IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received February 17, 2019, accepted February 25, 2019, date of publication February 27, 2019, date of current version March 18, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2902144

Artificial Noise Aided Hybrid Analog-Digital Beamforming for Secure Transmission in MIMO Millimeter Wave Relay Systems

SHAOYU WANG, XIAOMING XU, KAIZHI HUANG, XINSHENG JI, YAJUN CHEN, AND LIANG JIN

National Digital Switching System Engineering and Technological Research Center, Zhengzhou 450002, China

Corresponding author: Xiaoming Xu (ee_xiaomingxu@sina.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61501516, Grant 61701538, Grant 61871404, and Grant 61801435, in part by the Project funded by China Postdoctoral Science Foundation under Grant 2018M633733, in part by the Scientific and Technological Key Project of Henan Province under Grant 182102210449, and in part by the Scientific Key Research Project of Henan Province for Colleges and Universities under Grant 19A510024.

ABSTRACT Millimeter wave (mm-wave) communications, especially mm-wave relay systems, have been considered as a key technology for next-generation wireless networks due to the rich spectrum resources. However, the problem of information leakage in mm-wave relay systems has not been well investigated. In this paper, artificial noise (AN) aided two-stage secure hybrid beamforming algorithm is proposed in MIMO mm-wave relay system from the perspective of physical layer security. In each time slot of the relay communications, the RF analog beamforming matrices are designed in the first stage, and baseband digital beamforming matrices are designed in the second stage. Through the proposed algorithm, the joint optimization is avoided and the feedback is reduced, which brings low complexity. Moreover, the AN is applied to fight against the eavesdropper by deteriorating the eavesdropping channel. The simulation results show that the proposed hybrid beamforming algorithm considerably improves the performance and achieves a balance between complexity and performance.

INDEX TERMS MIMO millimeter wave relay systems, physical layer security, hybrid beamforming, artificial noise.

I. INTRODUCTION

A. BACKGROUND

The explosive growth of mobile data traffic and mobile terminals are putting more pressure for wireless service providers to overcome a global bandwidth shortage. Millimeter wave (mm-wave) can provide spectrum resources up to GHz bandwidth and is considered as one of the key technologies for future mobile communications [1]. Although mm-wave communications are characterized by very high propagation losses, there are many techniques to compensate [2]–[4]. The path loss can be compensated by using massive multiple-input-multiple-output (MIMO) at both the transmitter and the receiver. In addition, the use of relays that have modest benefits in current cellular networks can play a very important role in mm-wave space [5]. Relaying transmission is an essential strategy for improving the received power and enabling long-distance mm-wave communication.

The associate editor coordinating the review of this manuscript and approving it for publication was Prabhat Kumar Upadhyay.

However, due to the open architecture of mm-wave systems and the broadcast nature of wireless channels, the risk of information leakage is more severe [6]. Therefore, the security in mm-wave is of paramount importance. The traditional encryption mechanism relies on computational complexity. Physical layer security uses the ‘‘fingerprint’’ characteristics of the wireless channels and provides a new solution for wireless communication security from the aspect of information theory [7]–[9]. As an important supplement to the traditional encryption system, physical layer security technologies, such as artificial noise and beamforming, are well developed in traditional microwave systems [10]. However, in mm-wave systems, physical layer security signal processing faces more challenges. In microwave systems, the classical full-digital precoding can achieve the optimal antenna gain, while in mm-wave systems, it's not practical to deploy the same number of radio frequency (RF) chains as that of the antennas. As the number of RF chains is much smaller than the number of antennas in mm-wave systems, hybrid analog-digital beamforming has become a widely accepted beamforming method characterized by its simple hardware structure and low energy consumption [11]–[14]. Traditional beamforming methods are no longer suitable for millimeter wave systems because of changes in hardware structure. It is necessary to design a hybrid analog-digital beamforming algorithm that guarantees both the user communication rate and communication security. In this paper, we develop an efficient hybrid beamforming in a MIMO mm-wave relaying system to achieve secure communication.

B. RELATED WORKS AND MOTIVATION

In traditional microwave systems, the beamforming technologies are implemented in the baseband using digital signal processing, which allows better control over the beamforming matrices. Mm-wave communications typically employ much fewer RF chains than antennas. Under this constrain, the hybrid analog-digital architectures provide a compromise between hardware complexity and system performance. The transmitter performs a baseband digital precoding followed by an RF analog beamforming, and in the reverse order, the receiver implements an RF analog combining followed by a baseband digital decoding. Compared with the traditional beamforming design problem, the millimeter-wave hybrid beamforming design is a non-convex problem [15]. Furthermore, the digital beamforming matrix needs to be jointly designed with the analog beamforming/combining vector. The direct solution of the problem is not tractable. In [16], the millimeter-wave hybrid precoding problem is converted to Euclidean distance minimization problem. Paper [17] has further research. The problem is equivalent to sparse signal reconstruction problem and authors presented an algorithmic solution using orthogonal matching pursuit to reduce the design difficulty. Paper [18] proposes two coordinated algorithms for the multiuser MIMO Broadcast system. These iterative coordinated beamforming designs require a large feedback overhead and high computational complexity. The literature [19] develops an adaptive algorithm to estimate the mm-wave channel parameters. The poor scattering nature of the channel is exploited in the adaptive algorithm and the hardware constraints are overcome by a new hybrid analog/digital precoding algorithm. The beamforming design for the secure transmission has also been well investigated. The work in [20] develops a mathematical framework to analyse the connection outage probability, the secrecy outage probability and the achievable average secrecy rate from the perspective of the network. Reference [21] proposes a hybrid analog-digital precoder design to enhance the physical layer security of mm-wave multiple-input single-output (MISO) systems, which achieves comparable secrecy rate to that of the fully digital precoder. For the millimeter-wave MISO-OFDM system in [22], a closed-mixing precoding matrix is designed to maximize the security rate. However, it is assumed that the eavesdropping Channel State Information (CSI) is known in the transmitter, which is not practical in the system. Paper [23] proposes a hybrid precoder and combiner design for secure transmission in mm-wave MIMO wiretap system and use artificial noise to fight against eavesdroppers, but it doesn't consider relay and multi-user scenario. As for mm-wave relay systems, [24] investigates the robustness of the compressed sensing multi-hop scheme in the presence of one eavesdropper. Reference [25] considers resources allocation problem to enhance physical layer security in AF relay assisted wireless networks. In paper [26], RF and baseband beamforming designs are divided. The source node and relay node serve multiple destination nodes. MSE-based baseband beamformers were also developed. However, paper [24]–[26] doesn't concentrate on secure hybrid beamforming design in AF relay systems.

Nevertheless, to the best of our knowledge, the hybrid analog-digital beamforming for secure transmission in MIMO millimeter wave relay systems has not been studied yet. Information will be eavesdropped in each time slot of the relay communications. All of the aforementioned works do not pay enough attention to security issues in relay mm-wave systems and most algorithms require high computational complexity and feedback. We will propose a low-complexity yet efficient algorithm to secure mm-wave relay systems.

C. OUR WORK AND CONTRIBUTIONS

Motivated by the above observations and challenges, we apply physical layer security technology to MIMO mm-wave relay system. We provide a two-stage hybrid beamforming algorithm in both source-to-relay (phase-I) and relay-to-source (phase-II) phase. In each phase the beamforming matrices are divided into digital domain and analog domain. Furthermore, we use AN to prevent information from being eavesdropped. Our main contributions are summarized as follows:

- A MIMO mm-wave relay eavesdropping model is established from the perspective of PLS based on hybrid beamforming. The system model can be used in long-distance and high-security applications.
- A two-stage hybrid beamforming algorithm combined with AN is put forward to guarantee both the user communication rate and the communication security. The RF and baseband beamforming designs are separated to avoid joint optimization. The proposed algorithm in this paper is low-complexity but effectively protect private information from being eavesdropped.
- Secrecy performance analysis is conducted for the proposed algorithm in the presence of the eavesdropper. The analysis is helpful to understand understand how the proposed algorithm enhance the secure communications and provide direct insight in practical networks.

This paper is organized as follows. Section 2 introduces the system and channel models. Section 3 proposes an artificial noise aided two-stage secure hybrid beamforming algorithm. Simulation results are presented in Section 4. Section 5 concludes the paper.

Notations: $|\cdot|$, $\|\cdot\|$ and $\mathbb{E}(\cdot)$ denote absolute value, Frobenius norm, and expectation, respectively. $(\cdot)^T$ and $(\cdot)^H$ denote transpose and conjugate transpose, respectively. A bold capital letter $\mathbf{A}$ represents a matrix. $\mathbf{A}(i,j)$ represents the ith row, jth column element of $\mathbf{A}$. $tr(\mathbf{A})$ is its trace. $\mathbb{C}^{M\times N}$ represents spaces in $M\times N$ matrices with complex entries. $\mathcal{CN}$ denotes the complex Gaussian distribution.

II. SYSTEM AND CHANNEL MODELS

A. SYSTEM MODEL

Consider the MIMO millimeter wave downlink multi-user relay system as shown in Figure.1, where the source node and the relay node serve K destinations. Assume that there are no direct links between the source and destinations due to the long distance. The proposed algorithm focuses on a two-phase, half-duplexing amplify and forward (AF) relaying system, where the source transmits K data streams during phase-I, and the relay amplifies the received signals and forwards it to all of the K destinations during phase-II. We assume different eavesdroppers wiretap the kth destination in the both two phases. Non-colluding and passive eavesdropping case is considered, which is a common assumption in many literatures [27], [28]. The secrecy rate of the whole transmission depends on the minimum secrecy rate of the two phases [29]. In addition, assume the eavesdropper is passive in order to hidden its identity. Therefore, the channel state information (CSI) of the eavesdropper cannot be obtained for the source and relay by channel estimation techniques.

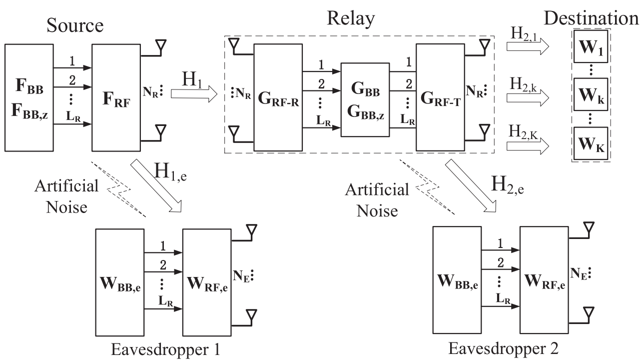


FIGURE 1. Hybrid analog-digital beamforming architecture for MIMO mm-wave relay eavesdropping system.

Hybrid beamforming structure is applied at each node. The source, relay, destinations and eavesdroppers are equipped with N_S, N_R, N_D and N_E antennas (L_S, L_R, L_D and L_E RF chains), respectively. The number of RF chains is much smaller than the number of antennas. We consider the multi-user beamforming case in which the source communicates with every destination via only one stream. Motivated by the maximum number of simultaneous service users of the described system, we have $L_S > K$, $L_R > K$. Each destination is equipped one RF chain, i.e. $L_D = 1$, which can reduce the processing complexity of the destination.

In phase-I, the source transmits K data streams to the relay. Let $\mathbf{s} = [s_1, s_2, \ldots, s_K]^T \in \mathbb{C}^{K\times 1}$ represent K data streams for all destinations. The transmitted signal from the source can be expressed as

$$\mathbf{x}_s = \mathbf{F}_{RF}\mathbf{F}_{BB}\mathbf{s}, \tag{1}$$

where $\mathbf{F}_{BB} \in \mathbb{C}^{L_S\times K}$ and $\mathbf{F}_{RF} \in \mathbb{C}^{N_S\times L_S}$ represent the baseband and RF beamforming matrices at the source, respectively. Let P_S denote the transmission power constraint at the source. $\mathbb{E}[\mathbf{s}\mathbf{s}^H] = \mathbf{I}_K$. Then the power constraint at the source is as follows:

$$\mathrm{tr}\left\{E[\mathbf{x}_s\mathbf{x}_s^H]\right\} = \mathrm{tr}\left\{\mathbf{F}_{RF}\mathbf{F}_{BB}\mathbf{F}_{BB}^H\mathbf{F}_{RF}^H\right\} = P_S. \tag{2}$$

The received signal at the relay is represented as

$$\mathbf{y}_r = \mathbf{H}_1\mathbf{F}_{RF}\mathbf{F}_{BB}\mathbf{s} + \mathbf{n}_r, \tag{3}$$

where $\mathbf{H}_1 \in \mathbb{C}^{N_R\times N_S}$ is the channel matrix between the source and the relay. $\mathbf{n}_r \in \mathbb{C}^{N_R\times 1} \sim \mathcal{CN}(0,\sigma_r^2)$ is the complex additive white Gaussian noise. Each entry of $\mathbf{F}_{RF}$ are constant modulus because the RF beamforming is implemented by analogue phase shifters. We normalize these entries to satisfy $|\mathbf{F}_{RF}(i,j)| = \frac{1}{\sqrt{N_S}}$. We assume that the angles of the analog phase shifters are quantized with a finite set of possible values. With these assumptions, $\mathbf{F}(i,j) = \frac{1}{\sqrt{N_S}}e^{j\phi}$, where ϕ is a quantized angle.

At the relay, analog combiner $\mathbf{G}_{RF-R} \in \mathbb{C}^{K\times N_R}$ is firstly employed to receive $\mathbf{y}_r$. Then one digital matrix $\mathbf{G}_{BB} \in \mathbb{C}^{L_R\times K}$ processes the signal in the baseband. Afterward, the analog precoder $\mathbf{G}_{RF-T} \in \mathbb{C}^{N_R\times L_R}$ is used to forward the transmitted signal at the relay to the destinations. The signal transmitted by the relay is represented as

$$\begin{aligned}\mathbf{x}_r &= \mathbf{G}_{RF-T}\mathbf{G}_{BB}\mathbf{G}_{RF-R}\mathbf{y}_r\\ &= \mathbf{G}_{RF-T}\mathbf{G}_{BB}\mathbf{G}_{RF-R}\mathbf{H}_1\mathbf{F}_{RF}\mathbf{F}_{BB}\mathbf{s}\\ &\quad + \mathbf{G}_{RF-T}\mathbf{G}_{BB}\mathbf{G}_{RF-R}\mathbf{n}_r.\end{aligned} \tag{4}$$

Assume the transmission power at relay is P_R. Then the power constraint at relay is

$$\begin{aligned}&\mathrm{tr}\left\{E[\mathbf{x}_r\mathbf{x}_r^H]\right\}\\ &= \mathrm{tr}\Big\{\mathbf{G}_{RF-T}\mathbf{G}_{BB}\mathbf{G}_{RF-R}\mathbf{H}_1\\ &\qquad \times \mathbf{F}_{RF}\mathbf{F}_{BB}\mathbf{F}_{BB}^H\mathbf{F}_{RF}^H\mathbf{H}_1^H\mathbf{G}_{RF-R}^H\mathbf{G}_{BB}^H\mathbf{G}_{RF-T}^H\\ &\qquad + \sigma_r^2\mathbf{G}_{RF-T}\mathbf{G}_{BB}\mathbf{G}_{RF-R}\mathbf{G}_{RF-R}^H\mathbf{G}_{BB}^H\mathbf{G}_{RF-T}^H\Big\} = P_R.\end{aligned} \tag{5}$$

Similarly, the intercepted signal by the eavesdropper during phase-I is as follows

$$\mathbf{y}_{e,1} = \mathbf{W}_{BB,e}^H\mathbf{W}_{RF,e}^H\mathbf{H}_{1,e}\mathbf{F}_{RF}\mathbf{F}_{BB}\mathbf{s} + \mathbf{W}_{BB,e}^H\mathbf{W}_{RF,e}^H\mathbf{n}_e, \tag{6}$$

where $\mathbf{H}_{1,e} \in \mathbb{C}^{N_E\times N_S}$ is the channel matrix between the source and the eavesdropper $\mathbf{W}_{RF,e} \in \mathbb{C}^{N_E\times L_E}$ and $\mathbf{W}_{BB,e} \in \mathbb{C}^{L_E\times K}$ are the analog combiner and digital combiner of the eavesdropper, $\mathbf{n}_e \in \mathbb{C}^{N_e\times 1} \sim \mathcal{CN}(0,\sigma_e^2)$.

At the end of phase-II, the kth destination receives signal from the relay, and the received signal is as follows

$$\mathbf{d}_k = \mathbf{H}_{2,k}\mathbf{x}_r + \mathbf{n}_k, \tag{7}$$

where $\mathbf{H}_{2,k} \in \mathbb{C}^{N_D \times N_R}$ is the second-hop channel matrix between the relay and destination k. $\mathbf{n}_k \in \mathbb{C}^{N_D \times 1} \sim \mathcal{CN}(0, \sigma_k^2)$ is the complex additive white Gaussian noise at the kth destination.

At the kth destination, the RF combiner $\mathbf{W}_k \in C^{N_D \times 1}$ is used to process the received signal:

$$\mathbf{y}_k = \mathbf{W}_k^H \mathbf{H}_{2,k} \mathbf{G}_{RF-T} \mathbf{G}_{BB} \mathbf{G}_{RF-R} \mathbf{H}_1 \mathbf{F}_{RF} \mathbf{F}_{BB} \mathbf{s} + \mathbf{W}_k^H \mathbf{H}_{2,k} \mathbf{G}_{RF-T} \mathbf{G}_{BB} \mathbf{G}_{RF-R} \mathbf{n}_r + \mathbf{W}_k^H \mathbf{n}_k. \quad (8)$$

The intercepted signal by the eavesdropper during phase-II is as follows:

$$\mathbf{y}_{e,2} = \mathbf{W}_{BB,e}^H \mathbf{W}_{RF,e}^H \mathbf{H}_{2,e} \mathbf{G}_{RF-T} \mathbf{G}_{BB} \mathbf{G}_{RF-R} \mathbf{H}_1 \mathbf{F}_{RF} \mathbf{F}_{BB} \mathbf{s} + \mathbf{W}_{BB,e}^H \mathbf{W}_{RF,e}^H \mathbf{H}_{2,e} \mathbf{G}_{RF-T} \mathbf{G}_{BB} \mathbf{G}_{RF-R} \mathbf{n}_r + \mathbf{W}_{BB,e}^H \mathbf{W}_{RF,e}^H \mathbf{n}_e. \quad (9)$$

The digital beamforming matrix $\mathbf{F}_{BB} \in \mathbb{C}^{L_S \times K}$ can be further expressed as $\mathbf{F}_{BB} = [\mathbf{F}_{BB,1}, \mathbf{F}_{BB,2}, \ldots, \mathbf{F}_{BB,K}]$. To correspond to the algorithm of this paper and the convenience of narration, we only consider $\mathbf{G}_{RF-R}$ during phase-I. $\mathbf{G}_{BB}$ and $\mathbf{G}_{RF-R}$ are considered during phase-II. To improve the secrecy performance, each source node adopts Wyners encoding scheme with transmission rate R_t and secrecy rate R_s. The difference between R_t and R_s is used as a redundancy rate against eavesdropping. The rate at the relay will be

$$\mathbf{R}_{k,1} = \log_2 \left(\frac{\left\| \mathbf{G}_{RF-R} \mathbf{H}_1 \mathbf{F}_{RF} \mathbf{F}_{BB,k} \right\|^2}{I_{k,1} + \|\mathbf{G}_{RF-R}\|^2 \sigma_e^2} \right), \quad (10)$$

where $I_{k,1} = \sum_{n \neq k} \left\| \mathbf{G}_{RF-R} \mathbf{H}_1 \mathbf{F}_{RF} \mathbf{F}_{BB,n} \right\|^2$ represents the interference between different data streams at the kth destination in phase-I.

The rate of the eavesdropper will be

$$\mathbf{R}_{e,1} = \log_2 \left(\frac{\left\| \mathbf{W}_{BB,e}^H \mathbf{W}_{RF,e}^H \mathbf{H}_{1,e} \mathbf{F}_{RF} \mathbf{F}_{BB,k} \right\|^2}{I_{e,1} + \left\| \mathbf{W}_{BB,e}^H \mathbf{W}_{RF,e}^H \right\|^2 \sigma_e^2} \right), \quad (11)$$

where $I_{e,1} = \sum_{n \neq k} \left\| \mathbf{W}_{BB,e}^H \mathbf{W}_{RF,e}^H \mathbf{H}_{1,e} \mathbf{F}_{RF} \mathbf{F}_{BB,n} \right\|^2$ denotes the interference between different data streams at the eavesdropper in phase-I.

The secrecy rate during phase-I will be [30]

$$\mathbf{R}_{\sec,1} = \left(\mathbf{R}_{k,1} - \mathbf{R}_{e,1} \right)^+. \quad (12)$$

During phase-II, the rate of the kth destination is given in (13), as shown at the bottom of this page [31], where $I_{k,2}$ represents the interference at the kth destination in phase-II.

For a typical destination k, the rate of the eavesdropper during phase-II is given in (14), as shown at the bottom of this page [31]. where $I_{e,2}$ represents the interference at the eavesdropper in phase-II, $I_{k,2}$ represents the interference at the kth destination in phase-II.

The secrecy rate during phase-II will be [30]

$$\mathbf{R}_{\sec,2} = \left(\mathbf{R}_{k,2} - \mathbf{R}_{e,2} \right)^+. \quad (15)$$

The secrecy rate of the kth destination cannot be greater than the secrecy rate both in the first time slot and in the second time slot. Similar with [29], The secrecy rate of the whole transmission will be

$$\mathbf{R}_{\sec,total} = \frac{1}{2} \min \left(\mathbf{R}_{\sec,1}, \mathbf{R}_{\sec,2} \right), \quad (16)$$

where the factor $\frac{1}{2}$ arises from the fact that two orthogonal time slots are required for completing the message transmission From (12), (15) and (16), if the eavesdropper has a channel advantage over the destinations, we cannot get a positive secrecy rate.

B. MILLIMETER-WAVE CHANNEL MODEL

In order to reflect the sparse scattering characteristics of the millimeter wave channel, the S-V (Saleh-Valenzuela) model is commonly used [14]. Assume the number of scattering clusters is represented by L, and each cluster contains one path. A uniform linear array is employed. The mm-wave channel matrices for the source-to-relay (S-R), relay-to-destination (R-D), source-to-eve (S-E) and relay-to-eve (R-E)

$$\mathbf{R}_{k,2} = \log_2 \left(1 + \frac{\left\| \mathbf{W}_k^H \mathbf{H}_{2,k} \mathbf{G}_{RF-T} \mathbf{G}_{BB} \mathbf{G}_{RF-R} \mathbf{H}_1 \mathbf{F}_{RF} \mathbf{F}_{BB,k} \right\|^2}{I_{k,2} + \left\| \mathbf{W}_k^H \mathbf{H}_{2,k} \mathbf{G}_{RF-T} \mathbf{G}_{BB} \mathbf{G}_{RF-R} \right\|^2 \sigma_r^2 + \|\mathbf{W}_k\|^2 \sigma_k^2} \right)$$
$$I_{k,2} = \sum_{n \neq k} \left\| \mathbf{W}_n^H \mathbf{H}_{2,n} \mathbf{G}_{RF-T} \mathbf{G}_{BB} \mathbf{G}_{RF-R} \mathbf{H}_1 \mathbf{F}_{RF} \mathbf{F}_{BB,n} \right\|^2 \quad (13)$$

$$\mathbf{R}_{e,2} = \log_2 \left(\frac{\left\| \mathbf{W}_{BB,e}^H \mathbf{W}_{RF,e}^H \mathbf{H}_{2,e} \mathbf{G}_{RF-T} \mathbf{G}_{BB} \mathbf{G}_{RF-R} \mathbf{H}_1 \mathbf{F}_{RF} \mathbf{F}_{BB,k} \right\|^2}{I_{e,2} + \left\| \mathbf{W}_{BB,e}^H \mathbf{W}_{RF,e}^H \mathbf{H}_{2,e} \mathbf{G}_{RF-T} \mathbf{G}_{BB} \mathbf{G}_{RF-R} \right\|^2 \sigma_r^2 + \left\| \mathbf{W}_{BB,e}^H \mathbf{W}_{RF,e}^H \right\|^2 \sigma_e^2} \right)$$
$$I_{e,2} = \sum_{n \neq k} \left\| \mathbf{W}_{BB,e}^H \mathbf{W}_{RF,e}^H \mathbf{H}_{2,e} \mathbf{G}_{RF-T} \mathbf{G}_{BB} \mathbf{G}_{RF-R} \mathbf{H}_1 \mathbf{F}_{RF} \mathbf{F}_{BB,n} \right\|^2 \quad (14)$$

links can be respectively expressed as

$$\begin{cases} \mathbf{H}_1 = \sqrt{\frac{N_S N_R}{L_{SD}}} \sum_{l=1}^{L_{SD}} \alpha_l \mathbf{a}_r(\theta_l) \mathbf{a}_s^H(\phi_l) \\ \mathbf{H}_{2,k} = \sqrt{\frac{N_R N_D}{L_{RD}}} \sum_{l=1}^{L_{RD}} \alpha_{k,l} \mathbf{a}_d(\theta_{k,l}) \mathbf{a}_r^H(\phi_{k,l}) \\ \mathbf{H}_{1,e} = \sqrt{\frac{N_S N_E}{L_{SE}}} \sum_{l=1}^{L_{SE}} \alpha_l \mathbf{a}_e(\theta_l) \mathbf{a}_s^H(\phi_l) \\ \mathbf{H}_{2,e} = \sqrt{\frac{N_D N_E}{L_{DE}}} \sum_{l=1}^{L_{RE}} \alpha_l \mathbf{a}_r(\theta_l) \mathbf{a}_e^H(\phi_l), \end{cases} \tag{17}$$

where L_{xy} denotes the cluster number for different links. α_l denotes the complex gain of the lth cluster and further suppose that$\alpha_l \sim \mathcal{CN}(\bar{\alpha}, 1)$. $\bar{\alpha}$ denote the average path-loss exponent. θ_l and φ_l are the AOA and AOD of the lth cluster, respectively, which are uniformly distributed over $(-\pi, +\pi)$. The array response vector is given by

$$\mathbf{a}(\psi) = \frac{1}{\sqrt{N}} \left[1, e^{j(2\pi/\lambda)d\sin(\psi)}, \ldots, e^{j(N-1)(2\pi/\lambda)d\sin(\psi)}\right]^T, \tag{18}$$

where N is the array antennas, λ is the radio wavelength, d is the distance between antenna elements and ψ is either AoA or AoD.

III. ARTIFICIAL NOISE AIDED TWO-STAGE SECURE HYBRID BEAMFORMING ALGORITHM

In this section, we put forward an artificial noise aided two-stage secure hybrid beamforming algorithm to maximize the secrecy rate of the typical destination. The secrecy rate of a typical destination in (12) and (15) cannot always be positive and artificial noise is preferred to get a high secrecy rate. Due to the constraints on the phase shifters, the analog beamforming/combining matrices can take only certain values. Hence, these matrices need to be selected from finite-size codebooks. Let $\mathcal{F}$, $\mathcal{W}$, $\mathcal{G}_R$ and $\mathcal{G}_T$ denote the set of RF beamforming matrices $\mathbf{F}_{RF}(:, l), l = 1, \ldots, L_S$, $\mathbf{W}_k$, $\mathbf{G}_{RF-R}(l, :), l = 1, \ldots, K$ and $\mathbf{G}_{RF-T}(:, l), l = 1, \ldots L_R$, respectively. Assume the codebooks of all these RF matrices are quantized by B bits for simplicity and then

$$\begin{cases} \mathcal{F} = \{\mathbf{a}_s(2\pi i/2^B) : i = 1, \ldots, 2^B\} \\ \mathcal{W} = \{\mathbf{a}_d(2\pi i/2^B) : i = 1, \ldots, 2^B\} \\ \mathcal{G}_R = \mathcal{G}_T = \{\mathbf{a}_s(2\pi i/2^B) : i = 1, \ldots, 2^B\}. \end{cases} \tag{19}$$

The problem to maximize $\mathbf{R}_{\sec,total}$ is an intractable problem because its solution requires a search over the entire space of all possible RF matrices' combinations [32]. Further, all the digital matrices need to be jointly designed with the analog ones, and this may require the large feedback of the channel matrices in practice, consequently increasing the complexity. In addition, the relay system is more complicated than direct transmission. The main idea of the proposed algorithm is to consider the beamforming design in phase-I and phase-II respectively. Then, for every phase, we divide the calculation of the beamforming matrices into two stages. The two-stage method is first proposed in [33], in which the beamforming design is split into two different domains, each with different constraints. In the first stage, the RF analog beamforming matrices are designed to obtain the large array gain provided by the vast number of antennas. In the second stage, the baseband digital beamforming matrices is designed to manage the interference between destinations. Artificial noise strategy is also applied based on Singular Value Decomposition (SVD) decomposition [34] in the second stage to deteriorate eavesdropping channel.

A. BEAMFORMING MATRICES DESIGN IN PHASE-I

The source transmits information-bearing signals and artificial noise to the relay during phase-I. Then the transmit signals become

$$\mathbf{x}_s = \mathbf{F}_{RF}\left(\mathbf{F}_{BB}\mathbf{s} + \mathbf{F}_{BB,z}\mathbf{z}_1\right), \tag{20}$$

where $\mathbf{z}_1$ represents the $(L_S - K) \times 1$ AN vector. $\mathbb{E}\left\{\mathbf{z}_1\mathbf{z}_1^H\right\} = \mathbf{I}_{L_S-K}$. $\mathbf{F}_{BB,z}$ is the digital precoder associated with the AN vector $\mathbf{z}_1$. Let $P_{N,1}$ denote the AN power at the source. $\left\|\mathbf{F}_{RF}\mathbf{F}_{BB,z}\right\| = P_{N,1}$, $P_S + P_{N,1} = P_{total}$. We aim to design $\mathbf{F}_{RF}$, $\mathbf{G}_{RF-R}$, $\mathbf{F}_{BB}$ and $\mathbf{F}_{BB,z}$ during phase-I.

In the first stage, the source and the relay design the RF beamforming and combining matrices $\mathbf{F}_{RF}$, $\mathbf{G}_{RF-R}$ to maximize the desired signal power, neglecting interference between different data streams. The joint design problem can be expressed by the following optimization problem:

$$\left\{\mathbf{g}_i^*, \mathbf{f}_i^*\right\} = \underset{\mathbf{g}_i \in \mathcal{G}_R \mathbf{f}_i \in \mathcal{F}}{\arg\max} \left\|\mathbf{g}_i \mathbf{H}_1 \mathbf{f}_i\right\|, \quad i = 1, 2, \ldots K, \tag{21}$$

where $\mathbf{g}_i$ and $\mathbf{f}_i$ denote the ith row of $\mathbf{G}_{RF-R}$ and the ith column of $\mathbf{F}_{RF}$ in a descending order according to their respective Frobenius norms. We select vectors $\mathbf{v}_i \in \mathcal{F}$ from the set $\mathcal{F}$ to fill the extra $L_S - K$ columns of $\mathbf{F}_{RF}$. The extra $L_S - K$ columns offers the extra $L_S - K$ spatial degree of freedom (DoF) seen from the baseband while keeping the low-complexity feature. Then assign them to the RF matrices:

$$\begin{cases} \mathbf{G}_{RF-R}^*(i, :) = \mathbf{g}_i^*, & i = 1, \ldots, K \\ \mathbf{F}_{RF}^*(:, i) = \mathbf{f}_i^*, & i = 1, \ldots, K \\ \mathbf{F}_{RF}^*(:, i) = \mathbf{v}_i, & i = K+1, \ldots, L_S. \end{cases} \tag{22}$$

This is the typical single-user RF beamforming design problem. There are many beam training algorithms developed for this problem such as [35] and [36], which have a low training overhead and low-complexity.

In the second stage, we can obtain the effective channel $\tilde{\mathbf{H}}_1 = \mathbf{G}_{RF-R}\mathbf{H}_1\mathbf{F}_{RF}$. Then, the source designs $\mathbf{F}_{BB}$ bases on zero-forcing (ZF). ZF scheme performs well in MIMO systems with low complexity [37]. $\mathbf{F}_{BB}$ should have a form of

$$\mathbf{F}_{BB} = \tilde{\mathbf{H}}_1^H\left(\tilde{\mathbf{H}}_1\tilde{\mathbf{H}}_1^H\right)^{-1}. \tag{23}$$

Then $\mathbf{F}_{BB}$ can be normalized as

$$\mathbf{F}_{BB} = \frac{\mathbf{F}_{BB}}{\left\|\mathbf{F}_{RF}\mathbf{F}_{BB}\right\|}. \tag{24}$$

As for the AN digital precoder $\mathbf{F}_{BB,z}$, an SVD-based method is employed to put AN in the null space of $\tilde{\mathbf{H}}_1$ so that AN doesn't degrade the reception of the relay. We should have

$$\tilde{\mathbf{H}}_1 \mathbf{F}_{BB,z} = 0. \tag{25}$$

Easy to know that $\tilde{\mathbf{H}}_1 \in C^{K \times L_S}$, $L_S > K$. No matter what $\tilde{\mathbf{H}}_1$ is, there is always a null space for $\tilde{\mathbf{H}}_1$. Extra RF chains ($L_S > K$) at the source provide freedom to generate AN. The SVD of the channel matrix $\tilde{\mathbf{H}}_1$ can be denoted by

$$\tilde{\mathbf{H}}_1 = \tilde{\mathbf{U}}_1 \tilde{\sum}_1 \tilde{\mathbf{V}}_1^H. \tag{26}$$

The digital precoder $\mathbf{F}_{BB,z}$ for the AN should have a form of

$$\mathbf{F}_{BB,z} = \tilde{\mathbf{V}}_1(:, K+1 : L_S). \tag{27}$$

Finally, $\mathbf{F}_{BB,z}$ can be normalized as

$$\mathbf{F}_{BB,z} = \frac{\mathbf{F}_{BB,z}}{\left\| \mathbf{F}_{RF} \mathbf{F}_{BB,z} \right\|}. \tag{28}$$

The proposed algorithm in phase-I is summarized in **Algorithm 1**.

Algorithm 1 The Proposed Algorithm in Phase-I

First stage:

1. The source and the relay select $\mathbf{g}_i^*$ and $\mathbf{f}_i^*$ that solve

$$\left\{\mathbf{g}_i^*, \mathbf{f}_i^*\right\} = \underset{\mathbf{g}_i \in \mathcal{G} \mathbf{f}_i \in \mathcal{F}}{\arg\max} \left\| \mathbf{g}_i \mathbf{H}_1 \mathbf{f}_i \right\|, \quad i = 1, 2, \ldots K$$

2. The source sets $\mathbf{F}_{RF} = \left[\mathbf{f}_1^*, \ldots, \mathbf{f}_K^*, \mathbf{v}_{K+1}, \ldots, \mathbf{v}_{L_S}\right]$

3. The relay sets $\mathbf{G}_{RF-R} = \left[\mathbf{g}_1^*, \ldots, \mathbf{g}_K^*\right]$

Second stage:

4. The relay feeds $\tilde{\mathbf{H}}_1 = \mathbf{G}_{RF-R} \mathbf{H}_1 \mathbf{F}_{RF}$ back to the source

5. The source designs $\mathbf{F}_{BB} = \tilde{\mathbf{H}}_1^H \left(\tilde{\mathbf{H}}_1 \tilde{\mathbf{H}}_1^H\right)^{-1}$ and normalizes $\mathbf{F}_{BB} = \frac{\mathbf{F}_{BB}}{\|\mathbf{F}_{RF}\mathbf{F}_{BB}\|}$

6. The source performs SVD decomposition $\tilde{\mathbf{H}}_1 = \tilde{\mathbf{U}}_1 \tilde{\sum}_1 \tilde{\mathbf{V}}_1^H$ and designs, finally normalizes $\mathbf{F}_{BB,z} = \tilde{\mathbf{V}}_1(:, K+1 : L_S)$, $\mathbf{F}_{BB,z} = \frac{\mathbf{F}_{BB,z}}{\|\mathbf{F}_{RF}\mathbf{F}_{BB,z}\|}$

Assume ZF is able to perform perfect interference cancellation and there is no artificial noise leaked to the destinations. Equation (10) becomes

$$\mathbf{R}_{k,1} = \log_2 \left(1 + \frac{\left\| \mathbf{G}_{RF-R} \mathbf{H}_1 \mathbf{F}_{RF} \mathbf{F}_{BB,k} \right\|^2}{\left\| \mathbf{G}_{RF-R} \right\|^2 \sigma_e^2}\right). \tag{29}$$

Equation (11) becomes as equation (30), shown at the bottom of this page.

B. BEAMFORMING MATRICES DESIGN IN PHASE-II

The relay forward signals from the source and AN to the destinations in phase-II. Then the transmit signals at relay become

$$\begin{aligned} \mathbf{x}_r = & \mathbf{G}_{RF-T} \mathbf{G}_{BB} \mathbf{G}_{RF-R} \mathbf{H}_1 \mathbf{F}_{RF} \mathbf{F}_{BB} \mathbf{s} \\ & + \mathbf{G}_{RF-T} \mathbf{G}_{BB,z} \mathbf{z}_2 + \mathbf{G}_{RF-T} \mathbf{G}_{BB} \mathbf{G}_{RF-R} \mathbf{n}_r. \end{aligned} \tag{31}$$

At a typical destination k, the received signals become

$$\begin{aligned} \mathbf{y}_k = & \mathbf{W}_k^H \mathbf{H}_{2,k} \mathbf{G}_{RF-T} \mathbf{G}_{BB} \mathbf{G}_{RF-R} \mathbf{H}_1 \mathbf{F}_{RF} \mathbf{F}_{BB} \mathbf{s} \\ & + \mathbf{W}_k^H \mathbf{H}_{2,k} \mathbf{G}_{RF-T} \mathbf{G}_{BB,z} \mathbf{z}_2 + \mathbf{W}_k^H \mathbf{H}_{2,k} \mathbf{G}_{RF-T} \\ & \times \mathbf{G}_{BB} \mathbf{G}_{RF-R} \mathbf{n}_r + \mathbf{W}_k^H \mathbf{n}_k, \end{aligned} \tag{32}$$

where $\mathbf{z}_2$ represents the $(L_R - K) \times 1$ AN vector $\mathbb{E}\left\{\mathbf{z}_2 \mathbf{z}_2^H\right\} = \mathbf{I}_{L_R-K}$. $\mathbf{G}_{BB,z}$ is the digital precoder associated with the AN vector $\mathbf{z}_2$. Let $P_{N,2}$ denote the AN power at the relay. $\left\| \mathbf{G}_{RF-T} \mathbf{G}_{BB,z} \right\| = P_{N,2}$, $P_R + P_{N,2} = P_{total}$. Define $\phi = \frac{P_{N,1}}{P_S} = \frac{P_{N,2}}{P_R}$ as the AN power allocation factor. We aim to design $\mathbf{W}_k$, $\mathbf{G}_{RF-T}$, $\mathbf{G}_{BB}$ and $\mathbf{G}_{BB,z}$ in phase-II.

In the first stage, the relay and each destination design the RF beamforming and combining matrices $\mathbf{G}_{RF-T}$, $\mathbf{W}_k$ to maximize the desired signal power, neglecting interference between different destinations. The joint design problem can be expressed by the following optimization problem:

$$\left\{\mathbf{w}_k^*, \mathbf{g}_k^*\right\} = \underset{\mathbf{w}_k \in \mathcal{W} \mathbf{g}_k \in \mathcal{G}_T}{\arg\max} \left\| \mathbf{w}_k^H \mathbf{H}_{2,k} \mathbf{g}_k \right\|, \quad k = 1, 2, \ldots K. \tag{33}$$

We simply generate random vector $\mathbf{v}_i \in \mathcal{G}_T$ to fill the extra columns of $\mathbf{G}_{RF-T}$, which offers the extra $L_R - K$ spatial degree of freedom (DoF) seen from the baseband $\mathbf{G}_{BB}$. Then assign them to the RF matrices

$$\begin{cases} \mathbf{W}_k^* = \mathbf{w}_k^*, & k = 1, \ldots, K \\ \mathbf{G}_{RF-T}^* (:, k) = \mathbf{g}_k^*, & k = 1, \ldots, K \\ \mathbf{G}_{RF-T}^* (:, i) = \mathbf{v}_i, & i = K+1, \ldots, L_R \end{cases} \tag{34}$$

This is the typical single-user RF beamforming design problem discussed in phase-I.

In the second stage, we can obtain the kth destinations effective channel $\tilde{\mathbf{H}}_{2,k} = \mathbf{W}_k^H \mathbf{H}_{2,k} \mathbf{G}_{RF-T}$. Then the source designs $\mathbf{G}_{BB}$ based on ZF scheme. Let $\tilde{\mathbf{H}}_2 = \left[\tilde{\mathbf{H}}_{2,1}^T, \ldots, \tilde{\mathbf{H}}_{2,k}^T\right]^T$. $\mathbf{G}_{BB}$ should have a form of

$$\mathbf{G}_{BB} = \tilde{\mathbf{H}}_2^H \left(\tilde{\mathbf{H}}_2 \tilde{\mathbf{H}}_2^H\right)^{-1}. \tag{35}$$

Then $\mathbf{G}_{BB}$ can be normalized as

$$\mathbf{G}_{BB} = \frac{\mathbf{G}_{BB}}{\left\| \mathbf{G}_{RF,T} \mathbf{G}_{BB} \right\|}. \tag{36}$$

$$\mathbf{R}_{e,1} = \log_2 \left(1 + \frac{\left\| \mathbf{W}_{BB,e}^H \mathbf{W}_{RF,e}^H \mathbf{H}_{1,e} \mathbf{F}_{RF} \mathbf{F}_{BB,k} \right\|^2}{I_{e,1} + \left\| \mathbf{W}_{BB,e}^H \mathbf{W}_{RF,e}^H \mathbf{H}_{1,e} \mathbf{F}_{RF} \mathbf{F}_{BB,z} \right\|^2 + \left\| \mathbf{W}_{BB,e}^H \mathbf{W}_{RF,e}^H \right\|^2 \sigma_e^2}\right) \tag{30}$$

As for the AN digital precoder $\mathbf{G}_{BB,z}$, an SVD-based method is employed to put AN in the null space of $\tilde{\mathbf{H}}_2$ so that AN doesn't degrade the reception of the destinations. We should have

$$\tilde{\mathbf{H}}_2\mathbf{F}_{BB,z} = 0 \tag{37}$$

Then, we can get $\tilde{\mathbf{H}}_2 \in C^{K\times L_R}$, $L_R > K$. No matter what $\tilde{\mathbf{H}}_2$ is, there is always a null space for $\tilde{\mathbf{H}}_2$. Extra RF chains ($L_R > K$) at the relay provide freedom to generate AN. The SVD of the channel matrix $\tilde{\mathbf{H}}_2$ can be denoted by

$$\tilde{\mathbf{H}}_2 = \tilde{\mathbf{U}}_2\tilde{\sum}_2\tilde{\mathbf{V}}_2^H. \tag{38}$$

The digital precoder $\mathbf{G}_{BB,z}$ for the AN should have a form of

$$\mathbf{G}_{BB,z} = \tilde{\mathbf{V}}_2(:, K+1 : L_R). \tag{39}$$

Finally, $\mathbf{G}_{BB,z}$ can be normalized as

$$\mathbf{G}_{BB,z} = \frac{\mathbf{G}_{BB,z}}{\left\|\mathbf{G}_{RF-T}\mathbf{G}_{BB,z}\right\|}. \tag{40}$$

The proposed algorithm in phase-II is summarized in **Algorithm 2**.

Just like the discussion in phase-I, we assume that ZF scheme is able to perform perfect interference cancellation between different destinations and there is no artificial noise leaked to the destinations, then equation (41) and (42), are shown at the bottom of this page.

Algorithm 2 The Proposed Algorithm in Phase-II

First stage:

1. For each destination k

The relay and the destination select and that solve

$$\{\mathbf{w}_k^*, \mathbf{g}_k^*\} = \underset{\mathbf{w}_k\in\mathcal{W}\mathbf{g}_k\in\mathcal{G}_T}{\arg\max} \left\|\mathbf{w}_k^H\mathbf{H}_{2,k}\mathbf{g}_k\right\|$$

The destination sets $\mathbf{W}_k^* = \mathbf{w}_k^*$

2. The relay sets $\mathbf{G}_{RF-T} = \left[\mathbf{g}_1^*, \ldots \mathbf{g}_K^*, \mathbf{v}_{K+1}, \ldots, \mathbf{v}_{L_R}\right]$

Second stage:

3. For each destination k

The destination feeds $\tilde{\mathbf{H}}_{2,k} = \mathbf{W}_k^H\mathbf{H}_{2,k}\mathbf{G}_{RF-T}$ back to the relay

$$\{\mathbf{w}_k^*, \mathbf{g}_k^*\} = \underset{\mathbf{w}_k\in\mathcal{W}\mathbf{g}_k\in\mathcal{G}_T}{\arg\max} \left\|\mathbf{w}_k^H\mathbf{H}_{2,k}\mathbf{g}_k\right\|$$

4. The relay designs $\mathbf{G}_{BB} = \tilde{\mathbf{H}}_2^H\left(\tilde{\mathbf{H}}_2\tilde{\mathbf{H}}_2^H\right)^{-1}$, $\tilde{\mathbf{H}}_2 = \left[\tilde{\mathbf{H}}_{2,1}^T, \ldots, \tilde{\mathbf{H}}_{2,k}^T\right]^T$; normalizes $\mathbf{F}_{BB} = \frac{\mathbf{F}_{BB}}{\|\mathbf{F}_{RF}\mathbf{F}_{BB}\|}$

5. The source performs SVD decomposition $\tilde{\mathbf{H}}_2 = \tilde{\mathbf{U}}_2\tilde{\sum}_2\tilde{\mathbf{V}}_2^H$ and designs $\mathbf{G}_{BB,z} = \tilde{\mathbf{V}}(:, K+1 : L_R)$, finally normalizes $\mathbf{G}_{BB,z} = \frac{\mathbf{G}_{BB,z}}{\|\mathbf{G}_{RF-T}\mathbf{G}_{BB,z}\|}$

IV. NUMERICAL RESULTS

In this section, we provide the simulation results to evaluate the secrecy rate of the proposed algorithm using numerical simulations. Unless otherwise stated, the source, relay, destination and eavesdropper are equipped with $N_S = 128$, $N_R = 64$, $N_D = 16$ and antennas $N_E = 64$ ($L_S = 6$, $L_R = 6$, $L_D = 1$ and $L_E = 6$ RF chains), respectively. The antenna spacing of all uniform linear arrays is $d = \lambda/2$. The source and the relay can simultaneously serve $K = 4$ destinations. The number of scattering clusters is $L = 3$. The AoA/AoD is assumed to be uniformly distributed in $[0, 2\pi]$. For simplicity, the noise variance σ_r^2, σ_k^2 and σ_e^2 are set to 1. The RF codebooks are quantized with $B = 4$ bits. The AN power allocation factor $\phi = 0.1$. The SNR is defined as $P_R/\sigma_k^2(P_R/\sigma_k^2)$. All simulation results are averaged over 1000 randomly generated channel realizations. We do not consider the CSI error.

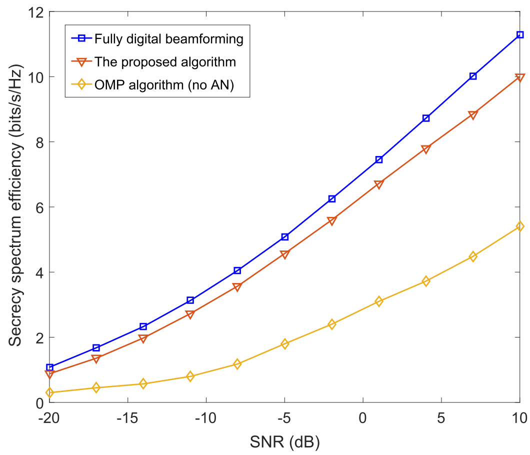


FIGURE 2. Secrecy spectrum efficiency comparison versus different SNR.

Fig.2 compares the performance of the proposed algorithm with the fully digital beamforming and orthogonal matching

$$\mathbf{R}_{k,2} = \log_2\left(1+\frac{\left\|\mathbf{W}_k^H\mathbf{H}_{2,k}\mathbf{G}_{RF-T}\mathbf{G}_{BB}\mathbf{G}_{RF-R}\mathbf{H}_1\mathbf{F}_{RF}\mathbf{F}_{BB,k}\right\|^2}{\left\|\mathbf{W}_k^H\mathbf{H}_{2,k}\mathbf{G}_{RF-T}\mathbf{G}_{BB}\mathbf{G}_{RF-R}\right\|^2\sigma_r^2+\|\mathbf{W}_k\|^2\sigma_k^2}\right) \tag{41}$$

$$\mathbf{R}_{e,2} = \log_2 \times\left(1+\frac{\left\|\mathbf{W}_{BB,e}^H\mathbf{W}_{RF,e}^H\mathbf{H}_{2,e}\mathbf{G}_{RF-T}\mathbf{G}_{BB}\mathbf{G}_{RF-R}\mathbf{H}_1\mathbf{F}_{RF}\mathbf{F}_{BB,k}\right\|^2}{I_{e,2}+\left\|\mathbf{W}_{BB,e}^H\mathbf{W}_{RF,e}^H\mathbf{H}_{2,e}\mathbf{G}_{RF-T}\mathbf{G}_{BB,z}\right\|^2+\left\|\mathbf{W}_{BB,e}^H\mathbf{W}_{RF,e}^H\mathbf{H}_{2,e}\mathbf{G}_{RF-T}\mathbf{G}_{BB}\mathbf{G}_{RF-R}\right\|^2\sigma_r^2+\left\|\mathbf{W}_{BB,e}^H\mathbf{W}_{RF,e}^H\right\|^2\sigma_e^2}\right) \tag{42}$$

pursuit (OMP) algorithm (no AN). The figure shows that the proposed algorithm outperforms the joint RF/baseband design using the OMP algorithm, which indicates that the AN strategy makes large contributions to the secrecy spectrum efficiency. By comparing the performance of the proposed hybrid beamforming and conventional fully digital beamforming, we observe that the proposed hybrid beamforming achieves satisfactory performance and keeps the number of RF chains much smaller than the number of antennas. This reduces hardware cost and power consumption. Conventional hybrid beamforming without secrecy design cannot cope with scenes with eavesdroppers. An AN based algorithm significantly increases secrecy spectrum efficiency although extra power is used to send AN.

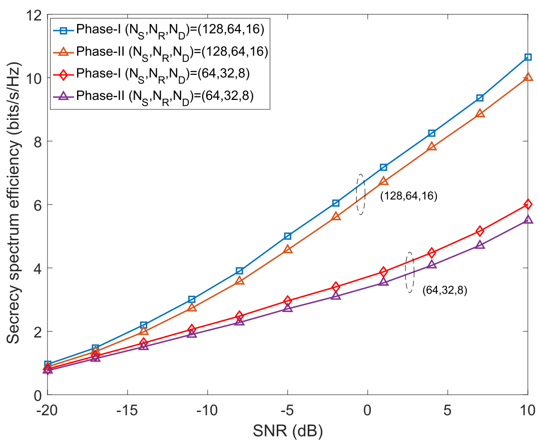


FIGURE 3. Comparison of secrecy spectrum efficiency for various numbers of antenna elements.

Fig.3 illustrates the performance changes with various numbers of antenna elements (with fixed number of RF chains). The figure shows that the secrecy spectrum efficiency can be significantly improved by increasing the number of antennas. Therefore, the number of RF chains employed in hybrid beamforming systems can be much less than the number antenna number, as long as the number of RF chains is larger than the number of destinations. We also notice that the secrecy spectrum efficiency in phase-I is higher than that in phase-II because more thermal noise is mixed into the information bearing signal. Fig.3 provides a guidance for practical system design: If the number of RF chains is limited due to the cost and consumption, we can increase antenna number to achieve higher system performance.

To illustrate the impact of RF quantization, Fig.4 shows the secrecy spectrum efficiency versus different numbers of quantization bits for the phase shifters. The performance of the system increases with the number of quantization bits increases. It should be noted that the power consumption and cost of the phase shifters become higher with increasing the quantization bit B. When the quantization bits increases to 5 or larger, the secrecy spectrum efficiency stays almost constant. That is to say infinitely increasing the

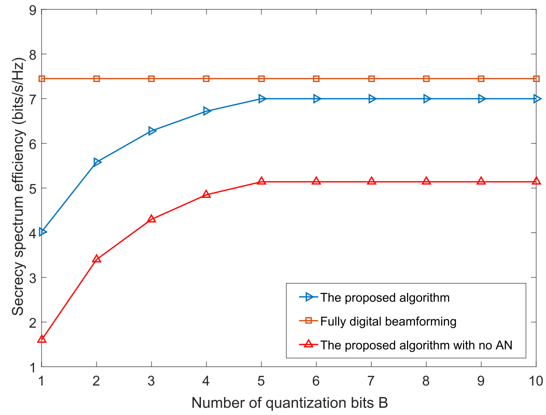


FIGURE 4. Effect of finite-resolution phase shifters on the secrecy spectrum efficiency with $SNR = 1dB$.

quantization accuracy is not necessary. The number of quantization bits needs to be the right size. The comparison between the proposed algorithm with AN and without AN suggests that the AN strategy can improve the secrecy spectrum efficiency.

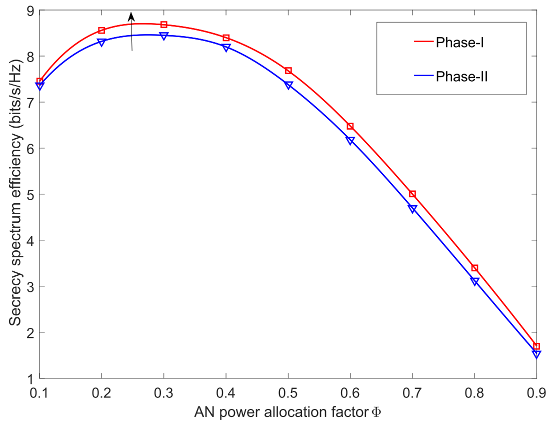


FIGURE 5. The secrecy spectrum efficiency VS with AN power allocation factor ϕ.

Fig.5 depicts the secrecy spectrum efficiency versus power allocation parameter ϕ with $SNR = 1dB$. As the artificial noise power allocation factor increases, eavesdropping link is degraded by artificial noise, and the safety spectrum efficiency gradually increases to the highest value. When the power allocation factor continues to increase, the transmit power of the information bearing signal is insufficient. The secrecy spectrum efficiency begins to decline. The optimal power allocation is almost in the region $\phi \in (0.2, 0.3)$, and the choice of ϕ is critical important to improve the secrecy rate. There is an optimal power distribution factor value, which makes the system performance optimal. At the same time, it should be pointed out that the power allocation factors are different under different SNR, so the power allocation factor needs to be robustly set.

V. CONCLUSION

In this paper, we propose an artificial noise aided two-stage secure hybrid beamforming algorithm in MIMO mm-wave relay eavesdropping system, in which the analog and digital beamforming designs are separated and the source and relay serve multiple destination nodes. Firstly, the system is modeled in the case of an eavesdropper from the perspective of physical layer security. Then the proposed beamforming algorithm is applied in both two phases. In phase-I, in the first stage, the source and the relay design the RF beamforming and combining matrices to maximize the desired signal power and neglect interference between different data streams. In the second stage, based on the effective channel, the source designs information signal digital beamforming matrix according to ZF scheme so that the interference between different destinations is cancelled. The AN digital beamforming matrix is designed to put in the null space of the effective channel based on SVD decomposition. The designs in phase-II is similar with that in phase-I. Furthermore, simulation results validate the effectiveness and the security of the proposed algorithm, which help us understand the proposed algorithm comprehensively.

REFERENCES

[1] T. S. Rappaport *et al.*, "Millimeter wave mobile communications for 5G cellular: It will work!" *IEEE Access*, vol. 1, pp. 335–349, 2013.

[2] M. Xiao *et al.*, "Millimeter wave communications for future mobile networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 9, pp. 1909–1935, Sep. 2017.

[3] L. Wei, R. Q. Hu, Y. Qian, and G. Wu, "Key elements to enable millimeter wave communications for 5G wireless systems," *IEEE Wireless Commun.*, vol. 21, no. 6, pp. 136–143, Dec. 2014.

[4] X. Yu, J. Zhang, M. Haenggi, and K. B. Letaief, "Coverage analysis for millimeter wave networks: The impact of directional antenna arrays," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 7, pp. 1498–1512, Jul. 2017.

[5] S. Biswas, S. Vuppala, J. Xue, and T. Ratnarajah, "On the performance of relay aided millimeter wave networks," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 3, pp. 576–588, Apr. 2016.

[6] 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.

[7] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

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

[9] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[10] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: A review," *China Commun.*, vol. 14, no. 12, pp. 1–14, 2017.

[11] S. Rangan, T. S. Rappaport, and E. Erkip, "Millimeter-wave cellular wireless networks: Potentials and challenges," *Proc. IEEE*, vol. 102, no. 3, pp. 366–385, Mar. 2014.

[12] A. Alkhateeb and R. W. Heath, Jr., "Frequency selective hybrid precoding for limited feedback millimeter wave systems," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 1801–1818, May 2016.

[13] W. Ni and X. Dong, "Hybrid block diagonalization for massive multiuser MIMO systems," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 201–211, Jan. 2016.

[14] X. Yu, J.-C. Shen, J. Zhang, and K. B. Letaief, "Alternating minimization algorithms for hybrid precoding in millimeter wave MIMO systems," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 3, pp. 485–500, Apr. 2016.

[15] X. Gao, L. Dai, S. Han, C.-L. I, and X. Wang, "Reliable beamspace channel estimation for millimeter-wave massive MIMO systems with lens antenna array," *IEEE Trans. Wireless Commun.*, vol. 16, no. 9, pp. 6010–6021, Sep. 2016.

[16] O. El Ayach, R. W. Heath, Jr., S. Abu-Surra, Z. Pi, and S. Rajagopal, "Low complexity precoding for large millimeter wave MIMO systems," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2012, pp. 3724–3729.

[17] O. El Ayach, S. Rajagopal, S. Abu-Surra, Z. Pi, and R. W. Heath, Jr., "Spatially sparse precoding in millimeter wave MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1499–1513, Mar. 2014.

[18] C.-B. Chae, T. Inoue, T. Inoue, and R. W. Heath, Jr., "Coordinated beamforming for the multiuser MIMO broadcast channel with limited feedforward," *IEEE Trans. Signal Process.*, vol. 56, no. 12, pp. 6044–6056, Dec. 2008.

[19] A. Alkhateeb, O. El Ayach, G. Leus, and R. W. Heath, Jr., "Channel estimation and hybrid precoding for millimeter wave cellular systems," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 831–846, Oct. 2014.

[20] S. Vuppala, Y. J. Tolossa, G. Kaddoum, and G. Abreu, "On the physical layer security analysis of hybrid millimeter wave networks," *IEEE Trans. Commun.*, vol. 66, no. 3, pp. 1139–1152, Mar. 2018.

[21] Y. R. Ramadan and H. Minn, "Artificial noise aided hybrid precoding design for secure mmWave MISO systems with partial channel knowledge," *IEEE Signal Process. Lett.*, vol. 24, no. 11, pp. 1729–1733, Nov. 2017.

[22] Y. R. Ramadan, H. Minn, and A. S. Ibrahim, "Hybrid analog–digital precoding design for secrecy mmWave MISO-OFDM systems," *IEEE Trans. Commun.*, vol. 65, no. 11, pp. 5009–5026, Nov. 2017.

[23] Z. Wang, M. Li, X. Tian, and Q. Liu, "Iterative hybrid precoder and combiner design for mmwave multiuser MIMO systems," *IEEE Commun. Lett.*, vol. 21, no. 7, pp. 1581–1584, Jul. 2017.

[24] L. Qing, H. Guangyao, and F. Xiaomei, "Physical layer security in multi-hop AF relay network based on compressed sensing," *IEEE Commun. Lett.*, vol. 22, no. 9, pp. 1882–1885, Sep. 2018.

[25] W. Aman, G. A. S. Sidhu, H. M. Furqan, and Z. Ali, "Enhancing physical layer security in AF relay–assisted multicarrier wireless transmission," *Trans. Emerg. Telecommun. Technol.*, no. 10, p. e3289, Jun. 2018.

[26] J.-S. Sheu, "Hybrid digital and analogue beamforming design for millimeter wave relaying systems," *J. Commun. Netw.*, vol. 19, no. 5, pp. 461–469, 2017.

[27] I. Krikidis and B. Ottersten, "Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling," *IEEE Signal Process. Lett.*, vol. 20, no. 2, pp. 141–144, Feb. 2013.

[28] H.-M. Wang, T. Zheng, and X.-G. Xia, "Secure MISO wiretap channels with multi-antenna passive eavesdropper via artificial fast fading," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 94–106, Jan. 2014.

[29] Q. Li, Y. Yang, W. K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks," *IEEE Trans. Signal Process.*, vol. 63, no. 1, pp. 206–220, Jan. 2015.

[30] W. Wang, K. C. Teh, and K. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1470–1482, Jun. 2017.

[31] S. Gong, C. Xing, Z. Fei, and S. Ma, "Millimeter-wave secrecy beamforming designs for two-way amplify-and-forward MIMO relaying networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2059–2071, Mar. 2017.

[32] J. G. Andrews, T. Bai, M. N. Kulkarni, A. Alkhateeb, A. K. Gupta, and R. W. Heath, Jr., "Modeling and analyzing millimeter wave cellular systems," *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 403–430, Jan. 2017.

[33] A. Alkhateeb, G. Leus, and R. W. Heath, Jr., "Limited feedback hybrid precoding for multi-user millimeter wave systems," *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6481–6494, Nov. 2015.

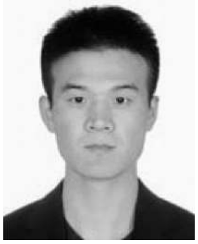
[34] T. Xie, L. Dai, X. Gao, M. Z. Shakir, and J. Li, "Geometric mean decomposition based hybrid precoding for millimeter-wave massive MIMO," *China Commun.*, vol. 15, no. 5, pp. 229–238, 2018.

[35] J. Wang *et al.*, "Beam codebook based beamforming protocol for multi-Gbps millimeter-wave WPAN systems," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 8, pp. 1390–1399, Oct. 2009.

[36] S. Hur, T. Kim, D. J. Love, J. V. Krogmeier, T. A. Thomas, and A. Ghosh, "Millimeter wave beamforming for wireless backhaul and access in small cell networks," *IEEE Trans. Commun.*, vol. 61, no. 10, pp. 4391–4403, Oct. 2013.

[37] H. Gao, T. Lv, S. Zhang, C. Yuen, and S. Yang, "Zero-forcing based MIMO two-way relay with relay antenna selection: Transmission scheme and diversity analysis," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4426–4437, Dec. 2012.

SHAOYU WANG received the B.E. degree from Xi'an Jiaotong University. He is currently pursuing the Ph.D. degree with the National Digital Switching System Engineering and Technological Research Center, Zhengzhou, China. His research interests include physical layer security in wireless networks and millimeter wave networks.



XIAOMING XU received the B.E. and B.S. degrees in communication engineering from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2011. He is currently an Instructor with the Laboratory of Mobile Communication Networks, National Digital Switching System Engineering and Technological Research Center. His research interests include stochastic geometry, cooperative communications, and physical-layer security of wireless communications.

KAIZHI HUANG received the B.E. degree in digital communication and the M.S. degree in communication and information system from the National Digital Switching System Engineering and Technological Research Center (NDSC), and the Ph.D. degree in communication and information system from Tsinghua University, Beijing, China, in 1995, 1998, and 2003 respectively. She has been a Faculty Member of NDSC, since 1998, where she is currently a Professor and the Director of Laboratory of Mobile Communication Networks. Her research interests include wireless network security and signal processing.

XINSHENG JI received the B.E. degree in digital communication and the M.S. degree from Fudan University, Shanghai, China, in 1984, and the M.S. degree from PLA Information Engineering University, Zhengzhou, China, in 1991. He is currently the Chief Engineer of the National Digital Switching System Engineering and Technological Research Center. He has been a member of the Network and Communication Specialist Group for the China 863 High Technology Program. He also has been the Senior Member of the China Institute of Communication. He has received as an Outstanding Expert of state in 2015. His major research interests include wireless communication, and security and signal processing.

YAJUN CHEN received the B.E. and the B.S. degrees from the University of Electronic Science and Technology of China and the Ph.D. degree from the National Digital Switching System Engineering and Technological Research Center, where he is currently an Instructor with the Laboratory of Mobile Communication Networks. His research interests include stochastic geometry, D2D communications, and the physical-layer security of wireless communications.

LIANG JIN received the Ph.D. degree from Xi'an Jiaotong University, Xi'an, China. He is currently a Professor and the Ph.D. supervisor with the National Digital Switching System Engineering and Technological Research Center. His research interests include wireless communication, physical layer security, and smart antenna.