# 基于短包通信的 NOMA 下行链路安全传输

孙钢灿[1,2,3]，赵少柯[1,2]，郝万明[2,3]，朱政宇[2,3]

（1. 郑州大学河南先进技术研究院，河南 郑州 450003；2. 郑州大学产业技术研究院，河南 郑州 450001；
3. 郑州大学信息工程学院，河南 郑州 450001）

**摘 要**：面向物联网业务中的低时延需求，将短包通信（SPC）和非正交多址接入（NOMA）技术相结合，针对存在窃听者的情况研究多用户 NOMA 系统中的安全传输问题。以最大化弱用户的安全吞吐量为目标，考虑用户译码错误概率约束、总功率约束和功率分配约束，提出了一种低复杂度的功率分配方案实现系统安全传输。为解决复杂的目标函数和不可靠的串行干扰消除（SIC）技术带来的问题，首先证明约束条件在取得最优解时的紧约束性，在最大译码错误概率约束下，对功率约束进行转化和计算，得到强用户发射功率范围，推导出基站向强用户的发射功率搜索集；然后利用一维搜索算法对功率进行分配，实现弱用户吞吐量最大化。仿真结果证明，所提方案可有效提高系统中弱用户的安全吞吐量。

**关键词**：短包通信；非正交多址接入；安全吞吐量；功率分配

**中图分类号**：TN929

**文献标识码**：A

**DOI:** 10.11959/j.issn.1000−436x.2021041

# Secure transmission for NOMA downlink based on short packet communication

SUN Gangcan[1,2,3], ZHAO Shaoke[1,2], HAO Wanming[2,3], ZHU Zhengyu[2,3]

1. Henan Institute of Advanced Technology, Zhengzhou University, Zhengzhou 450003, China
2. Industrial Technology Research Institute, Zhengzhou University, Zhengzhou 450001, China
3. School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China

**Abstract:** For the low-latency requirements of Internet of things (IoT) business, short packet communication (SPC) and non-orthogonal multiple access (NOMA) were combined to study the problem of secure transmission in the multi-user NOMA system with eavesdroppers. With the maximizing the secure throughput of weak uses as the objective, considering the user decoding error probability constraint, total power constraint and power allocation constraint, a low-complexity power allocation algorithm was proposed to realize secure transmission. In order to solve the problem caused by complex objective function formula and unreliable serial interference cancellation (SIC) technology, the proof that the compactness of the constraints was necessary to find the optimal solution. Under the constraint of maximum decoding error probability, the power constraint was transformed and calculated to obtain the strict limit of transmitting power for strong users, and the transmit power search set from base station to strong user was derived. Then, the one-dimensional search algorithm was used to allocate power resources to maximize the throughput of weak users. Simulation results prove that the proposed algorithm can effectively improve the security throughput of weak users in the system.

**Keywords:** short packet communication, non-orthogonal multiple access, secure throughput, power allocation

**收稿日期**：2020−08−06；**修回日期**：2020−09−25

**通信作者**：郝万明，iewmhao@zzu.edu.cn

**基金项目**：国家自然科学基金资助项目（No.61801435）；河南省科技攻关基金资助项目（No.202102210119）；郑州市重大科技创新专项基金资助项目（No.2019CXZX0037）

**Foundation Items:** The National Natural Science Foundation of China (No.61801435), Science and Technology Project of Henan Province (No.202102210119), Major Science and Technology Innovation Project of Zhengzhou (No.2019CXZX0037)

## 1　引言

随着第五代移动通信（5G, fifth-generation mobile communication）的普及和终端设备的小型化、智能化，未来无线通信将会出现更多的人与物、物与物之间的高速连接应用，因此物联网（IoT, Internet of things）技术将会得到快速发展[1-2]。根据全球移动通信系统协会统计数据显示，到 2020 年年底已有 126 亿个智能设备连接到工业自动化、智能城市、智能交通和智能家居等行业，预计 2025 年全球物联网设备（包括蜂窝及非蜂窝）联网数量将达到 246 亿[3-4]。在 IoT 中，机器设备之间的主要通信方式为机器类型通信（MTC, machine-type communication）。MTC 设备发送数据的时间是随机的，数据长度较短且不固定，可以从几字节到几百字节[5-7]，但是会在一段时间内以较高频率发送，这使发送设备为了传输内容而进行的信令交互占用的资源通常大于传输内容占用的资源。因此传统基于香农容量的无限包长通信技术不再适合 MTC 通信网络[8]，而采用有限包长的短包通信（SPC, short packet communication）技术逐渐受到学术界和工业界的关注。SPC 是指采用有限包长的短数据包进行通信的技术，它可以有效降低传输时延[9-10]。

与正交多址接入（OMA, orthogonal multiple access）技术不同[11]，非正交多址接入（NOMA, non-orthogonal multiple access）技术摆脱了正交性的约束，在信号发送端通过功率复用或叠加编码（SC, superposition coding）[12]，使不同用户可以占用相同的频谱、时间等资源，实现多个用户的资源共享，提高系统的频谱效率[13-14]。同时，NOMA 技术也带来了多用户干扰（MUI, multiple user interfere），需要在接收端采用串行干扰消除（SIC, serial interference cancellation）技术解调，消除 MUI[15-16]。

较高的安全性是 IoT 所必须具备的特性[17]。随着以人为中心的智能家居和智慧医疗等业务的出现，IoT 应用面临隐私泄露、财产损失和恶意入侵等安全挑战，由于无线通信的广播性质，IoT 系统容易被恶意窃听，因此需要通过加密技术来提高系统的安全性。采用通信协议栈的上层加密技术是比较常用的加密方法，但是需要分配大量资源进行密钥生成、分发和管理[18]，耗费资源较多，系统复杂度较高，相比之下，物理层安全性更具吸引力，它通过利用无线信道的随机性来实现保密功能，从而消除了对密钥的需求，大大降低了系统复杂度[19-20]。

与香农近似的信道容量准则不同，由于 SPC 的包长较小，因此在接收端的译码错误概率不可忽略，SPC 需以传输速率和译码错误概率作为系统有效性和可靠性的指标[21-22]。文献[23-24]从信息论的角度研究了 SPC 的性能，文献[23]分析了在给定包长和译码错误概率情况下的用户最大可达速率；文献[24]给出了 SPC 在信道分布和译码错误概率影响下的最大可达速率，并给出证明。近年来，SPC 技术在 NOMA 系统中的应用受到了业界的广泛关注。文献[25]研究了基于 SPC 的 NOMA 下行链路中强用户吞吐量最大化问题；文献[26]分析了 SPC 的多用户下行链路系统中总速率和译码错误概率之间的关系并权衡两者之间的性能；文献[27]在时延和译码错误概率一定情况下，研究了基站发送功率最小化问题。但是上述工作均未考虑 SPC 传输时的安全性。文献[28]研究了存在窃听者的 IoT 系统中 SPC 的安全性，但并未考虑多用户和 NOMA 场景。

针对以上问题，本文考虑存在窃听者的多用户 NOMA 系统中的短包安全传输问题，在满足最大译码错误概率约束、总功率约束和功率分配约束的情况下，对基站发射功率进行优化。在 NOMA 系统中，给定包长的译码错误概率函数相对于发射功率而言是不连续的，这使优化问题变得复杂。本文首先证明约束条件在最优解时为紧约束，在保证强用户一定的译码错误概率目标的同时，可通过一维线性搜索算法找到最优解，最大化弱用户的安全吞吐量，最终在用户吞吐量和公平性之间取得平衡。

## 2　系统模型

基于 SPC 的 NOMA 下行链路系统模型如图 1 所示。本文假设一个基站为 2 个合法用户提供服务，其中，基站、用户和窃听者均配备单天线。从基站到用户和窃听者的信道增益分别为 $h_i$（$i\in\{1,2\}$）和 $h_{\mathrm{e}}$，$h_i$ 和 $h_{\mathrm{e}}$ 为独立准静态瑞利衰落。假设 $0<|h_2|^2<|h_1|^2$，定义用户 2 为弱用户。本文考虑以下场景：用户 1 采用非保密的广播通信，用于台风警报、火灾警报等；用户 2 采用保密传输，根据 NOMA 技术原理，为了确保弱用户达到目标速率，基站将为信道质量较差的用户 2 分配较高的发射功率，同时窃听者窃听用户 2 的信息。


图 1 基于 SPC 的 NOMA 下行链路系统模型

### 2.1 弱用户信号传输模型

用户 2 接收到的信号为

$$y_2 = h_2\left(\sqrt{P_1}x_1 + \sqrt{P_2}x_2\right) + n_2 \tag{1}$$

其中，$x_1$ 和 $x_2$ 分别是基站向用户 1 和用户 2 发送的信号，$P_1$ 和 $P_2$ 分别是基站分配给 $x_1$ 和 $x_2$ 的发射功率，$n_2 \sim \mathcal{CN}\left(0,\sigma_2^2\right)$ 表示均值为 0 且方差为 $\sigma_2^2$ 的加性白高斯噪声（AWGN, additive white Gaussian noise）。

用户 2 处的 SPC 保密传输速率封闭表达式近似为[28-29]

$$R_2 = \mathrm{lb}\left(1+\gamma_2\right) - \mathrm{lb}\left(1+\gamma_{\mathrm{e}}\right) - \sqrt{\frac{V_2}{N_2}}\frac{Q^{-1}\left(\varepsilon_2\right)}{\ln 2} - \sqrt{\frac{V_{\mathrm{e}}}{N_2}}\frac{Q^{-1}\left(\delta\right)}{\ln 2} \tag{2}$$

其中，$\gamma_2$ 为用户 2 的信噪比（SNR, signal-to-noise ratio），$\gamma_{\mathrm{e}}$ 为窃听者的信干噪比（SINR, signal-to-interference-plus-noise ratio），$N_2$ 为分给用户 2 的包长，$V_2 = 1-\left(1+\gamma_2\right)^{-2}$ 和 $V_{\mathrm{e}} = 1-\left(1+\gamma_{\mathrm{e}}\right)^{-2}$ 分别为用户 2 和窃听者的信道色散，$\varepsilon_2$ 为用户 2 的译码错误概率，$\delta$ 为信息的保密速率约束，$Q^{-1}\left(\cdot\right)$ 为标准正态分布右尾函数 $Q\left(x\right) = \dfrac{\int_x^{\infty}\mathrm{e}^{\frac{-t^2}{2}}\mathrm{d}t}{\sqrt{2\pi}}$ 的反函数。由式(2)可得 $\gamma_2 > \gamma_{\mathrm{e}}$，否则用户 2 的保密传输速率为 0。

由于 $0 < \left|h_2\right|^2 < \left|h_1\right|^2$，用户 2 可将 $x_1$ 视为干扰，直接对 $x_2$ 进行解码，$x_2$ 在用户 2 处的 SINR 为

$$\gamma_2 = \frac{P_2\left|h_2\right|^2}{P_1\left|h_2\right|^2 + \sigma_2^2} \tag{3}$$

结合式(2)，对以译码错误率为变量的 $Q^{-1}\left(x\right)$ 取反函数，可得 $\gamma_2$ 对应得译码错误概率为

$$\varepsilon_2 = Q\left(f_1\left(\gamma_2, N_2, R_2\right)\right) \tag{4}$$

其中，$f_1\left(\gamma_2, N_2, R_2\right) = \sqrt{\dfrac{N_2}{V_2}}\left(\ln\dfrac{1+\gamma_2}{1+\gamma_{\mathrm{e}}} - Q^{-1}\left(\delta\right)\sqrt{\dfrac{V_{\mathrm{e}}}{N_2}} - R_2\ln 2\right)$。

在 NOMA 系统中，不同信道增益的用户采用不同的译码策略。由于 $0 < \left|h_2\right|^2 < \left|h_1\right|^2$，因此在用户 2 处仅存在一种译码策略，其有效译码错误率为

$$\bar{\varepsilon}_2 = \varepsilon_2 \tag{5}$$

### 2.2 强用户信号传输模型

用户 1 接收到的信号为

$$y_1 = h_1\left(\sqrt{P_1}x_1 + \sqrt{P_2}x_2\right) + n_1 \tag{6}$$

其中，$n_1 \sim \mathcal{CN}\left(0,\sigma_1^2\right)$ 表示均值为 0 且方差为 $\sigma_1^2$ 的 AWGN。

采用非保密传输的用户 1 的 SPC 传输速率可近似为[25]

$$R_1 = \mathrm{lb}(1+\gamma_1) - \sqrt{\frac{V_1}{N_1}}\frac{Q^{-1}\left(\varepsilon_1\right)}{\ln 2} \tag{7}$$

其中，$\gamma_1$ 为用户 1 接收信号的 SNR，$V_1 = 1-\left(1+\gamma_1\right)^{-2}$ 为用户 1 的信道色散，$N_1$ 为分配给用户 1 的数据包长，$\varepsilon_1$ 为用户 1 的译码错误概率。

由于 $0 < \left|h_2\right|^2 < \left|h_1\right|^2$，当用户 1 采用 SIC 解码时，将首先对 $x_2$ 译码，根据式(6)可得 $x_2$ 在用户 1 处的 SINR 为

$$\gamma_2^1 = \frac{P_2\left|h_1\right|^2}{P_1\left|h_1\right|^2 + \sigma_1^2} \tag{8}$$

结合式(2)，对 $Q^{-1}\left(x\right)$ 取反函数，可得 $x_2$ 在用户 1 处的译码错误率为

$$\varepsilon_2^1 = Q\left(f_1\left(\gamma_2^1, N_2, R_2\right)\right) \tag{9}$$

如果 SIC 解码成功，用户 1 将以 $1-\varepsilon_2^1$ 的概率移除 $x_2$，之后解码 $x_1$，则 $x_1$ 在用户 1 处的 SNR 和译码错误概率分别为

$$\gamma_1 = \frac{P_1\left|h_1\right|^2}{\sigma_1^2} \tag{10}$$

$$\varepsilon_1 = Q\left(f_2\left(\gamma_1, N_1, R_1\right)\right) \tag{11}$$

其中，$f_2\left(\gamma_1, N_1, R_1\right) = \mathrm{lb}\sqrt{\dfrac{N_1}{V_1}}\left(\mathrm{lb}\left(1+\gamma_1\right) - R_1\right)$。

当 SIC 解码失败时，用户 1 将 $x_2$ 视为干扰，首先对 $x_1$ 进行解码，则对应的 SINR 和译码错误概率分别为

$$\gamma_1' = \frac{P_1 |h_1|^2}{P_2 |h_1|^2 + \sigma_1^2} \tag{12}$$

$$\varepsilon_1' = Q\left(f_2\left(\gamma_1', N_1, R_1\right)\right) \tag{13}$$

根据以上分析，$x_1$ 在用户 1 处的有效译码错误概率为

$$\bar{\varepsilon}_1 = \left(1-\varepsilon_2^1\right)\varepsilon_1 + \varepsilon_2^1\varepsilon_1' = \varepsilon_1 + \varepsilon_2^1\left(\varepsilon_1' - \varepsilon_1\right) \tag{14}$$

### 2.3　窃听者信号传输模型

窃听者接收到的信号为

$$y_{\mathrm{e}} = h_{\mathrm{e}}\left(\sqrt{P_1}x_1 + \sqrt{P_2}x_2\right) + n_{\mathrm{e}} \tag{15}$$

其中，$n_{\mathrm{e}} \sim \mathcal{CN}(0, \sigma_{\mathrm{e}}^2)$ 表示均值为 0 且方差为 $\sigma_{\mathrm{e}}^2$ 的 AWGN。

在对用户 2 进行窃听时，窃听者需要通过 SIC 技术剔除接收到的用户 1 的信号，因此可采用类似用户 2 的接收机模型，将 $x_1$ 视为干扰而对 $x_2$ 进行解码，则 $x_2$ 在窃听者处的 SINR 为

$$\gamma_{\mathrm{e}} = \frac{P_2 |h_{\mathrm{e}}|^2}{P_1 |h_{\mathrm{e}}|^2 + \sigma_{\mathrm{e}}^2} \tag{16}$$

由于窃听者处接收机对 $x_2$ 的 SIC 解码成功与否不会影响用户 2 的传输速率以及吞吐量，因此不考虑窃听者的译码错误概率。

## 3　弱用户安全吞吐量最大化问题的形成

在基于 SPC 的多用户 NOMA 系统中，用户 $i$ 的有效吞吐量定义为

$$\bar{T}_i = \frac{N_i}{N} R_i \left(1 - \bar{\varepsilon}_i\right) \tag{17}$$

其中，$i \in \{1,2\}$ 表示用户，$N_i$ 和 $R_i$ 分别表示基站向用户 $i$ 发送的最大包长和传输速率，$\bar{\varepsilon}_i$ 表示用户 $i$ 处的有效译码错误概率。由于 SPC 每次都发送较短的信息，为了简化计算与优化过程，本文以单位信道传输比特数（BPCU, bit per channel use）代替 bit/s 来衡量传输速率的大小[26,28]，假设基站每次发送 $B$ bit 信息，则传输速率可重新定义为[30]

$$R_i = \frac{B}{N_i} \tag{18}$$

为了降低优化问题的复杂度，平均可达保密吞吐量可重新定义为[28]

$$\bar{T}_i = \frac{N_i}{N}\frac{B}{N_i}\left(1-\bar{\varepsilon}_i\right) = \frac{B}{N}\left(1-\bar{\varepsilon}_i\right) \tag{19}$$

本文的目标是在译码错误概率约束和功率约束条件下最大化弱用户（用户 2）的安全吞吐量，优化问题可表示为

$$\mathrm{P1}: \max_{\{N_1, N_2, P_1, P_2\}} \bar{T}_2 \tag{20}$$

$$\text{s.t.}\quad P_1 N_1 + P_2 N_2 \leqslant PN \tag{20a}$$

$$0 \leqslant P_1 \leqslant P_2 \tag{20b}$$

$$0 \leqslant \bar{\varepsilon}_1 \leqslant \varepsilon_0 \tag{20c}$$

$$\gamma_2 > \gamma_{\mathrm{e}} \tag{20d}$$

其中，式(20a)为系统总发射功率约束，$P$ 为基站最大发射功率；式(20b)确保基站向用户 2 分配更多传输功率；式(20c)为用户 1 的译码错误概率约束，$\varepsilon_0$ 为用户 1 的最大译码错误概率；式(20d)保证用户 2 的保密传输速率大于 0。

## 4　优化问题 P1 的求解

在 NOMA 系统中，基站可以通过 SC 对多个传输信号进行分层编码调制，在相同的时频资源块上，通过不同的功率分级，在功率域实现多址接入。相比于相同条件下的 OMA 系统，NOMA 可使通信系统的吞吐量提高 50%[31]，令 $N = N_1 = N_2$，则 P1 可转化为

$$\mathrm{P2}: \max_{\{P_1, P_2\}} \bar{T}_2 \tag{21}$$

$$\text{s.t.}\quad P_1 + P_2 \leqslant P \tag{21a}$$

$$0 \leqslant P_1 \leqslant P_2 \tag{21b}$$

$$0 \leqslant \bar{\varepsilon}_1 \leqslant \varepsilon_0 \tag{21c}$$

$$\gamma_2 > \gamma_{\mathrm{e}} \tag{21d}$$

由式(14)可得

$$\varepsilon_1 \leqslant \bar{\varepsilon}_1 = \varepsilon_1 + \varepsilon_2^1\left(\varepsilon_1' - \varepsilon_1\right) \tag{22}$$

结合式(22)和式(21c)可得

$$\varepsilon_1 \leqslant \varepsilon_0 \tag{23}$$

当以最低标准保证用户 1 的吞吐量时，可进一步最大化用户 2 的吞吐量，因此当式(23)取等号时，问题 P2 可取到最优解[30]，将 $\varepsilon_1 = \varepsilon_0$ 代入式(11)，可获得 $\gamma_1$ 的下界为

$$\gamma_1^{\mathrm{LB}} \triangleq f_2^{-1}\left(Q^{-1}\left(\varepsilon_0\right)\right) \tag{24}$$

定义 $P_1$ 的下界为

$$P_1^{\mathrm{LB}} \triangleq \frac{\gamma_1^{\mathrm{LB}}\sigma_1^2}{|h_1|^2} \tag{25}$$

**定理 1** 用户 2 的译码错误概率 $\varepsilon_2$ 是关于 $\gamma_2$ 的单调递减函数。

**证明** 由式(4)可推导出 $\varepsilon_2$ 关于 $\gamma_2$ 的偏导数为

$$\frac{\partial \varepsilon_2}{\partial \gamma_2}=-\frac{1}{\sqrt{2\pi}}\mathrm{e}^{-\frac{f_1^2(\gamma_2,N_2,R_2)}{2}}\frac{\partial f_1(\gamma_2,N_2,R_2)}{\partial \gamma_2} \tag{26}$$

其中，$-\frac{1}{\sqrt{2\pi}}\mathrm{e}^{-\frac{f_1^2(\gamma_2,N_2,R_2)}{2}}<0$。

令 $\phi=\mathrm{lb}(1+\gamma_{\mathrm{e}})+\sqrt{\frac{V_{\mathrm{e}}}{N_2}}\frac{Q^{-1}(\delta)}{\ln 2}>0$，有

$$f_1(\gamma_2,N_2,R_2)=\sqrt{\frac{N_2}{V_2}}\left(\mathrm{lb}(1+\gamma_2)-R_2-\phi\right)\ln 2 \tag{27}$$

令 $\varphi=R_2+\phi>0$，有

$$f_1(\gamma_2,N_2)=\sqrt{\frac{N_2}{V_2}}\left(\mathrm{lb}(1+\gamma_2)-\varphi\right)\ln 2=$$

$$\sqrt{\frac{N_2}{1-(1+\gamma_2)^{-2}}}\left(\mathrm{lb}(1+\gamma_2)-\varphi\right)\ln 2 \tag{28}$$

$f_1(\gamma_2,N_2)$ 关于 $\gamma_2$ 的偏导数为

$$\frac{\partial f_1(\gamma_2,N_2)}{\partial \gamma_2}=\sqrt{N_2}\frac{1+\frac{\mathrm{lb}(1+\gamma_2)-\varphi}{1-(1+\gamma_2)^2}\ln 2}{\sqrt{(1+\gamma_2)^2-1}} \tag{29}$$

令 $\psi=1+\gamma_2$，由 $\gamma_2>0$ 可得 $\psi>1$，定义函数 $\mathcal{U}(\psi)$ 为

$$\mathcal{U}(\psi)=\frac{\mathrm{lb}\,\psi}{\psi^2-1} \tag{30}$$

对 $\mathcal{U}(\psi)$ 求导可得

$$\mathcal{U}'(\psi)=\frac{\psi-\frac{1}{\psi}}{\ln 2}-2\psi\,\mathrm{lb}\,\psi}{\left(\psi^2-1\right)^2} \tag{31}$$

令 $u(\psi)=\frac{\psi-\frac{1}{\psi}}{\ln 2}-2\psi\,\mathrm{lb}\,\psi$，对 $u(\psi)$ 求导可得

$$u'(\psi)=-\frac{1-\frac{1}{\psi^2}}{\ln 2}-2\,\mathrm{lb}\,\psi \tag{32}$$

由于 $\psi>1$，因此 $u'(\psi)<0$，$u(\psi)$ 是一个单调递减函数，进而可得

$$u(\psi)<u(1)=0 \tag{33}$$

由于 $\left(\psi^2-1\right)^2>0$，将式(33)代入式(31)得 $\mathcal{U}'(\psi)<0$，因此 $\mathcal{U}(\psi)$ 是单调递减函数。对式(30)采用洛必达法则分析可得

$$\begin{cases}\lim\limits_{\psi\to 1}\mathcal{U}(\psi)=\lim\limits_{\psi\to 1}\dfrac{1}{2\psi^2\ln 2}=\dfrac{1}{2\ln 2}\\ \lim\limits_{\psi\to\infty}\mathcal{U}(\psi)=\lim\limits_{\psi\to\infty}\dfrac{1}{2\psi^2\ln 2}=0\end{cases} \tag{34}$$

结合式(34)和 $\mathcal{U}(\psi)$ 的单调性可得

$$0<\mathcal{U}(\psi)<\frac{1}{2\ln 2} \tag{35}$$

由式(35)可得

$$1-\ln 2\frac{\mathrm{lb}(1+\gamma_2)-\varphi}{(1+\gamma_2)^2-1}\geqslant 1+\ln 2\frac{\mathrm{lb}(1+\gamma_2)}{(1+\gamma_2)^2-1}=$$

$$1-\ln 2\mathcal{U}(\gamma_2+1)>1-\ln 2\frac{1}{2\ln 2}=\frac{1}{2}>0 \tag{36}$$

将式(36)代入式(29)，由于 $\sqrt{(1+\gamma_2)^2-1}>0$，因此可得

$$\frac{\partial f_1(\gamma_2,N_2)}{\partial \gamma_2}>0 \tag{37}$$

将式(37)代入式(26)可得

$$\frac{\partial \varepsilon_2}{\partial \gamma_2}<0 \tag{38}$$

即用户 2 的译码错误概率 $\varepsilon_2$ 是关于 $\gamma_2$ 的单调递减函数。类似地，由式(38)可以证明 $\varepsilon_1$、$\varepsilon_2^1$、$\varepsilon_1'$ 分别是关于 $\gamma_1$、$\gamma_2^1$、$\gamma_1'$ 的单调递减函数。

证毕。

本文的优化目标是保证用户 1 吞吐量达到一定标准的情况下最大化用户 2 的吞吐量。由式(19)可得，通过发射功率的提升，可以减少译码错误概率，进而增大用户的吞吐量，因此在不超过基站最大发射功率范围的情况下，应尽可能地将基站发射功率利用率最大化。因此根据定理 1，可得定理 2。

**定理 2** 约束式(21a)取等号时，优化问题 P2 可取得最优解。

**证明** 假设最佳功率分配方案为 $P_1'$ 和 $P_2'$，且满足

$$P_1'+P_2'<P \tag{39}$$

对应的最优解为 $\overline{T}_2'$，由式(3)可得 $\gamma_2'$ 为

$$\gamma_2' = \frac{P_2'|h_2|^2}{P_1'|h_2|^2 + \sigma_2^2} \tag{40}$$

令 $\lambda = \dfrac{P}{P_1' + P_2'}$，由式(39)得 $\lambda > 1$。因此可得 $P_1'' = \lambda P_1' > P_1'$，$P_2'' = \lambda P_2' > P_2'$，二者满足

$$P_1'' + P_2'' = P \tag{41}$$

对应的最优解为 $\overline{T}_2''$，对应的 $\gamma_2''$ 为

$$\gamma_2'' = \frac{P_2''|h_2|^2}{P_1''|h_2|^2 + \sigma_2^2} \tag{42}$$

将 $P_1''$ 和 $P_2''$ 代入式(42)可得

$$\gamma_2'' = \frac{\lambda P_2'|h_2|^2}{\lambda P_1'|h_2|^2 + \sigma_2^2} = \frac{P_2'|h_2|^2}{P_1'|h_2|^2 + \dfrac{\sigma_2^2}{\lambda}} \tag{43}$$

结合式(40)和式(43)可得

$$\gamma_2'' > \gamma_2' \tag{44}$$

根据定理 1 可得对应的译码错误概率关系为

$$\varepsilon_2'' < \varepsilon_2' \tag{45}$$

由式(19)可得 $\overline{T}_2$ 是关于 $\varepsilon_2$ 的单调递减函数，结合式(45)可得

$$\overline{T}_2'' > \overline{T}_2' \tag{46}$$

这与原假设矛盾，因此当式(21a)满足 $P_1 + P_2 = P$ 时可取得最优解。

证毕。

**定理 3**　为了使 $\varepsilon_2$ 有意义，必须保证 $\mathrm{lb}(1+\gamma_2) > \dfrac{B}{N_2}$。

**证明**　为了确保满足可靠性要求，译码错误概率 $\varepsilon_2$ 必须满足 $0 < \varepsilon_2 < 0.5$，结合式(4)可得

$$0 < \varepsilon_2 = Q\left(f_1\left(\gamma_2, N_2, R_2\right)\right) < 0.5 = Q(0) \tag{47}$$

因为高斯 $Q(x)$ 函数随 $x$ 单调递减，由式(47)得

$$f_1\left(\gamma_2, N_2, R_2\right) > 0 \tag{48}$$

结合式(18)和式(27)可得

$$\sqrt{\frac{N_2}{V_2}}\left(\mathrm{lb}(1+\gamma_2) - \frac{B}{N_2} - \phi\right)\ln 2 > 0 \tag{49}$$

$$\mathrm{lb}(1+\gamma_2) - \frac{B}{N_2} - \phi > 0 \tag{50}$$

$$\mathrm{lb}(1+\gamma_2) > \frac{B}{N_2} + \phi > \frac{B}{N_2} \tag{51}$$

证毕。

结合式(3)、式(51)以及定理 2 可得

$$P_1 < 2^{-\frac{B}{N_2}} P + \frac{2^{-\frac{B}{N_2}} - 1}{|h_2|^2}\sigma_2^2 \tag{52}$$

由式(21b)可得

$$0 \leqslant P_1 \leqslant \frac{P}{2} \tag{53}$$

结合式(52)和式(53)，定义 $P_1$ 的上界为

$$P_1^{\mathrm{UB}} = \min\left\{2^{-\frac{B}{N_2}} P + \frac{2^{-\frac{B}{N_2}} - 1}{|h_2|^2}\sigma_2^2, \frac{P}{2}\right\} \tag{54}$$

经过以上分析，问题 P2 可简化为

$$\text{P3:}\ \max_{P_1}\ \overline{T}_2 \tag{55}$$

$$\text{s.t.}\quad P_1 \in \mathcal{P} \tag{55a}$$

$$\gamma_2 > \gamma_{\mathrm{e}} \tag{55b}$$

其中，$\mathcal{P} \triangleq \left\{p | P_1^{\mathrm{LB}} \leqslant p \leqslant P_1^{\mathrm{UB}},\ P_2 = P - p\right\}$。

一维线性搜索算法是一种最简单的穷举算法，通过以给定的搜索精度 $\kappa$ 为渐进步长，在区间 $\left[P_1^{\mathrm{LB}}, P_1^{\mathrm{UB}}\right]$ 中进行线性采样搜索，直到超出区间范围结束[32]。通过一维线性搜索算法可以找到 P3 中最优的 $P_1^*$，进而通过 $P_2 = P - P_1$ 求出最优的 $P_2^*$，在式(55b)的约束下，即 $\dfrac{|h_2|^2}{\sigma_2^2} > \dfrac{|h_{\mathrm{e}}|^2}{\sigma_{\mathrm{e}}^2}$，结合式(4)、式(18)和式(19)求出最优解 $\overline{T}_2^*$。

功率分配算法的复杂度主要来自一维搜索的最大搜索次数，对于一个给定的搜索精度 $\kappa$，根据式(25)与式(54)所求得的 $P_1$ 的搜索区间 $[P_1^{\mathrm{LB}}, P_1^{\mathrm{UB}}]$，定义最大搜索次数 $\xi = \dfrac{P_1^{\mathrm{UB}} - P_1^{\mathrm{LB}}}{\kappa}$，则算法以一维搜索遍历所有元素的复杂度为 $\mathcal{O}(\xi)$。

## 5　仿真结果分析

在基于 SPC 的 NOMA 下行系统下，本文通过 MATLAB 仿真平台对所提方案的性能进行评估，具体仿真参数如表 1 所示。

**表 1 仿真参数**

| 参数 | 数值 |
|---|---|
| 总传输包长 $N$ /symbol | 100～200（图 2），100（图 3～图 5） |
| 传输比特数 $B$ /bit | 200（图 2、图 4 和图 5），100～200（图 3） |
| 用户噪声功率 $\sigma_i^2$ /dB | −5[33] |
| 窃听者噪声功率 $\sigma_e^2$ /dB | 2[33] |
| 用户 2 信息保密约束 $\delta$ | $10^{-2}$（图 2～图 5），$10^{-5}$（图 5） |
| 用户 1 最大译码错误概率 $\varepsilon_0$ | $10^{-5}$（图 2～图 5），$10^{-2}$（图 5） |
| 总功率 $P$ /dB | 20（图 2 和图 3），15～25（图 4），15～35（图 5） |
| 用户 1 信道增益 $h_1$ | 0.6（图 2～图 4），0.8（图 5） |
| 用户 2 信道增益 $h_2$ | 0.3 |
| 窃听者信道增益 $h_e$ | 0.2（图 2、图 3 和图 5），0.1（图 4） |
| OMA 方案中用户 2 资源分配系数 $\alpha$ | 50%，60% |

为评价所提 NOMA 方案的性能，本文以 OMA 方案作为基准，OMA 方案中用户 2 也采用保密传输。

用户 2 的安全吞吐量和总传输包长的关系如图 2 所示。从图 2 中可以看出，随着包长的增加，用户 2 的安全吞吐量先增后减，这是因为一定的包长可以实现较高的传输速率，但随着包长的增加，$B/N_2$ 减小，用户 2 的吞吐量也随之减少。此外，在相同包长情况下，NOMA 方案性能始终优于 OMA 方案，尤其是在总包长较小时，NOMA 方案能够以较短的包长达到与 OMA 方案相同的吞吐量，因此可以证明 NOMA 方案可以显著减少 SPC 中的通信时延。虽然 OMA 方案可以通过牺牲用户 1 部分性能，将更多的资源分配给用户 2 来提高用户 2 的吞吐量，但总体仍然劣于 NOMA 方案。

传输比特数对用户 2 安全吞吐量的影响如图 3 所示。从图 3 中可以看出，随着系统传输比特数的增加，用户 2 的安全吞吐量先增后减，原因是 $B/N_2$ 的增大使信息传输速率增加，但同时也使错误概率 $\bar{\varepsilon}_2$ 增加，当 $\bar{\varepsilon}_2$ 超过一定限值后，系统的通信质量快速下降。此外，所提 NOMA 方案总是优于 OMA 方案，因此 NOMA 方案更适合传输数据频繁且零碎的、采用 SPC 的大规模 MTC 网络。

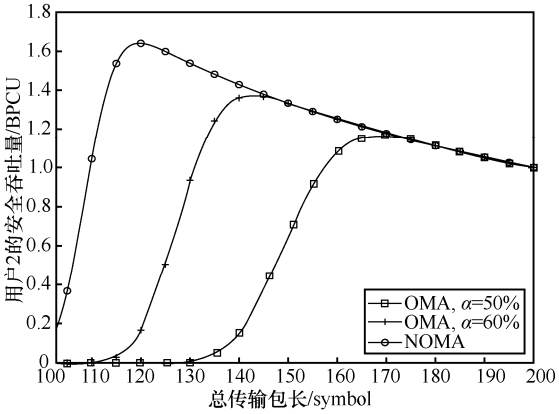


图 2 用户 2 的安全吞吐量和总传输包长的关系

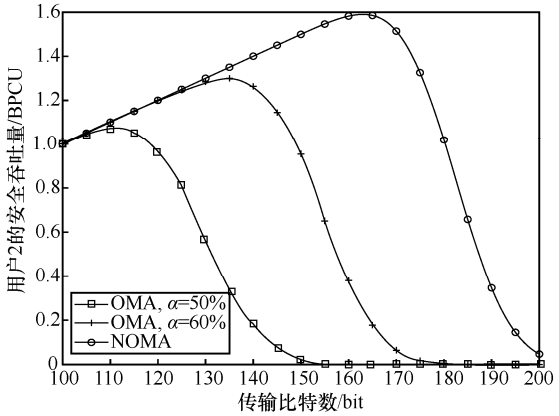


图 3 传输比特数对用户 2 的安全吞吐量的影响

用户 2 的安全吞吐量与基站传输总功率之间的关系如图 4 所示。由图 4 可以看出，随着基站传输总功率的增加，用户 2 的安全吞吐量将快速增加并趋于 $B/N_2$。这是由于随着总功率增加，分配给用户 2 的传输功率 $P_2$ 不断增加，使 $\bar{\varepsilon}_2$ 不断减小，直到对系统影响忽略不计。另外，从图 4 还可以发现 NOMA 方案总是优于 OMA 方案，在吞吐量相同时，消耗的功率更少，同时获得更好的传输性能。

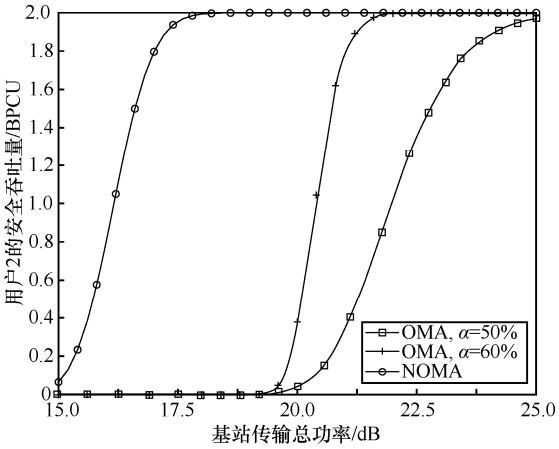


图 4 用户 2 的安全吞吐量与基站传输总功率之间的关系

不同 $\delta$ 和 $\varepsilon_0$ 约束下用户 2 的安全吞吐量随总功率的变化关系如图 5 所示。从图 5 中可以看出，在相同的总功率和 $\delta$ 条件下，增大 $\varepsilon_0$ 的值，即放松对用户 1 译码错误概率 $\bar{\varepsilon}_1$ 的约束，能够提高用户 2 的安全吞吐量，这是因为随着 $\varepsilon_0$ 的增大，基站需要分配给用户 1 的功率 $P_1$ 减少，相应地使 $P_2$ 增加，进而增大用户 2 的安全吞吐量。类似地，在相同的总功率和 $\varepsilon_0$ 条件下，增大 $\delta$ 的值，即放松对用户 2 的保密约束，能够提高用户 2 的安全吞吐量，这是因为窃听者的存在导致用户 2 存在传输速率损耗，随着 $\delta$ 的增大，传输速率损耗减小，传输性能提升。

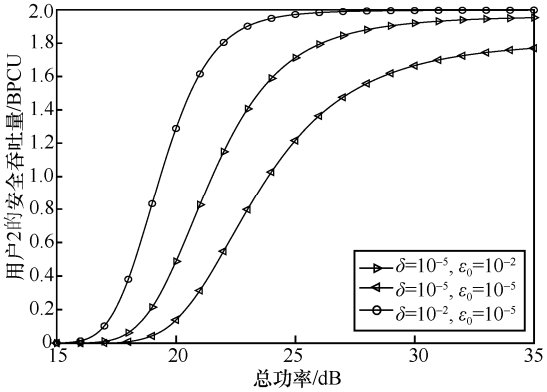


图 5　不同 $\delta$ 和 $\varepsilon_0$ 约束下用户 2 的安全吞吐量随总功率的变化关系

## 6　结束语

本文研究了基于 SPC 的 NOMA 系统中的安全传输问题，在满足最大译码错误概率约束、总功率约束和功率分配约束情况下，以 OMA 方案为基准，通过对基站发射功率的优化，在保证强用户性能的基础上，实现弱用户的安全吞吐量最大化。仿真和分析结果表明，与传统的 OMA 方案相比，所提 NOMA 方案能够有效提升系统中弱用户的安全传输性能、降低 SPC 的时延，同时获得更高的安全吞吐量。

## 参考文献：

[1] WANG D, CHEN D, SONG B, et al. From IoT to 5G I-IoT: the next generation IoT-based intelligent algorithms and 5G technologies[J]. IEEE Communications Magazine, 2018, 56(10):114-120.

[2] 张平, 陶运铮, 张治. 5G 若干关键技术评述[J]. 通信学报, 2016, 37(7): 15-29.
ZHANG P, TAO Y Z, ZHANG Z. Survey of several key technologies for 5G[J]. Journal on Communications, 2016, 37(7): 15-29.

[3] CHEN J, ZHANG L, LIANG Y C, et al. Resource allocation for wireless-powered IoT networks with short packet communication[J]. IEEE Transactions on Wireless Communications, 2019, 18(2):1447-1461.

[4] 钱志鸿, 王雪. 面向5G通信网的D2D技术综述[J]. 通信学报, 2016, 37(7): 1-14.
QIAN Z H, WANG X. Reviews of D2D technology for 5G communication networks[J]. Journal on Communications, 2016, 37(7): 1-14.

[5] HAN S J, XU X D, LIU Z L, et al. Energy-efficient short packet communications for uplink NOMA-based massive MTC networks[J]. IEEE Transactions on Vehicular Technology, 2019, 68(12): 12066-12078.

[6] BOCKELMANN C, PRATAS N, NIKOPOUR H, et al. Massive machine-type communications in 5G: physical and MAC-layer solutions[J]. IEEE Communications Magazine, 2016, 54(9): 59-65.

[7] BOCCARDI F, JR R W H, LOZANO A, et al. Five disruptive technology directions for 5G[J]. IEEE Communications Magazine, 2014, 52(2): 74-80.

[8] SUN C J, SHE C Y, YANG C Y, et al. Optimizing resource allocation in the short blocklength regime for ultra-reliable and low-latency communications[J]. IEEE Transactions on Wireless Communications, 2018, 18(1): 402-415.

[9] KHAN T A, HEATH R W, POPOVSKI P. Wirelessly powered communication networks with short packets[J]. IEEE Transactions on Communications, 2017, 65(12): 5529-5543.

[10] SHIRVANIMOGHADDAM M, MOHAMMADI M S, ABBAS R, et al. Short block-length codes for ultra-reliable low-latency communications[J]. IEEE Communications Magazine, 2019, 57(2): 130-137.

[11] 张平, 牛凯, 田辉, 等. 6G 移动通信技术展望[J]. 通信学报, 2019, 40(1): 141-148.
ZHANG P, NIU K, TIAN H, et al. Technology prospect of 6G mobile communications[J]. Journal on Communications, 2019, 40(1): 141-148.

[12] DING Z G, LIU Y W, CHOI J, et al. Application of non-orthogonal multiple access in LTE and 5G networks[J]. IEEE Communications Magazine, 2017, 55(2): 185-191.

[13] 曹雍, 杨震, 冯友宏. 新的 NOMA 功率分配策略[J]. 通信学报, 2017, 38(10): 157-165.
CAO Y, YANG Z, FENG Y H. New NOMA power allocation strategy[J]. Journal on Communications, 2017, 38(10): 157-165.

[14] HAO W M, ZENG M, CHU Z, et al. Energy-efficient power allocation in millimeter wave massive MIMO with non-orthogonal multiple access[J]. IEEE Wireless Communications Letters, 2017, 6(6): 782-785.

[15] 龚明言, 杨震. 针对 MIMO-NOMA 系统中配对弱用户的空时编码方案[J]. 通信学报, 2018, 39(6): 181-189.
GONG M Y, YANG Z. Space-time coding scheme for the paired weak user in MIMO-NOMA systems[J]. Journal on Communications, 2018, 39(6): 181-189.

[16] HAO W M, ZENG M, SUN G C, et al. Codebook-based max–min energy-efficient resource allocation for uplink mmWave MIMO-NOMA systems[J]. IEEE Internet of Things Journal, 2018, 5(2): 1299-1306.

[17] 彭安妮, 周威, 贾岩, 等. 物联网操作系统安全研究综述[J]. 通信学报, 2018, 39(3): 22-34.
PENG A N, ZHOU W, JIA Y, et al. Survey of the Internet of things operating system security[J]. Journal on Communications, 2018, 39(3): 22-34.

[18] 王潮, 胡广跃, 张焕国. 无线传感器网络的轻量级安全体系研究[J]. 通信学报, 2012, 33(2): 30-35.

WANG C, HU G Y, ZHANG H G. Lightweight security architecture design for wireless sensor network[J]. Journal on Communications, 2012, 33(2): 30-35.

[19] ZENG M, NGUYEN N P, DOBRE O A, et al. Securing downlink massive MIMO-NOMA networks with artificial noise[J]. IEEE Journal of Selected Topics in Signal Processing, 2019, 13(3): 685-699.

[20] 赵飞, 郝万明, 孙钢灿, 等. 基于 SWIPT 的毫米波大规模 MIMO-NOMA 系统下安全能效资源优化[J]. 通信学报, 2020, 41(8): 79-86.
ZHAO F, HAO W M, SUN G C, et al. Resource optimization of secure energy efficiency based on mmWave massive MIMO-NOMA system with SWIPT[J]. Journal on Communications, 2020, 41(8): 79-86.

[21] LEE B, PARK S, LOVE D J, et al. Packet structure and receiver design for low latency wireless communications with ultra-short packets[J]. IEEE Transactions on Communications, 2018, 66(2): 796-807.

[22] XU Y Q, SHEN C Y, CHANG T H, et al. Energy-efficient non-orthogonal transmission under reliability and finite blocklength constraints[C]//2017 IEEE Globecom Workshops. Piscataway: IEEE Press, 2017: 1-6.

[23] YANG W, DURISI G, KOCH T, et al. Quasi-static SIMO fading channels at finite blocklength[C]//IEEE International Symposium on Information Theory. Piscataway: IEEE Press, 2013: 1531-1535.

[24] POLYANSKIY Y, POOR H V, VERDU S. Channel coding rate in the finite blocklength regime[J]. IEEE Transmissions on Information Theory, 2010, 56(5): 2307-2359.

[25] SUN X F, YAN S H, YANG N, et al. Short-packet downlink transmission with non-orthogonal multiple access[J]. IEEE Transactions on Wireless Communications, 2018, 17(7): 4550-4564.

[26] HAGHIFAM M, MILI M R, MAKKI B, et al. Joint sum rate and error probability optimization: finite blocklength analysis[J]. IEEE Wireless Communications Letters, 2017, 6(6): 726-729.

[27] XIAO C Y, ZENG J, NI W, et al. Downlink MIMO-NOMA for ultra-reliable low-latency communications [J]. IEEE Journal on Selected areas in Communications, 2019, 37(4): 780-794.

[28] WANG H M, YANG Q, DING Z G, et al. Secure short-packet communications for mission-critical IoT applications[J]. IEEE Transactions on Wireless Communications, 2019, 18(5): 2565-2578.

[29] YANG W, SCHAEFER R F, POOR H V. Finite-blocklength bounds for wiretap channels[C]//2016 IEEE International Symposium on Information Theory. Piscataway: IEEE Press, 2016: 3087-3091.

[30] REN H, PAN C H, DENG Y S, et al. Joint power and blocklength optimization for URLLC in a factory automation scenario[J]. IEEE Transactions on Wireless Communications, 2020, 19(3): 1786-1801.

[31] HALEEMA S, MUHAMMAD Z, SHAHZAD A S. Performance analysis of downlink power domain NOMA under fading channels[C]// 2018 ELEKTRO. Piscataway: IEEE Press, 2018:1-6.

[32] 张立健, 金梁, 刘璐, 等. 多天线中继系统中人工噪声辅助的安全波束成形[J]. 通信学报, 2014, 35(11): 81-88.
ZHANG L J, JIN L, LIU L, et al. Artificial noise aided secure beamforming for multi-antenna relay systems[J]. Journal on Communications, 2014, 35(11): 81-88.

[33] FENG Y H, YAN S H, YANG Z. Secure transmission to the strong user in non-orthogonal multiple access[J]. IEEE Communications Letters, 2018, 22(12): 2623-2626.

[作者简介]

**孙钢灿**（1977– ），男，河南濮阳人，博士，郑州大学教授，主要研究方向为通信信号处理、通信信号关键参数盲估计、调制方式识别、机器人和智慧物流等。

**赵少柯**（1996– ），男，河南周口人，郑州大学硕士生，主要研究方向为短包通信、物理层安全等。

**郝万明**（1988– ），男，河南安阳人，博士，郑州大学讲师，主要研究方向为毫米波、NOMA 无线通信、边缘缓存和无线携能通信等。

**朱政宇**（1988– ），男，河南周口人，博士，郑州大学讲师，主要研究方向为携能传输、大规模 MIMO 等。