多用户干扰网络中基于干扰对齐的安全传输方案

胡林[1]，范家兵[1]，文红[2]，唐杰[2]，陈前斌[1]
（1. 重庆邮电大学通信与信息工程学院，重庆 400065；2. 电子科技大学航空航天学院，四川 成都 611731）

摘 要：面向物联网业务中的信息安全需求，考虑多用户干扰网络中存在多个窃听节点的场景，提出基于干扰对齐（IA, interference alignment）的物理层安全传输方案。为解决传统干扰对齐算法可能导致保密信号消除的问题，提出一种改进的交替最小化（AM, alternating minimization）方法，通过交替优化发射和接收矩阵消除多用户干扰，同时利用人工噪声（AN，artificial noise）辅助的最大特征模式波束成形（max-eigenmode beamforming）进行安全传输。为更加准确地分析该方案的可行性，提出将干扰对齐方程分解为独立的子方程及其组合，通过分析每个方程的可解性，得到了更严格的可行性必要条件。最后，通过优化保密信号和人工噪声之间的功率分配比例，在满足安全中断概率（SOP）的约束下，实现安全传输速率的最大化。仿真结果表明，该方案不但可以保证保密信号的质量，同时可以提高安全性能，因此可以更好地支持多用户干扰网络中的安全业务。

关键词：干扰对齐；物理层安全；人工噪声；安全中断概率；安全速率
中图分类号：TN918.82
文献标志码：A
doi: 10.11959/j.issn.2096−3750.2023.00331

Interference alignment based secure transmission scheme in multi-user interference networks

HU Lin[1], FAN Jiabing[1], WEN Hong[2], TANG Jie[2], CHEN Qianbin[1]
1. School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
2. School of Aeronautics and Astronautics, University of Electronic Science and Technology of China, Chengdu 611731, China

Abstract: Faced with the requirement of information security in internet of things, a scenario of multi-user interference networks with multiple eavesdroppers was considered, and an interference alignment (IA) scheme based physical layer secure transmission was proposed. Traditional IA security algorithm may result in secret signal cancellation. To overcome this threat, a modified alternating minimization (AM) method was proposed. The multi-user interference was eliminated by alternatively optimizing transceiver matrices, and artificial noise (AN) aided max-eigenmode beamforming was employed for secure transmission. To obtain a more accurate analysis of IA feasibility, the IA equation was divided into independent subsets and their combinations. By analyzing each case, a much tighter necessary condition for IA feasibility was established. Finally, the power allocation ratio between the secret signal and the AN signal was optimized to maximize the secrecy outage probability (SOP) constrained secrecy rate. Numerical results confirm that both the quality and security of the secret signal have been enhanced. Therefore, the proposed scheme is more suitable and reliable for security applications in interference networks.

Key words: interference alignment, physical layer security, artificial noise, secrecy outage probability, secrecy rate

收稿日期：2022−09−05；**修回日期：**2023−03−09
通信作者：胡林，lin.hu@ieee.org
基金项目：国家自然科学基金资助项目（No.61801060，No.61901089）；国家重点研发计划（No.2018YFB0904900，No.2018YFB0904905）；四川省科技计划项目（No.2022YFH0098）
Foundation Items: The National Natural Science Foundation of China (No.61801060, No.61901089), The National Key Research and Development Program of China (No.2018YFB0904900, No.2018YFB0904905), Sichuan Science and Technology Program (No.2022YFH0098)

0　引言

近年来，以低时延、低功耗、超大容量无线覆盖为特征的 5G 移动通信极大促进了物联网的发展[1-2]。物联网技术在可穿戴设备、环境监测、虚拟现实、智能家居和公共服务等多场景得到广泛应用[3]，将数字世界和物理世界紧密相连，加速万物互联时代的到来。

5G 和未来的 6G 无线通信系统具备高密度连接、高速率、低时延和高能效等特性，以支持同时为大量设备提供服务，并保证一定的谱效和能效[4-5]。为了实现上述目标，近年来出现了许多先进技术，如毫米波（mmWave, millimeter wave）技术[6-8]，无人机（UAV, unmanned aerial vehicle）通信[9-11]等。这些技术一方面可以提升通信系统的安全能力，另一方面也存在潜在的安全威胁。窃听者通过采集实时位置、健康状态、个人账户等隐私信息可以追溯设备使用者的相关信息。

对于用户信息的隐私安全，传统方法从密码学的角度进行考虑[12]。但是，加密会产生密文膨胀的问题，在传输过程中带来较大的通信开销。而物理层安全（PLS, physical layer security）技术利用无线信道的随机性实现保密功能，大大降低了系统复杂度，被认为是对密码学技术的重要补充[13-14]。现有的 PLS 技术主要包括大规模多输入多输出（MIMO, multiple-input multiple-output）、全双工技术、智能抗干扰优化算法，以及预编码和波束成形等。

1　相关研究

在无线通信网络中，人工噪声（AN, artificial noise）是增强物理层系统安全的有效手段。不论是快衰落信道（fast fading channel）还是慢衰落信道（slow fading channel）中，人工噪声辅助的安全通信都受到广泛的关注[15-21]。在快衰落信道中，各态历经速率（ESR, ergodic secrecy rate）被用作安全性能的衡量标准[15-16]。而在慢衰落信道中，通常将安全中断概率（SOP, secrecy outage probability）作为安全传输的性能指标[17-18]。此外，文献[19-21]研究了 SOP 约束下安全速率最大化（SRM, secrecy rate maximization）问题。然而，文献[15-21]的安全增强传输方案未考虑干扰抑制，不适用于多用户干扰网络。

在无线网络中，除了广播特性，多用户干扰也是其中一个基本特性，对于安全通信来说极为不利。通过设计发射和接收策略最小化干扰泄漏（ILM, interference leakage minimization），干扰对齐（IA, interference alignment）可以有效解决多用户网络中的干扰管理问题[22]。以干扰对齐为基础，文献[23]分析了多用户干扰网络的自由度（DoF, degrees of freedom）问题。由于干扰对齐问题的过约束性和非凸性，对一般 MIMO 干扰网络的可行性检验是一个 NP-hard 问题[24-25]。

虽然多用户干扰会影响通信质量，然而由于信号的叠加特性，多用户干扰网络具有更高的安全性。文献[26]提出了多用户干扰网络中基于干扰对齐的安全通信方案。在此基础上，文献[27]将来自合法发射机的干扰和人工噪声对齐到不同的子空间中，其优势在于可以进一步迷惑外部窃听者，从而提高安全速率。文献[28]将干扰对齐和协作干扰结合，提出了两种干扰机的预编码方案以干扰窃听。除了窃听节点之间相互独立的情况，文献[29]考虑了干扰网络中部分恶意用户合谋窃听的影响。此外，文献[30]提出了多小区多用户蜂窝网络中的反窃听设计方案，该方案可以在不需要知道窃听节点信道状态信息（CSI, channel state information）的情况下实现可达安全速率。

本文的主要创新点和贡献总结如下。

1) 文献[22]提出传统的干扰对齐算法可能会导致有用信号的消除。本文受此启发，针对传统干扰对齐算法的不足提出了一种改进式干扰对齐算法。通过最大特征模的安全传输方式有效解决信号被消除的问题。数值结果表明，改进后的算法更稳定、更有效。

2) 本文提出了一种更严格的可行性判断条件。具体而言，将干扰对齐的条件分为 3 个独立的子集和它们的组合，并给出了一种判断非对称网络可行性的必要条件。该条件能更加准确地分析非对称系统中干扰对齐的可行性。

3) 为了增强安全性能，本文提出了多用户干扰网络中 SOP 约束下的 SRM 问题。通过对目标函数以及约束条件的变换，将 SRM 问题转化为易于求解的功率分配问题。最后，利用数值方法可得到最优的功率分配比例及其对应的安全速率。另外，通过严格的数学证明得到了特定参数（如合法发送方（Alice）的发射功率和被动窃听者（Eve）的数量）对传输设计的影响。当 Alice 的发

射功率较大时，利用渐近分析得到最优功率分配比例的显式表达式。

2　系统模型

系统模型如图 1 所示，在多个 Eve 存在的情况下，Alice 通过人工噪声辅助的安全波束成形将保密信息传输到合法接收方（Bob）。此外，多用户干扰网络中还包含 K 个合法发射机发送公共信息，同时这 K 个合法发射机在安全传输中作为协作发射机。假设这 K 个发射机和接收机分别配备 M_k 和 N_k 根天线，Alice 和 Bob 分别配备 M_{a} 和 N_{b} 根天线，每个 Eve 均为单根天线。另外，假设所有信道均为一般信道，即信道系数均为独立产生的且服从连续的概率分布。

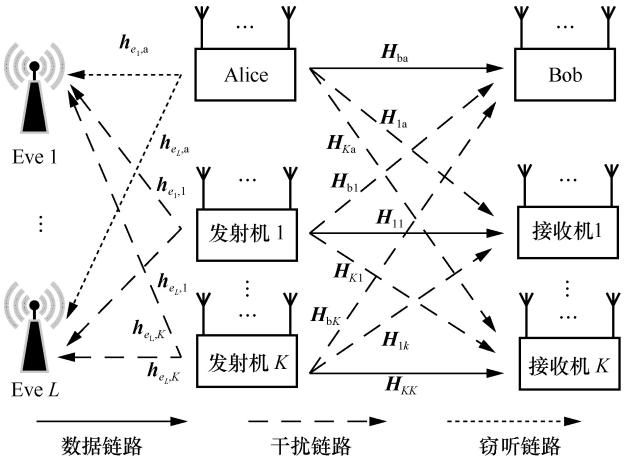

图 1　系统模型

具体而言，本文假设所有信道在平坦慢衰落环境下相互独立且服从瑞利分布。$\boldsymbol{H}_{\mathrm{ba}}\in\mathbb{C}^{N_{\mathrm{b}}\times M_{\mathrm{a}}}$、$\boldsymbol{H}_{k\mathrm{a}}\in\mathbb{C}^{N_k\times M_{\mathrm{a}}}$ 和 $\boldsymbol{h}_{\mathrm{e}_l,\mathrm{a}}\in\mathbb{C}^{M_{\mathrm{a}}}$ 分别表示 Alice 到 Bob、接收机和 Eve l 之间的信道，$l\in\mathcal{L}\triangleq\{1,\,2,\,\cdots,\,L\}$，$k\in\mathcal{K}\triangleq\{1,2,\cdots,K\}$。其中，$\boldsymbol{H}_{\mathrm{ba}}$ 表示主信道，$\boldsymbol{h}_{\mathrm{e}_l,\mathrm{a}}$ 表示窃听信道。$\boldsymbol{H}_{\mathrm{b}k}\in\mathbb{C}^{N_{\mathrm{b}}\times M_k}$、$\boldsymbol{H}_{jk}\in\mathbb{C}^{N_j\times M_k}$ 和 $\boldsymbol{h}_{\mathrm{e}_l,k}\in\mathbb{C}^{M_k}$ 分别表示发射机 k 到 Bob、接收机 j 和 Eve l 之间的信道，$j,k\in\mathcal{K}$。此外，$\boldsymbol{H}_{\mathrm{ba}}$ 和 $\boldsymbol{H}_{kk}$ 分别表示 Alice 到 Bob 和发射机 k 到接收机 k 之间的直连链路。由于很难获取窃听信道 $\boldsymbol{h}_{\mathrm{e}_l,\mathrm{a}}$，因此假设发射方只能够估计窃听信道的信道增益 Γ_{E}。此外，本文假设每个合法用户仅局部 CSI 可知。为了实现从 Alice 到 Bob 的安全传输，Alice 同时传输保密信号与人工噪声信号。因此，Alice 发射的信号 $\boldsymbol{s}_{\mathrm{a}}$ 可以表示为

$$\boldsymbol{s}_{\mathrm{a}}=\sqrt{P_{\mathrm{a}}\phi}\boldsymbol{v}_{\mathrm{a}}x_{\mathrm{a}}+\sqrt{P_{\mathrm{a}}(1-\phi)/d_{\mathrm{an}}}\boldsymbol{W}_{\mathrm{a}}\boldsymbol{z}_{\mathrm{a}}\tag{1}$$

其中，Alice 的传输功率为 P_{a}，$\phi\in(0,1]$ 表示 P_{a} 分配给保密信号的比例。此外，$x_{\mathrm{a}}\sim\mathcal{CN}(0,1)$ 表示 Alice 发送的保密信息，$\boldsymbol{v}_{\mathrm{a}}\in\mathbb{C}^{M_{\mathrm{a}}}$ 表示保密波束成形向量。类似地，$\boldsymbol{z}_{\mathrm{a}}\in\mathbb{C}^{d_{\mathrm{an}}}$ 表示 $d_{\mathrm{an}}\times1$ 维的人工噪声向量，$\boldsymbol{W}_{\mathrm{a}}\in\mathbb{C}^{M_{\mathrm{a}}\times d_{\mathrm{an}}}$ 表示人工噪声预编码矩阵。式(1)中右边的第一项表示保密信号，第二项表示人工噪声信号。

此外，发射机 k 发射的信号 $\boldsymbol{s}_k$ 表示为

$$\boldsymbol{s}_k=\sqrt{P_k/d_k}\boldsymbol{V}_k\boldsymbol{x}_k\tag{2}$$

其中，$\boldsymbol{x}_k\in\mathbb{C}^{d_k}$ 和 $\boldsymbol{V}_k\in\mathbb{C}^{M_k\times d_k}$ 分别表示发送的信号向量和其对应的预编码矩阵，d_k 表示数据流的个数，P_k 表示发射机 k 的发射功率。

由此，经过处理后 Bob 的接收信号为

$$\begin{aligned}\boldsymbol{y}_{\mathrm{b}}&=\boldsymbol{u}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ba}}\boldsymbol{s}_{\mathrm{a}}+\sum_{k=1}^{K}\boldsymbol{u}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{b}k}\boldsymbol{s}_k+\boldsymbol{u}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{n}_{\mathrm{b}}=\\&\underbrace{\sqrt{P_{\mathrm{a}}\phi}\boldsymbol{u}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ba}}\boldsymbol{v}_{\mathrm{a}}x_{\mathrm{a}}}_{\text{保密消息}}+\underbrace{\sqrt{\frac{P_{\mathrm{a}}(1-\phi)}{d_{\mathrm{an}}}}\boldsymbol{u}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ba}}\boldsymbol{W}_{\mathrm{a}}\boldsymbol{z}_{\mathrm{a}}}_{\text{人工噪声}}+\\&\underbrace{\sum_{k=1}^{K}\sqrt{\frac{P_k}{d_k}}\boldsymbol{u}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{b}k}\boldsymbol{V}_k\boldsymbol{x}_k}_{\text{多用户干扰}}+\boldsymbol{u}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{n}_{\mathrm{b}}\end{aligned}\tag{3}$$

其中，$\boldsymbol{u}_{\mathrm{b}}\in\mathbb{C}^{N_{\mathrm{b}}}$ 表示 Bob 处的接收向量，$\boldsymbol{n}_{\mathrm{b}}\in\mathbb{C}^{N_{\mathrm{b}}}$ 表示 Bob 处服从零均值单位方差的加性白高斯噪声（AWGN, additive white Gaussian noise）向量。

为了避免消除保密信号，本文在 Alice（Bob）处设计波束成形，选择 $\boldsymbol{H}_{\mathrm{ba}}$ 的最大奇异值对应的左（右）奇异向量作为 $\boldsymbol{u}_{\mathrm{b}}$（$\boldsymbol{v}_{\mathrm{a}}$）。这种传输方案被称为最大特征模式传输，可以有效避免人工噪声辅助干扰对齐导致有用信号被消除的情况。

此外，经过处理后接收机 k 的接收信号以及 Eve l 的接收信号可以表示为

$$\begin{aligned}\boldsymbol{y}_k&=\sum_{j=1}^{K}\boldsymbol{U}_k^{\mathrm{H}}\boldsymbol{H}_{kj}\boldsymbol{s}_j+\boldsymbol{U}_k^{\mathrm{H}}\boldsymbol{H}_{k\mathrm{a}}\boldsymbol{s}_{\mathrm{a}}+\boldsymbol{U}_k^{\mathrm{H}}\boldsymbol{n}_k=\\&\boldsymbol{U}_k^{\mathrm{H}}\boldsymbol{H}_{kk}\boldsymbol{s}_k+\sum_{j\neq k}^{K}\boldsymbol{U}_k^{\mathrm{H}}\boldsymbol{H}_{kj}\boldsymbol{s}_j+\boldsymbol{U}_k^{\mathrm{H}}\boldsymbol{H}_{k\mathrm{a}}\boldsymbol{s}_{\mathrm{a}}+\boldsymbol{U}_k^{\mathrm{H}}\boldsymbol{n}_k\end{aligned}\tag{4}$$

$$\boldsymbol{y}_{\mathrm{e}_l}=\boldsymbol{h}_{\mathrm{e}_l,\mathrm{a}}^{\mathrm{H}}\boldsymbol{s}_{\mathrm{a}}+\sum_{j=1}^{K}\boldsymbol{h}_{\mathrm{e}_l,j}^{\mathrm{H}}\boldsymbol{s}_j+\boldsymbol{n}_{\mathrm{e}_l},\quad l\in\mathcal{L}\tag{5}$$

其中，$\boldsymbol{U}_k$ 表示接收机 k 的接收矩阵，$\boldsymbol{n}_k$ 和 $\boldsymbol{n}_{\mathrm{e}_l}$ 分别表示接收机 k 处和 Eve l 处的 AWGN。

3　AN 辅助的干扰对齐算法

3.1　问题描述

在 AN 辅助的多用户干扰网络中，为了避免用户间的干扰，采用干扰对齐算法时需要同时满足以下条件

$$\boldsymbol{u}_{\mathrm{b}}^{\mathrm{H}}\left[\boldsymbol{H}_{\mathrm{ba}}\boldsymbol{W}_{\mathrm{a}},\left\{\boldsymbol{H}_{\mathrm{b}k}\boldsymbol{V}_k\right\}_{k=1}^{K}\right]=0 \tag{6}$$

$$\boldsymbol{U}_k^{\mathrm{H}}\left[\boldsymbol{H}_{k\mathrm{a}}\left[\boldsymbol{W}_{\mathrm{a}},\boldsymbol{v}_{\mathrm{a}}\right],\left\{\boldsymbol{H}_{kj}\boldsymbol{V}_j\right\}_{j\neq k}^{K}\right]=0,\ \forall k\in\mathcal{K} \tag{7}$$

$$\boldsymbol{u}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ba}}\boldsymbol{v}_{\mathrm{a}}\neq 0 \tag{8}$$

$$\mathrm{rank}\left(\boldsymbol{U}_k^{\mathrm{H}}\boldsymbol{H}_{kk}\boldsymbol{V}_k\right)=d_k,\ \forall k\in\mathcal{K} \tag{9}$$

其中，式(6)和式(7)等价于存在无干扰的信号空间，式(8)和式(9)保证了期望信号不会被消除。

讨论 1　假设所有信道均为一般信道，对于能够干扰对齐的配置，当信号的预编码与接收设计不与直连链路产生关联时，不会对信号空间的维度造成影响[22]。由式(6)和式(7)可知，$\boldsymbol{U}_k$ 和 $\boldsymbol{V}_k$ 的设计与直连链路 $\boldsymbol{H}_{kk}$ 无关，因此在执行 AM 或 ILM 等传统干扰对齐算法时，式(9)几乎必然成立。同时，由式(6)可以看出在设计 $\boldsymbol{W}_{\mathrm{a}}$ 和 $\boldsymbol{u}_{\mathrm{b}}$ 时需要依赖于直连链路 $\boldsymbol{H}_{\mathrm{ba}}$，因此式(8)不一定成立，从而导致保密信号可能被消除。

3.2　AN 辅助的改进干扰对齐算法设计

由讨论 1 可知，在 AN 辅助的干扰网络中，传统迭代干扰对齐可能导致保密信号被消除的问题。因此，为了消除多用户干扰，同时保证安全性能，本文基于传统 AM 算法[31]提出了一种改进干扰对齐算法。具体而言，将设计过程分为 3 个步骤：首先，选择 $\boldsymbol{H}_{\mathrm{ba}}$ 的最大奇异值对应的左（右）奇异向量作为 $\boldsymbol{u}_{\mathrm{b}}$（$\boldsymbol{v}_{\mathrm{a}}$）；其次，采用 AM 算法迭代更新预编码矩阵 $\boldsymbol{W}_{\mathrm{a}}$ 和 $\boldsymbol{V}_k$ 的干扰子空间；最后，迭代完成后，利用干扰子空间确定接收矩阵 $\boldsymbol{U}_k$。

信号被消除与否取决于式(8)和式(9)是否成立。由于本文中采用最大特征模的方式传输保密信号，式(8)自然成立。由讨论 1 可知，基于 AM 或 ILM 的干扰对齐算法，式(9)成立。因而所提改进干扰对齐算法可以有效避免消除信号。因此，若要实现干扰对齐，只需要同时满足式(6)和式(7)。根据文献[31]，干扰对齐的效果可以通过预编码矩阵和其对应的干扰子空间之间的距离衡量。因此，式(6)和式(7)可以重构为优化问题 P1。

P1：

$$\begin{aligned}&\min_{\boldsymbol{W}_{\mathrm{a}},\boldsymbol{V}_k,\boldsymbol{S}_k}\left\|\boldsymbol{u}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ba}}\boldsymbol{W}_{\mathrm{a}}\right\|_2^2+\sum_{k=1}^{K}\left\|\boldsymbol{u}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{b}k}\boldsymbol{V}_k\right\|_2^2+\\&\sum_{k=1}^{K}\left(\left\|\Pi_{\boldsymbol{S}_k}^{\perp}\boldsymbol{H}_{k\mathrm{a}}\left[\boldsymbol{W}_{\mathrm{a}},\boldsymbol{v}_{\mathrm{a}}\right]\right\|_{\mathrm{F}}^2+\sum_{j=1,j\neq k}^{K}\left\|\Pi_{\boldsymbol{S}_k}^{\perp}\boldsymbol{H}_{kj}\boldsymbol{V}_j\right\|_{\mathrm{F}}^2\right)\\&\text{s.t.}\quad\boldsymbol{W}_{\mathrm{a}}^{\mathrm{H}}\boldsymbol{W}_{\mathrm{a}}=\mathbf{I}_{d_{\mathrm{an}}},\ \boldsymbol{V}_k^{\mathrm{H}}\boldsymbol{V}_k=\mathbf{I}_{d_k},\ \boldsymbol{S}_k^{\mathrm{H}}\boldsymbol{S}_k=\mathbf{I}_{N_k-d_k},\ k\in\mathcal{K}\end{aligned} \tag{10}$$

其中，$\boldsymbol{S}_k\in\mathbb{C}^{N_k\times(N_k-d_k)}$ 表示接收机 k 干扰子空间中的一组正交基。此外，$\boldsymbol{S}_k$ 的列空间表示为 $\mathrm{span}(\boldsymbol{S}_k)=\mathrm{span}\left(\boldsymbol{H}_{k\mathrm{a}}\left[\boldsymbol{W}_{\mathrm{a}},\boldsymbol{v}_{\mathrm{a}}\right],\left\{\boldsymbol{H}_{kj}\boldsymbol{V}_j\right\}_{j=1,j\neq k}^{K}\right)$，$\Pi_{\boldsymbol{S}_k}^{\perp}=\mathbf{I}-\boldsymbol{S}_k\boldsymbol{S}_k^{\mathrm{H}}$ 表示 $\mathrm{span}(\boldsymbol{S}_k)$ 的正交补空间的投影矩阵。当 $\boldsymbol{S}_k$ 给定时，式(7)中的 $\boldsymbol{U}_k$ 可以通过求解 $\mathrm{null}(\boldsymbol{S}_k)$ 的一组正交基得到。值得注意的是，优化问题 P1 的目标函数也可以理解为合法接收机的总干扰泄漏。

为了在接收机处消除干扰同时避免消除有用信号，本文将介绍一种改进干扰对齐算法来求解优化问题 P1，具体步骤如下。

步骤 1　初始化预编码矩阵 $\boldsymbol{V}_k$ 和 $\boldsymbol{W}_{\mathrm{a}}$ 分别满足 $\boldsymbol{V}_k^{\mathrm{H}}\boldsymbol{V}_k=\mathbf{I}$ 和 $\boldsymbol{W}_{\mathrm{a}}^{\mathrm{H}}\boldsymbol{W}_{\mathrm{a}}=\mathbf{I}$。此外，为了避免有用信号消除，选取主信道 $\boldsymbol{H}_{\mathrm{ba}}$ 最大奇异值对应的左（右）奇异向量分别作为 Alice 和 Bob 的波束成形向量 $\boldsymbol{u}_{\mathrm{b}}$（$\boldsymbol{v}_{\mathrm{a}}$）。

步骤 2　为了使接收端能够估计出干扰协方差矩阵，通过发射机之间的协作，固定 Alice 和 K 个发射机每个波束的功率相同，记为 P_{c}，即 $P_{\mathrm{c}}=P_k/d_k$、$P_{\mathrm{a}}=\left(d_{\mathrm{an}}+1\right)P_{\mathrm{c}}$。

步骤 3　接收机 k 处的干扰协方差矩阵为

$$\begin{aligned}\boldsymbol{Q}_k=&\sum_{j=1,j\neq k}^{K}P_{\mathrm{c}}\boldsymbol{H}_{kj}\boldsymbol{V}_j\boldsymbol{V}_j^{\mathrm{H}}\boldsymbol{H}_{kj}^{\mathrm{H}}+\\&P_{\mathrm{c}}\boldsymbol{H}_{k\mathrm{a}}\left(\boldsymbol{v}_{\mathrm{a}}\boldsymbol{v}_{\mathrm{a}}^{\mathrm{H}}+\boldsymbol{W}_{\mathrm{a}}\boldsymbol{W}_{\mathrm{a}}^{\mathrm{H}}\right)\boldsymbol{H}_{k\mathrm{a}}^{\mathrm{H}}\end{aligned} \tag{11}$$

令矩阵 $\boldsymbol{S}_k$ 的列为 $\boldsymbol{Q}_k$ 的 $\left(N_k-d_k\right)$ 个主特征向量，$\Pi_{\boldsymbol{S}_k}^{\perp}=\boldsymbol{I}-\boldsymbol{S}_k\boldsymbol{S}_k^{\mathrm{H}}$。

步骤 4　令 $\boldsymbol{V}_k$ 的列向量为 $\boldsymbol{H}_{\mathrm{b}k}^{\mathrm{H}}\boldsymbol{u}_{\mathrm{b}}\boldsymbol{u}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{b}k}+\sum_{j=1,j\neq k}^{K}\boldsymbol{H}_{jk}^{\mathrm{H}}\Pi_{\boldsymbol{S}_j}^{\perp}\boldsymbol{H}_{jk}$ 的前 d_k 个最小特征向量，同时令 $\boldsymbol{W}_{\mathrm{a}}$ 的列向量为 $\boldsymbol{H}_{\mathrm{ba}}^{\mathrm{H}}\boldsymbol{u}_{\mathrm{b}}\boldsymbol{u}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ba}}+\sum_{k=1}^{K}\boldsymbol{H}_{k\mathrm{a}}^{\mathrm{H}}\Pi_{\boldsymbol{S}_k}^{\perp}\boldsymbol{H}_{k\mathrm{a}}$ 的前 d_{an} 个最小特征向量。

步骤 5　重复步骤 3、步骤 4 直至收敛。

步骤 6　令 $\boldsymbol{U}_k$ 的列为 $\mathrm{null}(\boldsymbol{S}_k)$ 中一组基向量。

所提改进干扰对齐算法为分布式算法。每个接

收端估计干扰协方差矩阵 $\boldsymbol{Q}_k$ 并更新 $\boldsymbol{S}_k$。接着根据 $\boldsymbol{S}_k$ 计算 $\boldsymbol{V}_k$ 和 $\boldsymbol{W}_{\mathrm{a}}$。设 $S=\max\limits_{1\leqslant k\leqslant K}\max(M_k,N_k)$，$T=\max(M_{\mathrm{a}},N_{\mathrm{b}})$，$q$ 表示接收信号的观测值个数。由此，每次迭代的计算复杂度可以表示为 $O(S^3K+S^2Kq+S^2KT+SKT^2+T^3)$。

3.3 可行性分析

人工噪声辅助下的干扰对齐问题的可行性取决于式(6)、式(7)是否有解。当干扰对齐问题可解时，一定是适当的，而当干扰对齐问题是非适当的时，一定不可解。为了避免检验方程中的所有子集复杂度高的问题，本文将从方程子集的角度对人工噪声辅助下干扰对齐问题的可行性进行分析。

首先，将式(6)、式(7)转化为以下 3 类子问题：

$$\left[\boldsymbol{H}_{\mathrm{b}k}^{\mathrm{H}}\boldsymbol{u}_{\mathrm{b}},\left\{\boldsymbol{H}_{jk}^{\mathrm{H}}\boldsymbol{U}_j\right\}_{j=1,j\neq k}^{K}\right]^{\mathrm{H}}\boldsymbol{V}_k=0,\quad k\in\mathcal{K} \tag{12}$$

$$\left[\left\{\boldsymbol{H}_{k\mathrm{a}}^{\mathrm{H}}\boldsymbol{U}_k\right\}_{k=1}^{K}\right]^{\mathrm{H}}\boldsymbol{v}_{\mathrm{a}}=0 \tag{13}$$

$$\left[\boldsymbol{H}_{\mathrm{ba}}^{\mathrm{H}}\boldsymbol{u}_{\mathrm{b}},\left\{\boldsymbol{H}_{k\mathrm{a}}^{\mathrm{H}}\boldsymbol{U}_k\right\}_{k=1}^{K}\right]^{\mathrm{H}}\boldsymbol{W}_{\mathrm{a}}=0 \tag{14}$$

式(12)～式(14)共有 $2^3-1=7$ 个方程子集，对应 7 个方程和变量之间的关系。这些关系可以总结为以下不等式

$$r_{\mathrm{U}}+r_{\mathrm{V}}\geqslant 2s_{\mathrm{a}}+s_{\mathrm{b}} \tag{15}$$

$$r_{\mathrm{V}}+r_{\mathrm{W}}\geqslant d_{\mathrm{an}}+(d_{\mathrm{an}}+1)s_{\mathrm{a}} \tag{16}$$

$$r_{\mathrm{U}}+r_{\mathrm{V}}+r_{\mathrm{W}}\geqslant d_{\mathrm{an}}+(d_{\mathrm{an}}+2)s_{\mathrm{a}}+s_{\mathrm{b}} \tag{17}$$

其中，$r_{\mathrm{U}}=\sum\limits_{k=1}^{K}d_k(N_k-d_k)$, $r_{\mathrm{V}}=\sum\limits_{k=1}^{K}d_k(M_k-d_k)$, $r_{\mathrm{W}}=(M_{\mathrm{a}}-d_{\mathrm{an}})d_{\mathrm{an}}$, $s_{\mathrm{a}}=\sum\limits_{k=1}^{K}d_k$, $s_{\mathrm{b}}=\sum\limits_{k=1}^{K}\sum\limits_{j\neq k}^{K}d_kd_j$。

定理 1 若人工噪声辅助下的干扰对齐问题有解，需要同时满足式(15)～式(17)。

讨论 2 定理 1 中给出的必要条件比文献[26-28]中比较总变量数和总方程数之间的关系所给出的条件更加严格。定理 1 的意义在于，如果不满足上述条件，那么认为干扰对齐问题是不可行的。

4 SOP 约束下的 SRM 问题

4.1 问题描述

本文假设能够干扰对齐，理论上所有接收机处的人工噪声和干扰可以被完全消除。那么，在 Bob 和 Eve$l$，$l\in\mathcal{L}$ 处的信干噪比（SINR, signal to interference plus noise ratio）可以分别表示为

$$\gamma_{\mathrm{b}}(\phi)=P_{\mathrm{a}}\phi\left|\boldsymbol{u}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ba}}\boldsymbol{v}_{\mathrm{a}}\right|^2 \tag{18}$$

$$\gamma_{\mathrm{e}_l}(\phi)=\frac{P_{\mathrm{a}}\phi\left|\boldsymbol{h}_{\mathrm{e}_l,\mathrm{a}}^{\mathrm{H}}\boldsymbol{v}_{\mathrm{a}}\right|^2}{1+\sum\limits_{k=1}^{K}\frac{P_k}{d_k}\left\|\boldsymbol{h}_{\mathrm{e}_l,k}^{\mathrm{H}}\boldsymbol{V}_k\right\|^2+\frac{P_{\mathrm{a}}(1-\phi)}{d_{\mathrm{an}}}\left\|\boldsymbol{h}_{\mathrm{e}_l,\mathrm{a}}^{\mathrm{H}}\boldsymbol{W}_{\mathrm{a}}\right\|^2} \tag{19}$$

根据文献[32]中的安全编码理论，为了防止信息被窃听，保密信息经过安全编码之后进行传输。因此，Alice 需要确定两个速率，即码字传输速率 R_{b} 和保密信息的传输速率 R_{s}（也称安全速率）。定义主信道的信道容量为 $C_{\mathrm{b}}=\mathrm{lb}(1+\gamma_{\mathrm{b}})$，为了保证保密消息的可靠传输，需要满足 $R_{\mathrm{b}}\leqslant C_{\mathrm{b}}$。由于主信道的 CSI 已知，码字传输速率可以达到信道容量，即 $R_{\mathrm{b}}=C_{\mathrm{b}}$。

此外，在信息传输时需要增加速率冗余来提供安全性，规避恶意窃听。定义冗余信息速率为 $R_{\mathrm{e}}\triangleq R_{\mathrm{b}}-R_{\mathrm{s}}$，其中 $R_{\mathrm{e}}\geqslant 0$。当存在多个独立窃听节点的情况下，只要有一个窃听节点的信道容量大于 R_{e}，则会发生安全中断。令 C_{e_l} 表示 Eve$l$ 的信道容量，相应的安全中断概率可以表示为

$$\begin{aligned}p_{\mathrm{out}}&=\Pr\left\{\max_{1\leqslant l\leqslant L}C_{\mathrm{e}_l}>R_{\mathrm{e}}\right\}=\\&\Pr\left\{\max_{1\leqslant l\leqslant L}\mathrm{lb}\left(1+\gamma_{\mathrm{e}_l}(\phi)\right)>R_{\mathrm{b}}-R_{\mathrm{s}}\right\}=\\&\Pr\left\{\max_{1\leqslant l\leqslant L}\gamma_{\mathrm{e}_l}(\phi)>2^{R_{\mathrm{b}}-R_{\mathrm{s}}}-1\right\}\end{aligned} \tag{20}$$

令 $\varepsilon_{\mathrm{th}}$ 表示最大可允许的安全中断概率，安全中断概率约束下的 SRM 问题可以表示为

$$\begin{aligned}&\max_{\phi}\quad R_{\mathrm{s}}\\&\text{s.t. }\ p_{\mathrm{out}}\leqslant\varepsilon_{\mathrm{th}};\ \ 0<\phi\leqslant 1\end{aligned} \tag{21}$$

由于 p_{out} 是 R_{s} 的单调递增函数。为了得到最大的安全速率，式(21)中的安全中断概率约束条件可以等价为

$$\varepsilon_{\mathrm{th}}=\Pr\left\{\max_{1\leqslant l\leqslant L}\gamma_{\mathrm{e}_l}(\phi)>2^{R_{\mathrm{b}}-R_{\mathrm{s}}}-1\right\} \tag{22}$$

根据以上分析，将式(21)重新描述为

$$\begin{aligned}&\max_{\phi}\quad R_{\mathrm{s}}\\&\text{s.t. 式(22)};\ \ 0<\phi\leqslant 1\end{aligned} \tag{23}$$

4.2 安全中断概率闭式表达式

受限于式(22)中安全中断概率的约束条件，SRM 问题难以直接求解。为了更好地分析中断约束条件，基于式(19)中 Eve$l$ 的 SINR 定义的辅助变量为

$$X_l=P_{\mathrm{a}}\phi\left|\boldsymbol{h}_{\mathrm{e}_l,\mathrm{a}}^{\mathrm{H}}\boldsymbol{v}_{\mathrm{a}}\right|^2,\quad Y_l=\sum_{k=1}^{K}\frac{P_k}{d_k}\left\|\boldsymbol{h}_{\mathrm{e}_l,k}^{\mathrm{H}}\boldsymbol{V}_k\right\|^2 \tag{24}$$

$$Z_l=\frac{P_{\mathrm{a}}(1-\phi)}{d_{\mathrm{an}}}\left\|\boldsymbol{h}_{\mathrm{e}_l,\mathrm{a}}^{\mathrm{H}}\boldsymbol{W}_{\mathrm{a}}\right\|^2,\ T_l=Y_l+Z_l \tag{25}$$

此外，为了简化分析，本文假设 Alice 以外其他发射机的发射功率和数据流个数均相同，即 $d_k=d$，$P_k=P$，$k\in\mathcal{K}$。根据本文对窃听信道的假设，即 $\boldsymbol{h}_{\mathrm{e}_l,\mathrm{a}}\sim\mathrm{CN}(0,\Gamma_{\mathrm{E}}\mathbf{I})$，$\boldsymbol{h}_{\mathrm{e}_l,k}\sim\mathrm{CN}(0,\mathbf{I})$，可以得到随机变量 X_l，Y_l 和 Z_l 的概率分布为

$$X_l\sim\mathrm{Exp}(\lambda),\ Y_l\sim\Gamma(\alpha_1,\lambda_1),\ Z_l\sim\Gamma(\alpha_2,\lambda_2) \tag{26}$$

其中，$\lambda=1/(P_{\mathrm{a}}\Gamma_{\mathrm{E}}\phi)$, $\lambda_1=d/P$, $\lambda_2=d_{\mathrm{an}}/\left(P_{\mathrm{a}}\Gamma_{\mathrm{E}}(1-\phi)\right)$, $\alpha_1=dK$, $\alpha_2=d_{\mathrm{an}}$。因此，式(19)中 Eve l 的 SINR 可以表示为

$$\gamma_{\mathrm{e}_l}(\phi)=\frac{X_l}{Y_l+Z_l+1}=\frac{X_l}{T_l+1},\ l\in\mathcal{L} \tag{27}$$

由式(27)可得，$\gamma_{\mathrm{e}_l}(\phi)$ 是关于 X_l、Y_l 和 Z_l 的函数。因此，可以将式(22)重新表示为

$$\begin{aligned}\varepsilon_{\mathrm{th}}&=1-\Pr\left\{\max_{1\leqslant l\leqslant L}\frac{X_l}{T_l+1}\leqslant 2^{R_{\mathrm{b}}-R_{\mathrm{s}}}-1\right\}=\\&1-\prod_{1\leqslant l\leqslant L}\Pr\left\{\frac{X_l}{T_l+1}\leqslant 2^{R_{\mathrm{b}}-R_{\mathrm{s}}}-1\right\}=\\&1-\left(\Pr\left(\frac{X_l}{T_l+1}\leqslant\mu\right)\right)^L\end{aligned} \tag{28}$$

其中，$\mu=2^{R_{\mathrm{b}}-R_{\mathrm{s}}}-1$。

命题 1　根据文献[11]的命题 1 中对 $\gamma_{\mathrm{e}_l}(\phi)$ 的互补累计分布函数的推导，式(28)可以重新表示为

$$\varepsilon_{\mathrm{th}}=1-\left[1-\frac{1}{e^{\lambda\mu}}\left(\frac{\lambda_1}{\lambda_1+\lambda\mu}\right)^{\alpha_1}\left(\frac{\lambda_2}{\lambda_2+\lambda\mu}\right)^{\alpha_2}\right]^L \tag{29}$$

4.3　SRM 问题求解

本节进一步将原始的 SRM 问题转换为易于求解的功率分配优化问题。将式(26)中的变量代入式(29)可以得到

$$\begin{aligned}\ln\left[\frac{1}{1-(1-\varepsilon_{\mathrm{th}})^{\frac{1}{L}}}\right]=&\frac{\omega}{P_{\mathrm{a}}\Gamma_{\mathrm{E}}}+\alpha_1\ln\left(1+\frac{\omega}{\lambda_1P_{\mathrm{a}}\Gamma_{\mathrm{E}}}\right)+\\&\alpha_2\ln\left(1+\frac{1-\phi}{\alpha_2}\omega\right)\end{aligned} \tag{30}$$

其中，$\omega=\mu/\phi$。

为了简化分析，令 $\gamma_{\mathrm{B}}\triangleq P_{\mathrm{a}}\left|\boldsymbol{u}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ba}}\boldsymbol{v}_{\mathrm{a}}\right|^2$ 代表满功率情况下保密信号的信噪比。由此，安全速率 R_{s} 可以表示为

$$R_{\mathrm{s}}=R_{\mathrm{b}}-\mathrm{lb}(1+\mu)=\mathrm{lb}\left(\frac{1+\phi\gamma_{\mathrm{B}}}{1+\phi\omega}\right) \tag{31}$$

需要注意的是，安全速率 R_{s} 的大小取决于参数 ω 和 ϕ。根据式(30)，ω 可以看作 ϕ 的函数，记为 $\omega(\phi)$。因此，式(23)可以重新描述为

$$\begin{aligned}&\max_{\phi}\ \ R_{\mathrm{s}}(\phi)=\mathrm{lb}\left(\frac{1+\phi\gamma_{\mathrm{B}}}{1+\phi\omega(\phi)}\right)\\&\text{s.t. 式(30);}\ \ 0<\phi\leqslant 1\end{aligned} \tag{32}$$

经过化简和变量替换，将难以直接求解的概率约束转化为了确定约束。下面将分析式(32)的目标函数与约束条件，并设计有效的数值方法求解 SRM 问题。

引理 1　函数 $\omega(\phi)$ 是关于 ϕ 的严格单调递增函数

证明　首先，对式(30)中的 ϕ 求导可得

$$\omega'(\phi)=\frac{P_{\mathrm{a}}\Gamma_{\mathrm{E}}\alpha_2\omega(\phi)\left[P\omega(\phi)+P_{\mathrm{a}}\Gamma_{\mathrm{E}}d\right]}{\left[\alpha_2+\omega(\phi)(1-\phi)+P_{\mathrm{a}}\Gamma_{\mathrm{E}}\alpha_2(1-\phi)\right]\left[P\omega(\phi)+P_{\mathrm{a}}\Gamma_{\mathrm{E}}d\right]+P_{\mathrm{a}}\Gamma_{\mathrm{E}}P\alpha_1\left[\alpha_2+(1-\phi)\omega(\phi)\right]} \tag{33}$$

由于 $\mu=2^{R_{\mathrm{b}}-R_{\mathrm{s}}}-1>0$, $\phi>0$，可得 $\omega(\phi)=\mu/\phi>0$。此外，式(33)中 $\alpha_2+(1-\phi)\omega(\phi)>0$，$P\omega(\phi)+P_{\mathrm{a}}\Gamma_{\mathrm{E}}d>0$，因此有 $\omega'(\phi)>0$。引理 1 得证。

引理 2　函数 $h(\phi)=\omega'(\phi)/\omega(\phi)$ 是关于 ϕ 的严格单调递增函数

证明　根据式(33)，函数 $h(\phi)$ 可以表示为

$$h(\phi)=\frac{P_{\mathrm{a}}\Gamma_{\mathrm{E}}\alpha_2}{\alpha_2+(1-\phi)\left[P_{\mathrm{a}}\Gamma_{\mathrm{E}}\alpha_2+\omega(\phi)\right]+P_{\mathrm{a}}\Gamma_{\mathrm{E}}P\alpha_1\dfrac{\alpha_2+(1-\phi)\omega(\phi)}{P\omega(\phi)+P_{\mathrm{a}}\Gamma_{\mathrm{E}}d}} \tag{34}$$

根据引理 1 可知，式(30)中等式右边的第一项和第二项都随 ϕ 单调递增，而等式左边不随 ϕ 变化。若式(30)成立，则 $\ln\left(1+\omega(\phi)(1-\phi)/\alpha_2\right)$ 必然随 ϕ 的增加而减少，因此函数 $\omega(\phi)(1-\phi)$ 是关于 ϕ 的严格单调递减函数。进一步，可以推导出式(34)中的分母是 ϕ 的严格单调递减函数，所以 $h(\phi)$ 是单调递增函数，至此引理 2 得证。

命题 2　SRM 问题式(32)中目标函数是关于 ϕ

的严格凹函数

证明 根据式(31)， $R_{\mathrm{s}}'(\phi)$ 为

$$R_{\mathrm{s}}'(\phi)=\frac{\gamma_{\mathrm{B}}-\omega(\phi)}{(1+\phi\gamma_{\mathrm{B}})[1+\phi\omega(\phi)]\ln 2}-\frac{h(\phi)}{\left[\frac{1}{\phi\omega(\phi)}+1\right]\ln 2} \tag{35}$$

根据引理 1 和引理 2，式(35)的右边第一项和第二项分别为关于 ϕ 的严格单调递减函数和严格单调递增函数，因此 $R_{\mathrm{s}}'(\phi)$ 是关于 ϕ 的严格单调递减函数，即 $R_{\mathrm{s}}''(\phi)<0$。根据文献[33]的二阶判定条件，命题 2 得证。

1) $R_{\mathrm{s}}'(1)\geqslant 0$

根据命题 2 可知，当 $R_{\mathrm{s}}'(1)\geqslant 0$ 时，函数 $R_{\mathrm{s}}(\phi)$ 随单调递增，因此最优解 $\phi^*=1$。这表明无人工噪声保密波束成形是最优策略。

2) $R_{\mathrm{s}}'(0^+)\leqslant 0$

根据命题 2 可知，当 $R_{\mathrm{s}}'(0^+)\leqslant 0$ 时，函数 $R_{\mathrm{s}}(\phi)$ 随 ϕ 单调递减，因此最优解 $\phi^*=0$。因此，对应的安全速率为 $R_{\mathrm{s}}(\phi^*)=0$，在这种情况下 Alice 应当停止安全传输。

3) $R_{\mathrm{s}}'(1)<0$ 并且 $R_{\mathrm{s}}'(0^+)>0$

根据命题 2 可知，函数 $R_{\mathrm{s}}(\phi)$ 是关于 ϕ 的严格凹函数，那么一定存在唯一的最优解 $\phi^*\in(0,1)$，对应的速率为 $R_{\mathrm{s}}(\phi^*)$。此外，当 $\phi\in(0,\phi^*)$ 时，可得 $R_{\mathrm{s}}(\phi^*)>R_{\mathrm{s}}(0^+)=0$，即安全速率大于零。接下来，最优功率分配比例求解算法见算法 1。

算法 1 最优功率分配比例求解算法

输入 发射功率 P_{a} 和 P，$\boldsymbol{h}_{\mathrm{e}_l,\mathrm{a}}$ 的统计信道状态信息，$\boldsymbol{H}_{\mathrm{ba}}$ 的准确信道状态信息，安全中断概率阈值 $\varepsilon_{\mathrm{th}}$，窃听信道增益 Γ_{E}，除 Alice 以外发射机的数据流个数 d，人工噪声信号的维度 d_{an}，窃听节点的个数 L

输出 最优功率分配比例 ϕ^* 和对应的最大安全速率 $R_{\mathrm{s}}(\phi^*)$

根据式(30)求解 $\omega(1)$ 和 $\omega(0)$

根据式(35)计算 $R_{\mathrm{s}}'(1)$ 和 $R_{\mathrm{s}}'(0^+)$

if $R_{\mathrm{s}}'(1)\geqslant 0$，then 函数 $R_{\mathrm{s}}(\phi)$ 是关于 ϕ 的严格单调递增函数

Obtain $\phi^*=1$

else if $R_{\mathrm{s}}'(0^+)\leqslant 0$，then 函数 $R_{\mathrm{s}}(\phi)$ 是关于 ϕ 的严格单调递减函数

Obtain $\phi^*=0$

else 函数 $R_{\mathrm{s}}(\phi)$ 在 $(0,1)$ 上有唯一的最优解

通过联立求解方程 $R_{\mathrm{s}}'(\phi^*)=0$ 和式(30)得到 ϕ^*

end if

计算 $R_{\mathrm{s}}(\phi^*)$

讨论 3 对于算法 1 的第 1 种情况，即 $R_{\mathrm{s}}'(1)\geqslant 0$，利用引理 1 可得安全速率大于零。首先，根据式(35)，在 $\phi=1$ 的情况下有

$$R_{\mathrm{s}}'(1)=\left(\frac{\gamma_{\mathrm{B}}}{1+\gamma_{\mathrm{B}}}-\frac{\omega(1)+\omega'(1)}{1+\omega(1)}\right)\frac{1}{\ln 2}\geqslant 0\Leftrightarrow\gamma_{\mathrm{B}}-\omega(1)\geqslant(1+\gamma_{\mathrm{B}})\omega'(1) \tag{36}$$

进一步根据引理 1 可得 $(1+\gamma_{\mathrm{B}})\omega'(1)>0$。因此，$\gamma_{\mathrm{B}}>\omega(1)$ 成立，根据式(31)可以保证可实现的安全速率大于零。

讨论 4 对于第 2 种情况，即 $R_{\mathrm{s}}'(0^+)\leqslant 0$，利用引理 1 可得安全速率等于零。首先，根据式(35)可得

$$\left(\gamma_{\mathrm{B}}-\omega(0^+)\right)\Big/\ln(2)\leqslant 0\Leftrightarrow\gamma_{\mathrm{B}}\leqslant\omega(0^+) \tag{37}$$

根据引理 1，可得对于 $\forall\phi\in(0,1)$，$\gamma_{\mathrm{B}}\leqslant\omega(\phi)$ 成立。根据式(31)可知，Alice 暂停安全传输是最佳策略。

讨论 5 对于第 3 种情况，即 $R_{\mathrm{s}}'(1)<0$ 并且 $R_{\mathrm{s}}'(0^+)>0$。在这种情况下，若要得到最优功率分配比例，需要联立求解 $R_{\mathrm{s}}'(\phi)$=0 和式(30)。由于 $\omega(\phi)$ 是关于 ϕ 的隐函数，因此需要同时求解两个未知变量 ω 和 ϕ，而在高信噪比条件下可以直接得出 ϕ^* 的显示表达式。当 Alice 的发射功率 P_{a} 足够大时，ϕ^* 可以近似为

$$\phi^*\approx\frac{1}{1+\sqrt{\dfrac{\alpha_2}{\left[1-(1-\varepsilon_{\mathrm{th}})^{\frac{1}{L}}\right]^{\frac{1}{\alpha_2}}}-\alpha_2}} \tag{38}$$

证明 当 Alice 的发射功率 P_{a} 足够大时，对应的 $\gamma_{\mathrm{B}}\triangleq P_{\mathrm{a}}\left|\boldsymbol{u}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ba}}\boldsymbol{v}_{\mathrm{a}}\right|^2$ 满足 $\gamma_B>\omega(0^+)$。进一步根据式(35)可得 $R_{\mathrm{s}}'(0^+)>0$，在此条件下可实现的安全速率大于零，同时 $\phi^*>0$。此外，在 $P_{\mathrm{a}}\to\infty$ 的情况下有 $P_{\mathrm{a}}\Gamma_{\mathrm{E}}\to\infty$，因此安全中断概率的约束条件式(30)可以近似为

$$\ln\left(\frac{1}{1-(1-\varepsilon_{\mathrm{th}})^{\frac{1}{L}}}\right)=\alpha_2\ln\left(1+\frac{1-\phi}{\alpha_2}\omega(\phi)\right) \tag{39}$$

对式(39)中的 $\omega(\phi)$ 求导可以得到

$$\omega'(\phi)=\frac{\alpha_2}{(1-\phi)^2}\left(\left[1-(1-\varepsilon_{\text{th}})^{\frac{1}{L}}\right]^{-\frac{1}{\alpha_2}}-1\right) \tag{40}$$

此外，当 P_{a} 足够大时，式(35)可以近似为

$$R_{\text{s}}'(\phi)=\left(\frac{1}{\phi}-\frac{\omega(\phi)+\phi\omega'(\phi)}{1+\phi\omega(\phi)}\right)\frac{1}{\ln 2}=\frac{1-\phi^2\omega'(\phi)}{\phi\left[1+\phi\omega(\phi)\right]\ln 2} \tag{41}$$

根据式(40)可得，随着 $\phi\to 1$，$\omega'(\phi)\to\infty$。进一步，由式(41)可知 $R_{\text{s}}'(1)<0$ 成立，在该条件下 $\phi^*<1$。最后，将式(40)代入式(41)可得

$$R_{\text{s}}'(\phi)=\frac{1-\left(\frac{\phi}{1-\phi}\right)^2\left(\alpha_2\left[1-(1-\varepsilon_{\text{th}})^{\frac{1}{L}}\right]^{-\frac{1}{\alpha_2}}-\alpha_2\right)}{\phi\left[1+\phi\omega(\phi)\right]\ln 2} \tag{42}$$

通过求解 $R_{\text{s}}'(\phi)=0$ 可得，ϕ^* 在高信噪比情况下的近似解为式(38)，证毕。

讨论 6　当除 Alice 外其他发射机的发射功率增大时，会对窃听节点产生更多的干扰。此时，Alice 能够分配给保密信息更多的功率，以提高安全速率。下面将分析 P_{a} 远小于 P 时，最优功率分配比例为 $\phi^*=1$。

首先，根据式(35)，$R_{\text{s}}'(1)\geqslant 0$ 等价为

$$\gamma_{\text{B}}>\omega(1)+\omega'(1)+\gamma_{\text{B}}\omega'(1) \tag{43}$$

当 P/P_{a} 足够大时，式(30)可以近似为

$$\omega(1)=\Gamma_{\text{E}}d\left(\left[1-(1-\varepsilon_{\text{th}})1/L\right]^{-1/\alpha_1}-1\right)P_{\text{a}}/P \tag{44}$$

由于式(44)中其他项均为常数，在 P_{a} 不变的前提条件下，当 P 增大时，$\omega(1)$ 减小。定义 $\tau=\Gamma_{\text{E}}d\left(\left[1-(1-\varepsilon_{\text{th}})^{1/L}\right]^{-1/\alpha_1}-1\right)$，$\omega(1)=\tau P_{\text{a}}/P$。需要指出，$\tau$ 为非零的常数。此外，将 $\phi=1$ 代入式(33)可得

$$\omega'(1)=\frac{P_{\text{a}}\Gamma_{\text{E}}\alpha_2\omega(1)\left[P\omega(1)+P_{\text{a}}\Gamma_{\text{E}}d\right]}{\alpha_2\left[P\omega(1)+P_{\text{a}}\Gamma_{\text{E}}d\right]+P_{\text{a}}\Gamma_{\text{E}}P\alpha_1\alpha_2}=\frac{P_{\text{a}}^2\left(\tau^2+\Gamma_{\text{E}}d\tau\right)}{P\left(P\alpha_1+\Gamma_{\text{E}}d+\frac{\tau}{\Gamma_{\text{E}}}\right)} \tag{45}$$

根据式(45)可以看出，当 P 增大时，$\omega'(1)$ 减小。特别地，当 $P/P_{\text{a}}\to\infty$ 时，可得 $\omega(1)\to 0$ 与 $\omega'(1)\to 0$。因此，可以判断当 P_{a} 远小于 P 时，$R_{\text{s}}'(1)\geqslant 0$。最优的功率分配比例为 $\phi^*=1$。

5　仿真结果和实验分析

本节通过数字仿真验证所提改进干扰对齐算法的性能，以安全速率为衡量指标，对应的单位为比特/信道利用（bpcu, bits per channel use）。若无特殊说明，本文的仿真参数设置如下：除 Alice 外其他发射机的个数 $K=3$，安全中断概率阈值 $\varepsilon_{\text{th}}=0.1$，窃听信道增益 $\Gamma_{\text{E}}=1$，发射机的发射天线数 $M_1=M_2=M_3=16$，接收机的接收天线数 $N_1=N_2=N_3=8$，Alice 发射的人工噪声向量的维度 $d_{\text{an}}=5$，其他发射机发射的数据流的个数 $d_1=d_2=d_3=5$。

系统总干扰泄漏和 SINR 随迭代次数的变化如图 2 所示。可以看出，随着迭代次数的增加，传统基于 AM 或 ILM 的干扰对齐算法和所提改进干扰对齐算法均能够对齐干扰。此外，传统 AM 或 ILM 算法随着干扰泄漏收敛，SINR 会趋于零，这是由于传统 AM 或 ILM 算法存在可能将信号和干扰一同消除的问题。而改进干扰对齐算法由于采用最大特征模的方式传输保密信号，SINR 可以稳定在较高的值，因此可以避免上述情况发生。

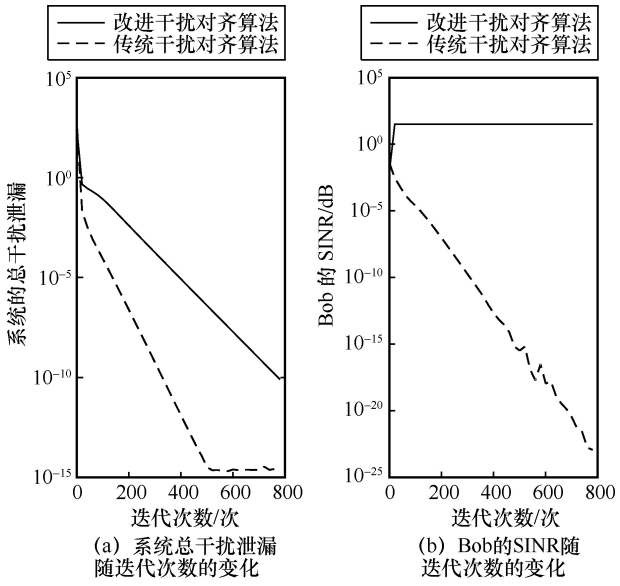

图 2　系统总干扰泄漏和 SINR 随迭代次数的变化

不同系统配置下的干扰对齐情况如图 3 所示，可以看出，随着窃听节点个数增加或者 P_{a} 变大，保密信息泄露的概率也会随之增大，因此 Alice 需要分配更多功率以干扰窃听者。此外，其他发射机的功率 P 增大，也可以对窃听节点造成干扰，因此最优的功率分配比例提高。另外，如讨论 5 所述，在高信噪比的情况下，当窃听节点个数 L、安全中断概率阈值 ε_{th} 等参数给定时，最优的功率分配比例收敛到定值。仿真结果验证了式(38)中对于 ϕ^* 近似的准确性。

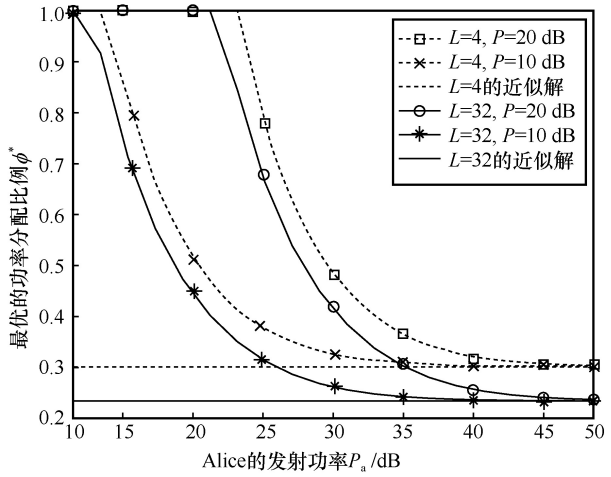

图 3　不同系统配置下的干扰对齐情况

$P=5$ dB、$L=4$ 时，不同方案的安全速率及最优功率分配比例比较如图 4 所示。当 Alice 的发射功率 P_a 增加时，安全速率也随之增大，并且忽略窃听节点噪声的安全速率与所提改进干扰对齐算法的差距随着 P_a 的增加而减少。而不发射人工噪声时则相反，这说明了人工噪声对窃听节点的干扰作用。此外，当 P_a 相对较小时，$\phi^*=1$，说明其他发射机的信号可以有效干扰窃听，因此 Alice 可以将全部功率用于波束成形。

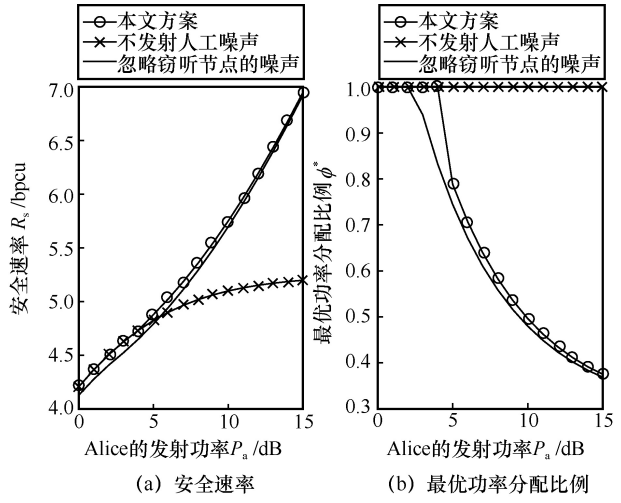

图 4　$P=5$ dB、$L=4$ 时，不同方案的安全速率及最优功率分配比例比较

P_a=20 dB 时，安全速率和最优功率分配比例随窃听节点个数 L 的变化情况如图 5 所示。可以看出，随着 Eve 数量的增加，安全速率和最优功率分配比例都会下降。此外，可以看出系统中协作发射机对于提高系统的安全性能有着积极的影响。当 Alice 的发射功率固定时，协作发射机的发射功率越大，对窃听节点产生的干扰也会越强，更多的功率可以分配给机密信号，因此对应的安全速率也就越高。此外，窃听信道增益 Γ_E 刻画了窃听节点的信道质量。当 Γ_E 增大时，需要分配更多功率给人工噪声以干扰窃听，因此可实现安全速率下降。

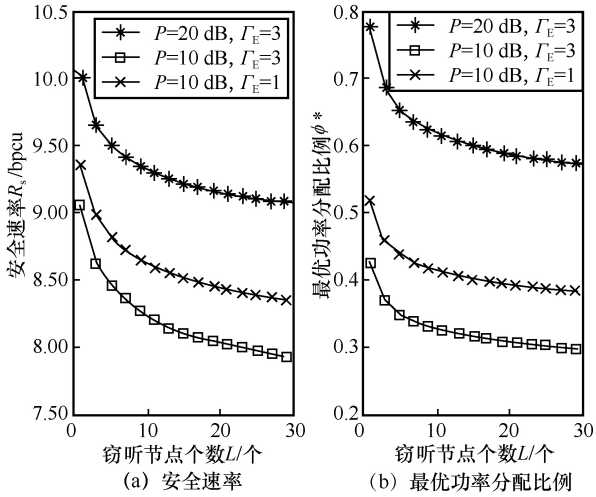

图 5　P_a=20 dB 时，安全速率和最优功率分配比例随窃听节点个数 L 的变化情况

P 对安全速率和最优功率分配比例的影响如图 6 所示，其中 $L=0$ 表示系统中没有窃听节点。可以看出，当 Alice 的发射功率增大时，安全速率增大，同时窃听节点接收到的信号也更强。为了干扰窃听，人工噪声信号的功率占比相应增加。而当 Alice 的发射功率 P_a 固定时，随着其他发射机的功率增加，窃听节点受到的干扰增强，因此安全速率增大，同时 Alice 能够分配更多功率给保密信号。特别地，如果 P 继续增大，Alice 无须发射人工噪声信号就可以实现安全传输，对应的 ϕ^* 等于 1，这与讨论 6 一致。

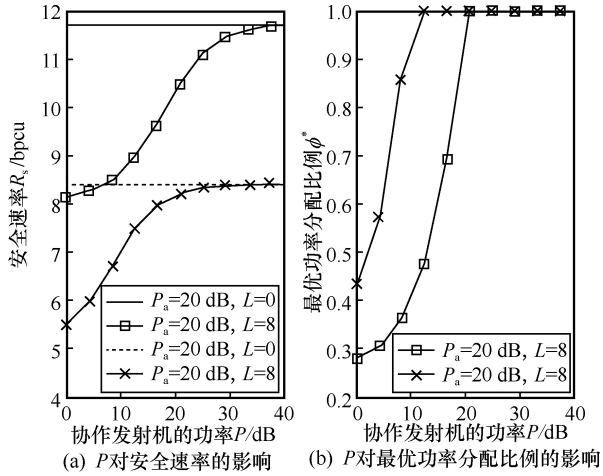

图 6　P 对安全速率和最优功率分配比例的影响

6　结束语

本文重点研究了多用户干扰信道与多个窃听者共存时的防窃听设计，其中多用户干扰是通信安全不可忽视的因素。联合利用人工噪声和固有的多用户干扰来增强安全性，设计了一种人工噪声辅助的干扰对齐算法。在该算法中，Alice 在发送保密消息的同时也会产生人工噪声以防止窃听，而在合法接收机处干扰和人工噪声被对齐以便于消除，因此可以在不影响合法传输的前提下干扰窃听。在前人对干扰对齐系统可行性分析的基础上，本文提出了一种更加严格的判断可行性的条件。此外，针对传统基于 AM 或 ILM 的干扰对齐算法可能存在消除有用信号的问题，本文提出了一种改进干扰对齐算法。仿真结果表明，与传统 AM 或 ILM 干扰对齐算法相比，所提改进干扰对齐算法能够有效解决消除信号问题，同时最大限度保证保密用户的通信质量。本文对合法信道的假设为每个合法用户的局部 CSI 已知，然而在实际信道获取过程中可能存在估计误差。因此在未来工作中，可以考虑存在信道估计误差的情况下基于干扰对齐设计安全传输算法。

参考文献：

[1] YOU X H, WANG C X, HUANG J, et al. Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts[J]. Science China Information Sciences, 2021, 64(1): 1-74.

[2] SU J, SHENG Z G, LIU AX, et al. Capture-aware identification of mobile RFID tags with unreliable channels[J]. IEEE Transactions on Mobile Computing, 2022, 21(4): 1182-1195.

[3] 范平志, 李里, 陈欢, 等. 面向大规模物联网的随机接入: 现状, 挑战与机遇[J]. 通信学报, 2021, 42(4): 1-21.
FAN P Z, LI L, CHEN H, et al. Random access for massive internet of things: current status, challenges and opportunities[J]. Journal on Communications, 2021, 42(4): 1-21.

[4] SHI W, XU W, YOU X H, et al. Intelligent reflection enabling technologies for integrated and green internet-of-everything beyond 5G: communication, sensing, and security[J]. IEEE Wireless Communications, 2022.

[5] GUO H Z, LI J Y, LIU J J, et al. A survey on space-air-ground-sea integrated network security in 6G[J]. IEEE Communications Surveys & Tutorials, 2021, 24(1): 53-87.

[6] 孙长印, 刘李延, 江帆, 等. 基于 DNN 的 Sub-6 GHz 辅助毫米波网络功率分配算法[J]. 通信学报, 2021, 42(9): 184-193.
SUN C Y, LIU L Y, JIANG F, et al. DNN-based Sub-6 GHz assisted millimeter wave network power allocation algorithm[J]. Journal on Communications, 2021, 42(9): 184-193.

[7] 廖勇, 杨馨怡, 杜洁汝. 基于两阶段的毫米波大规模 MIMO 低复杂度混合预编码算法[J]. 电子学报, 2021, 49(7): 1298.
LIAO Y, YANG X Y, DU J R. A two‐stage based low complexity hybrid precoding algorithm for millimeter‐wave massive MIMO[J]. Acta Electronica Sinica, 2021, 49(7): 1298-1304.

[8] XUE Q, LIU Y J, SUN Y, et al. Beam management in ultra-dense mmWave network via federated reinforcement learning: an intelligent and secure approach[J]. IEEE Transactions on Cognitive Communications and Networking, 2022, 9(1): 185-197.

[9] WANG J, WANG X X, GAO R F, et al. Physical layer security for UAV communications: a comprehensive survey[J]. China Communications, 2022, 19(9): 77-115.

[10] 陈新颖, 盛敏, 李博, 等. 面向 6G 的无人机通信综述[J]. 电子与信息学报, 2022, 44(3): 781-789.
CHEN X Y, SHENG M, LI B, et al. Survey on unmanned aerial vehicle communications for 6G[J]. Journal of Electronics & Information Technology, 2022, 44(3): 781-789.

[11] ZENG Y, WU Q Q, ZHANG R. Accessing from the sky: a tutorial on UAV communications for 5G and beyond[J]. Proceedings of the IEEE, 2019, 107(12): 2327-2375.

[12] 崔琪楣, 赵文静, 顾晓阳, 等. 面向 B5G 网络的高效切换认证与安全密钥更新机制[J]. 通信学报, 2021, 42(12): 96-108.
CUI Q M, ZHAO W J, GU X Y, et al. Efficient handover authentication and secure key-updating mechanism for B5G networks[J]. Journal on Communications, 2021, 42(12): 96-108.

[13] XIE N, ZHANG J H, ZHANG Q H. Security provided by the physical layer in wireless communications[EB]. 2022.

[14] CHORTI A, BARRETO A N, KOPSELL S, et al. Context-aware security for 6G wireless: the role of physical layer security[J]. IEEE Communications Standards Magazine, 2022, 6(1): 102-108.

[15] SHU F, YANG L L, JIANG X Y, et al. Beamforming and transmit power design for intelligent reconfigurable surface-aided secure spatial modulation[J]. IEEE Journal of Selected Topics in Signal Processing, 2022, 16(5): 933-949.

[16] SUN L, TIAN X Y. Physical layer security in multi-antenna cellular systems: joint optimization of feedback rate and power allocation[J]. IEEE Transactions on Wireless Communications, 2022, 21(9): 7165-7180.

[17] CAO W F, ZOU Y L, YANG Z, et al. Secrecy outage analysis of relay-user pairing for secure hybrid satellite-terrestrial networks[J]. IEEE Transactions on Vehicular Technology, 2022, 71(8): 8906-8918.

[18] HU L, WEN H, WU B, et al. Cooperative jamming for physical layer security enhancement in internet of things[J]. IEEE Internet of Things Journal, 2018, 5(1): 219-228.

[19] SONG H H, WEN H, HU L, et al. Optimal power allocation for secrecy rate maximization in broadcast wiretap channels[J]. IEEE Wireless Communications Letters, 2018, 7(4): 514-517.

[20] WANG B, MU P C, LI Z Z. Artificial-noise-aided beamforming design in the MISOME wiretap channel under the secrecy outage probability

constraint[J]. IEEE Transactions on Wireless Communications, 2017, 16(11): 7207-7220.

[21] HU L, WEN H, WU B, et al. Cooperative-jamming-aided secrecy enhancement in wireless networks with passive eavesdroppers. IEEE Transactions on Vehicular Technology, 2018, 67(3): 2108-2117.

[22] GOMADAM K, CADAMBE V R, JAFAR S A. A distributed numerical approach to interference alignment and applications to wireless interference networks[J]. IEEE Transactions on Information Theory, 2011, 57(6): 3309-3322.

[23] RAZAVIYAYN M, LYUBEZNIK G, LUO Z Q. On the degrees of freedom achievable through interference alignment in a MIMO interference channel[J]. IEEE Transactions on Signal Processing, 2012, 60(2): 812-821.

[24] MA L P, XU T Y, STERNBERG G. Computational complexity of interference alignment for symmetric MIMO networks[J]. IEEE Communications Letters, 2013, 17(12): 2308-2311.

[25] YETIS C M, GOU T G, JAFAR S A, et al. On feasibility of interference alignment in MIMO interference networks[J]. IEEE Transactions on Signal Processing, 2010, 58(9): 4771-4782.

[26] ZHAO N, YU F R, LI M, et al. Anti-eavesdropping schemes for interference alignment (IA)-based wireless networks[J]. IEEE Transactions on Wireless Communications, 2016, 15(8): 5719-5732.

[27] TIAN C, REN P Y, DU Q H, et al. An artificial noise-based security scheme for interference alignment-based wireless networks[C]//Proceedings of GLOBECOM 2017 - 2017 IEEE Global Communications Conference. Piscataway: IEEE Press, 2018: 1-6.

[28] GUO J, ZHAO N, YANG Z T, et al. Proactive jamming toward interference alignment networks: beneficial and adversarial aspects[J]. IEEE Systems Journal, 2019, 13(1): 412-423.

[29] ZHAO N, YU F R, LI M, et al. Physical layer security issues in interference- alignment-based wireless networks[J]. IEEE Communications Magazine, 2016, 54(8): 162-168.

[30] XIA H Y, ZHOU X K, HAN S, et al. Joint secure transceiver design and power allocation for AN-assisted MIMO networks[J]. IEEE Transactions on Wireless Communications, 2022, 21(1): 477-488.

[31] PETERS S W, HEATH R W. Cooperative algorithms for MIMO interference channels[J]. IEEE Transactions on Vehicular Technology, 2011, 60(1): 206-218.

[32] WYNER A D. The wire-tap channel[J]. The Bell System Technical Journal, 1975, 54(8): 1355-1387.

[33] BOYD S P, VANDENBERGHE L. Convex optimization[M]. Cambridge: Cambridge, University Press, 2004.

[作者简介]

胡林（1984– ），男，博士，重庆邮电大学讲师、硕士生导师，主要研究方向为物理层安全、多天线技术、物联网等。

范家兵（1997– ），男，重庆邮电大学硕士生，主要研究方向为无线通信、物理层安全。

文红（1969– ），女，博士，电子科技大学教授、博士生导师，主要研究方向为 5G 航空航天无线通信系统可靠与安全技术、移动互联网安全技术、物联网等。

唐杰（1988– ），男，博士，电子科技大学副教授、硕士生导师，主要研究方向为安全编码、物理层安全、物联网等。

陈前斌（1967– ），男，博士，重庆邮电大学教授、博士生导师，主要研究方向为无线通信与网络、信号融合检测与处理、物联网等。