combiner are calculated using proposed algorithm. Then, calculating $\mathbf{F}_D$ and $\mathbf{W}_{D,b}$ using SVD process based on an effective digital channel $\tilde{\mathbf{H}}_b \triangleq \left(\mathbf{W}_{A,b}\right)^H \mathbf{H}_b \mathbf{F}_A$ as:

$$\tilde{\mathbf{H}}_b = \tilde{\mathbf{U}}_b \tilde{\Sigma}_b \tilde{\mathbf{V}}_b^H, \tag{22}$$

$$\mathbf{F}_D = \tilde{\mathbf{V}}_b\left(:, k\right),\ k = 1, ..., N_s, \tag{23}$$

$$\mathbf{W}_{D,b} = \tilde{\mathbf{U}}_b\left(:, k\right),\ k = 1, ..., N_s, \tag{24}$$

where $\tilde{\mathbf{V}}_b$ and $\tilde{\mathbf{U}}_b$ define unitary matrices and $\tilde{\Sigma}_b$ indicates the diagonal matrix containing singular values. Lastly, normalization of the digital precoder is performed as

$$\mathbf{F}_D = \sqrt{N_s} \mathbf{F}_D \Big/ \left\|\mathbf{F}_A \mathbf{F}_D\right\|_F. \tag{25}$$

$\mathbf{W}_e$ is calculated for Eve based on effective channel $\mathbf{H}_{eff} = \mathbf{H}_e \mathbf{F}_A \mathbf{F}_D$ by using the minimum mean square error (MMSE) filter as follows

$$\mathbf{W}_e = \left(\mathbf{H}_{eff} \mathbf{H}_{eff}^H P + \mathbf{I}_{N_e}\right)^{-1} \mathbf{H}_{eff}. \tag{26}$$

IV. PERFORMANCE ANALYSIS

This section presents the outcomes of our secure hybrid precoder design in the mmWave MIMO communication systems. We assumed $N_a = N_b = N_e = 192$, $B = 2$, and exactly the same number of scatterers for bringing fairness in the results with [15]. In addition, it is more likely that Bob and Eve will share a few joint scatterers. The AoAs and AoDs are uniformly distributed in $\left[0, 2\pi\right]$. The values of noise variances are set equal to unity for simplicity. The ULA structure with antenna spacing of $d = 1/\lambda$ is implemented for Alice, Bob, and Eve. In the following simulation studies, the secrecy rate of our hybrid precoder is examined through the mentioned algorithms in low and high SNR regimes. Typically, we considered 20 dB as threshold value for defining the low and high SNR regimes for ease. The full-digital precoder based on GED scheme with PLS effort will serve as upper bound while hybrid precoder using the spatially sparse precoding (SSP) [20] without PLS will act as lower bound. R_b and R_e indicate the secrecy rate of Bob and Eve, respectively.

The secrecy rate comparison of proposed algorithm and algorithm reported in [15] is shown in Fig. 2, where we considered the worst scenario by assuming $N_s = N^{RF} = 2$ conditions. The outcomes of Fig. 2 clearly demonstrate that the our algorithm achieves performance gain of almost 9 bps/Hz than the SSP. On the other hand, approximately 5.5 bps/Hz of performance gain is obtained by algorithm reported in [15] as compared to SSP. The use of the proposed algorithm provides better results than its counterpart in worst scenario, i.e., around 3.5 bps/Hz enhancement in secrecy.

Figure 3 shows spectral efficiency of the hybrid precoders by considering $N_s = 4$, $N_a^{RF} = N_b^{RF} = N_e^{RF} = 8$. In this case, about 17.5 bps/Hz performance gain isrealized by the proposed algorithm , while 11.5 bps/Hz gain is attained by the algorithm reported in [15] as compared to SSP SSP. The use of proposed algorithm ensures nearly 6 bps/Hz secrecy rate enhancement thanits counterpart. It is also worth noting that significant improvement in secrecy rate is realized when N_s and N_{RF} are increased. Almost 20 bps/Hz secrecy performance gain is realized by the proposed algorithm when $N_s = N_a^{RF} = N_b^{RF} = N_e^{RF} = 2$ conditions are considered, whereas more than 39 bps/Hz secrecy performance gain is noticed in the Fig. 3.

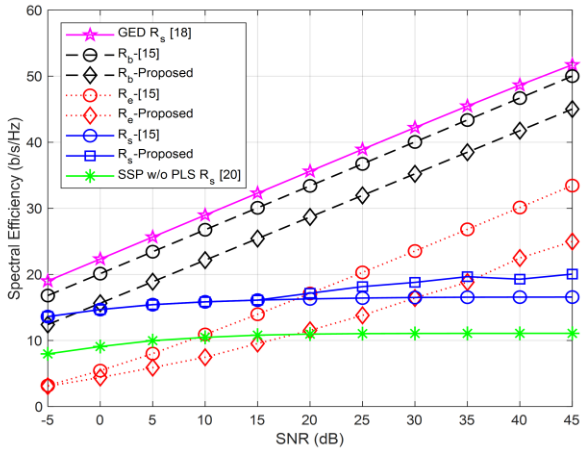

Fig. 2. Secrecy rate analysis results for $N_s = N_a^{RF} = N_b^{RF} = N_e^{RF} = 2$.

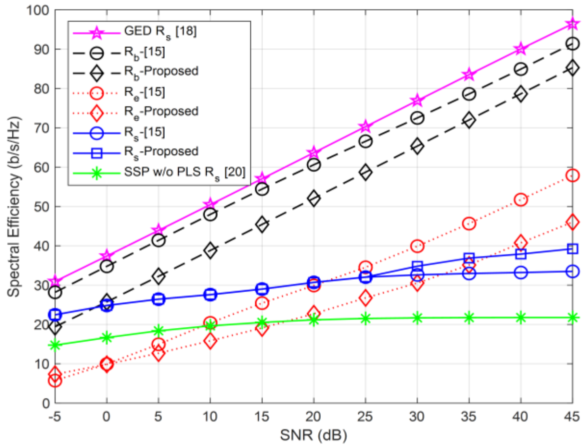

Fig. 3. Spectral efficiency results for $N_s = 4$, $N_a^{RF} = N_b^{RF} = N_e^{RF} = 8$.

The last results are shown in Fig. 4, which explains the secrecy rate performance for $SNR = 30\ dB$ and $N_a^{RF} = N_b^{RF} = N_e^{RF} = 8$.

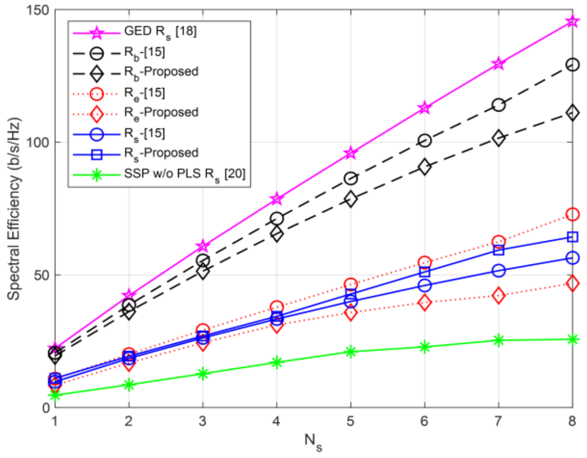

Fig. 4. Secrecy rate performance for $N_a^{RF} = N_b^{RF} = N_e^{RF} = 8$ and $SNR = 30\ dB$.

About 38.6 bps/Hz secrecy performance gain is presented by the proposed algorithm as compared to SSP. In contrast, almost 30.7 bps/Hz gain is obtained by the algorithm reported in [15] than SSP that also approves that use of proposed algorithm presents better secrecy rate performance of approximately 8 bps/Hz than the algorithm reported in [15]. It is also noticed that the proposed algorithm achieves nearly 64.5 bps/Hz secrecy performance gain while algorithm reported in [15] attains performance gains of almost 56.5 bps/Hz , which further confirms that the proposed algorithm provides superior secrecy rate performance than its counterpart at high SNR values.

As a final remark, it can be confirmed through the results presented from Fig. 2 to Fig. 4, the proposed algorithm demonstrates remarkable performance improvement in terms of protecting legitimate information from the eavesdropping than that of its counterparts.

V. CONCLUSIONS

Although the use of larger quantization bits guarantees a better analog precoder, it is impractical in mmWave communication systems owing to circuit complexity and high-energy consumptionissues. This paper presented the secrecy rate analysis of various approaches exploiting secure hybrid precoder and combiner in mmWave MIMO communication systems using low-resolution PSs. The extensive simulation studies clearly showed that the proposed algorithm offers approximately 8 bps/Hz better secrecy rate performance at high SNR values than the recently proposed algorithm, and it also exhibits same results with the compared algorithm at low SNR values. Furthermore, the proposed algorithm assures the minimum information leakage towards the Eve when compared to its counterparts, and it is able to provide more protected communication even in worse scenario.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] Y. Kabalci, “5G mobile communication systems: Fundamentals, challenges, and key technologies”, in *Smart Grids and Their Communication Systems*. Springer, Singapore, 2019, pp. 329–359. DOI: 10.1007/978-981-13-1768-2_10.

[2] Z. Pi and F. Khan, “An introduction to millimeter-wave mobile broadband systems”, *IEEE Commun. Mag.*, vol. 49, no. 6, pp. 101–107, 2011. DOI: 10.1109/MCOM.2011.5783993.

[3] Y. Kabalci and H. Arslan, “Hybrid precoding for mmWave massive MIMO systems with generalized triangular decomposition”, in *Proc. of 2018 IEEE 19th Wireless and Microwave Technology Conference (WAMICON)*, Florida, USA, 2018, pp. 1–6. DOI: 10.1109/WAMICON.2018.8363891.

[4] W. Zhang, X. Xia, Y. Fu, and X. Bao, “Hybrid and full-digital beamforming in mmWave Massive MIMO systems: A comparison considering low-resolution ADCs”, *China Commun.*, vol. 16, no. 6, pp. 91–102, 2019. DOI: 10.23919/JCC.2019.06.008.

[5] J. Zhang, Y. Huang, Q. Shi, J. Wang, and L. Yang, “Codebook design for beam alignment in millimeter wave communication systems”, *IEEE Trans. Commun.*, vol. 65, no. 11, pp. 4980–4995, 2017. DOI: 10.1109/TCOMM.2017.2730878.

[6] Y. Wu, A. Khisti, C. Xiao *et al.*, “A survey of physical layer security techniques for 5G wireless networks and challenges ahead”, *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, 2018. DOI: 10.1109/JSAC.2018.2825560.

[7] L. Fan, X. Lei, T. Q. Duong *et al.*, “Secure multiuser communications

in multiple amplify-and-forward relay networks", *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3299–3310, 2014. DOI: 10.1109/TCOMM.2014.2345763.

[8] G. Amarasuriya, R. F. Schaefer, and H. V. Poor, "Secure communication in massive MIMO relay networks", in *Proc. of 2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Edinburgh, UK, 2016, pp. 1–5. DOI: 10.1109/SPAWC.2016.7536731.

[9] Z. Li, R. Yates, and W. Trappe, "Secret Communication with a fading eavesdropper channel", in *Proc. of 2007 IEEE International Symposium on Information Theory*, Nice, France, 2007, pp. 1296–1300. DOI: 10.1109/ISIT.2007.4557402.

[10] L. Dong, Z. Han, A. P. Petropulu *et al*., "Improving wireless physical layer security via cooperative relays", *IEEE Trans. Signal Process*., vol. 58, no. 3, pp. 1875–1888, 2010. DOI: 10.1109/TSP.2009.2038412.

[11] N. Valliappan, A. Lozano, and R. W. Heath, "Antenna subset modulation for secure millimeter-wave wireless communication", *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3231–3245, 2013. DOI: 10.1109/TCOMM.2013.061013.120459.

[12] C. Chen, Y. Dong, X. Cheng *et al*., "An iterative FFT-based antenna subset modulation for secure millimeter wave communications", in *Proc. of 2017 International Conference on Computing, Networking and Communications (ICNC)*, USA, 2017, pp. 454–459. DOI: 10.1109/ICCNC.2017.7876171.

[13] X. Li, Y. Zhang, and W. Cadeau, "Hybrid massive MIMO for secure transmissions against stealthy eavesdroppers", *IEEE Commun. Lett.*, vol. 22, no. 1, pp. 81–84, 2018. DOI: 10.1109/LCOMM.2017.2762319.

[14] X. Tian, M. Li, Z. Wang *et al*., "Hybrid precoder and combiner design for secure transmission in mmWave MIMO systems", in *Proc. of 2017 IEEE Global Communications Conference*, Singapore, 2017, pp. 1–6. DOI: 10.1109/GLOCOM.2017.8254019.

[15] X. Tian, Q. Liu, Z. Wang *et al*., "Secure hybrid beamformers design in mmWave MIMO wiretap systems", *IEEE Syst. J.*, vol. 14, no. 1, pp. 548-559, 2020. DOI: 10.1109/JSYST.2019.2923819.

[16] S. Rappapport, G. R. MacCartney, M. K. Samimi *et al*., "Wide-band millimeter-wave propagation measurements and channel models for future wireless communication system design", *IEEE Trans. Commun*., vol. 63, no. 9, pp. 3029–3056, 2015. DOI: 10.1109/TCOMM.2015.2434384.

[17] E. Björnson, J. Hoydis, and L. Sanguinetti, *Massive MIMO networks: Spectral, energy, and hardware efficiency*. Now, 2017. DOI: 10.1561/2000000093.

[18] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel", *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, 2010. DOI: 10.1109/TIT.2010.2048445.

[19] A. Khisti, and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel", *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, 2010. DOI: 10.1109/TIT.2010.2068852.

[20] O. E. Ayach, S. Rajagopal, S. Abu-Surra *et al*., "Spatially sparse precoding in millimeter wave MIMO systems", *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1499–1513, 2014. DOI: 10.1109/TWC.2014.011714.130846.