中国科学: 信息科学 2022 年 第 52 卷 第 2 期: 239–252
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
6G 网络安全专题 · 论文

衰落高斯 MIMO 窃听信道下安全发送方案及其优化问题

马康宁[1], 徐寅飞[2], 邵硕[1*], 吴越[1*]

1. 上海交通大学电子信息与电气工程学院, 上海 200240
2. 东南大学信息科学与工程学院, 南京 211189
* 通信作者. E-mail: shuoshao@sjtu.edu.cn, wuyue@sjtu.edu.cn

收稿日期: 2021–07–29; 修回日期: 2021–09–13; 接受日期: 2021–10–29; 网络出版日期: 2022–01–10

国家重点研发计划 (批准号: 2020YFB1807504, 2020YFB1807500, SQ2020YFA070077)、国家自然科学基金 (批准号: 61901261, 61901105, 61941106, 52078117)、上海市扬帆计划 (批准号: 19YF1424200) 和江苏省自然科学基金 (批准号: BK20190343) 资助项目

摘要 自适应的物理层安全技术是 6G 通信中具有抗量子攻击实现通信安全一体化的重要挑战问题. 本文研究了合法用户信道状态随机衰落, 且各状态不满足退化关系的高斯多天线输入输出 (MIMO) 窃听信道的信道容量问题. 我们引入 “弱超多数化” (weak supermajorization) 理论对各状态排序. 并采用广播逼近 (broadcast approach) 技术, 即基于叠加编码 (superposition coding) 架构设计编码并予以优化, 从而完成信道状态信息 (channel state information, CSI) 未知情况下的物理层安全传输, 实现通信系统的内生安全. 该编码架构下的参数的优化问题可以表征为对数函数的非凸优化问题, 因此我们提出了求解该传输方案最优输入的快速算法.

关键词 高斯 MIMO 窃听广播信道, 衰落信道, 广播逼近, 叠加编码, 内生安全

1 引言

鉴于 6G 通信对于现有网络的集成要求, 网络安全成为了 6G 通信中的一个重要问题 [1]. 然而, 因为香农 (Shannon) 一次一密机制在现实中难以高效实现, 传统密码技术的安全性又因为量子计算的发展受到严重威胁 [2~4], 目前面向 6G 通信的安全保障技术研究已迫在眉睫. 在对 5G 超高可靠超低时延通信 (ultra reliable low latency communications) 场景的研究中, 信道物理层安全引起了大家的广泛关注 [5,6]. 物理层安全即为通过相应的编码技术手段, 使窃听者获得的信号与通信传递的消息统计上独立, 从而达到香农所描述的信息安全 [7]. 因此, 为了实现 6G 通信中的内生安全功能 [1], 我们必须研究更加具有鲁棒性的物理层安全实现技术, 保证通信系统在非理想状态下的安全性. 在众多应用场景

引用格式: 马康宁, 徐寅飞, 邵硕, 等. 衰落高斯 MIMO 窃听信道下安全发送方案及其优化问题. 中国科学: 信息科学, 2022, 52: 239–252, doi: 10.1360/SSI-2021-0255
Ma K N, Xu Y F, Shao S, et al. On the optimization problem in fading Gaussian MIMO wiretap channels (in Chinese). Sci Sin Inform, 2022, 52: 239–252, doi: 10.1360/SSI-2021-0255

下, 受现实通信情境驱动, 高斯 MIMO (Gaussian multiple input multiple output) 窃听信道上的编码实现一直是通信网络物理层安全的核心问题 [8].

高斯 MIMO 窃听信道是一类特殊的多用户高斯 MIMO 广播信道 [9], 其接收方中存在非法窃听者. 目前, 在 CSI (channel state information) 已知的情况下, 高斯窃听信道容量问题的研究已较为成熟. 在平均发送功率受限时, 研究表明信道容量可以通过高斯随机码簿实现 [10,11]. 文献 [12] 研究了标量广播信道下的容量. 文献 [13~17] 讨论了更复杂的 MIMO 场景的信道容量. 文献 [18~20] 研究了信道输入的协方差受限时的安全容量.

然而实际的通信系统中, 信道衰落是一个普遍现象, 信道状态往往随机而且非恒定 [21]. 因此, 研究人员开始将已有方案扩展到存在信道衰落的高斯 MIMO 窃听信道中 [22~25]. Liang 等 [22] 为了保证所有信道状态下都能成功通信, 采用分层广播逼近 [26,27] 的思路. 在这种策略下, 消息被分成一些独立的消息块, 分别编码后层层叠加作为信道输入. 在窃听者无法解码任何消息内容的前提下, 接收方尽可能多地解码这些消息. 能解码的最大消息层数取决于实际的信道状态. 方案的传输效率则体现为接收方平均可解码信息的码率.

设计分层编码时, 需要先对所有可能的信道状态进行优劣排序. 这会直接影响方案的传输效率. 标量信道时, 最优排序策略是按照每个状态下高斯噪声的协方差大小进行排序 [22]. 当扩展到 MIMO 信道时, 情况会复杂很多. 当各状态满足退化关系时, 各状态下的信道输出间会形成马尔可夫链 (Markov chain) [28], 能以此给出信道状态的强度的排序. 另一方面, 当各状态并不严格满足退化关系时, 文献 [26,27] 提出了一种基于信道范数矩阵奇异值的 “弱超多数化” 排序.

本文考虑如下这个贴近于实际的系统模型. 此系统中包括一个合法接收用户和一个窃听者, 信息通过衰落高斯 MIMO 信道进行传输. 假设发方和用户之间的主信道存在缓慢衰落, 而窃听者的窃听信道没有衰落. 因为即使窃听信道存在衰落, 发送方也必须始终考虑最坏的情况以防止信息泄漏. 此外发送时发方是未知 CSI 的, 而用户可以通过信道估计得知衰落增益.

在我们的模型中, 这种随机衰落增益会等效成信道中加性高斯噪声的随机可变协方差矩阵. 所有可能的噪声协方差矩阵会被近似量化成有限数量的矩阵. 我们进一步假设这些协方差矩阵的特征值满足弱超多数化排序关系. 由于缓慢衰落, 假设协方差矩阵在单个保密消息的发送周期中保持不变.

出于对通信系统内生安全机制的研究, 本文着力于针对上述系统设计具有鲁棒性的物理层安全通信方案. 我们希望通信方案在对 CSI 未知的请况下仍然可以安全的完成信息传输, 并且可以基于信道状态先验概率最大化码率的数学期望. 我们将文献 [22] 中的结果扩展到具有有限衰落状态的高斯 MIMO 信道, 采用文献 [26] 中基于弱超多数化排序的分层广播逼近策略, 并将其扩展到存在窃听者的场景中. 为了最大化方案的平均可解码速率, 我们通过解决一个非凸优化问题来确定每个通信层的功率分配. 然而这类非凸问题一般难以解决 [9]. 此时信道容量是两个互信息函数 [10] 的差的最大值, 传统注水方法 [29~31] 难以求解. 于是我们从 Karush-Kuhn-Tucker (KKT) 条件中总结了最优解必须满足的一些必要属性, 提出了一种大多数情况下都能有效求解最优解的算法, 进而设计出最优方案.

本文的主要贡献如下. 提出了一个不依赖于 CSI 信息的面向衰落高斯 MIMO 窃听信道的物理层安全传输编码方案. 通过超多数化理论设计所有信道状态的排序, 进而利用保密约束下的分层广播逼近, 我们证明了该方案的可达性. 进一步, 为了找到输入总功率受限时的码率数学期望最大化的广播方案, 刻画了一个非凸优化问题, 并提出快速算法予以解决. 该快速算法在部分情况下具有最优性, 例如在标量信道中, 该模型将退化为文献 [22] 中的模型, 而此时本文算法可以提供最优的功率分配方案.

本文结构如下. 第 2 节构建了信道的数学模型并简要介绍了分层广播逼近, 总结了表征最大平均可解码速率的优化问题. 第 3 节描述了方案的可达性并证明了保密性. 第 4 节通过解决总结的优化问

题来优化方案的输入, 并据此推导出有限功率下最佳方案的功率分配策略. 最后, 第 5 节总结全文.

2 模型设置

2.1 系统模型

本文研究具有单个发方和两个接收方 (合法用户和非法窃听者) 的无记忆高斯 MIMO 窃听广播信道. 发方和用户之间的主信道经历慢衰落, 具体表现为在每个区间里, 主信道中的加性高斯噪声的协方差取值是随机的, 而且发方无法预知这类 CSI. 这里考虑噪声可能的协方差的数量是有限的, 设为 T, 即有 T 种可能的信道状态.

在每一个发送区间, 发方将一条机密消息 W 记为多个相互独立消息的有序对 $(W_1, W_2, \dots, W_T)$, 其中 $W_t \in \mathcal{W}_t = \{1, 2, \dots, 2^{nR_t}\}$, $t = 1, 2, \dots, T$. 这里 $R_1, R_2, \dots, R_T \geqslant 0$, 为各个消息的码率. 发送方将消息编码为信道输入 $\boldsymbol{X}^n = (X_1, X_2, \dots, X_\ell)^n \in \mathbb{R}^{\ell \cdot n}$, 每个 $\boldsymbol{X}$ 都是实数向量空间 $\mathbb{R}^\ell$ 中一个的 ℓ 长序列. 即发送时发方分 n 次传输 $\boldsymbol{X}^n$, 每次通过 ℓ 根天线广播一组序列 $X_1, X_2, \dots, X_\ell$. 在每一次广播后, 合法用户 (简称为 A) 从主信道中收到 ℓ 长消息 $\boldsymbol{Y}_A$, 而窃听者 (简称为 B) 从窃听信道中窃听 ℓ 长消息 $\boldsymbol{Y}_B$. 它们都是被信道中的零均值加性白高斯噪声污染后的消息. 定义 $\boldsymbol{Y}_A^n, \boldsymbol{Y}_B^n \in \mathbb{R}^{\ell \cdot n}$ 分别表示 A 和 B 在 n 次传输中收到的信息. 在本文中, 发方想要将消息无错发送给用户, 同时对窃听者保密. 下面给出关于速率 $(R_1, R_2, \dots, R_T)$ 的可达性 (achievability) 定义.

定义1 如果存在

• 一个编码器 $f : \mathcal{W} \to \mathbb{R}^{\ell \cdot n}$, 能帮助发方将消息 $W = (W_1, W_2, \dots, W_T)$ 加密成信道输入 $\boldsymbol{X}^n$;

• T 个解码器 $\{\varphi_t : \mathbb{R}^{\ell \cdot n} \to \mathcal{W}_t, t = 1, 2, \dots, T\}$, 当第 t 个信道状态发生时, φ_t 能让用户 A 将接收消息 $\boldsymbol{Y}_A^n$ 解码为机密消息 W_t;

使得当任意第 t 个信道状态发生时,

• 当传输序列长度 $n \to \infty$, 用户 A 处解码出错率 $P_e = \Pr\{\varphi_t(\boldsymbol{Y}_A^n) \neq W_t\} \to 0$, 即用户 A 能够以可忽略的错误概率恢复机密消息 W_t.

• 当传输序列长度 $n \to \infty$, 互信息 $I(\boldsymbol{Y}_B^n; W_1, W_2, \dots, W_T) = 0$. 即当收到 $\boldsymbol{Y}_B^n$ 时, 非法窃听者 B 无法了解有关机密消息 W 的任何信息.

则称速率 $(R_1, R_2, \dots, R_T)$ 是可达的 (achievable).

2.2 问题归纳

在单次传输中, 信道输入 $\boldsymbol{X}$ 和信道输出 $\boldsymbol{Y}_A, \boldsymbol{Y}_B$ 的关系如下:

$$\boldsymbol{Y}_A = \boldsymbol{X} + \boldsymbol{N}_A, \tag{1}$$

$$\boldsymbol{Y}_B = \boldsymbol{X} + \boldsymbol{N}_B. \tag{2}$$

这里信道输入 $\boldsymbol{X} = (X_1, X_2, \dots, X_\ell)$ 是一个长度为 ℓ 的随机变量序列, 满足功率限制:

$$E(\boldsymbol{X}^{\mathrm{T}}\boldsymbol{X}) = E(X_1^2 + X_2^2 + \cdots + X_\ell^2) \leqslant \ell \cdot P, \tag{3}$$

其中 $P \in \mathbb{R}^+$, $\ell \cdot P$ 描述的是发方所有天线功率总和的上限. 两个 ℓ 长零均值高斯随机向量 $\boldsymbol{N}_A, \boldsymbol{N}_B$ 代表主信道和窃听信道中的加性噪声. 将两个噪声的协方差矩阵分别表示为严格正定矩阵 $\boldsymbol{K}_{\boldsymbol{N}_A}, \boldsymbol{K}_{\boldsymbol{N}_B}$.

因为主信道经历慢衰落, $\boldsymbol{N}_A$ 的协方差 $\boldsymbol{K}_{\boldsymbol{N}_A}$ 在每个发送区间随机取值, 但在单个区间内不变. 将所有可能的 $\boldsymbol{K}_{\boldsymbol{N}_A}$ 量化为 T 个矩阵 $\boldsymbol{K}_{\boldsymbol{N}_{A_1}}, \boldsymbol{K}_{\boldsymbol{N}_{A_2}}, \dots, \boldsymbol{K}_{\boldsymbol{N}_{A_T}}$. 用 $\boldsymbol{N}_{A_t}$, $t = 1, 2, \dots, T$ 表示协方差为

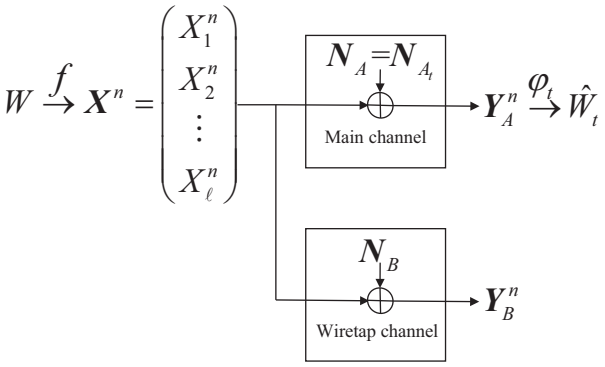

图 1　系统模型

Figure 1　System model

$\boldsymbol{K}_{\boldsymbol{N}_{A_t}}$ 的 T 个零均值高斯噪声. 于是主信道可以看成一共有 T 种信道状态的慢衰落信道, 且这 T 种信道状态分别对应噪声为 $\boldsymbol{N}_{A_1}, \boldsymbol{N}_{A_2}, \ldots, \boldsymbol{N}_{A_T}$ 的情况. 另外, 发方在发送区间开始前无法预测信道状态, 只知道 T 种信道状态发生的概率. 用户则可以通过信道估计得知 $\boldsymbol{K}_{\boldsymbol{N}_A}$. 系统模型如图 1 所示.

我们希望为这个信道状态时变的信道设计一个码率为 $(R_1, R_2, \ldots, R_T)$ 的可达编码方案, 同时要最大化方案的平均可解码速率. 受到文献 [26] 启发, 我们基于经典超多数化理论 [32], 设计了一种衡量 $\boldsymbol{N}_{A_1}, \boldsymbol{N}_{A_2}, \ldots, \boldsymbol{N}_{A_T}, \boldsymbol{N}_B$ 之间强弱关系的排序. 简单介绍一下弱超多数化 [32]: 对于两个 ℓ 长递增序列 $\boldsymbol{a} = \{a_1, a_2, \ldots, a_\ell\}$, $\boldsymbol{b} = \{b_1, b_2, \ldots, b_\ell\}$, 如果有 $\sum_{i=1}^k a_i \geqslant \sum_{i=1}^k b_i$, $k = 1, 2, \ldots, \ell$, 则称 $\boldsymbol{a}$ 弱超多数化于 $\boldsymbol{b}$, 表示为 $\boldsymbol{a} \prec^w \boldsymbol{b}$. 同时, 对于任意连续递减的凸函数 $g(\cdot)$, 有

$$\sum_{i=1}^{\ell} g(a_i) \leqslant \sum_{i=1}^{\ell} g(b_i). \tag{4}$$

假设所有噪声都可以通过弱超多数化进行排序. 令 $\boldsymbol{N}_{A_t}$ 的协方差 $\boldsymbol{K}_{\boldsymbol{N}_{A_t}}$ 的特征值为 $\boldsymbol{\lambda}_t = \{\lambda_{t,i}\}_{i=1}^{\ell}$, $t = 1, 2, \ldots, T$, $\boldsymbol{N}_B$ 的协方差 $\boldsymbol{K}_{\boldsymbol{N}_B}$ 的特征值为 $\boldsymbol{\lambda}_e = \{\lambda_{e,i}\}_{i=1}^{\ell}$. 我们有

$$\boldsymbol{\lambda}_e \prec^w \boldsymbol{\lambda}_T \prec^w \cdots \prec^w \boldsymbol{\lambda}_1. \tag{5}$$

可以看出窃听信道噪声强度最强, 然后主信道从第 T 个状态到第 1 个状态的噪声强度递减; 等价的, 这些信道状态下的信道信息传输能力是递增的.

为实现保密传输, 采用叠加编码设计分层广播逼近. 我们的方案是文献 [22] 中标量衰落信道方案的扩展 MIMO 版本. 在这个方案中, 信道输入 $\boldsymbol{X}$ 是一个零均值高斯随机向量, 其协方差矩阵 $\boldsymbol{K}_{\boldsymbol{X}} = k\boldsymbol{I}_\ell$, 其中 $\boldsymbol{I}_\ell$ 表示 ℓ 维单位矩阵, $0 \leqslant k \leqslant P$. 很明显 $\boldsymbol{K}_{\boldsymbol{X}}$ 满足约束 (3): $E(\boldsymbol{X}^{\mathrm{T}}\boldsymbol{X}) = \mathrm{Tr}(\boldsymbol{K}_{\boldsymbol{X}}) \leqslant \ell P$, 这里 $\mathrm{Tr}(\cdot)$ 表示矩阵的迹.

先简略说明传输方案. 在一个发送区间开始前, 消息 W 被划分为 T 个部分 $\{W_1, W_2, \ldots, W_T\}$, 并以速率 $(R_1, R_2, \ldots, R_T)$ 被分别编码为 $\boldsymbol{X}_1^n, \boldsymbol{X}_2^n, \ldots, \boldsymbol{X}_T^n$, 这里每个 $\boldsymbol{X}_t \sim \mathcal{N}(0, \boldsymbol{K}_t)$ 互相独立, 协方差 $\boldsymbol{K}_t = k_t\boldsymbol{I}_\ell$ 且 $k_t \geqslant 0$. 然后在区间内的每次传输中, 设置信道输入为这些码字的叠加 $\boldsymbol{X} = \sum_{t=1}^T \boldsymbol{X}_t$. 易得 $\sum_{t=1}^T k_t = k$. 此时若令

$$R_t = \frac{1}{2}\log\frac{|\sum_{i=1}^t \boldsymbol{K}_i + \boldsymbol{K}_{\boldsymbol{N}_{A_t}}|}{|\sum_{i=1}^{t-1} \boldsymbol{K}_i + \boldsymbol{K}_{\boldsymbol{N}_{A_t}}|} - \frac{1}{2}\log\frac{|\sum_{i=1}^t \boldsymbol{K}_i + \boldsymbol{K}_{\boldsymbol{N}_B}|}{|\sum_{i=1}^{t-1} \boldsymbol{K}_i + \boldsymbol{K}_{\boldsymbol{N}_B}|},\ t = 1, 2, \ldots, T, \tag{6}$$

则 $(R_1, R_2, \ldots, R_T)$ 是可达的. 与此同时, 当 $\boldsymbol{K}_{\boldsymbol{N}_A} = \boldsymbol{K}_{\boldsymbol{N}_{A_t}}$, 因为式 (5) 中的排序关系, 接收者 A 不仅可以解码机密消息 W_t, 同时也可以解码 $W_{t+1}, W_{t+2}, \ldots, W_T$. 因此, 接收方 A 处关于消息的可解码速率为 $\sum_{i=t}^{T} R_i$. 具体的传输方案及可达性证明将在第 3 节中展示.

于是可以得到平均可解码速率:

$$R = \mathop{E}_{t}\left(\sum_{i=t}^{T} R_i\right) = \sum_{t=1}^{T}\left(p_t \cdot \sum_{i=t}^{T} R_i\right), \tag{7}$$

这里对于每个 $t \in \{1, 2, \ldots, T\}$, 用 $p_t = \Pr(\boldsymbol{K}_{\boldsymbol{N}_A} = \boldsymbol{K}_{\boldsymbol{N}_{A_t}})$ 表示第 t 种信道状态发生的概率, 且 $p_t > 0$. 显然, 方案中协方差分配 $\{\boldsymbol{K}_t\}_{t=1}^{T}$ 决定了 R 的大小. 于是限制式 (3) 下分层广播逼近中 R 的最大化问题可以归纳为如下关于 $\{\boldsymbol{K}_t\}_{t=1}^{T}$ 的优化:

$$\begin{aligned} \max \quad & R = \sum_{t=1}^{T}\left(p_t \cdot \sum_{i=t}^{T} R_i\right) \\ \text{s.t.} \quad & \mathrm{Tr}\left(\sum_{t=1}^{T}\boldsymbol{K}_t\right) \leqslant \ell P, \\ & \boldsymbol{K}_t = k_t \boldsymbol{I}_\ell \succeq \boldsymbol{0},\ t = 1, 2, \ldots, T. \end{aligned} \tag{8}$$

为了确定这个最大的 R 和对应的最优分层广播策略, 关键是找到问题 (8) 的最优解, 即每层的最优协方差分配 $\{\boldsymbol{K}_t\}_{t=1}^{T}$. 我们将第 4 节中提供策略和算法来找出这个非凸优化问题的最优解.

推论1 对于 $\ell = 1$ 的特殊情况下, 即标量信道中, 可以通过求解式 (8) 获得达到全局最大平均可解码速率 R 的方案.

标量信道中, 模型将退化为标量衰落高斯窃听信道, 即文献 [22] 中讨论的具有离散信道状态的场景. 式 (8) 的最优解可以为其提出的全局最优方案提供最优功率分配.

3 可达广播方案

鉴于信道状态的不可预期性, 我们使用叠加编码的架构设计编码. 叠加编码生成码簿时对多层信息逐步精炼 (successive refinement), 在信道状态满足对应层要求时, 可以成功传输本层以及前序层所有消息. 因此, 在信道状态未知的情况下, 叠加编码依然可以保证信息的成功传输. 本节给出基于随机编码和叠加编码设计的分层广播方案, 并证明其可达性.

3.1 方案描述

首先为方案的 T 层编码构建 T 组子码本. 发方会对原始机密消息 $W = (W_1, W_2, \ldots, W_T)$ 中的每一个消息 W_t 分别进行编码. 在第 t 层 ($t \in \{1, 2, \ldots, T\}$), 随机独立生成 $2^{n(R_t + \tilde{R}_t)}$ 个码字 $\boldsymbol{X}_t^n$, 码字中每个 $\boldsymbol{X}_t$ 独立, 并且服从分布 $\mathcal{N}(0, \boldsymbol{K}_t)$. 令

$$R_t + \tilde{R}_t = \frac{1}{2}\log\frac{|\sum_{i=1}^{t}\boldsymbol{K}_i + \boldsymbol{K}_{\boldsymbol{N}_{A_t}}|}{|\sum_{i=1}^{t-1}\boldsymbol{K}_i + \boldsymbol{K}_{\boldsymbol{N}_{A_t}}|},\ \tilde{R}_t = \frac{1}{2}\log\frac{|\sum_{i=1}^{t}\boldsymbol{K}_i + \boldsymbol{K}_{\boldsymbol{N}_B}|}{|\sum_{i=1}^{t-1}\boldsymbol{K}_i + \boldsymbol{K}_{\boldsymbol{N}_B}|}. \tag{9}$$

于是可以推导出式 (6) 中第 t 层码率 R_t. 接着将每个可能的 W_t, V_t 索引到 $\boldsymbol{X}_t^n(W_t, V_t)$ 来构建子码本 $\mathcal{C}_t$, 这里 W_t 是从 W 划分出的机密消息, 它均匀分布在 $\mathcal{W}_t = \{1, 2, \ldots, 2^{nR_t}\}$; V_t 是用来干扰窃听者的随机生成的混淆信息, 它均匀分布在 $\mathcal{V}_t = \{1, 2, \ldots, 2^{n\tilde{R}_t}\}$.

发送方在根据机密消息 W 确定 $\{W_1, W_2, \ldots, W_T\}$ 后, 随机选取 $\{V_1, V_2, \ldots, V_T\}$ 的值. 再把 $\boldsymbol{X}^n = \sum_{t=1}^{T} \boldsymbol{X}_t^n(W_t, V_t)$ 作为信道输入广播到信道中. 合法用户 A 和非法窃听者 B 将分别收到 $\boldsymbol{Y}_A^n$ 和 $\boldsymbol{Y}_B^n$. 当 $\boldsymbol{K}_{\boldsymbol{N}_A} = \boldsymbol{K}_{\boldsymbol{N}_{A_t}}$ 时, 如果 A 能找到某组 $(\hat{W}_t, \hat{V}_t)$, 且存在某些 $(\{W_i\}_{i=t+1}^T, \{V_i\}_{i=t+1}^T)$, 使它们对应的输入与收到的消息是联合典型的, 即 $(\boldsymbol{X}_t^n(\hat{W}_t, \hat{V}_t), \{\boldsymbol{X}_i^n(W_i, V_i)\}_{i=t+1}^T, \boldsymbol{Y}_A^n) \in T_\varepsilon^n(P_{\boldsymbol{X}_t \cdots \boldsymbol{X}_T \boldsymbol{Y}_A})$, 则断定发送方发送了 $(\hat{W}_t, \hat{V}_t)$, 否则 A 声称有错误.

3.2 可达性证明

在上述收发方案中, 假设某个发送区间内 $\boldsymbol{K}_{\boldsymbol{N}_A} = \boldsymbol{K}_{\boldsymbol{N}_{A_t}}$ $(t \in \{1, 2, \ldots, T\})$. 接下来将证明 A 可以正确解码机密消息 $W_t, W_{t+1}, \ldots, W_T$ 而 B 将无法了解任何有关机密消息 W 的信息. 以此展示式 (6) 定义的速率 $(R_1, R_2, \ldots, R_T)$ 可达, 并且接收方 A 处关于消息的可解码速率为 $\sum_{i=t}^{T} R_i$.

根据大数定律和联合典型译码规律, 当 $n \to +\infty$ 且

$$\sum_{i=t}^{T}(R_i + \tilde{R}_i) \leqslant I(\{\boldsymbol{X}_i\}_{i=t}^T; \boldsymbol{Y}_A), \quad R_t + \tilde{R}_t \leqslant I(\boldsymbol{X}_t; \boldsymbol{Y}_A | \{\boldsymbol{X}_i\}_{i=t+1}^T), \tag{10}$$

A 能以可忽略的错误概率解码 (W_t, V_t). 这两个不等式在此时是成立的, 因为

$$\begin{aligned}\sum_{i=t}^{T}(R_i + \tilde{R}_i) &= \sum_{i=t}^{T} \frac{1}{2}\log\frac{|\sum_{j=1}^{i} \boldsymbol{K}_j + \boldsymbol{K}_{\boldsymbol{N}_{A_i}}|}{|\sum_{j=1}^{i-1} \boldsymbol{K}_j + \boldsymbol{K}_{\boldsymbol{N}_{A_i}}|} \overset{\text{(a)}}{\leqslant} \sum_{i=t}^{T} \frac{1}{2}\log\frac{|\sum_{j=1}^{i} \boldsymbol{K}_j + \boldsymbol{K}_{\boldsymbol{N}_{A_t}}|}{|\sum_{j=1}^{i-1} \boldsymbol{K}_j + \boldsymbol{K}_{\boldsymbol{N}_{A_t}}|} \\ &= \frac{1}{2}\log\frac{|\sum_{j=1}^{T} \boldsymbol{K}_j + \boldsymbol{K}_{\boldsymbol{N}_{A_t}}|}{|\sum_{j=1}^{t-1} \boldsymbol{K}_j + \boldsymbol{K}_{\boldsymbol{N}_{A_t}}|} = I\left(\sum_{i=t}^{T} \boldsymbol{X}_i; \boldsymbol{Y}_A\right) \overset{\text{(b)}}{=} I(\{\boldsymbol{X}_i\}_{i=t}^T; \boldsymbol{Y}_A), \end{aligned} \tag{11}$$

$$R_t + \tilde{R}_t = \frac{1}{2}\log\frac{|\sum_{i=1}^{t} \boldsymbol{K}_i + \boldsymbol{K}_{\boldsymbol{N}_{A_t}}|}{|\sum_{i=1}^{t-1} \boldsymbol{K}_i + \boldsymbol{K}_{\boldsymbol{N}_{A_t}}|} = I\left(\boldsymbol{X}_t; \boldsymbol{Y}_A - \sum_{i=t+1}^{T} \boldsymbol{X}_i\right) = I(\boldsymbol{X}_t; \boldsymbol{Y}_A | \{\boldsymbol{X}_i\}_{i=t+1}^T), \tag{12}$$

这里不等号 (a) 是因为对每个 $i \geqslant t$, 有

$$\log\frac{|\sum_{j=1}^{i} \boldsymbol{K}_j + \boldsymbol{K}_{\boldsymbol{N}_{A_i}}|}{|\sum_{j=1}^{i-1} \boldsymbol{K}_j + \boldsymbol{K}_{\boldsymbol{N}_{A_i}}|} = \sum_{r=1}^{\ell} \log\frac{\sum_{j=1}^{i} k_j + \lambda_{i,r}}{\sum_{j=1}^{i-1} k_j + \lambda_{i,r}} \overset{\text{(c)}}{\leqslant} \sum_{r=1}^{\ell} \log\frac{\sum_{j=1}^{i} k_j + \lambda_{t,r}}{\sum_{j=1}^{i-1} k_j + \lambda_{t,r}} = \log\frac{|\sum_{j=1}^{i} \boldsymbol{K}_j + \boldsymbol{K}_{\boldsymbol{N}_{A_t}}|}{|\sum_{j=1}^{i-1} \boldsymbol{K}_j + \boldsymbol{K}_{\boldsymbol{N}_{A_t}}|}, \tag{13}$$

其中 (c) 是因为 $\boldsymbol{\lambda}_i \prec^w \boldsymbol{\lambda}_t$ 且函数 $g(x) = \log[(\sum_{j=1}^{i} k_j + x)/(\sum_{j=1}^{i-1} k_j + x)]$ 在 $x \geqslant 0$ 时是连续的递减凸函数. 式 (11) 中的 (b) 是因为有马氏链 $\{\boldsymbol{X}_i\}_{i=t}^T \to \sum_{i=t}^{T} \boldsymbol{X}_i \to \boldsymbol{Y}_A$ 且 $I(\sum_{i=t}^{T} \boldsymbol{X}_i; \boldsymbol{Y}_A | \{\boldsymbol{X}_i\}_{i=t}^T) = 0$.

对于消息 $W_r \in \{W_{t+1}, W_{t+2}, \ldots, W_T\}$, 用户 A 可以用 $\boldsymbol{K}_{\boldsymbol{N}_A} = \boldsymbol{K}_{\boldsymbol{N}_{A_r}}$ 时解码 (W_r, V_r) 的策略进行解码. 这是因为此时互信息 $I(\{\boldsymbol{X}_i\}_{i=r}^T; \boldsymbol{Y}_A)$ 和 $I(\boldsymbol{X}_r; \boldsymbol{Y}_A | \{\boldsymbol{X}_i\}_{i=r+1}^T)$ 比 $\boldsymbol{K}_{\boldsymbol{N}_A} = \boldsymbol{K}_{\boldsymbol{N}_{A_r}}$ 时的大 (证明与式 (11) 中 (a) 的证明类似, 这里省略). 于是 A 也能以可忽略的错误概率解码 (W_r, V_r). 这意味着此时发方可以向 A 成功传输第 t 层以及前序层所有消息 $\{W_t, W_{t+1}, \ldots, W_T\}$, 可解码速率为 $\sum_{i=t}^{T} R_i$.

最后我们需要证明窃听者 B 在 $n \to \infty$ 时, $\frac{1}{n} I(\boldsymbol{Y}_B^n; W) = 0$, 即其获得的关于 W 的信息是可以忽略不计的. 这等价于证明在 $n \to \infty$ 时,

$$\frac{1}{n} H(W | \boldsymbol{Y}_B^n) = \frac{1}{n} H(W) = \frac{1}{n} H(\{W_t\}_{t=1}^T) = \sum_{t=1}^{T} R_t. \tag{14}$$

对此, 有

$$\frac{1}{n} H(W | \boldsymbol{Y}_B^n) = \frac{1}{n} \left[H(\boldsymbol{X}^n) + H(W, \boldsymbol{Y}_B^n | \boldsymbol{X}^n) - H(\boldsymbol{X}^n | W, \boldsymbol{Y}_B^n) - H(\boldsymbol{Y}_B^n)\right]$$

$$\begin{aligned}\geqslant&\frac{1}{n}\left[H(\boldsymbol{X}^n)+H(\boldsymbol{Y}_B^n|\boldsymbol{X}^n)-H(\boldsymbol{Y}_B^n)-H(\boldsymbol{X}^n|W,\boldsymbol{Y}_B^n)\right]\\=&\frac{1}{n}\left[H(\boldsymbol{X}^n)-I(\boldsymbol{Y}_B^n;\boldsymbol{X}^n)-H(\boldsymbol{X}^n|W,\boldsymbol{Y}_B^n)\right].\end{aligned}\tag{15}$$

分别考虑式 (15) 中的 3 项. 对于第 1 项, 因为输入 $\boldsymbol{X}^n=\sum_{t=1}^T\boldsymbol{X}_t^n(W_t,V_t)$ 且每个 $\boldsymbol{X}_t^n(W_t,V_t)$ 是从 $2^{n(R_t+\tilde{R}_t)}$ 个可能数值中均匀选取的, 于是 $\frac{1}{n}H(\boldsymbol{X}^n)=\sum_{t=1}^T(R_t+\tilde{R}_t)$. 对于第 2 项, 因为信道 n 次收发过程互相独立, 所以

$$\begin{aligned}\frac{1}{n}I(\boldsymbol{Y}_B^n;\boldsymbol{X}^n)\overset{\text{(a)}}{\leqslant}&I(\boldsymbol{Y}_B;\boldsymbol{X})+\varepsilon=I\left(\sum_{i=1}^T\boldsymbol{X}_i+\boldsymbol{N}_B;\sum_{i=1}^T\boldsymbol{X}_i\right)+\varepsilon=I\left(\sum_{i=1}^T\boldsymbol{X}_i+\boldsymbol{N}_B;\{\boldsymbol{X}_t\}_{t=1}^T\right)+\varepsilon\\=&\sum_{t=1}^T I\left(\sum_{i=1}^T\boldsymbol{X}_i+\boldsymbol{N}_B;\boldsymbol{X}_t|\{\boldsymbol{X}_i\}_{i=t+1}^T\right)+\varepsilon=\sum_{t=1}^T I\left(\sum_{i=1}^t\boldsymbol{X}_i+\boldsymbol{N}_B;\boldsymbol{X}_t\right)+\varepsilon\\=&\sum_{t=1}^T\frac{1}{2}\log\frac{|\sum_{i=1}^t\boldsymbol{K}_i+\boldsymbol{K}_{\boldsymbol{N}_B}|}{|\sum_{i=1}^{t-1}\boldsymbol{K}_i+\boldsymbol{K}_{\boldsymbol{N}_B}|}+\varepsilon=\sum_{t=1}^T\tilde{R}_t+\varepsilon,\end{aligned}\tag{16}$$

这里 (a) 是因为文献 [33, Lemma 8] 和 [34], 且 $\varepsilon\to 0$ 当 $n\to\infty$. 对于第 3 项, 考虑式 (9) 中 $\tilde{R}_t$ 定义. 根据大数定律, 给定 $\boldsymbol{Y}_B^n$, 窃听者 B 能够以可忽略的错误概率解码所有混淆消息 $\{V_t\}_{t=1}^T$. 因此, 给定 $\boldsymbol{Y}_B^n$ 和 W, 窃听者 B 能够以可忽略的错误概率恢复输入 $\boldsymbol{X}^n$, 定义错误概率为 η. 根据费诺不等式, 有

$$\frac{1}{n}H(\boldsymbol{X}^n|W,\boldsymbol{Y}_B^n)\leqslant\frac{1}{n}\left[1+\eta\log|\mathcal{X}|^n\right]=\frac{1}{n}+\eta\sum_{t=1}^T(R_t+\tilde{R}_t),\tag{17}$$

这里 $\eta\to 0$ 当 $n\to\infty$, $|\mathcal{X}|$ 表示 $\boldsymbol{X}$ 可能的取值数. 在 $n\to\infty$ 时, 将 3 项代入到式 (15), 有

$$\lim_{n\to\infty}\frac{1}{n}H(W|\boldsymbol{Y}_B^n)\geqslant\sum_{t=1}^T R_t.\tag{18}$$

结合 $H(W|\boldsymbol{Y}_B^n)\leqslant H(W)$, 证明了式 (14). 综上方案的可达性证毕.

4 信道输入优化

本节通过解决优化问题 (8) 来优化收发方案. 根据定义, 知道协方差分配 $\{\boldsymbol{K}_t\}_{t=1}^T$ 是由功率分配 $\boldsymbol{k}=(k_1,\ldots,k_T)^{\mathrm{T}}$ 确定的, 可以给出最优 $\boldsymbol{k}$ 的必要的 KKT 条件. 定义拉格朗日函数:

$$\mathcal{L}(\boldsymbol{k},w,\boldsymbol{v})=-R-w\left(P-\sum_{t=1}^T k_t\right)-\boldsymbol{v}^{\mathrm{T}}\boldsymbol{k},\tag{19}$$

其中这些非负的变量 $\boldsymbol{v}=(v_1,v_2,\ldots,v_T)^{\mathrm{T}}$, w 是对应于约束 $\{k_t\geqslant 0:t=1,2,\ldots,T\}$ 和 $\sum_{t=1}^T k_t\leqslant P$ 的拉格朗日乘子. 于是 KKT 必要条件包含

$$\nabla_{\boldsymbol{k}}\mathcal{L}(\boldsymbol{k},w,\boldsymbol{v})=\boldsymbol{0},\tag{20}$$

$$P-\sum_{t=1}^T k_t=0,\tag{21}$$

$$k_t\geqslant 0,\ t=1,2,\ldots,T,\tag{22}$$

$$v_t k_t = 0,\ t = 1, 2, \ldots, T. \tag{23}$$

这里式 (21) 是因为如果 $\sum_{t=1}^{T} k_t < P$, 可以增加 k_T 来增加 R_T, 同时 $R_1, \ldots, R_{T-1}$ 保持不变, R 增加, 所以只考虑功率完全分配的情况.

定义2 在 $x \in [0, P]$ 上定义如下一类函数:

$$f_t(x) = \frac{1}{2}\left(\sum_{r=1}^{\ell} \frac{1}{x + \lambda_{t,r}} - \sum_{r=1}^{\ell} \frac{1}{x + \lambda_{e,r}}\right) \cdot \sum_{j=1}^{t} p_j, \quad t \in \{1, 2, \ldots, T\}. \tag{24}$$

性质1 对任意 $t \in \{1, 2, \ldots, T\}$ 和 $i \in \{t+1, t+2, \ldots, T\}$, 如果 $f_t(x) - f_i(x) \geqslant 0$ 在 $x = x_0 \in (0, P]$ 成立, 那么对所有 $x \in [0, x_0)$ 有 $f_t(x) > f_i(x)$.

性质 1 在标量情况下总是成立的, 因为此时如果 $f_t(x) - f_i(x) \geqslant 0$, 那么函数 $f_t(x) - f_i(x)$ 的导数是负的. 即使在有衰落的高斯 MIMO 窃听信道中, 大多数情况下也是满足的. 如果模型参数满足这个性质, 就可以利用式 (20)∼(23) 推导出最优功率分配 $\boldsymbol{k}$.

现在假设性质 1 成立, 定义一个集合 $\mathcal{H} = \{h \in \{1, 2, \ldots, T\} : k_h > 0\} = \{h_1, h_2, \ldots, h_H\}$, 令 $H = |\mathcal{H}|$ 且 $h_1 < h_2 < \cdots < h_H$. 我们给出如下两个引理来确定最优的 $\boldsymbol{k}$, 证明分别见附录 A 和 B[1)].

引理1 对每个 $t \in \mathcal{H}$ 及 $i \in \{t+1, t+2, \ldots, T\}$, 有

$$f_t\left(\sum_{j=1}^{t} k_j\right) \geqslant f_i\left(\sum_{j=1}^{t} k_j\right). \tag{25}$$

引理2 对每个 $t \in \mathcal{H}$ 及 $i \in \{1, 2, \ldots, t-1\}$, 有

$$f_t\left(\sum_{j=1}^{t} k_j\right) > f_i\left(\sum_{j=1}^{t} k_j\right). \tag{26}$$

推论2 对每个 $t \in \mathcal{H}$, 有

$$f_t\left(\sum_{j=1}^{t} k_j\right) = \max_{i \in \{1, 2, \ldots, T\}} f_i\left(\sum_{j=1}^{t} k_j\right). \tag{27}$$

结合两个引理, 很容易得到推论 2. 于是我们可以在已知部分最优功率分配 $k_{t+1}, k_{t+2}, \ldots, k_T$ 后继续判断 t 是否属于 $\mathcal{H}$. 现在可以给出一些步骤来确定最优功率分配 $\boldsymbol{k}$.

Step 1. 确定 h_H: 在 $i \in \{1, 2, \ldots, T\}$ 中搜索最大化 $f_i(P)$ 的 i. 从推论 2 可得 $h_H = i$, 这是因为 $\sum_{j=1}^{h_H} k_j = \sum_{j=1}^{T} k_j = P$. 如果这样的 i 不是唯一的, 根据引理 2 应选择最小的一个.

Step 2. 按照下列步骤开启一个循环, 一一计算得到 (k_{h_m}, h_{m-1}) (从 $m = H$ 开始).

Step 3. 已知 h_m 和部分最优功率分配 $k_{h_m+1}, k_{h_m+2}, \ldots, k_T$, 如果下一个 h_{m-1} 存在, 因为等式关系 (A8) 和 $\sum_{j=1}^{h_{m-1}} k_j = \sum_{j=1}^{h_m - 1} k_j = P - \sum_{j=m}^{H} k_{h_j}$, 则有

$$f_{h_m}\left(P - \sum_{j=m}^{H} k_{h_j}\right) = f_{h_{m-1}}\left(P - \sum_{j=m}^{H} k_{h_j}\right). \tag{28}$$

1) 以下引理的证明是需要性质 1 的支撑, 在性质 1 成立时, 可以保证引理是可以推导并且成立的. 所以为了保证后续优化结果的准确性, 我们只讨论了性质 1 成立的情况. 同时性质 1 也只是引理成立的充分条件, 关于引理在性质 1 不成立时能否适用, 什么时候适用等问题还需要进行后续的相关研究.

同时, 根据引理 2 和推论 2, 可知

$$h_{m-1}=\min\left(\underset{i\in\{1,2,\ldots,T\}}{\arg\max}\left\{f_i\left(P-\sum_{j=m}^{H}k_{h_j}\right)\right\}\right). \tag{29}$$

所以为了判断下一个 h_{m-1} 是否存在, 让 k_{h_m} 在区间 $(0,P-\sum_{j=m+1}^{H}k_{h_j}]$ (区间 $(0,P]$ 如果 $m=H$) 上递增, 直到存在一个 $h_{m-1}\in\{1,2,\ldots,h_m-1\}$ 同时满足等式 (28) 和 (29). 注意, 若存在, 那么这样的 (k_{h_m},h_{m-1}) 是唯一的 (在附录 C 中证明).

Step 4. 如果在步骤 3 中, (k_{h_m},h_{m-1}) 存在且 $P-\sum_{j=m}^{H}k_{h_j}\neq 0$, 则对每个 $i\in\{h_{m-1}+1,h_{m-1}+2,\ldots,h_m-1\}$, 令 $k_i=0$. 更新参数 $m=m-1$, 返回步骤 3 继续搜索下一组 (k_{h_m},h_{m-1}). 否则, 停止循环进入下一步,

Step 5. 如果在步骤 3 中, (k_{h_m},h_{m-1}) 存在且 $P-\sum_{j=m}^{H}k_{h_j}=0$, 这说明虽然第 h_{m-1} 层是值得输入功率的, 但有限的总功率还是导致 $h_{m-1}\notin\mathcal{H}$. 如果在步骤 3 中没找到合适的 (k_{h_m},h_{m-1}), 这说明 h_{m-1} 不存在. 两种情况下都可得 $m=1$, $k_{h_m}=P-\sum_{j=m+1}^{H}k_{h_j}$ ($k_{h_m}=P$ 如果 $m=H$). 最后对每个 $i\in\{1,2,\ldots,h_m-1\}$, 令 $k_i=0$. 功率分配结束.

每组 (k_{h_m},h_{m-1}) 的唯一性保证了只有一组功率分配 $(k_1,k_2,\ldots,k_T)$ 可以满足 KKT 条件, 这意味着其最优性 [35]. 于是我们得到了优化问题 (8) 的最优解 $\{\boldsymbol{K}_t=k_t\boldsymbol{I}_\ell\}_{t=1}^{T}$, 即能够在功率限制 (3) 下, 最大化分层广播逼近中的平均可解码速率 R 的协方差分配. 基于这组解可以设计出最优的分层广播逼近策略. 我们将上述步骤总结为算法 1.

Algorithm 1 Find the optimal solution for the optimization problem (8)

Input: $\{\boldsymbol{K}_{\boldsymbol{N}_{A_t}}\}_{t=1}^{T}$, $\boldsymbol{K}_{\boldsymbol{N}_B}$, $\{p_t\}_{t=1}^{T}$, T, P, ℓ.
Initialize: $(k_1,k_2,\ldots,k_T)=(0,0,\ldots,0)$, $p=P$, $\{\boldsymbol{\lambda}_t=\mathrm{eig}(\boldsymbol{K}_{\boldsymbol{N}_{A_t}})\}_{t=1}^{T}$, $\boldsymbol{\lambda}_e=\mathrm{eig}(\boldsymbol{K}_{\boldsymbol{N}_B})$.
Define a class of functions $\{f_t(x)\}_{t=1}^{T}$ on $x\in[0,P]$ as in Definition 2;
Define a class of sets on $x\in[0,P]$: $\mathcal{F}(x)=\arg\max_{i\in\{1,2,\ldots,T\}}\{f_i(x)\}$;
while $p>0$ **do**
  $h=\min[\mathcal{F}(p)]$;
  Search $k\in(0,p]$ such that $h\in\mathcal{F}(p-k)$ and $h\neq\min[\mathcal{F}(p-k)]$;
  if k exists **then**
    Update $k_h=k$, $p=p-k$;
  else
    Update $k_h=p$, $p=0$;
  end if
end while
Output: $\{\boldsymbol{K}_t=k_t\boldsymbol{I}_\ell\}_{t=1}^{T}$.

由于性质 1, 算法 1 中的循环迭代次数 H 是会不超过 T 次的. 每次循环迭代中需要对 k_h 的值进行一维搜索, 根据之前的唯一性分析, 输出结果会随着搜索精度提高 (最小步长减少) 收敛到这组最优的功率分配. 同时, 算法 1 相比穷尽搜索法, 效率也大幅提高. 在算法 1 中, 可以采用二分法对每个 k_h 的值进行一维搜索, 整个算法的时间复杂度只有 $O(\log N)$. 相比复杂度为 $O(N^{T-1})$ 的穷尽搜索, 算法耗时大大减少.

我们分别选择了 3 组不同的 MIMO 窃听信道, 每组主信道均有 5 个可能的信道状态. 其对应的噪声协方差和信道状态概率详见表 1. 功率分配 $P\in[0,1]$ 时, 算法 1 和穷尽搜索法计算得到 R 的对比 (图 2), 可以看到二者是贴合的, 这验证了算法 1 输出的准确性.

表 1　数据组: 噪声方差及信道状态概率

Table 1　Data setting: noise variance matrices and channel state probability

	Data 1	Data 2	Data 3
$\boldsymbol{K}_{N_{A_1}}$	$\begin{bmatrix} 0.775 & -0.167 & -0.128 & 0.188 & -0.037 \\ -0.167 & 0.439 & -0.083 & 0.126 & 0.114 \\ -0.128 & -0.083 & 0.408 & -0.146 & -0.197 \\ 0.188 & 0.126 & -0.146 & 0.625 & -0.149 \\ -0.037 & 0.114 & -0.197 & -0.149 & 0.860 \end{bmatrix}$	$\begin{bmatrix} 0.579 & -0.132 & 0.195 & 0.152 & 0.024 \\ -0.132 & 0.575 & -0.151 & -0.281 & 0.130 \\ 0.195 & -0.151 & 0.301 & -0.026 & -0.093 \\ 0.152 & -0.281 & -0.026 & 0.641 & 0.116 \\ 0.024 & 0.130 & -0.093 & 0.116 & 1.002 \end{bmatrix}$	$\begin{bmatrix} 0.320 & 0.011 & 0.061 & 0.167 & -0.039 \\ 0.011 & 0.508 & -0.063 & 0.043 & -0.177 \\ 0.061 & -0.063 & 0.197 & 0.038 & 0.128 \\ 0.167 & 0.043 & 0.038 & 0.479 & 0.002 \\ -0.039 & -0.177 & 0.128 & 0.002 & 0.214 \end{bmatrix}$
$\boldsymbol{K}_{N_{A_2}}$	$\begin{bmatrix} 0.652 & -0.153 & -0.139 & -0.031 & -0.072 \\ -0.153 & 0.810 & -0.173 & 0.216 & 0.076 \\ -0.139 & -0.173 & 0.601 & -0.093 & 0.090 \\ -0.031 & 0.216 & -0.093 & 0.824 & 0.038 \\ -0.072 & 0.076 & 0.090 & 0.038 & 0.702 \end{bmatrix}$	$\begin{bmatrix} 0.816 & -0.096 & 0.100 & -0.126 & -0.058 \\ -0.096 & 0.809 & 0.141 & 0.037 & 0.135 \\ 0.100 & 0.141 & 0.906 & -0.101 & 0.041 \\ -0.126 & 0.037 & -0.101 & 0.785 & 0.045 \\ -0.058 & 0.135 & 0.041 & 0.045 & 0.725 \end{bmatrix}$	$\begin{bmatrix} 0.741 & -0.097 & -0.237 & 0.156 & 0.039 \\ -0.097 & 0.832 & -0.145 & 0.085 & 0.072 \\ -0.237 & -0.145 & 0.533 & 0.268 & 0.114 \\ 0.156 & 0.085 & 0.268 & 0.624 & -0.119 \\ 0.039 & 0.072 & 0.114 & -0.119 & 0.846 \end{bmatrix}$
$\boldsymbol{K}_{N_{A_3}}$	$\begin{bmatrix} 0.860 & -0.081 & 0.261 & 0.198 & -0.157 \\ -0.081 & 1.036 & -0.059 & -0.033 & 0.176 \\ 0.261 & -0.059 & 0.705 & -0.112 & 0.123 \\ 0.198 & -0.033 & -0.112 & 1.107 & 0.102 \\ -0.157 & 0.176 & 0.123 & 0.102 & 1.081 \end{bmatrix}$	$\begin{bmatrix} 0.919 & 0.167 & 0.145 & 0.140 & 0.082 \\ 0.167 & 1.031 & 0.084 & 0.119 & -0.204 \\ 0.145 & 0.084 & 0.801 & 0.061 & 0.000 \\ 0.140 & 0.119 & 0.061 & 0.901 & 0.121 \\ 0.082 & -0.204 & 0.000 & 0.121 & 0.938 \end{bmatrix}$	$\begin{bmatrix} 1.072 & -0.074 & -0.045 & 0.020 & -0.188 \\ -0.074 & 1.024 & -0.194 & 0.078 & -0.100 \\ -0.045 & -0.194 & 1.022 & 0.115 & -0.210 \\ 0.020 & 0.078 & 0.115 & 0.966 & 0.016 \\ -0.188 & -0.100 & -0.210 & 0.016 & 1.019 \end{bmatrix}$
$\boldsymbol{K}_{N_{A_4}}$	$\begin{bmatrix} 1.097 & -0.135 & 0.111 & 0.037 & -0.025 \\ -0.135 & 0.976 & 0.063 & -0.074 & -0.059 \\ 0.111 & 0.063 & 0.924 & -0.007 & -0.165 \\ 0.037 & -0.074 & -0.007 & 1.139 & -0.113 \\ -0.025 & -0.059 & -0.165 & -0.113 & 0.921 \end{bmatrix}$	$\begin{bmatrix} 1.045 & 0.192 & 0.020 & 0.140 & -0.040 \\ 0.192 & 0.999 & -0.158 & 0.037 & -0.112 \\ 0.020 & -0.158 & 1.129 & -0.039 & 0.017 \\ 0.140 & 0.037 & -0.039 & 1.126 & -0.096 \\ -0.040 & -0.112 & 0.017 & -0.096 & 0.991 \end{bmatrix}$	$\begin{bmatrix} 0.977 & 0.220 & -0.064 & 0.003 & 0.053 \\ 0.220 & 1.041 & 0.115 & 0.147 & -0.149 \\ -0.064 & 0.115 & 0.990 & -0.121 & 0.030 \\ 0.003 & 0.147 & -0.121 & 1.023 & -0.008 \\ 0.053 & -0.149 & 0.030 & -0.008 & 1.102 \end{bmatrix}$
$\boldsymbol{K}_{N_{A_5}}$	$\begin{bmatrix} 1.262 & 0.050 & -0.030 & -0.043 & -0.034 \\ 0.050 & 1.223 & -0.043 & 0.002 & 0.015 \\ -0.030 & -0.043 & 1.265 & -0.033 & 0.024 \\ -0.043 & 0.002 & -0.033 & 1.328 & -0.004 \\ -0.034 & 0.015 & 0.024 & -0.004 & 1.175 \end{bmatrix}$	$\begin{bmatrix} 1.226 & 0.056 & -0.140 & 0.064 & 0.055 \\ 0.056 & 1.131 & 0.197 & -0.074 & 0.116 \\ -0.140 & 0.197 & 1.183 & 0.070 & -0.044 \\ 0.064 & -0.074 & 0.070 & 1.267 & -0.029 \\ 0.055 & 0.116 & -0.044 & -0.029 & 1.168 \end{bmatrix}$	$\begin{bmatrix} 1.339 & -0.180 & 0.018 & -0.076 & -0.048 \\ -0.180 & 1.392 & -0.010 & -0.050 & 0.040 \\ 0.018 & -0.010 & 1.416 & 0.155 & -0.044 \\ -0.076 & -0.050 & 0.155 & 1.410 & 0.089 \\ -0.048 & 0.040 & -0.044 & 0.089 & 1.448 \end{bmatrix}$
$\boldsymbol{K}_{N_B}$	$\begin{bmatrix} 1.492 & -0.039 & 0.101 & -0.031 & -0.062 \\ -0.039 & 1.489 & -0.040 & 0.134 & 0.030 \\ 0.101 & -0.040 & 1.513 & -0.009 & -0.017 \\ -0.031 & 0.134 & -0.009 & 1.619 & -0.004 \\ -0.062 & 0.030 & -0.017 & -0.004 & 1.595 \end{bmatrix}$	$\begin{bmatrix} 1.451 & 0.096 & -0.069 & 0.050 & 0.048 \\ 0.096 & 1.365 & 0.090 & 0.069 & -0.170 \\ -0.069 & 0.090 & 1.368 & -0.064 & 0.094 \\ 0.050 & 0.069 & -0.064 & 1.508 & 0.006 \\ 0.048 & -0.170 & 0.094 & 0.006 & 1.438 \end{bmatrix}$	$\begin{bmatrix} 1.495 & -0.059 & 0.034 & -0.046 & 0.082 \\ -0.059 & 1.430 & -0.023 & -0.067 & 0.008 \\ 0.034 & -0.023 & 1.611 & 0.054 & -0.018 \\ -0.046 & -0.067 & 0.054 & 1.378 & 0.023 \\ 0.082 & 0.008 & -0.018 & 0.023 & 1.525 \end{bmatrix}$
Pr	$[0.238\ 0.143\ 0.284\ 0.209\ 0.125]$	$[0.035\ 0.384\ 0.306\ 0.181\ 0.093]$	$[0.049\ 0.166\ 0.326\ 0.215\ 0.244]$

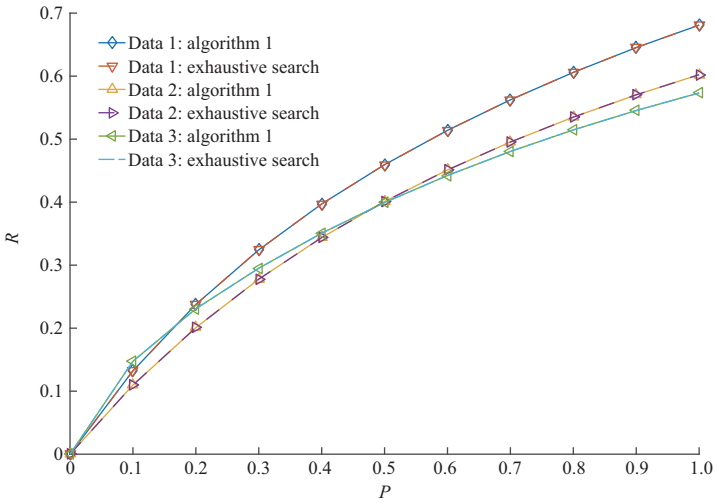

图 2　(网络版彩图) 算法输出对比

Figure 2　(Color online) Rate comparison

5　总结

本文研究了衰落高斯 MIMO 窃听信道中物理层安全的编码方案设计与优化. 该编码方案具有一定的鲁棒性, 在对 CSI 情况未知的情况下, 仍可以进行信息的安全传输, 从而实现系统的内生安全. 我们引入弱超多数化对每个可能的通道状态下噪声协方差的特征值进行排序, 从而设计了基于叠加编码的分层广播逼近方案, 并对该方案的参数进行优化, 使得码率的数学期望最大化. 该方案覆盖了部分

先前相关工作的结论. 例如在标量信道中, 该模型将退化为文献 [22] 中具有离散信道状态的标量衰落窃听信道, 此时我们的算法可以提供最优的功率分配方案.

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. Sci China Inf Sci, 2021, 64: 110301

2 Bloch M, Barros J, Rodrigues M R D, et al. Wireless information-theoretic security. IEEE Trans Inform Theory, 2008, 54: 2515–2534

3 Liang Y, Poor H V, Shamai S. Information Theoretic Security. Boston: Now Publishers Inc., 2009

4 Maurer U. Information-theoretic cryptography. In: Proceedings of Annual International Cryptology Conference, 1999. 47–65

5 Yoshizawa T, Baskaran S B M, Kunz A. Overview of 5G URLLC system and security aspects in 3GPP. In: Proceedings of IEEE Conference on Standards for Communications and Networking (CSCN), 2019

6 Chen R Q, Li C H, Yan S H, et al. Physical layer security for ultra-reliable and low-latency communications. IEEE Wirel Commun, 2019, 26: 6–11

7 Shannon C E. Communication theory of secrecy systems*. Bell Syst Technical J, 1949, 28: 656–715

8 Leung-Yan-Cheong S, Hellman M. The Gaussian wire-tap channel. IEEE Trans Inform Theory, 1978, 24: 451–456

9 Weingarten H, Steinberg Y, Shamai S S. The capacity region of the gaussian multiple-input multiple-output broadcast channel. IEEE Trans Inform Theory, 2006, 52: 3936–3964

10 Liang Y, Kramer G, Poor H V, et al. Compound wiretap channels. J Wirel Commun Netw, 2009, 2009: 142374

11 Ekrem E, Ulukus S. The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel. IEEE Trans Inform Theory, 2011, 57: 2083–2114

12 Ekrem E, Ulukus S. Secrecy capacity of a class of broadcast channels with an eavesdropper. EURASIP J Wirel Commun Netw, 2009, 2009: 824235

13 Oggier F, Hassibi B. The secrecy capacity of the MIMO wiretap channel. IEEE Trans Inform Theory, 2011, 57: 4961–4972

14 Li J, Petropulu A. Transmitter optimization for achieving secrecy capacity in Gaussian MIMO wiretap channels. 2009. ArXiv:0909.2622

15 Khisti A, Wornell G W. Secure transmission with multiple antennas–Part II: the MIMOME wiretap channel. IEEE Trans Inform Theory, 2010, 56: 5515–5532

16 Liu R H, Liu T, Poor H V, et al. Multiple-input multiple-output Gaussian broadcast channels with confidential messages. IEEE Trans Inform Theory, 2010, 56: 4215–4227

17 Khisti A, Wornell G, Wiesel A, et al. On the Gaussian MIMO wiretap channel. In: Proceedings of IEEE International Symposium on Information Theory, 2007. 2471–2475

18 Bustin R, Liu R H, Poor H V, et al. An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel. J Wirel Com Netw, 2009, 2009: 370970

19 Diggavi S N, Cover T M. The worst additive noise under a covariance constraint. IEEE Trans Inform Theory, 2001, 47: 3072–3081

20 Liu R H, Liu T, Poor H V, et al. A vector generalization of costa's entropy-power inequality with applications. IEEE Trans Inform Theory, 2010, 56: 1865–1879

21 Biglieri E, Proakis J, Shamai S. Fading channels: information-theoretic and communications aspects. IEEE Trans Inform Theory, 1998, 44: 2619–2692

22 Liang Y B, Lai L F, Poor H V, et al. A broadcast approach for fading wiretap channels. IEEE Trans Inform Theory, 2014, 60: 842–858

23 Shafiee S, Ulukus S. Achievable rates in Gaussian MISO channels with secrecy constraints. In: Proceedings of IEEE International Symposium on Information Theory, 2007. 2466–2470

24 Gopala P K, Lai L F, El Gamal H. On the secrecy capacity of fading channels. IEEE Trans Inform Theory, 2008, 54: 4687–4698

25 Khisti A, Tchamkerten A, Wornell G W. Secure broadcasting over fading channels. IEEE Trans Inform Theory, 2008,

54: 2453–2469
26 Shamai S, Steiner A. A broadcast approach for a single-user slowly fading MIMO channel. IEEE Trans Inform Theory, 2003, 49: 2617–2635
27 Tajer A, Steiner A, Shamai S. The broadcast approach in communication networks. Entropy, 2021, 23: 120
28 El Gamal A, Kim Y H. Lecture notes on network information theory. 2010. ArXiv:1001.3404
29 Jindal N, Rhee W, Vishwanath S, et al. Sum power iterative water-filling for multi-antenna Gaussian broadcast channels. IEEE Trans Inform Theory, 2005, 51: 1570–1580
30 Kobayashi M, Caire G. An iterative water-filling algorithm for maximum weighted sum-rate of Gaussian MIMO-BC. IEEE J Sel Areas Commun, 2006, 24: 1640–1646
31 Xing C W, Jing Y D, Wang S, et al. New viewpoint and algorithms for water-filling solutions in wireless communications. IEEE Trans Signal Process, 2020, 68: 1618–1634
32 Marshall A W, Olkin I, Arnold B C. Inequalities: Theory of Majorization and Its Applications. New York: Academic Press, 1979
33 Wyner A D. The wire-tap channel. Bell Syst Technical J, 1975, 54: 1355–1387
34 Csiszár I, Korner J. Broadcast channels with confidential messages. IEEE Trans Inform Theory, 1978, 24: 339–348
35 Chen B L. Optimization Theory and Algorithm. Beijing: Tsinghua University Press, 2005 [陈宝林. 最优化理论与算法. 北京: 清华大学出版社, 2005]

附录 A 引理 1 证明

这里先展开式 (20)

$$\frac{\partial R}{\partial k_t} - w + v_t = 0, \quad t = 1, 2, \ldots, T, \tag{A1}$$

其中

$$\frac{\partial R}{\partial k_t} = \frac{\partial \sum_{j=1}^{T} (p_j \cdot \sum_{i=j}^{T} R_i)}{\partial k_t} = \sum_{i=1}^{T} \left(\frac{\partial R_i}{\partial k_t} \cdot \sum_{j=1}^{i} p_j \right), \tag{A2}$$

$$\frac{\partial R_i}{\partial k_t} = \begin{cases} 0, & t > i, \\ \dfrac{1}{2} \left(\displaystyle\sum_{r=1}^{\ell} \frac{1}{\sum_{j=1}^{i} k_j + \lambda_{i,r}} - \sum_{r=1}^{\ell} \frac{1}{\sum_{j=1}^{i} k_j + \lambda_{e,r}} \right), & t = i, \\ \dfrac{1}{2} \displaystyle\sum_{r=1}^{\ell} \left(\frac{1}{\sum_{j=1}^{i} k_j + \lambda_{i,r}} - \frac{1}{\sum_{j=1}^{i-1} k_j + \lambda_{i,r}} \right) - \frac{1}{2} \sum_{r=1}^{\ell} \left(\frac{1}{\sum_{j=1}^{i} k_j + \lambda_{e,r}} - \frac{1}{\sum_{j=1}^{i-1} k_j + \lambda_{e,r}} \right), & t < i. \end{cases} \tag{A3}$$

令 $t = h_n \in \mathcal{H}$ 和 $n \in \{1, 2, \ldots, H\}$, 我们首先证明式 (25) 在 $i \in \{t+1, t+2, \ldots, h_{n+1} - 1\}$ 时成立 (这里设置 $h_{H+1} - 1 = T$). 联立式 (A1) 和 (A2),

$$w - v_t = \frac{\partial R}{\partial k_t} = \sum_{m=1}^{T} \left(\frac{\partial R_m}{\partial k_t} \sum_{j=1}^{m} p_j \right) \overset{\text{(a)}}{=} \sum_{m=n}^{H} \left(\frac{\partial R_{h_m}}{\partial k_t} \sum_{j=1}^{h_m} p_j \right), \tag{A4}$$

这里 (a) 是因为在 $k_j = 0$ 且 $t < j$ 时 $\partial R_j / \partial k_t = 0$. 同时, 因为 $t \in \mathcal{H}$ 所以 $k_t > 0$, 由式 (23) 可推得 $v_t = 0$, 代回到上式有

$$w = \sum_{m=n}^{H} \left(\frac{\partial R_{h_m}}{\partial k_t} \cdot \sum_{j=1}^{h_m} p_j \right). \tag{A5}$$

对任意 $i \in \{t+1, t+2, \ldots, h_{n+1} - 1\}$, 类似可得

$$w - v_i = \frac{\partial R}{\partial k_i} = \sum_{m=n+1}^{H} \left(\frac{\partial R_{h_m}}{\partial k_i} \cdot \sum_{j=1}^{h_m} p_j \right) + \frac{\partial R_i}{\partial k_i} \cdot \sum_{j=1}^{i} p_j. \tag{A6}$$

将式 (A5) 代入, 可推得

$$v_i = \frac{\partial R_t}{\partial k_t} \sum_{j=1}^{t} p_j - \frac{\partial R_i}{\partial k_i} \sum_{j=1}^{i} p_j = f_t \left(\sum_{j=1}^{t} k_j \right) - f_i \left(\sum_{j=1}^{i} k_j \right) \overset{\text{(a)}}{=} f_t \left(\sum_{j=1}^{t} k_j \right) - f_i \left(\sum_{j=1}^{t} k_j \right), \tag{A7}$$

这里 (a) 是因为在 $j\in\{t+1,t+2,\dots,i\}$ 时有 $k_j=0$. 又因为 $v_i\geqslant 0$, 可证明式 (25) 对每个 $i\in\{t+1,t+2,\dots,h_{n+1}-1\}$ 都成立.

接着考虑 $i=h_{n+1}$ 时 (如果 $n\neq H$), 类似可得 $w=\sum_{m=n+1}^{H}(\frac{\partial R_{h_m}}{\partial k_i}\cdot\sum_{j=1}^{h_m}p_j)$, 与式 (A5) 相减,

$$\begin{aligned}0=&\sum_{m=n}^{H}\left(\frac{\partial R_{h_m}}{\partial k_t}\cdot\sum_{j=1}^{h_m}p_j\right)-\sum_{m=n+1}^{H}\left(\frac{\partial R_{h_m}}{\partial k_i}\cdot\sum_{j=1}^{h_m}p_j\right)\overset{\text{(a)}}{=}\frac{\partial R_t}{\partial k_t}\cdot\sum_{j=1}^{t}p_j+\left(\frac{\partial R_i}{\partial k_t}-\frac{\partial R_i}{\partial k_i}\right)\cdot\sum_{j=1}^{i}p_j\\=&f_t\left(\sum_{j=1}^{t}k_j\right)-f_i\left(\sum_{j=1}^{i-1}k_j\right)\overset{\text{(b)}}{=}f_t\left(\sum_{j=1}^{t}k_j\right)-f_i\left(\sum_{j=1}^{t}k_j\right),\end{aligned}\tag{A8}$$

这里 (a) 是因为 i 固定时, $\partial R_i/\partial k_t$ 对每个 $t<i$ 都相等. 同时 (b) 是因为在 $j\in\{t+1,t+2,\dots,i-1\}$ 时 $k_j=0$. 这证明了在 $i=h_{n+1}$ 时, 式 (25) 成立, 且等号成立.

有了这些性质, 可以使用归纳法来证明引理 1. 对于 $t=h_H$, 已经证明了式 (25) 对每个 $i\in\{t+1,t+2,\dots,T\}$ 成立. 接下来, 假设对于 $t=h_n$, 式 (25) 对每个 $i\in\{t+1,t+2,\dots,T\}$ 成立. 继续考虑 $t=h_{n-1}$, 已经证明了式 (25) 对每个 $i\in\{t+1,t+2,\dots,h_n\}$ 成立. 至于剩下的每个 $i\in\{h_n+1,h_n+2,\dots,T\}$, 根据假设已知

$$f_{h_n}\left(\sum_{j=1}^{h_n}k_j\right)\geqslant f_i\left(\sum_{j=1}^{h_n}k_j\right)\tag{A9}$$

成立. 于是根据性质 1 和式 (A8) 有

$$f_{h_{n-1}}\left(\sum_{j=1}^{h_{n-1}}k_j\right)=f_{h_n}\left(\sum_{j=1}^{h_{n-1}}k_j\right)>f_i\left(\sum_{j=1}^{h_{n-1}}k_j\right).\tag{A10}$$

这证明了式 (25) 对每个 $i\in\{t+1,t+2,\dots,T\}$ 都成立. 归纳法证毕.

附录 B 引理 2 证明

我们用归纳法证明引理 2. 当 $t=h_1$, 对于每个 $i\in\{1,2,\dots,h_1-1\}$,

$$w-v_i=\frac{\partial R}{\partial k_i}=\sum_{m=1}^{H}\left(\frac{\partial R_{h_m}}{\partial k_i}\cdot\sum_{j=1}^{h_m}p_j\right)+\frac{\partial R_i}{\partial k_i}\cdot\sum_{j=1}^{i}p_j.\tag{B1}$$

将式 (A5) 代入,

$$v_i=\frac{\partial R_t}{\partial k_t}\sum_{j=1}^{t}p_j-\frac{\partial R_t}{\partial k_i}\sum_{j=1}^{t}p_j-\frac{\partial R_i}{\partial k_i}\sum_{j=1}^{i}p_j=f_t\left(\sum_{j=1}^{t-1}k_j\right)-f_i\left(\sum_{j=1}^{i}k_j\right)\overset{\text{(a)}}{=}f_t\left(0\right)-f_i\left(0\right)\geqslant 0,\tag{B2}$$

这里 (a) 是因为当 $j\in\{1,2,\dots,t-1\}$ 有 $k_j=0$. 接着用反证法证明式 (26) 对 $t=h_1$ 成立. 假设命题错误, 一定存在 $i\in\{1,2,\dots,t-1\}$ 使 $f_t(\sum_{j=1}^{t}k_j)\leqslant f_i(\sum_{j=1}^{t}k_j)$. 于是因为 $\sum_{j=1}^{t}k_j=k_t>0$, 根据性质 1, 有 $f_t(0)<f_i(0)$. 这和式 (B2) 矛盾, 所以式 (26) 在 $t=h_1$ 时成立.

然后, 假设当 $t=h_{n-1}\in\mathcal{H}$, 式 (26) 对每个 $i\in\{1,2,\dots,t-1\}$ 都成立. 继续考虑 $t=h_n$ 的情况, 依旧使用反证法, 如果式 (26) 对 t 不成立, 一定存在 $i\in\{1,2,\dots,h_n-1\}$ 使 $f_t(\sum_{j=1}^{t}k_j)\leqslant f_i(\sum_{j=1}^{t}k_j)$. 又因为 $\sum_{j=1}^{h_{n-1}}k_j<\sum_{j=1}^{t}k_j$, 根据性质 1 有

$$f_t\left(\sum_{j=1}^{h_{n-1}}k_j\right)<f_i\left(\sum_{j=1}^{h_{n-1}}k_j\right).\tag{B3}$$

但是, 根据引理 1 和递归假设, 对任意 $i\in\{1,2,\dots,h_n-1\}$ 要有

$$f_t\left(\sum_{j=1}^{h_{n-1}}k_j\right)=f_{h_{n-1}}\left(\sum_{j=1}^{h_{n-1}}k_j\right)\geqslant f_i\left(\sum_{j=1}^{h_{n-1}}k_j\right),\tag{B4}$$

这与式 (B3) 相矛盾. 所以式 (26) 在 $t=h_n$ 时也成立. 归纳法证明引理 2 完毕.

附录 C (k_{h_m}, h_{m-1}) 唯一性证明

已知 h_m 和部分最优功率分配 $k_{h_m+1}, k_{h_m+2}, \ldots, k_T$, 假设存在两个不同的组合 (k_{h_m}, h_{m-1}) 和 (k'_{h_m}, h'_{m-1}) 满足式 (28) 和 (29). 不失一般性, 假设 $k_{h_m} < k'_{h_m}$.

令 $x_1 = P - \sum_{j=m}^{H} k_{h_j}$, 由式 (28) 有 $f_{h_m}(x_1) = f_{h_{m-1}}(x_1)$. 再令 $x_2 = P - \sum_{j=m+1}^{H} k_{h_j} - k'_{h_m}$ ($x_2 = P - k'_{h_m}$ 如果 $m = H$), 由性质 1 以及 $x_1 > x_2 \geqslant 0$ 有 $f_{h_{m-1}}(x_2) > f_{h_m}(x_2)$. 同时, 由式 (28) 有 $f_{h'_{m-1}}(x_2) = f_{h_m}(x_2)$, 所以 $f_{h_{m-1}}(x_2) > f_{h'_{m-1}}(x_2)$. 这与 (k'_{h_m}, h'_{m-1}) 满足式 (29) 相矛盾. 证明了 (k_{h_m}, h_{m-1}) 应该是唯一的.

On the optimization problem in fading Gaussian MIMO wiretap channels

Kangning MA[1], Yinfei XU[2], Shuo SHAO[1*] & Yue WU[1*]

1. *School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai* 200240*, China*;
2. *School of Information Science and Engineering, Southeast University, Nanjing* 211189*, China*
* Corresponding author. E-mail: shuoshao@sjtu.edu.cn, wuyue@sjtu.edu.cn

Abstract Self-adaptive physical layer security technology is a major challenge for achieving anti-quantum endogenous security in 6G communication. We consider the maximum average decodable rate for a non-degraded Gaussian MIMO wiretap channel, whose the main channel suffers fading. We adopt the layered broadcast approach based on superposition coding to design and optimize the achievable and secrecy scheme, when the eigenvalues of the noise covariance in each channel state can be ordered by the weak supermajorization. With the scheme, the maximum average decodable rate can be characterized as a non-convex optimization problem of a log function. We propose an algorithm which can output the optimal solution for the optimization and thus help to obtain the optimal scheme in the scalar case and most MIMO cases.

Keywords Gaussian MIMO wiretap broadcast channel, fading channel, broadcast approach, superposition coding, endogenous security