D2D通信链路中基于时间反演的反窃听物理层传输方案

李方伟 周嘉维 张海波

(重庆邮电大学通信与信息工程学院 重庆 400065)

摘 要 针对D2D用户间通信信息容易被窃听的物理层安全问题,提出了一种基于时间反演(Time-Reversal,TR)技术提升安全速率的传输方案。首先,创建了多输入单输出(Multiple Input Single Output,MISO)窃听信道模型,在D2D通信链路上运用TR技术,利用其时空聚焦特性,提高了通信链路的安全速率。然后,设计了一种干扰协作机制来保障系统的安全速率,在该机制中建立了Stackelberg博弈拍卖模型,以保障干扰用户对D2D用户提供帮助,并证明了该博弈模型纳什均衡(NE)的存在性。最后,通过仿真表明,与已有的物理层传输方案相比,所提安全传输方案有效地提高了安全速率性能。

关键词 D2D,时间反演,Stackelberg博弈,安全速率,纳什均衡

中图法分类号 TN929.5 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.05.015

Anti-eavesdropping Physical Layer Transmission Scheme Based on Time-reversal in D2D Communication Link

LI Fang-wei ZHOU Jia-wei ZHANG Hai-bo

(College of Communication and Information Engineering,Chongqing University of Posts and Telecommunications,Chongqing 400065,China)

Abstract In view of the physical layer security problem that the communication information between D2D users is easy to be bugged,a transmission scheme based on time inversion (TR) technology was proposed to improve the safety rate. Firstly,the MISO wiretapping channel model is created,and TR technology on D2D link is used to improve system safety rate due to TR technology's spatiotemporal focusing characteristics. Secondly,an interference cooperation mechanism is designed to guarantee the security rate of the system. In this mechanism,the Stackelberg game auction model is established to guarantee the help of the interference users to the D2D users,and the existence of the Nash equilibrium (NE) of the game model is proved. In the end,the simulation results show that the proposed safe transmission scheme improves the safety rate performance effectively compared with the existing physical layer transmission scheme.

Keywords D2D,Time-reversal,Stackelberg game,Safe rate,Nash equilibrium

终端直通(Device To Device,D2D)技术能够在短距离内直接进行通信,而不用通过基站转发,减轻了基站的负载;并且D2D用户可以复用蜂窝用户频谱资源进行通信,有效地提高了系统的频谱利用率[1-3]。D2D通信存在诸多优势的同时,也给无线资源管理与传输带来了新的挑战。

D2D用户在复用蜂窝用户频谱资源进行通信时,会在两者之间产生严重的同频干扰。为了减小这种干扰,保障双方的通信服务质量(QOS),文献[4]提出了一种资源分配与功率控制相结合的方案,该方案通过D2D链路合理地分配资源以及动态调整D2D链路的发射功率,提高了D2D链路的通信质量。文献[5]利用基于随机几何的网络模型推导出了D2D发射功率的平衡累积分布函数,考虑到干扰有限和相对有损的环境情况,导出了功率CDF的封闭形式方程,最终有效地控制了D2D用户与蜂窝用户的同频干扰。文献[6]研究了一种协同全双工D2D通信,通过在D2D接收端和蜂窝用户CU接收端进行叠加编码来消除干扰,提升了通信性能。

在干扰管理研究取得了一定进展后,D2D研究向多个方向拓展,其中物理层安全问题成为了一个重要的研究领域。为了保障D2D通信不被窃听,文献[7]提出了一种基于人工噪声辅助的D2D异构蜂窝安全通信方法,该方法设计了一种不会对蜂窝用户以及D2D用户对造成影响的人工噪声,并且借助基站发射该噪声,削弱了窃听信道的质量,增大了D2D用户对与窃听信道的质量差异,最终通过功率控制以及联合优化算法,在保障蜂窝用户通信服务质量的前提下,得到了D2D的最优发射功率。文献[8]将把D2D用户作为一种有意的干扰来对抗窃听,并证明其可增加蜂窝用户的保密容量。文献[9]通过分析涉及D2D用户的社会特征的影响,选择合适的发射机和友好的干扰节点,恶化了窃听用户,提高了保密速率。文献[10]提出了传输保密中断概率,并且在各种因素下对其进行了研究。上述文献通过资源分配和基站的功率控制等不同方法改善了D2D通信链路的安全问题,但是现有文献鲜有关注D2D通信本身也存在的被窃听的问题,而时间反

到稿日期:2018-04-22 返修日期:2018-07-28 本文受国家自然科学基金(61771084,61271260,61102062),重庆市科委自然科学基金项目(cstc2015jcyjA40050),长江学者和创新团队发展计划基金资助项目(IRT16R72)资助。

李方伟(1960-),男,教授,主要研究方向为认知无线电、移动通信安全,E-mail:lifw@cqupt.edu.cn(通信作者);**周嘉维**(1992-),男,硕士生,主要研究方向为移动通信安全;**张海波**(1979-),男,副教授,主要研究方向为无线资源管理。

演(TR)技术是保障直通用户安全通信的最有潜力的技术之一。

时间反演技术能在均匀或非均匀媒质中实现自适应的空间和时间同步聚焦。空时聚焦是指电磁能量会在同一时间聚焦于目标点处，而在目标点的其他位置，电磁能量很低甚至可以忽略不计[11-12]。文献[13]将 TR 技术运用到 D2D 异构无线通信网络中，为了降低蜂窝用户与 D2D 用户的同频干扰，以及用户间的干扰等，提出了一种基于 TR 技术的无线优化机制，该机制通过在基站处运用时间反演镜(Time Reversal Mirror，TRM)技术消除干扰，对每个用户执行信道签名，提取有用信号，剔除干扰，并通过功率控制算法与凸优化相结合的方法保障蜂窝用户的通信服务质量。但文献[13]并未考虑 D2D 用户在通信过程中会存在被窃听的安全问题，而相关文献证明 TR 技术对于防窃听也有着显著的效果[14-17]。因此，本文将 TR 技术运用到 D2D 通信链路中，并用其空时聚焦性能最大程度地弱化窃听信道的质量，从而提高整个 D2D 链路的传输安全性。

针对 D2D 通信链路易被窃听的问题，本文综合考虑天线间的相关性和信道状态，在蜂窝小区中建立了一个 MISO 窃听信道模型。在此模型下，根据窃听用户与 D2D 接收端的位置的不同，本文给出了两种不同的解决方案。首先，针对窃听用户在 D2D 接收方信息聚焦点外的情况，通过运用 TR 技术的空时聚焦性保障信息传输中的安全性；其次，如果窃听用户在 D2D 接收方信息聚焦点内或附近，那么在运用 TR 技术的基础上设计一种协同干扰机制，并通过 Stackelberg 博弈拍卖模型优化该机制，以得到一个最优的安全速率。

1　系统模型

基于蜂窝覆盖下的通信系统模型如图 1 所示，基站和 D2D 发射端配备多根天线 N_t，M_t 蜂窝用户、D2D 接收端和窃听用户配备单天线。基站到蜂窝用户的信道增益为 h_{bc}，$h_{bc}=(h_{11},h_{12},\cdots,h_{1N_t})$是基站 b 到蜂窝用户的 $1\times N_t$ 维信道向量，其中 h_{1i}表示基站第 i 根天线到蜂窝用户的信道参数。类似地，h_{dc}，h_{dd} 分别表示 D2D 到蜂窝用户的信道增益和 D2D 用户间的链路信道益。h_e 作为窃听信道，在 D2D 用户互通消息时窃取其传输信息。P_B，P_D 分别表示基站的发射功率和 D2D 链路的传输功率，n_o 为高斯白噪声。

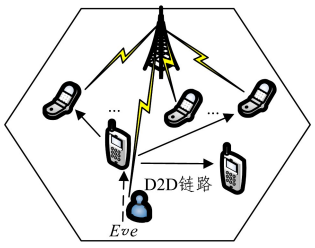

图 1　系统模型

Fig. 1　System mode

为了提高频谱的利用率，D2D 采用下行复用模式，即与蜂窝用户共享频谱资源块。为了方便分析，假设一个蜂窝用户频谱资源只能被一个 D2D 用户复用，且 D2D 用户通信产生的同频干扰不能影响到蜂窝用户的通信。

图 1 所示的系统模型是建立在室外蜂窝小区中的，信息传输过程要面临反射、折射等过程，传播路径较为复杂，而 TR 技术在复杂的多路径环境中拥有较好的聚焦性能，并且环境越复杂，其聚焦性能越好，因此本文运用 TR 技术来提升 D2D 链路的安全速率。在复杂的多径信道中，用 $n\in\{d,e\}$分别表示合法用户和窃听用户，合法信道与窃听信道可用维数为 $2M\times L$ 的矩阵 $\boldsymbol{H}=[h_{1,d},h_{2,d},\cdots h_{M_t,d},h_{1,e},h_{2,e},\cdots,h_{M_r,e}]^{\mathrm{T}}$表示，$L$ 为可分辨多径的条数。合法用户或窃听用户之间的信道冲击响应 CIR 表示为：

$$h_{mn}(t)=\sum_{l=1}^{L-1}\sigma_{mn,l}\delta(t-\tau_{mn,l}) \tag{1}$$

其中，$\sigma_{mn,l}$，$\tau_{mn,l}$分别代表第 l 条路径的幅度和时延，$0<l\leqslant L-1$，且 CIR 在时域上被离散化为一个矢量 $h_{mn}[l]\in c^{L\times 1}$并且满足 $h_{mn}[l]\in c^{L\times 1}=0$，$E[|h_{mn}[l]|^2]=\delta_{mn,l}^2=\mathrm{e}^{-lT_s/\sigma_T}$，$h_{mm}[l]$为循环对称复高斯随机变量。

信息序列由时间反演镜向量 $\boldsymbol{g}_{m,d}\in\boldsymbol{C}^{L\times 1}$调制，则 $\boldsymbol{g}_{m,d}$的每个分量为：

$$\boldsymbol{g}_{m,d}[l]=\frac{h_{m,d}^{*}[L-1-l]}{\sqrt{E[\sum_{l=0}^{L}|h_{m,d}(l)|^2]}} \tag{2}$$

其中，$h_{m,d}^{*}[L-1-l]$代表 $h_{m,d}[L-1-l]$的共轭卷积。

TR 技术传输分为 3 个阶段：第一阶段为探测阶段，首先由 D2D 接收方在时域上发送很短的探测脉冲，探测脉冲经过反射、折射、衍射，最后传到发送端；第二阶段为时间反转阶段，D2D 发送端把接收到的探测信号在时域上进行反转；第三阶段为再发射阶段，把信号按原路径传回接收端，形成空时聚焦。

由上述可知，D2D 接收端与窃听端接收到的信息分别为：

$$y_d=\alpha_{dd}\sqrt{P_D}\sum_{m=1}^{N_t}S(g_{m,d}*h_{m,d})+\sum_{j=1}^{M_t}\alpha_{bd}\sqrt{P_B}h_{b_jd}x_{jd}+n_d \tag{3}$$

$$y_e=\alpha_{de}\sqrt{P_D}\sum_{m=1}^{N_t}S(g_{m,e}*h_{m,e})+\sum_{j=1}^{M_t}\alpha_{be}\sqrt{P_B}h_{b_je}x_{je}+n_d \tag{4}$$

式(3)和式(4)由 3 部分组成：第一部分为用户接收的信息；第二部分为基站对用户的干扰；第三部分为高斯白噪声。其中，$\alpha_{ij}=d_{ij}^{-\beta}$代表路径损耗，$d_{ij}$代表传输距离，$\beta$代表损耗因子，$\sqrt{P_D}$和 $\sqrt{P_B}$分别代表 D2D 发送端和基站的发送功率，x_{jd}和 x_{je}分别代表基站到 D2D 接收端和窃听用户的干扰信号，n_d 和 n_e 为高斯白噪声。

2　基于 TR 技术的 D2D 网络安全通信理论分析

2.1　聚焦区域外的安全速率分析

在本文中，窃听用户 *Eve* 的主要目的是窃听 D2D 通信链路上的信息；D2D 发送端为了防止信息被窃听，利用时间反演技术提高系统的安全性。这里将安全速率 R_S 作为评判性能好坏的参数，根据 Wyner 的窃听信道模型[19]，能得出 D2D 链路的安全速率公式：

$$R_S=[\log_2(1+\gamma_{dd})-\log_2(1+\gamma_e)] \tag{5}$$

其中：

$$\gamma_{dd}=\frac{\alpha_{dd}P_D|\sum_{m=1}^{N_t}S(g_{m,d}*h_{m,d})|^2}{\sum_{j=1}^{M_t}\alpha_{bd}P_Bh_{b_jd}h_{b_jd}^{H}+\alpha_{dd}^2} \tag{6}$$

$$\gamma_e=\frac{\alpha_{de}P_D\left|\sum_{m=1}^{N_t}S(g_{m,e}*h_{m,e})\right|^2}{\sum_{j=1}^{M_t}\alpha_{be}P_Bh_{b_je}h_{b_je}^H+\sigma_e^2} \tag{7}$$

其中，γ_{dd}，γ_e 分别代表 D2D 对和窃听用户的信干燥比。P_B 和 P_D 为基站发射功率和 D2D 发射功率，α_{dd}^2 和 α_e^2 为噪声功率，$h_{b_jd}^H$，$h_{b_je}^H$ 分别为 h_{b_jd}，h_{b_je} 信道的转置，为了方便探究，令 $|h_{b_jd}|^2=h_{b_jd}h_{b_jd}^H$，$|h_{b_je}|^2$ 同理。

2.2 聚焦区域内的安全速率提升方案

这部分主要研究窃听用户在合法接收端信息聚集区域内窃听信息的情况。在封闭的腔体场景下运用 TR 技术，会在接收端产生一个小于 $\gamma/2$ 的聚集范围；但是在开放的蜂窝环境下，传播路径变长，使得信息聚焦点的范围（聚焦区域）大于腔体环境（约为 5～10m），因此当窃听用户与接收端距离足够近时，窃听用户有可能在接收端信息聚焦范围内窃听 D2D 接收端的信息，并窃听 D2D 通信链路的信息。针对上述问题，本文设计了一个协同干扰模型，如图 2 所示。

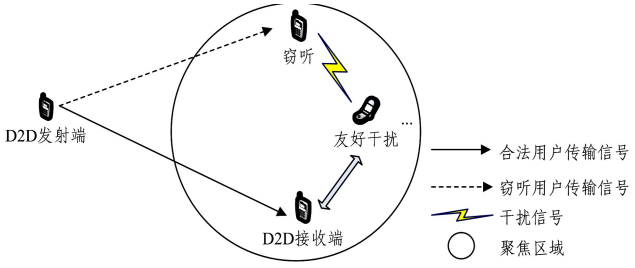

图 2 聚焦区域内的系统模型

Fig. 2 System model in focus area

图 2 所示模型由 3 部分组成，分别为 D2D 收发端、窃听用户以及友好干扰用户。其中，友好干扰用户与 D2D 收发端为合作的关系，与窃听用户为敌对的关系。干扰用户将同时对 D2D 接收端与窃听用户发送干扰信息，如式(8)所示：

$$Y_D=y_d+\sum_{j\in N}\alpha_{jd}\sqrt{P_J}h_{je}z_j \tag{8}$$

式(8)由两部分组成：第一部分 y_d 为未受友好干扰时的信号，如式(3)所示；第二部分 $\sum_{j\in N}\alpha_{jd}\sqrt{P_J}h_{je}z_j$ 为友好干扰用户对接收端的干扰信号，其中 α_{jd} 为路径损耗，P_J 为友好干扰用户的发射功率，h_{je} 为友好干扰用户到 D2D 接收端的信道增益，z_j 为干扰信息。由于干扰用户与 D2D 接收端是合作的关系，因此干扰信号能被 D2D 接收端解析和消除，故式(8)等价于：

$$Y_D=y_d \tag{9}$$

由于窃听用户与友好干扰用户为敌对的关系，因此窃听用户不能够分辨出干扰信息，故窃听用户会受到干扰信息影响，导致安全速率下降。窃听用户接收到的信息为：

$$Y_E=y_e+\sum_{j\in N}\alpha_{je}\sqrt{P_J}h_{je}z_j \tag{10}$$

因此，D2D 安全速率可表示为：

$$R_{S1}=[\log_2(1+\gamma_{dd1})-\log_2(1+\gamma_{e1})] \tag{11}$$

其中：

$$\gamma_{dd1}=\frac{\alpha_{dd}P_D\left|\sum_{m=1}^{M_t}S(g_{m,d}*h_{m,d})\right|^2}{\sum_{j=1}^{N_t}\alpha_{bd}P_Bh_{b_jd}h_{b_jd}^H+\sigma_{dd}^2} \tag{12}$$

$$\gamma_{e1}=\frac{\alpha_{de}P_D\left|\sum_{m=1}^{M_t}S(g_{m,e}*h_{m,e})\right|^2}{\sum_{j=1}^{N_t}\alpha_{be}P_Bh_{b_je}h_{b_je}^H+\alpha_{je}P_Jh_{je}h_{je}^H+\alpha_e^2} \tag{13}$$

其中，$\alpha_{je}P_Jh_{je}h_{je}^H$ 为友好干扰用户对窃听用户的干扰功率，其他参数与式(6)和式(7)的表述一致。

2.2.1 Stackelberg 博弈拍卖模型

由于友好干扰用户的发射功率是有限的，因此友好干扰用户具有自私性，不会无偿地帮助 D2D 用户。为了能让友好干扰用户帮助 D2D 用户并使 D2D 用户的收益最大化，这里建立一个 Stackelberg 博弈拍卖模型。

2.2.2 博弈设计与效用函数

本文以 D2D 整个通信链路作为买方，而友好干扰用户因为要拍卖干扰，所以作为卖方。买方的收益为链路的安全速率，但买方在提高收益的同时必将向卖方交付一定的费用，这费用必须在买方可承受的范围内，否则买方将停止交易，退出博弈。而卖方的收益是买方支付的费用，但在收取费用的同时也将损失一定的性能。卖方的收益必须要大于它损失的性能，若买方支付的价格过低，干扰用户不会与 D2D 合作。D2D 链路或买方与友好干扰用户或卖方的效用函数设计如下：

$$\begin{aligned}&U_{SD}=R_{S1}-\lambda_ip_j(U_{SD}>0)\\&\text{s.t. } p_j\in[0,\max P_D]\end{aligned} \tag{14}$$

其中，λ 为友好干扰节点的功率单价，R_s 为系统的收益，λp_j 是买方要支付的费用。

$$\begin{aligned}&U_J=\lambda_ip_j-\varepsilon p_j\\&\text{s.t. } \lambda_i\in[\varepsilon,+\infty]\end{aligned} \tag{15}$$

其中，ε 为友好干扰的功率成本，对于同一个友好干扰节点，这个值是固定的。卖方在获得买方支付的费用的同时，也会损失一定的性能 εp_j。由式(14)、式(15)，可知 Stackelberg 博弈拍卖模型的数学表达为：

$$G\langle\{SD,J\};p_j\in[0,P_j],\lambda_i\in[\varepsilon,+\infty];\{U_{SD},U_J\}\rangle \tag{16}$$

2.2.3 均衡点的证明

在 Stackelberg 博弈拍卖模型中，买卖双方都是理性的，都希望自己的收益最大化，但一方收益最大，必将损害另一方的收益，导致博弈破裂，因此必须要找到一个均衡点使得买卖双方都能够接受。下面进行均衡点的推导：

$$U_{SD}=R_{S1}-\lambda_ip_j=[\log(1+\gamma_{dd1})-\log(1+\gamma_{e1})]-\lambda p_j \tag{17}$$

当 λ 值固定，也就是干扰用户的单价固定时，D2D 链路收益对 p_j 求偏导数为：

$$\begin{aligned}\frac{\partial U_{SD}}{\partial p_j}&=\frac{1}{\ln 2}\frac{\gamma'_{e1}(1+\gamma_{e1})'}{1+\gamma_{e1}}-\lambda\\&=\frac{1}{\ln 2}\frac{\gamma'_{e1}\gamma'_{e1}}{1+\gamma_{e1}}-\lambda\end{aligned} \tag{18}$$

继续求其二阶导数为：

$$\frac{\partial^2U_{SD}}{\partial p_j^2}=\frac{\gamma'_{e1}(2\gamma''_{e1}(1+\gamma_{e1})-(\gamma'_{e1})^2)}{(1+\gamma_{e1})^2}<0 \tag{19}$$

由式(19)易知，$2\gamma''_{e1}(1+\gamma_{e1})-\gamma''^2_{e1}>0$，$\gamma'_{e1}<0$，$(1+\gamma_{e1})^2>0$，$\frac{\partial^2U_{SD}}{\partial p_j^2}<0$，因此函数为凸函数，故必然存在一个最优解。

令$\frac{\partial U_{SD}}{\partial p_j}=\frac{1}{\ln 2}\frac{\gamma'_{e1}(1+\gamma_{e1})'}{1+\gamma_{e1}}-\lambda=0$，可得：

$$\boldsymbol{p}_j^*=-\frac{2+(P_D h_e^2)}{2h_{je}^2}+\sqrt{\frac{P_D^2}{4}+\frac{P_D h_e^2}{\lambda h_{je}^2 \ln 2}} \tag{20}$$

从而得到最优值 $\boldsymbol{p}_j^*=\max(\min(\boldsymbol{p}_j^*,\boldsymbol{P}_j),0)$。

对于友好干扰而言，它的目的是使自己的单价最大化，因此对式(15)求一阶导可得：

$$\frac{\partial U_J}{\partial \lambda_i}=p_j+\lambda_i\frac{\partial p_j}{\partial \lambda_i}-\varepsilon\frac{\partial p_j}{\partial \lambda_i} \tag{21}$$

令式(21)为 0，把式(20)代入式(21)中可解得：

$$\lambda_i^*=\varepsilon-\boldsymbol{p}_j^*\frac{\partial \lambda_i}{\partial p_j} \tag{22}$$

因此，可得均衡点为：

$$\boldsymbol{v}=(\boldsymbol{p}_j^*,\lambda_j^*) \tag{23}$$

当买方收益大于 0 时，将采用均衡解；当买方收益等于 0 时，买方将会退出博弈，并寻找其他合作对象。公式如下：

$$U_{SD}=\begin{cases}U_{SD}(\boldsymbol{p}_j^*), & U_{SD}>0\\ 0, & U_{SD}\leqslant 0\end{cases} \tag{24}$$

由上述可知，D2D 链路最优策略在友好干扰单价固定时，选择最优的功率；同理，友好干扰用户也将在最优功率下获得最大值。由于 D2D 用户急于与友好干扰用户合作来提高自己的安全速率，因此只要自身收益大于 0，D2D 用户就会做出相应退让，与该友好干扰用户合作。

2.2.4　交叉迭代算法

根据式(20)、式(21)可得求解博弈均衡的交叉迭代算法：

1)初始化 $\lambda=\varepsilon+C$(C 为大于 0 的常数)；

2)将 λ 代入式(20)，求解出 p_j；

3)判断 U_{SD} 是否大于 0；

4)若 U_{SD} 大于 0，则将 p_j 代入式(21)求出 λ，否则退出循环；

5)重复步骤 2)－步骤 4)，直至 λ_i 和 p_j 不再变化。

2.3　功率控制分析

由式(5)、式(6)可知，增加 D2D 的发射功率势必会提高系统的安全速率，但由于 D2D 用户与蜂窝用户共享同一频谱资源，因此增加功率的同时也会增大对蜂窝用户的同频干扰。为了保障蜂窝用户的通信质量，本文引用了文献[10]的功率控制算法，为蜂窝用户与 D2D 用户分别设立功率调控因子进行功率调控，使得用户的信干噪比值满足门限要求，最终基站根据调控因子合理分配功率给 D2D 用户和蜂窝用户。

3　仿真分析

本文通过系统级的仿真平台 MATLAB 对所提方案进行仿真验证。首先将其与传统方案进行比较，接着分析了天线数目对安全速率的影响，最后探究了通信链路与干扰用户收益的变化。

在仿真中，D2D 网络场景设置在以基站为中心、半径为 500 m 的蜂窝小区内，其中路径损耗因子 $\alpha=3$，D2D 用户间相隔 100 m，D2D 发送功率为[0，10 w]，蜂窝用户发射功率为 10 w，噪声功率为 70 dbm，D2D 用户与基站间的距离为[0，500 m]，蜂窝用户平均分配在小区范围内。另外，D2D 合法信道和窃听信道均服从多径瑞利衰落，信道增益服从均值为 0、方差为 $\boldsymbol{E}|[\boldsymbol{h}_{mn}[\boldsymbol{l}]|^2]=\boldsymbol{\delta}_{mn,l}^2$ 的循环对称复高斯随机变量。设信道带宽 $B=500$ MHz，采样周期 $T_s=2$ ns，均方根延迟扩展 $\sigma_T=10$ B，典型信道长度为 $L=120$。

图 3 是多径信道环境下可达保密速率随 SNR 变化的仿真结果，发送天线为 2 根，SNR 的大小为[－50 db，50 db]。如图 3 所示，随着 SNR 的增大，可达保密速率先迅速增大，而后慢慢收敛于一个稳定值；本文所提方案优于文献[7]的方案，这是由于时间反演的空时聚焦性能能够极大化地增大合法用户信道与窃听信道的质量差异。因此，在相同条件下，相比于其他方案，运用时间反演技术能够得到更高的可达保密速率。

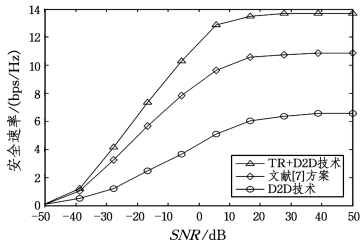

图 3　聚焦区外安全速率分析图

Fig. 3　Analysis diagram of safety rate outside focus area

图 4 是发送端天线对可达保密速率影响的仿真图，SNR 设置为 27 db。如图 4 所示，随着发端天线数目的增加，链路可达保密速率显著提高，相同条件下，相比于文献[7]的方案，本文方案能更大幅度地增加安全可达速率。TR 技术的空间聚焦性能会随着路径的增多而加强，从而降低窃听信道质量，进一步提升可达保密速率。

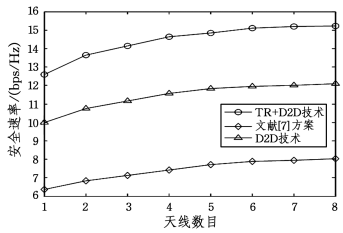

图 4　天线数目对安全速率的影响

Fig. 4　Influence of antenna number on safety rate

图 5 和图 6 分别是聚焦区域内运用博弈后，博弈双方效用函数的变化趋势图。其中，图 5 是关于通信链路安全速率随购买干扰功率增长的变化图。当购买友好干扰用户的功率较小时，通信链路的安全速率迅速增加，但随着购买干扰用户的功率越来越大，通信链路的收益将越来越小，最终通信链路收益将降为 0，因此买方(D2D 通信链路)将退出博弈或寻找其他干扰用户进行博弈。图 6 是干扰用户的效用与功率单价的关系，友好干扰用户在与通信链路合作的过程中会有一定的功率损耗，设功率损耗 $\varphi=1$，当 $\lambda\leqslant\varphi$ 功率单价时将不进行博弈；当功率单价较小时，干扰用户效用呈线性上升趋势，但是当单价功率到达某一个临界值时，干扰用户效用直接变为 0，这是由于干扰用户(卖方)开出的单价超出了通信链路(买方)的承受范围，因此，通信链路直接中断交易，退出博弈。综上所述，D2D 通信链路(买方)为了让自身安全速率(收益)达到最大，将做出一定的让步，而干扰用户为了使自己得到的功率收益最大，也将做出相应的退让，最终买卖双方将找到一个均衡点。

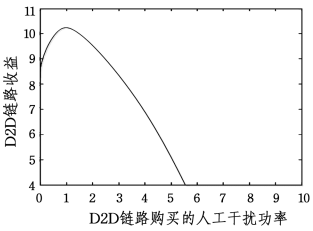

图 5 通信链路收益

Fig. 5 Communication link income map

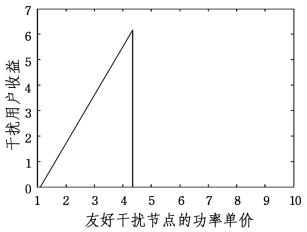

图 6 干扰用户收益

Fig. 6 Interference user income map

图 7 为引入协同干扰机制后 D2D 链路安全速率的变化图。当窃听用户在信息聚焦区域范围内窃听时，时间反演技术带给合法用户的信道增益会被削弱，这使得窃听用户可能会窃听到通信链路信息，相比图 3，安全可达速率要弱于信息聚焦区域外和文献[7]方案的安全可达速率。当引入了协同干扰机制后，由于对窃听信道的加扰，窃听用户较难正确识别有用信息，因此其安全速率下降，由此相对改善了 D2D 通信链路的安全速率。如图 7 所示，加入干扰后，系统的安全速率要优于文献[7]方案的安全可达速率。

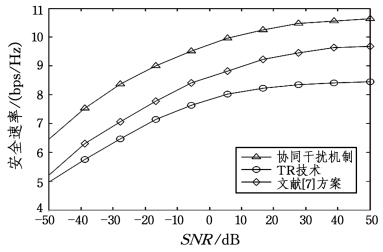

图 7 聚焦区域内的安全速率

Fig. 7 Security rate in focus area

结束语 针对 D2D 通信链路被窃听的问题，本文提出了一种基于 TR 技术的传输方案，通过理论分析得出了可达安全速率的表达式，并运用 MATLAB 仿真实验得出：*SNR* 越大，天线数目越多，则可达安全速率越大。其次，本文设计了一种基于 Stackelberg 博弈的干扰合作机制，用于解决使用 TR 技术后聚焦区域内存在的安全隐患，并且通过理论推导和仿真分析得到通信链路确实存在最优决策点，在此点上能够得到较好的收益。但是现实中 D2D 经常面临着两小区边缘通信的情况，在边缘地区 D2D 将面临着更加复杂的环境，故保障 D2D 边缘通信安全也将成为未来研究的重要课题。

参 考 文 献

[1] MUTHANNA A, MASEK P, HOSEK J, et al. Analytical Evaluatation of D2D Connectivity Potential in 5G Wireless Systems [C]// International Conference on Next Generation Wired/wireless Networking. Springer International Publishing, 2016.

[2] WANG M, YAN Z. Security in D2D Communications: A Review [C]// IEEE Trustcom/bigdatase/ispa. IEEE Computer Society, Helsinki, 2015: 1199-1204.

[3] QINA Z, WANG X. Reviews of D2D technology for 5G communication networks[J]. Journal on Communications, 2016, 129: 1-14.

[4] BANAGAR M, MAHAM B, POPOVSKI P, et al. Power Distribution of Device-to-Device Communications in UnderlaidCellular Networks[J]. IEEE Wireless Communications Letters, 2015, 5(2): 204-207.

[5] LUO Y, CUI L, YANG Y, et al. Power control and channel access for physical-layer security of D2D underlay communication [C]// International Conference on Wireless Communications & Signal Processing. Nanjing: IEEE Press, 2015: 1-5.

[6] LIU G, FENG W, HAN Z. et al. Performance Analysis and Optimization of CooperativeFull-Duplex D2D Communication-Underlaying Cellular Networks[OL]. https://arxiv. org/pdf/1805. 06645. pdf.

[7] KANG X L, JI X S, HUANG K Z. SecureD2D underlaying cellular communication based on artificial noise assisted[J]. Journal of communications, 2015, 36(10): 149-156.

[8] DOPPLER K, RINNE M P, PEKKA, et al. Device-to-Device Communications; Functional Prospects for LTE-Advanced Networks[C]// IEEE International Conference on Communications Workshops. Dresden: IEEE, 2009: 1-6.

[9] WANG L, WU H, STUBER G. Resource Allocation with Cooperative Jamming in Socially Interactive Secure D2D Underlay[C]// IEEE Vehicular Technology Conference. Nanjing: IEEE Press, 2016.

[10] CHEN Y, JI X, HUANG K, et al. Secrecy analysis in D2D-enabled cellular networks against spatially random eavesdroppers [C]// International Symposium on Wireless Personal Multimedia Communications. Shenzhen: IEEE Press, 2017: 262-267.

[11] QIU R C. A Theory of Time-Reversed Impulse Multiple-Input Multiple-Output (MIMO) for Ultra-Wideband (UWB) Communications[C]// IEEE 2006 International Conference on Ultra-Wideband. Waltham, MA, USA: IEEE, 2007: 587-592.

[12] QI X L, HUGHES T L, ZHANGS C. Topological field theory of time-reversal invariant insulators[J]. Physical Review B, 2008, 78(19): 195424.

[13] LI F W, ZHANG L L, ZHU J. A Mechanism of Radio Resource Optimization in Time-reversal Device-to-Device Communication [J]. Journal of computer science, 2017, 45(10): 78-82, 98. (in Chinese)
李方伟，张琳琳，朱江. D2D 通信网络中一种基于时间反演的无线资源优化机制[J]. 计算机科学，2017，45(10)：78-82，98.

[14] ZHU J, WANG Y, YANG T, et al. Time-Reversal Based Secure Transmission Scheme for 5G Networks over Correlated Wireless Multi-Path Channels[OL]. https://link. springer. com/article/10. 1007/s11277-018-5737-y.

[15] TRAN H V, TRAN H, KADDOUM G, et al. Effective secrecy-SINR analysis of time reversal employed systems over correlated multi-path channel[C]// The 11th International Conference on Wireless and Mobile Computing, Networking and Communications. Abu Dhabi: IEEE Press, 2015: 527-532.

[16] XU Q, REN P, DU Q, et al. Security-Aware Waveform and Artificial Noise Design for Time-Reversal-Based Transmission [J]. IEEE Transactions on Vehicular Technology, 2018, PP(99): 1.

[17] FOUDA A E, TEIXIERA F L, YAVUZ M E. Time-reversal techniques for MISO and MIMO wireless communication systems [OL]. http://adsabs. harvard. edu/abs/2012RaSc... 47. 0P02F.

[18] 代彬. 窃听信道及第二类窃听信道的新问题[D]. 上海：上海交通大学，2007.