中国科学: 信息科学 2022 年 第 52 卷 第 2 期: 217–238
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
6G 网络安全专题 · 论文

混合窃听环境下多波束符号级安全传输方法

邱彬, 程文驰*

西安电子科技大学综合业务网理论与关键技术国家重点实验室, 西安 710071
* 通信作者. E-mail: wccheng@xidian.edu.cn

收稿日期: 2021–08–15; 修回日期: 2021–10–10; 接受日期: 2021–12–17; 网络出版日期: 2022–02–07

国家重点研发计划 (批准号: 2021YFC3002100) 资助项目

摘要 针对毫米波在混合窃听无线通信系统面临的安全问题, 基于阵列收发结构, 提出了一种有效的无线物理层安全传输方法. 在发射端采用多波束符号级方向调制、人工噪声 (artificial noise, AN) 辅助、天线子集方法, 以及合法用户 (legitimate user, LU) 采用阵列接收确保混合窃听环境下的安全可靠传输. 考虑窃听者 (eavesdropper, Eve) 信息未知, 通过最小化发射信息功率准则设计发射波束形成矢量, 满足合法用户的接收信号指定符号级约束, 确保合法用户有效接收. 将剩余的发射功率分配给人工噪声, 最大限度扰乱窃听者的接收信号. 此外, 通过最小均方差无失真响应准则设计合法用户接收权矢量, 有效抑制干扰信号. 仿真结果证明了所提方法在能量效率和安全增强方面的优越性.

关键词 物理层安全, 人工噪声, 混合窃听, 多波束, 方向调制

1 引言

随着第五代移动通信 (5G) 逐步大规模商用, 第六代移动通信 (6G) 开始成为新一轮科技竞争的焦点. 6G 考虑引入全球覆盖、高频谱效率、高能源效率、高智能性和安全性等新的性能指标, 以满足快速增长的通信需求. 其中, 毫米波 (millimeter-wave, mmWave)、大规模多输入多输出 (multi-input multi-output, MIMO) 技术与轨道角动量技术将成为未来后 5G 移动通信 (beyond 5G, B5G)/6G 移动通信的关键技术之一 [1~4]. 通常采用波束成形技术提供阵列增益从而提高毫米波传输距离, 促使大规模阵列的发展 [5]. 安全性是无线通信系统的重要要求, 毫米波通信也不例外. 另外, 毫米波传输较大的带宽和严重的路径损耗, 使之更容易遭受噪声以及恶意干扰. 因此, 保证传输具备低检测 (low-probability of detection, LPD)/低截获概率 (low-probability of intercept, LPI) 特性, 实现信息安全可靠的传输是毫米波通信的重要目标 [6].

物理层安全 (physical layer security, PLS) 技术作为传统加密安全机制的一种有效互补技术, 在过去十年中引起了学术界极大兴趣 [7]. 无线物理层安全传输的关键思想是利用无线信道固有的随机

引用格式: 邱彬, 程文驰. 混合窃听环境下多波束符号级安全传输方法. 中国科学: 信息科学, 2022, 52: 217–238, doi: 10.1360/SSI-2021-0282
Qiu B, Cheng W C. Multi-beam symbol-level secure transmission against hybrid eavesdropping (in Chinese). Sci Sin Inform, 2022, 52: 217–238, doi: 10.1360/SSI-2021-0282

特征实现信息加密传输 [8,9]. 相控阵方向调制 (directional modulation, DM) 利用空间自由度和天线增益是增强物理层安全的有效方法之一 [10,11]. 方向调制技术能够使信号具有方向指向性, 实现空间中指定方位信号增强, 同时抑制其他非期望方向的信号. 文献 [12] 将方向调制与人工噪声 (artificial noise, AN) 结合, 进一步增强无线传输的安全性能. 人工噪声辅助波束成形方法能有效地降低窃听者 (eavesdropper, Eve) 接收信号的质量, 把信息隐藏在人工噪声中, 目标用户不受人工噪声影响, 而非期望用户受到人工噪声的扰乱, 达到防止窃听的目的. 文献 [13] 依据相控阵调节信号相位的传输模式, 针对单目标多径传输模型, 利用多边形构造方法设计波束成形矢量实现无线安全传输. 在实际应用中, 方位角测量误差不可避免. 于是, 针对系统存在测量误差的问题, 文献 [14] 提出了稳健波束成形优化方法, 以减小测量误差对期望用户的影响. 根据保密容量的定义, 文献 [15] 直接采用最大保密容量准则设计波束形成矢量增强物理层安全. 然而, 计算保密容量需要发射端获得窃听者精确的位置信息, 而被动窃听者为了避免暴露通常保持无线电缄默, 在实际应用中获取其信息是不可行的. 针对 MIMO 传输系统, 文献 [16,17] 提出了一种符号级预编码安全增强技术. 文献 [18,19] 将阵列方向调制技术应用在毫米波安全传输通信系统中, 通过随机天线选择开关相控阵方法, 在天线级进行处理实现方向指向性数据传输, 而在非期望方向实现星座混乱. 文献 [20] 提出了一种天线子集调制 (antenna subset modulation, ASM) 方法, 应用于毫米波传输系统, 具备低复杂度和高安全性. 天线子集技术以符号速率控制发射天线阵元的选通状态. 发射天线子阵随机切换, 目标导向矢量与发射权具有共轭对称性, 所以不同发射天线子集依然可以保证目标用户的可靠的通信, 而对非期望方向的接收信号进行扰乱. 文献 [21] 提出了一种新颖的发射结构, 混合相位控制 MIMO 传输, 将发射多天线分成多个子阵重叠, 每个子阵列传输相干正交的波形, 从而具有更高的角分辨率能力.

随着物理层安全技术的发展, 发射端采用保密增强技术确保高效稳定地将信息传输给指定用户, 同时避免窃听. 随之窃听者也采用先进的技术窃听保密信息以及破坏发射机与合法用户 (legitimate user, LU) 之间的通信 [22]. 考虑复杂窃听环境, 存在主动发射干扰信号用来阻塞和攻击合法用户接收的主动窃听者, 保持无线电缄默通过协作截获保密信息的多被动窃听者以及暴力截获保密信息的独立被动窃听者, 而且主动窃听者与被动窃听者能够随时切换 [23]. 由此, 采用上述单一安全传输方法已无法确保在复杂窃听环境下安全可靠传输.

针对上述问题, 本文首次考虑混合窃听环境下的阵列收发结构的无线物理层安全传输, 并且假设窃听者位置信息未知, 这更符合实际应用需求. 本文联合多种技术实现无线安全可靠传输. 首先, 发射端提出了符号级方向调制方法, 旨在满足合法用户接收符号级约束, 最小化发射信息功率, 为合法提供指定质量的传输. 其次, 将剩余的发射功率用于产生人工噪声, 结合随机选择天线子集扰乱窃听者的接收信号. 最后, 在接收端通过最小方差无失真响应 (minimum variance distortionless response, MVDR) 方法设计合法用户接收权矢量, 消除来自主动窃听者的干扰信号. 综上所述, 本文主要贡献如下所述.

(1) 基于相控阵发射结构, 提出了多波束符号级方向调制安全传输方法, 旨在满足所有合法用户符号级固定/松弛相位约束下, 最小发射信息功率设计波束形成矢量, 从而减少信息泄露, 并将剩余的发射功率分配给人工噪声. 符号级方向调制利用传输符号产生有益的干扰而不是完全消除用户间符号干扰.

(2) 发射端采用随机发射天线子集选取, 激活发射阵元数和阵元都随机选取, 从而产生随机导向矢量, 并结合依赖于发射符号的符号级方向调制以及人工噪声辅助波束成形, 扰乱各种类型的窃听者的接收信号, 进一步降低信息被窃听的可能性.

(3) 为抑制主动窃听者对合法用户的干扰, 合法接收端采用阵列接收结构, 基于 MVDR 准则设计接收权矢量消除干扰信号, 同时确保来自发射方向的信号无失真, 所提方法具有在干扰环境下实现可

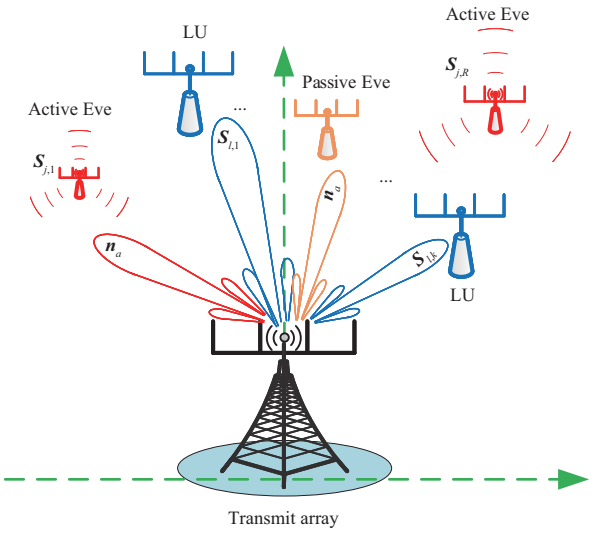

图 1　混合窃听环境方向调制系统示意图

Figure 1　Generic architecture of the directional modulation with hybrid eavesdroppers

靠传输的能力.

本文剩余部分内容安排如下: 第 2 节介绍了基于人工噪声辅助的阵列收发模型. 随后, 第 3 节提出了安全传输策略并进行求解. 第 4 节分析了所提方法的安全性能. 第 5 节中通过仿真验证了所提方法的有效性. 最后, 第 6 节总结全文.

本文符号说明如下: 粗体大写、粗体小写和小写字母分别表示矩阵、向量和标量. diag(·) 表示构造对角矩阵. ∘ 是逐元素的 Hadamard 乘积. 上标 $(\cdot)^{-1}$、$(\cdot)^{\mathrm{T}}$ 和 $(\cdot)^{\mathrm{H}}$ 分别表示逆、转置和 Hermitian 变换. Pr(·) 表示概率函数. E[·] 表示期望. tr(·) 表示矩阵的迹. Re{·}, Im{·} 和 arg{·} 分别表示取复数的实部、虚部和幅角. $\mathbb{R}$ 和 $\mathbb{C}$ 分别表示实数域和复数域的集合. $\|\cdot\|_2$ 和 $|\cdot|$ 分别表示 ℓ_2-范数和模. 矩阵 $\boldsymbol{I}_N$ 和 $\mathbf{0}_{N\times M}$ 分别表示 $N\times N$ 单位矩阵和 $N\times M$ 全零矩阵.

2　系统模型

考虑混合窃听环境下多目标毫米波通信系统, 如图 1 所示, 系统中有一个发射阵列, 由 N_t 个间距为 d_t 的阵元组成, 发射机将不同的信息流同时发送给相应的 K 个合法用户, 每个合法用户由 N_l 个间距为 d_l 的阵元组成, 阵列采用均匀各向同性线性阵列 (uniform linear array, ULA), 发射端发射总功率为 E_t. 主动窃听者和被动窃听者共存, 截获保密信息并发出干扰信号试图阻塞合法用户的有效接收.

不失一般性, 发射机和合法用户接收阵列的第 1 个阵元设为参考阵元. 考虑目标远场传输模型, 对于毫米波通信, 可以忽略视距 (line of sight, LoS) 传输中非常弱的多径分量, 由于与视距分量相比, 多径分量衰减超过 20 dB [24]. 那么, 依据自由空间路径损耗模型, 沿空间方向 θ 的单波束图表示为 [25]

$$\begin{aligned} B(\theta) &= \sum_{n=1}^{N_t} \rho w_n \mathrm{e}^{-\mathrm{j}2\pi f_c[t-\frac{r-(n-1)d_t\sin\theta}{c}]} \sum_{m=1}^{N_l} u_m \mathrm{e}^{-\mathrm{j}2\pi\frac{f_c(m-1)d_l\sin\theta}{c}} \\ &= \rho \mathrm{e}^{-\mathrm{j}2\pi f_c(t-\frac{r}{c})} \sum_{n=1}^{N_t} w_n \mathrm{e}^{-\mathrm{j}2\pi\frac{f_c(n-1)d_t\sin\theta}{c}} \sum_{m=1}^{N_l} u_m \mathrm{e}^{-\mathrm{j}2\pi\frac{f_c(m-1)d_l\sin\theta}{c}}, \end{aligned} \tag{1}$$

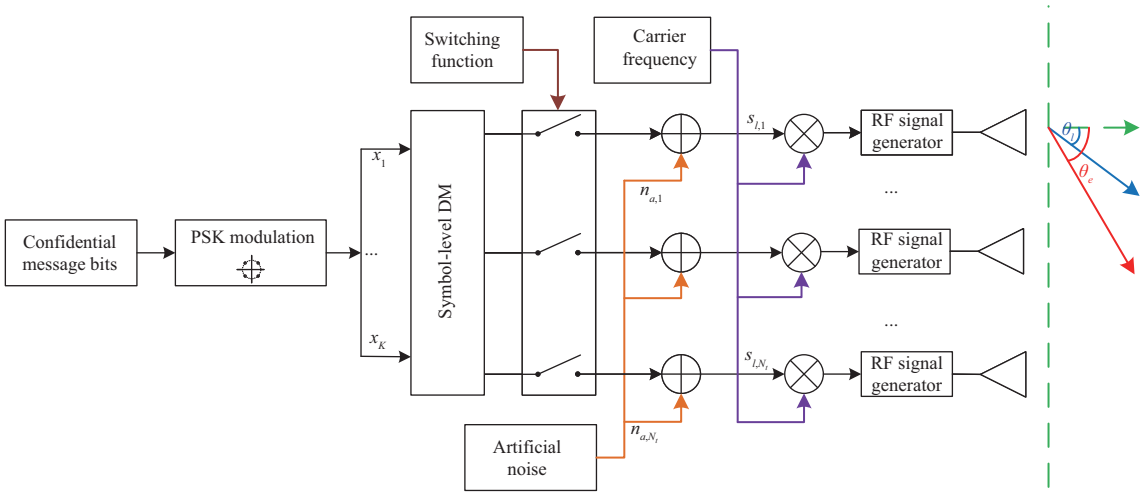

图 2 (网络版彩图) 多波束符号级方向调制的发射结构

Figure 2 (Color online) Generic architecture of the transmitter for multi-beam symbol-level DM

其中 c 表示光速, f_c 表示载频频率, w_n 表示发射波束成形因子, u_m 表示接收权因子, ρ 表示与传输距离相关的路径损耗因子. 为方便表述, 分别定义发送和接收阵列的导向向量为

$$\boldsymbol{h}(\theta) \triangleq \rho\left[1, \mathrm{e}^{-\mathrm{j}2\pi\frac{f_c d_t \sin\theta}{\mathrm{c}}}, \ldots, \mathrm{e}^{-\mathrm{j}2\pi\frac{f_c (N_t-1) d_t \sin\theta}{\mathrm{c}}}\right]^{\mathrm{H}}, \tag{2}$$

和

$$\boldsymbol{a}(\theta) \triangleq \left[1, \mathrm{e}^{-\mathrm{j}2\pi\frac{f_c d_l \sin\theta}{\mathrm{c}}}, \ldots, \mathrm{e}^{-\mathrm{j}2\pi\frac{f_c (N_l-) d_l \sin\theta}{\mathrm{c}}}\right]^{\mathrm{H}}. \tag{3}$$

采用人工噪声辅助多波束符号级方向调制子集发射方法, 如图 2 所示, 瞬时基带发送信号由下式给出:

$$\boldsymbol{s}_l = \boldsymbol{\tau} \circ \left(\sum_{k=1}^{K} \boldsymbol{w}_k x_k + \boldsymbol{n}_a\right), \tag{4}$$

其中 $\circ$ 表示 Hadamard 乘积, $\boldsymbol{\tau} = [\tau_1, \ldots, \tau_n, \ldots, \tau_{N_t}]^{\mathrm{T}} \in \mathbb{R}^{N_t \times 1}$ 表示开关向量, $\tau_n \in \{0, 1\}$, $\forall n \in \mathcal{N}_t$, $\mathcal{N}_t \triangleq \{1, 2, \ldots, N_t\}$, 表示时域控制第 n 个天线射频的开关, 发射天线子集通过随机选择阵元从而引入随机性. $\boldsymbol{w}_k \in \mathbb{C}^{N_t \times 1}$ 是控制调制符号 x_k 发射给合法用户 k 的波束形成矢量, x_k 为发送给用户 k 的 M-PSK 调制符号, 满足 $\mathrm{E}[|x_k|^2] = 1$, $\forall k \in \mathcal{K}$, $\mathcal{K} \triangleq \{1, 2, \ldots, K\}$, $\boldsymbol{n}_a$ 为人工噪声.

发射端通过使用波达方向 (direction of arrival, DoA) 估计算法 [26] 或 GPS 等方法获取合法用户的方位信息. 假设 $\theta_{l,k}$ 表示合法用户 k, $\forall k \in \mathcal{K}$, 相对于发射机的方位角. 合法用户采用相控阵接收处理, 消除主动窃听者发出的干扰信号, 如图 3 所示. 另外, 假设主动窃听者发射的窄带噪声干扰信号具有与载波相同的频率, 否则合法用户可以通过频域滤波消除干扰信号. 噪声干扰通过不间断的大功率噪声信号形成压制式干扰环境. 假设合法用户能够实现理想的频率和相位同步, 那么, 合法用户 k, $\forall k \in \mathcal{K}$, 接收到的下变频信号可表示为

$$y(\theta_{l,k}) = \boldsymbol{h}^{\mathrm{H}}(\theta_{l,k}) \boldsymbol{s}_l \boldsymbol{a}^{\mathrm{H}}(\theta_{l,k}) \boldsymbol{u}_k + \sum_{r=1}^{R} \rho_{k,r} \sqrt{E_{j,r}} s_{j,r} \boldsymbol{a}^{\mathrm{H}}(\theta_{j,k,r}) \boldsymbol{u}_k + n_{l,k}, \tag{5}$$

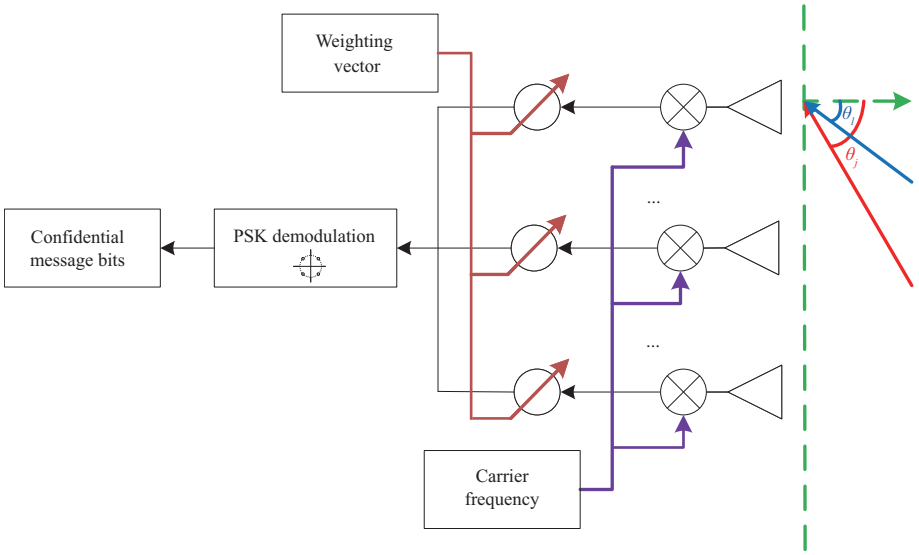

图 3 (网络版彩图) 合法用户阵列接收结构

Figure 3 (Color online) Generic architecture of the LU

其中 $s_{j,r}$ 是来自主动窃听者 r 的干扰信号, 满足 $\mathrm{E}[|s_{j,r}(t)|^2]=1$; $E_{j,r}$ 是主动窃听者 r 的发射干扰功率; $\rho_{k,r}$ 是主动窃听者 r 与合法用户 k 之间的路径损耗因子; $\theta_{j,k,r}$ 是主动窃听者 r 与合法用户 k 相对方位角; R 是系统中主动窃听者的总数; $\boldsymbol{u}_k\in\mathbb{C}^{N_l\times 1}$ 是合法用户 k 的接收权矢量; $n_{l,k}$ 是具有零均值 $\sigma_{l,k}^2$ 方差的复加性高斯白噪声 (additive white gaussian noise, AWGN), 满足 $n_{l,k}\sim\mathcal{CN}(0,\sigma_{l,k}^2)$.

在下文中, 考虑系统中存在多个窃听者, 即 $N_e\geqslant 1$. 那么, 窃听者的导向矩阵表示为

$$\boldsymbol{H}(\boldsymbol{\Theta}_e)\triangleq[\boldsymbol{h}(\theta_{e,1}),\boldsymbol{h}(\theta_{e,2}),\ldots,\boldsymbol{h}(\theta_{e,N_e})]. \tag{6}$$

根据多输入多输出多窃听者 (multi-input multi-output multi-eavesdropper, MIMOME) 窃听信道可知 [27], 天线阵列的导向矢量是相关的, 即满足 $\mathrm{rank}\{\boldsymbol{H}(\boldsymbol{\Theta}_e)\boldsymbol{H}^{\mathrm{H}}(\boldsymbol{\Theta}_e)\}=1$. 为了更有利于窃听信息, 窃听者应利用非相关信道. 于是, 多窃听者采用分布式结构, 并且假设窃听者能够通过合作消除由主动窃听者发出的干扰信号. 那么, 窃听者的接收信号可以表示为

$$\boldsymbol{y}(\boldsymbol{\Theta}_e)=\boldsymbol{H}^{\mathrm{H}}(\boldsymbol{\Theta}_e)\boldsymbol{s}_l+\boldsymbol{n}_e, \tag{7}$$

其中 $\boldsymbol{n}_e$ 为复 AWGN, 满足 $\boldsymbol{n}_e\sim\mathcal{CN}(0,\sigma_e^2\boldsymbol{I}_{N_e})$.

3 安全传输策略

为了实现无线信息安全传输, 不仅需要建立发射机与合法用户之间的可靠通信, 同时也要避免信息泄露. 为此, 通过优化发射阵列波束形成矢量、发射阵列子集选取、人工噪声投影矩阵设计, 以及计算合法用户接收权矢量, 实现混合窃听环境下无线安全传输.

3.1 阵列子集设计

发射机激活阵元数为 $N_a=\sum_{n=1}^{N_t}\tau_n$. 也就是说, 开关函数 $\boldsymbol{\tau}$ 中的元素为 0 值表示关闭阵元, 1 值表示激活阵元, 即满足 N_a 个 1 和 N_t-N_a 个 0. 随机子集传输创建了一个动态随机的导向矢量, 使窃

听者难以估计导向矢量的信息, 可以有效防止分布式协作窃听. 另一个好处是在非期望方向随机扰乱接收信号. 取 $N_a > K$, 激活阵元数和激活阵元按符号速率进行随机变换. 定义 $\mathcal{Z}$ 为所有可能的发射阵列子集组合的集合, 很容易得到所有发射阵列子集组合数为

$$|\mathcal{Z}| = \sum_{N_a=K+1}^{N_t} \binom{N_t}{N_a}, \tag{8}$$

其中 $\binom{\cdot}{\cdot}$ 表示取二项式系数. 此外, 激活发射天线及其数量的变换至少以符号速率更新. 也就是说, 控制天线模块按符号速率刷新发射阵列天线合成发射阵列子集. 由于该技术依赖于符号速率切换天线. 因此, 高速开关是发射机设计的关键部分. 为了实现快速的天线切换, 需要一系列能够以纳秒或亚纳秒的速度切换, 插入损耗低且隔离性能良好的高频单刀单掷开关.

3.2 固定相位波束形成矢量优化

人工噪声辅助阵列发射能够有效地降低窃听者接收信号的质量, 但是人工噪声需要消耗部分总发射功率. 因此, 发射信息功率与人工噪声功率的合理分配对于安全性能至关重要. 假设发射机的总发射功率是固定的, 那么更少的发射信息功率意味着: (1) 更少的信息泄漏可能性; (2) 更多的功率分配给人工噪声, 增加人工噪声对窃听者的干扰. 为此, 采用最小发射信息功率准则设计波束形成矢量, 满足合法用户接收信息符号级约束, 即接收信号的信噪比 (signal to noise ratio, SNR) 大于指定值, 以及接收信号指定相位. 首先, 构造优化问题为

$$\mathrm{P1}: \min_{\{\boldsymbol{w}_k\}_{k=1}^K} \left\| \boldsymbol{\tau} \circ \sum_{k=1}^K \boldsymbol{w}_k x_k \right\|_2^2 \tag{9a}$$

$$\text{s.t.} \ \left\| \boldsymbol{h}^{\mathrm{H}}(\theta_{l,k}) \left(\boldsymbol{\tau} \circ \sum_{k=1}^K \boldsymbol{w}_k x_k \right) \right\|_2^2 \geqslant \eta_k \sigma_{l,k}^2, \ \forall k \in \mathcal{K}, \tag{9b}$$

$$\arg \left\{ \boldsymbol{h}^{\mathrm{H}}(\theta_{l,k}) \left(\boldsymbol{\tau} \circ \sum_{k=1}^K \boldsymbol{w}_k x_k \right) \right\} = \varphi_k, \ \forall k \in \mathcal{K}, \tag{9c}$$

其中 $\eta_k \in \mathbb{R}$ 表示合法用户 k 接收信号的指定 SNR, $\varphi_k = \arg\{x_k\}$ 表示合法用户 k 接收信号的相位, $k \in \mathcal{K}$. 约束 (9b) 为了保护合法用户 k 接收信号的 SNR, 使得合法用户 k 的接收信号的 SNR 高于指定接收 SNR 阈值. 约束 (9c) 表示合法用户 k 接收信号的相位等于发射调制信号 x_k 的相位.

接下来, 求解优化问题 P1 的最优解. 定义整体波束形成矢量为

$$\boldsymbol{v} \triangleq \sum_{k=1}^K \boldsymbol{w}_k x_k. \tag{10}$$

那么, $\|\boldsymbol{\tau} \circ \boldsymbol{v}\|_2^2 = \|\boldsymbol{\tau} \circ \sum_{k=1}^K \boldsymbol{w}_k x_k\|_2^2$ 为发射信息总功率. 为了求解问题 P1, 采用同相正交约束代替 SNR 和相位约束. 由于合法用户 k 接收信号的相位与发射符号 x_k 的相位相同, 为了接收信号满足指定 SNR, 同相和正交分量与接收信号的 SNR 按相同的比增加. 那么, 接收信号的 SNR 约束 (9a) 等价表示为[1)]

$$\mathrm{Re}^2\{\boldsymbol{h}^{\mathrm{H}}(\theta_{l,k})(\boldsymbol{\tau} \circ \boldsymbol{v})\} \geqslant \eta_k \mathrm{Re}^2\{x_k\} \sigma_{l,k}^2, \ \forall k \in \mathcal{K}. \tag{11}$$

1) 需要注意的是, 当发射符号落在虚轴上时, x_k 的实部为 0, 将约束改为 $\mathrm{Im}\{\cdot\}$, 即 $\alpha_k = \frac{\pi}{2}$.

为了简化相位约束, 式 (9c) 等价表示为

$$\alpha_k \mathrm{Re}\{\boldsymbol{h}^{\mathrm{H}}(\theta_{l,k})(\boldsymbol{\tau}\circ\boldsymbol{v})\} - \mathrm{Im}\{\boldsymbol{h}^{\mathrm{H}}(\theta_{l,k})(\boldsymbol{\tau}\circ\boldsymbol{v})\} = 0, \tag{12}$$

其中 $\alpha_k = \tan(\varphi_k)$. 为了避免正切函数引起的相位模糊, 添加约束

$$\mathrm{Re}\{x_k\}\mathrm{Re}\{\boldsymbol{h}^{\mathrm{H}}(\theta_{l,k})(\boldsymbol{\tau}\circ\boldsymbol{v})\} \geqslant 0. \tag{13}$$

利用式 (11)∼(13), 问题 P1 等价于

$$\mathrm{P2}: \min_{\boldsymbol{v}} \|\boldsymbol{\tau}\circ\boldsymbol{v}\|_2^2 \tag{14a}$$

$$\text{s.t. } \mathrm{Re}\{x_k\}\mathrm{Re}\{\boldsymbol{h}^{\mathrm{H}}(\theta_{l,k})(\boldsymbol{\tau}\circ\boldsymbol{v})\} \geqslant \zeta_k \mathrm{Re}^2\{x_k\},\ \forall k\in\mathcal{K}, \tag{14b}$$

$$\alpha_k \mathrm{Re}\{\boldsymbol{h}^{\mathrm{H}}(\theta_{l,k})(\boldsymbol{\tau}\circ\boldsymbol{v})\} - \mathrm{Im}\{\boldsymbol{h}^{\mathrm{H}}(\theta_{l,k})(\boldsymbol{\tau}\circ\boldsymbol{v})\} = 0,\ \forall k\in\mathcal{K}, \tag{14c}$$

其中 $\zeta_k = \sqrt{\eta_k}\sigma_{l,k}$. 由于 $|x_k|^2 = 1$, $\zeta_k\mathrm{Re}^2\{x_k\} + \zeta_k\mathrm{Im}^2\{x_k\} = \zeta_k$, 那么接收信号指定 SNR 约束仍然成立. 另外, 不同于单独设计每个合法用户的波束形成矢量, 确保用户间符号无干扰 [28], 从优化问题 P2 可以看出, 单个波束形成矢量 $\boldsymbol{w}_k$ 不再出现在优化问题中, 通过计算整体波束形成矢量 $\boldsymbol{v}$ 实现多波束安全传输. 符号级方向调制利用传输符号产生有益的干扰增强接收信号功率而不是完全消除干扰.

将开关向量吸收到导向矢量中, 即 $\bar{\boldsymbol{h}}(\theta_{l,k}) = \boldsymbol{h}(\theta_{l,k})\circ\boldsymbol{\tau}$. 所有合法用户导向矢量构成合法用户导向矩阵, 即

$$\bar{\boldsymbol{H}}(\boldsymbol{\Theta}_l) \triangleq [\bar{\boldsymbol{h}}(\theta_{l,1}), \bar{\boldsymbol{h}}(\theta_{l,2}), \ldots, \bar{\boldsymbol{h}}(\theta_{l,K})]. \tag{15}$$

那么, 将优化问题 P2 转化为

$$\mathrm{P3}: \min_{\boldsymbol{v}} \|\boldsymbol{\tau}\circ\boldsymbol{v}\|_2^2 \tag{16a}$$

$$\text{s.t. } \boldsymbol{X}\mathrm{Re}\{\bar{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\boldsymbol{v}\} \geqslant \boldsymbol{\zeta}\circ\boldsymbol{x}_s, \tag{16b}$$

$$\boldsymbol{\Lambda}\mathrm{Re}\{\bar{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\boldsymbol{v}\} - \mathrm{Im}\{\bar{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\boldsymbol{v}\} = \boldsymbol{0}, \tag{16c}$$

其中 $\boldsymbol{\Lambda} = \mathrm{diag}(\boldsymbol{\alpha})$, $\boldsymbol{X} = \mathrm{diag}(\mathrm{Re}\{\boldsymbol{x}\})$, $\boldsymbol{x}_s = \mathrm{Re}\{\boldsymbol{x}\}\circ\mathrm{Re}\{\boldsymbol{x}\}$, $\boldsymbol{x} = [x_1, x_2, \ldots, x_K]^{\mathrm{T}}$ 是所有合法用户的符号向量, $\boldsymbol{\zeta} = [\zeta_1, \zeta_2, \ldots, \zeta_K]^{\mathrm{T}}$, 和 $\boldsymbol{\alpha} = [\alpha_1, \alpha_2, \ldots, \alpha_K]^{\mathrm{T}}$. 为了求解优化问题 P3, 首先利用 $\bar{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l) = \mathrm{Re}\{\bar{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\} + \mathrm{j}\mathrm{Im}\{\bar{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\}$ 和 $\boldsymbol{v} = \mathrm{Re}\{\boldsymbol{v}\} + \mathrm{j}\mathrm{Im}\{\boldsymbol{v}\}$ 将实部和虚部分开. 根据等式

$$\begin{aligned}\bar{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\boldsymbol{v} =& \mathrm{Re}\{\bar{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\}\mathrm{Re}\{\boldsymbol{v}\} - \mathrm{Im}\{\bar{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\}\mathrm{Im}\{\boldsymbol{v}\}\\ &+ \mathrm{j}\left[\mathrm{Im}\{\bar{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\}\mathrm{Re}\{\boldsymbol{v}\} + \mathrm{Re}\{\bar{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\}\mathrm{Im}\{\boldsymbol{v}\}\right],\end{aligned} \tag{17}$$

复数算法可以转换为

$$\mathrm{Re}\{\bar{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\boldsymbol{v}\} = \bar{\boldsymbol{H}}_1^{\mathrm{T}}\tilde{\boldsymbol{v}}, \tag{18}$$

$$\mathrm{Im}\{\bar{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\boldsymbol{v}\} = \bar{\boldsymbol{H}}_2^{\mathrm{T}}\tilde{\boldsymbol{v}}, \tag{19}$$

其中 $\tilde{\boldsymbol{v}} = [\mathrm{Re}\{\boldsymbol{v}^{\mathrm{T}}\}, \mathrm{Im}\{\boldsymbol{v}^{\mathrm{T}}\}]^{\mathrm{T}}$, $\bar{\boldsymbol{H}}_1^{\mathrm{T}} = [\mathrm{Re}\{\bar{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\}, -\mathrm{Im}\{\bar{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\}]$, $\bar{\boldsymbol{H}}_2^{\mathrm{T}} = [\mathrm{Im}\{\bar{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\}, \mathrm{Re}\{\bar{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\}]$. 注意 $\|\boldsymbol{v}\|_2^2 = \|\tilde{\boldsymbol{v}}\|_2^2$. 定义 $\boldsymbol{T} \triangleq \mathrm{diag}([\boldsymbol{\tau}^{\mathrm{T}}, \boldsymbol{\tau}^{\mathrm{T}}]^{\mathrm{T}})$. 基于上述变换, 问题 P3 可重构为

$$\mathrm{P4}: \min_{\tilde{\boldsymbol{v}}} \|\boldsymbol{T}\tilde{\boldsymbol{v}}\|_2^2 \tag{20a}$$

$$\text{s.t. } \boldsymbol{X}\bar{\boldsymbol{H}}_1^{\mathrm{T}}\tilde{\boldsymbol{v}} \succcurlyeq \boldsymbol{\zeta}\circ\boldsymbol{x}_s, \tag{20b}$$

$$(\boldsymbol{\Lambda}\bar{\boldsymbol{H}}_1^{\mathrm{T}} - \bar{\boldsymbol{H}}_2^{\mathrm{T}})\tilde{\boldsymbol{v}} = \boldsymbol{0}. \tag{20c}$$

为了消除等式约束 (20c), 将矩阵 $\boldsymbol{\Lambda}\bar{\boldsymbol{H}}_1^{\mathrm{T}} - \bar{\boldsymbol{H}}_2^{\mathrm{T}}$ 采用奇异值分解 (singular-value decomposition, SVD), 表示为

$$\boldsymbol{\Lambda}\bar{\boldsymbol{H}}_1^{\mathrm{T}} - \bar{\boldsymbol{H}}_2^{\mathrm{T}} = \left[\boldsymbol{U}^{(1)}\ \boldsymbol{U}^{(0)}\right]\begin{bmatrix}\boldsymbol{\Sigma} & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{0}\end{bmatrix}\left[\boldsymbol{V}^{(1)}\ \boldsymbol{V}^{(0)}\right]^{\mathrm{H}}, \tag{21}$$

其中 $\boldsymbol{\Sigma}$ 为对角矩阵. 为了确保优化问题 P4 存在最优解, 矩阵 $\boldsymbol{\Lambda}\bar{\boldsymbol{H}}_1^{\mathrm{T}} - \bar{\boldsymbol{H}}_2^{\mathrm{T}}$ 的零空间应该存在, 这意味着激活天线数必须满足 $2N_a - K > 0$. 根据 SVD 性质 [29], $\boldsymbol{V}^{(0)}$ 是后 $2N_a - K$ 零奇异值对应的右奇异向量. 定义 $\boldsymbol{B} \triangleq \boldsymbol{V}^{(0)}$. 用 $\boldsymbol{B}\boldsymbol{\xi}$ 替换 $\tilde{\boldsymbol{v}}$, 即 $\tilde{\boldsymbol{v}} \triangleq \boldsymbol{B}\boldsymbol{\xi}$, $\boldsymbol{\xi} \in \mathbb{R}^{(2N_a-K)\times 1}$, 得到以下优化问题:

$$\text{P5}: \min_{\boldsymbol{\xi}} \|\boldsymbol{T}\boldsymbol{B}\boldsymbol{\xi}\|_2^2 \tag{22a}$$

$$\text{s.t. } \boldsymbol{X}\bar{\boldsymbol{H}}_1^{\mathrm{T}}\boldsymbol{B}\boldsymbol{\xi} \succcurlyeq \boldsymbol{\zeta}\circ\boldsymbol{x}_s. \tag{22b}$$

接下来, 采用迭代算法来获得优化问题 P5 的最优解, 并证明得到的最优解具有稳定收敛性. 首先, 引入实值辅助向量 $\boldsymbol{\delta} \in \mathbb{R}^{K\times 1}$ 将式 (22b) 不等式约束转变为等式约束, 即 $\boldsymbol{X}\bar{\boldsymbol{H}}_1^{\mathrm{T}}\boldsymbol{B}\boldsymbol{\xi} = \boldsymbol{\zeta}\circ\boldsymbol{x}_s + \boldsymbol{\delta}$, $\boldsymbol{\delta} \succcurlyeq \boldsymbol{0}$. 然后, 应用罚函数方法 [30] 构建以下新优化问题:

$$\text{P6}: \min_{\{\boldsymbol{\xi},\boldsymbol{\delta}\}} \|\boldsymbol{T}\boldsymbol{B}\boldsymbol{\xi}\|_2^2 + \lambda\|\boldsymbol{X}\bar{\boldsymbol{H}}_1^{\mathrm{T}}\boldsymbol{B}\boldsymbol{\xi} - \boldsymbol{\zeta}\circ\boldsymbol{x}_s - \boldsymbol{\delta}\|_2^2. \tag{23}$$

当 $\lambda \to \infty$ 时, 优化问题 P6 等价于优化问题 P5. 首先, 通过固定 $\boldsymbol{\xi}$, 调整变量 $\boldsymbol{\delta}$ 来求解优化问题 P6, 那么优化问题转化为

$$\text{P7}: \min_{\boldsymbol{\delta}\succcurlyeq\boldsymbol{0}} \|\boldsymbol{X}\bar{\boldsymbol{H}}_1^{\mathrm{T}}\boldsymbol{B}\boldsymbol{\xi} - \boldsymbol{\zeta}\circ\boldsymbol{x}_s - \boldsymbol{\delta}\|_2^2. \tag{24}$$

为了解优化问题 P7, 最小化 $\boldsymbol{X}\bar{\boldsymbol{H}}_1^{\mathrm{T}}\boldsymbol{B}\boldsymbol{\xi} - \boldsymbol{\zeta}\circ\boldsymbol{x}_s$ 和 $\boldsymbol{\delta}$ 之间的距离. 由于固定 $\boldsymbol{\xi}$, 那么 $\boldsymbol{X}\bar{\boldsymbol{H}}_1^{\mathrm{T}}\boldsymbol{B}\boldsymbol{\xi} - \boldsymbol{\zeta}\circ\boldsymbol{x}_s$ 为确定值. 如果 $\boldsymbol{X}\bar{\boldsymbol{H}}_1^{\mathrm{T}}\boldsymbol{B}\boldsymbol{\xi} - \boldsymbol{\zeta}\circ\boldsymbol{x}_s$ 的元素为非负数, 则 $\boldsymbol{\delta}$ 取与 $\boldsymbol{X}\bar{\boldsymbol{H}}_1^{\mathrm{T}}\boldsymbol{B}\boldsymbol{\xi} - \boldsymbol{\zeta}\circ\boldsymbol{x}_s$ 相同的值. 如果 $\boldsymbol{X}\bar{\boldsymbol{H}}_1^{\mathrm{T}}\boldsymbol{B}\boldsymbol{\xi} - \boldsymbol{\zeta}\circ\boldsymbol{x}_s$ 元素为负, 由于 $\boldsymbol{\delta} \succcurlyeq \boldsymbol{0}$, 所以 $\boldsymbol{\delta}$ 的对应元素取零. 那么, 等效最优解为

$$\boldsymbol{\delta}^{\star} = \max\left\{\boldsymbol{X}\bar{\boldsymbol{H}}_1^{\mathrm{T}}\boldsymbol{B}\boldsymbol{\xi} - \boldsymbol{\zeta}\circ\boldsymbol{x}_s, \boldsymbol{0}\right\}. \tag{25}$$

接下来, 调整 $\boldsymbol{\xi}$, 把 $\boldsymbol{\delta}$ 视为固定值, 得到优化问题

$$\text{P8}: \min_{\boldsymbol{\xi}} \|\boldsymbol{T}\boldsymbol{B}\boldsymbol{\xi}\|_2^2 + \lambda\|\boldsymbol{X}\bar{\boldsymbol{H}}_1^{\mathrm{T}}\boldsymbol{B}\boldsymbol{\xi} - \boldsymbol{\zeta}\circ\boldsymbol{x}_s - \boldsymbol{\delta}\|_2^2. \tag{26}$$

优化问题 P8 的目标函数可构造为

$$f(\boldsymbol{\xi}) = \|\boldsymbol{T}\boldsymbol{B}\boldsymbol{\xi}\|_2^2 + \lambda\|\boldsymbol{X}\bar{\boldsymbol{H}}_1^{\mathrm{T}}\boldsymbol{B}\boldsymbol{\xi} - \boldsymbol{\zeta}\circ\boldsymbol{x}_s - \boldsymbol{\delta}\|_2^2. \tag{27}$$

当 $f(\boldsymbol{\xi})$ 关于 $\boldsymbol{\xi}$ 的梯度等于 0 时, 得到目标函数的最优解, 即

$$\boldsymbol{\xi}^{\star} = \left[\frac{(\boldsymbol{T}\boldsymbol{B})^{\mathrm{T}}\boldsymbol{T}\boldsymbol{B}}{\lambda} + (\boldsymbol{X}\bar{\boldsymbol{H}}_1^{\mathrm{T}}\boldsymbol{B})^{\mathrm{T}}\boldsymbol{X}\bar{\boldsymbol{H}}_1^{\mathrm{T}}\boldsymbol{B}\right]^{-1}(\boldsymbol{X}\bar{\boldsymbol{H}}_1^{\mathrm{T}}\boldsymbol{B})^{\mathrm{T}}(\boldsymbol{\zeta}\circ\boldsymbol{x}_s + \boldsymbol{\delta}). \tag{28}$$

求解优化问题 P5 迭代算法的详细过程见算法 1 所示.

Algorithm 1 Iterative algorithm for the problem P5

Input: Pick up an initial point $\boldsymbol{\xi}^0 \in \mathbb{R}^{(2N-K)\times 1}$, $\lambda \in [0, +\infty)$, and set $r = 1$.

1: Determine $\boldsymbol{\delta}^{r-1}$ by substituting $\boldsymbol{\xi}^{r-1}$ into (25);
2: Determine $\boldsymbol{\xi}^r$ by substituting $\boldsymbol{\delta}^{r-1}$ into (28);
3: **if** $f(\boldsymbol{\xi}^{r-1}) - f(\boldsymbol{\xi}^r) > \varepsilon$ **then**
4: $r = r + 1$;
5: Go to 1;
6: **else**
7: Return $\boldsymbol{\xi}$;
8: **end if**

Output: Get the finally optimal solution $\boldsymbol{\xi}^\star$.

下面证明迭代算法可以求得稳定收敛的最优解. 假定初始值选取 $\boldsymbol{\xi}^0$ 和 $\boldsymbol{\delta}^0$. 根据式 (25) 和 (28) 得到最优解 $\boldsymbol{\xi}^\star$ 和 $\boldsymbol{\delta}^\star$, 满足

$$f(\boldsymbol{\xi}^\star, \boldsymbol{\delta}^\star) \leqslant f(\boldsymbol{\xi}^0, \boldsymbol{\delta}^\star) \leqslant f(\boldsymbol{\xi}^0, \boldsymbol{\delta}^0). \tag{29}$$

显而易见, 由于目标函数 $f(\boldsymbol{\xi}, \boldsymbol{\delta})$ 的零下限, 算法 1 中的每次迭代都单调地接近最优值. 因此, 证明了迭代算法可以获得稳定收敛的最优解.

值得一提的是, 由于波束形成矢量取决于导向矢量、发射天线子阵和传输符号. 因此, 为了确保合法用户有效检测能力, 天线子集以符号速率更新, 同样需要以符号速率更新波束形成矢量.

3.3 松弛相位波束形成矢量优化

在 3.2 小节中, 波束形成矢量的设计旨在实现接收到的目标符号具有固定相位. 事实上, 不必设计波束形成矢量使得接收信号具有固定相位, 只要噪声不会将接收信号推到正确检测区域之外, 接收到的符号依然能够正确恢复码元信息, 这就使得接收信号的相位属于松弛区域. 鉴于此, 通过放松约束来设计波束形成矢量, 该约束允许接收的符号相位落入预定相位范围内的任何点, 在该范围内合法用户可以正确地恢复码元信息. 假设发送 M-PSK 调制符号, 将符号 x_0 的相位规定为参考相位 φ_0, 定义的松弛区域 $[\varphi_0 - \frac{\pi}{M}, \varphi_0 + \frac{\pi}{M}]$. 相位落在此松弛区域内依旧可以正确的解调. 于是, 松弛相位设计波束形成矢量优化问题可构造为

$$\mathrm{P9}: \min_{\{\boldsymbol{w}_k\}_{k=1}^K} \left\| \boldsymbol{\tau} \circ \sum_{k=1}^K \boldsymbol{w}_k x_k \right\|_2^2 \tag{30a}$$

$$\text{s.t.} \left\| \boldsymbol{h}^{\mathrm{H}}(\theta_{l,k}) \left(\boldsymbol{\tau} \circ \sum_{k=1}^K \boldsymbol{w}_k x_k \right) \right\|_2^2 \geqslant \zeta_k^2, \ \forall k \in \mathcal{K}, \tag{30b}$$

$$\arg \left\{ \boldsymbol{h}^{\mathrm{H}}(\theta_{l,k}) \left(\boldsymbol{\tau} \circ \sum_{k=1}^K \boldsymbol{w}_k x_k \right) \right\} \geqslant \varphi_0 - \frac{\pi}{M}, \ \forall k \in \mathcal{K}, \tag{30c}$$

$$\arg \left\{ \boldsymbol{h}^{\mathrm{H}}(\theta_{l,k}) \left(\boldsymbol{\tau} \circ \sum_{k=1}^K \boldsymbol{w}_k x_k \right) \right\} \leqslant \varphi_0 + \frac{\pi}{M}, \ \forall k \in \mathcal{K}, \tag{30d}$$

其中约束 (30b) 为了保护合法用户 k 的接收信号, 使合法用户 k 接收信号的 SNR 满足指定要求; 式 (30c) 和 (30d) 中的约束使得接收信号的相位落在松弛相区域内. 松弛区域可以由图 4 中的阴影部分

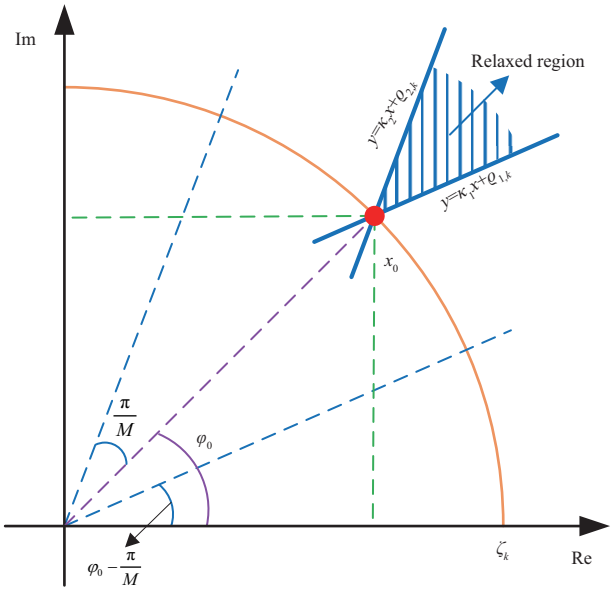

图 4　松弛相位的 M-PSK 调制符号分布

Figure 4　Structure of symbol level precoding with relaxed phase in the M-PSK modulation

表示, 该扇形区域由通过星座点为交叉点的两条边界平行线, 与中心方向相反的 $2\pi/M$ 度范围形成, 即满足线性约束 $[y=\kappa_1 x+\varrho_1, y=\kappa_2 x+\varrho_2]$. 为了将其应用于通用星座图点, 考虑 φ_0 和 φ_k 之间的相位差. 同理, 定义整体波束形成矢量 $\boldsymbol{v}\triangleq\sum_{k=1}^{K}\boldsymbol{w}_k x_k$. 利用基本几何操作, 优化问题 P9 等价于以下优化问题[2)]:

$$\mathrm{P10}:\ \min_{\boldsymbol{v}}\ \|\boldsymbol{\tau}\circ\boldsymbol{v}\|_2^2 \tag{31a}$$

$$\text{s.t. } \mathrm{Im}\{\boldsymbol{h}^{\mathrm{H}}(\theta_{l,k})(\boldsymbol{\tau}\circ\boldsymbol{v})\mathrm{e}^{\mathrm{j}\beta_k}\}\geqslant\kappa_1\mathrm{Re}\{\boldsymbol{h}^{\mathrm{H}}(\theta_{l,k})(\boldsymbol{\tau}\circ\boldsymbol{v})\mathrm{e}^{\mathrm{j}\beta_k}\}+\varrho_{1,k},\ \forall k\in\mathcal{K}, \tag{31b}$$

$$\mathrm{Im}\{\boldsymbol{h}^{\mathrm{H}}(\theta_{l,k})(\boldsymbol{\tau}\circ\boldsymbol{v})\mathrm{e}^{\mathrm{j}\beta_k}\}\leqslant\kappa_2\mathrm{Re}\{\boldsymbol{h}^{\mathrm{H}}(\theta_{l,k})(\boldsymbol{\tau}\circ\boldsymbol{v})\mathrm{e}^{\mathrm{j}\beta_k}\}+\varrho_{2,k},\ \forall k\in\mathcal{K}, \tag{31c}$$

其中 $\kappa_1=\tan(\varphi_0-\frac{\pi}{M})$, $\kappa_2=\tan(\varphi_0+\frac{\pi}{M})$, $\varrho_{1,k}=\zeta_k\sin(\varphi_0)-\zeta_k\cos(\varphi_0)\tan(\varphi_0-\frac{\pi}{M})$, $\varrho_{2,k}=-[\zeta_k\cos(\varphi_0)-\zeta_k\sin(\varphi_0)\cot(\varphi_0+\frac{\pi}{M})]\tan(\varphi_0+\frac{\pi}{M})$, $\beta_k\triangleq\varphi_0-\varphi_k$. 为了简化表述, 将开关向量和相位偏移吸收到导向矢量中, 定义 $\tilde{\boldsymbol{h}}(\theta_{l,k})=\boldsymbol{h}(\theta_{l,k})\circ\boldsymbol{\tau}\mathrm{e}^{\mathrm{j}\beta_k}$. 考虑所有合法用户的约束, 则优化问题 P10 转化为

$$\mathrm{P11}:\ \min_{\boldsymbol{v}}\ \|\boldsymbol{\tau}\circ\boldsymbol{v}\|_2^2 \tag{32a}$$

$$\text{s.t. } \mathrm{Im}\{\tilde{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\boldsymbol{v}\}\geqslant\kappa_1\mathrm{Re}\{\tilde{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\boldsymbol{v}\}+\boldsymbol{\varrho}_1, \tag{32b}$$

$$\mathrm{Im}\{\tilde{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\boldsymbol{v}\}\leqslant\kappa_2\mathrm{Re}\{\tilde{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\boldsymbol{v}\}+\boldsymbol{\varrho}_2, \tag{32c}$$

其中 $\boldsymbol{\varrho}_1=[\varrho_{1,1},\varrho_{1,2},\ldots,\varrho_{1,K}]^{\mathrm{T}}$, $\boldsymbol{\varrho}_2=[\varrho_{2,1},\varrho_{2,2},\ldots,\varrho_{2,K}]^{\mathrm{T}}$ 和 $\tilde{\boldsymbol{H}}(\boldsymbol{\Theta}_l)=[\tilde{\boldsymbol{h}}(\theta_{l,1}),\tilde{\boldsymbol{h}}(\theta_{l,2}),\ldots,\tilde{\boldsymbol{h}}(\theta_{l,K})]$. 将复数实部虚部分离, 通过

$$\tilde{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\boldsymbol{v}=\mathrm{Re}\{\tilde{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\}\mathrm{Re}\{\boldsymbol{v}\}-\mathrm{Im}\{\tilde{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\}\mathrm{Im}\{\boldsymbol{u}\}$$

2) 注意, 对于发射 QPSK (quadrature phase shift keying) 调制符号, 由于 κ_2 不存在, 式 (31c) 中约束用 $\mathrm{Im}\{\boldsymbol{h}^{\mathrm{H}}(\theta_{l,k})(\boldsymbol{\tau}\circ\boldsymbol{v})\mathrm{e}^{\mathrm{j}\beta_k}\}\geqslant\zeta_k$ 代替.

$$+\mathrm{j}[\mathrm{Im}\{\tilde{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\}\mathrm{Re}\{\boldsymbol{v}\}+\mathrm{Re}\{\tilde{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\}\mathrm{Im}\{\boldsymbol{v}\}]. \tag{33}$$

可得

$$\mathrm{Re}\{\tilde{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\boldsymbol{v}\}=\tilde{\boldsymbol{H}}_1^{\mathrm{T}}\tilde{\boldsymbol{v}}, \tag{34}$$

$$\mathrm{Im}\{\tilde{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\boldsymbol{v}\}=\tilde{\boldsymbol{H}}_2^{\mathrm{T}}\tilde{\boldsymbol{v}}, \tag{35}$$

其中 $\tilde{\boldsymbol{v}}=[\mathrm{Re}\{\boldsymbol{v}^{\mathrm{T}}\},\mathrm{Im}\{\boldsymbol{v}^{\mathrm{T}}\}]^{\mathrm{T}}$, $\tilde{\boldsymbol{H}}_1^{\mathrm{T}}=[\mathrm{Re}\{\tilde{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\},-\mathrm{Im}\{\tilde{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\}]$, $\tilde{\boldsymbol{H}}_2^{\mathrm{T}}=[\mathrm{Im}\{\tilde{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\},\mathrm{Re}\{\tilde{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\}]$. 将式 (34) 和 (35) 代入优化问题 P11, 可得

$$\mathrm{P12}:\ \min_{\tilde{\boldsymbol{v}}}\ \|\boldsymbol{T}\tilde{\boldsymbol{v}}\|_2^2 \tag{36a}$$

$$\text{s.t. } \boldsymbol{F}\tilde{\boldsymbol{v}}\geqslant\boldsymbol{\varrho}, \tag{36b}$$

其中

$$\boldsymbol{F}=\begin{bmatrix}\tilde{\boldsymbol{H}}_2^{\mathrm{T}}-\kappa_1\tilde{\boldsymbol{H}}_1^{\mathrm{T}}\\ \kappa_2\tilde{\boldsymbol{H}}_1^{\mathrm{T}}-\tilde{\boldsymbol{H}}_2^{\mathrm{T}}\end{bmatrix},\quad \boldsymbol{\varrho}=\begin{bmatrix}\boldsymbol{\varrho}_1\\ -\boldsymbol{\varrho}_2\end{bmatrix}. \tag{37}$$

不难看出上述优化问题 P12 与优化问题 P5 具有相同的结构. 因此, 通过类似的迭代算法 1 能够有效地求解该优化问题.

3.4 人工噪声投影矩阵设计

对于足够接收敏感度的窃听者有可能从旁瓣信息泄露功率中截获保密信息. 人工噪声被窃听者视为虚拟信息, 从而有效地隐藏信息. 人工噪声元素等于 $\boldsymbol{n}_a=\boldsymbol{P}_a\boldsymbol{z}$, 其中人工噪声投影矩阵 $\boldsymbol{P}_a\in\mathbb{C}^{N_a\times(N_a-K)}$ 用于控制干扰方向, 人工噪声向量 $\boldsymbol{z}\in\mathbb{C}^{(N_a-K)\times 1}$ 为随机变量, 由零均值和单位方差的复高斯变量组成, 满足 $\boldsymbol{z}\sim\mathcal{CN}(0,\boldsymbol{I}_{N_t-K})$. 根据 3.2 和 3.3 小节计算出最小发射信息功率, 将剩余的总发射功率分配给人工噪声. 人工噪声投影矩阵设计使得合法用户的接收信号不受人工噪声的影响, 恶化非期望方向的接收信号的质量, 从而提高保密性能. 接下来, 计算人工噪声投影矩阵 $\boldsymbol{P}_a$, 使其位于 $\bar{\boldsymbol{H}}_l^{\mathrm{H}}$ 的零空间消除人工噪声对合法用户的干扰, 同时满足剩余发射功率约束, 即

$$\begin{cases}\bar{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)\boldsymbol{P}_a=\boldsymbol{0},\\ \mathrm{tr}(\boldsymbol{P}_a\boldsymbol{P}_a^{\mathrm{H}})=E_t-\|\boldsymbol{\tau}\circ\boldsymbol{u}^{\star}\|_2^2.\end{cases} \tag{38}$$

通过对合法用户导向矩阵进行 SVD, 即 $\bar{\boldsymbol{H}}^{\mathrm{H}}(\boldsymbol{\Theta}_l)=\boldsymbol{U}_l\boldsymbol{\Sigma}_l\boldsymbol{V}_l^{\mathrm{H}}$. 定义 $\boldsymbol{\Phi}\in\mathbb{C}^{N_a\times(N_a-K)}$ 由 $\boldsymbol{V}_l$ 中最后 N_a-K 右奇异向量组成. 那么, 可将人工噪声投影矩阵设计为

$$\boldsymbol{P}_a=\sqrt{\frac{E_t-\|\boldsymbol{\tau}\circ\boldsymbol{u}^{\star}\|_2^2}{N_a-K}}\boldsymbol{\Phi}. \tag{39}$$

可以看出, 所提方法最小发射信息功率准则能够减少信息泄漏并精确控制信息与人工噪声之间发射功率分配. 在无线物理层安全通信中, 人工噪声辅助波束成形方法使得合法用户不受人工噪声的干扰, 而严重恶化窃听者接收信号的质量. 另外, 由于电磁波自由空间路径损耗, 窃听者离发射机越近, 截获到信号功率越强, 而窃听者受到人工噪声干扰的功率也越大. 实现任意旁瓣位置的非合法用户具有均匀且低的信干噪比 (signal-to-interference-plus-noise ratio, SINR). 因此, 人工噪声辅助波束成形为提高安全性能的有效手段 [31].

3.5 接收权矢量优化

为了使合法用户接收信号抑制主动窃听者的干扰, 合法用户接收阵列采用 MVDR 准则 [32], 优化得到接收阵列的权矢量. MVDR 准则无需事先知道干扰来向, 其目的是保持对期望方向无失真响应的同时将干扰噪声功率降至最低. 那么, 合法用户 k, $\forall k \in \mathcal{K}$, 抗干扰处理优化问题可以表示为

$$\mathrm{P13}: \min_{\boldsymbol{u}_k} \ \boldsymbol{u}_k^{\mathrm{H}} \boldsymbol{R}_y \boldsymbol{u}_k \tag{40a}$$

$$\text{s.t. } \boldsymbol{a}^{\mathrm{H}}(\theta_{l,k}) \boldsymbol{u}_k = 1, \tag{40b}$$

其中 $\boldsymbol{R}_y$ 表示接收信号的协方差矩阵. 根据文献 [32], 很容易获得优化问题 P13 的最优解, 即

$$\boldsymbol{u}_k^{\star} = \boldsymbol{R}_y^{-1} \boldsymbol{a}(\theta_{l,k}) \left[\boldsymbol{a}^{\mathrm{H}}(\theta_{l,k}) \boldsymbol{R}_y^{-1} \boldsymbol{a}(\theta_{l,k}) \right]^{-1}. \tag{41}$$

实际应用中, 接收信号的协方差矩阵 $\boldsymbol{R}_y$ 很难得到. 通常使用每个天线的样本协方差矩阵来代替 [21], 即 $\tilde{\boldsymbol{R}}_y = \frac{1}{L} \sum_{i=1}^{L} \boldsymbol{y}_i \boldsymbol{y}_i^{\mathrm{H}}$, 其中 $\{\boldsymbol{y}_i\}_1^L$ 是接收信号的快拍, L 是快拍的长度. 此方法可以有效去除噪声干扰, 特别是对于强干扰.

4 安全性能分析

为了进一步分析和度量系统的安全性能, 结合已有的无线物理层安全通信系统和适用于阵列天线安全传输的评价指标, 分别分析推导了保密速率和误符号率 (symbol error rate, SER) 分布, 并与现有方法进行比较.

4.1 与迫零方法比较

由于所提方法和传统迫零 (zero-forcing, ZF) 方法 [12, 33] 都采用阵列天线波束成形, 都适用于多用户且窃听者信息未知的情况下, 将所提方法与 ZF 方法进行比较, 为了公平比较, 设置为相同的合法用户指定接收 SNR. 于是, 采用 ZF 方法合法用户和窃听者的接收信号表示为

$$\boldsymbol{y}(\boldsymbol{\Theta}_l) = \boldsymbol{H}^{\mathrm{H}}(\boldsymbol{\Theta}_l) \sum_{k=1}^{K} \zeta_k \boldsymbol{w}_k x_k + \boldsymbol{n}_l, \tag{42}$$

$$\boldsymbol{y}(\boldsymbol{\Theta}_e) = \boldsymbol{H}^{\mathrm{H}}(\boldsymbol{\Theta}_e) \sum_{k=1}^{K} \zeta_k \boldsymbol{w}_k x_k + \boldsymbol{n}_e, \tag{43}$$

其中 $\zeta_k = \sqrt{\eta_k} \sigma_{l,k}$, $\eta_k \in \mathbb{R}$ 为合法用户 k 接收信号的指定 SNR. 定义 $\boldsymbol{W} \triangleq [\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_K]$. 使用 ZF 方法, 波束形成矩阵设计为

$$\boldsymbol{W}_{\mathrm{ZF}}^{\star} = \boldsymbol{H}(\boldsymbol{\Theta}_l) [\boldsymbol{H}^{\mathrm{H}}(\boldsymbol{\Theta}_l) \boldsymbol{H}(\boldsymbol{\Theta}_l)]^{-1}. \tag{44}$$

将式 (44) 代入式 (43), 合法用户接收信号表示为

$$\boldsymbol{y}(\boldsymbol{\Theta}_l) = \boldsymbol{\zeta} \circ \boldsymbol{x} + \boldsymbol{n}_l, \tag{45}$$

其中 $\boldsymbol{\zeta}=[\zeta_1,\zeta_2,\ldots,\zeta_K]^{\mathrm{T}}$. 窃听者通过分布式窃听技术消除方向性失真 [34], 这对窃取保密信息更有利. 假设存在足够的窃听者协作, 即 $N_e\geqslant N_t$, 使得 $\boldsymbol{H}(\boldsymbol{\Theta}_e)\boldsymbol{H}^{\mathrm{H}}(\boldsymbol{\Theta}_e)$ 可逆. 窃听者估计符号为

$$\begin{aligned}\hat{\boldsymbol{y}}(\boldsymbol{\Theta}_e)&=\boldsymbol{\Xi}\mathbf{y}(\boldsymbol{\Theta}_{\mathbf{e}})\\&=\boldsymbol{\zeta}\circ\boldsymbol{x}+\boldsymbol{H}^{\mathrm{H}}(\boldsymbol{\Theta}_l)[\boldsymbol{H}(\boldsymbol{\Theta}_e)\boldsymbol{H}^{\mathrm{H}}(\boldsymbol{\Theta}_e)]^{-1}\boldsymbol{H}(\boldsymbol{\Theta}_e)\boldsymbol{n}_e,\end{aligned}\tag{46}$$

其中 $\boldsymbol{\Xi}=\boldsymbol{H}^{\mathrm{H}}(\boldsymbol{\Theta}_l)[\boldsymbol{H}(\boldsymbol{\Theta}_e)\boldsymbol{H}^{\mathrm{H}}(\boldsymbol{\Theta}_e)]^{-1}\boldsymbol{H}(\boldsymbol{\Theta}_e)$. 采用分布式协作窃听方法是窃听者虚拟将自己置于合法用户的位置估计传输信息. 这样, 人工噪声干扰得到有效抑制, 即

$$\boldsymbol{\Xi}\boldsymbol{n}_a=\boldsymbol{H}^{\mathrm{H}}(\boldsymbol{\Theta}_l)[\boldsymbol{H}(\boldsymbol{\Theta}_e)\boldsymbol{H}^{\mathrm{H}}(\boldsymbol{\Theta}_e)]^{-1}\boldsymbol{H}(\boldsymbol{\Theta}_e)\boldsymbol{H}^{\mathrm{H}}(\boldsymbol{\Theta}_e)\boldsymbol{P}_a\boldsymbol{z}=\mathbf{0}.\tag{47}$$

从式 (46) 可以看出, 尽管窃听者接收信号的 SNR 会比合法用户差, 但对于足够高接收灵敏度的窃听者依然可以恢复调制符号. 而 ZF 方法的波束形成矢量设计仅依赖于静态的导向向量. 若窃听者获得足够的先验信息, 就可能恢复保密信息, 安全通信将失效. 而所提方法引入随机发射子集, 产生随机动态的发射导向矢量, 对窃听者产生了随机等效时变的导向矢量, 结合人工噪声辅助, 增加了各种窃听者窃取保密信息的难度, 增强无线传输的安全性能.

4.2 平均保密速率

根据式 (5), 合法用户 k 接收信号的 SINR 表示为

$$\gamma_l(\theta_{l,k})=\mathbb{E}\left\{\frac{\left|\boldsymbol{h}^{\mathrm{H}}(\theta_{l,k})(\boldsymbol{\tau}\circ\boldsymbol{v})\boldsymbol{a}^{\mathrm{H}}(\theta_{l,k})\boldsymbol{u}_k\right|^2}{\left|\boldsymbol{h}^{\mathrm{H}}(\theta_{l,k})(\boldsymbol{\tau}\circ\boldsymbol{n}_a)\boldsymbol{a}^{\mathrm{H}}(\theta_{l,k})\boldsymbol{u}_k\right|^2+\sum_{r=1}^{R}\left|\rho_{k,r}\sqrt{E_{j,r}}s_{j,r}\boldsymbol{a}^{\mathrm{H}}(\theta_{j,k,r})\boldsymbol{u}_k\right|^2+\sigma_{l,k}^2}\right\},\tag{48}$$

其中 $\mathbb{E}\{\cdot\}$ 表示遍历所有天线子集 $\mathcal{Z}$. 利用所提的阵列子集、波束形成矢量优化、人工噪声投影矩阵计算和接收权矢量设计, 合法用户 k 接收信号的 SINR 可以表示为

$$\gamma_l(\theta_{l,k})\geqslant\frac{\zeta_k^2}{\sigma_{l,k}^2}.\tag{49}$$

显然, 合法用户 k 接收信号的 SINR 满足指定接收 SNR 要求, 可以为合法用户提供所需的信号质量传输保证.

由于窃听者任意分布, 将合法用户方向主瓣以外的所有方向都视为存在窃听者的潜在方向, 即

$$\mathcal{D}_e=[-\pi,\pi]\backslash\bigcup_{k=1}^{K}\mathcal{D}_{l,k},\tag{50}$$

其中 $\mathcal{D}_{l,k}=[\theta_{l,k}-\frac{\theta_{\mathrm{BW}}}{2},\theta_{l,k}+\frac{\theta_{\mathrm{BW}}}{2}]$, $\theta_{\mathrm{BW}}=\frac{2c}{f_cN_td}$ 表示主瓣波束带宽 [35]. 然后, 根据式 (7), 在 $\theta_e\in\mathcal{D}_e$ 方向, 窃听者接收信号的 SINR 表示为

$$\gamma_e(\theta_e)=\mathbb{E}\left\{\frac{|\boldsymbol{h}^{\mathrm{H}}(\theta_e)(\boldsymbol{\tau}\circ\boldsymbol{v})|^2}{|\boldsymbol{h}^{\mathrm{H}}(\theta_e)(\boldsymbol{\tau}\circ\boldsymbol{n}_a)|^2+\sigma_e^2}\right\}.\tag{51}$$

很容易发现位于旁瓣的非期望接收机接收到的信号遭受严重的符号间干扰、发射子集随机干扰和人工噪声干扰. 可达速率定义为接收机可靠恢复信息的最大比特率. 由于预先指定接收 SNR, 当合法用户接收信号的 SINR 低于预定值时, 将视为无效接收, 可达速率为零. 选择合法用户中最小可达速率.

对于未知的窃听者, 在窃听区域选择最大可达速率, 即更有利于窃听的情况. 根据可达速率的定义 [25], 合法用户和窃听者的可达速率分别定义为

$$R_l \triangleq \begin{cases} \min\limits_{k\in\mathcal{K}} \log_2[1+\gamma_l(\theta_{l,k})], & \gamma_l(\theta_{l,k}) \geqslant \zeta_k, \\ 0, & \text{else}, \end{cases} \tag{52}$$

和

$$R_e \triangleq \max_{\theta_e\in\mathcal{D}_e} \log_2[1+\gamma_e(\theta_e)]. \tag{53}$$

合法用户和窃听者接收信号之间的互信息用于评估系统安全传输性能. 保密速率就是合法用户和窃听者可达速率之差或零. 于是, 定义平均保密速率为

$$R_s \triangleq \max\left\{R_l - R_e, 0\right\}. \tag{54}$$

4.3 误符号率

在下文中, 研究所提方法接收信号的 SER. 根据设计, 合法用户接收的信号满足指定 SNR 约束, 可以将其表示为

$$y(\theta_k) = \zeta_k x_k + n_k,\ \forall k \in \mathcal{K}. \tag{55}$$

将接收到的信号投影到实轴和虚轴上, 可得

$$[\mathrm{Re}\{y(\theta_k)\}, \mathrm{Im}\{y(\theta_k)\}] = [\zeta_k \cos(\arg\{x_k\}) + \mathrm{Re}\{n_k\}, \zeta_k \sin(\arg\{x_k\}) + \mathrm{Im}\{n_k\}]. \tag{56}$$

假设 x_k 固定, 接收到的信号 $y(\theta)$ 受到复 AWGN 叠加, 相应的概率密度函数 (probability density function, PDF) 表示为

$$\begin{aligned} \Pr\{y(\theta)|x_k\} = \frac{1}{\sigma^2\pi} \exp\left\{-\frac{\left[\mathrm{Re}\{y(\theta)\} - \zeta_k\cos(\arg\{x_k\})\right]^2}{\sigma^2}\right\} \\ \times \exp\left\{-\frac{\left[\mathrm{Im}\{y(\theta)\} - \zeta_k\sin(\arg\{x_k\})\right]^2}{\sigma^2}\right\}. \end{aligned} \tag{57}$$

定义 $A \triangleq \sqrt{\mathrm{Re}^2\{y(\theta)\} + \mathrm{Im}^2\{y(\theta)\}}$ 和 $\vartheta \triangleq \arg\{y(\theta)\}$. 然后, 根据极坐标变换 [36], 可将式 (57) 转变为

$$\begin{aligned} \Pr\{A, \vartheta|x_k\} = \frac{A}{\sigma^2\pi} \exp\left\{-\frac{A^2 + \zeta_k^2 + 2\zeta_k A\cos(\arg\{x_k\} + \vartheta)}{\sigma^2}\right\} \\ \times \exp\left\{-\frac{2\zeta_k A\sin(\arg\{x_k\} + \vartheta)}{\sigma^2}\right\}. \end{aligned} \tag{58}$$

于是, 通用 SER 表示为

$$P_e(x_k) = 1 - \int_{-\frac{\pi}{M}}^{+\frac{\pi}{M}} \int_{\zeta_k}^{+\infty} \Pr\{A, \vartheta|x_k\} \mathrm{d}\vartheta \mathrm{d}A. \tag{59}$$

4.4 计算复杂度

在这部分中分析所提方法的计算复杂度. 根据所提安全传输策略, 我们知道所提方法分 3 个步骤: (1) 固定/放松相位符号级方向调制设计波束形成矢量; (2) 人工噪声投影矩阵计算; (3) 计算接收权矢量. 固定相位设计波束形成矢量, 根据式 (21) 通过 SVD, 其计算复杂度为 $\mathcal{O}(2N_aK^2)$, 优化问题 P5 迭数算法的计算复杂度为 $\mathcal{O}((2N_a-K)^3\ln\varepsilon^{-1})$ [37]. 松弛相位设计波束形成矢量, 根据优化问题 P12, 计算复杂度为 $\mathcal{O}((2N_a)^3\ln\varepsilon^{-1})$. AN 投影矩阵计算, 根据式 (38) 和 (39), 计算复杂度为 $\mathcal{O}(N_aK^2+N_a(N_a-K))$. 接收权矢量, 根据式 (41), 计算复杂度为 $\mathcal{O}(N_l^3+3N_l^2+2N_l+N_l^2L+2)$. 另外, 采用 ZF 方法, 根据式 (44), 其计算预复杂度为 $\mathcal{O}(K^3+2KN_l^2+KN_l)$.

5 实验结果与分析

本节将给出仿真结果验证所提方法的安全性能, 也将所提方法与 ZF 方法作比较. 仿真中设置参数如下, 发射载波频率为 $f_c=35$ GHz 的毫米波通信系统. 该系统由一个 N_t 阵元的 ULA 发射机, K 个 N_l 阵元的合法用户组成, 合法用户的方位角分别为 $\theta_{l,k}$, $\forall k\in\mathcal{K}$. 为简单起见, 发射和接收端 ULA 阵元间距取 $d_t=d_l=c/2f_c$ (间距可不同) 以避免栅瓣效应. 假设所有合法用户背景热噪声方差和指定 SNR 相同, 即 $10\lg(\sigma_{l,k}^2)=-100$ dBm 和 $\eta=\eta_k$, $\forall k$. R 个主动窃听者发出的干扰信号, 其干扰噪声比 (jamming-to-noise ratio, JNR) 为 40 dB. 若无特别说明, 选取 QPSK 作为基带调制发射信号. 遵循自由空间中的电磁波传播路径损耗模型 [38], 信号衰减因子由载波频率和传输距离决定.

首先, 图 5 展示了发射和接收波束方向图, 取 $K=2$, $N_t=16$, $N_a=12$, $E_t=40$ dBm, $N_l=12$, $\eta=10$ dB, $\theta_{l,1}=-40°$, $\theta_{l,2}=5°$, $R=3$, $\theta_{j,1,1}=-70°$, $\theta_{j,1,2}=-10°$, $\theta_{j,1,3}=40°$, $\theta_{j,2,1}=-50°$, $\theta_{j,2,2}=30°$, $\theta_{j,2,3}=60°$. 如图 5 所示, 发射信号的 SINR 在合法用户的方向上综合出两个峰值, 其值等于指定接收 SNR 值 10 dB. 在弱的信息泄漏功率和人工噪声干扰共同作用下, 在其他非期望方向的 SINR 较低. 另外, 从合法用户接收方向图可以看出, 对于每个合法用户, 沿主动窃听者发出干扰信号的方向形成很深的零陷, 这表示合法用户可以有效地抑制干扰信号. 同时, 来自发射机方向的增益为零, 这表明接收端不影响发射机发射的信号. 综上所述, 所提方法可以有效抑制干扰信号, 并按照指定通信质量实现发射机与合法用户之间可靠传输, 同时降低窃听者截获保密信息的可能性, 能够达到在混合环境下安全传输的目的.

图 6 比较了所提方法与 ZF 方法发射符号方向图. 取 $K=2$, $N_t=16$, $N_a=12$, $E_t=40$ dBm, $\eta=10$ dB, $\theta_{l,1}=-40°$, $\theta_{l,2}=5°$, 100 个随机 QPSK 调制符号流发送给合法用户. 所提方法远场辐射信号的 SINR 和相位方向图随方位角变化的关系如图 6(a) 所示. 在期望方向接收信号的 SINR 符合指定 SNR 值, 相位和发射调制符号相位一致只有 4 个相位, 而且发射阵元子集和人工噪声随机变化不影响合法用户的接收信号. 同时可以看出由于人工噪声和发射子集的随机变化大大增加非期望方向的随机性, 非期望方向的信号遭到严重地随机扰乱. 此外, 图 6(b) 中显示 ZF 方法的 SINR 和相位方向图. 可以看出, ZF 方法能保证合法方向的有效接收, 在其他方向信号有一定扰乱, 但相对较固定. 对于窃听者可以通过研究接收信号的规律从而破解保密信息. 而所提方法在非期望方向造成的随机动态特性有利于无线通信安全. 另外, 所提方法使得主瓣宽度变得更窄, 可以有效提高无线传输安全性能.

图 7(a) 比较了所提方法与 ZF 方法所需的平均发射信息功率随激活天线数目变化曲线. 取 $K=4,8$, $\eta=10$ dB. 可以观察到, 与 ZF 方法相比, 在激活天线数目较少且合法用户数目更多情况下, 所提方法消耗较少的发射信息功率. 与固定相位方法相比, 松弛相位方法消耗更少的发射信息功率. 同样, 固定相位方法比 ZF 方法消耗更少的发射信息功率, 这是由于所提的符号级方向调制方法利用发射符

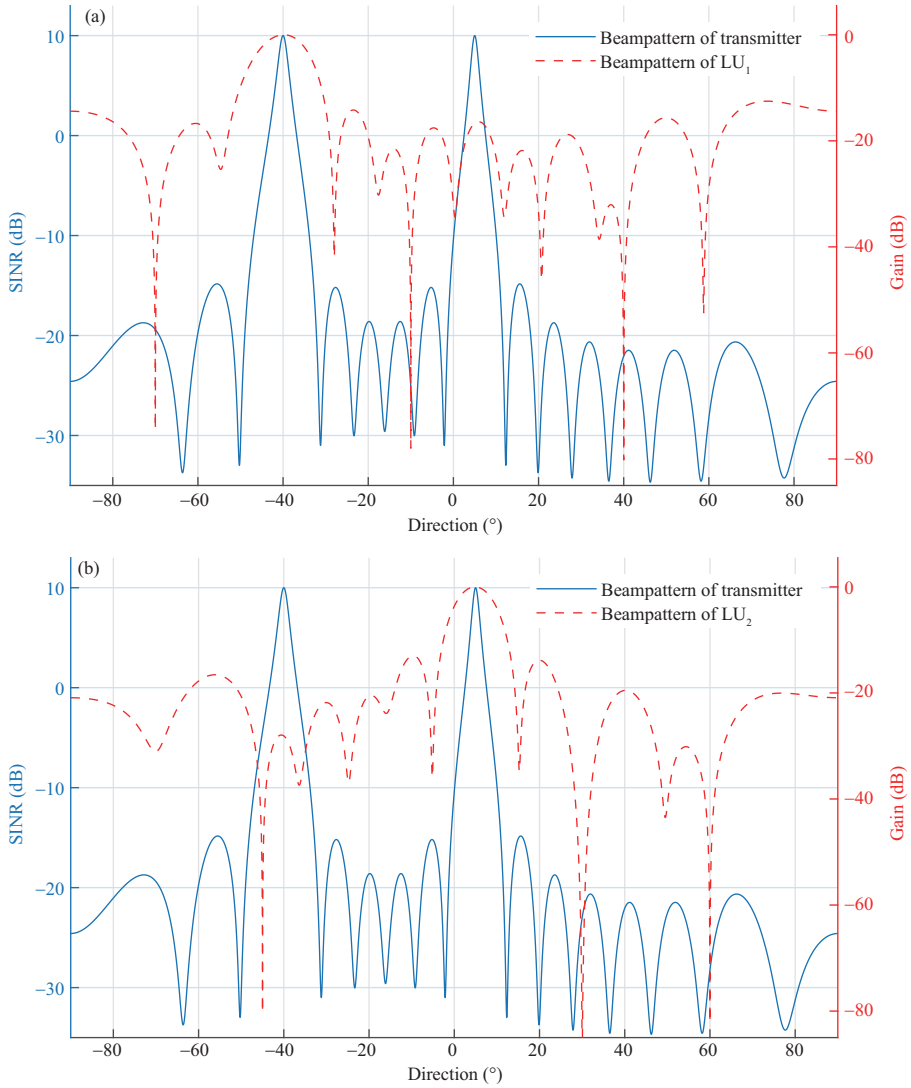

图 5　发射接收方向图

Figure 5　The transmit and receive beampatterns of (a) LU_1 and (b) LU_2 vs. direction

号间的干扰. 随着激活发射天线数量的增加, 所有方案消耗发射信息功率都减少, 发射信息功率差别也逐渐减小, 这是由于发射天线数量的增加会获得更多空间自由度.

图 7(b) 显示了所提方法与 ZF 方法指定 SNR 对平均发射信息功率的影响. 取 $K = 4, 8$, $N_t = 12$. 从图 7(b) 可以看出, 随着合法用户指定接收 SNR 的增加, 所有方法都需要消耗更多的发射信息功率才能满足合法用户所需接收信号质量. 此外, 在较多的合法用户时, 所提方法比 ZF 方法消耗更少发射信息功率.

图 8 描绘了合法用户接收到的 QPSK 和 8-PSK 调制符号星座图. 如图所示, 无噪声接收符号星座图的相对几何形状符合固定相位和松弛相位的约束. 所提设计方法消耗更少的发射信息功率确保所有合法用户按指定 SNR 接收信号, 这是因为所提方法将码间干扰转化为有利功率辅助其他符号. 此外, 由于所提方法在满足合法用户可靠接收的同时需要更少的发射信息功率, 在固定总发射功率情况

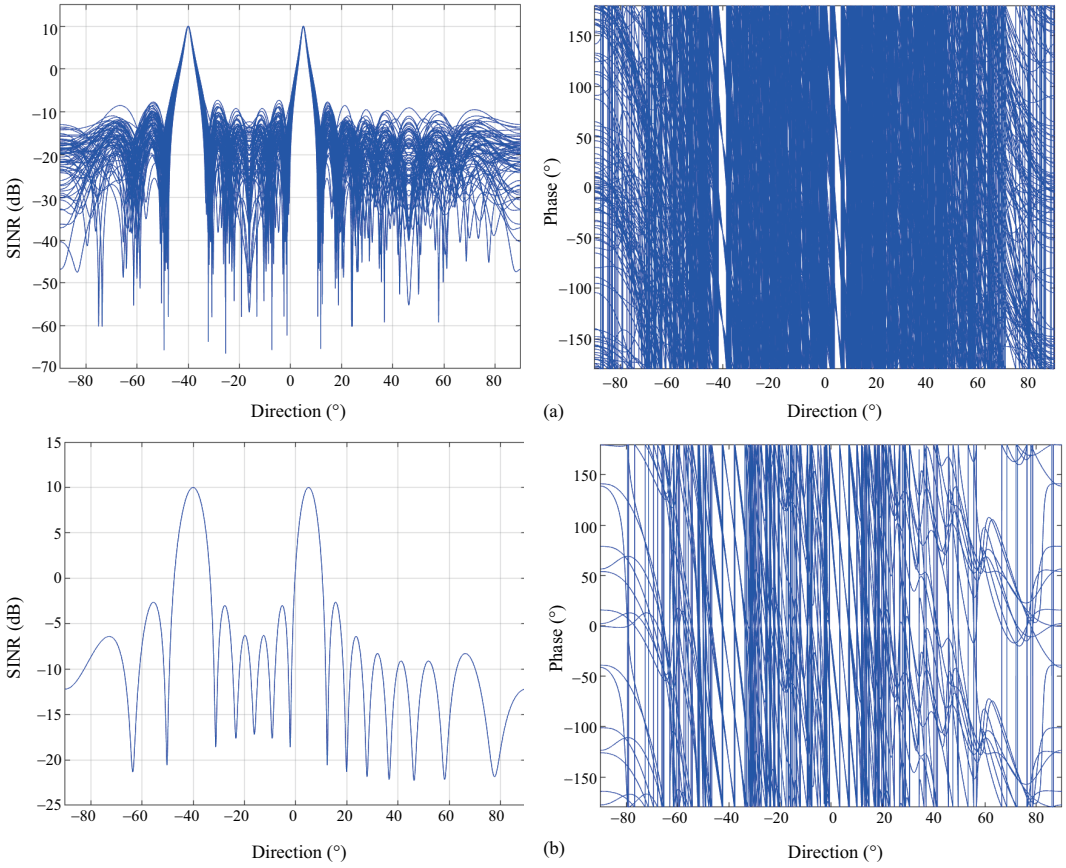

图 6　方向调制 SINR 和相位辐射方向图. (a) 所提方法和 (b) ZF 方法的方向

Figure 6　Far-field radiation patterns of SINR and phase vs. directions for the (a) proposed method and (b) ZF method

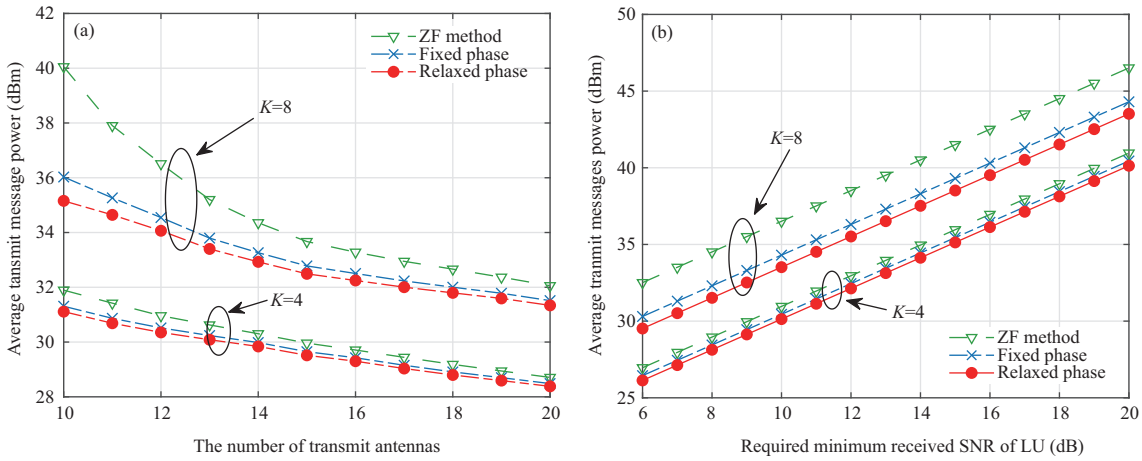

图 7　(a) 所提方法和 ZF 方法发射信息功率与发射天线数关系曲线和 (b) 所提方法和 ZF 方法发射信息功率与指定 SNR 关系曲线

Figure 7　(a) Transmit message power vs. the number of transmit antennas for the proposed method and ZF method; (b) transmit message power vs. the required SNR for the proposed method and ZF scheme

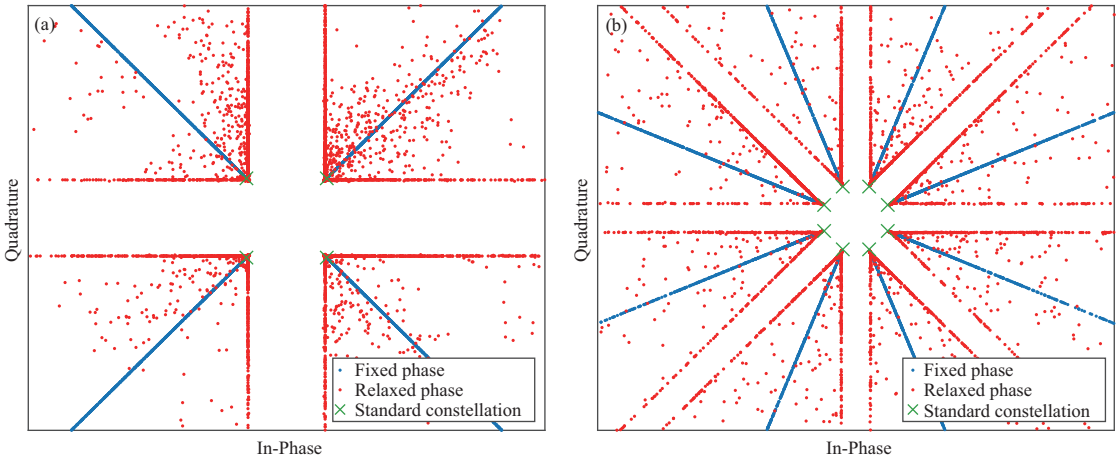

图 8　无噪声接收符号星座图. (a) QPSK 调制和 (b) 8-PSK

Figure 8　The scatter plots of the noise-free received symbols for (a) QPSK modulation and (b) 8-PSK modulation

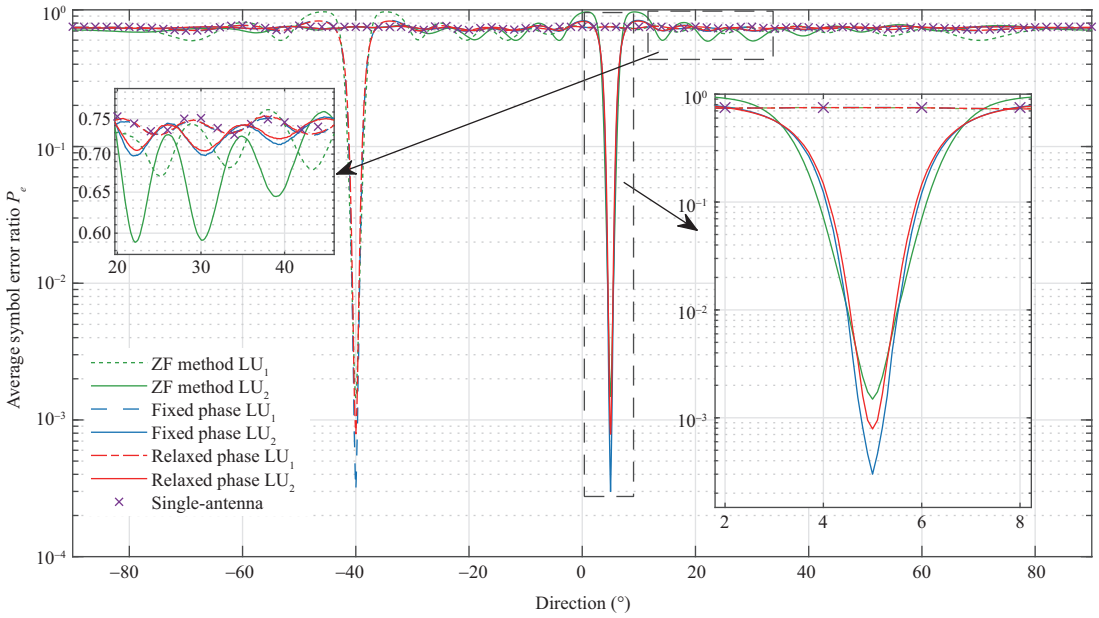

图 9　所提议方案和 ZF 方法的平均 SER 方向图

Figure 9　Average SER for the proposed method and ZF method vs. direction

下, 更多的发射功率可以分配给人工噪声, 从而增强保密性能.

图 9 进一步显示了 SER 分布随方位角变化的关系图. 取 $K=2$, $N_t=16$, $N_a=12$, $E_t=40$ dBm, $\eta=10$ dB, $\theta_{l,1}=-40°$, $\theta_{l,2}=5°$. 从图中可以看出, 在合法用户方向所提的松弛相位法比固定相位方法接收信号的 SER 略高, 松弛相位法比 ZF 方法具有更低的 SER. 在合法用户方向的主瓣外, 采用固定相位方法接收信号的 SER 波动大于松弛相位方法, 小于 ZF 方法. 随着远离合法用户方向, 所提方法接收信号的 SER 迅速下降. 换句话说, 所提方法使得接收信号的 SER 主瓣波束更窄, 并且更有效地抑制旁瓣接收信号的 SER 波动, 这更有利于减少窃听者拦截信息的可能性. 同时还验证合法用户

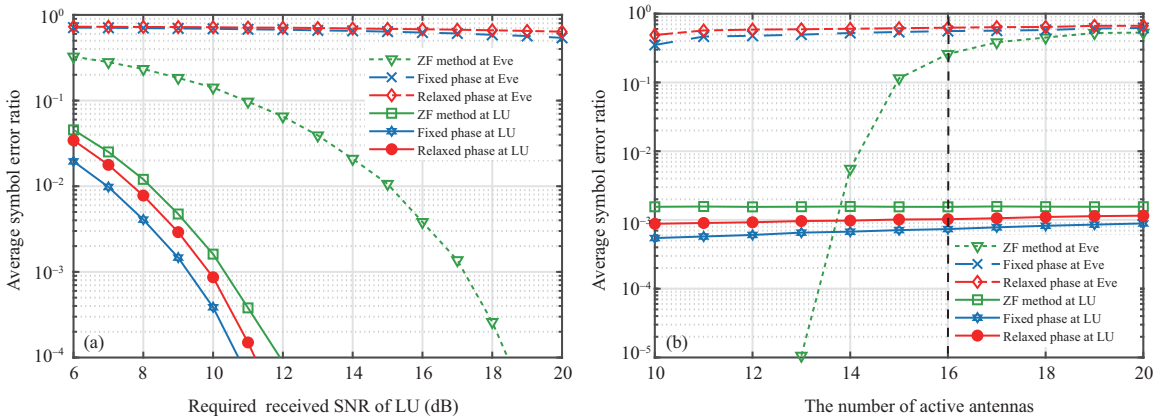

图 10　(a) 所提方法和 ZF 方法平均 SER 与指定 SNR 关系曲线和 (b) 所提方法和 ZF 方法平均 SER 与发射天线数关系曲线

Figure 10　(a) Average SER vs. required SNR for the proposed method and ZF method; (b) transmit message power vs. the number of transmit antennas for the proposed method and ZF method

可以同时正确获得各自的信息流.

图 10(a) 显示了所提方法和 ZF 方法在不同指定接收 SNR 对合法用户和窃听者接收信号平均 SER 的影响. 取 $K=4$, $N_t=16$, $N_e \geqslant N_t$, $E_t=40$ dBm. 从图 10(a) 可以看出, 合法用户的平均 SER 随着指定 SNR 的增加而降低. 与 ZF 方法相比, 所提方法在合法用户实现更低的 SER. ZF 方法在窃听者获得更低的 SER, 并且随着合法用户指定接收 SNR 增大而降低, 这意味着窃听者可以截获更多保密信息, 而采用所提方法, 窃听者一直保持较高的 SER. 这是由于当 $N_e \geqslant N_t$ 时, 采用了分布式合作窃听方法来截获保密符号更有利于窃听, 而所提方法采用随机发射阵列子集使得窃听者无法正确估计符号.

图 10(b) 描述了所提方法和 ZF 方法不同激活天线数随合法用户和窃听者接收信号的 SER 变换关系. 取 $N_e=16$. 从图中可以看出, 所提方法由于对合法用户接收信号的 SNR 约束, 使得合法用户接收的 SER 保持恒定. 与 ZF 方法相比, 所提方法在合法用户具有更低的 SER. 当 $N_e<N_t$ 时, 窃听者直接窃听保密信息, 所提方法在窃听者接收信号的 SER 略多于 ZF 方法. 另一方面, 随着发射天线数量的减少, 当 $N_e \geqslant N_t$ 时, 窃听者通过分布式方法, 根据式 (46) 估计保密信息. 此时采用 ZF 方法窃听者接收信号 SER 迅速下降, 而所提方法, 由于人工噪声和发射阵列子集的引入, 窃听者接收信号的 SER 依然很高.

图 11 比较了不同方法的平均保密速率随总发射功率变化关系, 取 $K=4,8$, $N_t=16$, $\eta=10$ dB. 为了保证合法用户的有效接收, 要求总发射功率超过所需的最小发射信息功率, 否则无法设计波束形成矢量, 其平均保密速率为零. 随着总发射功率的增加, 更多发射功率分配给了人工噪声, 平均保密速率增高, 具有更高的安全性能. 来自主动窃听者发出的干扰信号导致单天线合法用户无法有效地接收, 因此传统的单天线接收机的平均保密速率为零.

6　结论

本文考虑了混合窃听环境下的毫米波无线安全传输问题, 提出了一种人工噪声辅助多波束符号级方向调制发射子集、相控阵接收综合方法. 具体来说, 通过优化波束形成矢量来最大程度地降低发射

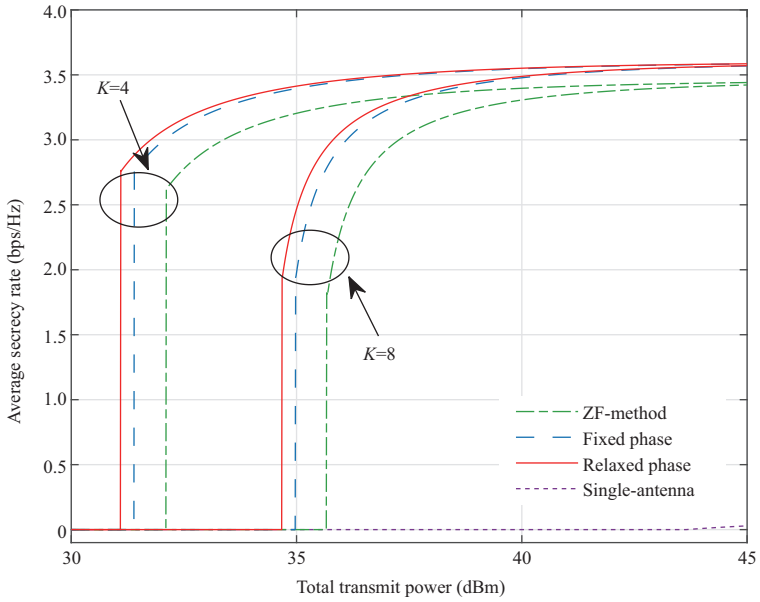

图 11　平均保密率与总发射功率关系曲线

Figure 11　The average secrecy rate vs. the total transmit power

信息功率, 满足每个合法用户符号级约束, 并结合人工噪声和发射天线子集最大限度地随机干扰窃听者的接收信号. 此外, 合法用户接收端通过 MVDR 方法优化接收权矢量, 使得合法用户可以有效消除来自主动窃听者的干扰信号. 所提方法各步骤均通过封闭式求解, 高效支撑后续工程实现. 最后仿真结果表明, 所提方法是混合窃听环境下实现无线安全传输的有效途径.

参考文献

1　Xiao M, Mumtaz S, Huang Y M, et al. Millimeter wave communications for future mobile networks. IEEE J Sel Areas Commun, 2017, 35: 1909–1935

2　Semiari O, Saad W, Bennis M, et al. Integrated millimeter wave and sub-6 GHz wireless networks: a roadmap for joint mobile broadband and ultra-reliable low-latency communications. IEEE Wirel Commun, 2019, 26: 109–115

3　Lyu R Y, Cheng W C, Zhang W. Modeling and performance analysis of OAM-NFC systems. IEEE Trans Commun, 2021, 69: 7986–8001

4　Cheng W C, Zhang W, Jing H Y, et al. Orbital angular momentum for wireless communications. IEEE Wirel Commun, 2019, 26: 100–107

5　Ju Y, Wang H M, Zheng T X, et al. Secure transmissions in millimeter wave systems. IEEE Trans Commun, 2017, 65: 2114–2127

6　Qi Q, Chen X M, Zhong C J, et al. Physical layer security for massive access in cellular Internet of Things. Sci China Inf Sci, 2020, 63: 121301

7　Wang C, Wang H M. Physical layer security in millimeter wave cellular networks. IEEE Trans Wirel Commun, 2016, 15: 5569–5585

8　Chorti A. Brief report on QoSec, context aware security and the role of physical layer security in 6G wireless. 2020. ArXiv:2011.07323

9　Ylianttila M, Kantola R, Gurtov A, et al. 6G white paper: research challenges for trust, security and privacy. 2020. ArXiv:2004.11665

10　Shu F, Shen T, Xu L, et al. Directional modulation: a physical-layer security solution to B5G and future wireless

networks. IEEE Netw, 2020, 34: 210–216
11 Shu F, Wu X M, You X H, et al. Directional modulation-based secure wireless transmission: basic principles, key techniques, and applications. Sci Sin Inform, 2017, 47: 1209–1225 [束锋, 吴肖敏, 尤肖虎, 等. 基于方向调制的物理层安全无线传输原理、关键技术与未来应用. 中国科学: 信息科学, 2017, 47: 1209–1225]
12 Xie T, Zhu J, Li Y. Artificial-noise-aided zero-forcing synthesis approach for secure multi-beam directional modulation. IEEE Commun Lett, 2018, 22: 276–279
13 Zhang X, Xia X G, He Z, et al. Phased-array transmission for secure mmWave wireless communication via polygon construction. IEEE Trans Signal Process, 2020, 68: 327–342
14 Shu F, Zhu W, Zhou X W, et al. Robust secure transmission of using main-lobe-integration-based leakage beamforming in directional modulation MU-MIMO systems. IEEE Syst J, 2018, 12: 3775–3785
15 Shu F, Jiang X Y, Liu X, et al. Precoding and transmit antenna subarray selection for secure hybrid spatial modulation. IEEE Trans Wirel Commun, 2021, 20: 1903–1917
16 Choi Y, Lee J, Rim M, et al. Constructive interference optimization for data-aided precoding in multi-user MISO systems. IEEE Trans Wirel Commun, 2019, 18: 1128–1141
17 Alodeh M, Chatzinotas S, Ottersten B. Energy-efficient symbol-level precoding in multiuser MISO based on relaxed detection region. IEEE Trans Wirel Commun, 2016, 15: 3755–3767
18 Valliappan N, Lozano A, Heath R W. Antenna subset modulation for secure millimeter-wave wireless communication. IEEE Trans Commun, 2013, 61: 3231–3245
19 Alotaibi N N, Hamdi K A. Switched phased-array transmission architecture for secure millimeter-wave wireless communication. IEEE Trans Commun, 2016, 64: 1303–1312
20 Shu F, Zhu L L, Cai W L, et al. Two efficient beamformers for secure precise jamming and communication with phase alignment. IEEE Wirel Commun Lett, 2020, 9: 406–410
21 Wang W Q, Zheng Z. Hybrid MIMO and phased-array directional modulation for physical layer security in mmWave wireless communications. IEEE J Sel Areas Commun, 2018, 36: 1383–1396
22 Wu Y P, Schober R, Ng D W K, et al. Secure massive MIMO transmission with an active eavesdropper. IEEE Trans Inform Theory, 2016, 62: 3880–3900
23 Chen H, Tao X F, Li N, et al. Secrecy performance analysis for hybrid wiretapping systems using random matrix theory. IEEE Trans Wirel Commun, 2019, 18: 1101–1114
24 Maltsev A, Pudeyev A, Bolotin I, et al. Millimetre-wave Evolution for Backhaul and Access. MiWEBA Germany Technical Report FP7-ICT, 2014
25 Lin J R, Li Q, Yang J T, et al. Physical-layer security for proximal legitimate user and eavesdropper: a frequency diverse array beamforming approach. IEEE Trans Inform Forensic Secur, 2018, 13: 671–684
26 Shu F, Qin Y L, Liu T T, et al. Low-complexity and high-resolution DOA estimation for hybrid analog and digital massive MIMO receive array. IEEE Trans Commun, 2018, 66: 2487–2501
27 Khisti A, Wornell G W. Secure transmission with multiple antennas — part II: the MIMOME wiretap channel. IEEE Trans Inform Theory, 2010, 56: 5515–5532
28 Shu F, Xu L, Wang J Z, et al. Artificial-noise-aided secure multicast precoding for directional modulation systems. IEEE Trans Veh Technol, 2018, 67: 6658–6662
29 Horn R A, Johnson C R. Matrix Analysis. Cambridge: Cambridge University Press, 2012
30 Bertsekas D P. Nonlinear programming. J Oper Res Soc, 1997, 48: 334–334
31 Nguyen V D, Duong T Q, Dobre O A, et al. Joint information and jamming beamforming for secrecy rate maximization in cognitive radio networks. IEEE Trans Inform Forensic Secur, 2016, 11: 2609–2623
32 van Trees H L. Detection, Estimation, and Modulation Theory, Part I: Detection, Estimation, and Linear Modulation Theory. Hoboken: John Wiley and Sons, 2004
33 Choi L U, Murch R D. A transmit preprocessing technique for multiuser MIMO systems using a decomposition approach. IEEE Trans Wirel Commun, 2004, 3: 20–24
34 Kalantari A, Soltanalian M, Maleki S, et al. Directional modulation via symbol-level precoding: a way to enhance

security. IEEE J Sel Top Signal Process, 2016, 10: 1478–1493
35 John D K, Ronald J M. Antennas: for All Applications. New York: McGraw Hill, 2002
36 Proakis J G, Salehi M. Digital Communications. New York: McGraw hill, 2001
37 Polyak R A. Projected gradient method for non-negative least square. Contemp Math, 2015, 636: 167–179
38 Goldsmith A. Wireless Communications. Cambridge: Cambridge University Press, 2005

Multi-beam symbol-level secure transmission against hybrid eavesdropping

Bin QIU & Wenchi CHENG*

The State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071*, China*
* Corresponding author. E-mail: wccheng@xidian.edu.cn

Abstract In this paper, we consider a physical layer security (PLS) problem for a hybrid wiretapping wireless system in millimeter-wave transmission, where the active eavesdropper and passive eavesdropper (Eve) may coexist to intercept the confidential messages and emit jamming signals. To achieve secure and reliable transmission, we propose a switched phased-array directional modulation (DM) scheme that employs multi-beam symbol-level precoding with aided artificial noise (AN) technique at the transmitter, and array reception at legitimate users (LU). Here we consider a more practical case that the information of the eavesdropper (Eve) is unknown by the transmitter. Leveraging DM beamforming, we aim to minimize transmit message power by optimizing the beamforming vector, subject to prescribed symbol-level constraints, thus generating exact/relaxed phases at LU. The remaining transmit power can be utilized to generate AN. Additionally, by means of the minimum variance distortionless response method at the LU, the jamming caused by active Eve can be efficiently eliminated. Simulation results demonstrate the superiority of the proposed scheme.

Keywords physical layer security, artificial noise, hybrid eavesdropping, multibeam, directional modulation