认知协作 NOMA 网络的安全性能分析

杨震[1,2]，朱梦瑶[1]，冯友宏[3]

（1. 南京邮电大学通信与信息工程学院，江苏 南京 210003；
2. 南京邮电大学通信与网络技术国家地方联合工程研究中心，江苏 南京 210003；
3. 安徽师范大学物理与电子信息学院，安徽 芜湖 241199）

摘 要：为了提高通信系统的安全性能且使有限的频谱得到高效利用，将填充式认知无线电（OCR）与非正交多址接入（NOMA）技术相结合，提出了一个次网络通过感知主用户是否占用频谱来实现辅助主网络通信或次网络通信的动态切换的系统模型。主次网络均采用人工噪声（AN）技术进一步改善系统的安全传输性能。通过分别推导主、次网络安全中断概率和安全吞吐量的表达式来研究系统的安全中断性能。仿真结果表明了所提出的认知协作 NOMA 方案在降低中断概率、提高吞吐量方面的有益效果，并且进一步给出了人工噪声功率分配因子对系统性能的影响。

关键词：填充式认知无线电；非正交多址接入；人工噪声；安全中断性能

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2020180

Secrecy performance analysis on cooperative CR-NOMA network

YANG Zhen[1,2], ZHU Mengyao[1], FENG Youhong[3]

1. College of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
2. National Local Joint Engineering Research Center for Communications and Network Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
3. School of Physical and Electronic Information, Anhui Normal University, Wuhu 241199, China

Abstract: In order to improve the secrecy performance of communication system and make efficient use of limited spectrum, overlay cognitive radio (OCR) technology was combined with non-orthogonal multiple access (NOMA) technology and the communication model was proposed, in which secondary network realized dynamic switching between assisting primary network communication and secondary network communication by sensing whether the primary user occupied the spectrum or not. Artificial noise (AN) aided technology was used in primary and secondary networks respectively to further improve the secrecy performance of the system. The secrecy performance of the system was studied by deducing the expressions of the primary and secondary network secrecy outage probability and secrecy throughput respectively. The simulation results show that the proposed cognitive cooperative NOMA communication scheme is beneficial in reducing secrecy outage probability and increasing secrecy throughput. Furthermore, the influence of AN power allocation factor on system performance is given.

Key words: overlay cognitive radio, non-orthogonal multiple access, artificial noise, secrecy outage performance

1 引言

物联网（IoT, Internet of things）需求的大幅增长给无线通信带来了巨大的挑战，预计接入蜂窝网络的设备数量将远远超过现有数量[1]。因此，提高频谱利用率是 5G 及未来移动通信技术关注的主要课题之一，非正交多址接入（NOMA, non-orthogonal multiple access）技术因能够通过分配相同的时间和

收稿日期：2020–04–23；**修回日期**：2020–08–04

基金项目：国家自然科学基金资助项目（No.61671252）；安徽省自然科学基金资助项目（No.2008085MF181）

Foundation Items: The National Natural Science Foundation of China (No.61671252), The Natural Science Foundation of Anhui Province (No.2008085MF181)

频率资源来同时服务于多个用户，提高频谱利用率，代替正交多址接入（OMA, orthogonal multiple access）技术成为了 5G 移动通信系统的重要组成部分[1-3]。为了解决因源端和目的端之间距离过远而造成通信性能下降的问题，许多文献提出了 NOMA 中继协作技术。在中继协作网络中，源端通过中继的辅助将信息发送到目的端，这进一步改善了系统性能。文献[4]提出了一种节省带宽的连续用户中继方案来提高频谱效率。文献[5]研究了一种基于 NOMA 的双向协作中继传输系统，通过联合优化时间和功率分配降低了系统的中断概率。文献[6]研究了不同中继选择方案对系统性能的影响，证明了基于两阶段的中继选择方案相比传统的最大−最小中继选择方案有更好的效果。

认知无线电（CR, cognitive radio）技术是另一种解决频谱稀缺问题的方法。与 NOMA 主要增强用户连通性不同，认知网络可以感知频谱空穴并灵活地访问主网络频谱以实现频谱共享，解决频谱利用率不足的问题，因此，将 CR 与 NOMA 这 2 种通过不同的方式提高频谱效率的技术相结合应用于未来移动通信是近年来研究的一个热点课题[7]。文献[8]研究了下垫式认知无线电（UCR, underlay cognitive radio）的信道状态信息不完全的 CR-NOMA 系统的中断性能。在下垫式（underlay）网络中，认知网络在发射功率对主用户的干扰可控时，主用户允许其接入授权频谱传输信息从而提高频谱利用率。文献[9]提出了协作认知中继多载波非正交多址系统的资源分配算法，认知网络辅助主网络进行信息传输从而提高主网络的系统性能。文献[10]研究了一种具有全双工（FD, full duplex）多天线中继辅助通信的 CR-NOMA 网络，该网络可在满足远端用户速率要求的前提下，最大化近端用户速率。

然而，由于无线传输的广播特性，无线通信很容易被窃听。因此，通信系统在设计时，安全性是一个不得不考虑的问题。传统方案中使用加密算法进行信息传输，但由于加密和解密的复杂性，近年来基于信息论的物理层安全（PLS, physical layer security）技术逐渐进入大众视野[11]。文献[12]研究了能量收集模式下存在窃听用户的合法单用户的物理层安全问题。文献[13]研究了多中继协作 NOMA 网络在 Nakagami-*m* 衰落信道下的安全中断性能，分析了不同的最优中继选择方案的中断概率并进行比较。文献[14]研究了分别采用解码转发（DF, decode-and-forward）和放大转发（AF, amplify-and-forward）时系统的安全容量和安全中断概率。文献[15]在现有技术的基础上研究了一个更实用的非线性能量收集模型，该模型基于同步的无线信息和功率传输，在安全和速率及能量收集约束条件下，通过人工辅助噪声波束成形设计，从而提高安全传输性能。文献[16]研究了主次用户协作工作的认知 NOMA 网络中，当次用户窃听主用户信息时，利用主用户信道增益配对或减少次用户数量来提高主用户的性能。

文献[7,9]将 NOMA 与填充式认知无线电（OCR, overlay cognitive radio）结合，但仅仅考虑频谱资源高效利用而没有考虑安全性问题。与文献[7,9]不同的是，本文方案同时考虑了频谱资源的高效利用和安全性。文献[16]主要研究次用户窃听主用户信息时主用户的安全问题，与文献[16]不同的是，本文方案主要在外部窃听者存在时综合考虑了主次网络的安全性能。值得注意的是，与文献[7,9,16]的协作策略中次网络需要解码主网络的信息不同的是，本文的协作策略中，主次网络不需要获取对方的信息和编码方式用于解码对方网络的信息，这种策略更符合实际场景，同时避免了主次网络间相互干扰，降低了窃听风险。在本文的协作策略中，认知无线电网络基于填充式（overlay）网络，通过感知主用户是否占用频谱实现辅助主网络通信和认知网络通信的动态切换，并在主次网络中分别使用人工噪声（AN, artificial noise）技术进一步提高安全传输性能。仿真结果表明，本文提出的认知协作 NOMA 方案相比于传统的非主次网络协作的策略，系统的安全中断性能有显著的提高，有效地提升了频谱利用率。

2 系统模型

考虑如图 1 所示的认知协作 NOMA 系统模型，该模型由主网络（PN, primary network）和次网络（SN, secondary network）组成。PN 由主发射机（PT, primary transmitter）和主用户（PU, primary user）构成；SN 由次发射机（ST, secondary transmitter）和次用户（SU_1, SU_2）构成。窃听用户（E, eavesdropper）试图截获主用户和次用户的信号。为了增强系统安全性能，PN 通过 ST 的辅助来转发信息。

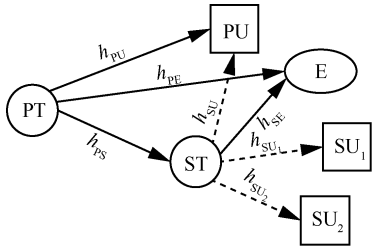


图 1　认知协作 NOMA 系统模型

SN 有 2 种工作模式：1)当 SN 感知到 PU 占用频谱时，ST 便作为 PN 的中继，接收来自 PT 的信息并放大转发给 PU, 从而提高 PN 的性能; 2)当 SN 感知到频谱空穴时，ST 发送次用户所需的信号。在 2 个网络中都采取了 AN 技术来提高安全性能。链路 PT—PU、PT—ST、ST—PU、ST— SU_1、ST— SU_2、PT—E、ST—E 的信道增益表示为 h_i，$i\in\{\mathrm{PU,PS,SU,SU_1,SU_2,PE,SE}\}$。假设所有的信道增益均服从均值为 0、方差为 $\sigma_{h_i}^2$ 的瑞利分布 $h_i\sim \mathrm{CN}(0,\sigma_{h_i}^2)$，且相互独立。

1) SN 工作在第一种模式

在第一个时隙中，PT 将 PU 所需要的信息和人工噪声混合叠加发送给 PU。SN 检测到频谱被占用后，将 ST 用于辅助 PT 转发信息，即作为 PN 的中继。PT 处的发送信号为 $\sqrt{a_1P_P}x_1+\sqrt{a_2P_P}x_2$，其中，$x_1$ 和 x_2 分别表示要发送给 PU 的机密信息和用来抵御窃听的干扰信息，该干扰信息是一个预设的伪随机信号并且提前存储在 PU 处用于干扰抵消[11]；P_{P} 表示 PT 处的总发送功率；a_1 和 a_2 分别表示 x_1 和 x_2 的功率分配系数，$a_1+a_2=1$。这一信号同时被窃听用户窃听，此时 PU、ST 和 E 接收到的信号分别表示为

$$y_{\mathrm{PU}}^1=h_{\mathrm{PU}}(\sqrt{a_1P_{\mathrm{P}}}x_1+\sqrt{a_2P_{\mathrm{P}}}x_2)+n_{\mathrm{PU}} \tag{1}$$

$$y_{\mathrm{ST}}=h_{\mathrm{PS}}(\sqrt{a_1P_{\mathrm{P}}}x_1+\sqrt{a_2P_{\mathrm{P}}}x_2)+n_{\mathrm{ST}} \tag{2}$$

$$y_{\mathrm{E}}^1=h_{\mathrm{PE}}(\sqrt{a_1P_{\mathrm{P}}}x_1+\sqrt{a_2P_{\mathrm{P}}}x_2)+n_{\mathrm{E}} \tag{3}$$

其中，$n_{\mathrm{PU}},n_{\mathrm{PS}},n_{\mathrm{PE}}\sim\mathrm{CN}(0,\sigma^2)$ 分别表示各节点处的加性高斯白噪声，σ^2 表示方差。由于 PU 可以分辨出干扰信号并去除，而窃听用户 E 只能将其作为背景噪声处理，PU 和 E 解码 x_1 的信噪比（SNR, signal-to-noise ratio）和信干噪比（SINR, signal-to-interference-noise ratio）分别为

$$\gamma_{\mathrm{PU}}^1=\left|h_{\mathrm{PU}}\right|^2a_1\rho_{\mathrm{P}} \tag{4}$$

$$\gamma_{\mathrm{E}}^1=\frac{\left|h_{\mathrm{PE}}\right|^2a_1\rho_{\mathrm{P}}}{\left|h_{\mathrm{PE}}\right|^2a_2\rho_{\mathrm{P}}+1} \tag{5}$$

其中，$\rho_{\mathrm{P}}=\dfrac{P_{\mathrm{P}}}{\sigma^2}$ 表示 PT 处的发射信噪比。

充当中继端的 ST 收到该重叠信号后，利用 AF 技术将重叠信号进行放大，在第二个时隙发送给 PU。放大因子 $G=\sqrt{\dfrac{P_{\mathrm{S}}}{P_{\mathrm{P}}\left|h_{\mathrm{PS}}\right|^2+\sigma^2}}$，其中，$P_{\mathrm{S}}$ 表示 ST 处的发射总功率。在第二个时隙中，PU 和 E 收到的信号分别如式(6)和式(7)所示。

$$y_{\mathrm{PU}}^2=h_{\mathrm{SU}}Gy_{\mathrm{ST}}+n_{\mathrm{PU}} \tag{6}$$

$$y_{\mathrm{R}}^2=h_{\mathrm{SE}}Gy_{\mathrm{ST}}+n_{\mathrm{E}} \tag{7}$$

因此，PU 和 E 在第二个时隙解码 x_1 的 SINR 分别如式(8)和式(9)所示。

$$\gamma_{\mathrm{PU}}^2=\frac{\rho_{\mathrm{S}}a_1\rho_{\mathrm{P}}\left|h_{\mathrm{PS}}\right|^2\left|h_{\mathrm{SU}}\right|^2}{\rho_{\mathrm{S}}\left|h_{\mathrm{SU}}\right|^2+\rho_{\mathrm{P}}\left|h_{\mathrm{PS}}\right|^2+1} \tag{8}$$

$$\gamma_{\mathrm{E}}^2=\frac{\rho_{\mathrm{S}}a_1\rho_{\mathrm{P}}\left|h_{\mathrm{PS}}\right|^2\left|h_{\mathrm{SE}}\right|^2}{\rho_{\mathrm{S}}a_2\rho_{\mathrm{P}}\left|h_{\mathrm{PS}}\right|^2\left|h_{\mathrm{SE}}\right|^2+\rho_{\mathrm{S}}\left|h_{\mathrm{SE}}\right|^2+\rho_{\mathrm{P}}\left|h_{\mathrm{PS}}\right|^2+1} \tag{9}$$

其中，$\rho_{\mathrm{S}}=\dfrac{P_{\mathrm{S}}}{\sigma^2}$ 表示 ST 处的发射信噪比。由于 PU 在 2 个时隙都接收到了信号，本文采用选择合并技术将收到的信号合并。

2) SN 工作在第二种模式

当 PU 不工作时，SN 检测到频谱空穴，那么 ST 利用下行 NOMA 信道向次用户发送信息。为了防止窃听，本文的协作策略在 ST 也采用 AN 技术。这种模式下，ST 向次用户发送的信息为 $\sqrt{b_1P_{\mathrm{S}}}x_{\mathrm{S1}}+\sqrt{b_2P_{\mathrm{S}}}x_{\mathrm{S2}}+\sqrt{b_3P_{\mathrm{S}}}x_a$，其中，$x_{\mathrm{S1}}$ 和 x_{S2} 分别表示 $\mathrm{SU_1}$ 和 $\mathrm{SU_2}$ 所需的信息；x_a 表示干扰噪声，该干扰噪声是一个提前存储在次用户处的预设伪随机信号；b_1、b_2 和 b_3 表示功率分配系数。一般假设用户的信道增益按升序排序，即 $0<\left|h_{\mathrm{SU_1}}\right|<\left|h_{\mathrm{SU_2}}\right|$[1-3]。因此，根据 NOMA 功率复用原理，$\mathrm{SU_1}$ 应该分配更多的发送功率，即 $b_1>b_2$。$\mathrm{SU_1}$ 和 $\mathrm{SU_2}$ 收到混合信号后，首先去除 AN，再利用串行干扰消除（SIC, successive interference cancellation）技术进行解码，解码过程如下。

$\mathrm{SU_1}$ 解码 x_{S1}。由于 $b_1>b_2$，信号 x_{S2} 在 $\mathrm{SU_1}$ 处被当作噪声，$\mathrm{SU_1}$ 直接对 x_{S1} 进行解码。此时 $\mathrm{SU_1}$ 端解码 x_{S1} 的 SINR 为

$$\gamma_{\mathrm{SU}_1}=\frac{b_1\rho_{\mathrm{S}}\left|h_{\mathrm{SU}_1}\right|^2}{b_2\rho_{\mathrm{S}}\left|h_{\mathrm{SU}_1}\right|^2+1} \tag{10}$$

SU_2 解码 x_{S2}。首先将自身信号当作噪声先把 x_{S1} 解码出来并去除，再解码自身信号。此时 SU_2 解码 x_{S2} 的 SINR 为

$$\gamma_{\mathrm{SU}_2}=b_2\rho_{\mathrm{S}}\left|h_{\mathrm{SU}_2}\right|^2 \tag{11}$$

此时 SN 中，E 窃听 x_{S1}、x_{S2} 的 SINR 分别为

$$\gamma_{\mathrm{E,S1}}=\frac{b_1\gamma_{\mathrm{S}}\left|h_{\mathrm{SE}}\right|^2}{(b_2+b_3)\gamma_{\mathrm{S}}\left|h_{\mathrm{SE}}\right|^2+1} \tag{12}$$

$$\gamma_{\mathrm{E,S2}}=\frac{b_2\gamma_{\mathrm{S}}\left|h_{\mathrm{SE}}\right|^2}{b_3\gamma_{\mathrm{S}}\left|h_{\mathrm{SE}}\right|^2+1} \tag{13}$$

3 性能分析

本节通过分别推导主网络和次网络的安全中断概率及安全吞吐量来分析本文的协作策略的中断性能。

3.1 PN 的安全中断概率

PN 中断定义为第一个时隙 PU 端未成功解码 x_1 且第二个时隙 PU 端也未能成功解码 x_1。首先根据信噪比得到 PN 在 2 个时隙的安全容量和分别为

$$C_{\mathrm{PN}}^1=\frac{1}{2}\left[\mathrm{lb}(1+\gamma_{\mathrm{PU}}^1)-\mathrm{lb}(1+\gamma_{\mathrm{E}}^1)\right] \tag{14}$$

$$C_{\mathrm{PN}}^2=\frac{1}{2}\left[\mathrm{lb}(1+\gamma_{\mathrm{PU}}^2)-\mathrm{lb}(1+\gamma_{\mathrm{E}}^2)\right] \tag{15}$$

PN 在 PU 处采用选择合并技术来输出信号，即 $C_{\mathrm{PN}}=\max\{C_{\mathrm{PN}}^1,C_{\mathrm{PN}}^2\}$，故 PN 的安全中断概率为

$$\begin{aligned}&P_{\mathrm{PN}}=\Pr\{C_{\mathrm{PN}}^1<R_{\mathrm{PU}},C_{\mathrm{PN}}^2<R_{\mathrm{PU}}\}=\\&\underbrace{\Pr\{C_{\mathrm{PN}}^1<R_{\mathrm{PU}}\}}_{\Omega_1}\underbrace{\Pr\{C_{\mathrm{PN}}^2<R_{\mathrm{PU}}\}}_{\Omega_2}\end{aligned} \tag{16}$$

其中，R_{PU} 表示 PU 的预设速率。

定理 1 Ω_1 的表达式为

$$\Omega_1\approx\chi\left(1-\mathrm{e}^{-\frac{y_l}{a_1\rho_{\mathrm{P}}}}\right) \tag{17}$$

其中，$\chi=\dfrac{\pi\varpi}{2L}\sum_{l=1}^{L}\dfrac{a_1\sqrt{1-\theta_l^2}}{\rho_{\mathrm{P}}\left(a_1-a_2a_l\right)^2}\mathrm{e}^{-\frac{a_l}{\rho_{\mathrm{P}}(a_1-a_2a_l)}}$，$\varpi=\dfrac{a_1}{a_2}$，$\theta_l=\cos\left(\dfrac{2l-1}{L}\pi\right)$，$a_l=\dfrac{(\theta_l+1)\varpi}{2}$，$y_l=2^{2R_{\mathrm{PU}}}(1+a_l)-1$，$L$ 表示复杂性–精确度平衡参数。

证明 根据式(4)、式(5)和式(14)，Ω_1 可化简为

$$\Omega_1=\Pr\left\{\gamma_{\mathrm{PU}}^1<2^{2R_{\mathrm{PU}}}(1+\gamma_{\mathrm{E}}^1)-1\right\}=\int_0^{\infty}F_{\gamma_{\mathrm{PU}}^1}(y)f_{\gamma_{\mathrm{E}}^1}(x)\mathrm{d}x \tag{18}$$

其中，$y=2^{2R_{\mathrm{PU}}}(1+x)-1$。

本文考虑瑞利衰落信道增益服从参数为 1 的指数分布，对于信道 h_i，$\left|h_i\right|^2$ 的概率密度函数为

$$f_{|h_i|^2}(x)=\mathrm{e}^{-x} \tag{19}$$

由此可得，γ_{PU}^1 和 γ_{E}^1 的累积分布函数分别为

$$F_{\gamma_{\mathrm{PU}}^1}(y)=\Pr\left(\left|h_{\mathrm{PU}}\right|^2a_1\rho_P<y\right)=1-\mathrm{e}^{-\frac{y}{a_1\rho_{\mathrm{P}}}} \tag{20}$$

$$F_{\gamma_{\mathrm{E}}^1}(x)=\Pr\left(\frac{\left|h_{\mathrm{PE}}\right|^2a_1\rho_{\mathrm{P}}}{\left|h_{\mathrm{PE}}\right|^2a_2\rho_{\mathrm{P}}+1}<x\right)=1-\mathrm{e}^{-\frac{x}{(a_1-a_2x)\rho_{\mathrm{P}}}} \tag{21}$$

由 $F_{\gamma_{\mathrm{E}}^1}(x)$ 可得

$$f_{\gamma_{\mathrm{E}}^1}(x)=\frac{a_1}{\rho_{\mathrm{P}}\left(a_1-a_2x\right)^2}\mathrm{e}^{-\frac{x}{(a_1-a_2x)\rho_{\mathrm{P}}}},0\leqslant x\leqslant\frac{a_1}{a_2} \tag{22}$$

将式(20)和式(22)代入式(18)，可得

$$\Omega_1=\int_0^{\frac{a_1}{a_2}}\frac{a_1}{\rho_{\mathrm{P}}\left(a_1-a_2x\right)^2}\left(1-\mathrm{e}^{-\frac{y}{a_1\rho_{\mathrm{P}}}}\right)\mathrm{e}^{-\frac{x}{(a_1-a_2x)\rho_{\mathrm{P}}}}\mathrm{d}x \tag{23}$$

由于式(23)的复杂性，无法得到其闭合表达式，根据 Gaussian-Chebyshev 求积公式[17]，得到式(23)的近似表达式，如式(17)所示。

证毕。

定理 2 Ω_2 的表达式为

$$\begin{aligned}&\Omega_2=\int_0^{\frac{a_1}{a_2}}\left\{1-\frac{2}{\rho_{\mathrm{S}}}\mathrm{e}^{-\left(\frac{1}{\rho_{\mathrm{P}}}+\frac{1}{\rho_{\mathrm{S}}}\right)y'}\sqrt{\frac{\rho_{\mathrm{S}}y'(y'+1)}{\rho_{\mathrm{P}}}}K_1\left(2\sqrt{\frac{y'(y'+1)}{\rho_{\mathrm{P}}\rho_{\mathrm{S}}}}\right)\right\}\cdot\\&\frac{2}{\rho_{\mathrm{S}}}\mathrm{e}^{-\left(\frac{1}{\rho_{\mathrm{P}}}+\frac{1}{\rho_{\mathrm{S}}}\right)f(x)}\left\{\left(\frac{1}{\rho_{\mathrm{P}}}+\frac{1}{\rho_{\mathrm{S}}}\right)f'(x)G(x)K_1[Z(x)]-\right.\\&\left.G'(x)K_1[Z(x)]+\frac{g'(x)}{2\rho_{\mathrm{P}}}(K_0[Z(x)]+K_2[Z(x)])\right\}\mathrm{d}x\end{aligned} \tag{24}$$

证明 根据式(8)、式(9)和式(15)，Ω_2 可化简为

$$\Omega_2=\Pr\left\{\gamma_{\mathrm{PU}}^2<2^{2R_{\mathrm{PU}}}(1+\gamma_{\mathrm{E}}^2)-1\right\}=\int_0^{\infty}F_{\gamma_{\mathrm{PU}}^2}(y)f_{\gamma_{\mathrm{E}}^2}(x)\mathrm{d}x \tag{25}$$

γ_{PU}^2 和 γ_{E}^2 的累积分布函数分别为

$$F_{\gamma_{\mathrm{PU}}^2}(y)=\Pr\left(\frac{\rho_{\mathrm{S}}a_1\rho_{\mathrm{P}}\left|h_{\mathrm{PS}}\right|^2\left|h_{\mathrm{SU}}\right|^2}{\rho_{\mathrm{S}}\left|h_{\mathrm{SU}}\right|^2+\rho_{\mathrm{P}}\left|h_{\mathrm{PS}}\right|^2+1}<y\right) \tag{26}$$

$$F_{\gamma_{\mathrm{E}}^2}(x)=\Pr\left(\frac{\rho_{\mathrm{S}}a_1\rho_{\mathrm{P}}\left|h_{\mathrm{PS}}\right|^2\left|h_{\mathrm{SE}}\right|^2}{\rho_{\mathrm{S}}a_2\rho_{\mathrm{P}}\left|h_{\mathrm{PS}}\right|^2\left|h_{\mathrm{SE}}\right|^2+\rho_{\mathrm{S}}\left|h_{\mathrm{SE}}\right|^2+\rho_{\mathrm{P}}\left|h_{\mathrm{PS}}\right|^2+1}<x\right) \tag{27}$$

从式(26)和式(27)中可以观察到，这两式都存在一个形如 $\frac{\left|h_1\right|^2\left|h_2\right|^2}{\left|h_1\right|^2+\left|h_2\right|^2+1}$ 的表达式。假设 h_1 和 h_2 分别服从参数为 λ_1 和 λ_2 的瑞利分布，$\frac{\left|h_1\right|^2\left|h_2\right|^2}{\left|h_1\right|^2+\left|h_2\right|^2+1}$ 的累积分布函数为

$$F_{|h_1|^2,|h_2|^2}(x)=\Pr\left(\frac{\left|h_1\right|^2\left|h_2\right|^2}{\left|h_1\right|^2+\left|h_2\right|^2+1}<x\right)=$$
$$\int_0^x f_{|h_1|^2}(u)\mathrm{d}u+\int_x^{\infty}\int_0^{\frac{x(u+1)}{u-x}} f_{|h_1|^2}(v)f_{|h_2|^2}(u)\mathrm{d}v\mathrm{d}u=$$
$$1-\frac{1}{\lambda_2}\mathrm{e}^{-\left(\frac{1}{\lambda_1}+\frac{1}{\lambda_2}\right)x}\int_x^{\infty}\mathrm{e}^{-\frac{1}{\lambda_2}(u-x)-\frac{x(x+1)}{\lambda_1(u-x)}}\mathrm{d}u \tag{28}$$

根据文献[18]可以得到

$$F_{|h_1|^2,|h_2|^2}(x)=$$
$$1-\frac{2}{\lambda_2}\mathrm{e}^{-\left(\frac{1}{\lambda_1}+\frac{1}{\lambda_2}\right)x}\sqrt{\frac{\lambda_2x(x+1)}{\lambda_1}}K_1\left(2\sqrt{\frac{x(x+1)}{\lambda_1\lambda_2}}\right) \tag{29}$$

式(26)可以写成

$$F_{\gamma_{\mathrm{PU}}^2}(y)=F_{\rho_{\mathrm{P}}|h_1|^2,\rho_{\mathrm{S}}|h_2|^2}(y') \tag{30}$$

其中，$y'=\frac{y}{a_1}$。将式(29)中的 λ_1 换成 $\lambda_1\rho_{\mathrm{P}}$，$\lambda_2$ 换成 $\lambda_2\rho_{\mathrm{S}}$，可得

$$F_{\gamma_{\mathrm{PU}}^2}(y)=$$
$$1-\frac{2}{\lambda_2\rho_{\mathrm{S}}}\mathrm{e}^{-\left(\frac{1}{\lambda_1\rho_{\mathrm{P}}}+\frac{1}{\lambda_2\rho_{\mathrm{S}}}\right)y'}\sqrt{\frac{\lambda_2\rho_{\mathrm{S}}y'(y'+1)}{\lambda_1\rho_{\mathrm{P}}}}K_1\left(2\sqrt{\frac{y'(y'+1)}{\lambda_1\lambda_2\rho_{\mathrm{P}}\rho_{\mathrm{S}}}}\right) \tag{31}$$

对于窃听用户 E，式(27)可以写成

$$F_{\gamma_{\mathrm{E}}^2}(x)=F_{\rho_{\mathrm{P}}|h_1|^2,\rho_{\mathrm{S}}|h_2|^2}\left[f(x)\right] \tag{32}$$

其中，$f(x)=\frac{x}{a_1-a_2x}$。将式(29)中的 λ_1 换成 $\lambda_1\rho_{\mathrm{P}}$，$\lambda_2$ 换成 $\lambda_2\rho_{\mathrm{S}}$，可得

$$F_{\gamma_{\mathrm{E}}^2}(x)=1-\frac{2}{\lambda_2\rho_{\mathrm{S}}}\mathrm{e}^{-\left(\frac{1}{\lambda_1\rho_{\mathrm{P}}}+\frac{1}{\lambda_2\rho_{\mathrm{S}}}\right)f(x)}\cdot$$
$$\sqrt{\frac{\lambda_2\rho_{\mathrm{S}}f(x)(f(x)+1)}{\lambda_1\rho_{\mathrm{P}}}}K_1\left(2\sqrt{\frac{f(x)(f(x)+1)}{\lambda_1\lambda_2\rho_{\mathrm{P}}\rho_{\mathrm{S}}}}\right) \tag{33}$$

式(33)中的 $K_{\mathrm{p}}(z)$ 为第二类修正贝塞尔函数，由定义 $-2\frac{\mathrm{d}}{\mathrm{d}z}K_{\mathrm{p}}(z)=K_{\mathrm{p-1}}(z)+K_{\mathrm{p+1}}(z)$ 可得 $\frac{\mathrm{d}}{\mathrm{d}z}K_1(z)=-\frac{K_0(z)+K_2(z)}{2}$。由此可根据式(33)得到

$$f_{\gamma_{\mathrm{E}}^2}(x)=\frac{2}{\lambda_2\rho_{\mathrm{S}}}\mathrm{e}^{-\left(\frac{1}{\lambda_1\rho_{\mathrm{P}}}+\frac{1}{\lambda_2\rho_{\mathrm{S}}}\right)f(x)}\left\{\left(\frac{1}{\lambda_1\rho_{\mathrm{P}}}+\frac{1}{\lambda_2\rho_{\mathrm{S}}}\right)f'(x)\cdot\right.$$
$$G(x)K_1\left[Z(x)\right]-G'(x)K_1\left[Z(x)\right]+$$
$$\left.\frac{g'(x)}{2\rho_{\mathrm{P}}}\left(K_0\left[Z(x)\right]+K_2\left[Z(x)\right]\right)\right\} \tag{34}$$

其中，$f'(x)=\frac{a_1}{\left(a_1-a_2x\right)^2}$，$G(x)=\left(\frac{\lambda_2\rho_{\mathrm{S}}g(x)}{\lambda_1\rho_{\mathrm{P}}}\right)^{\frac{1}{2}}$，$g(x)=f(x)(f(x)+1)$，$Z(x)=2\left(\frac{g(x)}{\lambda_1\lambda_2\rho_{\mathrm{P}}\rho_{\mathrm{S}}}\right)^{\frac{1}{2}}$。将式(31)和式(34)代入式(25)，令 $\lambda_1=\lambda_2=1$，即可得式(24)中的表达式。

故 PN 的安全中断概率为

$$P_{\mathrm{PN}}=\Omega_1\Omega_2 \tag{35}$$

证毕。

3.2　SN 的安全中断概率

SN 中断分为 3 种情况：1) SU_1 端成功解码 x_{S1}，SU_2 端未成功解码 x_{S2}；2) SU_2 端成功解码 x_{S2}，SU_1 端未成功解码 x_{S1}；3) SU_1 端未成功解码 x_{S1}，SU_2 端未成功解码 x_{S2}。根据信噪比可得到 SU_1 和 SU_2 的安全容量和分别为

$$C_{\mathrm{SU}_1}=\mathrm{lb}(1+\gamma_{\mathrm{SU}_1})-\mathrm{lb}(1+\gamma_{\mathrm{E,S1}}) \tag{36}$$

$$C_{\mathrm{SU}_2}=\mathrm{lb}(1+\gamma_{\mathrm{SU}_2})-\mathrm{lb}(1+\gamma_{\mathrm{E,S2}}) \tag{37}$$

SU_1 端和 SU_2 端安全中断概率分别为

$$\Delta_1=\Pr\left\{C_{\mathrm{SU}_1}<R_{\mathrm{S}}\right\} \tag{38}$$

$$\Delta_2=\Pr\left\{C_{\mathrm{SU}_2}<R_{\mathrm{S}}\right\} \tag{39}$$

其中，R_{S} 表示次用户的预设速率。SN 的安全中断

概率为

$$P_{\mathrm{SN}}=1-(1-\Delta_1)(1-\Delta_2) \tag{40}$$

定理 3 Δ_1 的表达式为

$$\Delta_1\approx\chi_1\left(1-\mathrm{e}^{-\frac{z_l'}{(b_1-b_2z_l')\rho_{\mathrm{S}}}}\right)+\mathrm{e}^{-\frac{\xi}{[b_1-(b_2+b_3)\xi]\rho_{\mathrm{S}}}} \tag{41}$$

其中，$\chi_1=\dfrac{\pi\xi}{2L}\sum_{l=1}^{L}\dfrac{b_1\sqrt{1-\theta_l^2}}{\rho_{\mathrm{S}}[b_1-(b_2+b_3)a_l']^2}\mathrm{e}^{-\frac{a_l'}{\rho_{\mathrm{S}}[b_1-(b_2+b_3)a_l']}}$，$a_l'=\dfrac{(\theta_l+1)\xi}{2}$，$z_l'=2^{R_{\mathrm{S}}}(1+a_l')-1$。

证明 根据式(10)、式(12)和式(36)，Δ_1 可化简为

$$\Delta_1=\Pr\left\{\gamma_{\mathrm{SU}_1}<2^{2R_{\mathrm{S}}}(1+\gamma_{\mathrm{E,S1}})-1\right\}=\int_0^{\infty}F_{\gamma_{\mathrm{SU}_1}}(z)f_{\gamma_{\mathrm{E,S1}}}(x)\mathrm{d}x \tag{42}$$

其中，$z=2^{R_{\mathrm{S}}}(1+x)-1$。类似式(20)～式(22)，可以得到

$$\Delta_1=\int_0^{\xi}\frac{b_1}{[b_1-(b_2+b_3)x]^2\rho_s}\mathrm{e}^{-\frac{x}{[b_1-(b_2+b_3)x]\rho_s}}\left(1-\mathrm{e}^{-\frac{z}{(b_1-b_2z)\rho_s}}\right)\mathrm{d}x+\int_{\xi}^{\frac{b_1}{b_2+b_3}}\frac{b_1}{[b_1-(b_2+b_3)x]^2\rho_s}\mathrm{e}^{-\frac{x}{[b_1-(b_2+b_3)x]\rho_s}}\mathrm{d}x \tag{43}$$

其中，$\xi=\min\left\{\dfrac{b_1}{b_2+b_3},\left(\dfrac{b_1}{b_2}+1\right)2^{-R_{\mathrm{S}}}-1\right\}$。同样根据 Gaussian-Chebyshev 求积公式[17]可得式(41)。

证毕。

定理 4 Δ_2 的表达式为

$$\Delta_2\approx\chi_2\left(1-\mathrm{e}^{-\frac{z_l''}{b_2\rho_{\mathrm{S}}}}\right) \tag{44}$$

其中，$\chi_2=\dfrac{\pi\omega}{2L}\sum_{l=1}^{L}\dfrac{b_2\sqrt{1-\theta_l^2}}{\rho_{\mathrm{S}}(b_2-b_3a_l'')^2}\mathrm{e}^{-\frac{a_l''}{\rho_{\mathrm{S}}(b_2-b_3a_l'')}}$，$\omega=\dfrac{b_2}{b_3}$，$a_l''=\dfrac{(\theta_l+1)\omega}{2}$，$z_l''=2^{R_{\mathrm{S}}}(1+a_l'')-1$。

证明 根据式(11)、式(13)和式(37)，可化简 Δ_2，类似式(20)～式(22)，可得

$$\Delta_2=\int_0^{\frac{b_2}{b_3}}\frac{b_2}{\rho_{\mathrm{S}}(b_2-b_3x)^2}\left(1-\mathrm{e}^{-\frac{z}{b_2\rho_{\mathrm{S}}}}\right)\mathrm{e}^{-\frac{x}{(b_2-b_3x)\rho_{\mathrm{S}}}}\mathrm{d}x \tag{45}$$

根据 Gaussian-Chebyshev 求积公式[17]可得式(44)。

故 SN 的安全中断概率为

$$\mathrm{P}_{\mathrm{SN}}=1-(1-\Delta_1)(1-\Delta_2)=1-\left(1-\chi_1\left(1-\mathrm{e}^{-\frac{z_l'}{(b_1-b_2z_l')\rho_{\mathrm{S}}}}\right)-\mathrm{e}^{-\frac{\xi}{[b_1-(b_2+b_3)\xi]\rho_{\mathrm{S}}}}\right)\left(1-\chi_2\left(1-\mathrm{e}^{-\frac{z_l''}{b_2\rho_{\mathrm{S}}}}\right)\right) \tag{46}$$

证毕。

系统吞吐量的定义为传输速率和成功通信概率的乘积。在本文中，PN 和 SN 的安全吞吐量分别为

$$T_{\mathrm{PN}}=R_{\mathrm{PU}}(1-P_{\mathrm{PN}})=R_{\mathrm{PU}}(1-\Omega_1\Omega_2) \tag{47}$$

$$T_{\mathrm{SN}}=(R_{\mathrm{S}}+R_{\mathrm{S}})(1-P_{\mathrm{SN}})=2R_{\mathrm{S}}(1-\Delta_1)(1-\Delta_2) \tag{48}$$

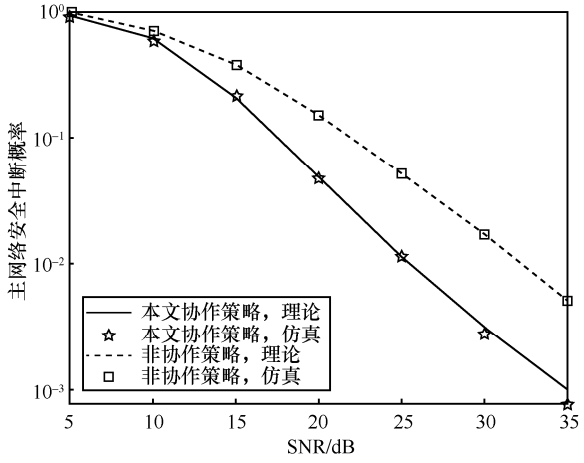
其中，$1-P_{\mathrm{PN}}$ 和 $1-P_{\mathrm{SN}}$ 分别表示主次网络从基站到用户成功通信的概率。

4 仿真结果及分析

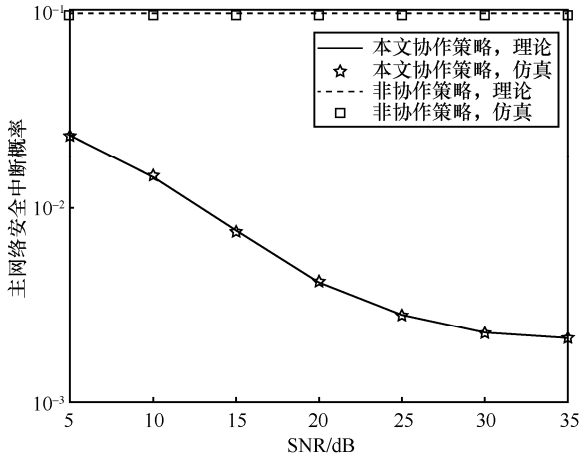
本节使用 MATLAB 对本文的协作策略下系统的安全性能进行 Monte Carlo 仿真。从主次网络的安全中断概率和安全吞吐量 2 个方面分别分析本文策略下通信系统的性能，并与文献[12]中的策略进行比较。如非特殊说明，$a_1=0.7$，a_2=0.3；$b_1=4b_2$；$L=10$，$R_{\mathrm{PU}}=1\,\mathrm{bit}\cdot(\mathrm{s}\cdot\mathrm{Hz})^{-1}$，$R_{\mathrm{S}}=0.5\,\mathrm{bit}\cdot(\mathrm{s}\cdot\mathrm{Hz})^{-1}$；方差 $\sigma_{h_i}^2$ 为 1，$i\in\{\mathrm{PU,PS,SU,SU_1,SU_2,PE,SE}\}$。

图 2(a)是当 ST 发射信噪比 $\rho_{\mathrm{S}}=20\,\mathrm{dB}$ 时，PN 的安全中断概率随 PT 发射信噪比变化的曲线。从图 2(a)中可以看出，理论结果与仿真结果一致，验证了理论推导的正确性。随着 SNR 的提高，安全中断概率不断减小。将本文的协作策略与非协作策略相比，本文策略可以有效改善 PN 系统的安全中断性能。这是因为在本文的协作策略中，ST 作为中继辅助 PN 的信息传输，使 PU 端可以实现分集接收。图 2(b)是当 PT 发射信噪比 $\rho_{\mathrm{P}}=20\,\mathrm{dB}$ 时，PN 的安全中断概率随 ST 发射信噪比变化的曲线。从图 2(b)中可以看出，随着 ρ_{S} 增加，本文协作策略中 PN 的安全中断概率有小幅下降，而非协作策略无变化。这是因为本文策略中，ST 作为中继辅助转发信息时，ρ_{S} 提高虽然有益于降低中断概率，但 ρ_{P} 是主要影响因素，所以提高 ρ_{S} 对 PN 中断性能的改善幅度较小，PN 的中断概率最终会达到下限；而在对比策略中，因为没有协作时隙，所以当 $\rho_{\mathrm{P}}=20\,\mathrm{dB}$ 时，安全中断概率恒定，且大于本文策略中的安全中断概率。由图 2 可以看出，随着 PT 和 ST 发射信噪比增加，本文策略中的主网络安全中断性能都能

得到提升，并且优于对比策略。



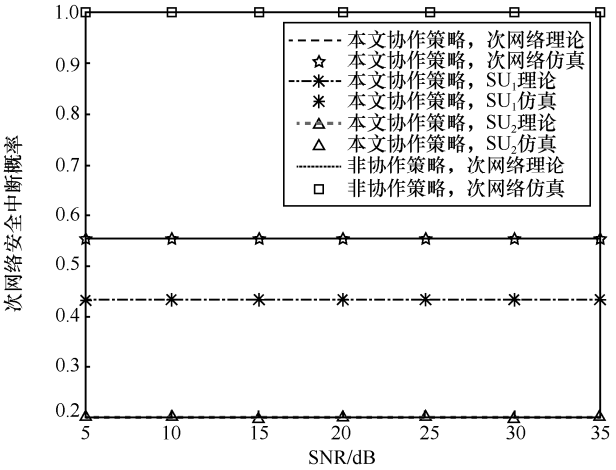
(a) ρ_S=20 dB时PN安全中断概率随PT发射信噪比变化的情况



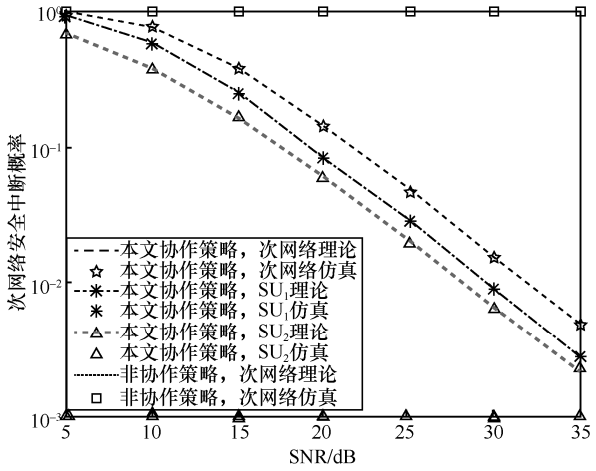
(b) ρ_P=20 dB时PN安全中断概率随ST发射信噪比变化的情况

图 2　PN 安全中断概率变化情况

图 3(a)是当 ST 传输信噪比 $\rho_S = 20$ dB 时，SN 的安全中断概率随 PT 发射信噪比变化的曲线。从图 3(a)可以看出，本文协作策略和非协作策略安全中断概率均保持不变，因为 SN 的中断性能只与 ST 的发射信噪比有关而与 PT 的发射信噪比无关。图 3(b)是当 PT 传输信噪比 $\rho_P = 20$ dB 时，系统安全中断概率随 ST 发射信噪比变化的曲线。首先，从图 3 中可以看出，理论结果与仿真结果相吻合，验证了理论推导的正确性。其次，随着 SNR 的提高，SN 的安全中断概率不断减小。由于 ST 到 SU_2 端信道条件优于 ST 到 SU_1 端信道条件，因此相同参数条件下，SU_2 端的安全中断概率小于 SU_1 的安全中断概率。此外，从图 3 还可以观察到，非协作策略的 SN 安全中断概率一直为 1，实际上，非协作策略中没有应用 CR 技术，所以不存在次网络；而本文策略采用动态切换模式，在主网络频谱未被占用时进行认知网络即次网络通信，实现了频谱复用，显著提高了频谱利用率。



(a) ρ_S=20 dB时SN安全中断概率随PT发射信噪比变化的情况



(b) ρ_P=20 dB时SN安全中断概率随ST发射信噪比变化的情况

图 3　SN 安全中断概率变化情况

图 4 和图 5 分别是 PN 和 SN 的安全中断概率随干扰噪声功率分配因子 a_2 和 b_3 变化的情况。仿真中设置 $\rho_P = \rho_S = 20$ dB。从图 4 和图 5 中可以观察到，在一定范围内提高 a_2 和 b_3，PN 和 SN 的安全中断概率均会降低，表明了本文的协作策略中的人工噪声方案在综合改善 PN 和 SN 系统安全性能方面的有效性；超过某一阈值后，安全中断概率开始增大，这是因为虽然提高干扰噪声的发射功率有益于抵御窃听用户攻击，但当过多的功率分配给干扰噪声时，分配给合法用户的功率随之减小，影响了合法用户的正常通信，中断性能随之降低。这说明调整功率分配参数可获得最优的安全中断性能。仿真结果给出了当预设速率分别为

0.4、0.6、0.8 时，PN 和 SN 的安全中断概率随 a_2 和 b_3 分别变化的情况。从仿真结果可以看出，随着预设速率的增加，PN 和 SN 的安全中断概率均上升，这说明了传输速率的提高需要以降低中断性能为代价。

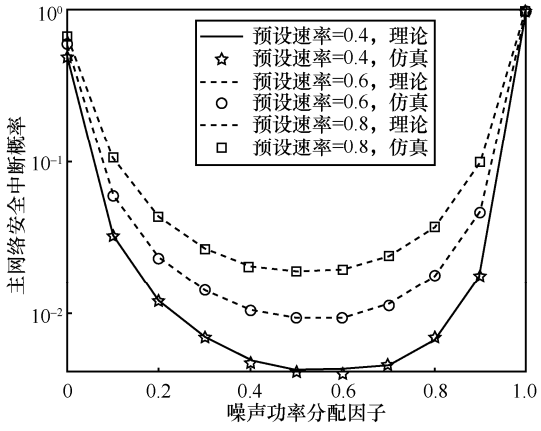


图 4 PN 安全中断概率随 a_2 变化的情况

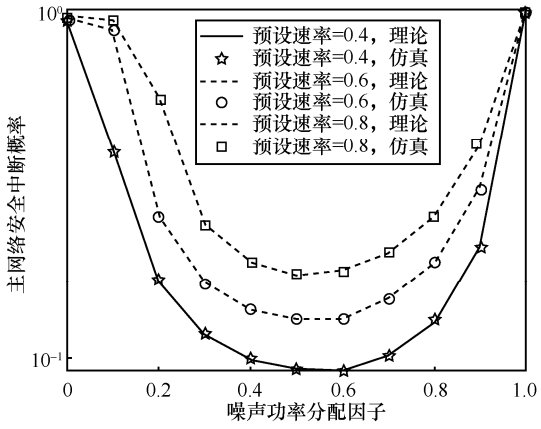
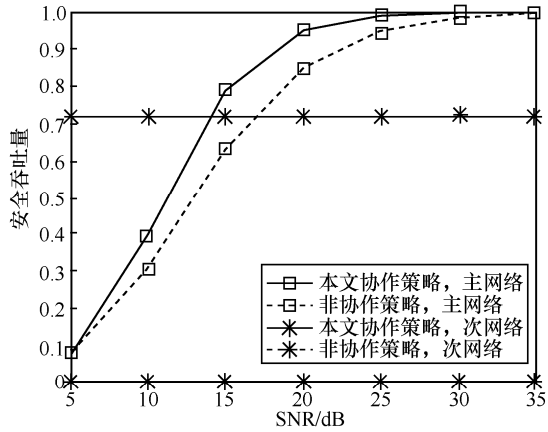
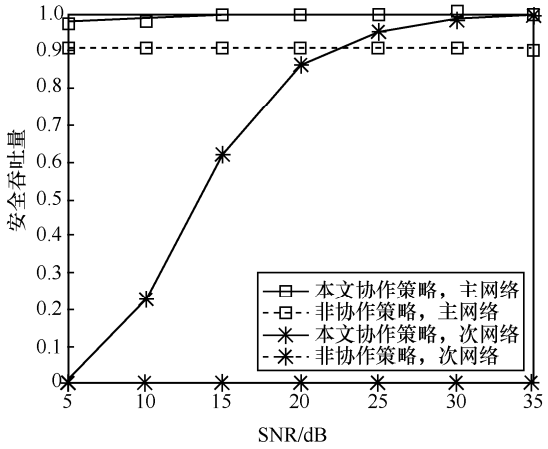


图 5 SN 安全中断概率随 b_3 变化的情况

当 ST 传输信噪比 $\rho_S = 20$ dB 时，PN 和 SN 的安全吞吐量随 PT 发射信噪比变化的曲线如图 6(a)所示。从图 6(a)中可以观察到，本文策略中主网络和次网络的安全吞吐量均高于对比策略，随着 ρ_P 的增加，主网络的吞吐量不断增加，次网络的吞吐量不变，与图 2 和图 3 的结果相呼应，进一步验证了本文策略的有效性。当 PT 传输信噪比 $\rho_P = 20$ dB 时，PN 和 SN 的安全吞吐量随 ST 发射信噪比变化的曲线如图 6(b)所示。从图 6(b)可以看出，本文协作策略中主网络和次网络的吞吐量均高于对比策略，说明了本文策略对系统安全性能的提升。随着 ρ_S 的增加，本文策略中 PN 的安全吞吐量小幅增加，SN 的安全吞吐量则有大幅上涨，这是因为改变 ST 的发射信噪比对 SN 的影响较大。此外，从图 6(a)和图 6(b)中均可以看出，本文策略中采用 CR 技术，使认知网络可以接入主网络频谱进行通信，有效地改善了认知网络的吞吐量，使频谱得到高效利用。



（a）ρ_S=20 dB 时安全吞吐量随PT发射信噪比变化的情况



（b）ρ_P=20 dB时安全吞吐量随ST发射信噪比变化的情况

图 6 安全吞吐量变化情况

5 结束语

本文研究了认知协作 NOMA 网络中的物理层安全问题；在提出的协作策略中，认知网络通过感知主网络频谱空穴进行辅助主用户信息传输和认知用户信息传输的动态切换，并与 NOMA 结合，实现了频谱复用。在主次网络中分别采用 AN 技术，进一步提高了主次网络的安全性能。对主次网络的安全中断概率和安全吞吐量分别进行分析，仿真结果表明，本文方案的系统安全性能有显著的提升，并且能有效地提高频谱利用率。

参考文献：

[1] DING Z, LIU Y, CHOI J, et al. Application of non-orthogonal multiple

access in LTE and 5G networks[J]. IEEE Communications Magazine, 2017, 55(2): 185-191.

[2] DING Z, ADACHI F, POOR H V. The application of MIMO to non-orthogonal multiple access[J]. IEEE Transactions on Wireless Communications, 2016, 15(1): 537-552.

[3] ISLAM S M R, AVAZOV N, DOBRE O A, et al. Power-domain non-orthogonal multiple access (NOMA) in 5G systems: potentials and challenges[J]. IEEE Communications Surveys & Tutorials, 2017, 19(2): 721-742.

[4] LIAU Q Y, LEOW C Y. Successive user relaying in cooperative NOMA System[J]. IEEE Wireless Communications Letters, 2019, 8(3): 921-924.

[5] BAE J, HAN Y. Joint power and time allocation for two-way cooperative NOMA[J]. IEEE Transactions Vehicle Technology, 2019, 68(12): 12443-12447.

[6] DING Z, DAI H, POOR H V. Relay selection for cooperative NOMA[J]. IEEE Wireless Communications Letters, 2016, 5(4): 416-419.

[7] LV L, CHEN J, NI Q, et al. Cognitive non-orthogonal multiple access with cooperative relaying: a new wireless frontier for 5G spectrum sharing[J]. IEEE Communications Magazine, 2018, 56(4): 188-195.

[8] 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.

[9] SUN Y, NG D W K, SCHOBER R. Resource allocation for MC-NOMA systems with cognitive relaying[C]// Proceedings IEEE Globecom Workshops. Piscataway: IEEE Press, 2017: 1-7.

[10] MOHAMMADI M, CHALISE B K, HAKIMI A, et al. Beamforming design and power allocation for full-duplex non-orthogonal multiple access cognitive relaying[J]. IEEE Transactions Communications, 2018, 66(12): 5952-5965.

[11] ZOU Y, ZHU J, WANG X, et al. A survey on wireless security: technical challenges, recent advances, and future trends[J]. Proceedings of the IEEE, 2016, 104(9): 1727-1765.

[12] SHARMA S, ROY S D，KUNDU S. Secrecy outage of a multi-relay cooperative communication network with accumulation of harvesting energy at relays[J]. IET Communications, 2019, 13(18): 2986-2995.

[13] LEI H, YANG Z, PARK K H, et al. Secrecy outage analysis for cooperative NOMA systems with relay selection schemes[J]. IEEE Transactions on Communications, 2019, 67(9): 6282-6298.

[14] CHEN J, YANG L, ALOUINI M S. Physical layer security for cooperative NOMA systems[J]. IEEE Transactions Vehicle Technology, 2018, 67(5): 4645-4649.

[15] ZHOU F, CHU Z, SUN H, et al. Artificial noise aided secure cognitive beamforming for cooperative MISO-NOMA using SWIPT[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(4): 918-931.

[16] XIANG Z, YANG W, CAI Y, et al. Physical layer security in cognitive radio inspired NOMA network[J]. IEEE Journal of Selected Topics in Signal Processing, 2019, 13(3): 700-714.

[17] HILDEBRAND E. Introduction to numerical analysis[M]. New York: Dover Publication, 1987.

[18] GRADSHTEYN I S, RYZHIK I M. Table of integral, series and products[M]. 7th ed. New York: Academic Press, 2007.

[作者简介]

杨震（1961− ），男，江苏苏州人，博士，南京邮电大学教授、博士生导师，主要研究方向为语音处理与现代语音通信、无线通信中的通信与信号处理技术。

朱梦瑶（1997− ），女，江苏泰兴人，南京邮电大学硕士生，主要研究方向为认知无线电和上行非正交多址接入技术。

冯友宏（1979− ），男，安徽池州人，博士，安徽师范大学副教授，主要研究方向为超可靠低时延通信、无人机通信、网络安全。