中继选择NOMA无线系统的物理层安全

罗延翠，李光球，叶明珠，高辉，张亚娟
（杭州电子科技大学，浙江 杭州 310018）

摘　要：针对解码转发协作非正交多址接入（non-orthogonal multiple access，NOMA）系统物理层安全（physical layer security，PLS）性能较差，以及在多窃听者场景下PLS性能恶化的问题，提出了一种采用修改转发（modify-and-forward，MF）协议的多中继选择NOMA无线系统PLS模型。利用高斯−切比雪夫正交定理推导了非合谋或合谋窃听场景下多中继选择MF-NOMA无线系统的安全中断概率和渐近安全中断概率的近似表达式。仿真结果验证了多中继选择MF-NOMA无线系统PLS性能分析的准确性。结果同时也表明中继数目越多或窃听者数目越少，多中继选择MF-NOMA无线系统的PLS性能越好；合谋窃听比非合谋窃听更不利于多中继MF-NOMA无线系统的安全传输。

关键词：非正交多址接入；修改转发；中继选择；物理层安全；安全中断概率
中图分类号：TN918.1
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2024077

Physical layer security of relay selection NOMA wireless systems

LUO Yancui, LI Guangqiu, YE Mingzhu, GAO Hui, ZHANG Yajuan
Hangzhou Dianzi University, Hangzhou 310018, China

Abstract: Aiming at poor performance of physical layer security (PLS) of decode-and-forward cooperative non-orthogonal multiple access (NOMA) systems and its performance deterioration in the presence of multi-eavesdropper, the PLS model of multi-relay selection NOMA wireless systems using modify-and-forward (MF) protocol was proposed. The approximate expressions of secrecy outage probability(SOP) and asymptotic SOP of multi-relay selection MF-NOMA wireless systems with non-colluding or colluding eavesdropping scenarios were derived by using Gauss-Chebyshev Quadrature theorem. The simulation results verify the accuracy of PLS performance analysis of the above MF-NOMA wireless systems. The results also indicate that the PLS performance of multi-relay selection MF-NOMA wireless systems will be improved when the number of relays increases or the number of eavesdroppers decreases, and that colluding eavesdropping is more detrimental to secure transmission of multi-relay MF-NOMA wireless systems than non-colluding eavesdropping.

Key words: non-orthogonal multiple access, modify-and-forward, relay selection, physical layer security, secrecy outage probability

收稿日期：2023−11−29；修回日期：2024−01−09

0　引言

非正交多址接入（non-orthogonal multiple access，NOMA）技术具有频谱效率高、支持大规模连接等优点，被视为未来无线网络中有前景的多址技术[1-2]。相较于正交多址接入技术，NOMA技术允许源节点在同一资源块同时为多个用户发送混合信号，然后采用串行干扰消除（successive interference cancellation，SIC）技术消除同道干扰，有效提高了频谱效率[3]。文献[4]推导了下行NOMA系统的和速率闭合表达式。文献[5]推导了多用户NOMA系统的可达容量闭合表达式。将协作技术与NOMA结合，可以改善其频谱效率和可靠性[6]。文献[7]推导了解码转发（decode-and-forward，DF）协作NOMA系统的可达平均速率闭合表达式。文献[8]推导了放大转发（amplify-and-forward，AF）协作NOMA系统的遍历和速率和中断概率近似表达式。文献[9]推导了最大化源到中继链路信噪比的部分中继选择（partial relay selection，PRS）协作NOMA系统的遍历容量和中断概率闭合表达式。文献[10]提出了一种可以改进协作NOMA系统中断概率的两阶段中继选择（two-stage relay selection，TRS）方案，其目的是在满足远端用户目标数据速率的条件下最大化近端用户的信道容量。

NOMA系统的无线广播特性使其面临着信息泄露的问题，物理层安全（physical layer security，PLS）可以利用物理介质固有的随机性，以及合法链路与窃听链路的差异性，保证信息的安全传输[11-12]，是NOMA系统安全性设计的一个重要选择。文献[13-17]研究了单窃听场景下NOMA系统的PLS性能。文献[13]推导了窃听者具有SIC或并行干扰消除（parallel interference cancellation，PIC）能力时，NOMA系统的安全中断概率（secrecy outage probability，SOP）闭合表达式。协作技术同样可以提高NOMA系统的安全性能[14]，文献[15]推导了AF或DF协作NOMA系统的SOP和渐近SOP闭合表达式。文献[16-17]推导了TRS协作NOMA系统的SOP和渐近SOP闭合表达式，结果表明，增加中继节点数量可以提升协作NOMA系统的安全性能。文献[18-20]进一步研究了协作NOMA系统中存在多个窃听者时的PLS性能。文献[18]推导了非合谋窃听场景下PRS协作NOMA系统的SOP近似表达式。文献[19]推导了合谋窃听场景下PRS协作NOMA系统的SOP近似表达式。文献[20]推导了非合谋或合谋窃听场景下TRS协作NOMA系统的SOP近似表达式。

针对DF协作系统PLS性能不理想的问题，文献[21]采用MF协议来增强协作系统的PLS性能，推导了单窃听者场景下MF协作系统的SOP闭合表达式。文献[22]进一步推导了合谋窃听场景下MF中继选择网络的SOP和渐近SOP闭合表达式，文献[23]采用发射天线选择技术，对其PLS性能进行了提升。文献[24]研究MF协议来改善协作NOMA系统的安全性能，推导其SOP和渐近SOP近似表达式，结果表明采用MF协议可以提升协作NOMA系统的PLS性能。

鉴于协作NOMA系统可以同时为多个用户提供服务，多个窃听者是其经常遇到的场景，文献[24]仅考虑单窃听者场景情况且信道衰落为小尺度衰落，然而在实际应用中还要同时考虑路径损耗；此外，中继选择可以改善MF协作系统的安全性能[23]，可以将其扩展至NOMA系统，为此，本文提出一种多窃听场景下多中继选择MF-NOMA无线系统的PLS模型，在中继节点处考虑了PRS和TRS两种中继选择方案，推导了非合谋或合谋窃听场景下多中继选择MF-NOMA无线系统的SOP和渐近SOP近似表达式，并进行了数值计算和仿真。

1 系统模型

考虑图1所示的非合谋或合谋窃听场景下多中继选择MF-NOMA无线系统的PLS模型，由基站S、K个半双工中继R_k、近端用户D_1、远端用户D_2以及M个被动窃听者E_m组成，所有节点均配备单根天线。假定：

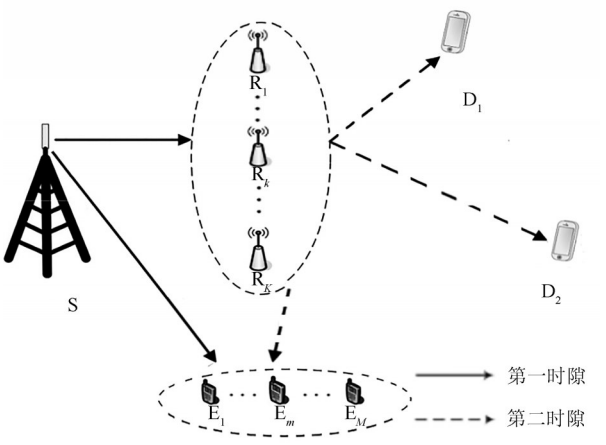


图1 多中继选择MF-NOMA无线系统PLS模型

（1）D_1和D_2与S之间没有直达链路，需要由R_k协助S向D_1和D_2发送保密信号；

（2）源节点的发射功率为P_{S}；K个中继节点的发射功率均为P_{R}，且均使用MF协议；

（3）R_k和D_1具有理想的SIC技术，D_2不具备SIC技术，E_m具有理想的PIC技术[24]；

（4）$\mathrm{X}\to\mathrm{Y}$链路具有理想的CSI，采用文献[9, 24]中的信道模型，信道衰落系数$h_{\mathrm{XY}}=\tilde{h}_{\mathrm{XY}}/\sqrt{d_{\mathrm{XY}}^{\alpha}}$，其中，$\tilde{h}_{\mathrm{XY}}$为X与Y间的链路增益，且服从独立复高斯分布$\mathrm{CN}(0,1)$，$d_{\mathrm{XY}}$为X与Y间的距离，$\alpha$为路径损耗系数，$\mathrm{XY}\in\{\mathrm{SR}_k,\mathrm{SE}_m,\mathrm{R}_k\mathrm{D}_1,\mathrm{R}_k\mathrm{D}_2,\mathrm{R}_k\mathrm{E}_m\}$。

（5）R_k、D_1、D_2和E_m接收天线上的加性高斯白噪声为n_{I}，$\mathrm{I}\in\{\mathrm{R}_k,\mathrm{D}_1,\mathrm{D}_2,\mathrm{E}_m\}$，$n_{\mathrm{I}}$服从$\mathrm{CN}(0,N_{\mathrm{I}})$分布。

整个传输过程分为两个时隙，第一时隙，S基于NOMA技术的原理，向R_k和E_m广播叠加信号$\sqrt{a_1P_{\mathrm{S}}}\,x_1+\sqrt{a_2P_{\mathrm{S}}}\,x_2$，$x_i$为S发送给$\mathrm{D}_i$的保密信号，$i=1,2$，$a_i$为功率分割因子，且$a_1<a_2$，$a_1+a_2=1$。第二时隙，被选择的$\mathrm{R}_k$使用文献[21]中的MF协议对解码后的信号进行修改，并采用NOMA技术将修改后的叠加信号$\sqrt{a_1P_{\mathrm{R}}}\,x_1'+\sqrt{a_2P_{\mathrm{R}}}\,x_2'$广播给$\mathrm{D}_i$和$\mathrm{E}_m$。

1.1 主信道

主信道由$\mathrm{S}\to\mathrm{R}_k$、$\mathrm{R}_k\to\mathrm{D}_1$和$\mathrm{R}_k\to\mathrm{D}_2$链路组成。在第一时隙中，$\mathrm{R}_k$处的接收信号为：

$$y_{\mathrm{SR}_k}=h_{\mathrm{SR}_k}\left(\sqrt{a_1P_{\mathrm{S}}}\,x_1+\sqrt{a_2P_{\mathrm{S}}}\,x_2\right)+n_{\mathrm{R}_k} \quad (1)$$

R_k的解码过程如下：R_k将x_1视为干扰信号，先解码x_2；之后采用SIC技术将x_2产生的干扰消除后，再解码x_1。

当R_k的安全容量大于D_i的目标安全速率δ_i时，R_k能够成功解码x_i。令$g_1(c_1,\rho,h)=c_1\rho|h|^2$，$g_2(c_1,c_2,\rho,h)=c_2\rho|h|^2/\left(c_1\rho|h|^2+1\right)$，则$\mathrm{R}_k$解码$x_1$、$x_2$的瞬时信干噪比（signal-to-interference-plus-noise ratio，SINR）分别为$\gamma_{\mathrm{R}_k\mathrm{D}_1}=g_1\left(a_1,\rho_{\mathrm{S}},h_{\mathrm{SR}_k}\right)$和$\gamma_{\mathrm{R}_k\mathrm{D}_2}=g_2\left(a_1,a_2,\rho_{\mathrm{S}},h_{\mathrm{SR}_k}\right)$，其中，$\rho_{\mathrm{S}}=P_{\mathrm{S}}/N_{\mathrm{R}}$，表示$\mathrm{S}\to\mathrm{R}_k$链路的平均信噪比（signal-to-noise ratio，SNR）。

在第二时隙中，D_i处的接收信号为：

$$y_{\mathrm{D}_i}=h_{\mathrm{R}_k\mathrm{D}_i}\left(\sqrt{a_1P_{\mathrm{R}}}\,x_1'+\sqrt{a_2P_{\mathrm{R}}}\,x_2'\right)+n_{\mathrm{D}_i} \quad (2)$$

同R_k的解码过程：D_1将x_1'视为干扰信号，先解码出x_2'，之后采用SIC技术解码出x_1'。D_1解码x_1'、x_2'的瞬时SINR为$\gamma_{\mathrm{D}_1}=g_1\left(a_1,\rho_{\mathrm{R}},h_{\mathrm{R}_k\mathrm{D}_1}\right)$和$\gamma_{\mathrm{D}_1\mathrm{D}_2}=g_2\left(a_1,a_2,\rho_{\mathrm{R}},h_{\mathrm{R}_k\mathrm{D}_1}\right)$，其中，$\rho_{\mathrm{R}}=P_{\mathrm{R}}/N_i$，表示$\mathrm{R}_k\to\mathrm{D}_i$链路的平均SNR。

D_2将x_1'视为干扰信号直接解码x_2'，解码x_2'的瞬时SINR为$\gamma_{\mathrm{D}_2}=g_2\left(a_1,a_2,\rho_{\mathrm{R}},h_{\mathrm{R}_k\mathrm{D}_2}\right)$。

1.2　非合谋窃听和合谋窃听

窃听信道由$S\to E_m$和$R_k\to E_m$链路构成。根据MF协议的工作原理，E_m只能窃听到第一时隙中S广播给R_k的叠加信号，此时E_m处的接收信号为：

$$y_{SE_m}=h_{SE_m}\left(\sqrt{a_1P_S}\,x_1+\sqrt{a_2P_S}\,x_2\right)+n_E \quad (3)$$

在非合谋窃听中，每个E_m独立解码接收信号，具有最大瞬时SINR的窃听者对MF-NOMA无线系统的PLS性能危害最大。非合谋窃听场景下窃听x_i的最大瞬时SINR为$\gamma_{ED_i}^{N}=a_i\rho_E\max\limits_{1\le m\le M}\left\{\left|h_{SE_m}\right|^2\right\}$，其中，$\rho_E=P_S/N_E$，表示$S\to E_m$链路的平均SNR。

为了使分析更简便，令$\gamma_E^N=\max\limits_{1\le m\le M}\rho_E\left|h_{SE_m}\right|^2$，根据文献[18]中的式（12）可得，$\gamma_E^N$的概率密度函数（probability density function，PDF）为：

$$f_{\gamma_E^N}(x)=\sum_{m=1}^{M}I_{m,M}\frac{md_{SE_m}^{\alpha}}{\rho_E}\exp\left(-\frac{md_{SE_m}^{\alpha}x}{\rho_E}\right) \quad (4)$$

其中，$I_{m,M}=\binom{M}{m}(-1)^{m-1}$。

对于合谋窃听，E_m之间可以共享接收信号，所有接收信号都可以由一个中心节点进行处理[20]，合谋窃听场景下窃听x_i的瞬时SINR为$\gamma_{ED_i}^{C}=a_i\rho_E\sum\limits_{m=1}^{M}\left|h_{SE_m}\right|^2$。

令$\gamma_E^C=\sum\limits_{m=1}^{M}\rho_E\left|h_{SE_m}\right|^2$，根据文献[23]的式（4）可得，$\gamma_E^C$的PDF为：

$$f_{\gamma_E^C}(x)=\frac{d_{SE_m}^{\alpha M}x^{M-1}}{\rho_E{}^{M}(M-1)!}\exp\left(-\frac{d_{SE_m}^{\alpha M}x}{a_i\rho_E}\right) \quad (5)$$

2　安全性能分析

在图1的多中继MF-NOMA无线系统中，由于D_1的信道容量受限于$S\to R_k$和$R_k\to D_1$链路中的最小SINR，所以D_1的安全容量为：

$$C_1=\frac{1}{2}\left[\mathrm{lb}\left(\frac{1+\min\left(\gamma_{R_kD_1},\gamma_{D_1}\right)}{1+\gamma_{ED_1}}\right)\right]^{+} \quad (6)$$

其中，$[x]^{+}=\max\{0,x\}$。

同理，由于D_2的信道容量受限于$S\to R_k$、$R_k\to D_2$和$R_k\to D_1$链路中的最小SINR，所以D_2的安全容量为：

$$C_2=\frac{1}{2}\left[\mathrm{lb}\left(\frac{1+\min\left(\gamma_{R_kD_2},\gamma_{D_2},\gamma_{D_1D_2}\right)}{1+\gamma_{ED_2}}\right)\right]^{+} \quad (7)$$

下文分别分析了基于PRS和TRS的MF-NOMA系统的安全性能。

2.1　PRS方案的安全性能分析

PRS方案选择使$S\to R_k$链路瞬时SINR最大的中继来转发信号，所选最优中继为[18]：

$$R_{k^*}=\underset{1\le k\le K}{\mathrm{argmax}}\left\{\left|h_{SR_k}\right|^2\right\} \quad (8)$$

此时，图1所示系统简称PRS-MF-NOMA系统。

2.1.1　安全中断概率

PRS-MF-NOMA系统的SOP可以定义为在D_1和D_2中，至少有一个用户其安全容量C_i小于其目标安全速率δ_i的概率，即[18]：

$$\begin{aligned}P_{PRS}&=\Pr\left(C_1<\delta_1\ \text{或}\ C_2<\delta_2\right)=\\&1-\Pr\left(\frac{1+\gamma_1}{1+\gamma_{ED_1}}>\varepsilon_1,\frac{1+\gamma_2}{1+\gamma_{ED_2}}>\varepsilon_2\right)\end{aligned} \quad (9)$$

其中，$\gamma_1=\min\left(\gamma_{R_kD_1},\gamma_{D_1}\right)$，$\gamma_2=\min\left(\gamma_{R_kD_2},\gamma_{D_2},\gamma_{D_1D_2}\right)$，$\varepsilon_1=2^{2\delta_1}$，$\varepsilon_2=2^{2\delta_2}$，$\Pr(\cdot)$表示概率。由于式（9）中$\gamma_i$、$\gamma_{ED_i}$是相关的，难以获得$P_{PRS}$的精确表达式，因此，本文着重分析高SNR区域，可以得到γ_2的上界：$\gamma_{R_kD_2}\approx\gamma_{D_2}\approx\gamma_{D_1D_2}\approx a_2/a_1$，$P_{PRS}$可以表示为：

$$\begin{aligned}P_{PRS}&=1-\Pr\left(\gamma_1>\varepsilon_1\left(1+a_1\gamma_E\right)-1,\gamma_E<\tau\right)=\\&1-\int_0^{\tau}f_{\gamma_E}(x)\left(1-F_{\gamma_1}^{PRS}\left(\varepsilon_1a_1x+z_1\right)\right)\mathrm{d}x\end{aligned} \quad (10)$$

其中，$\gamma_E \in \left\{\gamma_E^N, \gamma_E^C\right\}$，$z_1=\varepsilon_1-1$，$\tau=(1-\varepsilon_2 a_1)/(\varepsilon_2 a_1 a_2)$。由于$\tau>0$，则$a_1<1/\varepsilon_2$，若$a_1>1/\varepsilon_2$，则SOP为1。

由$h_{SR_{k^*}}$和$h_{R_kD_1}$均服从CN(0,1)分布可得，PRS方案下γ_1的累积分布函数（cumulative distribution function，CDF）为：

$$F_{\gamma_1}^{PRS}(x)=1-\Pr\left(\left|h_{SR_{k^*}}\right|^2>\frac{x}{a_1\rho_S}\right)$$

$$\Pr\left(\left|h_{R_kD_1}\right|^2>\frac{x}{a_1\rho_R}\right)=1-\sum_{k=1}^{K} I_{k,K}\exp(-w_1 x/a_1) \tag{11}$$

其中，$I_{k,K}=\binom{K}{k}(-1)^{k-1}$，$w_1=\left(kd_{SR_k}^{\alpha}\rho_R+d_{R_kD_1}^{\alpha}\rho_S\right)/(\rho_S\rho_R)$。

将式（4）和式（11）代入式（10），同时利用文献[25]的（3.381.1）可得非合谋窃听场景下PRS-MF-NOMA系统的SOP为：

$$P_{PRS}^{N}=1-\sum_{k=1}^{K}\sum_{m=1}^{M} I_{k,K}I_{m,M}\frac{w_2 e^{-w_1 z_1/a_1}}{w_1\varepsilon_1+w_2}\left(1-e^{-(w_1\varepsilon_1+w_2)\tau}\right) \tag{12}$$

其中，$w_2=md_{SE_m}^{\alpha}/\rho_E$。

同理，将式（5）和式（11）代入式（10），同时利用文献[25]的（3.381.1）可得合谋窃听场景下PRS-MF-NOMA系统的SOP为：

$$P_{PRS}^{C}=1-\sum_{k=1}^{K}\frac{I_{k,K}w_3^{M}e^{-w_1 z_1/a_1}}{(w_1\varepsilon_1+w_3)^{M}v!}\gamma\left(M,(w_1\varepsilon_1+w_3)\tau\right) \tag{13}$$

其中，$w_3=d_{SE_m}^{\alpha}/\rho_E$，$v=M-1$，$\gamma(\cdot)$为下不完全伽马函数。

根据式（12）和式（13）可以得定理1。

定理1 非合谋窃听和合谋窃听场景下PRS-MF-NOMA系统的SOP均与中继数K、窃听者数M、合法链路平均信噪比ρ_S和ρ_R、窃听链路平均信噪比ρ_E、基站和中继的功率分割因子a_1、距离d_{XY}和目标安全速率δ_1和δ_2等参数有关。

当窃听者数M为1，中继数K为1，且不考虑路径损耗系数（可令$\alpha=0$）时，图1的多窃听多中继选择MF-NOMA系统退变为文献[24]中的MF-NOMA系统，式（12）和式（13）可退变为文献[24]中的式（10），可见，本文的结果更具一般性。

2.1.2 渐近安全中断概率

为了对PRS-MF-NOMA系统有更深入的见解，分析了PRS-MF-NOMA系统当$\rho_S\to\infty$，$\rho_{R_k}\to\infty$时的渐近SOP，具体表达式如下。

当$\rho_S\to\infty$、$\rho_{R_k}\to\infty$时，$\gamma_1\to\infty$，两种窃听场景下的渐近SOP由D_2决定，因此系统在非合谋窃听和合谋窃听场景下的渐近SOP分别为：

$$P_{PRS,\infty}^{N}=\sum_{k=1}^{K}\sum_{m=1}^{M} I_{k,K}I_{m,M}\exp(-w_2\tau) \tag{14}$$

和

$$P_{PRS,\infty}^{C}=1-\sum_{k=1}^{K} I_{k,K}\frac{\gamma(M,w_3\tau)}{v!} \tag{15}$$

根据式（14）和式（15）可得定理2。

定理2 PRS-MF-NOMA系统的安全分集增益为0，且存在一个由窃听者数M、窃听链路平均信噪比ρ_E、基站和中继的功率分割因子a_1和远端用户的目标安全速率δ_2等参数决定的安全性能平台。

2.2 TRS方案的安全性能分析

同参考文献[20]，假设可以获得所有合法链路和窃听链路的CSI，可以采用TRS提高协作NOMA系统的安全性能。TRS策略的主要目标是在满足远端用户D_2的目标安全速率δ_2的情况下，尽可能地最大化近端用户D_1的可达安全速率。TRS策略为：（1）建立一个满足D_2目标安全速率δ_2的中继集合；（2）在集合中选择一个使D_1的可达安全速率最大化的中继。

第一阶段，先建立一个满足以下条件的中继集合S_R：

$$S_{\mathrm{R}}=\left\{\frac{1+\gamma_1}{1+\gamma_{\mathrm{ED}_2}}\geqslant\varepsilon_2,1\leqslant k\leqslant K\right\}\tag{16}$$

第二阶段，在S_{R}中选择一个最优中继，所选中继为：

$$\mathrm{R}_{k^*}=\underset{k}{\operatorname{argmax}}\left\{\frac{1+\gamma_1}{1+\gamma_{\mathrm{ED}_1}},k\in S_{\mathrm{R}}\right\}\tag{17}$$

此时，图1所示系统简记为TRS-MF-NOMA系统。

2.2.1　安全中断概率

在TRS中，整个系统发生中断有两种互不相容的事件：（1）事件o_1定义为S_R为空集，即所有中继均使D_2的安全容量小于其目标安全速率δ_2；（2）事件o_2定义为S_R不为空集，但所选的最优中继无法保证D_1的安全容量大于其目标安全速率δ_1，因此TRS-MF-NOMA系统的SOP为[20]：

$$P_{\mathrm{TRS}}=\Pr(\mathrm{o}_1)+\Pr(\mathrm{o}_2)\tag{18}$$

基于事件o_1的描述，$\Pr(\mathrm{o}_1)$用计算式可以表示为：

$$\Pr(\mathrm{o}_1)=\Pr(|S_{\mathrm{R}}|=0)=\Pr\left(\max_{k\in K}\left\{\frac{1+\gamma_2}{1+\gamma_{\mathrm{ED}_2}}\right\}<\varepsilon_1\right)=\prod_{k=1}^{K}P_2^{\mathrm{TRS}}\tag{19}$$

其中，$|S_{\mathrm{R}}|$表示候选集S_{R}的大小，$P_2^{\mathrm{TRS}}=\Pr\left((1+\gamma_2)/\left(1+\gamma_{\mathrm{ED}_2}\right)<\varepsilon_1\right)$。

P_2^{TRS}可以表示为[17]：

$$P_2^{\mathrm{TRS}}=\int_0^{\infty}f_{\gamma_{\mathrm{E}}}(x)F_{\gamma_2}(\varepsilon_2a_2x+z_2)\,\mathrm{d}x\tag{20}$$

其中，$z_2=\varepsilon_2-1$。由于h_{SR_k}、$h_{\mathrm{R}_k\mathrm{D}_1}$和$h_{\mathrm{R}_k\mathrm{D}_2}$均服从$\mathrm{CN}(0,1)$分布，因此$\gamma_2$的CDF为：

$$F_{\gamma_2}^{\mathrm{TRS}}(x)=\begin{cases}1-\exp\left(-\dfrac{w_4x}{a_2-a_1x}\right),x\leqslant a_2/a_1\\1,x>a_2/a_1\end{cases}\tag{21}$$

其中，$w_4=\left(d_{\mathrm{SR}_k}^{\alpha}\rho_{\mathrm{R}}+d_{\mathrm{R}_k\mathrm{D}_1}^{\alpha}\rho_{\mathrm{S}}+d_{\mathrm{R}_k\mathrm{D}_2}^{\alpha}\rho_{\mathrm{S}}\right)/\left(\rho_{\mathrm{S}}\rho_{\mathrm{R}}\right)$。

将式（4）和式（21）代入式（20）可得非合谋窃听场景下P_2^{TRS}为：

$$P_2^{\mathrm{TRS,N}}=1-\sum_{m=1}^{M}I_{m,M}\int_0^{\tau}w_2\exp\left(-\frac{w_4(\varepsilon_2a_2x+z_2)}{a_2-a_1(\varepsilon_2a_2x+z_2)}-w_2x\right)\mathrm{d}x\tag{22}$$

为了求得式（22），令：

$$\varphi(b_1,b_2,b_3,b_4)=\int_0^{\tau}b_1x^{b_2}\exp\left(-\frac{b_3(\varepsilon_2a_2x+z_2)}{a_2-a_1(\varepsilon_2a_2x+z_2)}-b_4x\right)\mathrm{d}x\tag{23}$$

由于式（23）的精确值难以获得，采用文献[26]中的高斯−切比雪夫正交定理（25.4.38）可以得到它的近似值为：

$$\varphi(b_1,b_2,b_3,b_4)\approx\frac{\tau\pi b_1}{2N}\sum_{n=0}^{N}\theta_n{s_n}^{b_2}\cdot\exp\left(-\frac{b_3(\varepsilon_2a_2s_n+z_2)}{a_2-a_1(\varepsilon_2a_2s_n+z_2)}-b_4s_n\right)\tag{24}$$

其中，$s_n=\tau(x_n+1)/2$，$x_n=\cos\left((2n-1)\pi/(2N)\right)$，$\theta_n=\sqrt{1-{x_n}^2}$。

结合式（22）、式（23）和式（24）可得非合谋窃听场景下$P_2^{\mathrm{TRS},N}$为：

$$P_2^{\mathrm{TRS},N}=1-\sum_{m=1}^{M}I_{m,M}\varphi(w_2,0,w_4,w_2)\tag{25}$$

同理，结合式（5）、式（20）、式（21）、式（23）和式（24）可得合谋窃听场景下$P_2^{\mathrm{TRS,C}}$为：

$$P_2^{\mathrm{TRS,C}}=1-\varphi\left(\frac{w_3^M}{v!},v,w_4,w_3\right)\tag{26}$$

根据第二阶段选择方案的描述，$\Pr(\mathrm{o}_2)$用计算式可以表示为：

$$\Pr(\mathrm{o}_2)=\Pr\left(\frac{1+\gamma_{k^*}}{1+\gamma_{\mathrm{ED}_1}}<\varepsilon_1,|S_{\mathrm{R}}|>0\right)=\sum_{k=1}^{K}\Pr\left(\frac{1+\gamma_{k^*}}{1+\gamma_{\mathrm{ED}_1}}<\varepsilon_1\middle||S_{\mathrm{R}}|=k\right)\Pr(|S_{\mathrm{R}}|=k)=\sum_{k=1}^{K}\binom{K}{k}\left(1-P_2^{\mathrm{TRS}}-\mathrm{J}\right)^k\left(P_2^{\mathrm{TRS}}\right)^{K-k}\tag{27}$$

其中，$\gamma_{k^*}=\max\left(\gamma_1,\forall k\in S_{\mathrm{R}}\right)$，$J=\Pr\left(\frac{1+\gamma_1}{1+\gamma_{\mathrm{ED}_1}}>\varepsilon_1,\frac{1+\gamma_2}{1+\gamma_{\mathrm{ED}_2}}>\varepsilon_2\right)$。

与式（9）同理，由于γ_i、γ_{ED_i}是相关的，重点分析高SNR区域，J可以表示为：

$$J=\int_0^{\tau}f_{\gamma_{\mathrm{E}}}(x)\left(1-F_{\gamma_1}^{\mathrm{TRS}}\left(\varepsilon_1a_1x+z_1\right)\right)\mathrm{d}x \quad (28)$$

为了得到式（28）的闭合表达式，需要先得到TRS下γ_1的CDF，由于h_{SR_k}和$h_{\mathrm{R}_k\mathrm{D}_1}$均服从$\mathrm{CN}(0,1)$分布，因此$\gamma_1$的CDF为：

$$F_{\gamma_1}^{\mathrm{TRS}}(x)=1-\exp\left(-\frac{w_5x}{a_1}\right) \quad (29)$$

其中，$w_5=\left(d_{\mathrm{SR}_k}^{\alpha}\rho_{\mathrm{R}}+d_{\mathrm{R}_k\mathrm{D}_1}^{\alpha}\rho_{\mathrm{S}}\right)/\left(\rho_{\mathrm{S}}\rho_{\mathrm{R}}\right)$。

将式（4）和式（29）代入式（28）可得非合谋窃听场景下J_{N}为：

$$J_{\mathrm{N}}=\sum_{m=1}^{M}\frac{I_{m,M}w_2\mathrm{e}^{-w_5z_1/a_1}}{w_2+\varepsilon_1w_5}\left(1-\mathrm{e}^{-\left(w_5\varepsilon_1+w_2\right)\tau}\right) \quad (30)$$

将式（5）和式（29）代入式（28）可得合谋窃听场景下J_{C}为：

$$J_{\mathrm{C}}=\frac{{w_3}^{M}\mathrm{e}^{-w_5z_1/a_1}}{\left(w_5\varepsilon_1+w_3\right)^{M}v!}\gamma\left(M,\left(w_5\varepsilon_1+w_3\right)\tau\right) \quad (31)$$

分别将式（25）代入式（19），式（25）和式（30）代入式（27）可以得到$\Pr(\mathrm{o}_1)$和$\Pr(\mathrm{o}_2)$的近似表达式，再将$\Pr(\mathrm{o}_1)$和$\Pr(\mathrm{o}_2)$的近似表达式代入式（18）可得非合谋窃听场景下TRS-MF-NOMA系统的SOP为：

$$P_{\mathrm{TRS}}^{\mathrm{N}}=\sum_{k=0}^{K}\binom{K}{k}\left(\sum_{m=1}^{M}I_{m,M}\left(\varphi\left(w_2,0,w_4,w_2\right)-\frac{w_2\left(1-\mathrm{e}^{-\left(w_5\varepsilon_1+w_2\right)\tau}\right)}{w_2+\varepsilon_1w_5}\mathrm{e}^{-\frac{w_5z_1}{a_1}}\right)\right)^{k}\times\left(1-\sum_{m=1}^{M}I_{m,M}\varphi\left(w_2,0,w_4,w_2\right)\right)^{K-k} \quad (32)$$

结合式（18）、式（19）、式（26）、式（27）和式（31）可得合谋窃听场景下TRS-MF-NOMA系统的SOP为：

$$P_{\mathrm{TRS}}^{\mathrm{C}}=\sum_{k=0}^{K}\binom{K}{k}\left(\varphi\left(\frac{w_3^{M}}{v!},v,w_4,w_3\right)-\frac{{w_3}^{M}\gamma\left(M,\left(w_5\varepsilon_1+w_3\right)\tau\right)}{\left(w_5\varepsilon_1+w_3\right)^{M}!}\mathrm{e}^{-\frac{w_5z_1}{a_1}}\right)^{k}\times\left(1-\varphi\left(\frac{w_3^{M}}{v!},v,w_4,w_3\right)\right)^{K-k} \quad (33)$$

根据式（32）和式（33）可得定理3。

定理3 TRS-MF-NOMA系统在非合谋窃听和合谋窃听场景下的SOP均与中继数K、窃听者数M、合法链路平均信噪比ρ_{S}和ρ_R、窃听链路平均信噪比ρ_{E}、基站和中继的功率分割因子a_1、距离d_{XY}和目标安全速率δ_1、δ_2等参数有关。当$a_1>1/\varepsilon_2$或$a_2<a_1\left(\varepsilon_2\rho_{\mathrm{E}}+z_2\right)$时，SOP为1。

此外，当窃听者数M为1，中继数K为1，且不考虑路径损耗系数（可令$\alpha=0$）时，式（32）和式（33）可退变为文献[24]中的式（10），可见，本文的结果更具一般性。

2.2.2 渐近安全中断概率

同PRS策略，当$\rho_{\mathrm{S}}\to\infty$，$\rho_{\mathrm{R}_k}\to\infty$时，$\gamma_1\to\infty$，即$\Pr(\mathrm{o}_2)\to0$，TRS的渐近SOP由$\Pr(\mathrm{o}_1)$决定，因此，TRS-MF-NOMA系统在非合谋窃听和合谋窃听场景下的渐近SOP分别为：

$$P_{\mathrm{TRS},\infty}^{\mathrm{NC}}=\left(\sum_{m=1}^{M}\binom{M}{m}(-1)^{m-1}\exp\left(-w_2\tau\right)\right)^{K} \quad (34)$$

和

$$P_{\mathrm{TRS},\infty}^{\mathrm{C}}=\left(1-\frac{\gamma\left(M,w_4\tau\right)}{v!}\right)^{K} \quad (35)$$

根据式（34）和式（35）可以得到定理4。

定理4 TRS-MF-NOMA系统的安全分集增

益为0，改变窃听者天线数M、窃听链路平均信噪比ρ_{E}、基站和中继的功率分割因子a_1和远端用户的目标安全速率δ_2等参数会影响系统的安全性能。

3　数值计算与仿真

下面通过蒙特卡洛仿真验证多中继选择MF-NOMA无线系统的SOP和渐近SOP性能分析的准确性，每个蒙特卡洛仿真进行了10^5次独立实验。在部分中继选择方案或两阶段中继选择方案下，研究中继数目K、窃听者数目M、合法链路平均信噪比ρ_{S}和ρ_{R}、窃听链路平均信噪比ρ_{E}和功率分割因子a_1等参数的变化对多中继选择MF-NOMA无线系统的影响。若无特别说明，图2~图6的参数设置参考文献[9，24]，对链路间的距离进行归一化，其中，$d_{\mathrm{SD}_2}=1$，$d_{\mathrm{R}_k\mathrm{D}_1}<d_{\mathrm{R}_k\mathrm{D}_2}$，发射功率$P_{\mathrm{S}}=P_{\mathrm{R}}$，噪声功率$N_I=1$，则$\rho=\rho_{\mathrm{S}}=\rho_{\mathrm{R}}$，其他参数设置见表1。

不同远端用户目标安全速率δ_2时多中继选择MF-NOMA无线系统在非合谋或合谋窃听场景下的安全中断概率性能曲线如图2所示，由图2可以得出以下结论。

（1）在两种窃听场景下，随着ρ_{S}的增大，系统的SOP均减小，这是因为ρ_{S}的增大使系统的安全容量增大，提升了系统的安全性能。

（2）在高SNR区域，SOP趋于一个稳定值，这是因为NOMA协议中的功率分割因子a_2/a_1限制了D_2的可达数据速率，而E_m具有PIC能力，其可达数据速率不受功率分割因子的影响。

（3）SOP随着δ_2的增大而增大，比如，当$\rho=10$ dB时，δ_2从0.1增加到0.2，PRS-MF-NOMA系统在非合谋窃听场景下SOP从0.013恶化到0.27，合谋窃听场景下SOP从0.029恶化到0.066；TRS-MF-NOMA系统在非合谋窃听场景下SOP从6×10^{-4}恶化到10^{-3}，合谋窃听场景下SOP从1.2×10^{-3}恶化到2.8×10^{-3}，这是因为δ_2的增大使D_2的安全容量大于δ_2的概率降低，所以D_2的SOP增大，系统的SOP也随之增大。

（4）在PRS方案和TRS方案中，MF-NOMA系统的渐近SOP曲线与SOP仿真结果在高SNR下能很好的逼近；同时，当K=1，M=1，不考虑路径损耗的影响（即令$\alpha=0$）时，图2中的相应曲线与文献[24]中图2的相应曲线吻合，以上都验证了本文数值计算结果的准确性。

不同窃听节点数M时的多中继选择MF-NOMA无线系统在非合谋或合谋窃听场景下的安全中断概率性能曲线如图3所示，由图3可以得出以下结论。

（1）随着窃听节点数M的增大，系统的SOP均增大，当$\rho=10$ dB，M从2增加到3时，PRS-

表1　多中继选择MF-NOMA无线系统的仿真参数

参数名称	符号表示	参数值	参数说明
功率分割因子	a_1、a_2	0.3、0.7	图2~图3、图5~图6
中继节点数	K	3	图2~图5
窃听节点数	M	2	图2、图4~图6
窃听链路平均信噪比/dB	ρ_{E}	0	图2~图5
路径损耗系数	α	4	图2~图5
目标安全速率/(bit·(s·Hz)$^{-1}$)	δ_1、δ_2	1、0.2	图3~图6
S与R_k间的距离	d_{SR_k}	0.5	图2~图4、图6
R_k与D_i间的距离	$d_{\mathrm{R}_k\mathrm{D}_1}$、$d_{\mathrm{R}_k\mathrm{D}_2}$	0.25、0.5	图2~图6
S与E_m间的距离	d_{SE_m}	1.2	图2~图6
高斯-切比雪夫项数	N	100	图2~图6

MF-NOMA 系统在非合谋窃听场景下SOP由0.027恶化到0.037，合谋窃听场景下SOP从0.065恶化到0.18；TRS-MF-NOMA系统在非合谋窃听场景下SOP从10^{-3}恶化到1.5×10^{-3}，合谋窃听场景下SOP从3×10^{-3}恶化到1.5×10^{-2}。这是因为窃听节点越多，窃听到保密信号的可能性越大，相当于增大了窃听信道的容量，降低了系统的安全容量，使系统的SOP减小。

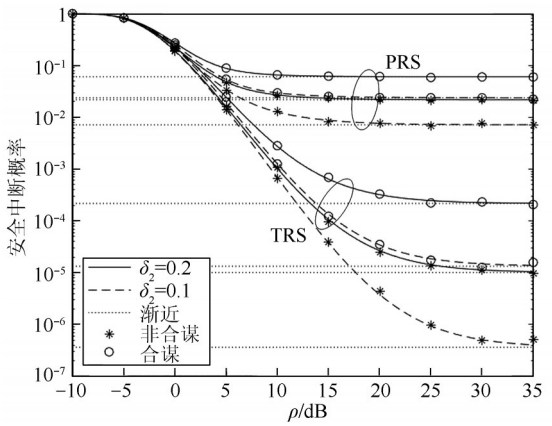


图2　不同δ_2时多中继选择MF-NOMA无线系统的SOP性能曲线

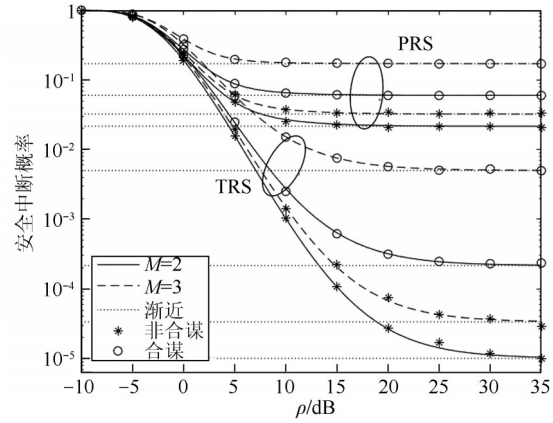


图3　不同M时多中继MF-NOMA无线系统的SOP性能曲线

（2）合谋窃听对系统的安全性能影响更大，增大窃听节点数M，系统在合谋窃听场景下的SOP急剧下降，这是因为在非合谋窃听情景下，窃听SINR取决于具有最大瞬时SINR的单个窃听者，而在合谋窃听场景下，窃听SINR取决于M个窃听者解码x_i的瞬时SINR之和，相当于增大了窃听信道的容量，降低了系统的安全容量，所以系统的SOP增大。

不同功率分割因子a_1时多中继选择MF-NOMA无线系统在非合谋或合谋窃听场景下的安全中断概率性能曲线如图4所示，其中$\rho=10$ dB，由图4可以看出，PRS-MF-NOMA系统在非合谋场景下的最优功率分割因子$a_1^*\approx0.19$；在合谋窃听场景下$a_1^*\approx0.17$。TRS-MF-NOMA系统在非合谋场景下的最优功率分割因子$a_1^*\approx0.22$；在合谋窃听场景下$a_1^*\approx0.27$。当$a_1<a_1^*$时，系统SOP随着a_1的增大而减小，$a_1>a_1^*$时，系统SOP随着a_1的增大而增大，这是因为在$a_1<a_1^*$时，随着a_1的增大，D_1成功解码x_1的概率增大，$a_1=a_1^*$时，系统SOP达到最小值；之后随着a_1的继续增大，分配给D_2的功率减小，使D_2的安全信息传输无法得到保证，因此系统的安全容量降低，SOP增大。

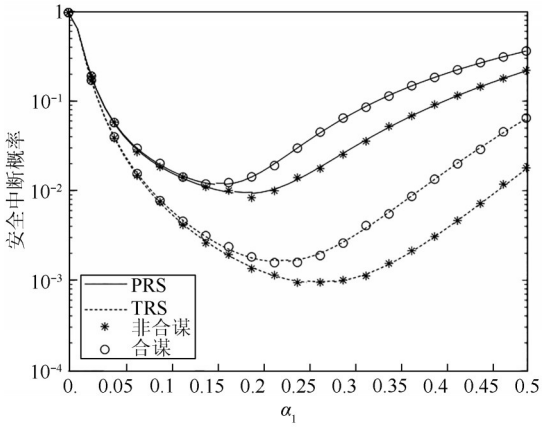


图4　不同a_1时多中继选择MF-NOMA无线系统的SOP性能曲线

不同距离d_{SR_k}时多中继选择MF-NOMA无线系统在非合谋或合谋窃听场景下的安全中断概率性能曲线如图5所示，由图5可知，改变基站与中继之间的距离，会影响系统的安全性能，d_{SR_k}增大使两种中继选择方案下系统的SOP均增大，这是因为d_{SR_k}的增大减小了合法用户的SINR，从而降低了系统的安全容量。此外，高SNR时，

d_{SR_k}的改变将不再影响系统的安全性能。

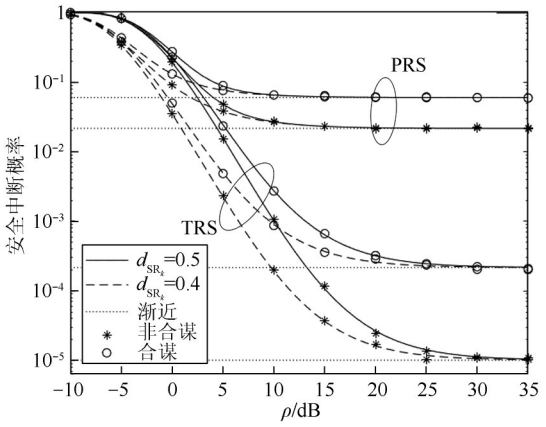


图5　不同距离时多中继选择MF-NOMA无线系统的SOP性能曲线

不同中继节点数K、窃听链路平均信噪比ρ_{E}时单窃听多中继选择MF-NOMA无线系统的安全中断概率性能曲线如图6所示。

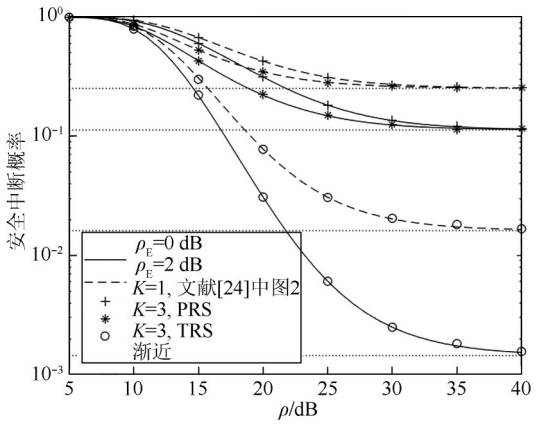


图6　不同K、ρ_{E}时多中继选择MF-NOMA无线系统的SOP性能曲线

（1）增大中继数目K，系统的安全中断概率降低，这是因为系统采用中继选择，可以增大合法链路的信道容量，提高系统的安全性能。此外，随着ρ的增大，系统采用PRS方案的SOP在$K=3$时，与$K=1$时趋于相等，说明PRS方案所带来的增益受限，而系统采用TRS方案，$K=3$时的SOP一直优于$K=1$时的SOP。

（2）随着ρ_{E}增大，系统的SOP增加，当$\rho=25$ dB，ρ_{E}从0 dB增大到2 dB，$K=1$时，MF-NOMA系统的SOP从0.18恶化到0.31；$K=3$时，PRS-MF-NOMA系统的SOP从0.15恶化到0.28，TRS-MF-NOMA系统在非合谋窃听场景下SOP从6×10^{-3}恶化到0.031，这是因为ρ_{E}的增加使窃听信道的容量增大，相当于降低了D_1和D_2的安全容量，从而使多中继MF-NOMA无线系统的安全性能降低，SOP增大。

4　结束语

本文在非合谋或合谋窃听场景下，分别研究了采用部分中继选择和两阶段中继选择来提升MF-NOMA系统的物理层安全性能，推导了多中继选择MF-NOMA系统的安全中断概率和渐近安全中断概率的近似表达式。数值计算和仿真结果表明，增加中继节点，可以提升MF-NOMA系统的物理层安全性能；当发射功率保持恒定时，分配给远用户的功率越大，多中继选择MF-NOMA系统的物理层安全性能越好；窃听者数目增多，会使MF-NOMA系统的物理层安全性能下降；合谋窃听比非合谋窃听更不利于MF-NOMA系统的安全传输。此外，本文仅研究了多中继选择MF-NOAM系统的PLS性能，后续可以进一步对多中继选择MF-NOMA系统的安全性能进行优化研究。

参考文献：

[1] DAI L L, WANG B C, YUAN Y F, et al. Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends[J]. IEEE Communications Magazine, 2015, 53(9): 74-81.

[2] DAI L L, WANG B C, DING Z G, et al. A survey of non-orthogonal multiple access for 5G[J]. IEEE Communications Surveys & Tutorials, 2018, 20(3): 2294-2323.

[3] YANG Q, WANG H M, NG D W K, et al. NOMA in downlink sdma with limited feedback: performance analysis and optimization[J]. IEEE Journal on Selected Areas in Communications, 2017, 35(10): 2281-2294.

[4] ABU MAHADY I, BEDEER E, IKKI S, et al. Sum-rate maxi-

mization of NOMA systems under imperfect successive interference cancellation[J]. IEEE Communications Letters, 2019, 23(3): 474-477.

[5] MAGABLEH A, ALDALAGAMOUNI T, MUHAIDAT S, et al. Capacity analysis of non-orthogonal multiple access systems over N-Nakagami fading channels for 5G and beyond[C]//2020 7th International Conference on Electrical and Electronics Engineering (ICEEE). 2020: 232-236.

[6] IBRAHIM A S, SADEK A K, SU W, et al. Cooperative communications with relay-selection: when to cooperate and whom to cooperate with?[J]. IEEE Transactions on Wireless Communications, 2008, 7(7): 2814-2827.

[7] KIM J B, LEE I H. Capacity analysis of cooperative relaying systems using non-orthogonal multiple access[J]. IEEE Communications Letters, 2015, 19(11): 1949-1952.

[8] ABBASI O, EBRAHIMI A, MOKARI N. NOMA inspired cooperative relaying system using an AF relay[J]. IEEE Wireless Communications Letters, 2019, 8(1): 261-264.

[9] TREGANCINI A, OLIVO E E B, OSORIO D P M, et al. Performance analysis of full-duplex relay-aided NOMA systems using partial relay selection[J]. IEEE Transactions on Vehicular Technology, 2020, 69(1): 622-635.

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

[11] SHIM K, NGUYEN T V, AN B. Exploiting opportunistic scheduling schemes to improve physical-layer security in MU-MISO NOMA systems[J]. IEEE Access, 2019(7): 180867-180886.

[12] WANG D, BAI B, ZHAO W, et al. A survey of optimization approaches for wireless physical layer security[J]. IEEE Communications Surveys & Tutorials, 2019, 21(2): 1878-1911.

[13] HUU T P, THI-THANH T N, NGUYEN-YEN C, et al. Secrecy outage probability and fairness of packet transmission time in a NOMA system[J]. IEEE Access, 2020(8): 79637-79649.

[14] 张继荣, 刘玉. 存在窃听者的协作中继NOMA系统安全性能分析[J]. 西安邮电大学学报, 2023, 28(2): 19-28
ZHANG J R, LIU Y. Security performance analysis of NOMA cooperative relay system with the presence of eavesdropper[J]. Journal of Xi 'an University of Post and Telecommunications, 2023, 28(2): 19-28.

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

[16] LI A. Enhancing the physical layer security of cooperative NOMA system[C]//2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). Piscataway: IEEE Press, 2019: 2194-2198.

[17] LI H, CHEN Y P, ZHU M F, et al. Secrecy outage probability of relay selection based cooperative NOMA for IoT networks[J]. IEEE Access, 2021(9): 1655-1665.

[18] HOANG T M, DUNG L T, NGUYEN B C, et al. Secrecy outage performance of FD-NOMA relay system with multiple non-colluding eavesdroppers[J]. IEEE Transactions on Vehicular Technology, 2021, 70(12): 12985-12997.

[19] ZAGHDOUD N, MNAOUER A B, BOUJEMAA H, et al. Secrecy performance of cooperative NOMA system with multiple full-duplex relays against non-colluding/colluding eavesdroppers[C]//Proceedings of 2020 IEEE 45th LCN Symposium on Emerging Topics in Networking (LCN Symposium). Piscataway: IEEE Press, 2020: 70-77.

[20] YU C, KO H L, PENG X, et al. Secrecy outage performance analysis for cooperative NOMA over Nakagami-m channel[J]. IEEE Access, 2019(7): 79866-79876.

[21] KIM S W. Modify-and-forward for securing cooperative relay communications[C]//Proceedings of 2014 International Zurich Seminar on Communications. [S.L.:s.n.], 2014:136 – 139.

[22] CHU S I. Secrecy analysis of modify-and-forward relaying with relay selection[J]. IEEE Transactions on Vehicular Technology, 2019, 68(2): 1796-1809.

[23] 程英, 李光球, 沈静洁, 等. MF中继选择系统的物理层安全性能[J]. 电信科学, 2021, 37(9): 95-104.
CHENG Y, LI G Q, SHEN J J, et al. Physical layer security performance of MF relay selection systems[J]. Telecommunications Science, 2021, 37(9): 95-104.

[24] 张延良, 田月华, 李兴旺, 等. 基于MF协议的协作NOMA系统物理层安全性能研究[J]. 电子与信息学报, 2023, 45(4): 1211-1218.
ZHANG Y L, TIAN Y H, LI X W, et al. Research on physical layer security of cooperative NOMA system based on MF protocol [J]. Journal of Electronics & Information Technology, 2023, 45(4): 1211-1218.

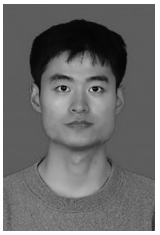
[25] GRADSHTEIN I S, RYZHIK I M, JEFFREY A. Table of integrals, series, and products[M]. Boston: Academic Press, 2007.

[26] ABRAMOWITZ M, STEGUN I A, MILLER D. Handbook of mathematical functions with formulas, graphs and mathematical tables (national bureau of standards applied mathematics series no. 55) [J]. Journal of Applied Mechanics, 1965, 32(1): 239-239.

[作者简介]

罗延翠（1998– ），女，杭州电子科技大学硕士生，主要研究方向为无线通信。

李光球（1966– ），男，博士，杭州电子科技大学教授，主要研究方向为无线通信、信息论与编码。



高辉（1997– ），男，杭州电子科技大学硕士生，主要研究方向为无线通信。

叶明珠（1999– ），女，杭州电子科技大学硕士生，主要研究方向为无线通信。

张亚娟（1998– ），女，杭州电子科技大学硕士生，主要研究方向为无线通信。