DOI：10.7652/xjtuxb201908017

5G非正交多址系统中使用全双工基站干扰的安全传输方案

王夕予[1]，陈亚军[2]，肖敏[3]，许晓明[2]
（1.南京大学金陵学院，210019，南京；2.国家数字交换系统工程技术研究中心，450002，郑州；
3.南京邮电大学自动化学院，210046，南京）

摘要：为了保证5G非正交多址(NOMA)系统中私密信息上行传输过程的信息安全，提出了一种基于全双工基站干扰的物理层安全传输方案。首先，分别使用二项式点过程和泊松点过程，对NOMA上行传输系统中用户设备和窃听者的空间位置分布进行刻画，建立NOMA上行传输系统模型；其次，为了使低硬件复杂度的用户设备付出较小的开销实现安全传输，全双工基站在接收信息的同时发送人工噪声干扰潜在窃听者；最后，基于全双工基站干扰方案，使用随机几何理论对系统的可靠性和安全性进行分析。理论和仿真结果表明：用户设备距离基站越近，全双工基站干扰方案对安全吞吐量的提升越明显；即使对于距基站最远的用户设备，在最优的噪声功率下，该方案仍可以使其安全吞吐量提高约41%。

关键词：物理层安全；非正交多址；全双工；上行传输
中图分类号：TN918.91 **文献标志码**：A **文章编号**：0253-987X(2019)08-0129-06

A Secure Transmission Scheme Using Full-Duplex Base Station Jamming in 5G Non-Orthogonal Multiple Access Systems

WANG Xiyu[1], CHEN Yajun[2], XIAO Min[3], XU Xiaoming[2]
(1. Jinling College, Nanjing University, Nanjing 210019, China; 2. National Digital Switching System Engineering and Technological Research Center, Zhengzhou 450002, China; 3. School of Automation, Nanjing University of Posts and Telecommunications, Nanjing 210046, China)

Abstract: A secure physical layer transmission scheme using full-duplex base station jamming is proposed to guarantee the information security during the uplink transmission in 5G non-orthogonal multiple access (NOMA) systems. Firstly, the binomial point processes and Poisson point processes are used to characterize the spatial distribution of user equipments and eavesdroppers in a NOMA uplink transmission system, and a NOMA uplink transmission model is established. Then, in order to achieve secure transmission with limited overhead increment by user equipment with low hardware complexity, the base stations not only receive the signals but also keep emitting jamming signals all the time to degrade the performance of any potential eavesdropper. Finally, based on the full-duplex jamming scheme the reliability and security of the system are analyzed using the stochastic geometry theory. Simulation and theoretical results show that the user equipments that are closer to the base station have more security enhancement using the proposed scheme. Even for the user equipment that is farthest from the base station, the

收稿日期：2018-11-14。 作者简介：王夕予(1984—)，女，讲师；陈亚军(通信作者)，男，助理研究员。 基金项目：国家自然科学基金资助项目(61501516,61573194)。
网络出版时间：2019-05-16 网络出版地址：http://kns.cnki.net/kcms/detail/61.1069.T.20190516.2059.004.html

proposed scheme can still increase its secrecy throughput by about 41% at the optimal jamming power.

Keywords: physical layer security; non-orthogonal multiple access; full-duplex; uplink transmission

作为 5G 通信中的一种重要多址方式,非正交多址(NOMA)技术允许多个用户设备(UE)共用一个正交的资源块,能够缓解频谱资源不足带来的压力[1-2]。在上行 NOMA 传输中,基站(BS)会使用连续干扰消除(SIC)技术以最大程度减少用户间的相互干扰,其原理如下:BS 首先解码接收信号强度最大的 UE 的信号,此时,将其他用户的信号当作干扰;然后,将解码出的信号恢复为模拟信号,并从所有的接收信号中将此信号消除[2]。依此类推,解码接收信号最强的 UE 信号时受到的用户间干扰最大,解码接收信号最弱的 UE 信号时不会受到干扰。相比于传统正交多址技术,NOMA 技术能够大大提高频谱效率,在 5G 通信系统中将有着巨大的应用前景[3-4]。

然而,由于 NOMA 上行传输中无线信号的开放性和广播特性,窃听者(Eve)可以对传输中的私密信息进行窃听。为了保证私密信息的安全传输,物理层安全技术利用合法信道和窃听信道间的差异,能够实现私密信号传输的完美安全,已成为传统密钥体制的一种良好补充[5-6]。目前,围绕 NOMA 物理层安全传输技术已有一些研究工作。文献[7-8]考虑单发送者对多个接收者进行 NOMA 传输的场景,对安全波束赋形和功率分配等参数进行优化设计,但该场景没有考虑实际蜂窝通信系统中发送者与接收者的位置分布特点。针对 NOMA 蜂窝通信系统,文献[9]考虑 BS 配备单天线和多天线的场景,分别采用安全保护域和人工噪声策略,对系统 NOMA 下行传输的安全性能进行分析;文献[10]采用混合单播与多播的波束赋形方案,对系统频谱效率和安全性的提升进行分析。但是,上述研究都仅关注 NOMA 下行传输场景,而没有对 NOMA 上行传输场景展开研究。

在 NOMA 上行传输中,UE 大多仅配备单天线,且计算能力和功率受限,而上述文献中所使用波束赋形和人工噪声等物理层安全策略要求发送方配备多天线,且计算复杂度较大,因此无法应用于上行 NOMA 传输系统。文献[11]针对上行 NOMA 蜂窝通信系统展开研究,提出一种上行 NOMA 物理层安全性能分析框架,但是,该文献仅考虑两个用户设备共用同一资源块的情况,难以推广到多个用户设备共用资源块的一般情况,且没有提出能够提高安全性能的传输策略。

针对上行 NOMA 蜂窝通信系统中私密信号的传输缺乏相应安全保障策略的问题,本文提出一种全双工基站干扰策略,并对系统的安全性能提升进行分析。在全双工基站干扰策略中,用户设备在上行传输私密信息的同时,全双工基站会发送人工噪声干扰潜在的窃听者。对于全双工技术带来的自干扰,可以通过高效的自干扰消除技术分别从模拟电路域、数字电路域和空域进行消除[12]。本文策略将安全通信的开销从发送者转移到了接收者,适宜用于用户设备计算能力和功率都受限的上行通信场景。在此基础上,本文考虑多个用户共用一个资源块的一般情况,进一步推导出 NOMA 上行传输系统的覆盖概率和安全中断概率,分别对系统可靠性和安全性进行衡量,并采用安全传输速率综合衡量系统的可靠性和安全性。本文的研究结果可为 NOMA 上行蜂窝传输系统的部署和后续维护提供理论指导。

1 系统模型

1.1 网络拓扑与信道模型

本文针对单小区上行蜂窝通信系统展开研究,如图 1 所示。与传统上行 NOMA 传输研究类似[13],假设 BS 位于平面中的原点,多个用户均匀分布在以基站为圆心、R 为半径的圆内。在 NOMA 上行传输中,假设 N 个 UE 会共用同一个正交的资源块,即在用户调度过程中,基站会选择 N 个 UE 使用同一个资源块。由于在用户调度时的随机性,N 个 UE 的位置分布 φ_{U} 可视为二项式点过程(BPP)[13]。对于被动窃听的 Eves,由于其在窃听过程中长期保持静默状态,无法获得其位置信息,因此采用泊松点过程(PPP)φ_{E} 对 Eves 空间分布的随机性进行刻画。假设 UE 和 BS 都配备单天线,窃听者为了伪装自身,也仅配备单天线。对于无线信道,假设信号会经历大尺度路径损耗和小尺度瑞利衰落。其中,大尺度路径损耗仅与传输距离有关,损耗系数为 α;小尺度瑞利衰落增益由均值为 1 的负指

数分布进行刻画，且不同信道间小尺度衰落相互独立；节点 m 与 n 之间小尺度瑞利信道增益用 h_{mn} 表示。

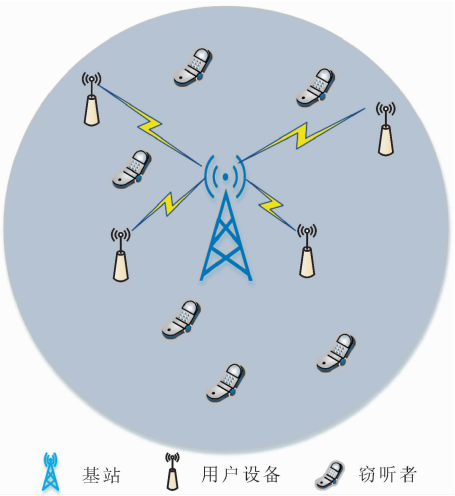

图 1　单小区 NOMA 上行传输系统示意图

1.2　干扰模型

根据 NOMA 上行传输的原理，多个 UE 共用同一个资源块，因此用户之间会相互干扰。在使用 SIC 消除用户间干扰时，BS 需要首先根据接收信号的强弱确定干扰消除的顺序。考虑到信道路径损耗对接收信号强度带来的影响远大于信道小尺度衰落带来的影响，因此本文考虑根据 UE 到 BS 的距离的远近作为判断接收信号强弱的依据[14]。值得指出的是，此方案忽略了小尺度衰落带来的影响，能够大大减少用于信道估计的信令开销，更加贴近实际上行 NOMA 传输系统。在此方案下，假设 N 个 UE 距 BS 从近到远为 $\mathrm{u}_1,\mathrm{u}_2,\cdots,\mathrm{u}_N$，其到 BS 的距离分别为 $d_1,d_2,\cdots,d_N$。在解码 $\mathrm{u}_k(1\leqslant k\leqslant N)$ 发送的信息时，BS 会先消除 $\mathrm{u}_1,\cdots,\mathrm{u}_{k-1}$ 的信息，然后将 $\mathrm{u}_{k+1},\cdots,\mathrm{u}_N$ 的信息看作干扰。因此，对于 u_k，其受到的用户间干扰可表示为

$$I_k=\sum_{i=k+1}^{N}P_{\mathrm{U}}h_{\mathrm{B},\mathrm{u}_i}d_i^{-\alpha} \tag{1}$$

式中：P_{U} 表示 UE 的信号发送功率。

同时，假设在用户调度过程中，使用相同资源块的 N 个 UE 间距离差距足够大，使得 BS 能够成功进行 SIC。需要指出的是，出于模型复杂度的考虑，完美 SIC 假设被广泛应用于 NOMA 系统的分析中，如文献[15-16]。

1.3　安全传输策略

为了保障 UE 私密信息传输的安全性，假设 BS 能够工作在全双工模式，在接收 UE 信息的同时发送随机噪声干扰潜在的窃听者。由于信道中 NOMA 带来的小区内干扰和基站全双工模型带来的自干扰强度远大于热噪声，因此可认为此系统为干扰受限系统，即可以忽略系统中热噪声带来的影响。此时，对于 $\mathrm{u}_k\in\varphi_{\mathrm{u}}$，其信干比 γ_k 可表示为

$$\gamma_k=\frac{P_{\mathrm{U}}h_{\mathrm{B},\mathrm{u}_k}d_k^{-\alpha}}{I_k+\eta P_{\mathrm{n}}} \tag{2}$$

式中：P_{n} 表示 BS 发送干扰噪声的功率；η 表示全双工状态下自干扰消除能力。对于窃听者 $\mathrm{Eve}\in\varphi_{\mathrm{E}}$，假设其有足够强的多用户信号检测能力，即 E 能够将使用同一正交资源块中不同用户的信号分离开。因此，其信干比 γ_{E} 可表示为

$$\gamma_{\mathrm{E}}=\frac{P_{\mathrm{U}}h_{\mathrm{E},\mathrm{u}_k}d_{\mathrm{E},\mathrm{u}_k}^{-\alpha}}{P_{\mathrm{n}}h_{\mathrm{BE}}d_{\mathrm{BE}}^{-\alpha}} \tag{3}$$

式中：$d_{\mathrm{E},\mathrm{u}_k}$ 表示 Eve 与 u_k 之间的距离；d_{BE} 表示 BS 与 Eve 之间的距离。此处，通过过高估计窃听者的多用户检测能力，对私密信号传输可能面临的最严峻的场景进行研究，因此所求出的安全性能可看作系统安全性能的下界。

考虑到 UE 有限的计算能力，本文采用固定速率 Wyner 安全编码方案[17]。在该方案中，码字传输速率为 R_{C}，私密信息传输速率为 $R_{\mathrm{S}}(R_{\mathrm{S}}<R_{\mathrm{C}})$，冗余速率 $R_{\mathrm{E}}=R_{\mathrm{C}}-R_{\mathrm{S}}$ 是为了对抗窃听者对私密信息的窃听。当合法信道容量大于 R_{C} 时，则合法接收方能够成功解码私密信号；当窃听信道容量大于 R_{E} 时，则窃听者能成功获取部分私密信号，此时便发生了安全中断。基于固定速率 Wyner 安全编码，可以通过覆盖概率和安全中断概率对系统的可靠性和安全性进行刻画。

2　性能分析

2.1　覆盖概率

首先，使用覆盖概率对系统可靠性进行衡量。覆盖概率定义为 BS 能够成功解码 *UE* 信息的概率。用 $P(\cdot)$ 表示事件发生的概率，数学上，u_k 的覆盖概率可表示为

$$p_k=P(\mathrm{lb}(1+\gamma_k)>R_B) \tag{4}$$

引理 1　对于 u_k，其覆盖概率可由下式表示

$$p_k=\int_0^R\exp\left(-\frac{r^{\alpha}\eta P_{\mathrm{n}}(2^{R_B}-1)}{P_{\mathrm{U}}}\right)f_{d_k}(r)\cdot\left(\frac{2(G(R)-G(r))}{\mu r^{\alpha}(\alpha+2)(R^2-r^2)}\right)^{N-k}\mathrm{d}r \tag{5}$$

式中

$$G(r)=r_2^{2+\alpha}F_1\left(1,1+\frac{2}{\alpha},2+\frac{2}{\alpha},-\frac{r^{\alpha}}{sP_{\mathrm{U}}}\right) \tag{6}$$

$$f_{d_k}(r)=\frac{2}{R}\frac{\Gamma(k+1/2)\Gamma(N+1)}{\Gamma(k)\Gamma(N+1.5)}\cdot \beta\left(\frac{r^2}{R^2};k+1/2;N-k+1\right) \tag{7}$$

其中，$F_1(\cdot)$表示高斯超几何函数，$\Gamma(\cdot)$表示 Gamma 函数，$\beta(x;a;b)$为 Beta 分布 $B(a;b)$的概率密度函数，表达式为 $\beta(x;a;b)=\frac{x^{a-1}(1-x)^{b-1}}{B(a;b)}$。

证明 将式(2)代入式(4)，覆盖概率可进一步表示为

$$p_k=E_{d_k}\left[P\left(h_{u_k b}>\frac{\mu(I_k+\eta P_{\mathrm{n}})}{P_{\mathrm{U}}d_k^{-\alpha}}\right)\right]\overset{(a)}{=} E_{d_k}\left[\exp\left(-\frac{\eta P_{\mathrm{n}}\mu}{P_{\mathrm{U}}d_k^{-\alpha}}\right)L_{I_k}\left(\frac{\mu}{P_{\mathrm{U}}d_k^{-\alpha}}\right)\right]= \int_0^R \exp\left(-\frac{r^\alpha\eta P_{\mathrm{n}}\mu}{P_{\mathrm{U}}}\right)L_{I_k}\left(\frac{r^\alpha\mu}{P_{\mathrm{U}}}\right)f_{d_k}(r)\mathrm{d}r \tag{8}$$

式中：$E_x\{\cdot\}$表示关于 x 的期望；(a)表示 $h_{u_k b}$满足均值为 1 的负指数分布；$f_{d_k}(r)$表示 u_k 到 b 距离的概率密度函数。根据 BPP 的性质，可以获得 $f_{d_k}(r)$的闭式表达式。具体来说，对于一个圆内随机分布的 N 个节点，到圆心第 k 远的点，其到圆心距离的概率密度函数服从 beta 分布，具体表达式如式(7)所示[13]。

在给定 $d_k=r$ 的情况下，NOMA 传输中用户间干扰的拉普拉斯变换 L_{I_k}进一步可表示为

$$L_{I_k|r}(s)=E_{h_{\mathrm{B},\mathrm{u}_i},d_i|r}\left[\exp\left(-s\sum_{i=k+1}^{N}P_{\mathrm{U}}h_{\mathrm{B},\mathrm{u}_i}d_i^{-\alpha}\right)\right]\overset{(a)}{=} \prod_{i=k+1}^{N}E_{d_i|r}\left[\frac{1}{1+sP_{\mathrm{U}}d_i^{-\alpha}}\right]\overset{(b)}{=} \left(\int_r^R\frac{1}{1+sP_{\mathrm{U}}r_j^{-\alpha}}\frac{2r_j}{R^2-r^2}\mathrm{d}r_j\right)^{N-k} \tag{9}$$

式中：(a)表示不同信道小尺度衰落相互独立且服从均值为 1 的负指数分布；(b)表示在 $d_k=r$ 的条件下 $d_i(k<i\leqslant N)$的概率密度函数可得。通过对式(9)进行积分，并将结果代入式(8)中，便可得到引理 1 中覆盖概率的表达式。

结论 1 由上述分析可得，随着噪声功率的增加，覆盖概率会减小。这是因为噪声在干扰 Eve 的同时，也会通过自干扰对 BS 自身带来干扰，同时 UE 距离 BS 的远近次序会对覆盖概率带来复杂的影响。具体来说，当 UE 距离 BS 越近时，其受到的路径损耗越小，但 SIC 后受到的用户间干扰也越大。

2.2 安全中断概率

对于系统的安全性能，使用安全中断概率对其进行刻画。此时，考虑威胁性最大的窃听者。该窃听者不一定距离 u_k 最近，而是到 u_k 的信道增益最大。当该窃听者到 u_k 的信道容量大于冗余编码速率时，则称系统发生了安全中断。令 $\beta=2^{R_{\mathrm{C}}-R_{\mathrm{S}}}-1$，数学上，安全中断概率可以表示为

$$p_{\mathrm{so},k}=P(\mathrm{lb}_2(1+\max_{e\in\varphi_e}\{\gamma_{\mathrm{E}}\})>R_{\mathrm{C}}-R_{\mathrm{S}})=P(\max_{e\in\varphi_e}\{\gamma_{\mathrm{E}}\}>\beta) \tag{10}$$

引理 2：对于 u_k，其安全中断概率可由下式表示

$$p_{\mathrm{so},k}=1-\exp(-2\pi\lambda_e\int_0^\infty Cd_{\mathrm{E,B}}\mathrm{d}d_{\mathrm{E,B}}) \tag{11}$$

其中

$$C=\frac{1}{2\pi}\int_0^{2\pi}\int_0^R f_{d_k}(r)\cdot\frac{1}{1+\beta P_{\mathrm{U}}^{-1}d_{\mathrm{E,B}}^{\alpha}P_{\mathrm{n}}(r^2+d_{\mathrm{E,B}}^2-2d_{\mathrm{E,B}}r\cos\theta)^{-\alpha/2}}\mathrm{d}r\mathrm{d}\theta \tag{12}$$

证明 根据随机几何理论，$p_{\mathrm{so},k}$可进一步表示为

$$p_{\mathrm{so},k}=E_{\varphi_{\mathrm{E}}}\left[\prod_{e\in\phi_e}P(\gamma_{\mathrm{E}}>\beta)\right]\overset{(a)}{\leqslant} 1-\exp\left(-2\pi\lambda_{\mathrm{E}}\int_0^\infty\underbrace{P(\gamma_{\mathrm{E}}>\beta)}_{C}d_{\mathrm{E,B}}\mathrm{d}d_{\mathrm{E,B}}\right) \tag{13}$$

式中(a)表示由 PPP 的概率生成函数(PGFL)与 Jensen 不等式求得[18]。与证明 1 的求解步骤一致，式(12)中的 C 可进一步表示为

$$C=E_{d_{\mathrm{E},\mathrm{u}_k}}\left[\frac{1}{1+\beta P_{\mathrm{U}}^{-1}d_{\mathrm{E,B}}^{\alpha}P_{\mathrm{n}}d_{\mathrm{u}_k}^{-\alpha}}\right] \tag{14}$$

式中：$d_{\mathrm{E},\mathrm{u}_k}=\sqrt{d_k^2+d_{\mathrm{E,B}}^2-2d_{\mathrm{E,B}}d_k\cos\theta}$；$\theta$ 为在$[0,2\pi]$间均匀分布[19]。因此，C 最终表达式如式(12)所示。将式(12)代入式(11)中，便可得到用户 u_k 安全中断概率的表达式。

结论 2 由上述分析可得，由于噪声对 Eves 的干扰，随着噪声功率的增加，安全中断概率逐渐减小。同时，UE 距离 BS 的远近次序越小，安全中断概率也越大。这是因为当 UE 距 BS 越近时，BS 噪声对其周围 Eve 的影响就越大，因此该 UE 通信的安全性就越强。

在结论 1 和结论 2 的基础上，采用安全吞吐量 ζ_k 综合衡量 u_k 信息传输的可靠性与安全性。安全吞吐量 ζ_k 表示 u_k 可靠且安全发送信息的平均安全速率，其数学表达式为[20]

$$\zeta_k=R_{\mathrm{S}}p_k(1-p_{\mathrm{so},k}) \tag{15}$$

结论 3 由结论 1 和结论 2 可得，噪声功率给系统可靠性和安全性带来相反的影响，因此噪声功率的选取需要考虑系统可靠性和安全性的折中。通过选取最优的噪声功率，使安全吞吐量达到最大，能够有效改善系统的可靠性和安全性，达到可靠性和安全

性折中。

3　数值仿真

本章中，使用蒙特卡罗仿真对理论分析结果进行验证，为实际 NOMA 上行传输系统的部署和后续维护提供理论指导。系统仿真参数预设如下：码字传输速率 $R_C=1$ b/(s·Hz)，私密信息传输速率 $R_S=0.5$ b/(s·Hz)，BS 半径 $R=300$ m，共用同一资源块用户数 $N=5$，路径损耗系数 $\alpha=4$，窃听者密度 $\lambda_E=10^{-5}$ m^{-2}，自干扰消除系数 $\eta=-100$ dB，噪声发射功率 $P_n=20$ dBm，上行用户发射功率 $P_U=20$ dBm。同时，在[0,1 000] m×[0,1 000] m 内对 PPP 模型进行仿真。

首先，分析了 UE 到 BS 距离的远近次序对覆盖概率与安全中断概率的影响。由图 2 可得，覆盖概率的仿真值与理论值十分接近，由此可证明本文理论推导的正确性。对于安全中断概率，仿真值比理论值略小，这是由于在推导安全中断概率时，使用 Jensen 不等式得到了其实际值的上界。对于距 BS 由近到远的 UE，一方面，UE 到基站的距离增加，路径损耗增加，导致系统的可靠性降低；另一方面，UE 在 NOMA 传输中受到的用户间干扰变小，使得通信的可靠性增强，因此，这些 UE 的覆盖概率先减小后增大。对于安全中断概率，由于 UE 到 BS 越远，BS 的噪声对其周围的 Eves 影响就越小，因此安全中断概率增加。

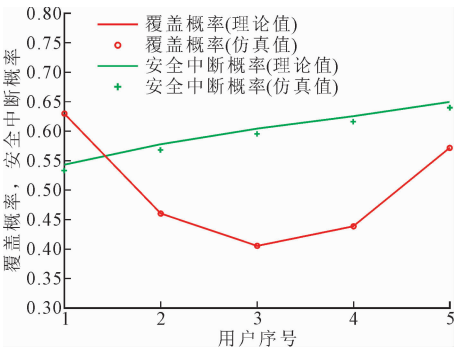

图 2　覆盖概率和安全中断概率示意图

图 3 分析了噪声功率对不同 UE 安全传输速率的影响。由图 3 可得，对于距 BS 最近的 3 个 UE($k=1,2,3$)，安全传输速率 ζ_k 随着噪声功率 P_n 的增大而增加；对于距 BS 较远的 2 个 UE($k=4,5$)，安全传输速率 ζ_k 随着噪声功率 P_n 的增大先增大后减小。其主要原因是：全双工噪声干扰策略以牺牲可靠性为代价提升系统安全性能，因此存在一个最优的 P_n 使 ζ_k 最大。当 UE 距 BS 越近，噪声带来的安全增益越大，所以最优的 P_n 值也越大。同时，即使对于距基站最远的用户设备，在最优的噪声功率下，该方案仍可以使其安全吞吐量提高约 41%

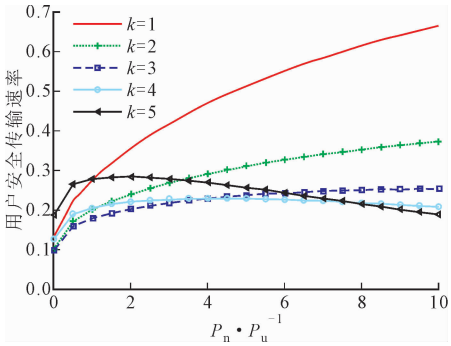

图 3　不同用户安全传输速率示意图

4　结　论

针对 NOMA 上行系统中私密信息的安全传输问题，考虑到上行 UE 有限的计算能力和功耗，提出一种全双工基站干扰策略提高系统安全性能。首先，为了对 NOMA 传输系统带来的用户间干扰进行刻画，提出一种基于随机几何的理论分析模型；其次，在该模型的基础上，求出覆盖概率和安全中断概率的表达式，对全双工干扰策略下系统的可靠性和安全性进行分析。理论和仿真结果表明，全双工干扰策略能够有效提高系统的安全性能，同时，UE 距离 BS 越近，其获得的安全增益便越大。需要指出的是，本文基于理想 SIC 的假设，非理想 SIC 下 NOMA 系统物理层安全性能的分析将作为后续工作。

参考文献：

[1] DING Z G, ADACHI F, POOR H V. The application of MIMO to non-orthogonal multiple access [J]. IEEE Transactions on Wireless Communications, 2015, 15(1): 537-552.

[2] 李钊，戴晓琴，陈柯宇，等. 非正交多址接入下行链路用户匹配与功率优化算法 [J]. 电子与信息学报，2017，39(8)：1804-1811.
LI Zhao, DAI Xiaoqin, CHEN Keyu, et al. User matching and power optimization algorithm for downlink NOMA [J]. Journal of Electronics & Information Technology, 2017, 39(8): 1804-1811.

[3] DING Z G, YANG Z, FAN P, et al. On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users [J]. IEEE Signal Processing Letters, 2014, 21(12): 1501-1505.

[4] 丁婷婷，刘彦君，张宁波，等. 5G 大连接场景下混合

多址随机接入 [J]. 北京邮电大学学报，2018，41(3)：1-6.
DING Tingting，LIU Yanjun，ZHANG Ningbo，et al. A hybrid random access for massive connections in 5G systems [J]. Journal of Beijing University of Posts and Telecommunications，2018，41(3)：1-6.

[5] XU X M，YANG W W，CAI Y M，et al. On the secure spectral-energy efficiency tradeoff in random cognitive radio networks [J]. IEEE Journal on Selected Areas in Communications，2016，34(10)：2706-2722.

[6] 白慧卿，金梁，肖帅芳，等. 多天线系统中面向物理层安全的极化编码方法 [J]. 电子与信息学报，2017，39(11)：2587-2593.
BAI Huiqing，JIN Liang，XIAO Shuaifang，et al. Polar code for physical layer security in multi-antenna systems [J]. Journal of Electronics & Information Technology，2017，39(11)：2587-2593.

[7] ZHANG Y，WANG H M，YANG Q，et al. Secrecy sum rate maximization in non-orthogonal multiple access [J]. IEEE Communications Letters，2016，20(5)：930-933.

[8] HE B，LIU A，YANG N，et al. On the design of secure non-orthogonal multiple access systems [J]. IEEE Journal on Selected Areas in Communications，2016，35(10)：2196-2206.

[9] LIU Y W，QIN Z，ELKASHLAN M，et al. Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks [J]. IEEE Transactions on Wireless Communications，2017，16(3)：1656-1672.

[10] DING Zhiguo，ZHAO Zhongyuan，PENG Mugen，et al. On the spectral efficiency and security enhancements of NOMA assisted multicast-unicast streaming [J]. IEEE Transactions on Communications，2017，65(7)：3151-3163.

[11] ZHANG Shuai，XU Xiaoming，PENG Jianhua，et al. Analysis of uplink NOMA in cellular IoT：a physical layer security perspective [C]// 88th Vehicular Technology Conference. Piscataway，NJ，USA：IEEE，2019：8690567.

[12] 许江涛，唐炳俊，翟羽健，等. 应用于同频带全双工中的宽带自干扰射频抵消技术 [J]. 西安交通大学学报，2018，52(9)：71-75.
XU Jiangtao，TANG Bingjun，ZHAI Yujian，et al. Wide bandwidth self-interference radio frequency cancelling technique for single channel full duplex [J]. Journal of Xi'an Jiaotong University，2018，52(9)：71-75.

[13] TABASSUM H，HOSSAIN E. Modeling and analysis of uplink non-orthogonal multiple access in large-scale cellular networks using Poisson cluster processes [J]. IEEE Transactions on Communications，2016，65(8)：3555-3570.

[14] ZHANG S，XU X，WANG H，et al. Enhancing the physical layer security of uplink non-orthogonal multiple access in cellular internet of things [J]. IEEE Access，2018，6：58405-58417.

[15] LIU Y，DERAKHSHANI M，LAMBOTH S. Outage analysis and power allocation in uplink non-orthogonal multiple access systems [J]. IEEE Communications Letters，2018，22(2)：336-339.

[16] DING Z，ZHAO Z，PENG M，et al. On the spectral efficiency and security enhancements of NOMA assisted multicast-unicast streaming [J]. IEEE Transactions on Communications，2017，65(7)：3151-3163.

[17] 钟艺玲，穆鹏程. 单发多收无线窃听信道中的自适应保密速率传输方案 [J]. 西安交通大学学报，2015，49(4)：104-109.
ZHONG Yiling，MU Pengcheng. An adaptive secret transmission rate scheme in SIMO wireless wiretap channel [J]. Journal of Xi'an Jiaotong University，2015，49(4)：104-109.

[18] DENG Y，WANG L，ELKASHLAN M，et al. Physical layer security in three-tier wireless sensor networks：a stochastic geometry approach [J]. IEEE Transactions on Information Forensics and Security，2017，11(6)：1128-1138.

[19] ZHENG T X，WANG H M，YANG Q，et al. Safeguarding decentralized wireless networks using Full-duplex jamming receivers [J]. IEEE Transactions on Wireless Communications，2016，16(1)：546-554.

[20] HE B，SHE Y，LAU V K. Artificial noise injection for securing single-antenna systems [J]. IEEE Transactions on Vehicular Technology，2017，66(10)：9577-9581.

（编辑 刘杨）