

毫米波下行多用户系统安全混合波束成形算法

黄开枝 王少禹* 许晓明 陈亚军

(国家数字交换系统工程技术研究中心 郑州 450002)

摘要: 毫米波混合波束成形结构受到日益广泛的认可, 但缺乏以安全性为着眼点的混合波束成形算法研究, 特别是当窃听者具有多用户译码能力时, 系统安全性能无法得到保障。针对上述问题, 该文基于人工噪声辅助的思想提出一种毫米波下行多用户系统安全混合波束成形算法。首先, 将混合波束成形矩阵的模拟部分和数字部分解耦独立求解, 在充分考虑信道特性的基础上, 通过最大化用户接收信号能量和迫零思想分别设计有用信号的模拟和数字波束成形矩阵; 然后, 通过SVD分解设计人工噪声的基带数字预编码矩阵, 将人工噪声置于合法用户零空间。仿真结果表明, 人工噪声辅助的安全混合波束成形算法有效解决了存在具有多用户译码能力窃听者时系统的安全问题。

关键词: 毫米波多用户系统; 混合波束成形; 物理层安全; 人工噪声

中图分类号: TN92

文献标识码: A

文章编号: 1009-5896(2019)04-0952-07

DOI: 10.11999/JEIT180713

Security Hybrid Beamforming Algorithm for Millimeter Wave Downlink Multiuser System

HUANG Kaizhi WANG Shaoyu XU Xiaoming CHEN Yajun

(National Digital Switching System Engineering & Technological R & D Center,
Zhengzhou 450002, China)

Abstract: The millimeter-wave hybrid beamforming becomes a widely accepted beamforming method in millimeter-wave systems. However there is almost no hybrid beamforming algorithm based on security. Especially when the eavesdropper has multi-user decoding capability, the system security performance can not be guaranteed. To solve this problem, a security hybrid beamforming algorithm is proposed for millimeter wave downlink multiuser system based on artificial noise. First, the analog part and the digital part of the hybrid beamforming matrix are decoupled. Based on the channel characteristics, the analog and digital beamforming matrices of useful signals are designed by maximizing the user's received signal energy and Zero-Forcing (ZF). Then, the artificial noise baseband digital precoding matrix is designed by Singular Value Decomposition (SVD), and the artificial noise is placed in null space of the legal users and worsening eavesdropping channel. Simulation results show that the artificial noise-assisted secure hybrid beamforming algorithm solves effectively the security problem of the system when there are multi-user decoding ability eavesdroppers.

Key words: Millimeter wave multiuser system; Hybrid beamforming; Physical layer security; Artificial noise

1 引言

毫米波通信拥有丰富的可用频谱资源, 能够极大提升系统通信速率, 被认为是未来移动通信的关键技术之一^[1,2]。作为未来移动通信的重要组成部分,

毫米波通信所处的网络架构更加开放, 业务和场景更加多样, 面临大量未知的安全威胁, 泄露风险也大为增加。传统加密机制具有依赖计算复杂度和“补丁”式安全等弊端, 物理层安全利用无线信道的指纹特性, 挖掘系统的内生安全潜力, 从信息论角度为无线通信安全提供了新的解决思路^[3,4]。在毫米波通信系统中, 一方面发送端配备了大规模天线阵列, 为物理层安全信号处理提供了新的自由度; 另一方面, 毫米波系统中普遍采用的混合波束成形结构给传统物理层安全信号处理带来新的挑战^[5]。

收稿日期: 2018-07-17; 改回日期: 2018-12-20; 网络出版: 2019-01-02

*通信作者: 王少禹 2694183974@qq.com

基金项目: 国家自然科学基金(61701538, 61601514, 61501516, 61871404)

Foundation Items: The National Natural Science Foundation of China (61701538, 61601514, 61501516, 61871404)

相比于传统波束成形设计问题，毫米波混合波束成形问题涉及到多变量联合优化，且约束条件非凸，设计难度较大。文献[6]将毫米波混合预编码问题等效为欧式距离最小化问题，文献[7]进一步将该问题等效为稀疏信号重构问题，利用匹配追踪原理，提出了逼近无约束最优解的算法。文献[8]在单用户场景下，设计了一种低复杂度的信道估计算法，并将混合预编码设计问题等效为稀疏信号重构问题加以解决。文献[6-8]的解决思路相似，能够很好地逼近无约束最优解，但算法复杂度较高，模型局限于单用户系统，且未考虑系统窃听问题。在毫米波混合预编码物理层安全研究中，文献[9]针对毫米波MISO-OFDM系统，以最大化安全速率为目标设计了闭式混合预编码矩阵，但其假设已知窃听信道状态信息CSI(Channel State Information)，无法有效应对窃听信道CSI未知的情形。文献[10]在已知窃听信道状态信息的情况下，通过移除窃听信道和主信道的公有部分，设计了发送预编码和接收成形矩阵；在未知窃听者CSI时，设计了人工噪声策略，但其系统模型局限于单用户系统。本文同样考虑引入人工噪声策略增强安全性能。

本文将研究扩展到多用户系统且考虑窃听者具有多用户译码能力的情形，同时力求降低算法复杂度。相比于单用户系统，采用空分多址的多用户系统可以获得更大的系统容量，毫米波发送端的大规模天线阵列为多用户系统的实现提供了基础[5]。多个用户之间使用相同的时间和频率资源块，不可避免地带来用户间干扰，因此本文算法需要考虑如何消除用户间干扰。一般能力的窃听者(不具有多用户译码能力)会受到其他用户的叠加干扰，从而恶化窃听信道，通过合理的预编码设计方案、资源调度方案可获得物理层安全增益，但当窃听者具有多用户译码能力时，用户间干扰将失去作用，此时需要人工噪声技术对窃听者进行加扰。人工噪声技术以功率和发送端信号处理自由度为代价换取安全增益，能够有效抵抗具有多用户译码能力的窃听者。

针对以上问题，本文基于人工噪声辅助的思想提出了一种毫米波下行多用户系统安全混合波束成形算法。首先，构建了毫米波下行多用户系统窃听模型，并指出混合波束成形矩阵难以设计的问题；然后，在充分考虑信道特性的基础上，通过两阶段的设计过程将混合预编码矩阵分为模拟和数字两部分进行求解，在第1个阶段通过最大化用户接收信号能量设计有用信号的模拟波束成形矩阵，在第2个阶段利用迫零思想设计有用信号的数字波束成形矩阵；最后，通过SVD分解设计人工噪声的基带

数字预编码矩阵，将人工噪声置于合法用户零空间。仿真分析了模拟移相器量化精度、基站天线数目、人工噪声功率分配因子等对安全性能的影响。结果表明，该算法有效提升了毫米波下行多用户系统对抗具有多用户译码能力窃听者的安全性能。

2 系统模型

2.1 毫米波下行多用户系统窃听模型

考虑如图1所示的单小区毫米波下行多用户通信系统， K 个数据流通过基站同时同频地服务 K 个用户，分别表示为 U_1, U_2, \dots, U_K 。基站采用混合波束成形结构，如图2所示，该结构由基带的数字预编码器 F_{BB} 与射频频带的模拟预编码器 F_{RF} 连接而成，配备 N_t 根天线以及 L_t 条射频链路，为减少射频链路数，假设 $N_t \gg L_t$ ；为保证通信的有效性，需满足 $L_t > K$ ，若 $L_t \leq K$ ，当前用户无法被同时服务，采取适当的用户调度策略即可。用户处配备 N_r 根天线以及1条射频链路，仅采用模拟接收成形，以此降低用户终端的处理复杂度。窃听者配备 N_e 根天线， $N_e < N_t$ ，且具有多用户译码能力[1]。

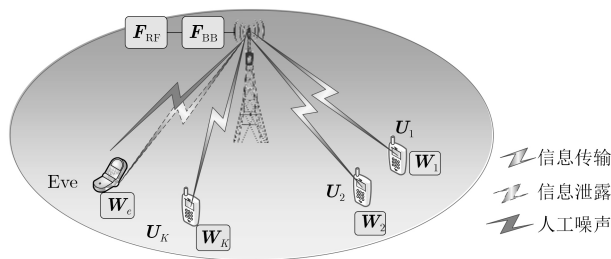


图1 毫米波下行多用户窃听系统模型

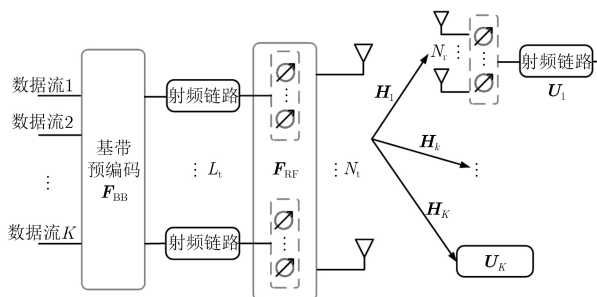


图2 混合波束成形结构

通信过程可简单描述为：基站端的 K 个数据流首先经过基带数字预编码处理，然后经过射频带模拟预编码发送出去；用户端信号在模拟域使用移相器进行接收处理。在下行信号发送过程中，窃听者试图窃听某一特定用户的信息。

K 个数据流经基站端混合预编码处理后，基站

端的发射信号可以表示为

$$\mathbf{x} = \mathbf{F}_{\text{RF}} \mathbf{F}_{\text{BB}} \mathbf{s} \quad (1)$$

$\mathbf{s} = [s_1, s_2, \dots, s_K]^T$ 且满足 $\mathbb{E}[\mathbf{s}\mathbf{s}^H] = \frac{P\mathbf{I}_K}{K}$, 其中, P 是基站发射功率; $\mathbf{F}_{\text{BB}} = [\mathbf{f}_1^{\text{BB}}, \mathbf{f}_2^{\text{BB}}, \dots, \mathbf{f}_K^{\text{BB}}] \in \mathbb{C}^{L_t \times K}$ 表示基带预编码矩阵, 相位和幅度均连续可调; $\mathbf{F}_{\text{RF}} \in \mathbb{C}^{N_t \times L_t}$ 表示射频带模拟预编码, 通过移相器实现, 满足恒模约束, 即 $|\mathbf{F}_{\text{RF}}^{ij}| = 1/\sqrt{N_t}$. 基站总功率约束为 $\|\mathbf{F}_{\text{RF}} \mathbf{F}_{\text{BB}}\|_F^2 = K$.

$$R_k = \log_2 \left(1 + \frac{\frac{P}{K} \mathbb{E} \left[\left\| \mathbf{W}_k^H \mathbf{H}_k \mathbf{F}_{\text{RF}} \mathbf{f}_k^{\text{BB}} \right\|^2 \right]}{\frac{P}{K} \sum_{n=1, n \neq k}^K \mathbb{E} \left[\left\| \mathbf{W}_k^H \mathbf{H}_k \mathbf{F}_{\text{RF}} \mathbf{f}_n^{\text{BB}} \right\|^2 \right] + \sigma^2} \right) \quad (3)$$

同理, 窃听者处截获的信号为

$$\mathbf{y}_{e,k} = \mathbf{W}_e^H \mathbf{H}_{e,k} \mathbf{F}_{\text{RF}} \sum_{n=1}^K \mathbf{f}_n^{\text{BB}} s_n + \mathbf{n}_e \quad (4)$$

其中, $\mathbf{H}_{e,k} \in \mathbb{C}^{N_e \times N_t}$ 是窃听信道矩阵; $\mathbf{W}_e \in \mathbb{C}^{N_e \times 1}$ 表示窃听者处的接收成形矩阵. $\mathbf{n}_e \in \mathbb{C}^{N_e \times 1}$ 是窃听者处的加性高斯白噪声, 功率同样设为 σ^2 . 由于窃听者具有多用户译码能力, 窃听者处的用户间干扰项可忽略. 针对第 k 个用户, 窃听者处的频谱效率为

$$R_{e,k} = \log_2 \left(1 + \frac{\frac{P}{K} \mathbb{E} \left[\left\| \mathbf{W}_e^H \mathbf{H}_{e,k} \mathbf{F}_{\text{RF}} \mathbf{f}_k^{\text{BB}} \right\|^2 \right]}{\sigma^2} \right) \quad (5)$$

由物理层安全理论可知, 用户 k 的安全频谱效率为

$$R_s = [R_k - R_{e,k}]^+ \quad (6)$$

将用户总安全速率作为优化目标, 则毫米波多用户系统的波束成形设计问题可表示为

$$\left. \begin{aligned} & \left\{ \mathbf{F}_{\text{RF}}^*, \mathbf{F}_{\text{BB}}^*, \{ \mathbf{W}_k^* \}_{k=1}^K \right\} \\ & = \arg \max \sum_{k=1}^K \log_2 [R_k - R_{e,k}]^+ \\ \text{s.t. } & \mathbf{F}_{\text{RF}}(:, l) \in \mathcal{F}, \forall l = 1, 2, \dots, L_t \\ & \mathbf{W}_k \in \mathcal{W}, k = 1, 2, \dots, K \\ & \|\mathbf{F}_{\text{RF}} \mathbf{F}_{\text{BB}}\|_F^2 = K \end{aligned} \right\} \quad (7)$$

受移相器无法连续调相限制, $\mathbf{F}_{\text{RF}}(:, l)$ 和 \mathbf{W}_k 属于特定码本 \mathcal{F} 和 \mathcal{W} , 设移相器量化精度为 B bit, 则每个移相器的相位调整步长为 $2\pi/2^B$. $\|\mathbf{F}_{\text{RF}} \mathbf{F}_{\text{BB}}\|_F^2 = K$ 是功率归一化条件. 该问题需要联合设计 \mathbf{F}_{RF} ,

第 k 个用户处的接收信号为

$$\mathbf{y}_k = \mathbf{W}_k^H \mathbf{H}_k \mathbf{F}_{\text{RF}} \sum_{n=1}^K \mathbf{f}_n^{\text{BB}} s_n + \mathbf{n}_k \quad (2)$$

其中, $\mathbf{H}_k \in \mathbb{C}^{N_r \times N_t}$ 是第 k 个用户的信道矩阵; $\mathbf{W}_k \in \mathbb{C}^{N_r \times 1}$ 是第 k 个用户的接收成形矩阵, 通过移相器实现且满足 $|\mathbf{W}_{ij}| = \frac{1}{\sqrt{N_r}}$; $\mathbf{n}_k \in \mathbb{C}^{N_r \times 1}$ 是第 k 个用户处的加性高斯白噪声, 以 σ^2 表示高斯白噪声的功率.

第 k 个用户处的频谱效率为

\mathbf{F}_{BB} 和 \mathbf{W}_k , 寻找全局最优解非常棘手. 同时由于窃听者相对用户具有能力上的优势, 导致系统安全速率较低. 针对这些问题, 本文考虑将混合波束成形模拟部分和数字部分分别独立设计^[12], 解决全局最优解难以寻找的问题, 同时采用人工噪声加扰策略提高系统安全速率.

2.2 毫米波信道模型

为了体现毫米波信道的稀疏散射特性, 通常采用S-V (Saleh-Valenzuela)模型^[13]. 假设第 k 个用户信道的散射簇数目为 L , 每个簇包含1条路径, 则 \mathbf{H}_k 可表示为

$$\mathbf{H}_k = \sqrt{\frac{N_t N_r}{L}} \sum_{l=1}^L \alpha_{k,l} \mathbf{a}_r(\theta_{k,l}) \mathbf{a}_t^H(\phi_{k,l}) \quad (8)$$

其中, $\alpha_{k,l}$ 代表第 k 个用户信道的第 l 条路径的复增益; $\mathbf{a}_r(\theta_{k,l})$ 和 $\mathbf{a}_t(\phi_{k,l})$ 分别表示用户处和基站端的天线阵列响应; $\theta_{k,l} \in [0, 2\pi]$ 和 $\phi_{k,l} \in [0, 2\pi]$ 分别表示第 l 条路径的到达角(AOA)和离开角(AOD). 假设基站端和用户端均采用均匀线性阵列(Uniform Linear Array, ULA), $\mathbf{a}_r(\theta_{k,l})$ 和 $\mathbf{a}_t(\phi_{k,l})$ 可进一步表示为

$$\mathbf{a}_r(\theta_{k,l}) = \frac{1}{\sqrt{N_r}} \cdot \left[1, e^{j(2\pi/\lambda)d \sin(\theta_{k,l})}, \dots, e^{j(N_r-1)(2\pi/\lambda)d \sin(\theta_{k,l})} \right]^T \quad (9)$$

$$\mathbf{a}_t(\phi_{k,l}) = \frac{1}{\sqrt{N_t}} \cdot \left[1, e^{j(2\pi/\lambda)d \sin(\phi_{k,l})}, \dots, e^{j(N_t-1)(2\pi/\lambda)d \sin(\phi_{k,l})} \right]^T \quad (10)$$

其中, d 表示天线之间的间距, λ 代表毫米波信号的波长。

同理, 窃听信道 $\mathbf{H}_{e,k}$ 可表示为

$$\mathbf{H}_{e,k} = \sqrt{\frac{N_t N_e}{L}} \sum_{l=1}^L \alpha_{e,l} \mathbf{a}_r(\theta_{e,l}) \mathbf{a}_t^H(\phi_{e,l}) \quad (11)$$

本文算法将充分考虑上述毫米波信道特性。

3 毫米波下行多用户系统安全混合波束成形算法

本文算法首先通过两阶段的设计过程将混合波束成形矩阵的数字部分和模拟部分解耦合, 在第1个阶段通过最大化用户接收信号能量准则设计基站端和用户处的模拟波束成形矩阵, 在第2个阶段利用迫零思想设计基站端有用信号的数字波束成形矩阵; 然后在第2个阶段过程中通过SVD分解设计人工噪声的数字波束成形矩阵, 将人工噪声置于合法用户零空间。

3.1 混合波束成形矩阵解耦合

考虑将混合波束成形矩阵的模拟部分和数字部分解耦合设计, 首先忽略用户间干扰, 联合设计基站端的模拟预编码矩阵和用户端的模拟接收成形矩阵, 使每一个目标用户的功率最大化; 然后根据第 k 个用户的等效基带信道矩阵, 采用迫零数字预编码技术消除用户间干扰。迫零(Zero-Forcing, ZF)预编码在大规模天线中性能较好, 且复杂度低^[14]。可总结为如下两阶段的过程。

阶段1 基站端与各个用户联合选择 \mathbf{W}_k 和 \mathbf{f}_k^{RF} , 其中 $\mathbf{W}_k \in \mathcal{W}$, $\mathbf{f}_k \in \mathcal{F}$ 。由于移相器恒模限制且相位无法连续可调, \mathcal{W} 和 \mathcal{F} 分别属于特定码本。用户功率最大化准则可表示为

$$\{\mathbf{f}_k^*, \mathbf{W}_k^*\} = \arg \max_{\mathbf{W}_k \in \mathcal{W}, \mathbf{f}_k \in \mathcal{F}} |\mathbf{W}_k^H \mathbf{H}_k \mathbf{f}_k^{\text{RF}}| \quad (12)$$

设置 $\mathbf{W}_k = \mathbf{W}_k^*$, $\mathbf{F}_{\text{RF}} = [\mathbf{f}_1^* \cdots \mathbf{f}_K^*, \mathbf{v}_{K+1} \cdots \mathbf{v}_{L_t}]$ 。为了简便起见, 设 $\mathbf{v}_i, i = K+1, K+2, \dots, L_t$ 为 \mathcal{F} 中任意码本。从基带 \mathbf{F}_{BB} 的角度看, 额外的 $L_t - K$ 个自由度由任意码本向量组成可降低算法复杂度。

阶段2 定义第 k 个用户的等效基带信道矩阵为

$$R_s = \left[\log_2 \left(1 + \frac{(1-\phi)P}{K} \frac{|\mathbf{W}_k^H \mathbf{H}_k \mathbf{F}_{\text{RF}} \mathbf{f}_k^{\text{BB}}|^2}{\sigma^2} \right) \right] - \log_2 \left(1 + \frac{(1-\phi)P}{K} \frac{\mathbb{E} \left[|\mathbf{W}_e^H \mathbf{H}_{e,k} \mathbf{F}_{\text{RF}} \mathbf{f}_k^{\text{BB}}|^2 \right]}{\frac{\phi P}{K} \mathbb{E} \left[|\mathbf{W}_e^H \mathbf{H}_{e,k} \mathbf{F}_{\text{RF}} \mathbf{F}_{\text{BB},z}|^2 \right] + \sigma^2} \right) \right]^+ \quad (16)$$

人工噪声分配因子 ϕ 可根据简单的1维搜索求得。

3.3 算法流程

算法整体流程如表1所示。

$$\tilde{\mathbf{H}}_k = \mathbf{W}_k^H \mathbf{H}_k \mathbf{F}_{\text{RF}} \quad (13)$$

计算等效基带信道矩阵 $\tilde{\mathbf{H}} = [\tilde{\mathbf{H}}_1^T, \tilde{\mathbf{H}}_2^T, \dots, \tilde{\mathbf{H}}_K^T]^T$, 采用ZF准则, 设置 $\mathbf{F}_{\text{BB}} = \tilde{\mathbf{H}}^H (\tilde{\mathbf{H}} \tilde{\mathbf{H}}^H)^{-1}$ 。对 \mathbf{F}_{BB} 进行归一化处理: $\mathbf{f}_k^{\text{BB}} = \mathbf{f}_k^{\text{BB}} / \|\mathbf{F}_{\text{RF}} \mathbf{f}_k^{\text{BB}}\|_{\text{F}}$, $k = 1, 2, \dots, K$ 。

3.2 人工噪声预编码设计

为进一步满足合法用户的安全需求, 在上述阶段2过程中引入人工噪声策略, 实现对窃听者的加扰。在人工噪声策略下, 基站端的发射信号为

$$\mathbf{x} = \mathbf{F}_{\text{RF}} \mathbf{F}_{\text{BB}} \mathbf{s} + \mathbf{F}_{\text{RF}} \mathbf{F}_{\text{BB},z} \mathbf{z} \quad (14)$$

其中, $\mathbf{s} = [s_1, s_2, \dots, s_K]^T$ 表示有用信号且满足 $\mathbb{E}[\mathbf{s} \mathbf{s}^H] = (1-\theta) \mathbf{P} \mathbf{I}_K / K$, $\mathbf{z} = [z_1, z_2, \dots, z_{L_t-K}]^T$ 表示人工噪声信号且满足 $\mathbb{E}[\mathbf{z} \mathbf{z}^H] = (\theta \mathbf{P} \mathbf{I}_K) / K$, θ 为人工噪声功率分配因子。 $\mathbf{F}_{\text{BB},z} = [\mathbf{f}_1^{\text{BB}}, \mathbf{f}_1^{\text{BB}}, \dots, \mathbf{f}_{L_t-K}^{\text{BB}}] \in \mathbf{C}^{L_t \times (L_t-K)}$ 表示人工噪声信号的基带预编码矩阵。

K 个合法用户接收到的信号可统一表示为

$$\mathbf{y} = \tilde{\mathbf{H}} \mathbf{F}_{\text{BB}} \mathbf{s} + \tilde{\mathbf{H}} \mathbf{F}_{\text{BB},z} \mathbf{z} + \mathbf{n} \quad (15)$$

其中, $\tilde{\mathbf{H}} = [\tilde{\mathbf{H}}_1^T, \tilde{\mathbf{H}}_2^T, \dots, \tilde{\mathbf{H}}_K^T]^T$, $\tilde{\mathbf{H}}_k = \mathbf{W}_k^H \mathbf{H}_k \mathbf{F}_{\text{RF}}$, $\mathbf{n} = [\mathbf{n}_1, \mathbf{n}_2, \dots, \mathbf{n}_K]$ 。人工噪声策略下有用信号的基站预编码矩阵和用户的接收成形矩阵设计算法不变, 即 \mathbf{F}_{RF} 和 \mathbf{F}_{BB} 的设计同3.1节。下面将说明, 为了将人工噪声置于所有合法用户的零空间, 只需设计 $\mathbf{F}_{\text{BB},z}$ 。

为了消除人工噪声对合法用户的干扰, 只需 $\mathbf{F}_{\text{BB},z}$ 落在 $\tilde{\mathbf{H}}$ 的零空间中^[15]。易知 $\tilde{\mathbf{H}} \in \mathbf{C}^{K \times L_t}$, 当 $L_t > K$ 时, 无论等效基带信道矩阵 $\tilde{\mathbf{H}}$ 如何设计, 均能找到非零 $\mathbf{F}_{\text{BB},z}$, 使得人工噪声落于 $\tilde{\mathbf{H}}$ 的零空间。将 $\tilde{\mathbf{H}}$ 进行SVD分解, $\tilde{\mathbf{H}} = \tilde{\mathbf{U}} \tilde{\Sigma} \tilde{\mathbf{V}}^H$, 设 $\mathbf{F}_{\text{BB},z} = \tilde{\mathbf{V}}(:, K+1, \dots, L_t)$, 由矩阵论SVD分解结论可知, $\mathbf{F}_{\text{BB},z}$ 由矩阵 $\tilde{\mathbf{H}}$ 的零奇异值对应的右奇异向量组成, 此时 $\mathbf{F}_{\text{BB},z}$ 位于所有合法用户信道矩阵 $\tilde{\mathbf{H}}$ 的零空间。将 $\mathbf{F}_{\text{BB},z}$ 归一化处理: $\mathbf{F}_{\text{BB},z} = \mathbf{F}_{\text{BB},z} / \|\mathbf{F}_{\text{RF}} \mathbf{F}_{\text{BB},z}\|_{\text{F}}$ 。此时安全频谱效率为

4 仿真分析

仿真系统模型设置: 毫米波频段为60 GHz, 如无特别说明, 发射端天线数 $N_t = 192$, 射频链路

表 1 毫米波下行多用户系统安全混合波束成形算法

算法步骤:
输入: $\mathbb{F}, \mathbb{W}, P, \phi$;
第1阶段:
对每个用户 $k, k = 1, 2, \dots, K$
基站和用户联合计算:
$\{\mathbf{f}_k^*, \mathbf{W}_k^*\} = \arg \max_{\mathbf{W}_k \in \mathbb{W}, \mathbf{f}_k \in \mathbb{F}} \mathbf{W}_k^H \mathbf{H}_k \mathbf{f}_k^{\text{RF}} $
用户 k 设置 $\mathbf{W}_k = \mathbf{W}_k^*$
基站设置 $\mathbf{F}_{\text{RF}} = [\mathbf{f}_1^* \dots \mathbf{f}_K^*, \mathbf{v}_{K+1} \dots \mathbf{v}_{L_t}]$
第2阶段:
对每个用户 $k, k = 1, 2, \dots, K$
用户计算等效基带信道矩阵 $\tilde{\mathbf{H}}_k = \mathbf{W}_k^H \mathbf{H}_k \mathbf{F}_{\text{RF}}$
用户向基站反馈信道状态信息 $\tilde{\mathbf{H}}_k$
基站计算 $\tilde{\mathbf{H}} = [\tilde{\mathbf{H}}_1^T, \tilde{\mathbf{H}}_2^T, \dots, \tilde{\mathbf{H}}_K^T]^T, \mathbf{F}_{\text{BB}} = \tilde{\mathbf{H}}^H (\tilde{\mathbf{H}} \tilde{\mathbf{H}}^H)^{-1}$; 基
站进行奇异值分解 $\tilde{\mathbf{H}} = \tilde{\mathbf{U}} \tilde{\mathbf{\Sigma}} \tilde{\mathbf{V}}^H$, 设置 $\mathbf{F}_{\text{BB}, s} = \tilde{\mathbf{V}}(:, K+1, \dots, L_t)$
输出: 基站端模拟预编码 \mathbf{F}_{RF} , 基站端数字预编码 \mathbf{F}_{BB} , 人工噪声数字预编码 $\mathbf{F}_{\text{BB}, s}$, 用户处模拟接收成形矩阵 \mathbf{W}_k .

$L_t = 8$; 用户数 $K = 6$, 每个用户配备天线数 $N_r = 16$, 射频链路数配备1条, 即在用户处采用模拟波束成形; 窃听者处配备天线数 $N_e = 128$. 移相器量化精度 $B = 4$ bit. 各节点天线间距 $d = \lambda/2$. 人工噪声功率分配因子 $\phi = 0.1$.

仿真信道模型设置: 每个用户信道散射簇数 $L = 3$, 发射角 $\theta_{k,l} \in [0, 2\pi]$ 和到达角 $\phi_{k,l} \in [0, 2\pi]$ 均服从均匀分布, 路径复增益 $\alpha_{k,l}$ 服从 $(0, 1)$ 复高斯分布.

图3给出了采用人工噪声策略时系统用户处频谱效率、窃听者处频谱效率以及安全频谱效率随SNR增大时的变化情况。如图3所示, 随着SNR的增大, 窃听者处的频谱效率一直维持在较低水平, 人工噪声的使用使得窃听信道受到限制, 特别是在低信噪比时人工噪声的作用更加明显。不难推出, 增大人工噪声功率分配因子, 窃听者会受到更加严

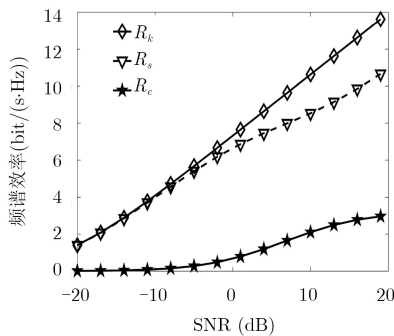


图 3 不同SNR时系统频谱效率

重的限制。说明即使窃听者具有多用户译码能力, 但在人工噪声的作用下, 窃听者仍然受到严重干扰, 从而验证了人工噪声策略的有效性。

图4给出了不同波束成形算法在不同信噪比下的安全频谱效率变化曲线。由图可知, 传统纯数字波束成形算法具有最优的系统性能, 但它所需的射频链路数与基站天线数目相同, 导致巨大的系统实现成本和能量消耗。模拟波束成形算法只能改变信号相位, 系统性能受到极大限制。不难看出, 混合波束成形与纯数字波束成形相比, 系统性能较为接近, 其损失的部分性能主要是由基站模拟预编码矩阵和用户端模拟接收成形矩阵的恒模特性引起的。综合考虑系统成本、功耗和性能等因素, 混合波束成形是毫米波系统的最佳选择。

图5给出了当SNR = 3 dB时, 系统安全频谱效率随基站天线数目增大时的变化情况(基站天线数目减少, 窃听者天线数目对应减少)。4条曲线分别代表在不同移相器量化精度下的系统安全频谱效率情况。由图可知, 在低分辨率时, 系统性能较差, 随着移相器量化精度的提升, 系统安全频谱效率的提升逐渐放缓且逼近分辨率无限的情况, 因此需要设置合适的移相器量化精度使得系统性能和计算复杂度取得折中。同时随着基站天线数量不断增大, 系统安全速率不断提高, 充分体现了增加天线数目

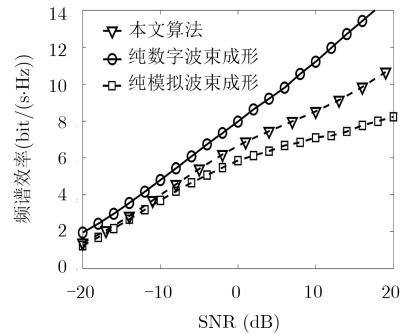


图 4 不同波束成形算法的比较

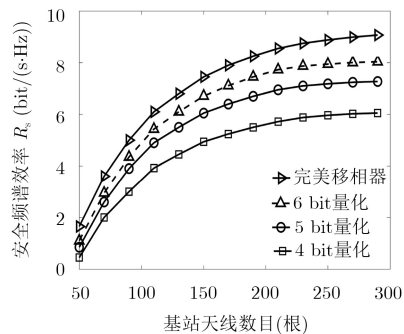


图 5 安全频谱效率随天线数目的变化以及与移相器量化精度的关系

给性能提升所带来的好处，但是系统安全速率随着天线数增多性能增加的幅度越来越小，为了节约系统安装成本需要取适中的发射端天线数。

图6给出了当SNR = 0 dB时，系统安全频谱效率随人工噪声功率分配因子的变化情况。当人工噪声功率分配因子为0时，此时由于窃听者具有多用户译码能力，可以窃听得到用户的全部信息，安全频谱效率几乎为0。随着人工噪声功率分配因子的增大，窃听者窃听能力受到抑制，安全频谱效率逐渐增大到最高值；继续增大功率分配因子，有用信号的发射功率不足，而人工噪声对窃听者的干扰作用逐渐弱化，因此，安全速率开始下降。因此，若单纯以安全频谱效率为指标，则存在一个最优的功率分配因子值，使得安全指标最优。同时需要指出，不同信噪比下的功率分配因子不同，因此功率分配因子需要自适应设置。

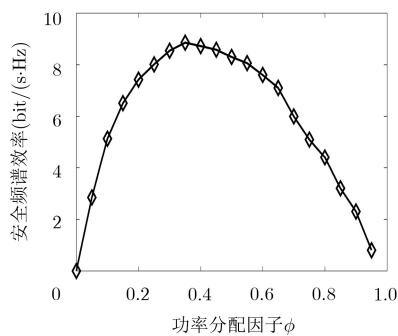


图6 安全频谱效率随人工噪声功率分配因子的变化

5 结束语

本文针对基于混合波束成形的毫米波下行多用户系统，为了对抗具有多用户译码能力的窃听者，提出一种毫米波下行多用户系统安全混合波束成形算法。为解决混合波束成形全局最优解难以求解的问题，将各部分波束成形矩阵解耦合进行设计。首先通过最大化用户接收信号能量和迫零思想分别设计有用信号的模拟波束成形矩阵和数字波束成形矩阵；然后，引入人工噪声策略，通过SVD分解设计人工噪声的基带数字预编码矩阵，将人工噪声置于合法用户零空间，达到恶化窃听信道，保障正常通信的目的。仿真结果验证了人工噪声策略的有效性，同时表明提高模拟移相器量化精度，增大基站天线数目，合理设置人工噪声功率分配因子均可提升系统安全性能。

参考文献

[1] RAPPAPORT T S, SUN Shu, MAYZUS R, *et al.*

Millimeter wave mobile communications for 5G cellular: It will work![J]. *IEEE Access*, 2013, 1: 335–349. doi: [10.1109/ACCESS.2013.2260813](https://doi.org/10.1109/ACCESS.2013.2260813).

- [2] RANGAN S, RAPPAPORT T S, and ERKIP E. Millimeter-wave cellular wireless networks: Potentials and challenges[J]. *Proceedings of the IEEE*, 2014, 102(3): 366–385. doi: [10.1109/JPROC.2014.2299397](https://doi.org/10.1109/JPROC.2014.2299397).
- [3] WANG Chao and WANG Huiming. Physical layer security in millimeter wave cellular networks[J]. *IEEE Transactions on Wireless Communications*, 2016, 15(8): 5569–5585. doi: [10.1109/TWC.2016.2562010](https://doi.org/10.1109/TWC.2016.2562010).
- [4] WU Yongpeng, KHISTI A, XIAO Chengshan, *et al.* A survey of physical layer security techniques for 5G wireless networks and challenges ahead[J]. *IEEE Journal on Selected Areas in Communications*, 2018, 36(4): 679–695. doi: [10.1109/JSAC.2018.2825560](https://doi.org/10.1109/JSAC.2018.2825560).
- [5] ANDREWS J G, BAI Tianyang, KULKARNIul M N, *et al.* Modeling and analyzing millimeter wave cellular systems[J]. *IEEE Transactions on Communications*, 2017, 65(1): 403–430. doi: [10.1109/TCOMM.2016.2618794](https://doi.org/10.1109/TCOMM.2016.2618794).
- [6] AYACH O E, HEATH R W, ABU-SURRA S, *et al.* Low complexity precoding for large millimeter wave MIMO systems[C]. *IEEE International Conference on Communications*, Ottawa, Canada, 2012: 3724–3729. doi: [10.1109/ICC.2012.6363634](https://doi.org/10.1109/ICC.2012.6363634).
- [7] AYACH O E, RAJAGOPAL S, ABU-SURRA S, *et al.* Spatially sparse precoding in millimeter wave MIMO systems[J]. *IEEE Transactions on Wireless Communications*, 2014, 13(3): 1499–1513. doi: [10.1109/TWC.2014.011714.130846](https://doi.org/10.1109/TWC.2014.011714.130846).
- [8] ALKHATEEB A, AYACH O E, LEUS G, *et al.* Channel estimation and hybrid precoding for millimeter wave cellular systems[J]. *IEEE Journal of Selected Topics in Signal Processing*, 2014, 8(5): 831–846. doi: [10.1109/JSTSP.2014.2334278](https://doi.org/10.1109/JSTSP.2014.2334278).
- [9] RAMADAN Y R, MINN H, and IBRAHIM A S. Hybrid analog–digital precoding design for secrecy mmWave MISO-OFDM systems[J]. *IEEE Transactions on Communications*, 2017, 65(11): 5009–5026. doi: [10.1109/TCOMM.2017.2734666](https://doi.org/10.1109/TCOMM.2017.2734666).
- [10] WANG Zihuan, LI Ming, TIAN Xiaowen, *et al.* Iterative hybrid precoder and combiner design for mmWave multiuser MIMO systems[J]. *IEEE Communications Letters*, 2017, 21(7): 1581–1584. doi: [10.1109/LCOMM.2017.2682087](https://doi.org/10.1109/LCOMM.2017.2682087).
- [11] CHEN Yajun, JI Xinsheng, HUANG Kaizhi, *et al.* Artificial noise-assisted physical layer security in D2D-enabled

- cellular networks[J]. *EURASIP Journal on Wireless Communications and Networking*, 2017, 2017: 178. doi: [10.1186/s13638-017-0969-1](https://doi.org/10.1186/s13638-017-0969-1).
- [12] ALKHATEEB A, LEUS G, and HEATH R W. Limited feedback hybrid precoding for multi-user millimeter wave systems[J]. *IEEE Transactions on Wireless Communications*, 2015, 14(11): 6481–6494. doi: [10.1109/TWC.2015.2455980](https://doi.org/10.1109/TWC.2015.2455980).
- [13] GONZALEZ-COMA J P, RODRIGUEZ-FERNANDEZ J, GONZALEZ-PRELCIC N, *et al.* Channel estimation and hybrid precoding for frequency selective multiuser mmWave MIMO systems[J]. *IEEE Journal of Selected Topics in Signal Processing*, 2018, 12(2): 353–367. doi: [10.1109/JSTSP.2018.2819130](https://doi.org/10.1109/JSTSP.2018.2819130).
- [14] 黄天宇, 马林华, 胡星, 等. 一种实用的毫米波大规模MIMO混合预编码算法[J]. *电子与信息学报*, 2017, 39(8): 1788–1795. doi: [10.11999/JEIT161211](https://doi.org/10.11999/JEIT161211).
- HUANG Tianyu, MA Linhua, HU Xing, *et al.* Practical hybrid precoding algorithm for millimeter wave massive MIMO[J]. *Journal of Electronics & Information Technology*, 2017, 39(8): 1788–1795. doi: [10.11999/JEIT161211](https://doi.org/10.11999/JEIT161211).
- [15] ZHU Jun, XU Wei, and WANG Ning. Secure massive MIMO systems with limited RF chains[J]. *IEEE Transactions on Vehicular Technology*, 2017, 66(6): 5455–5460. doi: [10.1109/TVT.2016.2615885](https://doi.org/10.1109/TVT.2016.2615885).
- 黄开枝: 女, 1973年生, 教授、博士生导师, 研究方向为移动通信网络及信息安全.
- 王少禹: 男, 1993年生, 硕士生, 研究方向为移动通信安全.
- 许晓明: 男, 1988年生, 助理研究员, 研究方向为移动通信安全.