基于非完美信道信息的协作 NOMA 系统中保密通信技术研究

陈 杨，张忠培*，李彬睿

(电子科技大学通信抗干扰技术国家级重点实验室 成都 611731)

【摘要】该文针对协作 NOMA 系统中保密通信进行了研究，在该 NOMA 系统中，一个有高保密需求的用户 (LU1) 被多个非合作窃听者窃听，另一个普通用户 (LU2) 同时与基站 (Alice) 进行通信。为了提高系统的安全性能，在系统中引入了一个协作干扰者 (Charlie) 来扰乱窃听者。考虑更加贴近实际场景的非完美信道信息情况，基于 LU1 的保密需求和 LU2 的 QoS 要求，提出了一个自适应功率分配算法来解决安全速率最大化问题。仿真结果验证了该方案的有效性和灵活性，并且验证了非完美信道信息会降低系统安全性能以及能效。

关 键 词 非完美信道信息； 非正交多址接入； 功率分配； 保密中断概率； 保密速率

中图分类号 TN918 **文献标志码** A doi:10.12178/1001-0548.2020066

Secure Communications for Cooperative NOMA Networks with Imperfect CSI

CHEN Yang, ZHANG Zhong-pei*, and LI Bin-rui

(National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China Chengdu 611731)

Abstract This paper studied secure transmission in cooperative non-orthogonal multiple access (NOMA) networks, where one legitimate user with high-level security requirement (LU1) is overhead by multiple non-colluding eavesdroppers (Eves), and another normal user (LU2) is served by the source (Alice) simultaneously. Aiming to improve the secrecy performance, a cooperative jammer (Charlie) is employed to confound the Eves. In this more practical communication scenario, take both secrecy outage restriction of LU1 and the desired quality of service (QoS) demand of LU2 into consideration, the paper propose an adaptive power allocation strategy for maximizing secrecy rate under imperfect channel state information (CSI). Numerical results are provided to verify the effectiveness of the proposed scheme and show that the system security would be seriously degenerated with channel uncertainty.

Key words imperfect channel state information; non-orthogonal multiple access; power allocation; secrecy outage probability; secrecy rate

非正交多址接入 (NOMA) 技术能显著提高频谱效率，因此被视为第五代移动无线通信系统中的关键技术[1]。与传统的正交多址接入技术 (OMA) 不同，NOMA 技术利用功率域来同时为多个用户提供服务[2]。由于 NOMA 技术在提高频谱效率和增大覆盖面积方面的性能表现优秀，协作 NOMA 技术成为了近年来研究人员关心的热点[3]。

由于无线信道的开放特性，协作 NOMA 系统的安全性面临严峻考验。近年来，作为新兴的有效抗窃听方案，物理层安全技术吸引了研究人员的广泛关注且被应用在协作 NOMA 系统中[4-6]。文献 [4] 在协作 NOMA 系统中讨论了放大转发 (AF) 和解码转发 (DF) 协议，并推导了保密中断概率 (SOP) 和保密速率表达式。文献 [5] 分析了干扰者协助的协作 NOMA 系统中，采用随机和 max-min 两种中继选择方案得到的分析和渐进 SOP 表达式。文献 [6] 提出了一种新的非正交干扰 DF 方案来提高协作 NOMA 系统的保密速率并且减少信息泄露。

然而，在上述关于协作 NOMA 系统的工作中均考虑的是主信道的信道信息基站和协作节点完美

收稿日期：2020－02－24；修回日期：2020－04－14
基金项目：广东省重大科技专项 (2018B010115001)
作者简介：陈杨 (1988－)，男，博士生，主要从事协作通信与物理层安全方面的研究.
通信作者：张忠培，Email：zhangzp@uesct.edu.cn

已知的情况，在实际应用中这是不容易实现的。非完美信道信息会导致严重的安全性能下降，因此在协作 NOMA 安全传输系统中讨论非完美信道信息是很有必要的[7-10]。文献 [7] 推导了非完美信道信息条件下认知无线电中继 NOMA 系统的中断概率表达式。文献 [8] 讨论了两种信道不确定模型，并以此为基础研究了协作无线携能 NOMA 通信系统中波束赋形和功率分配设计的问题。文献 [9] 将小区边缘用户用作 DF中继来协助信息传输，并研究了非完美信道信息对协作无线携能 NOMA 通信系统性能的影响。考虑配置多天线的基站，文献 [10] 对非完美信道信息场景中协作无线携能 NOMA 物联网系统的容量进行了分析。

但目前还没有讨论对非完美信道信息场景中，引入协作干扰者帮助的协作 NOMA系统中基于保密中断概率限制条件的保密速率最大化问题。基于此，本文考虑了两用户多输入单输出 (MISO) 协作 NOMA 系统，在这个系统中，一个用户 (LU1) 有较高的速率和安全要求 (例如银行工作人员、政府工作人员等)，而另外一个用户 (LU2) 仅有服务质量 QoS 限制 (例如公共天气预报)[11]，并对该系统在非完美信道信息条件下保密速率最大化的问题进行了研究。同时考虑两个用户保密需求和速率需求，本文提出了一种自适应功率分配算法来使得保密速率最大化。此外，本文将 LU1 的保密速率与 LU2 的传输速率之和定义为有效和速率，将有效和速率与总功率的比值定义为有效能量效率并进行讨论。仿真结果验证了本文所提出算法的有效性，并阐述了非完美信道信息对系统性能的影响。

1　系统模型和问题阐述

1.1　系统模型

本文讨论的 MISO-NOMA 系统模型如图 1 所示，一个基站 (Alice) 同时对两个单天线用户 (LU1 和 LU2) 进行通信，系统中存在多个单天线窃听者对 LU1 的信息进行窃听。与此同时，引入了一个协作干扰者 (Charlie) 来增强系统的安全性能。Alice 和 Charlie 分别配置了N_a和N_c根天线，其中$N_c>2$。此外，窃听者的集合定义为$\mathcal{M}\triangleq\{1,2,\cdots,M\}$。

从 Alice 到两个用户和 Alice 到第m个窃听者的信道分别表示为$\boldsymbol{h}_{ak}\in\mathbb{C}^{1\times N_a}$，$k\in\{1,2\}$ 和$\boldsymbol{h}_{ae,m}\in\mathbb{C}^{1\times N_a}$，且所有信道假设为服从独立同分布的瑞利衰落信道。

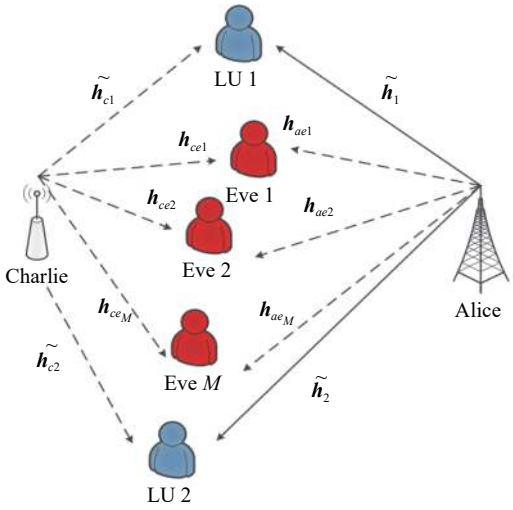


图 1　协作 MISO-NOMA 安全传输模型

由于发送端 Alice 和 Charlie 与用户之间信道信息非完美，参考在 TDD 系统中被广泛应用的高斯不确定信道模型[9,12]，则 Alice 与两个用户之间的实际信道可以被表示为：

$$\boldsymbol{h}_{ak}=\widetilde{\boldsymbol{h}_{ak}}+\boldsymbol{e}_{ak}\quad k\in\{1,2\}\tag{1}$$

式中，$\widetilde{\boldsymbol{h}_{ak}},k\in\{1,2\}$表示 Alice 与用户之间的估计信道；$\boldsymbol{e}_{ak}\sim\mathcal{CN}(0,\sigma_{ak}^2\boldsymbol{I}_{N_a})$，表示信道估计误差向量，$k\in\{1,2\}$；且$\widetilde{\boldsymbol{h}_{ak}}$与$\boldsymbol{e}_{ak}$不相关。同理，Charlie 与两个用户之间的实际信道可以被表示为：

$$\boldsymbol{h}_{ck}=\widetilde{\boldsymbol{h}_{ck}}+\boldsymbol{e}_{ck}\quad k\in\{1,2\}\tag{2}$$

式中，$\widetilde{\boldsymbol{h}_{ck}},k\in\{1,2\}$表示 Charlie 与用户之间的估计信道；$\boldsymbol{e}_{ck}\sim\mathcal{CN}(0,\sigma_{ck}^2\boldsymbol{I}_{N_c})$，为信道估计误差向量，$k\in\{1,2\}$；且$\widetilde{\boldsymbol{h}_{ck}}$与$\boldsymbol{e}_{ck}$不相关。不失一般性，本文假设 Alice 与用户之间的估计信道增益呈降序排列[8]，即$|\widetilde{\boldsymbol{h}_{a2}}|^2\leqslant|\widetilde{\boldsymbol{h}_{a1}}|^2$。

根据 NOMA 原理[13]，Alice 分别对 LU1 和 LU2 发送信号x_1和x_2。用$\boldsymbol{t}\in\mathbb{C}^{N_a\times1}$表示 Alice 传输的信号，因此$\boldsymbol{t}$可以表述为：

$$\boldsymbol{t}=\sqrt{P_a a_1}\boldsymbol{w}_s x_1+\sqrt{P_a a_2}\boldsymbol{w}_s x_2\tag{3}$$

式中，P_a表示 Alice 的传输功率；信号$x_k\sim\mathcal{CN}(0,1)$，$k\in\{1,2\}$；a_1和a_2分别为信号x_1和x_2的功率分配系数[3]，且满足条件$a_1\leqslant a_2$以及$a_1+a_2=1$。此外，由于用户 LU1 在本系统中是优先考虑的服务对象，为了保证 LU1 的有效信道增益，Alice 采用最大传输比波束赋形[9]，即$\boldsymbol{w}_s=\widetilde{\boldsymbol{h}_{a1}}/\|\widetilde{\boldsymbol{h}_{a1}}\|$。

在本系统中，Charlie 作为外部协作干扰者发送人工噪声对窃听者进行干扰，同时不对用户造成影响，即$\widetilde{\boldsymbol{h}_{ck}}\boldsymbol{t}_c=0$，$k\in\{1,2\}$，因此 Charlie 发送的信号可以设计为：

$$\boldsymbol{t}_c = \sqrt{\frac{P_c}{N_c-2}}\boldsymbol{V}\boldsymbol{s} \tag{4}$$

式中，P_c代表 Charlie 的传输功率；$\boldsymbol{V}\in\mathbb{C}^{N_c\times(N_c-2)}$为矩阵$(\widetilde{\boldsymbol{h}_{a1}},\widetilde{\boldsymbol{h}_{a2}})$零空间的一组正交基；$\boldsymbol{s}$为服从$\mathcal{CN}(0,\boldsymbol{I}_{N_c-2})$分布的高斯干扰信号。

根据式 (1) 和式 (2)，用户k和窃听者m的接收信号可分别表示为：

$$y_k = \left(\widetilde{\boldsymbol{h}_{ak}}+\boldsymbol{e}_{ak}\right)\left(\sqrt{P_a a_1}\boldsymbol{w}_s x_1+\sqrt{P_a a_2}\boldsymbol{w}_s x_2\right)+\left(\widetilde{\boldsymbol{h}_{ck}}+\boldsymbol{e}_{ck}\right)\boldsymbol{t}_c+n_k \tag{5}$$

$$y_{e,m} = \sqrt{P_a a_1}\boldsymbol{h}_{ae,m}\boldsymbol{w}_s x_1+\sqrt{P_a a_2}\boldsymbol{h}_{ae,m}\boldsymbol{w}_s x_2+\sqrt{\frac{P_c}{N_c-2}}\boldsymbol{h}_{ce,m}\boldsymbol{V}\boldsymbol{s}+n_{e,m} \tag{6}$$

式中，n_k和$n_{e,m}\in\mathcal{CN}(0,1)$分别表示用户$k$和窃听者$m$的加性高斯白噪声。

在 NOMA 系统中，用户利用连续干扰消除 (SIC) 来检测接收到的信号。因此，LU1 首先将x_1视为噪声来解码x_2，然后利用 SIC 消除x_2来解码需求的信号x_1。根据文献 [8]，信道估计误差所产生的噪声和终端噪声可以视为高斯噪声。综上，LU1 和 LU2 的信干噪比 (SINR) 可以分别表示为：

$$\zeta_1 = \frac{P_a a_1\|\widetilde{\boldsymbol{h}_{a1}}\|^2}{P_a\sigma_{a1}^2+P_c\sigma_{c1}^2+1} \tag{7}$$

$$\zeta_2 = \frac{P_a(1-a_1)\|\widetilde{\boldsymbol{h}_{a2}}\boldsymbol{w}_s\|^2}{P_a a_1\|\widetilde{\boldsymbol{h}_{a2}}\boldsymbol{w}_s\|^2+P_a\sigma_{a2}^2+P_c\sigma_{c2}^2+1} \tag{8}$$

窃听者m关于信号x_1的 SINR 可以表示为：

$$\zeta_{e,m} = \frac{P_a a_1\|\boldsymbol{h}_{ae,m}\boldsymbol{w}_s\|^2}{1+P_a(1-a_1)\|\boldsymbol{h}_{ae,m}\boldsymbol{w}_s\|^2+\frac{P_c}{N_c-2}\|\boldsymbol{h}_{ce,m}\boldsymbol{V}\|^2} \tag{9}$$

本系统中，为了实行保密传输，Alice 采用了 Wyner 编码方案，则用户的码字速率和保密速率可以分别表示为$R_k=\log_2(1+\zeta_k), k\in\{1,2\}$和$R_s$，冗余速率$R_k-R_s$可以被利用来对抗窃听。由文献 [12] 和 [14] 可知，在非协作窃听场景中，最大被窃听信息由所有窃听者中最大的 SINR 决定，因此$C_e=\log_2(1+\max_{m\in\mathcal{M}}\zeta_{e,m})$。当$C_e>R_e$时，系统保密传输中断。综上，用户 LU1 的保密中断概率 (SOP) 可以表示为：

$$P_{\text{out}}(R_s,a_1) = \Pr(C_e>R_e) = \Pr(\max_{m\in\mathcal{M}}\zeta_{e,m}>2^{R_1-R_s}-1) \tag{10}$$

1.2 问题描述

为了描述最优化问题，首先定义 LU2 需求的最小传输速率为R_{th}，则受一定保密中断概率约束的保密速率最大最大化 (SRM) 问题可以描述为：

$$\begin{aligned}&\max_{0<a_1\leqslant 0.5}\quad [R_s]^+\\ &\text{s.t.}\quad P_{\text{out}}(R_s,a_1)\leqslant\varepsilon\qquad \log_2(1+\zeta_2)\geqslant R_{th}\end{aligned} \tag{11}$$

式中，$[\cdot]^+$表示 MAX 函数 $\max(\cdot,0)$；$\varepsilon\in(0,1)$为系统可以容忍的最大 SOP。为了简化分析，分别定义 LU1 可以取得的最大有效 SINR 为$\zeta=P_a\|\widetilde{\boldsymbol{h}_{a1}}\|^2/\left(P_a\sigma_{a1}^2+P_c\sigma_{c1}^2+1\right)$及$\delta=2^{R_1-R_s}-1$。因此，式 (11) 可以转化为：

$$\begin{aligned}&\max_{0<a_1\leqslant 0.5}\quad R_s=\log_2\left(\frac{1+\zeta a_1}{1+\delta}\right)\\ &\text{s.t.}\quad \varepsilon=\Pr(\max_{m\in\mathcal{M}}\zeta_{e,m}>\delta)\\ &\qquad \log_2(1+\zeta_2)\geqslant R_{th}\end{aligned} \tag{12}$$

2 自适应功率分配方案

本节提出了一种有效的自适应方法来最大化式 (12) 中的保密速率R_s。值得注意的是，观察式 (12)，a_1的取值需要在一定的范围内才能满足用户 LU2 的 QoS 限制。如果 Alice 无法对 LU2 提供服务，那么 Alice 将会执行文献 [14] 中的协作干扰 (CJ) 方案来保障用户 LU1 的保密通信。

2.1 重新描述 SOP 限制

首先假设式 (12) 中的用户 LU2 的 QoS 限制条件已经满足。为了简化分析，定义$\varepsilon_m=\Pr(\zeta_{e,m}>\delta)$，$m\in\mathcal{M}$，此外还定义如下这些新变量：

$$T_{1,m} = P_a a_1\|\boldsymbol{h}_{ae,m}\boldsymbol{w}_s\|^2 \tag{13}$$

$$T_{2,m} = P_a(1-a_1)\|\boldsymbol{h}_{ae,m}\boldsymbol{w}_s\|^2 \tag{14}$$

$$T_{3,m} = \frac{P_c}{N_c-2}\|\boldsymbol{h}_{ce,m}\boldsymbol{V}\|^2 \tag{15}$$

$$U_m = T_{2,m}+T_{3,m} \tag{16}$$

借助随机理论知识，易得$T_{1,m}\sim\text{Exp}(\kappa_{1,m})$；$T_{2,m}\sim\text{Exp}(\kappa_{2,m})$；$\kappa_{1,m}=1/P_a a_1$；$\kappa_{2,m}=1/P_a(1-a_1)$；$\text{Exp}(\lambda)$表示参数为$\lambda$的指数分布。根据文献 [12]，矩阵$\boldsymbol{h}_{ce,m}$的元服从独立的$\mathcal{CN}(0,1)$分布，因此其每个元的模的平方服从均值为 1 的指数分布。可以得到$\|\boldsymbol{h}_{ce,m}\boldsymbol{V}\|^2\sim\Gamma(N_c-2,1)$，其中，$\Gamma(\alpha,\beta)$表示形状参数为$\alpha$，逆尺度参数为$\beta$的伽马分布。进而可以推出$T_{3,m}\sim\Gamma(N_c-2,\kappa_{3,m})$，$\kappa_{3,m}=N_c-2/P_c$。综上，式 (12) 中的 SOP 表达式可以重写为：

$$\varepsilon_m = \Pr\{\zeta_{e,m}>\delta\} = \Pr\{T_{1,m}>\delta+\delta U_m\} \tag{17}$$

综合式 (13)～式 (17)，再参考文献 [14]，可以得到ε_m的一个闭式表达式。由于篇幅限制，这里省略具体计算过程。因此，ε_m可以重写为：

$$\varepsilon_m = \frac{1}{e^{\kappa_{1,m}\delta}}\left(\frac{\kappa_{2,m}}{\kappa_{2,m}+\kappa_{1,m}\delta}\right)\left(\frac{\kappa_{3,m}}{\kappa_{3,m}+\kappa_{1,m}\delta}\right)^{N_c-2} \tag{18}$$

由于本文考虑多个非协作窃听者场景，由文献 [12,14]，每个窃听者的 SINR 是相互独立的。因此式 (12) 中的 SOP 限制可以改写为：

$$\varepsilon = 1-\Pr(\max_{m\in\mathcal{M}}\zeta_{e,m}\leqslant\delta) = 1-(1-\varepsilon_m)^M \tag{19}$$

定义$\rho(a_1)=\delta/a_1$；$A(a_1)=1+(1-a_1)\rho(a_1)$；$B(a_1)=1+P_c\rho(a_1)/(P_a(N_c-2))$。将式(18) 带入式(19) 中，可得：

$$\ln\left(\frac{1}{1-(1-\varepsilon)^{\frac{1}{M}}}\right) = \frac{\rho(a_1)}{P_a}+\ln[A(a_1)]+(N_c-2)\ln[B(a_1)] \tag{20}$$

2.2　功率分配最优化

讨论功率分配的优化首先需要考虑式 (12) 中用户 LU2 的传输速率限制。可通过计算得到a_1取值的上界：

$$a_1^U = \frac{P_a\|\widetilde{\boldsymbol{h}_{a2}}\boldsymbol{w}_s\|^2-\left(2^{R_{th}}-1\right)\left(P_a\sigma_{a2}^2+P_c\sigma_{c2}^2+1\right)}{2^{R_{th}}P_a\|\widetilde{\boldsymbol{h}_{a2}}\boldsymbol{w}_s\|^2} \tag{21}$$

观察式 (20)，可知$\rho(a_1)>0$。对式 (20) 两边关于a_1进行求导，经过一些等式变换可得：

$$\rho'(a_1) = \frac{P_aB(a_1)\rho(a_1)}{A(a_1)B(a_1)+P_aB(a_1)(1-a_1)+A(a_1)P_c} \tag{22}$$

可得$\rho'(a_1)>0$，因此可以得到$\rho(a_1)$为关于a_1的单调递增函数。

由式 (22)，可得：

$$\frac{\rho'(a_1)}{\rho(a_1)} = \frac{P_aB(a_1)}{A(a_1)B(a_1)+P_aB(a_1)(1-a_1)+A(a_1)P_c} \tag{23}$$

式中，右边分子部分关于a_1单调递增；而分母部分关于a_1单调递减。因此，可得出$\rho'(a_1)/\rho(a_1)$为关于a_1的单调递增函数。

根据式 (12)，$R_s'(a_1)$可以表示为：

$$R_s'(a_1) = \frac{1}{\ln 2}\left[\frac{\zeta}{1+\zeta a_1}-\frac{\rho(a_1)+a_1\rho'(a_1)}{1+a_1\rho(a_1)}\right] \tag{24}$$

$$= \frac{\zeta-\rho(a_1)}{(1+\zeta a_1)[1+a_1\rho(a_1)]\ln 2}-\frac{\dfrac{\rho'(a_1)}{\rho(a_1)}}{\left[1+\dfrac{1}{a_1\rho(a_1)}\right]\ln 2} \tag{25}$$

结合前面所得出的结论，式 (25) 中，右边第一项为关于a_1的严格单减函数，第二项为关于a_1的严格单增函数。因此可得$R_s''(a_1)<0$。根据凸优化理论[15]，可得R_s为关于a_1的凹函数。

利用上述讨论的结果，可以得出一个能有效解决式 (12) 的自适应方案。根据不同情况具体讨论步骤如下：

1) 情况 1：$a_1^U\leqslant 0$。此时用户 LU2 的 QoS 需求无法被满足，因此 Alice 停止对 LU2 进行服务，采用文献 [14] 中提出的传统正交多址接入 CJ 方案来对 LU1 进行保密通信。此时，功率分配系数$a_1\in[0,1]$。

2) 情况 2：$a_1^U>0.5$。此时用户 LU2 的 QoS 需求无论如何都会被满足，因此式 (12) 中可去掉关于 LU2 的 QoS 限制条件。此时，对用户 LU1 来说，信号x_2可以被视为 Alice 生成的用来对抗窃听的人工噪声，进而参考文献 [14] 中提出的 CJ 方案得到a_1^*。

3) 情况 3：$0<a_1^U\leqslant 0.5$。该情况下，需要在 LU1 的保密速率和 LU2 的 QoS 需求之间做权衡。假设$a_{1,\text{opt}}\in(0,0.5]$和$R_s^*(a_1)$分别表示满足$R_s'(a_{1,\text{opt}})=0$的最优特解和相应的最大保密速率。接下来需要分不同情况进行讨论：

① 若$R_s'(0.5)\geqslant 0$，可得$\zeta>\rho(0.5)$。因此，若$a_1^U=0.5$，可得$a_1^*=0.5$, $R_s^*(a_1)=R_s(0.5)$，否则，$a_1^*=a_1^U$，$R_s^*(a_1)=R_s(a_1^U)$；

② 若$R_s'(0.5)<0$ 且 $R_s'(0)>0$，根据凹函数的特性，一定存在特解$a_{1,\text{opt}}$。因此，若$a_{1,\text{opt}}\leqslant a_1^U$，则$a_1^*=a_{1,\text{opt}}$, $R_s^*(a_1)=R_s(a_{1,\text{opt}})$，否则，$a_1^*=a_1^U$,$R_s^*(a_1)=R_s(a_1^U)$；

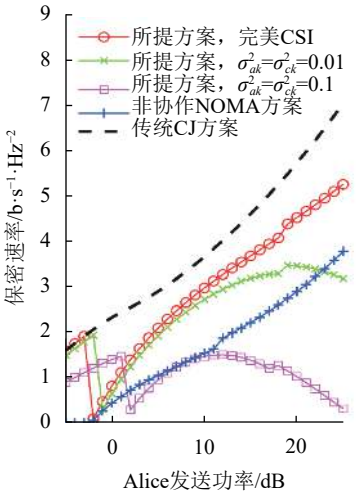
③ 若$R_s'(0)\leqslant 0$，由式 (24) 可得，$\zeta<\rho(0)$。因此 Alice 停止保密传输，此时$a_1^*=0^+$且$R_s^*(a_1)=R_s(0^+)$。

3　仿真结果及分析

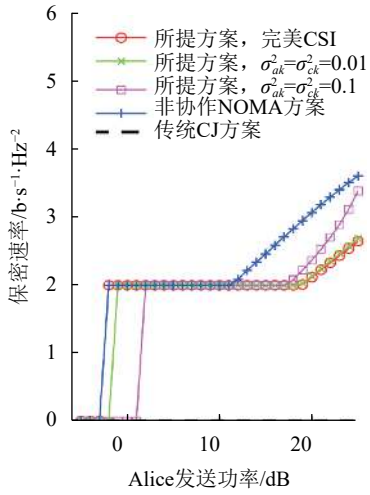
本节对所提方案在完美信道信息和非完美信道信息场景中的性能进行仿真，并与文献 [11] 所提非协作 NOMA 方案以及文献 [14] 所提的传统 CJ 方案 (仅对 LU1 服务) 进行对比。基本参数设置如下：$N_a=4$；$N_c=4$；$M=4$；$\varepsilon=0.01$；$P_c=10$ dB；$\|\widetilde{\boldsymbol{h}_{a1}}\|^2=10$ dB；$\|\widetilde{\boldsymbol{h}_{a2}}\|^2=5$ dB 以及$R_{th}=2$ bit/s/Hz。不失一般性，仿真中假设$\sigma_{ak}^2=\sigma_{ck}^2$，$k\in\{1,2\}$。本节中每次实验结果都是通过 200 次仿真取平均得到的。

图 2 分别对比了用户 LU1 的保密速率和用户 LU2 的传输速率表现。从图 2 可以看出，由于需要执行 NOMA 规则同时对 LU1 和 LU2 进行服务，对比传统 CJ 方案，本文所提方案在保密速率上不可避免有一定损失。由图 2a 可以看出，所提方案性能明显优于非协作方案，特别是当$P_a<-3$，$a_1^U<0$时，本文方案通过自适应策略调整对功率分配系数进行了优化。具体来说，当$P_a<-3$，用户 LU2 的 QoS 要求不能被满足，Alice 停止对 LU2 服务，Alice 采用传统 CJ 方案对 LU1 进行保密传输。当$P_a\geqslant-2$ 时，Alice 开始根据 NOMA 原理对 LU2 进行服务，为了同时对 LU1 和 LU2 进行服务，LU1 的保密速率R_s首先降至 0，而后随着P_a的增加而增长。图 2b 的结果证明了所提功率分配方案的有效性，当P_a从–3 dB 增长到 19 dB，a_1^*被设置为a_1^U，而R_2维持在R_{th}。同非协作 NOMA 方案相比，由于有协作干扰的帮助，在本方案中，当 LU2 的 QoS 需求被满足时，Alice 可以分配更多的功率用于服务 LU1。此外，从图 2 结果可知，若信道信息非完美，a_1^U将相应地减小，不仅导致 LU2 的 QoS 要求更难被满足，还使得 LU1 信息被泄露，造成保密性能急剧下降。

图 3 对比了几种方案的有效和速率和有效能量效率性能表现。可以看出在绝大部分总功率范围内，本文方案性能表现明显更优。同时，图 3 再次验证了非完美信道信息对系统性能造成的严重影响，且对系统的影响程度随着信道不确定程度的增加而增加。

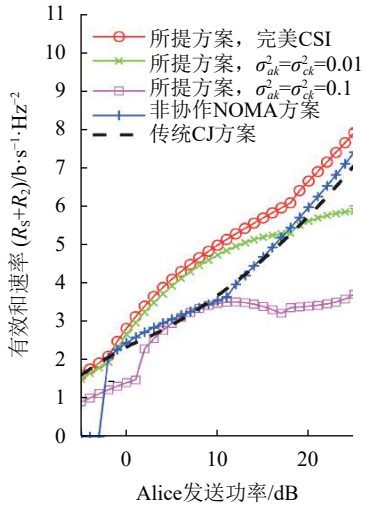


a. 不同方案 LU1 保密速率比较

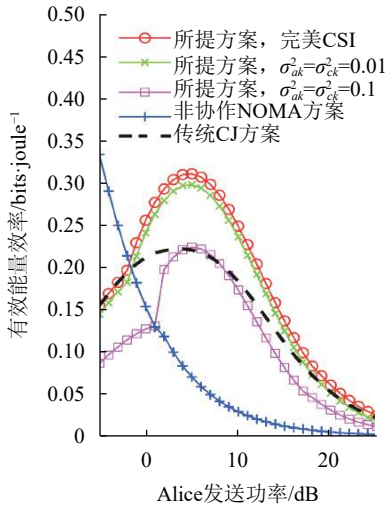


b. 不同方案 LU2 传输速率比较

图 2 LU1 保密速率和 LU2 传输速率性能比较



a. 不同方案有效和速率比较



b. 不同方案有效能量速率比较

图 3 有效和速率与有效能量效率性能比较

4 结束语

本文在非完美信道信息场景中，针对协作NOMA系统中保密中断概率限制条件下的保密速率最大化问题，提出了一种自适应功率分配算法。仿真结果验证了本方案能有效灵活地提高系统安全性能和能效，具有环境适应性。同时，仿真结果表明，非完美信道信息会导致严重的系统安全性能以及能效下降，如何应对非完美信道信息对协作NOMA系统带来的影响有待进一步研究。

参 考 文 献

[1] DAI Ling-long, WANG Bai-chai, YUAN Yi-fei, et al. Non-orthogonal multiple access for 5G: Solutions, challenges, opportunities, and future research trends[J]. IEEE Communications Magazine, 2015, 53(9): 74-81.

[2] DING Zhi-guo, LEI Xian-fu, KARAGIANNIDIS G K, et al. A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends[J]. IEEE Journal on Selected Areas in Communications, 2017, 35(10): 2181-2195.

[3] DING Zhi-guo, PENG Mu-gen, POOR H V. Cooperative non-orthogonal multiple access in 5G systems[J]. IEEE Communications Letters, 2015, 19(8): 1462-1465.

[4] CHEN Jian-chao, YANG Liang, ALOUINI M S. Physical layer security for cooperative NOMA systems[J]. IEEE Transactions on Vehicular Technology, 2018, 67(5): 4645-4649.

[5] YU Chao, KO H L, PENG Xin, et al. Jammer-aided secure communications for cooperative NOMA systems[J]. IEEE Communications Letters, 2019, 23(11): 1935-1939.

[6] CAO Yang, ZHAO Nao, PAN Gao-feng, et al. Secrecy analysis for cooperative NOMA networks with multi-antenna full-duplex relay[J]. IEEE Transactions on Communications, 2019, 67(8): 5574-5587.

[7] ARZYKULOV S, TSIFTSIS T A, NAURYZBAYEV G, et al. Outage performance of cooperative underlay CR-NOMA with imperfect CSI[J]. IEEE Communication Letters, 2019, 23(1): 176-179.

[8] SU Bin-bin, NI Qiang, YU Wen-juan. Robust transmit beamforming for SWIPT-enabled cooperative NOMA with channel uncertainties[J]. IEEE Transactions on Communications, 2019, 67(6): 4381-4392.

[9] YUAN Yi, XU Peng, YANG Zheng, et al. Joint robust beamforming and power-splitting ratio design in SWIPT-based cooperative NOMA systems with CSI uncertainty[J]. IEEE Transactions on Vehicular Technology, 2019, 68(3): 2386-2400.

[10] VO V N, SOIN C, TRAN H, et al. On security and throughput for energy harvesting untrusted relays in IoT systems using NOMA[J]. IEEE Access, 2019, 7: 149341-149354.

[11] FENG You-hong, YAN Shi-hao, YANG Zhen. Secure transmission to the strong user in non-orthogonal multiple access[J]. IEEE Communications Letters, 2018, 22(12): 2623-2626.

[12] CHEN Yang, ZHANG Zhong-pei. UAV-aided secure transmission in MISOME wiretap channels with imperfect CSI[J]. IEEE Access, 2019, 7: 98107-98121.

[13] LV Lu, DING Zhi-guo, NI Qiang, et al. Secure MISO-NOMA transmission with artificial noise[J]. IEEE Transactions on Vehicular Technology, 2018, 67(7): 6700-6705.

[14] HU Lin, WEN Hong, WU Bin, et al. Cooperative-jamming-aided secrecy enhancement in wireless networks with passive eavesdroppers[J]. IEEE Transactions on Vehicular Technology, 2018, 67(3): 2108-2117.

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

编　辑　刘飞阳