基于发射天线选择的修改转发协作D2D网络的物理层安全

刘会芝，李光球，张亚娟，叶明珠，高辉
（杭州电子科技大学通信工程学院，浙江 杭州 310018）

摘　要：为了进一步提升与蜂窝网络共享频谱资源的解码转发（decode-and-forward，DF）协作终端直通（device-to-device，D2D）网络的物理层安全（physical layer security，PLS）性能，提出了一种D2D发送端采用发射天线选择（transmit antenna selection，TAS）的修改转发（modify-and-forward，MF）协作D2D-蜂窝网络PLS模型。配备多根发射天线的D2D发送端采用TAS技术，选择使D2D发送端至MF中继节点链路信干噪比最大的天线发送信号；中继采用MF协议将解码得到的合法信息进行修改后再转发，以避免被动窃听者能够解码出此阶段发送的合法信息，从而改善了D2D网络的PLS性能。推导了MF协作D2D网络的安全中断概率、非零安全容量概率和渐近安全中断概率的解析表达式，并与DF协作D2D网络的PLS性能进行对比分析。数值计算与仿真结果表明，MF协作D2D网络的PLS性能优于DF协作D2D网络，并且增大D2D发送端的发射天线数量，可以增强D2D网络的PLS性能。

关键词：终端直通；发射天线选择；物理层安全；修改转发；安全中断概率
中图分类号：TN918.1
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2024079

Physical layer security of modify-and-forward cooperative D2D networks based on transmit antenna selection

LIU Huizhi, LI Guangqiu, ZHANG Yajuan, YE Mingzhu, GAO Hui
School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China

Abstract: To further improve the physical layer security (PLS) performance of decode-and-forward (DF) cooperative device-to-device (D2D) network that shared spectrum resources with cellular network, a modify-and-forward (MF) cooperative D2D-cellular PLS model was proposed which the D2D transmitter adopted transmit antenna selection (TAS). The D2D transmitter equipped with multiple transmit antennas which adopted TAS technology, then the antenna with the maximum signal-to-interference-plus-noise ratio between the D2D transmitter and MF relay link was selected to send signal. The relay used MF protocol to modify the decoded legal information before forwarding, to avoid passive eavesdropper decoding the legitimate information sent at this stage, which improved the PLS performance of D2D network. The analytical expressions of secrecy outage probability, probability of non-zero secrecy ca-

收稿日期：2024−01−05；修回日期：2024−03−18

pacity and asymptotic secrecy outage probability of MF cooperative D2D network were derived, and the PLS performance of DF cooperative D2D network was compared and analyzed. The numerical and simulation results show that the PLS performance of MF cooperative D2D network is better than that of DF cooperative D2D network. The PLS performance of D2D network can be enhanced by increasing the number of transmit antennas at the D2D transmitter.
Key words: device-to-device, transmit antenna selection, physical layer security, modify-and-forward, secrecy outage probability

0　引言

终端直通（device-to-device，D2D）技术是指通信网络中邻近设备之间直接交换信息的技术，可通过共享蜂窝网络的频谱资源来实现移动终端的海量接入，具有频谱效率高、功耗低等优点，在救灾、文件共享、流量卸载和内容共享等领域中具有广阔的应用前景[1-3]。文献[4]提出了一种最优功率分配方法，可最大化提升蜂窝网络与D2D网络的总平均可达速率。文献[5]提出一种功率控制策略，使得D2D用户的吞吐量最大。文献[4-5]研究的是存在直达链路的D2D网络，然而，在一些应用场景中，由于D2D链路收发端距离过长或存在障碍物的遮挡，需要由中继进行转发，才能实现D2D收发端的正常通信[6-8]。文献[6]推导了解码转发（decode-and-forward，DF）协作D2D网络的可达和速率表达式。文献[7]提出一种提升了DF协作D2D网络和速率的最优功率分配方法。文献[8]推导了一种采用次优功率分配方法的DF协作D2D网络的中断概率表达式。性能好、实现复杂度低的发射天线选择（transmit antenna selection，TAS）技术可进一步提升协作D2D网络的性能[9-10]。文献[9]推导了D2D发送端采用TAS技术的DF中继协作D2D网络的中断概率闭合表达式。文献[10]研究了D2D发送端采用TAS技术的多中继协作D2D网络的中断性能，结果表明，随着发射天线数目增加，中继协作D2D网络的中断性能得到改善。

然而，由于无线传输的开放性使得协作D2D-蜂窝网络面临被窃听的威胁，同时物理层安全（physical layer security，PLS）可实现无线系统在信息论意义上的安全通信，因此协作D2D-蜂窝网络的PLS是当前无线通信的一个重要研究课题[11-17]，其主要研究内容集中在蜂窝用户（cellular user，CU）或D2D网络的PLS性能。文献[11]推导了放大转发协作D2D-蜂窝网络中CU的安全中断概率（secrecy outage probability，SOP）和渐近SOP解析表达式。文献[12]推导了DF协作D2D-蜂窝网络中CU的SOP、渐近SOP和非零安全容量概率（probability of non-zero secrecy capacity，PNSC）解析表达式。文献[13-14]推导了理想或过时信道状态信息（channel state information，CSI）下基站和中继采用TAS的协作D2D-蜂窝网络中CU的SOP、渐近SOP以及PNSC解析表达式，随着天线数量的增加，CU的PLS性能得到了提升，而D2D网络却更易受到窃听攻击，因此其PLS性能研究受到关注[15-17]。文献[15]推导了多跳DF协作D2D网络的SOP、渐近SOP和PNSC闭合表达式。文献[16]推导了DF中继选择D2D网络的SOP、渐近SOP和PNSC解析表达式。文献[17]研究了采用TAS的最优或次优DF中继选择D2D网络的SOP、渐近SOP、PNSC性能，然而，该场景只考虑仅中继节点被窃听的场景，D2D发送端和中继节点都被窃听的场景尚须进一步研究。

针对DF协议PLS性能不够理想的问题，文献[18-19]提出了性能更优的修改转发（modify-and-forward，MF）协议，其基本原理是中继利用中继与目的节点之间的唯一CSI将接收到的合法信息进行修改后再转发，目的节点可解码合法

信息，而窃听者不能，从而使得窃听者在第二时隙无法得知合法信号，相较于DF协议，PLS性能更优。文献[19]推导了MF协作系统的SOP精确表达式，研究结果表明MF协作系统的PLS性能始终优于DF协作系统。文献[20]提出了一种使MF中继系统SOP最低的最优传输策略。文献[21]研究了MF中继选择系统的SOP、渐近SOP性能。文献[22]推导了联合TAS技术的MF中继选择系统的SOP解析表达式，随着天线数量的增加，系统的PLS性能提升。

综上，D2D网络通过与蜂窝网络共享频谱资源提升频谱效率的同时，也会由于无线传输固有的开放性而面临安全威胁，因此，本文主要研究提升协作D2D-蜂窝网络中D2D网络的PLS性能。此外，MF协议和TAS技术可以有效改进协作无线系统的PLS性能，虽然现有文献分别对D2D、MF协议和TAS技术进行了较多的研究，但尚未见相关研究将D2D、MF协议和TAS技术相结合来提升D2D网络的PLS性能，因此本文基于文献[17]，考虑D2D发送端和中继节点均被窃听的场景，提出一种D2D发送端采用TAS技术的MF协作D2D-蜂窝网络（以下简称MF协作D2D-蜂窝网络）PLS模型，并推导出MF协作D2D网络的SOP、渐近SOP以及PNSC解析表达式，然后与DF协作D2D网络进行对比分析，最后采用MATLAB软件进行仿真验证。

1 系统模型

1.1 物理层安全模型

MF协作D2D-蜂窝网络PLS模型如图1所示。MF协作D2D网络由采用TAS的发送端T、半双工MF中继R、接收端D组成；蜂窝网络由基站BS和蜂窝用户CU组成；T配备N根发射天线，R、D、BS、CU、被动窃听者E均配备单根天线。同时假定：

（1）T与D间的通信需要经MF中继R转发才能完成。

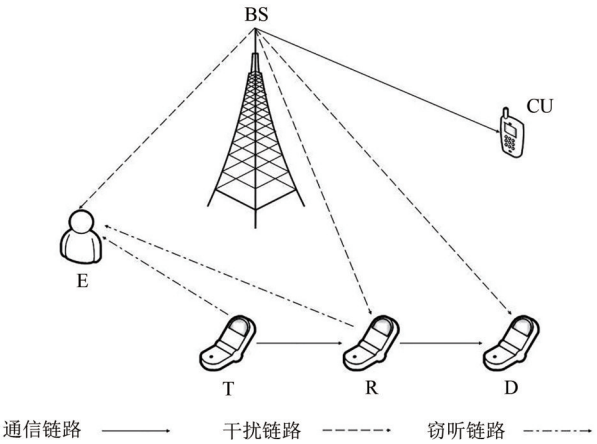


图1 MF协作D2D-蜂窝网络PLS模型

（2）E只窃听MF协作D2D网络传输的保密信号。

（3）D2D网络采用underlay模式共享蜂窝网络的频谱资源。

（4）采用文献[17]中的D2D网络和蜂窝网络相互干扰模型，即BS发送给CU的信号会对R、D、E产生干扰，CU会受到T和R发送信号的干扰。

（5）T的第i根发射天线$\rightarrow$R的链路系数为$h_{\mathrm{TR},i}$，BS$\rightarrow$R、R$\rightarrow$D、BS$\rightarrow$D、BS$\rightarrow$E以及T$\rightarrow$E、R$\rightarrow$E的链路系数分别为h_{BR}、h_{RD}、h_{BD}、h_{BE}、h_{TE}、h_{RE}，上述链路系数均服从相互独立的复高斯分布$\mathrm{CN}(0,1)$。

（6）所有通信链路均具有理想的CSI。

（7）节点R、D、E接收天线上的加性白高斯噪声（additive white Gaussian noise，AWGN）相互独立，且分别服从$\mathrm{CN}\left(0,\sigma_{\mathrm{R}}^2\right)$、$\mathrm{CN}\left(0,\sigma_{\mathrm{D}}^2\right)$、$\mathrm{CN}\left(0,\sigma_{\mathrm{E}}^2\right)$。

1.2 传输过程

MF协作D2D-蜂窝网络保密信号传输需要两个时隙：在第一时隙，T采用TAS技术从N根发射天线中选择使T$\rightarrow$R链路信干噪比（signal to interference plus noise ratio，SINR）最大的第i^*根天线向R发送信号x_d；在第二时隙，R采用文

献[18-22]中的MF协议，将MF中继解码后的信号修改为$x_d'=x_d+\partial$，∂为偏移量，然后再转发给D。在两个时隙中，BS均发送信号x_b给CU，E实施被动窃听。

由于信道的互易性，D利用其与R之间的唯一CSI获得x_d'与x_d的差值∂，因此可以解码出MF中继R发送的修改后的信号x_d'，E实施被动窃听，当E与D之间的距离超过波长的一半时，R与E之间的窃听信道就独立于R与D之间的合法信道，因此E无法获得差值∂，从而无法解码出MF中继R发送的修改后的信号x_d'，即对于MF协议，E只能窃听上述第一时隙内发送的保密信号，则MF协议确保了R与D之间的安全传输[21]。

1.2.1　主信道

主信道由T→R链路和R→D链路组成。在第一个时隙，R的接收信号可表示为：

$$y_{\mathrm{R}}=\sqrt{P_{\mathrm{T}}}\,h_{\mathrm{TR},i^*}x_d+\sqrt{P_{\mathrm{B}}}\,h_{\mathrm{BR}}x_b+n_{\mathrm{R}} \tag{1}$$

其中，P_{T}和P_{B}分别表示T和BS的发射功率，n_{R}为R接收天线上的AWGN。R解码信号x_d的SINR为$\gamma_{\mathrm{TR}}=\dfrac{\gamma_{\mathrm{tr}}}{\gamma_{\mathrm{br}}+1}$，并且$\gamma_{\mathrm{tr}}=P_{\mathrm{T}}\left|h_{\mathrm{TR},i^*}\right|^2/\sigma_{\mathrm{R}}^2$，$\gamma_{\mathrm{br}}=P_{\mathrm{B}}|h_{\mathrm{BR}}|^2/\sigma_{\mathrm{R}}^2$，其中，$\left|h_{\mathrm{TR},i^*}\right|^2=\max\limits_{i\in\{1,\cdots,N\}}\left\{\left|h_{\mathrm{TR},i}\right|^2\right\}$。

T采用TAS技术发送保密信号，参照文献[17]可推导出γ_{TR}的累积分布函数（cumulative distribution function，CDF）为：

$$F_{\gamma_{\mathrm{TR}}}(\gamma)=1-\sum_{i=0}^{N-1}G_{i,N}\frac{\exp\left(-\dfrac{\gamma(i+1)}{\mu_1}\right)}{1+\dfrac{\mu_2}{\mu_1}\gamma(i+1)} \tag{2}$$

其中，$G_{i,N}=\binom{N-1}{i}\dfrac{(-1)^i N}{(i+1)}$，$\mu_1=P_{\mathrm{T}}/\sigma_{\mathrm{R}}^2$和$\mu_2=P_{\mathrm{B}}/\sigma_{\mathrm{R}}^2$分别为T→R链路和BS→R链路的平均信噪比。

在第二个时隙，D的接收信号可表示为：

$$y_{\mathrm{D}}=\sqrt{P_{\mathrm{R}}}\,h_{\mathrm{RD}}x_d'+\sqrt{P_{\mathrm{B}}}\,h_{\mathrm{BD}}x_b+n_{\mathrm{D}} \tag{3}$$

其中，P_{R}为R的发射功率，n_{D}为D接收天线上的AWGN。D解码信号x_d'的SINR为$\gamma_{\mathrm{RD}}=\dfrac{\gamma_{\mathrm{rd}}}{\gamma_{\mathrm{bd}}+1}$，其中$\gamma_{\mathrm{rd}}=P_{\mathrm{R}}|h_{\mathrm{RD}}|^2/\sigma_{\mathrm{D}}^2$，$\gamma_{\mathrm{bd}}=P_{\mathrm{B}}|h_{\mathrm{BD}}|^2/\sigma_{\mathrm{D}}^2$。

由于h_{RD}服从$\mathrm{CN}(0,1)$分布，同上述求γ_{TR}的CDF，可得γ_{RD}的CDF为：

$$F_{\gamma_{\mathrm{RD}}}(\gamma)=1-\frac{\exp\left(-\dfrac{\gamma}{w_1}\right)}{1+\dfrac{w_2}{w_1}\gamma} \tag{4}$$

其中，$w_1=P_{\mathrm{R}}/\sigma_{\mathrm{D}}^2$和$w_2=P_{\mathrm{B}}/\sigma_{\mathrm{D}}^2$分别为R→D链路和BS→D链路的平均信噪比。

1.2.2　窃听信道

窃听信道由T→E链路和R→E链路组成。基于MF协议的工作原理，E无法获得修改后的信号x_d'与原始信号x_d的差值∂，从而无法解码出信号x_d'，因此相当于窃听信道只需要考虑T→E链路。T→R链路的发射天线选择对于E来说相当于随机天线选择。

在第一时隙中E的接收信号可表示为：

$$y_{\mathrm{E}}=\sqrt{P_{\mathrm{T}}}\,h_{\mathrm{TE}}x_d+\sqrt{P_{\mathrm{B}}}\,h_{\mathrm{BE}}x_b+n_{\mathrm{E}} \tag{5}$$

其中，n_{E}为E接收天线上的AWGN。E解码信号x_d的SINR为$\gamma_{\mathrm{TE}}=\dfrac{\gamma_{\mathrm{te}}}{\gamma_{\mathrm{be}}+1}$，其中$\gamma_{\mathrm{te}}=P_{\mathrm{T}}|h_{\mathrm{TE}}|^2/\sigma_{\mathrm{E}}^2$，$\gamma_{\mathrm{be}}=P_{\mathrm{B}}|h_{\mathrm{BE}}|^2/\sigma_{\mathrm{E}}^2$。

参考文献[12]可求得γ_{TE}的概率密度函数（probability density function，PDF）为：

$$f_{\gamma_{\mathrm{TE}}}(\gamma)=\frac{1}{w_3w_4}\exp\left(-\frac{\gamma}{w_3}\right)\frac{1+\dfrac{\gamma}{w_3}+\dfrac{1}{w_4}}{\left(\dfrac{\gamma}{w_3}+\dfrac{1}{w_4}\right)^2} \tag{6}$$

其中，$w_3=P_{\mathrm{T}}/\sigma_{\mathrm{E}}^2$和$w_4=P_{\mathrm{B}}/\sigma_{\mathrm{E}}^2$分别为T→E链路和BS→E链路的平均信噪比。

MF协作D2D-蜂窝网络中，X→Y链路的信道容量可表示为：

$$C_{\mathrm{XY}}=\frac{1}{2}\mathrm{lb}(1+\gamma_{\mathrm{XY}}) \tag{7}$$

其中，$\mathrm{XY}\in\{\mathrm{TR},\mathrm{RD},\mathrm{TE}\}$。

MF协作D2D网络的主信道容量受限于

T→R链路和R→D链路的较小信道容量，因此MF协作D2D网络的主信道容量可表示为：

$$C_{\mathrm{D}}=\min\left(C_{\mathrm{TR}},C_{\mathrm{RD}}\right) \tag{8}$$

由于E无法解码MF中继修改后的信号x_d'，因此窃听链路的信道容量取决于T→E链路，即有$C_{\mathrm{E}}=C_{\mathrm{TE}}$。于是可得MF协作D2D网络的安全容量为：

$$C_{\mathrm{S}}=\max\left(C_{\mathrm{D}}-C_{\mathrm{E}},0\right) \tag{9}$$

若不修改接收、解码得到的信息，MF协议将退化为DF协议[19]。MF协议与DF协议仅在第二时隙对窃听者的影响不同，因此MF协议与DF协议的主信道容量相同，窃听信道容量不同。根据DF的工作原理，E在第二时隙可以解码信号x_d，SINR为$\gamma_{\mathrm{RE}}=\dfrac{\gamma_{\mathrm{re}}}{\gamma_{\mathrm{be}}+1}$，其中，$\gamma_{\mathrm{re}}=w_5\left|h_{\mathrm{RE}}\right|^2$，$w_5=P_{\mathrm{R}}/\sigma_{\mathrm{E}}^2$为R→E链路的平均信噪比。考虑E采用选择合并技术，则DF协作D2D网络中窃听链路的信道容量为：

$$C_{\mathrm{E}}^{\mathrm{DF}}=\max\left(C_{\mathrm{TE}},C_{\mathrm{RE}}\right) \tag{10}$$

其中，$C_{\mathrm{RE}}=\dfrac{1}{2}\mathrm{lb}\left(1+\gamma_{\mathrm{RE}}\right)$。因此，DF协作D2D网络的安全容量为：

$$C_{\mathrm{S}}^{\mathrm{DF}}=\max\left(C_{\mathrm{D}}-C_{\mathrm{E}}^{\mathrm{DF}},0\right) \tag{11}$$

同上述求γ_{TE}的PDF，可求得γ_{RE}的PDF为：

$$f_{\gamma_{\mathrm{RE}}}(\gamma)=\frac{1}{w_5w_4}\exp\left(-\frac{\gamma}{w_5}\right)\frac{1+\dfrac{\gamma}{w_5}+\dfrac{1}{w_4}}{\left(\dfrac{\gamma}{w_5}+\dfrac{1}{w_4}\right)^2} \tag{12}$$

2 协作D2D网络的安全性能分析

结合第1节中对MF协作D2D网络模型以及信道容量的分析，本节将通过分析MF协作D2D网络的安全中断概率、非零安全容量概率和渐近安全中断概率来评估系统的安全性能；另外，本文模型下采用DF协议且两个时隙均被窃听的情况很少被研究，因此，作为对比给出了DF协作D2D网络的PLS性能指标解析表达式。

2.1 安全中断概率

2.1.1 MF协作D2D网络

图1所示的MF协作D2D网络的安全中断概率P^{MF}可定义为其安全容量C_{S}小于目标安全速率R_{S}的概率，利用式（8）以及式（9）可将其表示为[23]：

$$P^{\mathrm{MF}}=\Pr\left(C_{\mathrm{S}}<R_{\mathrm{S}}\right)=1-\Pr\left(C_{\mathrm{TR}}-C_{\mathrm{TE}}\geqslant R_{\mathrm{S}}\right)\Pr\left(C_{\mathrm{RD}}-C_{\mathrm{TE}}\geqslant R_{\mathrm{S}}\right) \tag{13}$$

其中，$\Pr(\cdot)$表示求概率。

分析式（13）可知，推导P^{MF}分3步进行，①推导$\Pr\left(C_{\mathrm{TR}}-C_{\mathrm{TE}}\geqslant R_{\mathrm{S}}\right)$；②推导$\Pr\left(C_{\mathrm{RD}}-C_{\mathrm{TE}}\geqslant R_{\mathrm{S}}\right)$；③将$\Pr\left(C_{\mathrm{TR}}-C_{\mathrm{TE}}\geqslant R_{\mathrm{S}}\right)$与$\Pr\left(C_{\mathrm{RD}}-C_{\mathrm{TE}}\geqslant R_{\mathrm{S}}\right)$代入式（13）。为下文表述方便，定义如下函数并结合式（7）将其表示为：

$$I_{a,b}=\Pr\left(C_a-C_b\geqslant R_{\mathrm{S}}\right)=\Pr\left(\gamma_a\geqslant\theta\gamma_b+\alpha\right)=1-\int_0^{\infty}F_{\gamma_a}(\theta x+\alpha)f_{\gamma_b}(x)\mathrm{d}x \tag{14}$$

其中，$a\in\{\mathrm{TR},\mathrm{RD}\}$，$b\in\{\mathrm{TE},\mathrm{RE}\}$，分别表示T→R链路、R→D链路、T→E链路和R→E链路；$\theta=2^{2R_{\mathrm{S}}}$，$\alpha=\theta-1$。根据式（14）可知，若要推导$I_{\mathrm{TR,TE}}$和$I_{\mathrm{RD,TE}}$，需要将$\gamma_{\mathrm{TR}}$和$\gamma_{\mathrm{RD}}$的CDF分别和$\gamma_{\mathrm{TE}}$的PDF进行积分运算。

首先，将式（2）和式（6）代入式（14）进行积分运算可得$I_{\mathrm{TR,TE}}$为：

$$I_{\mathrm{TR,TE}}=1-\left(1-\sum_{i=0}^{N-1}\frac{G_{i,N}\mu_1\exp\left(-\dfrac{(i+1)\alpha}{\mu_1}\right)}{\theta\mu_2w_4(i+1)}\int_0^{\infty}\frac{(x+A_2)\exp(-A_1x)}{(x+A_3)(x+A_4)^2}\mathrm{d}x\right)=\sum_{i=0}^{N-1}\frac{G_{i,N}\mu_1}{\theta\mu_2w_4(i+1)}\exp\left(-\frac{(i+1)\alpha}{\mu_1}\right)\int_0^{\infty}\frac{(x+A_2)\exp(-A_1x)}{(x+A_3)(x+A_4)^2}\mathrm{d}x \tag{15}$$

其中，$A_1=\frac{(i+1)\theta}{\mu_1}+\frac{1}{w_3}$，$A_2=w_3\left(1+\frac{1}{w_4}\right)$，$A_3=\frac{1}{\theta}\left(\frac{\mu_1}{(i+1)\mu_2}+\alpha\right)$，$A_4=w_3/w_4$。

为了推导式（15），定义如下函数且利用文献[24]中的式（3.353.3）和式（3.352.4）进行计算可得：

$$\xi(a_1,a_2,a_3,a_4)=\int_0^{\infty}\frac{(x+a_2)\exp(-a_1x)}{(x+a_3)(x+a_4)^2}\mathrm{d}x=\frac{a_2-a_3}{(a_3-a_4)^2}\left(\varsigma(a_1a_4)-\varsigma(a_1a_3)\right)+\frac{a_2-a_4}{a_3-a_4}\left(\varsigma(a_1a_4)+\frac{1}{a_4}\right)\tag{16}$$

其中，$\varsigma(mn)=\mathrm{Ei}[-mn]\exp(mn)$，$\mathrm{Ei}[\cdot]$为指数积分函数。

由式（15）并结合式（16）的结果可得$I_{\mathrm{TR,TE}}$的解析表达式为：

$$I_{\mathrm{TR,TE}}=\sum_{i=0}^{N-1}\frac{G_{i,N}\mu_1}{\theta\mu_2w_4(i+1)}\exp\left(-\frac{(i+1)\alpha}{\mu_1}\right)\xi(A_1,A_2,A_3,A_4)\tag{17}$$

其次，将式（4）和式（6）代入式（14）进行积分运算，并利用式（16），整理可得$I_{\mathrm{RD,TE}}$的解析表达式为：

$$I_{\mathrm{RD,TE}}=1-\left(1-\frac{w_1}{\theta w_2w_4}\exp\left(-\frac{\alpha}{w_1}\right)\times\int_0^{\infty}\frac{(x+B_2)\exp(-B_1x)}{(x+B_3)(x+B_4)^2}\mathrm{d}x\right)=\frac{w_1}{\theta w_2w_4}\exp\left(-\frac{\alpha}{w_1}\right)\xi(B_1,B_2,B_3,B_4)\tag{18}$$

其中，$B_1=\frac{\theta}{w_1}+\frac{1}{w_3}$，$B_2=w_3\left(1+\frac{1}{w_4}\right)$，$B_3=\frac{1}{\theta}\left(\frac{w_1}{w_2}+\alpha\right)$，$B_4=w_3/w_4$。

最终，将式（17）以及式（18）代入式（13）中，可得MF协作D2D网络的SOP解析表达式为：

$$P^{\mathrm{MF}}=1-\frac{w_1\exp\left(-\frac{\alpha}{w_1}\right)}{\theta w_2w_4}\xi(B_1,B_2,B_3,B_4)\times\sum_{i=0}^{N-1}\frac{G_{i,N}\mu_1}{\theta\mu_2w_4(i+1)}\exp\left(-\frac{(i+1)\alpha}{\mu_1}\right)\xi(A_1,A_2,A_3,A_4)\tag{19}$$

2.1.2　DF协作D2D网络

相较于MF协议，窃听者可以解码DF中继转发的信号，结合式（7）～式（8）、式（10）～式（11）以及式（14）可将DF协作D2D网络的SOP表示为：

$$P^{\mathrm{DF}}=\Pr\left(C_{\mathrm{S}}^{\mathrm{DF}}<R_{\mathrm{S}}\right)=1-I_{\mathrm{TR,TE}}\times I_{\mathrm{RD,TE}}\times I_{\mathrm{TR,RE}}\times I_{\mathrm{RD,RE}}\tag{20}$$

同上述推导P^{MF}，将式（2）、式（4）分别代入式（14）与式（12）进行积分运算得到$I_{\mathrm{TR,RE}}$、$I_{\mathrm{RD,RE}}$，并将$I_{\mathrm{TR,RE}}$、$I_{\mathrm{RD,RE}}$与式（17）～式（18）代入式（20）可求得DF协作D2D网络的SOP解析表达式为：

$$P^{\mathrm{DF}}=1-\tau^2\xi(B_1,B_2,B_3,B_4)\xi(M_1,M_2,M_3,M_4)\sum_{i=0}^{N-1}\frac{G_{i,N}\mu_1\exp\left(-\frac{(i+1)\alpha}{\mu_1}\right)}{\theta\mu_2w_4(i+1)}\times\xi(A_1,A_2,A_3,A_4)\times\sum_{i=0}^{N-1}\frac{G_{i,N}\mu_1\exp\left(-\frac{(i+1)\alpha}{\mu_1}\right)}{\theta\mu_2w_4(i+1)}\xi(K_1,K_2,K_3,K_4)\tag{21}$$

其中，$\tau=w_1\exp\left(-\frac{\alpha}{w_1}\right)/(\theta w_2w_4)$，$K_1=\frac{(i+1)\theta}{\mu_1}+\frac{1}{w_5}$，$K_2=w_5\left(1+\frac{1}{w_4}\right)$，$K_3=\frac{1}{\theta}\left(\frac{\mu_1}{(i+1)\mu_2}+\alpha\right)$，$K_4=w_5/w_4$，$M_1=\frac{\theta}{w_1}+\frac{1}{w_5}$，$M_2=w_5\left(1+\frac{1}{w_4}\right)$，$M_3=\frac{1}{\theta}\left(\frac{w_1}{w_2}+\alpha\right)$，$M_4=w_5/w_4$。

由式（19）和式（21）可得定理1。

定理1　MF协作D2D网络的SOP与T的发射天线数N、目标安全速率R_{S}、T→R链路的平均信噪比μ_1、BS→R链路的平均信噪比μ_2、R→D链路的平均信噪比w_1、BS→D链路的平

均信噪比 w_2、T→E 链路的平均信噪比 w_3、BS→E 链路的平均信噪比 w_4 这些参数有关；DF 协作 D2D 网络的 SOP 还与 R→E 链路的平均信噪比 w_5 有关。相较于 DF 协议，窃听者无法解码 MF 中继 R 转发的修改后的信号，因此在相同条件下，MF 协作 D2D 网络的 SOP 低于 DF 协作 D2D 网络，PLS 性能更优。

2.2 非零安全容量概率

2.2.1 MF 协作 D2D 网络

MF 协作 D2D 网络的非零安全容量概率 $\mathrm{PNSC}^{\mathrm{MF}}$ 定义为其安全容量 C_{S} 大于 0 的概率，根据式（8）和式（9）可知 $\mathrm{PNSC}^{\mathrm{MF}}$ 的表达式为：

$$\mathrm{PNSC}^{\mathrm{MF}}=\Pr\left(C_{\mathrm{S}}>0\right)=\Pr\left(C_{\mathrm{TR}}-C_{\mathrm{TE}}>0\right)\Pr\left(C_{\mathrm{RD}}-C_{\mathrm{TE}}>0\right) \quad (22)$$

由式（22）可知，推导 $\mathrm{PNSC}^{\mathrm{MF}}$ 可分 3 步进行，①推导 $\Pr\left(C_{\mathrm{TR}}-C_{\mathrm{TE}}>0\right)$；②推导 $\Pr\left(C_{\mathrm{RD}}-C_{\mathrm{TE}}>0\right)$；③将 $\Pr\left(C_{\mathrm{TR}}-C_{\mathrm{TE}}>0\right)$ 与 $\Pr\left(C_{\mathrm{RD}}-C_{\mathrm{TE}}>0\right)$ 代入式（22）。对比分析 $\Pr\left(C_a-C_{\mathrm{TE}}>0\right)$ 与 $\Pr\left(C_a-C_{\mathrm{TE}}\geqslant R_{\mathrm{S}}\right)$，$a\in(\mathrm{TR},\mathrm{RD})$ 可以发现，令 $\Pr\left(C_a-C_{\mathrm{TE}}\geqslant R_{\mathrm{S}}\right)$ 结果中的 $R_{\mathrm{S}}=0$ 即可求得 $\Pr\left(C_a-C_{\mathrm{TE}}>0\right)$。因此，令式（17）与式（18）中的 $\alpha=0$、$\theta=1$，并代入式（22）可得 MF 协作 D2D 网络的 PNSC 解析表达式为：

$$\mathrm{PNSC}^{\mathrm{MF}}=\frac{w_1}{w_2w_4}\xi\left(J_1,J_2,J_3,J_4\right)\sum_{i=0}^{N-1}\frac{G_{i,N}\mu_1}{\mu_2w_4(i+1)}\xi\left(D_1,D_2,D_3,D_4\right) \quad (23)$$

其中，$D_1=\dfrac{i+1}{\mu_1}+\dfrac{1}{w_3}$，$D_2=w_3\left(1+\dfrac{1}{w_4}\right)$，$D_3=\dfrac{\mu_1}{\mu_2(i+1)}$，$D_4=w_3/w_4$；$J_1=\dfrac{1}{w_1}+\dfrac{1}{w_3}$，$J_2=w_3\left(1+\dfrac{1}{w_4}\right)$，$J_3=w_1/w_2$，$J_4=w_3/w_4$。

2.2.2 DF 协作 D2D 网络

结合上述 MF 协作 D2D 网络的 PNSC 表达式以及式（8）和式（10）～式（11）可得 DF 协作 D2D 网络的 PNSC 表达式为：

$$\mathrm{PNSC}^{\mathrm{DF}}=\Pr\left(C_{\mathrm{S}}^{\mathrm{DF}}>0\right)=\mathrm{PNSC}^{\mathrm{MF}}\Pr\left(C_{\mathrm{TR}}-C_{\mathrm{RE}}>0\right)\Pr\left(C_{\mathrm{RD}}-C_{\mathrm{RE}}>0\right) \quad (24)$$

同上述推导 $\mathrm{PNSC}^{\mathrm{MF}}$，令式（14）中的 $R_{\mathrm{S}}=0$，将式（2）、式（4）分别代入式（14）中与式（12）进行积分，并将求得的结果与式（23）一起代入式（24）可得 DF 协作 D2D 网络的 PNSC 解析表达式为：

$$\mathrm{PNSC}^{\mathrm{DF}}=\left(\frac{w_1}{w_2w_4}\right)^2\xi\left(J_1,J_2,J_3,J_4\right)\xi\left(Z_1,Z_2,Z_3,Z_4\right)\times\sum_{i=0}^{N-1}\frac{G_{i,N}\mu_1}{\mu_2w_4(i+1)}\xi\left(D_1,D_2,D_3,D_4\right)\times\sum_{i=0}^{N-1}\frac{G_{i,N}\mu_1}{\mu_2w_4(i+1)}\xi\left(Q_1,Q_2,Q_3,Q_4\right) \quad (25)$$

其中，$Q_1=\dfrac{i+1}{\mu_1}+\dfrac{1}{w_5}$，$Q_2=w_5\left(1+\dfrac{1}{w_4}\right)$，$Q_3=\dfrac{\mu_1}{\mu_2(i+1)}$，$Q_4=w_5/w_4$，$Z_1=\dfrac{1}{w_1}+\dfrac{1}{w_5}$，$Z_2=w_5\left(1+\dfrac{1}{w_4}\right)$，$Z_3=w_1/w_2$，$Z_4=w_5/w_4$。

由式（23）和式（25）可得定理 2。

定理 2 MF 协作 D2D 网络的 PNSC 与 T 的发射天线数 N、T→R 链路的平均信噪比 μ_1、BS→R 链路的平均信噪比 μ_2、R→D 链路的平均信噪比 w_1、BS→D 链路的平均信噪比 w_2、T→E 链路的平均信噪比 w_3、BS→E 链路的平均信噪比 w_4 这些参数有关；DF 协作 D2D 网络的 PNSC 还与 R→E 链路的平均信噪比 w_5 有关。在相同条件下，MF 协作 D2D 网络的 PNSC 高于 DF 协作 D2D 网络。

2.3 渐近安全中断概率

2.3.1 MF 协作 D2D 网络

为了更好地理解高信噪比下，MF 协作 D2D 网络的物理层安全性能，接下来将研究 $\mu_1\to\infty$、$w_1\to\infty$ 时，MF 协作 D2D 网络的渐近安全中断概率。

首先，利用文献[24]中的式（1.211.1），将

$F_{\gamma_{\mathrm{TR}}}(\gamma)$进行泰勒展开，只保留展开式的前两项，忽略更高阶项，可得γ_{TR}的渐近CDF为[25]：

$$F_{\gamma_{\mathrm{TR}}}^{\infty}(\gamma)=\sum_{p=0}^{N}\binom{N}{p}\Gamma(p+1)\mu_2{}^{p}\left(\frac{\gamma}{\mu_1}\right)^{N}+o\left(\frac{\gamma}{\mu_1}\right) \tag{26}$$

其中，$\Gamma(\cdot)$表示伽马函数。同上述求γ_{TR}的CDF，结合式（4）可得γ_{RD}的渐近CDF为：

$$F_{\gamma_{\mathrm{RD}}}^{\infty}(\gamma)=\frac{1}{w_1}(w_2+1)\gamma+o\left(\frac{\gamma}{w_1}\right) \tag{27}$$

其次，将式（6）和式（26）代入式（14）进行积分运算可得$\mu_1\to\infty$时的$I_{\mathrm{TR,TE}}$为：

$$I_{\mathrm{TR,TE}}^{\infty}=1-\sum_{p=0}^{N}\sum_{m=0}^{1}\sum_{s=0}^{N}\sum_{v=0}^{s}\binom{N}{p}\mu_2^{p}\Gamma(p+1)\binom{1}{m}\frac{\Gamma(m+1)}{w_3w_4}\binom{N}{s}\alpha^{N-1}\theta^{s}\times$$
$$\exp\left(\frac{1}{w_4}\right)w_3{}^{m+1}\binom{s}{v}\left(-\frac{w_3}{w_4}\right)^{s-v}\Gamma\left(v-m,\frac{1}{w_4}\right)w_3{}^{v-m}\mu_1^{-N} \tag{28}$$

其中，$\Gamma(\cdot,\cdot)$为上不完全伽马函数。

同上述计算式（28），将式（6）和式（27）代入式（14）进行积分运算可得$w_1\to\infty$时的$I_{\mathrm{RD,TE}}$为：

$$I_{\mathrm{RD,TE}}^{\infty}=1-\frac{w_2+1}{w_4w_1}\left(w_3\theta\exp\left(\frac{1}{w_4}\right)\Gamma\left(0,\frac{1}{w_4}\right)+w_4\alpha\right) \tag{29}$$

最终，将式（28）和式（29）代入式（13）整理并忽略更高阶项可得MF协作D2D网络的渐近SOP为：

$$P^{\infty}=\begin{cases}\left(\dfrac{\mu_2+1}{w_4\mu_1}+\dfrac{w_2+1}{w_4w_1}\right)\left(w_3\theta\exp\left(\dfrac{1}{w_4}\right)\Gamma\left(0,\dfrac{1}{w_4}\right)+w_4\alpha\right), & N=1\\ \dfrac{w_2+1}{w_4w_1}\left(w_3\theta\exp\left(\dfrac{1}{w_4}\right)\Gamma\left(0,\dfrac{1}{w_4}\right)+w_4\alpha\right), & N\geqslant 2\end{cases} \tag{30}$$

令$\rho=\mu_1=w_1$为主信道的平均信噪比，可得MF协作D2D网络的安全分集增益为[21]：

$$d=\lim_{\rho\to\infty}\frac{\log P(R_{\mathrm{S}})}{\log\rho} \tag{31}$$

2.3.2　DF协作D2D网络

参照上述求MF协作D2D网络的渐近SOP，将式（26）、式（27）分别代入式（14）与式（12）进行积分运算并将得到的结果与式（28）和式（29）一起代入式（20）可得DF协作D2D网络的渐近SOP为：

$$P_{\mathrm{DF}}^{\infty}=\begin{cases}(w_3+w_5)\left(\dfrac{\mu_2+1}{w_4\mu_1}+\dfrac{w_2+1}{w_4w_1}\right)\left(\theta\exp\left(\dfrac{1}{w_4}\right)\Gamma\left(0,\dfrac{1}{w_4}\right)+w_4\alpha\right), & N=1\\ \dfrac{(w_2+1)(w_3+w_5)}{w_4w_1}\left(\theta\exp\left(\dfrac{1}{w_4}\right)\Gamma\left(0,\dfrac{1}{w_4}\right)+w_4\alpha\right), & N\geqslant 2\end{cases} \tag{32}$$

由式（30）～式（32）可得定理3。

定理3　MF/DF协作D2D网络的安全分集增益为1，即安全中断概率曲线的斜率，表示安全中断概率曲线随T→R链路平均信噪比μ_1变化的快慢。MF协作D2D网络的渐近SOP与目标安全速率R_{S}、R→D链路的平均信噪比w_1、BS→D链路的平均信噪比w_2、T→E链路的平均信噪比w_3、BS→E链路的平均信噪比w_4这些参数有关，当$N=1$时，还与T→R链路的平均信噪比μ_1、BS→R链路的平均信噪比μ_2有关；DF协作D2D网络的渐近SOP还与R→E链路的平均信噪比w_5有关。

3　数值计算与仿真结果

下面使用MATLAB软件对MF协作D2D网络的SOP、渐近SOP以及PNSC进行数值计算和仿真，研究主信道平均信噪比μ_1、T的发射天线数N等参数对MF协作D2D网络物理层安全性能的影响，仿照以往MF协作系统中将MF协议与DF协议进行对比[19-22]，本文将其推广到MF协作D2D网络中，将MF协作D2D网络与DF协作D2D网络的PLS性能进行对比。参照文献[17]的

参数设置，假设所有节点的加性高斯白噪声方差为1，T的发射功率P_T和R的发射功率P_R相等，MF/DF协作D2D网络的仿真参数见表1。

表1　MF/DF协作D2D网络的仿真参数

参数名称	参数值	参数说明
T的发射天线数N	3	图3～图4、图6
BS→R链路的平均信噪比μ_2/dB	10	图2～图6
BS→D链路的平均信噪比w_2/dB	10	图2～图6
T→E链路的平均信噪比w_3/dB	5	图2、图4、图5
B→E链路的平均信噪比w_4/dB	10	图2～图6
目标安全速率$R_S/\left(\text{bit}\cdot(\text{s}\cdot\text{Hz})^{-1}\right)$	1	图2～图3、图5～图6

图2给出了不同发射天线数N下MF/DF协作D2D网络的SOP性能曲线，由图2可得以下结论。

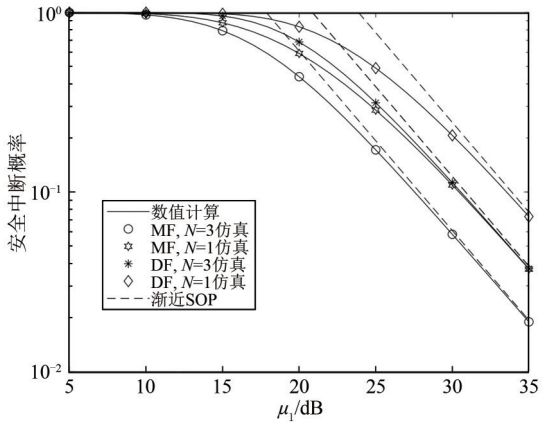


图2　不同发射天线数N下MF/DF协作D2D网络的SOP性能曲线

（1）随着发射天线数N的增大，MF/DF协作D2D网络的SOP均减小，这是由于增大N后，T采用TAS技术使R的接收SINR增大，主信道的信道容量增大，窃听信道容量不变，因此D2D网络的安全容量增大，SOP减小。例如，当$\mu_1=25$ dB时，若N从1增大到3，MF协作D2D网络的SOP从0.29降低到0.17，DF协作D2D网络的SOP从0.49降低到0.31，PLS性能提升。

（2）随着D2D网络的平均信噪比μ_1增大，MF/DF协作D2D网络的SOP均减小，这是由于增大μ_1后，主信道容量增大，但窃听信道容量不变，因而D2D网络的安全容量增大，SOP减小，PLS性能提升。例如，当$N=3$、μ_1从20 dB增加到25 dB时，MF协作D2D网络的SOP从0.43降低到0.17，DF协作D2D网络的SOP从0.68降低到0.31。

图3给出了不同窃听链路平均信噪比w_3下MF/DF协作D2D网络的SOP性能曲线，由图3可得，w_3的增加会降低D2D网络的PLS性能。例如，当$\mu_1=25$ dB时，w_3从0 dB增加到5 dB时，MF协作D2D网络的SOP从0.12增加到0.17，DF协作D2D网络的SOP从0.23增加到0.31。这是由于w_3的增加使窃听信道容量增大，D2D网络的主信道容量不变，因此，其安全容量减小，PLS性能降低。

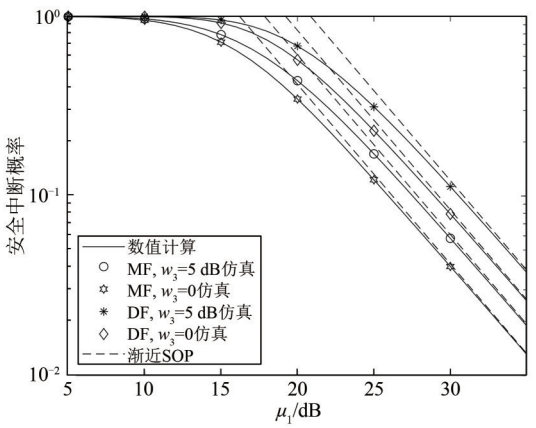


图3　不同窃听链路平均信噪比w_3下MF/DF协作D2D网络的SOP性能曲线

不同目标安全速率R_S下MF/DF协作D2D网络的SOP性能曲线如图4所示。由图4可知，随着目标安全速率R_S的减小，D2D网络的SOP减小。例如，当$\mu_1=25$ dB、R_S从1变为0.5时，MF协作D2D网络的SOP由0.17减小到0.07，DF协作D2D网络的SOP由0.31减小到0.14。这是由于减小目标安全速率，对D2D网络的信息安全传输要求逐渐宽松，需要的安全容量减少，SOP降低。

由图2～图4可得，MF协作D2D网络的PLS

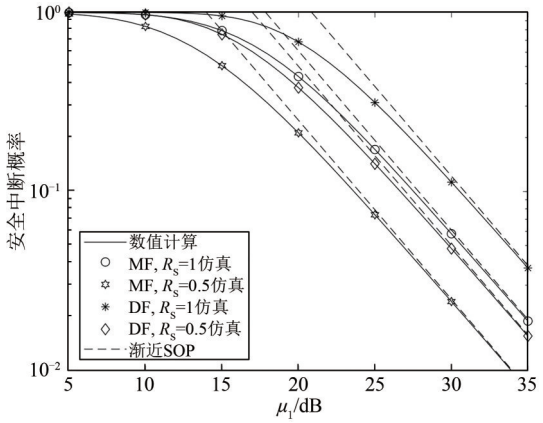


图4　不同目标安全速率R_S下MF/DF协作D2D网络的SOP性能曲线

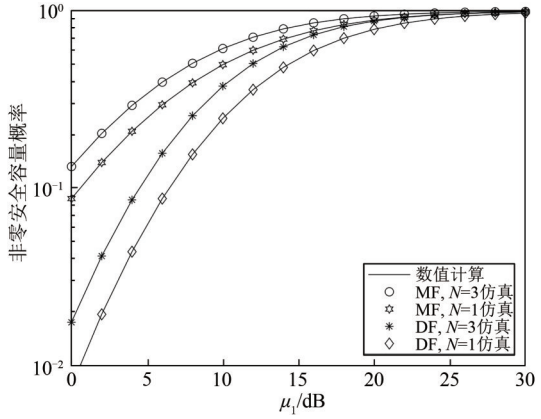


图5　不同发射天线数N下MF/DF协作D2D网络的PNSC性能曲线

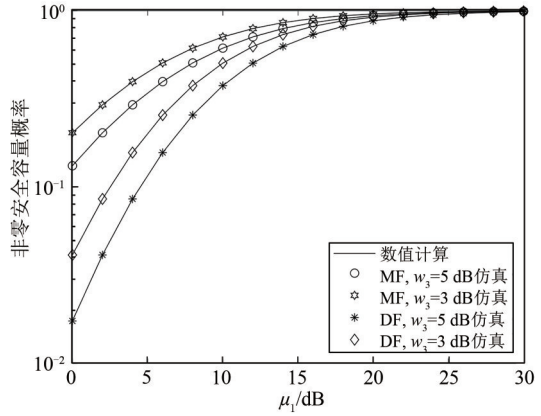


图6　不同窃听链路平均信噪比w_3下MF/DF协作D2D网络的PNSC性能曲线

性能优于DF协作D2D网络。例如，在图2中，当$N=3$、$\mu_1=25$ dB时，MF协作D2D网络的SOP为0.17，DF协作D2D网络的SOP为0.31，在图3中，当$w_3=0$ dB、$\mu_1=20$ dB时，MF协作D2D网络的SOP为0.34，DF协作D2D网络的SOP为0.57，这是因为MF中继R对接收到的信号进行修改，E不能解码修改后的信息，因此窃听信道容量降低，而主信道容量不变，所以安全容量增大，SOP减小，PLS性能提升。

不同发射天线数N下MF/DF协作D2D网络的PNSC性能曲线如图5所示，由图5可得，发射天线数N越大，D2D网络的PNSC越大，这是由于增大N后，R的接收SINR增大，主信道容量增大，窃听信道容量不变，因而D2D网络的安全容量增大，PLS性能提升。例如，当$\mu_1=10$ dB，N从1增大到3时，MF协作D2D网络的PNSC从0.49增大到0.61，DF协作D2D网络的PNSC从0.25增大到0.38。

不同窃听链路平均信噪比w_3下MF/DF协作D2D网络的PNSC性能曲线如图6所示，由图6可以看出，w_3的增加会降低D2D网络的PNSC，例如，当$\mu_1=10$ dB时，w_3从3 dB增加到5 dB时，MF协作D2D网络的PNSC从0.71减小到0.61，DF协作D2D网络的PNSC从0.5减小到0.38。这是由于随着w_3的增加，窃听信道容量增大，主信道容量不变，使得其安全容量减小，因此MF/DF协作D2D网络的PNSC明显减小，PLS性能降低。

由图5～图6可得，MF协作D2D网络的PNSC大于DF协作D2D网络，MF协作D2D网络的PLS性能优于DF协作D2D网络。例如，在图5中，当$N=3$、$\mu_1=10$ dB时，MF协作D2D网络的PNSC为0.61，DF协作D2D网络的PNSC为0.38；在图6中，当$\mu_1=20$ dB、$w_3=5$ dB时，MF协作D2D网络的PNSC为0.94，DF协作D2D网络的PNSC为0.87。

在图2～图6中，MF/DF协作D2D网络的SOP以及PNSC数值计算与仿真结果吻合，证明了本文数值计算的正确性；在高信噪比情况下，

渐近SOP曲线很好地逼近SOP曲线，再次证明了本文数值计算的正确性。

4 结束语

本文将MF协议、TAS技术与D2D网络相结合，提出了一种D2D发送端采用TAS技术的MF协作D2D-蜂窝网络物理层安全模型，研究了MF协作D2D网络的物理层安全性能，利用指数积分函数推导了安全中断概率、非零安全容量概率和渐近安全中断概率的解析表达式，并与DF协作D2D网络进行对比分析。根据仿真实验和数值计算结果可得，MF协议可有效提升DF协作D2D网络的物理层安全性能；增大发射天线数量、发射功率可进一步提升MF协作D2D网络的物理层安全性能。本文可为实现协作D2D网络物理层安全性能的提升提供理论参考。但是，本文仅分析了MF协作D2D网络的安全性能，有关MF协作D2D网络的安全性能优化是未来进一步的研究方向。

参考文献：

[1] ALIBRAHEEMI A M H, HINDIA M N, DIMYATI K, et al. A survey of resource management in D2D communication for B5G networks[J]. IEEE Access, 2023(11): 7892-7923.

[2] GISMALLA M S M, AZMI A I, BIN SALIM M R, et al. Survey on device to device (D2D) communication for 5GB/6G networks: concept, applications, challenges, and future directions[J]. IEEE Access, 2022(10): 30792-30821.

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

[4] LEE J, LEE J H. Performance analysis and resource allocation for cooperative D2D communication in cellular networks with multiple D2D pairs[J]. IEEE Communications Letters, 2019, 23(5): 909-912.

[5] 钱志鸿, 田春生, 王鑫, 等 . D2D网络中信道选择与功率控制策略研究[J]. 电子与信息学报, 2019, 41(10): 2287-2293.
QIAN Z H, TIAN C S, WANG X, et al. Research on channel selection and power control strategy for D2D networks[J]. Journal of Electronics & Information Technology, 2019, 41(10): 2287-2293.

[6] ISLAM S N, MAHMUD M A, T OO A M. Achievable sum rate analysis of relay aided overlay device to device communication among multiple devices[J]. Journal of Communications and Networks, 2017, 19(4): 309-318.

[7] HOANG T D, LE L B, LE-NGOC T. Joint mode selection and resource allocation for relay-based D2D communications[J]. IEEE Communications Letters, 2017, 21(2): 398-401.

[8] LIU G L, FENG W J, HAN Z, et al. Performance analysis and optimization of cooperative full-duplex D2D communication underlaying cellular networks[J]. IEEE Transactions on Wireless Communications, 2019, 18(11): 5113-5127.

[9] XU L W, ZHANG H, GULLIVER T A. Joint TAS and power allocation for D2D cooperative networks[J]. Peer-to-Peer Networking and Applications, 2017, 10(4): 945-953.

[10] XU L W, ZHANG H, WANG J J, et al. Joint TAS/SC and power allocation for IAF relaying D2D cooperative networks[J]. Wireless Networks, 2017, 23(7): 2135-2143.

[11] MOUALEU J M, NGATCHED T M N. Physical-layer security enhancement via relay-aided D2D communications underlaying cellular networks[J]. IEEE Open Journal of the Communications Society, 2020(1): 413-427.

[12] KHOSHAFA M H, NGATCHED T M N, AHMED M H. On the physical layer security of underlay relay-aided device-to-device communications[J]. IEEE Transactions on Vehicular Technology, 2020, 69(7): 7609-7621.

[13] KHOSHAFA M H, NGATCHED T M N, AHMED M H, et al. Enhancing physical layer security using underlay full-duplex relay-aided D2D communications[C]//Proceedings of the 2020 IEEE Wireless Communications and Networking Conference (WCNC). Piscataway: IEEE Press, 2020: 1-7.

[14] 沈静洁, 李光球, 罗延翠, 等 . 过时CSI下全双工中继辅助D2D网络的物理层安全[J]. 电信科学, 2023, 39(3): 89-99.
SHEN J J, LI G Q, LUO Y C, et al. Physical layer security of full-duplex relay-assisted D2D networks under outdated CSI[J]. Telecommunications Science, 2023, 39(3): 89-99.

[15] KHOSHAFA M H, NGATCHED T M N, AHMED M H. On the physical layer security of underlay multihop device-to-device relaying[C]//Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC). Piscataway: IEEE Press, 2019: 1-6.

[16] KHOSHAFA M H, NGATCHED T M N, AHMED M H. Se-

cure transmission in underlay D2D communications using optimal relay selection[C]//Proceedings of the 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall). Piscataway: IEEE Press, 2020: 1-6.

[17] KHOSHAFA M H, NGATCHED T M N, AHMED M H. Relay selection for improving physical layer security in D2D underlay communications[J]. IEEE Access, 2022(10): 95539-95552.

[18] CHEN X M, NG D W K, GERSTACKER W H, et al. A survey on multiple-antenna techniques for physical layer security[J]. IEEE Communications Surveys & Tutorials, 2017, 19(2): 1027-1053.

[19] KIM S W. Modify-and-forward for securing cooperative relay communications[J]. arXiv preprint, arXiv:1403.655, 2014.

[20] VIEN Q T, LE T A, NGUYEN H X, et al. A physical layer network coding based modify-and-forward with opportunistic secure cooperative transmission protocol[J]. Mobile Networks and Applications, 2019, 24(2): 464-479.

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

[22] 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.

[23] LI X W, QI H Y, DO D T, et al. IQ-impaired wireless-powered modify-and-forward relaying for IoT networks: an In-depth physical-layer security analysis[J]. IEEE Internet of Things Journal, 2023, 10(17): 14912-14924.

[24] GRADSHTEĬN I S, RYZHIK I M, JEFFREY A, et al. Table of integrals, series and products: 7th ed[M]. Oxford: Academic, 2007.

[25] KHOSHAFA M H, NGATCHED T M N, AHMED M H, et al. Improving physical layer security of cellular networks using full-duplex jamming relay-aided D2D communications[J]. IEEE Access, 2020(8): 53575-53586.

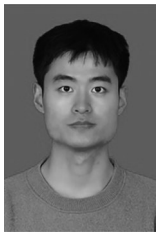
[作者简介]

刘会芝（1997– ），女，杭州电子科技大学通信工程学院硕士生，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。

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

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



高辉（1997– ），男，杭州电子科技大学通信工程学院硕士生，主要研究方向为无线通信。