

MIMO异构网络中一种基于人工噪声的抗主动窃听者的鲁棒安全传输方案

张波^① 黄开枝*^① 林胜斌^② 易鸣^① 陈亚军^①

^①(战略支援部队信息工程大学 郑州 450001)

^②(陆军工程大学通信士官学校 重庆 400035)

摘要: 为保证MIMO异构网络面临多天线主动窃听时的安全性, 该文提出一种基于人工噪声的抗主动窃听者的鲁棒安全传输方案。首先, 考虑窃听者发送上行导频干扰的情形, 研究了其发送的上行导频干扰对合法用户信道估计的影响。随后, 基于信道估计结果对宏基站、微基站的下行数据与噪声信号的预编码矩阵进行设计, 并推导了此种情形下系统安全速率的表达式。然后, 以系统安全速率最大化为目标对基站的下行数据与噪声信号的发送功率进行优化设计, 并提出一种基于1维线性搜索的求解方法。进一步地, 考虑窃听者在发送上行导频干扰后, 继而发送噪声干扰用户下行通信的情形, 提出一种基于离散零和博弈方法来获取最优的发送功率设计。仿真结果验证了所提方案的安全性和鲁棒性。

关键词: 异构网络; 多输入多输出; 物理层安全; 主动窃听

中图分类号: TN915

文献标识码: A

文章编号: 1009-5896(2020)09-2186-08

DOI: 10.11999/5EIT190649

A Robust Secure Transmission Scheme Based on Artificial Noise for Resisting Active Eavesdropper in MIMO Heterogeneous Networks

ZHANG Bo^① HUANG Kaizhi^① LIN Shengbin^② YI Ming^① CHEN Yajun^①

^①(Information Engineering University, Zhengzhou 450001, China)

^②(Communication Sergeant School, Army Engineering University, Chongqing 400035, China)

Abstract: To ensure the security of MIMO heterogeneous networks while facing the active multi-antenna eavesdropping, a robust secure transmission scheme based on artificial noise is proposed. Firstly, considering that the eavesdropper sends uplink pilot interference signal, the influence of uplink pilot interference on the channel estimation of legitimate users is studied. Then, based on the channel estimation results, the precoding matrix of downlink data and noise signals of macro base station and micro base station are designed, respectively. The expression of system security rate in this case is derived; After that, for maximizing the system security rate, the transmission power of downlink data and noise signal of base station are optimized, and a solution method based on one-dimensional linear search is proposed. Furthermore, considering the situation that the eavesdropper sends the uplink pilot interference and then sends the noise to interfere with the downlink communication of the legitimate user, a discrete zero-sum game method is proposed to obtain the optimal transmission power design. The simulation results verify the security and robustness of the proposed scheme.

Key words: Heterogeneous network; Multiple Input Multiple Output (MIMO); Physical layer security; Active eavesdropping

1 引言

随着5G的脚步日趋临近, 异构网络作为一种

能够满足5G网络无缝覆盖、高吞吐量需求的有效手段, 备受瞩目^[1]。然而, 由于无线信道具有天然的广播性, 使得其很易遭受非法窃听者(Eavesdropper, Eve)的窃听、干扰、甚至攻击, 异构网络架构的开放性进一步加剧了这种情形。作为传统高层加密手段的补充, 近年来出现的物理层安全技术^[2,3]利用无线信道的物理层特性探索解决通信安全问题, 越来越受到业界的广泛关注。

收稿日期: 2019-08-28; 改回日期: 2020-06-08; 网络出版: 2020-07-13

*通信作者: 黄开枝 zb100403@126.com.cn

基金项目: 国家自然科学基金(61871404, 61701538)

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

目前, 业界对异构网络的物理层安全研究正在如火如荼地进行着, 且成果颇丰^[4-13]。具体而言, 考虑Eve采取被动窃听方式获取私密信息的情形, 文献[4]对基于人工噪声辅助的异构网络的物理层安全进行研究, 提出一种基于安全门限的接入策略。类似地, 文献[5,6]分别对利用多点协作传输、全双工中继辅助方法提高异构网络的安全性能进行了探讨。与文献[4-6]关注于网络的下行通信安全不同, 文献[7]对异构网络的上行安全性能进行研究。可以注意到, 上述文献[4-7]均集中于对异构网络的物理层安全性能分析, 相关成果可为未来网络结构优化及参数设计提供理论依据和指导。基于此, 文献[8-10]进一步对如何优化、设计异构网络参数以达到系统安全性能的最优进行了研究。具体而言, 文献[8,9]采用基站间协作调度策略, 分别对宏基站(Macro Base Station, MBS)、微基站(Femto Base Station, FBS)间的协作波束成形技术展开了研究。在此基础上, 文献[10]综合考虑安全通信与绿色通信的融合, 进一步对通过基站协作波束成形以最大化系统安全能量效率展开了研究。综合上述分析可知, 目前针对异构网络的物理层安全研究均集中在Eve仅进行被动窃听的情形, 且所用的提升系统安全性的方法大多为波束成形或人工噪声。然而, 无论是波束成形还是人工噪声方法均需要发送端事先获取合法收发端通信之间的信道状态信息(Channel State Information, CSI)。当Eve采取主动窃听方式时, 可发送导频干扰信号干扰合法信道估计过程; 同时, Eve也可在下行通信过程中发送干扰信号从而恶化合法接收方的接收性能。此时, 系统安全将面临严重的威胁, 而目前对Eve采取主动窃听方式下的研究^[11,12]均集中在传统的单层网络或少数通信节点场景, 针对异构网络的相关研究却鲜有人问津; 而且, 由于异构网络架构与传统单层网络架构存在着很大不同, 现有单层网络中抵御主动窃听的相关研究成果无法直接适用于其节点数目众多、层间干扰复杂的场景。

针对上述问题, 本文对异构网络面临主动窃听情形下的物理层安全进行研究, 并提出一种基于人工噪声的抗主动窃听者的鲁棒安全传输方案。具体而言, 考虑一个双层的基于时分双工(Time Division Duplexing, TDD)多输入输出(Multiple Input Multiple Out, MIMO)异构网络, 网络中存在的多天线Eve可能采取以下两种主动窃听方式: (1)上行导频攻击, Eve发送导频干扰信号干扰MU与MBS之间的信道估计过程; (2)上行导频与下行噪声干扰联

合攻击, Eve不仅发送上行导频干扰信号, 进一步可发送噪声信号干扰MU的下行通信过程, 且Eve可以对上行导频与下行噪声干扰信号的发送功率分配进行优化以增强其窃听性能。针对Eve的上述两种主动窃听方式, 首先对Eve发送的上行导频干扰对信道估计的影响进行研究, 发现上行信道估计是MU主信道、MU与FU间干扰信道和Eve窃听信道的线性相加; 随后, 基于信道估计结果设计MBS和FBS的下行数据与噪声信号的预编码矩阵, 并推导出系统安全速率的表达式; 最后, 针对上述两种主动窃听情形下的系统安全速率最大化问题进行研究, 并分别提出一种基于1维线性搜索和离散零和博弈的方法来获取最优的MBS下行数据与噪声信号的发送功率设计。仿真结果验证了所提方案的安全性和鲁棒性。

2 系统模型

考虑一个双层的基于TDD的MIMO异构网络: 在1个MBS覆盖范围内分布着1个FBS, MBS和FBS复用相同的上、下行频谱资源分别与1个MU和FU进行上行信道估计和下行数据传输^[11]。同时, 网络中存在1个恶意Eve试图窃听MBS发送给MU的下行私密信息。而且, Eve为提升自身的窃听性能, 可能采取以下两种主动窃听方式: (1)上行导频攻击, 即在MBS与MU之间进行上行信道估计的过程中, Eve用其全部的发送功率发送上行导频干扰信号, 使MBS与MU之间的信道估计矢量与实际值存在很大偏差, 从而MBS发送给MU的下行私密信息泄露给Eve的机会增大; (2)上行导频与下行噪声干扰联合攻击, 即Eve利用其部分发送功率发送上行导频干扰信号, 进一步在MBS向MU发送下行数据的过程中用剩余的功率发送噪声信号干扰其下行通信过程, 且Eve可以对上行导频与下行噪声干扰信号功率分配进行优化^[12]。假设MBS, FBS及Eve的天线数目分别为 N_M , N_F , N_E , 合法用户(MU, FU)的天线数目为 N_U , $N_M > N_U \geq 2$, $N_F > N_U \geq 2$, $N_E \geq N_U \geq 2$; MBS, FBS, MU, FU和Eve总发送功率分别为 P_M , P_F , P_{MU} , P_{FU} 和 P_E 。

2.1 上行信道估计

在信道估计过程中, 假设Eve已经获知MBS发送给MU的导频序列, 并采用与MU相同的天线数发送上行导频干扰信号, 则MBS的上行接收信号可以表示为

$$\mathbf{y}_{\text{MBS}} = \sqrt{P_{\text{MU}}\beta_{\text{MUM}}}\mathbf{H}_{\text{MUM}}\mathbf{x}_{\text{P}} + \sqrt{P_{\text{FU}}\beta_{\text{FUM}}}\mathbf{H}_{\text{FUM}}\mathbf{x}_{\text{P}} + \sqrt{P_{\text{E}}\beta_{\text{EM}}}\mathbf{H}_{\text{EM}}\mathbf{x}_{\text{P}} + \mathbf{n}_{\text{MBS}} \quad (1)$$

其中, P_{MU} , P_{FU} 和 P_{Ep} 分别为MU, FU和Eve发送上行导频信号的功率, 当Eve采取第1种主动窃听方式时, $P_{\text{Ep}}=P_{\text{E}}$, 否则 $P_{\text{Ep}} \leq P_{\text{E}}$; $\sqrt{\beta_{\text{MUM}}}$, $\sqrt{\beta_{\text{FUM}}}$ 和 $\sqrt{\beta_{\text{EM}}}$ 分别为MU, FU, Eve至MBS的大尺度衰落系数, 即 $\sqrt{\beta_{\text{MUM}}} = \kappa(d_{\text{MUM}}/d_0)^{-\alpha}$, $\sqrt{\beta_{\text{FUM}}} = \kappa(d_{\text{FUM}}/d_0)^{-\alpha}$, $\sqrt{\beta_{\text{EM}}} = \kappa(d_{\text{EM}}/d_0)^{-\alpha}$, 其中 d_{MUM} , d_{FUM} , d_{EM} 及 d_0 分别为MU, FU, Eve至MBS之间的距离及参考距离, α 和 κ 为路径损耗常数; $\mathbf{H}_{\text{MUM}} \in \mathbb{C}^{N_{\text{M}} \times N_{\text{U}}}$, $\mathbf{H}_{\text{FUM}} \in \mathbb{C}^{N_{\text{M}} \times N_{\text{U}}}$, $\mathbf{H}_{\text{EM}} \in \mathbb{C}^{N_{\text{M}} \times N_{\text{U}}}$ 分别表示MU, FU, Eve和MBS之间的上行小尺度块衰落矩阵, 假设其中的每个参数均服从均值为0、方差为1的复高斯分布, 即 $\mathcal{CN}(0, 1)$; $\mathbf{x}_{\text{p}} \in \mathbb{C}^{N_{\text{U}} \times 1}$ 为发送的上行归一化导频信号, $\mathbf{x}_{\text{p}}\mathbf{x}_{\text{p}}^{\text{H}} = \mathbf{I}$; $\mathbf{n}_{\text{MBS}} \in \mathbb{C}^{N_{\text{M}} \times 1}$ 是MBS处的加性复高斯白噪声矩阵, $\mathbf{n}_{\text{MBS}} \sim \mathcal{CN}(0, \sigma_{\text{MBS}}^2)$ 。同时, 根据信道互易性易知 $\mathbf{H}_{\text{MUM}} = \mathbf{H}_{\text{MMU}}^{\text{T}}$, $\mathbf{H}_{\text{FUM}} = \mathbf{H}_{\text{MFU}}^{\text{T}}$, $\mathbf{H}_{\text{EM}} = \mathbf{H}_{\text{ME}}^{\text{T}}$, 其中 $\mathbf{H}_{\text{MMU}} \in \mathbb{C}^{N_{\text{U}} \times N_{\text{M}}}$, $\mathbf{H}_{\text{MFU}} \in \mathbb{C}^{N_{\text{U}} \times N_{\text{M}}}$, $\mathbf{H}_{\text{ME}} \in \mathbb{C}^{N_{\text{U}} \times N_{\text{M}}}$ 分别为MBS至MU, FU和Eve的下行小尺度块衰落矩阵。

类似地, FBS的上行接收信号可以表示为

$$\mathbf{y}_{\text{FBS}} = \sqrt{P_{\text{FU}}\beta_{\text{FUF}}}\mathbf{H}_{\text{FUF}}\mathbf{x}_{\text{p}} + \sqrt{P_{\text{MU}}\beta_{\text{MUF}}}\mathbf{H}_{\text{MUF}}\mathbf{x}_{\text{p}} + \sqrt{P_{\text{Ep}}\beta_{\text{EF}}}\mathbf{H}_{\text{EF}}\mathbf{x}_{\text{p}} + \mathbf{n}_{\text{FBS}} \quad (2)$$

其中, $\sqrt{\beta_{\text{FUF}}}$, $\sqrt{\beta_{\text{MUF}}}$, $\sqrt{\beta_{\text{EF}}}$ 分别为MU, FU, Eve至FBS的大尺度衰落系数; $\mathbf{H}_{\text{FUF}} \in \mathbb{C}^{N_{\text{F}} \times N_{\text{U}}}$, $\mathbf{H}_{\text{MUF}} \in \mathbb{C}^{N_{\text{F}} \times N_{\text{U}}}$, $\mathbf{H}_{\text{EF}} \in \mathbb{C}^{N_{\text{F}} \times N_{\text{U}}}$ 分别表示FU, MU, Eve至FBS之间的小尺度块衰落矩阵; $\mathbf{n}_{\text{FBS}} \in \mathbb{C}^{N_{\text{F}} \times 1}$ 是FBS处的加性复高斯白噪声矩阵, $\mathbf{n}_{\text{FBS}} \sim \mathcal{CN}(0, \sigma_{\text{FBS}}^2)$ 。

假设MBS和FBS可以获知MU和FU的上行发送功率和接收信号的总功率, 且利用线性最小均方误差(Minimum Mean Square Error, MMSE)算法进行信道估计, 则MBS与MU之间的信道 \mathbf{H}_{MUM} 的估计结果为

$$\hat{\mathbf{H}}_{\text{MUM}} = \frac{P_{\text{MU}}\beta_{\text{MUM}}\mathbf{H}_{\text{MUM}}}{P_{\text{MU}}\beta_{\text{MUM}} + P_{\text{FU}}\beta_{\text{FUM}} + P_{\text{Ep}}\beta_{\text{EM}} + \sigma_{\text{MBS}}^2} + \frac{\sqrt{P_{\text{MU}}\beta_{\text{MUM}}P_{\text{Ep}}\beta_{\text{EM}}}\mathbf{H}_{\text{EM}}}{P_{\text{MU}}\beta_{\text{MUM}} + P_{\text{FU}}\beta_{\text{FUM}} + P_{\text{Ep}}\beta_{\text{EM}} + \sigma_{\text{MBS}}^2} + \frac{\sqrt{P_{\text{MU}}\beta_{\text{MUM}}P_{\text{FU}}\beta_{\text{FUM}}}\mathbf{H}_{\text{FUM}}}{P_{\text{MU}}\beta_{\text{MUM}} + P_{\text{FU}}\beta_{\text{FUM}} + P_{\text{Ep}}\beta_{\text{EM}} + \sigma_{\text{MBS}}^2} + \frac{\sqrt{P_{\text{MU}}\beta_{\text{MUM}}}\mathbf{n}_{\text{MBS}}\mathbf{x}_{\text{p}}^{\text{H}}}{P_{\text{MU}}\beta_{\text{MUM}} + P_{\text{FU}}\beta_{\text{FUM}} + P_{\text{Ep}}\beta_{\text{EM}} + \sigma_{\text{MBS}}^2} \quad (3)$$

分析式(3)可知, MBS与MU之间的信道估计结果会受到Eve和FU导频干扰的显著影响。该估计值

是主信道 \mathbf{H}_{MUM} 、干扰信道 \mathbf{H}_{FUM} 和窃听信道 \mathbf{H}_{EM} 的线性相加, 相应的加权系数均与其发送功率成正相关。类似地, \mathbf{H}_{MUF} 和 \mathbf{H}_{FUF} 的信道估计结果可分别表示为

$$\hat{\mathbf{H}}_{\text{FUF}} = \frac{P_{\text{FU}}\beta_{\text{FUF}}\mathbf{H}_{\text{FUF}}}{P_{\text{FU}}\beta_{\text{FUF}} + P_{\text{MU}}\beta_{\text{MUF}} + P_{\text{Ep}}\beta_{\text{EF}} + \sigma_{\text{FBS}}^2} + \frac{\sqrt{P_{\text{FU}}\beta_{\text{FUF}}P_{\text{MU}}\beta_{\text{MUF}}}\mathbf{H}_{\text{MUF}}}{P_{\text{FU}}\beta_{\text{FUF}} + P_{\text{MU}}\beta_{\text{MUF}} + P_{\text{Ep}}\beta_{\text{EF}} + \sigma_{\text{FBS}}^2} + \frac{\sqrt{P_{\text{FU}}\beta_{\text{FUF}}P_{\text{Ep}}\beta_{\text{EF}}}\mathbf{H}_{\text{EF}}}{P_{\text{FU}}\beta_{\text{FUF}} + P_{\text{MU}}\beta_{\text{MUF}} + P_{\text{Ep}}\beta_{\text{EF}} + \sigma_{\text{FBS}}^2} + \frac{\sqrt{P_{\text{FU}}\beta_{\text{FUF}}}\mathbf{n}_{\text{FBS}}\mathbf{x}_{\text{p}}^{\text{H}}}{P_{\text{FU}}\beta_{\text{FUF}} + P_{\text{MU}}\beta_{\text{MUF}} + P_{\text{Ep}}\beta_{\text{EF}} + \sigma_{\text{FBS}}^2} \quad (4)$$

$$\hat{\mathbf{H}}_{\text{FUM}} = \frac{P_{\text{FU}}\beta_{\text{FUM}}\mathbf{H}_{\text{FUM}}}{P_{\text{FU}}\beta_{\text{FUM}} + P_{\text{MU}}\beta_{\text{MUM}} + P_{\text{Ep}}\beta_{\text{EM}} + \sigma_{\text{MBS}}^2} + \frac{\sqrt{P_{\text{FU}}\beta_{\text{FUM}}P_{\text{MU}}\beta_{\text{MUM}}}\mathbf{H}_{\text{MUM}}}{P_{\text{FU}}\beta_{\text{FUM}} + P_{\text{MU}}\beta_{\text{MUM}} + P_{\text{Ep}}\beta_{\text{EM}} + \sigma_{\text{MBS}}^2} + \frac{\sqrt{P_{\text{FU}}\beta_{\text{FUM}}P_{\text{Ep}}\beta_{\text{EM}}}\mathbf{H}_{\text{EM}}}{P_{\text{FU}}\beta_{\text{FUM}} + P_{\text{MU}}\beta_{\text{MUM}} + P_{\text{Ep}}\beta_{\text{EM}} + \sigma_{\text{MBS}}^2} + \frac{\sqrt{P_{\text{FU}}\beta_{\text{FUM}}}\mathbf{n}_{\text{MBS}}\mathbf{x}_{\text{p}}^{\text{H}}}{P_{\text{FU}}\beta_{\text{FUM}} + P_{\text{MU}}\beta_{\text{MUM}} + P_{\text{Ep}}\beta_{\text{EM}} + \sigma_{\text{MBS}}^2} \quad (5)$$

2.2 下行数据传输

(1) 下行发送信号设计: MBS需要根据估计的主信道设计下行发送信号和人工噪声预编码矩阵 \mathbf{W}_{M} 和 \mathbf{W}'_{M} 。假设MBS用于发送下行数据信号、噪声信号的功率分别为 P_{sig} , $P_{\text{M}} - P_{\text{sig}}$, 且在所有发射天线上均匀分配发送功率, 此时经预编码后的下行数据和人工噪声信号 \mathbf{x}_{M} 可以表示为

$$\mathbf{x}_{\text{M}} = \sqrt{P_{\text{sig}}}\mathbf{W}_{\text{M}}\mathbf{s}_{\text{M}} + \sqrt{P_{\text{M}} - P_{\text{sig}}}\mathbf{W}'_{\text{M}}\mathbf{z}_{\text{M}} \quad (6)$$

其中, $\mathbf{W}_{\text{M}} \in \mathbb{C}^{N_{\text{M}} \times d}$, $\mathbf{W}'_{\text{M}} \in \mathbb{C}^{N_{\text{M}} \times (N_{\text{M}} - d)}$ 分别为MBS下行数据信号 $\mathbf{s}_{\text{M}} \in \mathbb{C}^{d \times 1}$ 和噪声信号 $\mathbf{z}_{\text{M}} \in \mathbb{C}^{(N_{\text{M}} - d) \times 1}$ 的预编码矩阵, d , $N_{\text{M}} - d$ 分别表示MBS发送的数据及人工噪声信号的维数, $\mathbf{s}_{\text{M}}, \mathbf{z}_{\text{M}} \sim \mathcal{CN}(0, 1)$ 。同时, 人工噪声满足式(7)

$$\mathbf{H}_{\text{MMU}}\mathbf{W}'_{\text{M}} = \mathbf{H}_{\text{MFU}}\mathbf{W}'_{\text{M}} = \mathbf{0}, \quad \mathbf{H}_{\text{ME}}\mathbf{W}'_{\text{M}} \neq \mathbf{0} \quad (7)$$

此时一般取 \mathbf{W}_{M} 和 \mathbf{W}'_{M} 分别为 $[(\mathbf{H}_{\text{MMU}})^{\text{T}} (\mathbf{H}_{\text{MFU}})^{\text{T}}]^{\text{T}}$ 的子空间和零空间向量组。类似地, 考虑FBS利用预编码 \mathbf{W}_{F} 对其下行数据信号进行调制, 以提升其对FU的服务性能, 即

$$\mathbf{x}_{\text{F}} = \sqrt{P_{\text{F}}}\mathbf{W}_{\text{F}}\mathbf{s}_{\text{F}} \quad (8)$$

其中, $\mathbf{W}_{\text{F}} \in \mathbb{C}^{N_{\text{F}} \times N_{\text{F}}}$ 为 \mathbf{H}_{FFU} 的子空间向量组, $\mathbf{s}_{\text{F}} \in \mathbb{C}^{N_{\text{F}} \times 1}$ 为FBS发送的下行数据信号, $\mathbf{s}_{\text{F}} \sim \mathcal{CN}(0, 1)$ 。

(2) 下行信号接收: 当Eve采取第1种主动窃听方式时, 则MU, Eve的接收信号可分别表示为

$$\mathbf{y}_{\text{MU}} = \sqrt{\beta_{\text{MMU}}}\mathbf{H}_{\text{MMU}}\mathbf{x}_{\text{M}} + \sqrt{\beta_{\text{FMU}}}\mathbf{H}_{\text{FMU}}\mathbf{x}_{\text{F}} + \mathbf{n}_{\text{MU}} \quad (9)$$

$$\mathbf{y}_{\text{Eve}} = \sqrt{\beta_{\text{ME}}}\mathbf{H}_{\text{ME}}\mathbf{x}_{\text{M}} + \sqrt{\beta_{\text{FE}}}\mathbf{H}_{\text{FE}}\mathbf{x}_{\text{F}} + \mathbf{n}_{\text{Eve}} \quad (10)$$

其中, $\beta_{\text{MMU}} = \beta_{\text{MUM}}$, $\beta_{\text{FMU}} = \beta_{\text{MUF}}$, $\beta_{\text{FE}} = \beta_{\text{EF}}$; $\mathbf{x}_{\text{M}} \in \mathbb{C}^{N_{\text{M}} \times 1}$, $\mathbf{x}_{\text{F}} \in \mathbb{C}^{N_{\text{F}} \times 1}$ 分别为MBS, FBS发送的下行信号; $\mathbf{n}_{\text{MU}} \in \mathbb{C}^{N_{\text{MU}} \times 1}$, $\mathbf{n}_{\text{Eve}} \in \mathbb{C}^{N_{\text{E}} \times 1}$ 分别为MU, Eve处的加性高斯白噪声矩阵, $\mathbf{n}_{\text{MU}} \sim \mathcal{CN}(0, \sigma_{\text{MU}}^2)$, $\mathbf{n}_{\text{Eve}} \sim \mathcal{CN}(0, \sigma_{\text{Eve}}^2)$ 。

当Eve采取第2种主动窃听方式时, 则MU的下行接收信号可表示为

$$\mathbf{y}_{\text{MU}} = \sqrt{\beta_{\text{MMU}}}\mathbf{H}_{\text{MMU}}\mathbf{x}_{\text{M}} + \sqrt{\beta_{\text{FMU}}}\mathbf{H}_{\text{FMU}}\mathbf{x}_{\text{F}} + \sqrt{\beta_{\text{EMU}}}\mathbf{H}_{\text{EMU}}\mathbf{x}_{\text{E}} + \mathbf{n}_{\text{MU}} \quad (11)$$

其中, $\sqrt{\beta_{\text{EMU}}}$, $\mathbf{H}_{\text{EMU}} \in \mathbb{C}^{N_{\text{MU}} \times N_{\text{E}}}$ 分别为Eve至MU的大尺度和小尺度衰落系数, $\mathbf{x}_{\text{E}} \in \mathbb{C}^{N_{\text{E}} \times 1}$ 为Eve发送的下行噪声干扰信号。

3 基于人工噪声的抗主动窃听者的鲁棒安全传输方案

3.1 导频攻击下的鲁棒安全传输方案

3.1.1 基站侧下行发送预编码矩阵的设计

在Eve进行上行导频干扰攻击的情形下, 首先将获取的信道估计矩阵进行合并, 获得新的信道矩阵 $\left[\left(\hat{\mathbf{H}}_{\text{MMU}} \right)^{\text{T}} \left(\hat{\mathbf{H}}_{\text{MFU}} \right)^{\text{T}} \right]^{\text{T}}$; 然后, 对新的信道矩阵进行奇异值分解, 令MBS的下行数据信号的预编码矩阵 \mathbf{W}_{M} 为其右奇异向量组、噪声信号的预编码矩阵 \mathbf{W}'_{M} 为其零空间向量组。类似地, 对于FBS的下行数据信号预编码设计可令 \mathbf{W}_{F} 为 $\hat{\mathbf{H}}_{\text{FFU}} = \left(\hat{\mathbf{H}}_{\text{FUF}} \right)^{\text{T}}$ 的右奇异向量组。

3.1.2 系统安全速率的推导

为推导系统安全速率表达式, 分别令 \mathbf{T}_{M} , \mathbf{T}'_{M} 和 \mathbf{T}_{E} , \mathbf{T}'_{E} 为 $\left[\left(\hat{\mathbf{H}}_{\text{MMU}} \right)^{\text{T}} \left(\hat{\mathbf{H}}_{\text{MFU}} \right)^{\text{T}} \right]^{\text{T}}$, \mathbf{H}_{ME} 的子空间和零空间向量组, 其中 \mathbf{T}_{M} , \mathbf{T}_{E} 分别为相应信道矩阵的子空间向量组。由于 $[\mathbf{W}_{\text{M}}; \mathbf{W}'_{\text{M}}]$, $[\mathbf{T}_{\text{M}}; \mathbf{T}'_{\text{M}}]$ 和 $[\mathbf{T}_{\text{E}}; \mathbf{T}'_{\text{E}}]$ 是3个基矩阵, 则一定存在基变换矩阵 $\mathbf{C}_{\text{M}} \in \mathbb{C}^{N_{\text{M}} \times N_{\text{M}}}$, $\mathbf{C}_{\text{E}} \in \mathbb{C}^{N_{\text{M}} \times N_{\text{M}}}$ 满足关系式(12)

$$[\mathbf{W}_{\text{M}}; \mathbf{W}'_{\text{M}}] = [\mathbf{T}_{\text{M}}; \mathbf{T}'_{\text{M}}]\mathbf{C}_{\text{M}} = [\mathbf{T}_{\text{E}}; \mathbf{T}'_{\text{E}}]\mathbf{C}_{\text{E}} \quad (12)$$

结合式(3)、式(5)可知, 当FU的发送功率经过基站间协作保持在较小水平时, 如果 \mathbf{H}_{EM} 的加权系数远大于 \mathbf{H}_{MUM} 的加权系数, 即 $P_{\text{MU}}\beta_{\text{MUM}} \ll P_{\text{E}}\beta_{\text{EM}}$ 时, 则 $\mathbf{C}_{\text{E}} \approx \mathbf{I}$, 表示信道估计矩阵 $\hat{\mathbf{H}}_{\text{MMU}}$ 与窃听信道 \mathbf{H}_{ME} 相似度很高, 那么他们的右奇异矩阵

也相近, 此时MBS发送给MU的下行信息会更多地泄露给Eve且MBS发送噪声对其干扰性能降低, 系统安全性会严重下降; 相反, 如果 $P_{\text{MU}}\beta_{\text{MUM}} \gg P_{\text{E}}\beta_{\text{EM}}$, 则 $\mathbf{C}_{\text{M}} \approx \mathbf{I}$, 则MBS发送给MU的下行信息泄露给Eve的量减少, 系统的安全性损失则较小。

进一步地, 对 \mathbf{C}_{M} 进行分块, 将其分块为 $\mathbf{C}_{\text{M}}^1 \in \mathbb{C}_d^{N_{\text{M}} \times d}$ 和 $\mathbf{C}_{\text{M}}^2 \in \mathbb{C}_{N_{\text{M}}-d}^{N_{\text{M}} \times (N_{\text{M}}-d)}$ 两部分, 即 $\mathbf{C}_{\text{M}} = [\mathbf{C}_{\text{M}}^1; \mathbf{C}_{\text{M}}^2]$ 。类似地, 将 \mathbf{C}_{E} 分块为 $\mathbf{C}_{\text{E}}^1 \in \mathbb{C}_d^{N_{\text{M}} \times d}$, $\mathbf{C}_{\text{E}}^2 \in \mathbb{C}_{N_{\text{M}}-d}^{N_{\text{M}} \times (N_{\text{M}}-d)}$, 则 \mathbf{W}_{M} 和 \mathbf{W}'_{M} 可分别表示为

$$\mathbf{W}_{\text{M}} = [\mathbf{T}_{\text{M}}; \mathbf{T}'_{\text{M}}]\mathbf{C}_{\text{M}}^1 = [\mathbf{T}_{\text{E}}; \mathbf{T}'_{\text{E}}]\mathbf{C}_{\text{E}}^1 \quad (13a)$$

$$\mathbf{W}'_{\text{M}} = [\mathbf{T}_{\text{M}}; \mathbf{T}'_{\text{M}}]\mathbf{C}_{\text{M}}^2 = [\mathbf{T}_{\text{E}}; \mathbf{T}'_{\text{E}}]\mathbf{C}_{\text{E}}^2 \quad (13b)$$

类似地, 将 \mathbf{T}_{F} , \mathbf{T}'_{F} 和 \mathbf{T}_{FE} , \mathbf{T}'_{FE} 分别为 \mathbf{H}_{FFU} , \mathbf{H}_{FE} 子空间和零空间向量组, 则有

$$[\mathbf{W}_{\text{F}}; \mathbf{W}'_{\text{F}}] = [\mathbf{T}_{\text{F}}; \mathbf{T}'_{\text{F}}]\mathbf{C}_{\text{F}} = [\mathbf{T}_{\text{FE}}; \mathbf{T}'_{\text{FE}}]\mathbf{C}_{\text{FE}} \quad (14)$$

同样地, 对 \mathbf{C}_{F} 进行分块, 将其分块为 $\mathbf{C}_{\text{F}}^1 \in \mathbb{C}_{d_2}^{N_{\text{F}} \times d_2}$ 和 $\mathbf{C}_{\text{F}}^2 \in \mathbb{C}_{N_{\text{F}}-d_2}^{N_{\text{F}} \times (N_{\text{F}}-d_2)}$ 两部分, 即 $\mathbf{C}_{\text{F}} = [\mathbf{C}_{\text{F}}^1; \mathbf{C}_{\text{F}}^2]$ 。类似地, 将 \mathbf{C}_{FE} 分块为 $\mathbf{C}_{\text{FE}}^1 \in \mathbb{C}_d^{N_{\text{M}} \times d}$, $\mathbf{C}_{\text{FE}}^2 \in \mathbb{C}_{N_{\text{M}}-d}^{N_{\text{M}} \times (N_{\text{M}}-d)}$, 则 \mathbf{W}_{F} 和 \mathbf{W}'_{F} 可分别表示为

$$\mathbf{W}_{\text{F}} = [\mathbf{T}_{\text{F}}; \mathbf{T}'_{\text{F}}]\mathbf{C}_{\text{F}}^1 = [\mathbf{T}_{\text{FE}}; \mathbf{T}'_{\text{FE}}]\mathbf{C}_{\text{FE}}^1 \quad (15a)$$

$$\mathbf{W}'_{\text{F}} = [\mathbf{T}_{\text{F}}; \mathbf{T}'_{\text{F}}]\mathbf{C}_{\text{F}}^2 = [\mathbf{T}_{\text{FE}}; \mathbf{T}'_{\text{FE}}]\mathbf{C}_{\text{FE}}^2 \quad (15b)$$

需要注意的是, 式(15a)、式(15b)中的 $d_2 = N_{\text{F}}$ 。结合式(13a)和式(13b), 对式(8)和式(9)进行重新表示, 可将最终系统的安全速率为表示为

$$R_{\text{S}} = \left\{ \log_2 \left| \frac{\mathbf{I}_{N_{\text{M}}} + P_{\text{sig}}\beta_{\text{MMU}}\mathbf{H}_{\text{MMU}}\mathbf{T}_{\text{M}}}{\mathbf{C}_{\text{M}}^{11}(\mathbf{C}_{\text{M}}^{11})^{\text{H}}\mathbf{T}_{\text{M}}^{\text{H}}\mathbf{H}_{\text{MMU}}^{\text{H}}\mathbf{K}_{\text{M}}^{-1}/d} \right| - \log_2 \left| \frac{\mathbf{I}_{N_{\text{E}}} + P_{\text{sig}}\beta_{\text{ME}}\mathbf{H}_{\text{ME}}}{\mathbf{T}_{\text{E}}\mathbf{C}_{\text{E}}\mathbf{C}_{\text{E}}^{\text{H}}\mathbf{T}_{\text{E}}^{\text{H}}\mathbf{H}_{\text{ME}}^{\text{H}}\mathbf{K}_{\text{ME}}^{-1}/d} \right| \right\}^+ \quad (16)$$

其中, $\{a\}^+ = \max\{0, a\}$, $\mathbf{C}_{\text{M}}^{11} \in \mathbb{C}^{d \times d}$, $\mathbf{C}_{\text{M}}^{22} \in \mathbb{C}^{d \times (N_{\text{M}}-d)}$, $\mathbf{C}_{\text{F}}^{11} \in \mathbb{C}^{d_2 \times d_2}$, $\mathbf{C}_{\text{E}}^{11} \in \mathbb{C}^{d \times d}$, $\mathbf{C}_{\text{E}}^{22} \in \mathbb{C}^{d \times (N_{\text{M}}-d)}$ 和 $\mathbf{C}_{\text{FE}}^{11} \in \mathbb{C}^{d_2 \times d_2}$ 分别为 \mathbf{C}_{M}^1 , \mathbf{C}_{M}^2 , \mathbf{C}_{F}^1 , \mathbf{C}_{E}^1 , \mathbf{C}_{E}^2 和 \mathbf{C}_{FE}^1 的上分块矩阵; \mathbf{K}_{M} 和 \mathbf{K}_{E} 分别为MU, Eve处的干扰及噪声协方差矩阵, 且可分别表示为

$$\mathbf{K}_{\text{M}} = P_{\text{sig}}\beta_{\text{MMU}}\mathbf{H}_{\text{MMU}}\mathbf{T}_{\text{M}}\mathbf{C}_{\text{M}}^{22}(\mathbf{C}_{\text{M}}^{22})^{\text{H}}\mathbf{T}_{\text{M}}^{\text{H}}\mathbf{H}_{\text{MMU}}^{\text{H}}/d + P_{\text{F}}\beta_{\text{FMU}}\mathbf{H}_{\text{FMU}}\mathbf{T}_{\text{F}}\mathbf{C}_{\text{F}}^{11}(\mathbf{C}_{\text{F}}^{11})^{\text{H}}\mathbf{T}_{\text{F}}^{\text{H}}\mathbf{H}_{\text{FMU}}^{\text{H}} + \sigma_{\text{MU}}^2\mathbf{I}_{N_{\text{M}}} \quad (17a)$$

$$\mathbf{K}_{\text{E}} = P_{\text{sig}}\beta_{\text{ME}}\mathbf{H}_{\text{ME}}\mathbf{T}_{\text{E}}\mathbf{C}_{\text{E}}^{22}(\mathbf{C}_{\text{E}}^{22})^{\text{H}}\mathbf{T}_{\text{E}}^{\text{H}}\mathbf{H}_{\text{ME}}^{\text{H}}/d + P_{\text{F}}\beta_{\text{FE}}\mathbf{H}_{\text{FE}}\mathbf{T}_{\text{FE}}\mathbf{C}_{\text{FE}}^{11}(\mathbf{C}_{\text{FE}}^{11})^{\text{H}}\mathbf{T}_{\text{FE}}^{\text{H}}\mathbf{H}_{\text{FE}}^{\text{H}} + \sigma_{\text{Eve}}^2\mathbf{I}_{N_{\text{E}}} \quad (17b)$$

3.1.3 MBS下行发送数据信号与噪声信号的功率优化

在此种攻击方式下, 式(3)—式(6)中的 $P_{E_p} = P_E$ 。此时, 为提升系统安全速率, 可以将对下行发送数据和噪声信号功率的优化建模为以下最优化问题

$$\max_{P_{\text{sig}}} \{R_S(P_{\text{sig}})\} \quad (18a)$$

$$\text{s.t. } 0 \leq P_{\text{sig}} \leq P_M \quad (18b)$$

$$P_{E_p} = P_E \quad (18c)$$

该问题不是一个凸的优化问题, 无法直接进行求解获取最优功率分配的闭式解。但同时我们注意到, 该问题是一个关于 P_{sig} 的1维优化问题。因此, 考虑计算精度与复杂度的折中, 本文采用均匀采样法对优化问题式(18)进行求解。具体而言, 分别令 $P_{\text{sig}} = [0, \Delta_{P_{\text{sig}}}, \dots, P_M - \Delta_{P_{\text{sig}}}, P_M]$, 得到相应的功率分配下的系统安全速率, 然后通过遍历比较获取系统安全速率最大值, 从而获得最优的功率分配值及其对应的安全速率值, 其中 $\Delta_{P_{\text{sig}}}$ 为均匀采样间隔。

3.2 导频攻击和噪声干扰联合攻击下的鲁棒安全传输方案

3.2.1 下行发送预编码的设计及系统安全速率的推导

(1) 下行发送预编码设计: 基站侧下行发送预编码的设计与3.1.1节类似, 此处就不再赘述。

(2) 系统安全速率的推导: 此种情形下, Eve为提升自身窃听性能, 必定会完全分配其发送总功率, 即 $P_{E_p} + P_{E_d} = P_E$ 。此时, 系统安全速率可以重新表示为

$$R_S = \left\{ \log_2 \left| \frac{\mathbf{I} + P_{\text{sig}} \beta_{\text{MMU}} \mathbf{H}_{\text{MMU}} \mathbf{T}_M}{\mathbf{C}_M^{11} (\mathbf{C}_M^{11})^H \mathbf{T}_M^H \mathbf{H}_{\text{MMU}}^H \mathbf{K}_{M2}^{-1} / d} \right| - \log_2 \left| \frac{\mathbf{I} + P_{\text{sig}} \beta_{\text{ME}} \mathbf{H}_{\text{ME}} \mathbf{T}_E \mathbf{C}_E}{\mathbf{C}_E^H \mathbf{T}_E^H \mathbf{H}_{\text{ME}}^H \mathbf{K}_{ME}^{-1} / d} \right| \right\}^+ \quad (19)$$

其中,

$$\begin{aligned} \mathbf{K}_{M2} = & P_{\text{sig}} \beta_{\text{MMU}} \mathbf{H}_{\text{MMU}} \mathbf{T}_M \mathbf{C}_M^{22} (\mathbf{C}_M^{22})^H \mathbf{T}_M^H \mathbf{H}_{\text{MMU}}^H / d \\ & + P_F \beta_{\text{FMU}} \mathbf{H}_{\text{FMU}} \mathbf{T}_F \mathbf{C}_F^{11} (\mathbf{C}_F^{11})^H \mathbf{T}_F^H \mathbf{H}_{\text{FMU}}^H \\ & + P_{E_d} \beta_{\text{EMU}} \mathbf{H}_{\text{EMU}} \mathbf{H}_{\text{EMU}}^H / N_E + \sigma_{\text{MU}}^2 \mathbf{I}_{N_M} \end{aligned} \quad (20)$$

3.2.2 MBS下行发送数据信号与噪声信号的功率优化

由式(19)可知, 在MBS, Eve的总发送功率限制下, Eve目标是为了降低系统安全速率, 而MBS则想增大系统安全速率, 显然双方之间存在竞争关系。针对这种存在竞争的物理层安全问题, 本文考虑利用零和博弈的方法来对其进行分析求解以获得

此种情形下的最优系统安全速率。具体而言, 首先, 将MBS, Eve之间竞争关系建立为一个以最大化最差情形下系统安全速率为目标的零和博弈模型; 然后, 通过求解他们之间的纳什均衡解, 得到MBS, Eve双方各自最优的功率分配值及对应的系统安全速率值。此时, 结合式(19)、式(20), 博弈过程可以建模为以下最优化问题

$$\max_{P_{\text{sig}}} \left\{ \min_{P_{E_p}} \{R_S(P_{\text{sig}}, P_{E_p})\} \right\} \quad (21a)$$

$$\text{s.t. } 0 \leq P_{\text{sig}} \leq P_S, 0 \leq P_{E_p} \leq P_E \quad (21b)$$

问题式(21)不是一个凸优化问题。因此, MBS与Eve之间的零和博弈不存在纯策略均衡, 即MBS不存在特定的下行数据信号发送功率 P_{sig}^* 使系统安全性能最优。此时, 只能采用混合策略均衡求解该博弈。首先, 根据MBS, Eve的总发送功率约束, 将式(21b)离散化, 得到MBS与Eve的混合策略集 Ψ 和 Φ , 分别表示为

$$\Psi = \{0, \Delta_M, 2\Delta_M, \dots, P_M - \Delta_M, P_M\} \quad (22a)$$

$$\Phi = \{0, \Delta_E, 2\Delta_E, \dots, P_E - \Delta_E, P_E\} \quad (22b)$$

其中, Δ_M, Δ_E 分别为均匀划分 P_M, P_E 所采用的间隔。分析可知, 该零和博弈是一个有限的离散博弈, 且对于每个策略空间中的值 $(P_{\text{sig}}, P_{E_p})$ 同时对应一个非负的系统安全速率值 $R_S(P_{\text{sig}}, P_{E_p})$ 。于是, 根据整个混合策略集可以相应地得到一个2维的非负收益矩阵 \mathbf{A} , 其中 $\mathbf{A}(i, j) = R_S(P_{\text{sig}}, P_{E_p})$ 表示当 P_{sig} 取 Ψ 中第 i 个值、 P_{E_p} 取 Φ 中第 j 个值时所求得的安全速率。随后, 令MBS, Eve分别以概率 $\mathbf{p} = (p_1, p_2, \dots, p_{n_S})$, $\mathbf{q} = (q_1, q_2, \dots, q_{n_E})$ 取策略集 Ψ, Φ 中的离散值, 其中 n_S, n_E 分别表示 P_{sig}, P_{E_p} 的离散值个数。最终, 基于上述分析, 求解混合策略下的最优安全速率问题可建模为

$$\begin{aligned} & R_S(p_1, \dots, p_{n_S}, q_1, \dots, q_{n_E}) \\ & = \mathbf{p}^T R_S(P_{\text{sig}}(i), P_{E_p}(j)) \mathbf{q} \end{aligned} \quad (23a)$$

$$\text{s.t. } \sum_{i=1}^{n_S} p_i = 1, \sum_{j=1}^{n_E} q_j = 1 \quad (23b)$$

针对这个收益矩阵, MBS通过设计 $\mathbf{p} = (p_1, p_2, \dots, p_{n_S})$ 来提升系统安全速率, 而Eve则通过设计 $\mathbf{q} = (q_1, q_2, \dots, q_{n_E})$ 意图降低系统安全速率。为求解问题式(23), 本文借助于文献[13]中的极大极小定理: 如果存在一个非负数 v , 使得对任意的 j 有 $\sum_{i=1}^{n_S} A_{ij} p_i \geq v$, 对任意的 i 有 $\sum_{j=1}^{n_E} A_{ij} q_j \leq v$, 那么 $(\mathbf{p}^*, \mathbf{q}^*)$ 是该博弈的混合策略均衡。

由于 \mathbf{A} 是非负的, 分析可知 v 是一个非负数,

令 $a_i = p_i/v$, $b_j = q_j/v$, $i \in [1, n_S]$, $j \in [1, n_E]$ 。根据文献[13]中的定理可知该零和博弈的混合策略纳什均衡分别可通过对以下两个问题的求解来获得。具体而言, 为确定 $\mathbf{p} = (p_1, p_2, \dots, p_{n_S})$, 可以通过求解以下问题

$$\min \sum_{i=1}^{n_S} a_i \quad (24a)$$

$$\text{s.t.} \sum_{i=1}^m A_{ij} a_i \geq 1, \quad j \in [1, n_E] \quad (24b)$$

$$0 \leq a_i, \quad i \in [1, n_S] \quad (24c)$$

通过对问题式(24)求解, 可以获得其解为 $\mathbf{p} = (va_1, va_2, \dots, va_{n_S})$, 即 \mathbf{p} 为均衡时MBS发送下行数据信号功率的概率分布。同时, 为确定 $\mathbf{q} = (q_1, q_2, \dots, q_{n_E})$, 可以通过求解以下问题

$$\max \sum_{j=1}^{n_E} b_j \quad (25a)$$

$$\text{s.t.} \sum_{j=1}^{n_E} A_{ij} b_j \leq 1, \quad i \in [1, n_S] \quad (25b)$$

$$0 \leq b_j, \quad j \in [1, n_E] \quad (25c)$$

该问题的最优解为 $\mathbf{q} = (vb_1, vb_2, \dots, vb_{n_E})$, 即 \mathbf{q} 为均衡时Eve发送上行导频干扰信号的概率分布。进一步地, 可以得出最终的混合策略均衡下系统安全速率值为

$$R_S = v = \frac{1}{\sum_{i=1}^{n_S} a_i} = \frac{1}{\sum_{j=1}^{n_E} b_j} \quad (26)$$

4 仿真分析

本章通过仿真对所提出的鲁棒安全传输方案的性能进行评估。对于信道模型, 本文考虑简化的大尺度衰落与小尺度衰落模型^[8], 各节点之间的大尺度路径衰落系数为 $\alpha = 2$, $\kappa = 1$, 参考距离为 $d_0 = 1$; 小尺度衰落服从瑞利衰落, 且各信道之间相互独立。网络中各节点天线数目为 $N_M = 7$, $N_F = 5$, $N_U = N_E = 2$; 各节点总发送功率为 $P_M = 40$ dBm, $P_F = 35$ dBm, $P_{MU} = 20$ dBm, $P_E = 20$ dBm, $P_{FU} = 20$ dBm; 离散个数 $n_S = n_E = 20$ 。

图1给出了在Eve采用上行导频攻击的情形下, 系统安全速率随MBS发送天线数目 N_M 的变化情形。如图1所示, 随着 N_M 的增大, 系统安全速率也会均随之提升。这是因为 N_M 的增大可以使MBS在上行信道估计阶段接收到更多的MU发送的上行导频估计信号, 从而使信道估计所获得的信道

矩阵更加准确; 在下行数据传输阶段, N_M 的增大可以使得MBS发送的下行数据信号针对MU的指向性有所提升, 噪声信号对MU的影响减少, 从而能够提升MU的下行接收性能, 增大系统安全速率。同时, 纵向观察还可以看出, 在相同的参数设置下, 经过安全传输优化方案后的系统安全速率比优化前均有明显地提升, 验证了本文所提方案的安全性和抵抗主动窃听的鲁棒性。这是因为经过安全传输优化设计后, MBS可以更加合理地分配其下行发送数据信号和噪声信号的功率, 从而使MU的下行接收性能获得提升, Eve的接收性能下降。

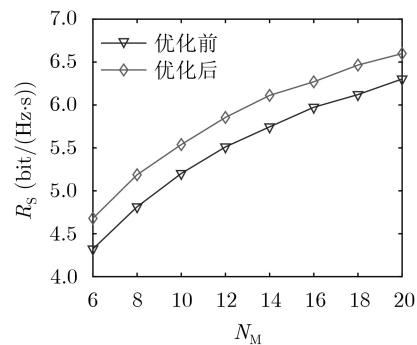


图1 导频攻击下系统安全速率与MBS发送天线数目的关系

图2给出了在Eve采用上行导频攻击的情形下, 系统安全速率随MBS总发送功率 P_M 的变化情形。如图2所示, 系统安全速率随 P_M 的增大也相应的随之增加。因为 P_M 的增大可以增强发送的下行数据信号功率提升MU的接收性能, 同时发送的下行噪声信号也会相应提升进一步降低Eve的接收性能。同时, 我们发现在相同的参数设置下, 在采用安全传输优化方案后, 系统安全速率均获得了明显的提升, 进一步验证了本文所提方案的有效性。性能提升的原因与图1类似, 此处就不再赘述。综合对图1、图2的分析来看, 本文提出的导频攻击下的鲁棒安全传输方案可以明显地提升系统安全速率。

图3给出了在Eve采用导频与噪声干扰联合攻击的情形下, 系统安全速率随MU, Eve总发送功率

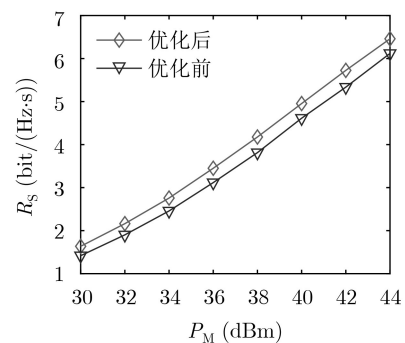


图2 导频攻击下系统安全速率与MBS总发送功率的关系

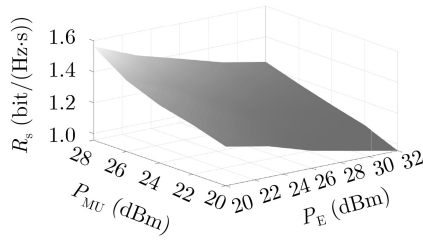


图3 导频与噪声干扰联合攻击下系统安全速率与MU, Eve总发送功率关系

P_{MU} , P_E 的变化情形。观察图3可以看出, 当 P_E 固定, P_{MU} 增大时, 系统安全速率随之上升。这是因为从式(3)可以看出, P_{MU} 的增大可以增强MBS获取的估计信道 \hat{H}_{MUM} 准确性, 减小 \hat{H}_{MUM} 与实际信道 H_{MUM} 的误差, 从而使得在下行发送过程中数据信号泄露给Eve的机会降低, 同时减少了MBS下行噪声对MU自身的影响。相反地, 如果当 P_{MU} 固定, P_E 增大时, 系统安全速率随之下降。因为 P_E 的增大会加剧估计信道 \hat{H}_{MUM} 的不准确性, 使得MBS发送的下行数据信号泄露给Eve的机会增大, 噪声信号对MU影响增大, 从而Eve的接收性能获得提升, MU接收性能下降, 系统安全性降低。此外还发现, 当 $P_{MU} < P_E$ 时, 系统仍能在一定范围内获得大于零的安全速率, 说明所提出的鲁棒安全传输方案仍可以在Eve发送上行导频干扰和噪声总功率较大时, 在一定范围内保证系统安全性, 从而验证了本文所提方案的有效性。

5 结论

本文针对MIMO异构网络中存在的Eve进行主动窃听情形进行研究, 并提出了一种基于人工噪声的抗主动窃听者的鲁棒安全传输方案。当Eve采取上行导频攻击方式时, 发现合法用户的上行信道估计是主信道、干扰信道和窃听信道的线性相加, 随后提出一种基于一维线性搜索的方法以获取最优的MBS下行发送数据信号与人工噪声信号功率。进一步地, 在Eve采取上行导频与下行噪声干扰联合攻击的情形下, 首先建立MBS与Eve之间以最大化系统安全速率为目标函数的离散零和博弈, 然后根据确定的离散策略集求解混合策略纳什均衡, MBS依据获得均衡合理地分配其下行数据信号与噪声信号功率。最后, 仿真结果表明, 所提方案能很好地保证系统安全性。

参考文献

- [1] TANG Weijun, FENG Suili, DING Yuehua, *et al.* Physical layer security in heterogeneous networks with jammer selection and full-duplex users[J]. *IEEE Transactions on*
- [2] 彭建华, 张帅, 许晓明, 等. 物联网中一种抗大规模天线阵列窃听者的噪声注入方案[J]. 电子与信息学报, 2019, 41(1): 67-73. doi: 10.11999/JEIT180342.
- [3] 洪涛, 张更新. 人工噪声辅助的物理层安全信号峰均功率比减低算法[J]. 电子与信息学报, 2018, 40(6): 1426-1432. doi: 10.11999/JEIT170739.
- [4] WANG Huiming, ZHENG Tongxing, YUAN Jinhong, *et al.* Physical layer security in heterogeneous cellular networks[J]. *IEEE Transactions on Communications*, 2016, 64(3): 1204-1219. doi: 10.1109/TCOMM.2016.2519402.
- [5] XU Min, TAO Xiaofeng, FAN Yang, *et al.* Enhancing secured coverage with CoMP transmission in heterogeneous cellular networks[J]. *IEEE Communications Letters*, 2016, 20(11): 2272-2275. doi: 10.1109/LCOMM.2016.2598536.
- [6] NGUYEN N P, KUNDU C, NGO H Q, *et al.* Secure full-duplex small-cell networks in a spectrum sharing environment[J]. *IEEE Access*, 2016, 4: 3087-3099. doi: 10.1109/ACCESS.2016.2582486.
- [7] DI RENZO M and GUAN Peng. Stochastic geometry modeling and system-level analysis of uplink heterogeneous cellular networks with multi-antenna base stations[J]. *IEEE Transactions on Communications*, 2016, 64(6): 2453-2476. doi: 10.1109/TCOMM.2016.2552163.
- [8] REN Yuan, LÜ Tiejun, GAO Hui, *et al.* Secure wireless information and power transfer in heterogeneous networks[J]. *IEEE Access*, 2017, 5: 4967-4979. doi: 10.1109/ACCESS.2017.2682277.
- [9] LI Bin, FEI Zesong, CHU Zheng, *et al.* Secure transmission for heterogeneous cellular networks with wireless information and power transfer[J]. *IEEE Systems Journal*, 2018, 12(4): 3755-3766. doi: 10.1109/JSYST.2017.2713881.
- [10] HU Xin, LI Bin, HUANG Kaizhi, *et al.* Secrecy energy efficiency in wireless powered heterogeneous networks: A distributed ADMM approach[J]. *IEEE Access*, 2018, 6: 20609-20624. doi: 10.1109/ACCESS.2018.2825387.
- [11] HU Die, ZHANG Wei, HE Lianghua, *et al.* Secure transmission in multi-cell multi-user massive MIMO systems with an active eavesdropper[J]. *IEEE Wireless*

Communications, 2017, 16(12): 7982-7995. doi: 10.1109/TWC.2017.2755640.

PENG Jianhua, ZHANG Shuai, XU Xiaoming, *et al.* A noise injection scheme resistant to massive MIMO eavesdropper in IoT[J]. *Journal of Electronics & Information Technology*, 2019, 41(1): 67-73. doi: 10.11999/JEIT180342.

HONG Tao and ZHANG Gengxin. Peak-to-average power ratio reduction algorithm of artificial-noise-aided secure signal[J]. *Journal of Electronics & Information Technology*, 2018, 40(6): 1426-1432. doi: 10.11999/JEIT170739.

WANG Huiming, ZHENG Tongxing, YUAN Jinhong, *et al.* Physical layer security in heterogeneous cellular networks[J]. *IEEE Transactions on Communications*, 2016, 64(3): 1204-1219. doi: 10.1109/TCOMM.2016.2519402.

XU Min, TAO Xiaofeng, FAN Yang, *et al.* Enhancing secured coverage with CoMP transmission in heterogeneous cellular networks[J]. *IEEE Communications Letters*, 2016, 20(11): 2272-2275. doi: 10.1109/LCOMM.2016.2598536.

NGUYEN N P, KUNDU C, NGO H Q, *et al.* Secure full-duplex small-cell networks in a spectrum sharing environment[J]. *IEEE Access*, 2016, 4: 3087-3099. doi: 10.1109/ACCESS.2016.2582486.

DI RENZO M and GUAN Peng. Stochastic geometry modeling and system-level analysis of uplink heterogeneous cellular networks with multi-antenna base stations[J]. *IEEE Transactions on Communications*, 2016, 64(6): 2453-2476. doi: 10.1109/TCOMM.2016.2552163.

REN Yuan, LÜ Tiejun, GAO Hui, *et al.* Secure wireless information and power transfer in heterogeneous networks[J]. *IEEE Access*, 2017, 5: 4967-4979. doi: 10.1109/ACCESS.2017.2682277.

LI Bin, FEI Zesong, CHU Zheng, *et al.* Secure transmission for heterogeneous cellular networks with wireless information and power transfer[J]. *IEEE Systems Journal*, 2018, 12(4): 3755-3766. doi: 10.1109/JSYST.2017.2713881.

HU Xin, LI Bin, HUANG Kaizhi, *et al.* Secrecy energy efficiency in wireless powered heterogeneous networks: A distributed ADMM approach[J]. *IEEE Access*, 2018, 6: 20609-20624. doi: 10.1109/ACCESS.2018.2825387.

HU Die, ZHANG Wei, HE Lianghua, *et al.* Secure transmission in multi-cell multi-user massive MIMO systems with an active eavesdropper[J]. *IEEE Wireless*

- Communications Letters*, 2019, 8(1): 85–88. doi: [10.1109/LWC.2018.2859329](https://doi.org/10.1109/LWC.2018.2859329).
- [12] ALAGELI M, IKHLEF A, and CHAMBERS J. SWIPT massive MIMO systems with active eavesdropping[J]. *IEEE Journal on Selected Areas in Communications*, 2019, 37(1): 233–247. doi: [10.1109/JSAC.2018.2872370](https://doi.org/10.1109/JSAC.2018.2872370).
- [13] BASAR T and OLSDER G J. *Dynamic Noncooperative Game Theory*[M]. 2nd ed. New York: Academic Press, 1995: 23–28.
- 张波: 男, 1993年生, 博士生, 研究方向为移动通信安全.
黄开枝: 女, 1973年生, 教授、博士生导师, 研究方向为移动通信网络及信息安全.
林胜斌: 男, 1990年生, 讲师, 研究方向为无线物理层安全.
易鸣: 男, 1986年生, 助理研究员, 研究方向为物理层安全编码.
陈亚军: 男, 1988年生, 助理研究员, 研究方向为移动通信安全.
- 责任编辑: 余蓉