认知无线电非正交多址接入随机网络物理层安全性能分析

于宝泉 蔡跃明* 胡健伟
(陆军工程大学 南京 210007)

摘 要：该文针对干扰源以及窃听节点均随机分布的通信场景，分析了认知无线电启发式非正交多址接入(CR-NOMA)网络中次用户通信对的安全通信性能。采用随机几何理论，将窃听节点和干扰节点建模为服从特定分布的齐次泊松点过程(PPP)。首先，在保证主用户通信对通信可靠性的前提下，得到了发端设定的功率分配系数，进一步得到了次用户通信对的连接中断概率和安全中断概率的闭式表达式。随后，得到了功率分配系数随主用户可靠性能约束的变化规律。最后，研究了次用户对的中断概率随着窃听节点密度、发端发送功率的变化情况，结果表明干扰信号的增强在降低网络可靠性能的同时，换来了安全性能的提高。仿真结果验证了理论分析的正确性。

关键词：认知无线电；物理层安全；启发式非正交多址接入；随机分布；功率分配
中图分类号：TN926 **文献标识码**：A **文章编号**：1009-5896(2020)04-0950-07
DOI: 10.11999/JEIT190049

Performance Analysis of Physical Layer Security for Cognitive Radio Non-Orthogonal Multiple Access Random Network

YU Baoquan CAI Yueming HU Jianwei
(*The Army Engineering University of PLA*, *Nanjing* 210007, *China*)

Abstract: This paper analyzes the security communication performance of secondary user communication pairs in Cognitive Radio Non-Orthogonal Multiple Access (CR-NOMA) networks, where interference sources and eavesdropping nodes are randomly distributed. The stochastic geometry theory is used to model the eavesdropping nodes and the interfering nodes as a homogeneous Poisson Point Processes (PPP). Firstly, to ensure the reliability of the primary user communication pairs, the power allocation coefficient set of the sender is obtained, and the closed expressions of the connection outage probability and the secrecy outage probability of the secondary user are further obtained. Then, the variation of the power distribution coefficient with the constraint of the primary user's reliability is analyzed. Finally, the relationship between outage probability of secondary user communication pairs and the density of the eavesdropping nodes and the transmission power is studied. The research shows that the enhancement of interfering signal reduces the reliability of the system, but brings about a significant improvement of security performance. The simulation results verify the correctness of the theoretical analysis.

Key words: Cognitive Radio (CR); Physical layer security; Heuristic Non-Orthogonal Multiple Access (NOMA); Random distribution; Power allocation

1 引言

随着移动通信技术的蓬勃发展，物联网成为5G和后5G时代重要的应用场景，这使得无线通信量将呈现爆发式的增长。然而，由于无线通信的开放性和广播性，使得其很容易受到窃听者的窃听和攻击。同时，随着计算机计算能力的不断提高，传统的加密技术已经不能满足无线通信安全设计的需要。作为传统通信安全方式的重要补充，物理层安全技术利用链路的动态特性，通过主窃信道性能之差，从信息论的角度保证通信的安全，是解决无线通信安全的新思路[1]。然而，现有的物理层安全技术如波束赋形[2]、人工噪声[3]等，由于其实现较为复杂，不能适应物联网终端低硬件复杂度、低功耗的特点，使其应用大为受限。

非正交多址接入(NOMA)技术因其高频谱效率的特点被认为是5G和后5G时代关键性的技术之

收稿日期：2019-01-17；改回日期：2019-06-30；网络出版：2020-01-11
*通信作者： 蔡跃明 caiym@vip.sina.com
基金项目：国家自然科学基金(61771487, 61371122, 61471393)
Foundation Items: The National Natural Science Foundation of China(61771487, 61371122,61471393)

一[4]。TDMA, OFDMA等传统的正交多址技术，依靠信号之间的相互正交来保证相互之间不会产生干扰。与之不同的是，功率域NOMA技术利用功率差异来区分不同的用户，保证用户能够正确接收信号[5,6]。目前NOMA常用的技术有功率控制的多址技术和编码控制的多址技术。同时，认知无线电技术在保证授权用户正常通信的前提下，允许非授权用户动态接入授权频谱，是提高频谱资源利用率的关键技术[7,8]。为了结合认知无线电技术和NOMA多址接入技术的优势。文献[9]基于认知无线电概念提出了一种新的下行NOMA功率分配原则，称为认知无线电启发式NOMA(CR-NOMA)。其核心思想是将NOMA看作认知无线电网络的一个特殊情况：将信道质量较差的用户看作认知网络中的主用户，通过调整功率分配系数，保证主用户的通信质量，只有当发端分配的资源能够满足主用户的通信需求时，剩余的资源才会分配给其他用户[10]。因此，采用认知无线电启发式方式时，为了确保网络中信道状况较差用户的通信质量，分配给其他用户的信道资源会被严格限制。NOMA技术通过分配给信道质量较差的用户更多资源的方式，保证网络的公平性。CR-NOMA在保留NOMA公平性的优点的基础上，通过认知无线电技术，可以确保信道质量较差用户的通信质量。

随着高频谱效率需求的提升，结合了认知无线电技术和NOMA技术优势的CR-NOMA技术凸显出广阔的应用前景。文献[11]研究了在CR-NOMA通信网络中，将信道质量较好的次用户作为中继，提高主用户通信的可靠性能。文献[12]在非理想的信道质量状况下研究了CR-NOMA的中断性能。文献[13]提出一个两阶段的合作策略以提高CR-NOMA通信网络中的公平性。文献[14]研究了在CR-NOMA中发送单播和多播信号，并利用多播信号的接收者作为中继节点，提高单播和多播用户的通信质量。

通过上述文献发现，现有的研究大多采用确知节点的通信网络模型，且未考虑节点随机分布下的物理层安全问题。然而，由于无线通信环境的复杂性，窃听节点可以随时随地动态接入授权频谱，使得发端很难精确获知窃听节点的数目和位置信息。同时，随着通信设备呈现出数量大规模化、种类多样化的特点，使得干扰源的位置分布也呈现出随机化的特点。在这种情况下，随机几何理论在物理层安全的研究中得到了广泛的应用[15–18]。本文考虑窃听节点以及干扰源随机分布的通信场景，研究CR-NOMA网络的安全通信性能。同时，为了减少信道导频资源的开销，发端采用固定的传输速率进行通信，然而由于信道状态的随时变化，信道容量的大小不是一成不变的，信息传输速率不能绝对满足信道容量大小的约束，网络无法实现绝对可靠和安全的通信。对此，本文采用on-off机会传输方案，先给定主用户连接中断概率的阈值，在保证主用户通信可靠性的前提下，发端选择发送信息。得到了随机网络下CR-NOMA的功率分配系数，进而得到次用户的连接中断概率和安全中断概率的闭式表达式，并得到了其在不同通信环境下的变化规律。

2　网络模型

2.1　网络输入输出关系

如图1所示，考虑一个干扰受限模型，在干扰节点Bob和窃听节点Eve均随机分布的情况下，发端Alice发送一段线性混合信号给用户1、用户2。将用户1看作认知网络中的主用户，用户2看作认知网络中的次用户。

发端Alice采用NOMA技术，发出的线性混合信号包含有发给两个用户的信息。假设总的信号功率为P_1, a_1, a_2为发端对用户1、用户2的功率分配系数，则发端发给用户1、用户2的信号分别为$a_1\sqrt{P_1}x_1$和$a_2\sqrt{P_1}x_2$，线性混合信号为$a_1\sqrt{P_1}x_1+a_2\sqrt{P_1}x_2$。假设用户1的信道质量较差，用户2信道质量较好。则用户2可以先译码用户1的信息并将其剔除，再译码自身的信息，使得发送给用户1的信号$a_1\sqrt{P_1}x_1$不会对用户2造成干扰。x'为每个干扰源发送的信号，信号功率为P_2。因此合法用户以及窃听者接收到的信号可以分别表示为

$$y_1=\left(a_1\sqrt{P_1}x_1\right)g_{\mathrm{A1}}+\underbrace{\left(a_2\sqrt{P_1}x_2\right)g_{\mathrm{A1}}+\sqrt{P_2}x'\sum_{\mathrm{B}\in\phi_{\mathrm{B}}}h_{\mathrm{B1}}d_{\mathrm{B1}}^{-\frac{\alpha}{2}}}_{\text{用户1接收的干扰信号}} \tag{1}$$

$$y_2=\left(a_2\sqrt{P_1}x_2\right)g_{\mathrm{A2}}+\underbrace{\sqrt{P_2}x'\sum_{\mathrm{B}\in\phi_{\mathrm{B}}}h_{\mathrm{B2}}d_{\mathrm{B2}}^{-\frac{\alpha}{2}}}_{\text{用户2接收的干扰信号}} \tag{2}$$

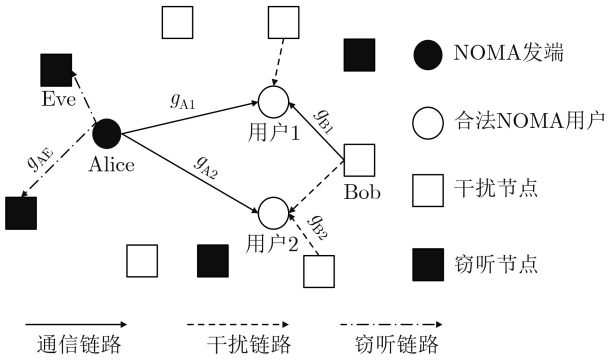

图 1 网络模型示意图

$$y_{\mathrm{E}}=\left(a_2\sqrt{P_1}x_2\right)g_{\mathrm{AE}}+\underbrace{\left(a_1\sqrt{P_1}x_1\right)g_{\mathrm{AE}}+\sqrt{P_2}x'\sum_{\mathrm{B}\in\phi_{\mathrm{B}}}h_{\mathrm{BE}}d_{\mathrm{B}E}^{-\frac{\alpha}{2}}}_{\text{窃听节点接收的干扰信号}} \tag{3}$$

其中，$g_{ij}=h_{ij}{d_{ij}}^{-\frac{\alpha}{2}}$, d_{ij}表示节点i到节点j的距离，α表示为路径损耗因子，$h_{ij}\sim\mathrm{CN}(0,1)$为节点$i$和节点$j$间信道的小尺度瑞利衰落系数。$\phi_{\mathrm{B}}$为对通信网络产生影响的干扰源Bob的集合。

2.2 合法用户和窃听节点处的接收信干比

假设用户1为主用户，用户2为次用户。用户1和用户2的功率分配系数分别为a_1和a_2，在保证用户1通信可靠性的前提下，剩余的功率全部分配给用户2，因此$a_1^2+a_2^2=1$。假设Alice的发射信号功率为P_1，其余干扰节点的发送功率为P_2，则用户1接收到的信干比为

$$\gamma_1=\frac{P_1a_1^2|g_{\mathrm{A1}}|^2}{P_1a_2^2|g_{\mathrm{A1}}|^2+P_2\sum\limits_{\mathrm{B}\in\phi_{\mathrm{B}}}|h_{\mathrm{B1}}|^2d_{\mathrm{B1}}^{-\alpha}} \tag{4}$$

由于用户2的信道质量较好，因此在解码自身信息时可以先将发送给用户1的信息正确解码并排除，避免信息之间的干扰，因此用户2接收到的信干比为

$$\gamma_2=\frac{P_1a_2^2|g_{\mathrm{A2}}|^2}{P_2\sum\limits_{\mathrm{B}\in\phi_{\mathrm{B}}}|h_{\mathrm{B2}}|^2d_{\mathrm{B2}}^{-\alpha}} \tag{5}$$

同样，对于某一窃听节点Eve，在解码Alice发送给次用户的信息时，接收到的信干比为

$$\gamma_{\mathrm{E}}=\frac{P_1a_2^2|g_{\mathrm{AE}}|^2}{P_1a_1^2|g_{\mathrm{AE}}|^2+P_2\sum\limits_{\mathrm{B}\in\phi_{\mathrm{B}}}|h_{\mathrm{BE}}|^2d_{\mathrm{BE}}^{-\alpha}} \tag{6}$$

为了表述方便，以后的分析中令$I_i^2=\sum\limits_{\mathrm{B}\in\phi_{\mathrm{B}}}|h_{\mathrm{Bi}}|^2d_{\mathrm{Bi}}^{-\alpha}$，$i$为合法接收节点或窃听节点。

在得到接收节点处的信干比后。下面，研究随机网络下CR-NOMA的功率分配系数以及网络的可靠性、安全性和有效性。

3 功率分配系数及安全通信性能

3.1 功率分配系数

为减小信道的导频资源开销，本文采用固定的传输速率进行通信。给定主用户的连接中断概率阈值，通过调整功率分配系数使得主用户的连接中断概率小于对应的阈值，得到满足可靠性能约束的主用户功率分配系数。

当发端Alice和用户1之间信道的信道容量小于信息传输速率时，用户1不能正常解码有用信息，此时发生连接中断。由此可得，连接中断概率为

$$\begin{aligned}P_{\mathrm{co1}}&=\Pr\{R_{\mathrm{t1}}>C_1\}\\&=\Pr\left\{\log_2\left(1+\frac{P_1a_1^2|g_{\mathrm{A1}}|^2}{P_1a_2^2|g_{\mathrm{A1}}|^2+P_2I_1^2}\right)<R_{\mathrm{t1}}\right\}\\&=\Pr\left\{\left[\mathrm{P}_1a_1^2-P_1\left(1-a_1^2\right)\varepsilon_{\mathrm{t1}}\right]|h_{\mathrm{A1}}|^2\right.\\&\left.<P_2I_1^2\varepsilon_{\mathrm{t1}}d_{\mathrm{A1}}^{\alpha}\right\}\end{aligned} \tag{7}$$

其中$\varepsilon_{\mathrm{t1}}=2^{R_{\mathrm{t1}}}-1$, R_{t1}为主用户传输速率。

当$a_1^2-\left(1-a_1^2\right)\varepsilon_{\mathrm{t1}}<0$，即$a_1^2\le\dfrac{\varepsilon_{\mathrm{t1}}}{\varepsilon_{\mathrm{t1}}+1}$时，式(7)可表示为

$$P_{\mathrm{co1}}=\Pr\left\{|h_{\mathrm{A1}}|^2>\frac{P_2I_1^2\varepsilon_{\mathrm{t1}}d_{\mathrm{A1}}^{\alpha}}{P_1a_1^2-P_1\left(1-a_1^2\right)\varepsilon_{\mathrm{t}}}\right\}=1 \tag{8}$$

不满足实际通信需求，因此考虑$a_1^2-\left(1-a_1^2\right)\varepsilon_{\mathrm{t1}}>0$，即$a_1^2>\dfrac{\varepsilon_{\mathrm{t1}}}{\varepsilon_{\mathrm{t1}}+1}$，式(7)可写为

$$\begin{aligned}P_{\mathrm{co1}}&=\Pr\left\{|h_{\mathrm{A1}}|^2<\frac{P_2I_1^2\varepsilon_{\mathrm{t1}}d_{\mathrm{A1}}^{\alpha}}{P_1a_1^2-P_1\left(1-a_1^2\right)\varepsilon_{\mathrm{t}}}\right\}\\&=1-\exp\left(-\frac{P_2I_1^2\varepsilon_{\mathrm{t1}}d_{\mathrm{A1}}^{\alpha}}{P_1a_1^2-P_1\left(1-a_1^2\right)\varepsilon_{\mathrm{t1}}}\right)\end{aligned} \tag{9}$$

假设连接中断概率阈值为δ，根据文献[19]，当干扰节点为均匀泊松点分布时，式(7)可写为

$$P_{\mathrm{co1}}=1-\exp\left(-\pi\Gamma\left(1+\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right)\lambda_B\left(\frac{P_2}{P_1}\right)^{\frac{2}{\alpha}}\frac{\varepsilon_{\mathrm{t1}}^2d_{\mathrm{A1}}^2}{\left[a_1^2-\left(1-a_1^2\right)\varepsilon_{\mathrm{t1}}\right]^{\frac{2}{\alpha}}}\right)\le\delta \tag{10}$$

其中，λ_{s}为干扰节点的密度。

由此可得，主用户的功率分配系数应满足

$$a_1^2\ge\frac{\sqrt[\frac{2}{\alpha}]{\dfrac{\pi\Gamma\left(1+\dfrac{2}{\alpha}\right)\Gamma\left(1-\dfrac{2}{\alpha}\right)\lambda_{\mathrm{B}}\left(\dfrac{P_2}{P_1}\right)^{\frac{2}{\alpha}}\varepsilon_{\mathrm{t1}}^{\frac{2}{\alpha}}\mathrm{d}_{\mathrm{A1}}^2}{\ln(1-\delta)^{-1}}}+\varepsilon_{\mathrm{t1}}}{1+\varepsilon_{\mathrm{t1}}} \tag{11}$$

为了在保证主用户正常通信的前提下，提高次用户的通信性能，则主用户的功率分配系数取下限。因此主用户的功率分配系数为

$$a_1^2=\min\left(\frac{\sqrt[\frac{2}{\alpha}]{\dfrac{\pi\Gamma\left(1+\dfrac{2}{\alpha}\right)\Gamma\left(1-\dfrac{2}{\alpha}\right)\lambda_{\mathrm{s}}\left(\dfrac{P_2}{P_1}\right)^{\frac{2}{\alpha}}\varepsilon_{\mathrm{t1}}^{\frac{2}{\alpha}}\mathrm{d}_{\mathrm{A1}}^2}{\ln(1-\delta)^{-1}}}+\varepsilon_{\mathrm{t1}}}{1+\varepsilon_{\mathrm{t1}}},1\right)\tag{12}$$

可以发现，主用户的功率分配系数与干扰信号和传输信号的功率比、干扰节点密度、传输速率、距离等因素有关。当干扰信号功率与发端总信号功率的比值降低时，a_1增大。这是因为当主用户信息传输速率一定时，干扰信号功率增大，主用户通信对接收端的信干比会下降，这导致一定的信道功率增益下信道容量下降，链路的可靠性下降。对此，为保证主用户通信对的正常通信，要增大a_1，提高发端分配给主用户的功率，以保证主用户通信对链路的可靠性；当发端发送的总功率降低时，使得发端分配给主用户的功率下降，同样会使得主用户接收端信干比下降，从而不能保证主用户通信链路的可靠性，为此，发端要增大对主用户的功率分配系数，来保证CR-NOMA中主用户通信对的通信质量。当主用户通信对传输速率提高时，需要提高主用户功率分配系数，以增大主用户通信对的信道容量，来满足主用户通信对的通信需求。同样，当发端和主用户的距离增大时，信号传输过程中面临更大的衰耗，提高主用户功率分配系数可以提高接收端的信干比，保证主信道通信容量。同时，考虑到当主信道的通信环境较差，或者主用户的传输速率需求较高时，数值计算得到的主用户的功率分配系数可能会超过1，即$a_1>1$。这时，为最大化地满足主用户的通信需求，所有的功率都会分配给主信道，次用户则分配不到功率。

3.2 次用户的安全通信性能

在保证主用户正常通信的情况下，得到了发端给两个用户的功率分配系数，在此基础上，下面分析次用户的连接中断概率、安全中断概率等性能。

3.2.1 连接中断概率

当发端Alice和次用户之间信道的信道容量小于信息传输速率时，次用户不能正常解码有用信息，此时发生连接中断。由此可得，连接中断概率为

$$\begin{aligned}P_{\mathrm{co2}}&=\Pr\left\{\log_2\left(1+\frac{P_1a_2^2|g_{\mathrm{A2}}|^2}{P_2I_2^2}\right)<R_{\mathrm{t2}}\right\}=\Pr\left\{\frac{P_1a_2^2|g_{\mathrm{A2}}|^2}{P_2I_2^2}<\varepsilon_{\mathrm{t2}}\right\}\\&=\Pr\left\{|h_{\mathrm{A2}}|^2<\frac{\varepsilon_{\mathrm{t2}}P_2I_2^2d_{\mathrm{A2}}^{\alpha}}{a_2^2P_1}\right\}=1-\exp\left[-\frac{\varepsilon_{\mathrm{t2}}P_2I_2^2d_{\mathrm{A2}}^{\alpha}}{a_2^2P_1}\right]\\&=1-\exp\left[-\pi\Gamma\left(1+\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right)\lambda_B\left(\frac{P_2}{P_1}\right)^{\frac{2}{\alpha}}\frac{d_{\mathrm{A2}}^2\varepsilon_{\mathrm{t2}}^{\frac{2}{\alpha}}}{a_2^{\frac{4}{\alpha}}}\right]\end{aligned}\tag{13}$$

其中，R_{t2}为次用户传输速率，$\varepsilon_{\mathrm{t2}}=2^{R_{\mathrm{t2}}}-1$。

从式(13)可以发现，次用户的连接中断概率和干扰信号与发送信号的功率比、干扰节点的密度、发端与次用户的距离、次用户的传输速率等因素有关。可以发现，当干扰增强，即当发生干扰节点密度增大、干扰信号与有用信号的比值增大等情况时，次用户的连接中断概率增大。比较主用户的功率分配系数可以发现，干扰信号增强在导致了主用户的功率分配系数的增大的同时，使得次用户的可靠性降低。

3.2.2 安全中断概率

窃听信道的信道容量为$C_{\mathrm{E}}=\log_2(1+\gamma_{\mathrm{E}})$，由于发端Alice不能获知Eve的瞬时信道状态信息，因此绝对安全无法实现。为了提高网络的安全性，采用安全保护域下的On-Off传输方案：只有当保护域范围$\mathcal{B}(D)$内无窃听节点时，发端才选择发送信息，否则发端选择静默。保护域内窃听节点的概率分布函数为

$$P(N=k)=\exp\left(-\pi D^2\lambda_{\mathrm{E}}\right)\frac{\left(\pi D^2\lambda_{\mathrm{E}}\right)^k}{k!}\tag{14}$$

其中，N表示保护域内窃听节点的数目，D为保护域半径，λ_{E}为窃听节点密度，则N是服从均值为$\pi D^2\lambda_{\mathrm{E}}$的泊松随机变量。

当$N=0$时，即保护域内无窃听节点，此时发端发送信息。因此很容易得到信息发送概率为

$$P_{\mathrm{tx}}=P(N=0)=\exp\left(-\pi D^2\lambda_{\mathrm{E}}\right)\tag{15}$$

当Alice选定冗余速率R_{E2}进行传输时，网络的安全中断概率可以表示为

$$
\begin{aligned}
P_{\mathrm{so2}} &= \Pr\{C_{\mathrm{E}} > R_{\mathrm{E2}}\} = \Pr\left\{\log_2\left(1+\gamma_{\mathrm{E}}\right) > R_{\mathrm{E2}}\right\} \\
&= \Pr\left\{\max_{\mathrm{E}\in\phi_{\mathrm{E}}}\left\{\log_2\left(1+\frac{P_1 a_2^2|g_{\mathrm{AE}}|^2}{P_2 I_{\mathrm{E}}^2+P_1 a_1^2|g_{\mathrm{AE}}|^2}\right) > R_{\mathrm{E2}}\right\}\right\} \\
&= 1-E_{\phi_{\mathrm{B}}}\left\{E_{\phi_{\mathrm{E}}}\left\{\prod_{\mathrm{E}\in\phi_{\mathrm{E}}}\left(1-\Pr\left(\log_2\left(1+\frac{P_1 a_2^2|g_{\mathrm{AE}}|^2}{P_2 I_{\mathrm{E}}^2+P_1 a_1^2|g_{\mathrm{AE}}|^2}\right) > R_{\mathrm{E2}}\,|\phi_{\mathrm{B}},\phi_{\mathrm{E}}\right)\right)\right\}\right\} \\
&= 1-E_{\phi_{\mathrm{B}}}\left\{\exp\left(-\lambda_{\mathrm{E}}\int\limits_{R^2/\mathcal{B}(D)}\Pr\left(\log_2\left(1+\frac{P_1 a_2^2|g_{\mathrm{AE}}|^2}{P_2 I_{\mathrm{E}}^2+P_1 a_1^2|g_{\mathrm{AE}}|^2}\right) > R_{\mathrm{E2}}\,|\phi_{\mathrm{B}}\right)\mathrm{d}e\right)\right\}
\end{aligned}
\tag{16}
$$

其中，积分变量e表示以次用户发端与窃听节点Eve之间的距离长度为半径的圆的面积。

由于很难精确获知安全中断概率的闭式表达式，根据文献[9]，利用Jensen不等式可得P_{so}上界为

$$
\begin{aligned}
P_{\mathrm{so2}} &\le 1-\exp\left(-\lambda_{\mathrm{E}}\int\limits_{R^2/\mathcal{B}(D)}\Pr\left(\log_2\left(1+\frac{P_1 a_2^2|g_{\mathrm{AE}}|^2}{P_2 I_{\mathrm{E}}^2+P_1 a_1^2|g_{\mathrm{AE}}|^2}\right) > R_{\mathrm{E2}}\right)\mathrm{d}e\right) \\
&= 1-\exp\left(-\lambda_{\mathrm{E}}\int\limits_{R^2/\mathcal{B}(D)}\Pr\left\{P_1\left[a_2^2-\left(1-a_2^2\right)\varepsilon_{\mathrm{E2}}\right]|g_{\mathrm{AE}}|^2 > P_2\varepsilon_{\mathrm{E2}}I_{\mathrm{E}}^2\right\}\mathrm{d}e\right)
\end{aligned}
\tag{17}
$$

其中，$\varepsilon_{\mathrm{E2}}=2^{R_{\mathrm{E2}}}-1$。

当$\left[a_2^2-\left(1-a_2^2\right)\varepsilon_{\mathrm{E2}}\right]<0$，即$a_2^2\le\dfrac{\varepsilon_{\mathrm{E2}}}{1+\varepsilon_{\mathrm{E2}}}$时，$P_{\mathrm{so}}=1$，不满足实际通信需求。因此，当$a_2^2>\dfrac{\varepsilon_{\mathrm{E2}}}{1+\varepsilon_{\mathrm{E2}}}$时，安全中断概率可以表示为

$$
\begin{aligned}
P_{\mathrm{so2}} &\le 1-\exp\left[-\lambda_{\mathrm{E}}\int\limits_{R^2/\mathcal{B}(D)}\exp\left(-\frac{P_2 I_{\mathrm{E}}^2\varepsilon_{\mathrm{E2}}d_{\mathrm{AE}}^{\alpha}}{P_1 a_2^2-P_1\left(1-a_2^2\right)\varepsilon_{\mathrm{E2}}}\right)\mathrm{d}e\right] \\
&= 1-\exp\left[-\pi\lambda_{\mathrm{E}}\int_D^{\infty}\exp\left(-\pi\Gamma\left(1+\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right)\lambda_{\mathrm{B}}\left(\frac{P_2}{P_1}\right)^{\frac{2}{\alpha}}\frac{\varepsilon_{\mathrm{E2}}^{2/\alpha}d_{\mathrm{AE}}^2}{\left[a_2^2-\left(1-a_2^2\right)\varepsilon_{\mathrm{E2}}\right]^{2/\alpha}}\right)\mathrm{d}d_{\mathrm{AE}}^2\right] \\
&= 1-\exp\left(\frac{-\lambda_{\mathrm{E}}\exp\left(-\pi\Gamma\left(1+\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right)\lambda_{\mathrm{B}}\left(\frac{P_2}{P_1}\right)^{\frac{2}{\alpha}}\frac{\varepsilon_{\mathrm{E2}}^{\frac{2}{\alpha}}D^2}{\left[a_2^2-\left(1-a_2^2\right)\varepsilon_{\mathrm{E2}}\right]^{2/\alpha}}\right)}{\Gamma\left(1+\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right)\lambda_{\mathrm{B}}\left(\frac{P_2}{P_1}\right)^{2/\alpha}\dfrac{\varepsilon_{\mathrm{E2}}^{2/\alpha}}{\left[a_2^2-\left(1-a_2^2\right)\varepsilon_{\mathrm{E2}}\right]^{2/\alpha}}}\right)
\end{aligned}
\tag{18}
$$

通过式(18)可以发现，次用户的安全中断概率与干扰信号、窃听节点密度、安全保护域半径等因素有关。其中，虽然干扰信号的增强会降低网络的可靠性，但是同时由于干扰信号会干扰窃听节点对信号的接收，因此干扰信号的增强反过来会提高次用户通信的安全性。同样，式(18)表明安全中断概率是关于保护域半径的单调递减函数，因此增大安全保护域的范围同样可以提高网络的安全性，这与实际情况相符。增大安全保护域的半径可以排除距离发端较近的窃听节点，而距离越近的窃听节点，往往更容易窃听到有用信息。因此发端选择在保护域内没有窃听节点时发送信号，可以有效提高网络的安全性。但同时，安全保护域的增大使得保护域内无窃听节点的概率降低，发端因此常常处于静默状态，这使得网络的通信时延增大。因此，安全保护域范围的设置造成了有效性和安全性的折中。

本节在保证发端与主用户之间正常通信的前提下，研究了网络的功率分配系数。得到了次用户通信的连接中断概率、安全中断概率的闭式表达式。本文通过仿真验证理论分析的正确性。

4 仿真结果与分析

本节参考文献[20]，在密集异构蜂窝网络场景下研究系统的通信性能，利用理论曲线以及仿真结果给出了功率分配系数以及中断概率的变化情况。如无特殊说明，本网络预设参数如下：发端和主用户之间的距离为$d_{\mathrm{A1}}=250$ m，发端和次用户之间的距离为$d_{\mathrm{A2}}=120$ m，路径衰落因子为4，主用户

的传输速率为$R_{\mathrm{t1}}=1.0$ bit/(s·Hz)，主用户连接中断概率阈值$\delta=0.05$，次用户的传输速率为$R_{\mathrm{t2}}=1.2$ bit/(s·Hz)，次用户的冗余信息速率为$R_{\mathrm{E2}}=0.5$ bit/(s·Hz)，发端发送功率为$P_1=17$ dBm，干扰源发送功率$P_2=10$ dBm，干扰源的密度$\lambda_{\mathrm{B}}=10^{-3}/\mathrm{m}^2$，窃听节点密度$\lambda_{\mathrm{E}}=10^{-4}/\mathrm{m}^2$，保护域半径$D=30$ m。蒙特卡洛仿真次数为50000次。

图2给出了NOMA方式的功率分配系数随着主用户的连接中断概率阈值的变化情况。从图中可以看到，随着主用户对可靠性的要求逐渐降低，分配给主用户的功率也逐渐降低。同时，从图中可以发现，在相同的主用户连接中断概率约束下，随着主用户信息传输速率提高，主用户的功率分配系数也随之提高。这与实际情况相符，当用户的信息传输速率提高时，提高发送功率可以增大接收节点处的信干比，进而提高信道容量，以满足主用户的可靠性能约束。

图3给出了连接中断概率和安全中断概率随着发端发送功率的变化情况。从图中可以发现，仿真结果与理论曲线基本重合，验证了理论分析的正确性。随着发送功率的增大，连接中断概率下降，而安全中断概率提高。这与实际情况相符，发送功率的增强，增大了合法节点和窃听节点处的信干比，从而提高了节点与发端之间信道的容量，进而影响了网络的可靠性能和安全性能。同时，在相同的发送功率下，干扰信号的增强在降低网络的可靠性能的同时，使得网络的安全性能显著提升。这说明在网络的安全性能较差，同时对可靠性能要求不高时，人为地适当提高干扰可以有效改善通信质量。

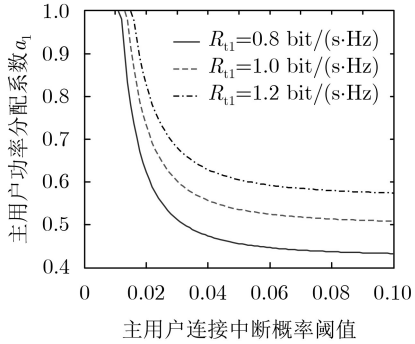

图 2 功率分配系数随主用户中断概率阈值变化图

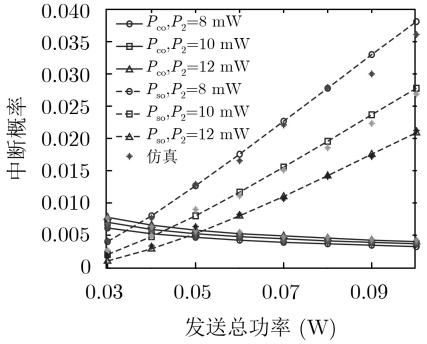

图 3 中断概率随发送总功率变化图

图4给出了中断概率随着窃听节点密度的变化情况。从图中可以发现，仿真结果与理论曲线基本重合，验证了理论分析的正确性。随着窃听节点密度的增大，网络的连接中断概率不变，安全中断概率提高。在窃听节点密度较低时，信息被窃听者窃听的概率很低，而随着窃听节点密度的增大，网络的安全中断概率逐渐提高，容易发生泄密。同时，安全中断概率采用Jensen不等式取其上界，从图中可以发现，窃听节点密度较低时，本文给出的安全中断概率的上界与仿真结果拟合程度较好。当窃听节点密度较大时，由于窃听节点的仿真规模受限，不能较好地模拟实际通信中大量的窃听节点的分布情况，使得理论得到的安全中断概率上界与仿真结果拟合较差。

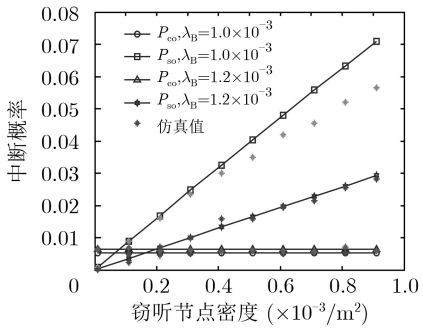

图 4 中断概率随窃听节点密度变化图

5　结束语

本文针对干扰源以及窃听节点均随机分布的通信场景，研究了CR-NOMA中次用户的物理层安全通信性能，得到了CR-NOMA中满足主用户可靠性能约束时的功率分配系数。在此基础上，理论分析得到了CR-NOMA中次用户通信的连接中断概率和安全中断概率的闭式表达式，得到了其随发送功率以及窃听节点密度的变化规律，仿真结果验证了理论分析的正确性。本研究为分析CR-NOMA随机网络中的物理层安全通信性能提供了参考。下一阶段可以将两个用户扩展到多用户，研究多用户的安全通信性能。

参 考 文 献

[1] YANG Nan, WANG Lifeng, GERACI G, *et al*. Safeguarding 5G wireless communication networks using physical layer security[J]. *IEEE Communications Magazine*, 2015, 53(4): 20–27. doi: 10.1109/MCOM.2015.7081071.

[2] MARZBAN M F, KASHEF M, ABDALLAH M, *et al*. Beamforming and power allocation for physical-layer security in hybrid RF/VLC wireless networks[C]. The 13th International Wireless Communications and Mobile Computing Conference, Valencia, Spain, 2017: 258–263. doi: 10.1109/IWCMC.2017.7986296.

[3] WANG Huiming, WANG Chao, NG D W K, *et al*. Artificial noise assisted secure transmission for distributed antenna systems[J]. *IEEE Transactions on Signal Processing*, 2016, 64(15): 4050–4064. doi: 10.1109/TSP.2016.2558164.

[4] DAI Linglong, WANG Bichai, YUAN Yifei, *et al*. Non-orthogonal multiple access for 5G: Solutions, challenges, opportunities, and future research trends[J]. *IEEE Communications Magazine*, 2105, 53(9): 74–81. doi: 10.1109/MCOM.2015.7263349.

[5] HE Biao, LIU An, YANG Nan, *et al*. On the design of secure non-orthogonal multiple access systems[J]. *IEEE Journal on Selected Areas in Communications*, 2017, 35(10): 2196–2206. doi: 10.1109/JSAC.2017.2725698.

[6] 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. doi: 10.11999/JEIT161197.
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. doi: 10.11999/JEIT161197.

[7] CHANDWANI N, JAIN A, and VYAVAHARE P D. Throughput comparison for cognitive radio network under various conditions of primary user and channel noise signals[C]. 2015 Radio and Antenna Days of the Indian Ocean, Belle Mare, 2015: 1–2. doi: 10.1109/RADIO.2015.7323379.

[8] CICIOĞLU M, CICIOĞLU S, and ÇALHAN A. Performance analysis of software-defined network approach for wireless cognitive radio networks[C]. The 26th Signal Processing and Communications Applications Conference, Izmir, Turkey, 2018: 1–4. doi: 10.1109/SIU.2018.8404691.

[9] DING Zhiguo, FAN Pingzhi, and POOR H V. Impact of user pairing on 5G nonorthogonal multiple-access downlink transmissions[J]. *IEEE Transactions on Vehicular Technology*, 2016, 65(8): 6010–6023. doi: 10.1109/TVT.2015.2480766.

[10] LIU Yuanwei, DING Zhiguo, ELKASHLAN M, *et al*. Nonorthogonal multiple access in large-scale underlay cognitive radio networks[J]. *IEEE Transactions on Vehicular Technology*, 2016, 65(12): 10152–10157. doi: 10.1109/TVT.2016.2524694.

[11] LÜ Lu, CHEN Jian, and NI Qiang. Cooperative non-orthogonal multiple access in cognitive radio[J]. *IEEE Communications Letters*, 2016, 20(10): 2059–2062. doi: 10.1109/LCOMM.2016.2596763.

[12] ARZYKULOV S, TSIFTSIS T A, NAURYZBAYEV G, *et al*. Outage performance of cooperative underlay CR-NOMA with imperfect CSI[J]. *IEEE Communications Letters*, 2019, 23(1): 176–179. doi: 10.1109/LCOMM.2018.2878730.

[13] CHEN Yingyang, WANG Li, and JIAO Bingli. Cooperative multicast non-orthogonal multiple access in cognitive radio[C]. 2017 IEEE International Conference on Communications, Paris, France, 2017: 1–6.

[14] LÜ Lu, CHEN Jian, NI Qiang, *et al*. Design of cooperative non-orthogonal multicast cognitive multiple access for 5G systems: User scheduling and performance analysis[J]. *IEEE Transactions on Communications*, 2017, 65(6): 2641–2656. doi: 10.1109/TCOMM.2017.2677942.

[15] WANG Huiming, WANG Chao, ZHENG Tongxing, *et al*. Impact of artificial noise on cellular networks: A stochastic geometry approach[J]. *IEEE Transactions on Wireless Communications*, 2016, 15(11): 7390–7404. doi: 10.1109/TWC.2016.2601903.

[16] HU Xiang, ZHANG Xing, HUANG Haozhou, *et al*. Secure transmission via jamming in cognitive radio networks with possion spatially distributed eavesdroppers[C]. The 27th IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications, Valencia, Spain, 2016: 1–6. doi: 10.1109/PIMRC.2016.7794918.

[17] CHEN Hui, TAO Xiaofeng, LI Na, *et al*. Secrecy performance analysis of hybrid eavesdroppers system using stochastic geometry and random matrix theory[C]. 2017 IEEE International Conference on Communications, Paris, France, 2017: 1–6. doi: 10.1109/ICC.2017.7996465.

[18] DENG Yansha, WANG Lifeng, 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*, 2016, 11(6): 1128–1138. doi: 10.1109/TIFS.2016.2516917.

[19] CAI Yueming, XU Xiaoming, and YANG Weiwei. Secure transmission in the random cognitive radio networks with secrecy guard zone and artificial noise[J]. *IET Communications*, 2016, 10(15): 1904–1913. doi: 10.1049/iet-com.2016.0117.

[20] 黄开枝, 王兵, 许晓明, 等. 基于安全保护域的增强型多点协作传输机制[J]. 电子与信息学报, 2018, 40(1): 108–115. doi: 10.11999/JEIT170478.
HUANG Kaizhi, WANG Bing, XU Xiaoming, *et al*. An enhanced coordinated multipoint transmission policy based on secrecy guard zone[J]. *Journal of Electronics & Information Technology*, 2018, 40(1): 108–115. doi: 10.11999/JEIT170478.

于宝泉：男，1996年生，博士生，主要研究方向为移动通信等.

蔡跃明：男，1961年生，教授，博士生导师，主要研究方向为移动通信、协同通信等.

胡健伟：男，1990年生，博士生，主要研究方向为移动通信、协同通信等.