doi:10.11959/j.issn.1000-436x.2015194

基于人工噪声辅助的 D2D 异构蜂窝安全通信方法

康小磊[1]，季新生[1,2]，黄开枝[1]
（1. 国家数字交换系统工程技术研究中心，河南 郑州 450002；2. 移动互联网安全技术国家工程实验室，北京 100876）

摘 要：针对 D2D 通信安全性受资源限制问题，提出一种基于人工噪声辅助的 D2D 异构蜂窝安全通信方法。首先建立系统可达保密速率模型，然后在基站的蜂窝通信信号中添加人工噪声，以最大化系统保密速率为目标设计蜂窝用户期望信号与人工噪声的波束矢量。同时，基于公平性约束提出一种基站功率分配、期望信号预编码向量以及 D2D 功率控制的联合优化算法。仿真结果表明，相比于传统的 SVD 预编码法和 ZF 方法，此方法下系统可达保密速率最高提升约 2.7 bit·s^{-1}·Hz^{-1}。

关键词：D2D 通信；系统可达保密速率；人工噪声；物理层安全
中图分类号：TN925 **文献标识码**：A

Secure D2D underlaying cellular communication based on artificial noise assisted

KANG Xiao-lei[1], JI Xin-sheng[1, 2], HUANG Kai-zhi[1]
(1. China National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, China;
2. Wireless Technology Innovation Institute, National Engineering Laboratory for Mobile Network Security, Beijing 100876, China)

Abstract: A secure communication scheme based on artificial noise assisted from base station (BS) was proposed to improve the system secrecy rate of the D2D underlaying cellular. Firstly, the system secrecy rate was modeled. Then the BS with multi-antennas added artificial noise (AN) in cellular user's signal as well as designed beam vectors of the desired signal and artificial noise to maximize system secrecy rate. In the end, a joint optimization scheme based on the fairness constraint was introduced to optimize beam vectors of the desired signal, the power allocation for BS's information signal and AN and the D2D power control. Simulation results show that the system ergodic secrecy rate can be improved 2.7 bit·s^{-1}·Hz^{-1} more than the schemes based on SVD and zero-forcing at most.

Key words: D2D; system secrecy rate; artificial noise; physical layer security

1 引言

D2D(device to device)通信是一种基于蜂窝系统的终端直通技术，它允许移动终端在蜂窝系统的控制下使用蜂窝系统授权频段进行点到点通信[1]。由于具有节省终端发射功率、改善边缘用户的服务质量（QoS）、提高系统频谱效率等诸多优势，因此受到越来越多的关注与研究，成为下一代移动通信（5G）的关键技术之一。传统解决 D2D 通信安全性手段主要来自高层加密，但是由于终端天线数、带宽、功率等资源受限，加之无线传输的开放性，D2D 通信仍然难以有效防范物理层窃听问题，将成为移动通信的安全瓶颈，亟待解决。

D2D 通信的研究目前主要集中于性能增益的提升与无线资源管理等方面，而安全性研究还鲜有提及。文献[2]分析了基于 LTE-A 蜂窝系统的 D2D 通信所能面临的可能的安全威胁，并提出了相应的安全构架。文献[3]将 D2D 通信信号当做一种有意

收稿日期：2014-11-08；**修回日期**：2015-02-08
基金项目：国家自然科学基金资助项目（61379006, 61401510, 61471396, 61501516）；国家高技术研究发展计划（“863”计划）基金资助项目（2014AA01A701）
Foundation Items: The National Natural Science Foundation of China (61379006, 61401510, 61471396, 61501516); The National High Technology Research and Development Program of China (863 Program) (2014AA01A701)

的干扰用来对抗窃听，并证明其可以增加蜂窝用户的保密容量。文献[4]将传统蜂窝通信建模为三节点的中继通信，认为 D2D 通信能够减少信息传输次数并降低传输功率，所以具有天然的防窃听优势，并能够带来保密中断概率的降低。基于相同信道资源，文献[5]将蜂窝用户与 D2D 用户联合考虑，衡量相同信道资源下的保密总容量，并给出了相应的基于图论模型的无线信道资源分配算法。以上文献都从不同的侧面研究了 D2D 部署下的蜂窝网安全通信问题，但是还存在 2 个问题：1)简单地将用户干扰当成人工噪声使用，没有充分考虑窃听者高灵敏度窃听的问题，当存在远近效应时窃听者完全可以通过串行干扰消除同时窃取蜂窝用户与 D2D 用户的通信信号；2)没有充分考虑 D2D 的安全问题，当窃听者接近 D2D 用户时，上述所述方法都将无法保证 D2D 通信安全。

针对上述 2 个问题，本文提出一种基于人工噪声辅助的 D2D 异构蜂窝网安全通信方法。首先，通过最小最大准则，建立合理的蜂窝用户与 D2D 用户兼顾的系统可达保密速率模型；然后，借助于基站的多天线辅助，在基站与蜂窝用户的通信信号（期望信号）中添加人工噪声，在满足蜂窝用户的安全服务质量（QoSS, quality of securing service）约束下设计人工干扰和期望信号预编码：人工干扰同时置于蜂窝用户与 D2D 用户的信道零空间，避免对蜂窝用户和 D2D 用户产生干扰；期望信号预编码向量满足对 D2D 用户干扰最小；最后，以最大化系统保密容量为目标优化基站功率分配以及 D2D 功率控制。在此基础上，提出满足系统可达保密速率最大化的基站功率分配以及 D2D 功率控制的联合优化算法。仿真结果表明，相比于传统的 SVD 预编码和 ZF 预编码，本文方法能够获得较高的性能提升，最大提升约 2.7 $\text{bit}\cdot\text{s}^{-1}\cdot\text{Hz}^{-1}$。

命名规则及符号说明如下：A 代表基站，CU_i 代表第 i 个蜂窝用户，DU_i 代表第 i 个 D2D 用户，外部窃听者用 *Eve* 表示，$(\cdot)^{-1}$、$(\cdot)^{\mathrm{T}}$ 以及 $(\cdot)^{\mathrm{H}}$ 分别代表矩阵求逆、转置以及共轭转置，$[\cdot]^+$ 代表 $\max\{\cdot,0\}$，h、$\boldsymbol{h}$、$\boldsymbol{H}$ 分别代表变量、向量和矩阵，$\boldsymbol{I}_M$ 表示对角元素全为 1 的 $M\times M$ 矩阵。

2 系统模型及可达保密速率

2.1 系统模型

基于蜂窝覆盖下的 D2D 通信系统模型如图 1 所示，蜂窝基站配备多天线 N_t，所有合法终端（CU_i 与 DU_i）配备单天线，同时 *Eve* 为了达到窃听目的，配置比普通的终端要高，假设其也配备多天线 N_e。$\boldsymbol{h}_{ac}=(h_{11}\ h_{12}\ \cdots\ h_{1N_t})$ 为从基站 A 到 CU_i 的 $1\times N_t$ 维信道向量，其中元素 h_{1i} 为从基站 A 的第 i 个天线到 CU_i 的信道参数；$\boldsymbol{h}_{ad_1}$，$\boldsymbol{h}_{d_1a}$ 以此类推。$\boldsymbol{H}_{ae}$ 为从基站 A 到 *Eve* 的 $N_e\times N_t$ 维信道矩阵，其中元素 h_{ij} 表示从基站 A 的第 j 个天线到 *Eve* 第 i 个天线的信道参数。$h_{d_1d_2}$、h_{d_1c} 分别为从 DU_{i1} 到 DU_{i2} 和 CU_i 的信道参数。TD-LTE 系统的所有蜂窝用户分配相互正交的频带资源，占用不同的物理资源块（PRB）进行通信。所以蜂窝用户之间不存在相互干扰，D2D 为了最大地提升频谱效率而采用复用模式[1]，即与蜂窝用户共享频带资源进行通信。那么小区间会存在同频干扰（D2D 对蜂窝用户的干扰以及蜂窝对 D2D 的干扰）。为了便于分析，假设所有系统中只有 1 个蜂窝用户和 1 对 D2D 用户，所有资源都分配给该蜂窝用户进行通信。在 t 时刻，A 向 CU_i 传送的信号为 $\boldsymbol{x}_c$，D2D 用户对 DU_{i1} 向 DU_{i2} 传送的信号为 x_{d1}，那么 CU_i、DU_{i2} 以及 *Eve* 接收到的信号分别为

$$y_{ci}=\boldsymbol{h}_{ac}\boldsymbol{x}_c+h_{d_1c}x_{d_1}+n_1 \tag{1}$$

$$y_d=h_{d_1d_2}x_{d_1}+\boldsymbol{h}_{ad_2}\boldsymbol{x}_c+n_2 \tag{2}$$

$$\boldsymbol{y}_e=\boldsymbol{H}_{ae}\boldsymbol{x}_c+\boldsymbol{h}_{d_1e}x_{d_1}+\boldsymbol{n}_3 \tag{3}$$

其中，$n_i(i=1,2)$ 分别为 CU_i 和 DU_{i2} 的信道噪声，服从均值为 0，方差为 1 的复高斯分布；$\boldsymbol{n}_3$ 为高斯噪声向量，其中各元素独立同分布。由式（1）可知，CU_i 接收信号由 3 部分组成：期望信号、来自 DU_{i2} 的干扰信号以及背景噪声；同理 DU_{i2} 也有期望信号 $h_{d_1d_2}x_{d_1}$、来自蜂窝的干扰信号和噪声 3 部分；*Eve* 同时可以窃听蜂窝用户和 D2D 用户，所以其接收也分为 3 部分。

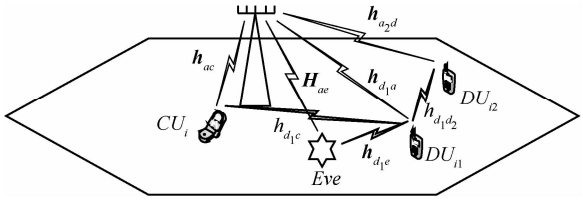

图 1 系统模型

基于物理层安全的保密容量定义为合法用户

与 *Eve* 的互信息之间的差异，即 $\max(I(\boldsymbol{x}_c,\boldsymbol{y}_c)-I(\boldsymbol{x}_c,\boldsymbol{y}_e))$，由信息论可知最大值的获得与输入的分布有关。因此通过衡量 CU_i 和 DU_{i2} 的可达保密速率来衡量安全性能。通过高斯信道容量可知，CU_i 和 DU_{i2} 的可达保密速率 R_{s1} 和 R_{s2} 分别为

$$C_{s1}\geqslant R_{s1}=I(\boldsymbol{x}_c,y_c)-I(\boldsymbol{x}_c,\boldsymbol{y}_e)$$
$$=\log\left(1+SINR_c\right)-\log\left(1+SINR_{ec}\right) \quad (4)$$

$$C_{s2}\geqslant R_{s2}=I(x_{d_1},y_d)-I(x_{d_1},\boldsymbol{y}_e)$$
$$=\log\left(1+SINR_d\right)-\log\left(1+SINR_{ed}\right) \quad (5)$$

其中，C_{s1} 和 C_{s2} 分别为 CU_i 和 DU_{i2} 的保密容量，*SINR* 表示信干噪比。此处假设 *Eve* 具有更加优越的接收性能，即它可以通过功率、调制等不同区分 DU_{i2} 信号和 CU_i 信号，并可以针对性地消除另一种用户信号干扰，选择窃听一种用户。

2.2　系统可达保密速率

文献[5]中将上述 CU_i 与 DU_{i2} 用户的保密容量之和作为系统保密容量，并通过优化无线资源分配最大化系统总的保密容量，该模型最大的不足在于难以刻画单用户的安全性能。而在实际应用中，安全性衡量往往是由最差的用户决定。由式（4）和式（5）可知，在该信道资源上，系统的保密容量应由 CU_i 和 DU_{i2} 最差的性能决定，因此本文定义此信道资源上系统可达保密速率为

$$R_i=\min\{R_{s1},R_{s2}\} \quad (6)$$

若该蜂窝下存在 *M* 个蜂窝用户以及 *K* 对 D2D 用户(所有 D2D 对都采用复用模式)，那么可定义整个蜂窝系统保密吞吐量为

$$T_c=\max\sum_{i=1}^{M}R_i \quad (7)$$

显而易见，系统可达保密速率就是蜂窝用户为 1 时的系统保密吞吐量。为了简化分析，本文暂不讨论多 CU_i 下系统保密吞吐量问题，主要致力于系统可达保密速率的优化，即考虑：$\max\limits_{\boldsymbol{u},p_d}\{\min\{R_{s1},R_{s2}\}\}$。

3　基于人工噪声辅助的 D2D 异构蜂窝网安全通信

从式（4）和式（5）中还可以看到，CU_i 可以借助于基站多天线有效提升自身 *SINR*，但是 DU_{i2} 的可达保密速率完全由 D2D 用户对与窃听者之间的信道质量差异决定。更不幸的是，*Eve* 也可以通过其多天线接收提升接收信噪比，因此 DU_{i2} 的安全性很难得到保证。需要借助其他手段提升 DU_{i2} 或者恶化 *Eve* 的 *SINR* 来提升安全性能。为此，基于文献[6]，在基站侧做如下工作：令 $\boldsymbol{x}_c=\boldsymbol{s}_c+\boldsymbol{z}=\boldsymbol{u}s+\boldsymbol{z}$，即设计蜂窝通信信号由 2 部分组成：期望信号 $\boldsymbol{s}_c$ 与人工噪声 $\boldsymbol{z}$，$\boldsymbol{u}$ 为预编码向量（下文将讨论如何设计），s 为期望传输的有用信号。令人工噪声 $\boldsymbol{z}$ 对 CU_i 和 DU_{i2} 无影响（下文将讨论如何设计）。其中，$\mathrm{E}\{|s|^2\}=p_s=(1-\vartheta)P_0$ 为期望信号功率，ϑ 为功率分配因子；人工噪声信号功率为 $\mathrm{E}\{|z|^2\}=p_z=\vartheta P_0$。综上，可以重写式（1）~式（3）为

$$y_{ci}=\boldsymbol{h}_{ac}\boldsymbol{u}s+h_{d_1c}x_{d_1}+n_1 \quad (8)$$

$$y_d=h_{d_1d_2}x_{d_1}+\boldsymbol{h}_{ad_2}\boldsymbol{u}s+n_2 \quad (9)$$

$$\boldsymbol{y}_e=\boldsymbol{H}_{ae}\boldsymbol{u}s+\boldsymbol{H}_{ae}\boldsymbol{z}+\boldsymbol{H}_{d_1e}x_{d_1}+\boldsymbol{n}_3 \quad (10)$$

由式（4）、式（5）、式（8）~式（10）可得

$$R_{s1}=\log\left(1+\frac{\left\|\boldsymbol{h}_{ac}\boldsymbol{u}\right\|^2}{\sigma_1^2+p_{d_1}\left|h_{d_1c}\right|^2}\right)-$$
$$\mathrm{lb}\det\left[\boldsymbol{I}_{N_e}+\frac{\boldsymbol{H}_{ae}\boldsymbol{u}\boldsymbol{u}^{\mathrm{H}}\boldsymbol{H}_{ae}^{\mathrm{H}}}{\sigma_3^2\boldsymbol{I}_{N_e}+\boldsymbol{H}_{ae}\boldsymbol{z}\boldsymbol{z}^{\mathrm{H}}\boldsymbol{H}_{ae}^{\mathrm{H}}}\right] \quad (11)$$

$$R_{s2}=\log\left(1+\frac{p_{d_1}\left|h_{d_1d_2}\right|^2}{\sigma_2^2+\left\|\boldsymbol{h}_{ad_2}\boldsymbol{u}\right\|^2}\right)-$$
$$\mathrm{lb}\det\left[\boldsymbol{I}_{N_e}+\frac{p_{d_1}\left|\boldsymbol{h}_{d_1e}\boldsymbol{h}_{d_1e}^{\mathrm{H}}\right|}{\sigma_3^2\boldsymbol{I}_{N_e}+\boldsymbol{H}_{ae}\boldsymbol{z}\boldsymbol{z}^{\mathrm{H}}\boldsymbol{H}_{ae}^{\mathrm{H}}}\right] \quad (12)$$

考虑实际情况，本文假设 *Eve* 的信道状态未知，为此，需要考察用户的遍历可达保密速率，即 $\tilde{R}_{s1}=E_{\boldsymbol{H}_{ae}}\{R_{s1}\}$，$\tilde{R}_{s2}=E_{\boldsymbol{H}_{ae},\boldsymbol{h}_{d_1e}}\{R_{s2}\}$。综上，保证系统遍历保密速率最大的优化问题可以建模为

$$\max_{\boldsymbol{u},p_d}\left\{\min\left\{\tilde{R}_{s1},\tilde{R}_{s2}\right\}\right\}$$
$$\text{s.t. } p_s=\mathrm{tr}\{\boldsymbol{u}\boldsymbol{u}^{\mathrm{H}}\}\leqslant(1-\vartheta)P_0$$
$$p_{d_1}\leqslant p_d$$
$$\vartheta\in[0,1] \quad (13)$$

其中，p_d 为 DU_i 的最大传输功率。

为了获得遍历可达保密速率及最优的信号设计方案，首先本文给出如下引理及推论。

引理 1　基于 D2D 的异构蜂窝网的系统遍历可达保密速率存在上界。

证明　对于式（11），等号右边第 1 项 $R_c=$

$\log\left(1+\dfrac{\left\|\boldsymbol{h}_{ac}\boldsymbol{u}\right\|^2}{\sigma_1^2+p_{d_1}\left|h_{d_1c}\right|^2}\right)$，当基站发送功率 $P_0\to\infty$ $R_c\to\infty$；第 2 项 $R_{ec}=\mathrm{lb}\det\left[\boldsymbol{I}_{N_e}+\dfrac{\boldsymbol{H}_{ae}\boldsymbol{u}\boldsymbol{u}^{\mathrm{H}}\boldsymbol{H}_{ae}^{\mathrm{H}}}{\sigma_3^2\boldsymbol{I}_{N_e}+\boldsymbol{H}_{ae}\boldsymbol{z}\boldsymbol{z}^{\mathrm{H}}\boldsymbol{H}_{ae}^{\mathrm{H}}}\right]$，当 $P_0\to\infty$ 时，是只与 ϑ 有关的常数，所以当 $P_0\to\infty$ 时 $R_{s1}\to\infty$；当 $P_0\to 0$ 时，显而易见 $R_{s1}\to 0$。

对于式 (12)，等号右边第 1 项 $R_d=\log\left(1+\dfrac{p_{d_1}\left|h_{d_1d_2}\right|^2}{\sigma_2^2+\left\|\boldsymbol{h}_{ad_2}\boldsymbol{u}\right\|^2}\right)$，当 $P_0\to\infty$ 时 $R_d\to 0$，第 2 项，$R_{ed}=\mathrm{lb}\det\left[\boldsymbol{I}_{N_e}+\dfrac{p_{d_1}\left|\boldsymbol{h}_{d_1e}\boldsymbol{h}_{d_1e}^{\mathrm{H}}\right|}{\sigma_3^2\boldsymbol{I}_{N_e}+\boldsymbol{H}_{ae}\boldsymbol{z}\boldsymbol{z}^{\mathrm{H}}\boldsymbol{H}_{ae}^{\mathrm{H}}}\right]$，当 $P_0\to\infty$ 时，$R_{ed}\to 0$，因此，当 $P_0\to\infty$ 时，$R_{s2}\to 0$；当 $P_0\to 0$ 时，显而易见 $R_{s2}\to\zeta$，其中 $\zeta=\log\left(1+\dfrac{p_{d_1}\left|h_{d_1d_2}\right|^2}{\sigma_2^2}\right)$，在 D2D 用户对信道与发送功率一定时为常数。

综上，有 $\lim\limits_{P_0\to\infty}R_s=0$ 且 $\lim\limits_{P_0\to 0}R_s=0$。由 $\log(\cdot)$ 函数的连续可导性可知，R_s 在功率域上存在上界。即 $R_s=\max\limits_{P_0}\{\min\{R_{s1},R_{s2}\}\}\leqslant R_s^{\max}$，证毕。

推论 1 功率受限的 D2D 异构蜂窝网的系统可达保密速率存在唯一极大值，并且等于最优解。

证明 重写式 (11) 和式 (12)：$\tilde{R}_{s1}=\log(1+\alpha\boldsymbol{h}_{ac}\boldsymbol{Q}_{\boldsymbol{u}}\boldsymbol{h}_{ac}^{\mathrm{H}})-\mathrm{E}_{\boldsymbol{H}_{ae}}\left\{\mathrm{lb}\left|\boldsymbol{I}_{N_e}+\boldsymbol{N}\boldsymbol{H}_{ae}\boldsymbol{Q}_{\boldsymbol{u}}\boldsymbol{H}_{ae}^{\mathrm{H}}\right|\right\}$，其中，$\alpha=\dfrac{1}{\sigma_1^2+p_{d_1}\left|h_{d_1c}\right|^2}$，$\boldsymbol{N}=\dfrac{\boldsymbol{I}_{N_e}}{\sigma_3^2\boldsymbol{I}_{N_e}+\boldsymbol{H}_{ae}\boldsymbol{z}\boldsymbol{z}^{\mathrm{H}}\boldsymbol{H}_{ae}^{\mathrm{H}}}$，$\boldsymbol{Q}_{\boldsymbol{u}}=\boldsymbol{u}\boldsymbol{u}^{\mathrm{H}}$ 为期望信号功率协方差。由文献[7]中的引理 2 可知，$\tilde{R}_{s1}$ 为输入协方差的凸增函数；对于 $\tilde{R}_{s2}$，第 2 项与 $\boldsymbol{Q}_{\boldsymbol{u}}=\boldsymbol{u}\boldsymbol{u}^{\mathrm{H}}$ 无关，利用 $\dfrac{\partial\boldsymbol{h}_{ad_2}\boldsymbol{Q}_{\boldsymbol{u}}\boldsymbol{h}_{ad_2}^{\mathrm{H}}}{\partial\boldsymbol{Q}_{\boldsymbol{u}}}=p_s\boldsymbol{h}_{ad_2}\boldsymbol{h}_{ad_2}^{\mathrm{H}}$，对 $\tilde{R}_{s2}$ 求导，得：$\dfrac{\partial\tilde{R}_{s2}}{\partial\boldsymbol{Q}_{\boldsymbol{u}}}=\dfrac{-\beta p_s\boldsymbol{h}_{ad_2}\boldsymbol{h}_{ad_2}^{\mathrm{H}}}{\boldsymbol{h}_{ad_2}\boldsymbol{Q}_{\boldsymbol{u}}\boldsymbol{h}_{ad_2}^{\mathrm{H}}\left(\boldsymbol{h}_{ad_2}\boldsymbol{Q}_{\boldsymbol{u}}\boldsymbol{h}_{ad_2}^{\mathrm{H}}+\beta\right)}$，显而易见，有 $\dfrac{\partial\tilde{R}_{s2}}{\partial\boldsymbol{Q}_{\boldsymbol{u}}}<0$，即 D2D 用户对的遍历保密速率为基站有用信号发送功率的凸减函数。加上引理 1 则可知，保密速率在功率受限 $(0,P_0]$ 上必然存在极大值，而且此时的极大值就是最大值，并且在 $\tilde{R}_{s1}$ 与 $\tilde{R}_{s2}$ 的相交处取得，得证。

3.1 噪声设计

为了保证合法用户 CU_i 与 DU_{i2} 的接收不受人工噪声影响，首先需要设计人工噪声 $\boldsymbol{z}$，让其满足与合法用户信道正交，最简单的设计可参考文献[6]中的零陷成形，即通过预编码将人工噪声信号置于合法用户 CU_i 和 DU_{i2} 信道的零空间中，即 $\left(\boldsymbol{h}_{ad_1},\boldsymbol{h}_{ad_2},\boldsymbol{h}_{ac}\right)\boldsymbol{z}=\boldsymbol{0}$，为此设计 $\boldsymbol{z}=\boldsymbol{V}\boldsymbol{w}$，其中，$\boldsymbol{V}$ 是预编码矩阵，可以设计为合法用户信道的零空间的正交基所构成的编码矩阵；$\boldsymbol{w}$ 可以设计为随机产生的 $(N_t-3)\times 1$ 维的人工噪声向量，其元素相互独立，满足期望为 0，功率为 σ^2 的高斯分布。因此有：$p_z=(N_t-3)\sigma^2$。

3.2 期望信号设计

期望信号预编码为：$\boldsymbol{s}_c=\boldsymbol{u}s$，其中，$\boldsymbol{u}$ 为预编码向量，s 为期望传输的有用信号。期望信号的预编码可以分为 2 种极端情况：一种是满足到蜂窝用户信噪比最大准则，即基于 SVD 分解的波束成形或信道滤波 $\boldsymbol{u}=\dfrac{\boldsymbol{h}^{\mathrm{H}}}{\|\boldsymbol{h}\|}$ [8]；另一种是满足对 D2D 设备无干扰准则，即零空间分解：$\boldsymbol{u}\in\mathrm{null}(\boldsymbol{h}_{ad_1},\boldsymbol{h}_{ad_2})$。最优的预编码向量应使两类用户安全性能较为均衡，即最优的结果为 $\max\limits_{\boldsymbol{u}}\left\|\boldsymbol{h}_{ab}\boldsymbol{u}\right\|\ \&\ \min\limits_{\boldsymbol{u}}\left\|\boldsymbol{h}_{ad}\boldsymbol{u}\right\|$。由于实际中基站发射功率远大于 DU_i，对 D2D 干扰较强，为此将上述优化进行 2 种适当变换：1）严格约束基站期望信号对 DU_i 无影响，并最大化 CU_i 接收功率；2）期望信号接收功率满足一定阈值，最小化对 DU_i 干扰。

对于第 1 种情况，预编码优化问题可以建模如下

$$\max_{\boldsymbol{u}}\left|\boldsymbol{h}_{ab}\boldsymbol{u}\right|\quad \text{s.t.}\begin{cases}\left|\boldsymbol{h}_{ad}\boldsymbol{u}\right|=0\\ p_s=\mathrm{tr}\{\boldsymbol{u}\boldsymbol{u}^{\mathrm{H}}\}=(1-\vartheta)P_0\end{cases}\tag{14}$$

该优化问题可以通过文献[9]简单求解

$$\boldsymbol{u}=\frac{\sqrt{(1-\vartheta)\ P_0}}{\left\|\left(\boldsymbol{I}_N-\boldsymbol{P}_{ad}\right)\boldsymbol{h}_{ab}^{\dagger}\right\|}\left(\boldsymbol{I}_N-\boldsymbol{P}_{ad}\right)\boldsymbol{h}_{ab}^{\dagger}$$

其中，$\boldsymbol{P}_{ad}=\ \boldsymbol{h}_{ad}^{\mathrm{H}}\left(\boldsymbol{h}_{ad}\boldsymbol{h}_{ad}^{\mathrm{H}}\right)^{-1}\boldsymbol{h}_{ad}$。

第 2 种情况，由于

$$\boldsymbol{h}_{ac}\boldsymbol{u}\boldsymbol{u}^{\dagger}\ \boldsymbol{h}_{ac}^{\dagger}\leqslant(1-\vartheta)P_0\left\|\boldsymbol{h}_{ac}\right\|^2=(1-\vartheta)P_0\lambda_{\max}$$

其中，$\lambda_{\max}$ 为 $\boldsymbol{h}_{ac}$ 的最大奇异值[7]，设定基站在 CU_i 处接收功率受限于 γ_0，那么建模如下

$$\min_{\boldsymbol{u}} \left|\boldsymbol{h}_{ad}\boldsymbol{u}\right| \quad \text{s.t.} \begin{cases} \left|\boldsymbol{h}_{ac}\boldsymbol{u}\right|=\gamma_0 \leqslant \lambda_{\max}\sqrt{(1-\vartheta)P_0} \\ p_s=\mathrm{tr}\{\boldsymbol{u}\boldsymbol{u}^{\mathrm{H}}\}=(1-\vartheta)P_0 \end{cases} \tag{15}$$

当阈值 γ_0 固定后，式(15)的变量只剩下 $\boldsymbol{u}$，其求解可参考文献[7]中的式(26)。式(14)的物理意义就是让蜂窝用户期望信号的波束零空间对准 D2D，达到的效果是对 D2D 干扰最小，但是这样的处理导致蜂窝用户性能的提升受到很大限制；而式(15)是在引入适当对 D2D 用户的干扰时，保证蜂窝用户一定性能，可以通过调节阈值 γ_0 使这两者平衡。基于此，本文提出的算法将采用式（15）的优化模型。

3.3　基站功率分配

由式(12)和式(13)可知，干扰功率分配越大，*Eve* 所受到的干扰越严重，对于 DU_i 带来安全增益远大于 CU_i，如果干扰功率进一步增大，那么期望信号功率过小则可能会带来 CU_i 的安全性能损失，因此需要寻求最佳的分配比例。为此，独立分析这 2 种用户的保密速率：首先对于 CU_i，在不考虑 DU_i 干扰情况下，CU_i 的窃听模型是典型的 MISOME 模型，文献[10]通过定理 2 证明了当 *Eve* 信道已知时，最佳的功率分配方案为将所有的功率分配给期望信号，并且当期望信号预编码为 $\boldsymbol{u}=\boldsymbol{u}_{\lambda_{\max}}$ 时，保密速率最大，其中 $\lambda_{\max}$ 为 $(I_N+\boldsymbol{h}_{ac}^{\dagger}\boldsymbol{h}_{ac}, I_N+\boldsymbol{H}_{ae}^{\dagger}\boldsymbol{H}_{ae})$ 的最大广义特征值，$\boldsymbol{u}_{\lambda_{\max}}$ 为 $\lambda_{\max}$ 所对应的广义特征向量。当 *Eve* 信道未知时，文献[8]证明了最佳的功率分配比例只与发送功率以及发送天线数有关，低信噪比时将更多功率分配给期望信号是最佳策略；其次，对于 DU_i，可以建模为最简单的三节点窃听模型，在没有蜂窝干扰的情况下该模型的安全性仅仅依赖合法用户与窃听方信道质量的差异。因此为了恶化 *Eve* 接收信道，需要对 *Eve* 注入更多的干扰才能保证 DU_i 的安全。综上，本文模型下的最佳功率分配需要与 DU_i 的功率控制联合考虑。

3.4　DU_i 功率控制

由式（12）和式（13）可知，两类用户的可达保密速率相互影响。经过上述信号设计后，基站以平衡可达保密速率为目标，对 DU_i 进行功率控制，DU_i 的功率大小应随信道变化而变化。提升 DU_i 功率能够带来 DU_i 可达保密速率的提升但是势必降低 CU_i 的可达保密速率，这一对矛盾的最佳平衡就需要通过基站侧的控制来实现。为了获得最佳的可达保密速率，需要满足 R_{s1} 与 R_{s2} 二者之差不能太大，因此给出如下公平性约束

$$\left|\tilde{R}_{s1}-\tilde{R}_{s2}\right| \leqslant \frac{1}{\xi} \tag{16}$$

其中，ξ 为安全服务公平因子，衡量系统中用户的安全服务公平性，取值越大，系统用户之间的公平性越好。上式表明基站应该通过功率分配及 DU_i 功率控制，使 CU_i 与 DU_i 的可达保密速率满足一定的公平性要求。进一步地，在 *Eve* 信道信息未知情况下，公平性应该满足如下要求

$$\left|\frac{\left\|\boldsymbol{h}_{ac}\boldsymbol{u}\right\|^2}{\sigma_1^2+p_{d_1}\left|h_{d_1c}\right|^2}-\frac{p_{d_1}\left|h_{d_1d_2}\right|^2}{\sigma_2^2+\left\|\boldsymbol{h}_{ad_2}\boldsymbol{u}\right\|^2}\right| \leqslant \frac{1}{\zeta} \tag{17}$$

3.5　联合优化随机搜索算法

基于 3.2 节和 3.3 节的分析，本文给出基于可达保密速率最大化的基站功率分配及 DU_i 功率控制联合优化的随机搜索算法。

算法 1　联合优化随机搜索算法

1) 设定初始值 p_d、P_0、ϑ、γ_0、ξ，按照 3.1 节零空间分解法求出 $\boldsymbol{z}$。

2) 按照式(15)求出 $\boldsymbol{u}$，并按照式(6)、式(11)、式(12)求出 $\tilde{R}_s$。

3) 固定 $\boldsymbol{u}$，按照式(17)求出 p'_{d_1}，计算此时 $\tilde{R}_s'$，若 $\tilde{R}_s' \geqslant R_s$，更新 $p_{d_1}=p'_{d_1}$。

4) 固定 $p_{d_1}=p'_{d_1}$，按照（15）式求出 $\boldsymbol{u}'$，计算出 R_s''，若 $R_s'' \geqslant R_s'$，更新 $\boldsymbol{u}=\boldsymbol{u}'$。

5) 重复迭代步骤 3）和步骤 4），直至收敛。

6) ϑ 添加扰动 $\vartheta'=\vartheta+\Delta$，并求出添加扰动之后的 $\tilde{R}_s$，若较之前性能有所提升，那么更新 ϑ，并返回步骤 2）；若不再增加，那么 ϑ 为最优值。

4　数值结果

这部分将采用数值仿真验证上文的理论分析。为了简化分析，建立一维的圆形蜂窝网，网络拓扑如图 2 所示，基站位于原点，CU_i 离基站较近，DU_i 位于蜂窝边缘，*Eve* 在蜂窝中的位置随机布设。所有信道假设服从路径损耗模型[注1]：由距离衰落和随

注1　必须说明的是，实际蜂窝环境中对信道的处理应该考虑多径衰落，此处考虑到只要合法用户与窃听者信道模型相同，即信道模型不影响本文方法效果，所以采用简单的路损模型。

机相位 2 部分组成，即 $h_{ij}=d_{ij}^{\frac{-k}{2}}\mathrm{e}^{\mathrm{j}\varphi}$，其中 d_{ij} 为 i 到 j 的距离，k 为尺度衰落因子，文中取 k=3.5，φ 为服从 $(0,2\pi]$ 均匀分布的随机相位。基站天线数为 N_t=8，N_e=4。CU_i 的坐标为（3,0），DU_1 的坐标为（5,1），DU_2 的坐标为（5,0），每次实验 *Eve* 的坐标在蜂窝覆盖范围内随机选取，实验次数 10 000 次。$\tilde{\zeta}$=5，$\gamma_0=0.7\lambda_{\max}\sqrt{(1-\vartheta)P_0}$。

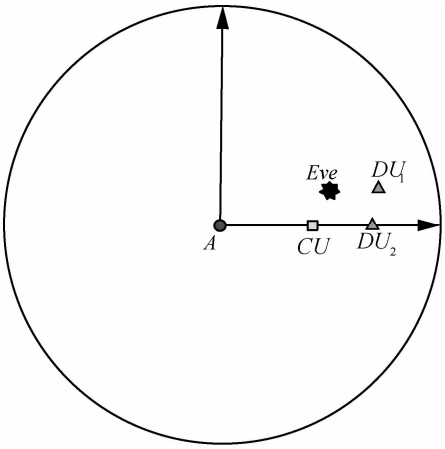

图 2 仿真拓扑

设定基站发射功率为 10，D2D 发送功率为 1，基于SVD波束成形与ZF分解方法下的*CU* 与*DU* 的可达保密速率随功率分配因子变化如图 3 所示。当采用 SVD 波束成形时，*CU* 的可达保密速率远高于 *DU* 用户，并且比采用 ZF 方法高，差值最大为 4.1 bit·s^{-1}·Hz^{-1}（θ=0），但是此时 D2D 的可达保密速率却远低于零空间分解法，差值最大为 1.8 bit·s^{-1}·Hz^{-1}；采用 ZF 方法时 *DU* 的可达保密速率高于 *CU*，并且比采用 SVD 波束成形方法高，当功率分配因子等于 0.3 时提升了 1 bit·s^{-1}·Hz^{-1}，但是此时 *CU* 的可达保密速率却远低于零空间分解法。上述结果也是与实际理论相符合的：SVD 波束成形是以最大化 *CU* 的速率为目标，因此会对 *DU* 产生严重干扰；ZF 分解是以最小化 *DU* 干扰为目标，因此会大大降低 *CU* 的速率，与 3.2 节的分析一致。

为了验证引理 1 的结论，设定 D2D 发送功率为 1，功率分配因子 θ=0.5，基于 ZF 分解方法，基站发射功率从 10 W 开始以 10 个单位为间隔取到 100 W，*CU* 与 *DU* 可达保密速率随基站功率变化如图 4 所示，随着发送功率的增大，*CU* 的可达保密速率持续增大，但是 *DU* 的可达保密速率在功率为 50 dB 时达到 7.5 bit·s^{-1}·Hz^{-1}，之后不再增加。考虑式(12)可知，当功率增大到 50 dB 时，第 2 项 *Eve* 的速率几乎已经为零，而第 1 项在零空间基础上将与功率无关，因此 *DU* 的可达保密速率将趋近于其通信速率，与引理结论一致。

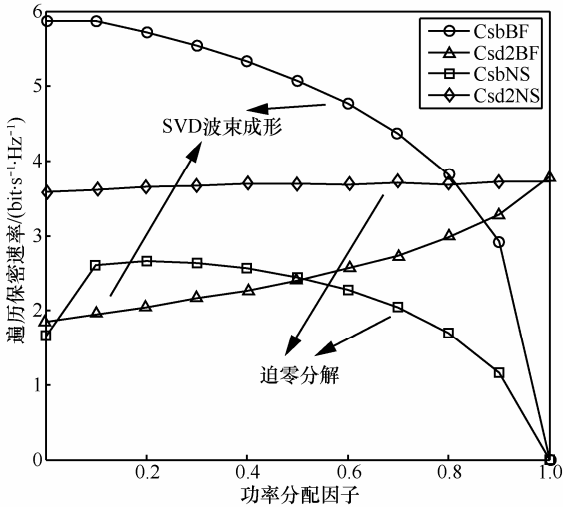

图 3 不同用户的可达保密速率随功率分配因子变化

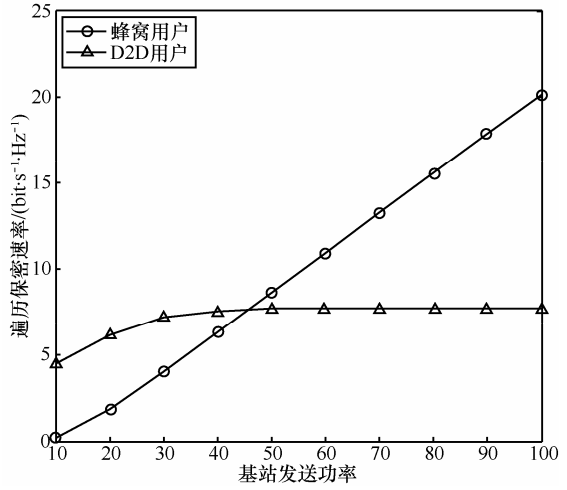

图 4 *CU* 与 *DU* 可达保密速率随基站功率变化情况

图 5 和图 6 分别分析了 SVD 波束成形方法和 ZF 分解方法下用户可达保密速率随 *DU* 发射功率变化情况，并同时分为添加噪声（θ=0.5）和不添加噪声（θ=0）2 种情况考虑。总体而言，随着 *DU* 功率的增大，*CU* 的可达保密速率受到干扰也在增大，因此可达保密速率一直下降，而 *DU* 的保密速率持续提升。此外可以看出，无论哪种方法，添加人工噪声都能够提高 *DU* 的可达保密速率，但是基于 SVD 波束成形方法时添加人工噪声反而降低了 *CU* 的可达保密速率，该结果在图 3 中已有所反映，产生原因在于当 *Eve* 信道

状态未知时，将更多功率传向 *CU* 的策略是最佳的，因此当分出一半功率进行干扰时，干扰所能带来的安全增益没有损失的增益大。因此可达保密速率不升反降。

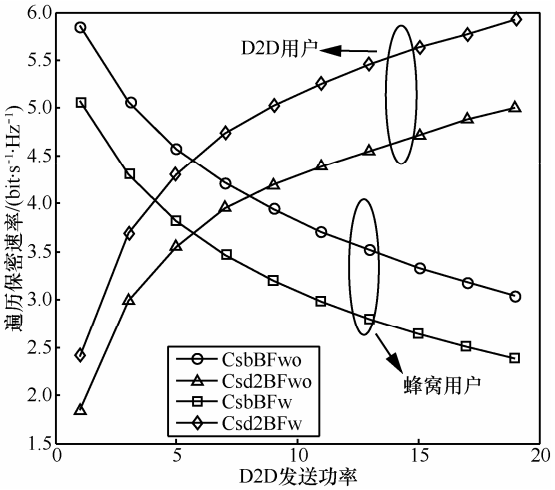

图 5　基于 SVD 波束成形方法下的用户保密容量随 *DU* 发送功率变化情况（w：有人工噪声；wo：无人工噪声）

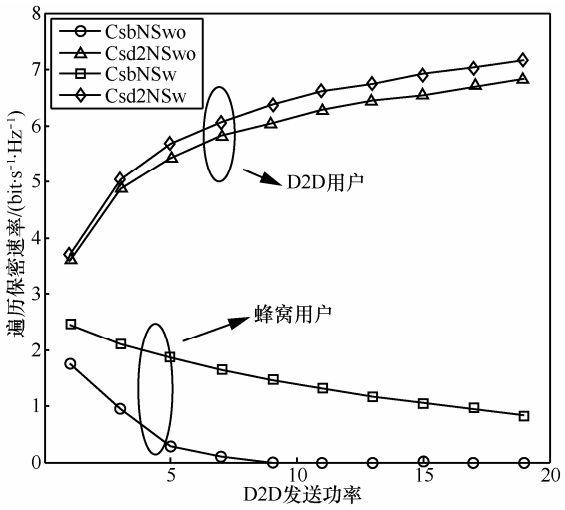

图 6　基于 ZF 分解方法的可达保密速率随 *DU* 发射功率变化情况（w：有人工噪声；wo：无人工噪声）

图 7 给出了本文算法与 SVD 波束成形以及 ZF 分解方法下的系统可达保密速率对比。从图中可以看出，当功率分配因子在 0.7 以下时，本文方法均优于传统的 2 种方法，当分配因子大于 0.7 时，本文方法依旧大于SVD波束成形方法，但是不及ZF 分解方法。这是因为，随着噪声功率比例的不断增大，本文算法下 *CU* 用户的可达保密速率下降很快并低于 *DU* 用户的可达保密速率，此时 *CU* 用户的可达保密速率决定系统可达保密速率；相反地，ZF 分解方法能够持续提升 *DU* 用户的保密速率（如图 3 所示），同时 *CU* 用户的安全性能下降速度慢于本文方法，所以系统性能略高于本文算法。但是，显而易见地，图中所示的 2 种传统方法的系统最大可达保密速率皆没有本文方法高，加之考虑到 *CU* 用户的服务质量，不能将噪声功率分配太大，造成性能损失，因此最佳点可以选择 θ=0.1，此时本文方法比迫零方法高 1 bit·s^{-1}·Hz^{-1}，比零空间分解方法高 2.7 bit·s^{-1}·Hz^{-1}。

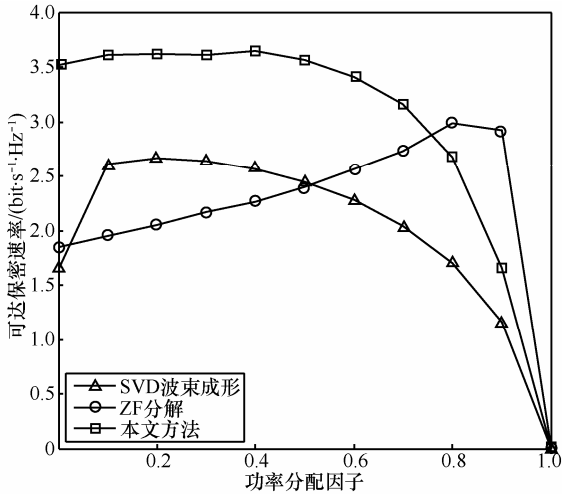

图 7　本文方法下的系统保密容量与传统方法对比

此外，还衡量了 *DU* 距离对用户保密速率的影响。如图 8 所示，横坐标为 D2D 之间距离与基站到蜂窝用户距离之比，随着 *DU* 用户距离的增大，*DU* 的保密速率急剧下降，当距离增大到基站到蜂窝用户距离的一半（0.5）时保密速率为零，但是 *CU* 的保密速率几乎不受影响。因此基站在确定用户是否采取 D2D 通信模式时还应考虑用户之间的通信距离是否满足保密要求。

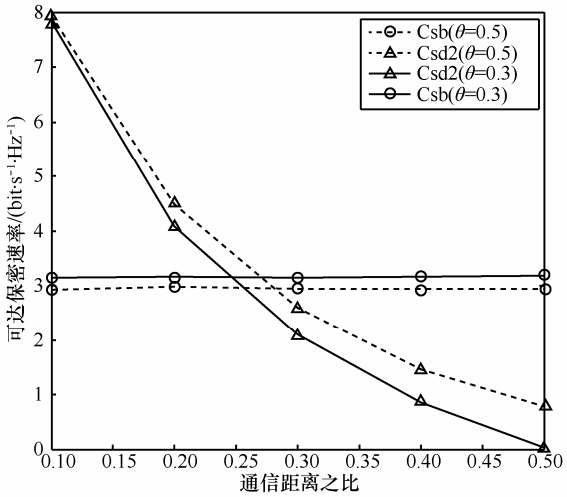

图 8　D2D 距离对可达保密速率的影响

5 结束语

本文针对 D2D 部署下异构蜂窝网通信存在的 2 个安全问题，提出了一种基于人工噪声辅助的 D2D 异构蜂窝网安全通信方法。借助于基站的多天线资源，在蜂窝通信信号中添加人工噪声，通过设计蜂窝用户期望信号与人工噪声的波束矢量，同时达到对蜂窝用户和 D2D 用户对的防窃密保护。在此基础上，提出一种基于公平性约束的联合优化随机搜索算法来获得最优的基站功率分配、期望信号预编码向量以及 D2D 功率控制策略。仿真结果表明，相比于传统的 SVD 预编码法和 ZF 预编码方法本文方法具有较高的性能提升。在未来的工作中，将对多用户的 D2D 异构蜂窝系统的安全吞吐量问题做进一步研究。

参考文献：

[1] JANIS P, YU C H, DOPPLER K, *et al*. Device-to-device communication under-laying cellular communications systems[J]. International Journal Communications Network and System Sciences, 2009, 2(3): 169-178.

[2] ALAM M, DU YANG, RODRIGUEZ J, *et al*. Secure device-to-device communication in LTE-A[J]. IEEE Communications Magazine, 2014, 52(4): 66-73.

[3] YUE J T, MA C, YU H, *et al*. Secrecy-based channel assignment for device-to-device communication: an auction approach[A]. 2013 International Conference on Wireless Communications & Signal Processing (WCSP)[C]. Hangzhou, China, 2013. 1-6.

[4] ZHU D H, SWINDLEHURST A L, FAKOORIAN S A A, *et al*. Device-to-device communications: the physical layer security advantage[A]. 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)[C]. Florence, 2014. 1606-1610.

[5] ZHANG H, WANG T Y, SONG L Y, *et al*. Radio resource allocation for physical-layer security in D2D underlay communications[A]. 2014 IEEE International Conference on Communications (ICC)[C]. Sydney, NSW, 2014.2319-2324.

[6] GOEL S, NEGI R. Guaranteeing secrecy using artificial noise[J]. IEEE Transactions on Wireless Communications, 2008, 7(6): 2180-2189.

[7] LI J Y, PETROPULU A P. On ergodic secrecy rate for gaussian MISO wiretap channels[J]. IEEE Transactions on Wireless Communications, 2011, 10(4): 1176-1187.

[8] XIONG Q, GONG Y, LIANG Y C, *et al*. Achieving secrecy of MISO fading wiretap channels via jamming and precoding with imperfect channel state information[J]. IEEE Wireless Communications Letters, 2014, 3(4): 357-360.

[9] DONG L, HAN Z, PETROPULU A P, *et al*. Improving wireless physical layer security via cooperating relays[J]. IEEE Transactions on Signal Processing, 2010, 58(3): 1875-1888.

[10] KHISTI A, WORNELL, GREGORY W. Secure transmission with multiple antennas—part I: the MISOME wiretap channel[J]. IEEE Transactions on Information Theory, 2010, 56(7): 3088-3104.

作者简介：

康小磊（1986-），男，陕西咸阳人，国家数字交换系统工程技术研究中心博士生，主要研究方向为无线物理层安全、D2D 通信等。

季新生（1968-），男，江苏南通人，国家数字交换系统工程技术研究中心教授、博士生导师，主要研究方向为移动通信网络、拟态安全等。

黄开枝（1973-），女，安徽滁州人，国家数字交换系统工程技术研究中心教授、博士生导师，主要研究方向为移动通信网络、物理层安全等。