

# 基于链路间干扰辅助的 中继 D2D 系统安全通信方法

朱 宸, 黄开枝, 康小磊, 钟 州

(国家数字交换系统工程技术研究中心, 河南郑州 450002)

**摘要:** 在包含中继节点的 D2D (Device-to-Device) 系统中, 针对蜂窝链路与 D2D 链路同时受窃听的问题, 提出一种基于链路间干扰辅助的中继 D2D 系统安全通信方法. 首先, 确定蜂窝链路与 D2D 链路上下行发送模式; 然后, 在基站与中继节点的发送信号中添加人工噪声, 协作干扰窃听器; 最后, 对基站功率分配与 D2D 功率控制进行了优化, 以实现不同类型链路间干扰辅助保障系统安全. 仿真结果表明, 所提出的安全通信方法在保密速率方面比 SVD (Singular Value Decomposition) 与 ZF (Zero-Forcing) 预编码方法提高了 1.5 bit/s/Hz.

**关键词:** D2D 通信; 窃听器; 人工噪声; 保密速率

**中图分类号:** TN925      **文献标识码:** A      **文章编号:** 0372-2112 (2017)06-1443-06

**电子学报 URL:** <http://www.ejournal.org.cn>      **DOI:** 10.3969/j.issn.0372-2112.2017.06.023

## Jamming Based Secure Relay-Aided D2D Transmission Method

ZHU Chen, HUANG Kai-zhi, KANG Xiao-lei, ZHONG Zhou

(China National Digital Switching System Engineering & Technological R&D Center, Zhengzhou, Henan 450002, China)

**Abstract:** To cope with eavesdropping in both the cellular link and the D2D (Device-to-Device) link of relay-aided D2D system, this paper proposes a jamming based secure transmission method. Firstly, the transmission procedures of both the cellular link and the D2D link are modeled. Secondly, an artificial noise (AN) is added into the signal of the base station (BS) and the relay to interfere the eavesdropper. Finally, a joint optimization scheme for the power allocation of BS and the power control of D2D is introduced to maximize the system secrecy rate. Simulation results show that the system ergodic secrecy rate is increased by 1.5 bit/s/Hz, which is great improvement compared with the scheme based on SVD and ZF.

**Key words:** D2D; secure transmission method; artificial noise; secrecy rate

## 1 引言

终端直通技术 (D2D, Device-to-Device) 就是基站 (BS, Base Station) 通过控制链路给间隔距离近、对蜂窝链路干扰小的用户终端 (UE, User Equipment) 分配资源, 使 UE 间直接进行数据通信的一种新型技术. 由于能够提高频谱利用率、节省终端发射功率并分流传统蜂窝数据流量, D2D 通信已被认为是未来 5G 通信系统中, 增强蜂窝网络性能的技术之一<sup>[1]</sup>. 然而, 现有研究成果大多认为 D2D 用户间距离较近时才符合直通条件, 而当 D2D 用户间距离较大时, 链路质量较差, 大大限制了 D2D 通信的实用性.

当无线通信直达链路质量较差时, 可通过建立中

继链路的方法改善用户通信质量. 文献[2]在源、目的节点与中继节点均装备单天线的系统中, 以能量效率最大化同时保证一定的频谱效率为目标分析了源节点与中继节点的最佳发送功率. 文献[3]将多输入多输出 (MIMO, Multiple-Input Multiple-Output) 技术与中继技术进行结合, 在装备 MIMO 系统的源、目的节点之间引入 MIMO 中继进行放大转发 (AF, Amplify-and-Forward), 并以系统容量最大化的下界与最小均方误差的上界为限制条件, 针对发送过程中源节点与中继的联合功率分配问题进行了研究. 文献[4]同样在进行 AF 的 MIMO 中继系统中, 以能量效率最大化为目标对 MIMO 源节点与 MIMO 中继进行了联合功率分配优化. 文献[5]研究了多个装备多天线的系统的中继组成双向中继系统辅助

两个用户进行通信的场景,并假设下行接收用户可以窃听上行发送用户的信息,并以加权最小均方误差最小化为原则设计了协作中继系统发送预编码矩阵.现有研究表明,中继通信技术可以有效改善直达链路通信质量差的问题.

有学者针对 D2D 直达链路距离受限的问题,提出将中继技术引入 D2D 通信.文献[6]分析了 D2D 直达链路中断概率受限的情况下,引入中继的必要性,阐述了如何选择中继节点、中继与 D2D 用户间的工作模式选择等问题,并通过仿真验证了中继的引入能够提升 D2D 通信系统覆盖范围.文献[7]提出了一种 D2D 场景下的中继选择算法.文献[8]分析了引入中继对 D2D 网络容量与覆盖率的影响.研究现有文献不难发现,在 D2D 通信中引入中继能够改善通信质量,解决 D2D 通信距离受限的问题.因此,中继 D2D 系统在未来 5G 移动通信中有较好的应用前景.

但 D2D 技术在快速发展的同时也面临着被窃听、被干扰等安全问题.目前已有学者开始关注 D2D 通信的安全问题.文献[9]分析了 D2D 设备发现过程,并在 LTE 框架下提出一种基于物理层信号设计的设备发现方案,筛选安全可靠的设备接入网络.文献[10]将 D2D 用户的信号视为对窃听者的干扰,并基于拍卖理论设计了一种信道分配方案.文献[11]同样将 D2D 用户的信号视为对窃听者的干扰,根据不同 D2D 用户对窃听者干扰的强弱设计了一种考虑系统安全性的设备接入方案.文献[12]建立了包含一对 D2D、一个窃听者、一个 BS 的四节点模型,并认为用户工作于 D2D 模式下能够减少信号暴露次数,具有天然的抗窃听优势.文献[13]认为,在受窃听的蜂窝网络中引入 D2D 能够提高频谱利用率,但会干扰蜂窝用户(CU, Cellular User).为此,文献[13]对 D2D 用户与蜂窝用户的匹配问题进行分析,使配对后的系统保密速率最大.以上文献从不同侧面对 D2D 通信的安全问题进行了研究,但并未考虑 D2D 通信中引入中继后,信号由一跳传输变为两跳传输,增加了信号被窃听者获取的可能.

针对以上安全问题,本文提出一种基于链路间干扰辅助的中继 D2D 系统安全通信方法.首先,确定蜂窝链路与 D2D 链路上下行信号发送模式:BS 向蜂窝用户发送信号时, D2D 用户向中继节点(Relay)发送信号; Relay 向 D2D 用户转发信号时, CU 向 BS 发送信号.然后,分别在 BS 与 Relay 的发送信号中添加人工噪声对窃听者 Eve 进行协作干扰.最后,在 CU 的安全服务质量(QoS, Quality of Securing Service)约束下设计人工噪声和期望信号预编码,并以最大化系统保密速率为目标,优化总功率受限时期望信号与人工噪声的功率分配比例以及 D2D 发送功率控制.仿真结果表明,应用本

文所提出的方法时系统保密速率比应用奇异值分解(SVD, Singular Value Decomposition)<sup>[14]</sup>与迫零(ZF, Zero-Forcing)<sup>[15]</sup>两种传统方法时提升了 1.5bit/s/Hz.

## 2 系统模型

中继 D2D 系统如图 1 所示,包含一个 BS、一个 CU、一个 Relay 与一对 D2D 用户. BS、Relay 与 Eve 装备天线数分别为  $N_B$ 、 $N_R$  与  $N_E$  的多天线系统.合法终端(CU 与  $D_T$ 、 $D_R$ )由于尺寸限制均装备单天线.  $\mathbf{H}_{BC} = [h_{11}, h_{12}, \dots, h_{1N_B}]$  为从 BS 到 CU 的  $1 \times N_B$  维信道矩阵,其中的元素  $h_{1i}$  表示由 BS 的第  $i$  根发送天线与 CU 接收天线所构成信道的信道参数.  $\mathbf{H}_{RD_T}$ 、 $\mathbf{H}_{RD_R}$ 、 $\mathbf{H}_{BD_T}$ 、 $\mathbf{H}_{BD_R}$ 、 $\mathbf{H}_{CD_T}$ 、 $\mathbf{H}_{CD_R}$ 、 $\mathbf{H}_{BR}$ 、 $\mathbf{H}_{RE}$ 、 $\mathbf{H}_{D_T E}$ 、 $\mathbf{H}_{D_R E}$ 、 $\mathbf{H}_{CE}$ 、 $h_{D_T C}$ 、 $h_{D_R C}$  依此类推.

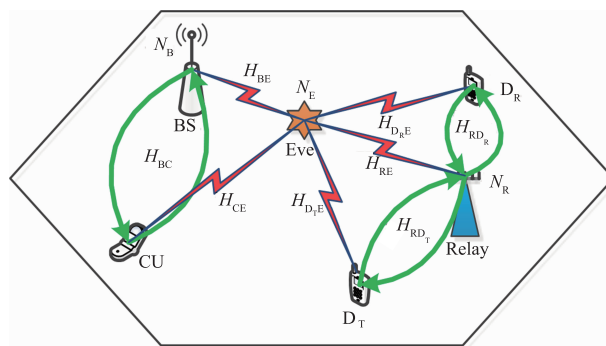


图 1 系统模型示意图

由图可见,除蜂窝链路受到窃听的问题外,Relay 的引入导致 D2D 链路通信受窃听问题更加严重,需要同时提升两条链路的安全性能.文献[10]将 D2D 信号作为对 Eve 的干扰,能够保证蜂窝链路安全,但并未考虑中继 D2D 链路的安全需求.不难发现,在本文系统模型下,仅仅依靠单一节点无法在整个通信过程中对 Eve 进行有效干扰.为此,本文规定 BS 与 Relay 在不同阶段发送信号,并在二者的发送信号中添加人工噪声实现协作干扰,使 Eve 始终无法进行有效窃听,从而同时提高蜂窝链路与 D2D 链路的安全性能.

## 3 基于链路间干扰辅助的中继 D2D 系统安全通信方法

首先将通信过程定义为两个阶段:在第 1 阶段, BS 向 CU 发送信号  $\mathbf{X}_B$ ,其中包含人工噪声,  $D_T$  与  $D_R$  分别向 Relay 发送信号  $x_{D_T}$  与  $x_{D_R}$ ;在第 2 阶段, CU 向 BS 发送信号  $x_C$ , Relay 分别向  $D_T$  与  $D_R$  转发信号  $\mathbf{X}_{RD_T}$  与  $\mathbf{X}_{RD_R}$ ,同时发送人工噪声.

基于文献[16],对 BS 与 Relay 的发射信号与人工噪声做如下设计:

### 3.1 期望信号设计

第 1 阶段,令  $\mathbf{X}_B = \mathbf{H}_B \times \mathbf{S}_B + \mathbf{Z}_B$ ,其中  $\mathbf{H}_B$  为 BS 发送

预编码矩阵,  $\mathbf{S}_B$  为期望信号,  $\mathbf{Z}_B$  为人工噪声, BS 发送功率为最大值为  $P_B$ , 功率分配因子为  $\alpha$ . 设 BS 期望信号与人工噪声的实际功率分别为  $P_{S_B}$  与  $P_{Z_B}$ , 则二者满足条件:  $P_{S_B} = E\{|\mathbf{S}_B|^2\} \leq (1-\alpha)P_B$ ,  $P_{Z_B} = E\{|\mathbf{Z}_B|^2\} \leq \alpha P_B$ . 假设  $D_T, D_R$  的实际发送功率分别为  $P_{D_T}$  与  $P_{D_R}$ . 若  $P_D$  为 D2D 用户发送功率最大值, 则令  $P_{D_T} = P_{D_R} \leq P_D$ . 假设人工噪声对合法用户不产生干扰(后文介绍如何实现), 且 Relay 与 Eve 均有能力区分  $\mathbf{X}_{RD_T}$  与  $\mathbf{X}_{RD_R}$ . 综上可得蜂窝链路及 D2D 链路的保密速率分别为:

$$R_{s_1} = \log\left(1 + \frac{(1-\alpha)P_B \times \|\mathbf{H}_{BC}\mathbf{H}_B\|^2}{\sigma_1^2 + P_{D_T} \times |h_{D,C}|^2 + P_{D_R} \times |h_{D,C}|^2}\right) - \log\left(1 + \frac{(1-\alpha)P_B \times \|\mathbf{H}_{BE}\mathbf{H}_B\|^2}{\sigma_3^2 + \alpha P_B \times |h_{BE}|^2}\right) \quad (1)$$

$$R_{s_2} = \log\left(1 + \frac{P_{D_T} \times \|\mathbf{H}_{RD_T}\|^2 + P_{D_R} \times \|\mathbf{H}_{RD_R}\|^2}{\sigma_2^2 + (1-\alpha)P_B \times \|\mathbf{H}_{BR}\mathbf{H}_B\|^2}\right) - \log\left(1 + \frac{P_{D_T} \times \|\mathbf{H}_{D,E}\|^2}{\sigma_3^2 + \alpha P_B \times \|\mathbf{H}_{BE}\|^2}\right) - \log\left(1 + \frac{P_{D_R} \times \|\mathbf{H}_{D,E}\|^2}{\sigma_3^2 + \alpha P_B \times \|\mathbf{H}_{BE}\|^2}\right) \quad (2)$$

由于 Eve 信道状态未知, 需要考察用户的遍历保密速率, 即  $\bar{R}_{s_1} = E_{h_{bc}}\{R_{s_1}\}$ ,  $\bar{R}_{s_2} = E_{h_{bc}, h_{be}}\{R_{s_2}\}$ . 而两种链路中保密速率最低者决定了系统整体安全性能的最差情况, 因此考察  $\bar{R}_{s_1}$  与  $\bar{R}_{s_2}$  中较小者. 综上, 第 1 阶段的系统遍历保密速率优化问题可以建模为:

$$\max_{h_{bc}} \{\min\{\bar{R}_{s_1}, \bar{R}_{s_2}\}\} \quad \text{s. t. } P_{S_B} \leq (1-\alpha)P_B, \alpha \in [0, 1], P_{D_T}, P_{D_R} \leq P_D \quad (3)$$

BS 的期望信号有两种传统预编码方式:

(1) 满足 CU 接收信干噪比最大. 可采用 SVD 分解法实现, 即  $\mathbf{H}_B = \mathbf{H}_{BC}^H / \|\mathbf{H}_{BC}\|$ . 这种方法可以保证蜂窝链路保密速率最高, 但 BS 发送信号的旁瓣将对 Relay 产生较大干扰;

(2) 满足 BS 发送信号对 Relay 无干扰. 可采用零空间分解法实现, 即  $\mathbf{H}_B \in \text{null}\{\mathbf{H}_{BR}\}$ . 此时 BS 发送信号不干扰 Relay 的接收, 但蜂窝链路保密速率不是最优.

以上两种预编码方法只能使某一条链路达到理想接收状态, 然而本系统整体安全性能由两条链路中安全性能最差者决定, 两条链路接收性能差异不能过大. 为同时优化两条链路的接收性能, 即使蜂窝链路的安全性能最优, 同时使 Relay 受到的干扰最小, 本文将优化目标做如下两种变形:

(1) 严格限制 BS 发送信号对 Relay 无影响, 同时使 CU 接收信号功率最大化:

$$\max\{\|\mathbf{H}_{BC}\mathbf{H}_B\|\} \text{ s. t. } \begin{cases} \|\mathbf{H}_{BR}\mathbf{H}_B\| = 0 \\ P_{S_B} = (1-\alpha)P_B \end{cases} \quad (4)$$

参考文献[11]中的方法对以上优化目标进行求解

得到如下结果:

$$\mathbf{H}_B = \frac{\sqrt{(1-\alpha)P_B}}{\|(\mathbf{I} - \mathbf{H}_{BR}^H(\mathbf{H}_{BR}\mathbf{H}_{BR}^H)^{-1}\mathbf{H}_{BR})\mathbf{H}_{BR}^H\|} \cdot (\mathbf{I} - \mathbf{H}_{BR}^H(\mathbf{H}_{BR}\mathbf{H}_{BR}^H)^{-1}\mathbf{H}_{BR})\mathbf{H}_{BR}^H \quad (5)$$

(2) 设置 CU 接收信号功率门限值, 同时使 BS 发送信号对 Relay 影响最小:

$$\min\{\|\mathbf{H}_{BR}\mathbf{H}_B\|\} \quad \text{s. t. } \begin{cases} \|\mathbf{H}_{BC}\mathbf{H}_B\| = \phi_0 \leq \lambda_{\max}\sqrt{(1-\alpha)P_B} \\ P_{S_B} = (1-\alpha)P_B \end{cases} \quad (6)$$

其中  $\lambda_{\max}$  为  $\mathbf{H}_{BC}$  的最大奇异值,  $\phi_0$  为 BS 在 CU 处的功率门限值. 当  $\phi_0$  固定时, 式(6)中的变量仅剩  $\mathbf{H}_B$ . 这种优化目标下对预编码矩阵  $\mathbf{H}_B$  求解过程与文献[17]中对(26)式的求解过程相似.

第 2 阶段, 令  $\mathbf{X}_R = \mathbf{X}_{RD_T} + \mathbf{X}_{RD_R} + \mathbf{Z}_B = \mathbf{H}_R \times \mathbf{S}_R + \mathbf{Z}_R$ , 其中  $\mathbf{H}_R$  为 Relay 发送预编码矩阵,  $s_R$  为期望信号,  $z_R$  为人工噪声, Relay 总功率为  $P_R$ , 功率分配因子为  $\beta$ , 期望信号与人工噪声功率分别为  $P_{S_R}$  与  $P_{Z_R}$ , CU 发送功率为  $P_{CU}$ . 参照  $\bar{R}_{s_1}$  与  $\bar{R}_{s_2}$  的推导可得到此阶段的用户遍历保密速率  $\bar{R}_{s_3}$  与  $\bar{R}_{s_4}$ , 优化目标与式(3)类似.

在实际应用中, Relay 天线数不应多于 BS, 因此无法在 BS 接收信道零空间中发送信号. 因此 Relay 发送信号预编码优化问题仅有一种情况: 设置 D2D 用户接收功率门限值, 同时使 Relay 发送信号对 BS 影响最小. 优化问题与式(6)相似.

### 3.2 人工噪声设计

第 1 阶段, 可通过预编码将 BS 发送的人工噪声置于 CU 与 Relay 的信道零空间中. 为此, 令  $\mathbf{Z}_B = \mathbf{U}_B \times \mathbf{V}_B$ , 其中  $\mathbf{U}_B$  是由 CU 与 Relay 接收信道零空间正交基生成的预编码矩阵;  $\mathbf{V}_B$  为  $(N_B - 2) \times 1$  维噪声向量, 其元素服从均值为 0、方差为  $\sigma^2$  的高斯分布.

第 2 阶段, 由于 Relay 的天线数不多于 BS, 因此 Relay 无法在 BS 的零空间中发送信号, 但可通过预编码将人工噪声置于  $D_T$  与  $D_R$  的信道零空间中. 为此, 令  $\mathbf{Z}_R = \mathbf{U}_R \times \mathbf{V}_R$ , 其中  $\mathbf{U}_R$  是由 D2D 用户信道零空间正交基生成的预编码矩阵;  $\mathbf{V}_R$  为  $(N_R - 3) \times 1$  维噪声向量, 其元素服从均值为 0、方差为  $\sigma^2$  的高斯分布.

### 3.3 功率分配与控制优化

文献[2~5]针对不同的中继系统通信场景, 在节点功率受限、能量效率约束、频谱效率约束、最小均方误差约束等限制条件下, 对发送节点进行了联合功率分配. 然而以上文献中节点只发送期望信号进行通信, 所进行的功率分配过程是将自身功率合理地分配给不同发送天线. 与以上文献不同, 在本文场景下, BS 与 Relay 不仅需要发送期望信号, 还要利用自身多天线优势发送人工噪声干扰窃听器, 而 BS 或 Relay 采用不同功率

比例发送信号与噪声将对系统保密速率产生不同影响. 因此, 在 BS 与 Relay 总功率受限的情况下, 需要寻找 BS 与 Relay 的最佳功率分配因子  $\alpha$  与  $\beta$ , 并限制 D2D 用户的发送功率.

第 1 阶段, 从式(2)看出, BS 分配给人工噪声的功率越多, Eve 受到的干扰越强, 其接收 SINR 越低; 而人工噪声不影响 Relay 的接收, 因此 D2D 用户保密速率相应增大. 当人工噪声功率过强时, 期望信号功率过低, 将导致蜂窝链路保密速率大幅下降. D2D 用户的发送信号也会影响蜂窝链路的接收质量. 因此, BS 为平衡两种链路的安全性能, 需要对自身发送功率进行合理分配, 同时对 D2D 用户进行功率控制. 由于蜂窝链路与 D2D 链路中保密速率最低者决定了系统整体安全性能的最差情况, 因此蜂窝链路与 D2D 链路保密速率差值, 即  $\bar{R}_{s1}$  与  $\bar{R}_{s2}$  之差不能过大. 为此做出如下平衡约束:

$$|\bar{R}_{s1} - \bar{R}_{s2}| \leq \frac{1}{\xi} \quad (7)$$

其中  $\xi$  为平衡约束因子, 其值越大, 表明  $\bar{R}_{s1}$  与  $\bar{R}_{s2}$  之差越小, 即两种链路间安全性差异越小. 上式表明, BS 应当合理分配自身发送功率, 同时对 D2D 用户进行功率控制, 以达到平衡约束条件.

第 2 阶段, 综合考虑两种链路时可得与第 1 阶段相似的结论: Relay 需要对自身发送功率进行合理分配, 保证第 2 阶段最佳安全性能. 由于 Relay 没有对 CU 进行功率控制的权限, 故此阶段不涉及 CU 功率控制问题.

综上所述, 本文提出的安全通信方法步骤如下:

**步骤 1** 将信号发送模式规定为两个阶段: 第 1 阶段, BS 向 CU 发送信号, 同时 D2D 用户向 Relay 发送信号; 第 2 阶段, CU 向 BS 发送信号, 同时 Relay 向 D2D 用户转发信号;

**步骤 2** 分析第 1 阶段各链路保密速率, 确定优化目标:

$$\begin{aligned} & \max_{H_B} \{ \min \{ \bar{R}_{s1}, \bar{R}_{s2} \} \} \\ & \text{s. t. } p_{s_s} \leq (1 - \alpha) P_B, \alpha \in [0, 1], P_{D_t}, P_{D_r} \leq P_D \end{aligned}$$

**步骤 3** 根据 3.2 节的分析设计人工噪声;

**步骤 4** 根据 3.1 节的分析, 设定初始值  $P_D, P_B, \alpha, \zeta$  求出  $\mathbf{Z}_B$ ;

**步骤 5** 按照式(5)求出  $\mathbf{H}_B$ , 并求出  $\bar{R}_{s1}, \bar{R}_{s2}$ , 进而求出  $R_s^{\text{Stage1}}$ ;

**步骤 6** 固定  $\mathbf{H}_B$ , 按照式(1)、(2)、(7)求出  $P'_D$ , 计算此时  $R_s^{\text{Stage1}'}$ , 若  $R_s^{\text{Stage1}'} \geq R_s^{\text{Stage1}}$ , 更新  $P_D = P'_D$ ;

**步骤 7** 固定  $P'_D$ , 按照式(5)求出  $\mathbf{H}'_B$ , 计算出  $R_s^{\text{Stage1}''}$ , 若  $R_s^{\text{Stage1}''} \geq R_s^{\text{Stage1}'}$ , 更新  $\mathbf{H}_B = \mathbf{H}'_B$ ;

**步骤 8** 重复迭代步骤 6、7, 直至收敛;

**步骤 9** 添加扰动  $\alpha' = \alpha + \Delta$ , 并求出添加扰动之后的  $R_s^{\text{Stage1}}$ , 若较之前性能有所提升, 那么更新  $\alpha$ , 并返回步骤 2); 若不再增加, 那么  $\alpha$  为最优值;

**步骤 10** BS 采用所求预编码矩阵与功率分配因子  $\alpha$  发送信号;

**步骤 11** 分析第 2 阶段各链路保密速率, 优化目标与第 1 阶段类似;

**步骤 12** 根据 3.1、3.2 节的分析设计 Relay 的期望信号与人工噪声;

**步骤 13** 参考步骤 4~9, 求解 Relay 的预编码矩阵与功率分配因子  $\beta$ , 发送信号.

## 4 仿真分析

本节通过仿真对所提方法性能进行验证. 建立二维蜂窝网络, 拓扑结构如表 1 所示:

表 1 仿真拓扑参数表

节点	BS	CU	D <sub>T</sub>	D <sub>R</sub>	Relay
坐标	(0,0)	(3,0)	(6,3)	(6,-2)	(6,0)

假设信道模型包含大尺度与小尺度衰落:  $\mathbf{H}_{AB} = d_{AB}^{-\frac{k}{2}} \times e^{-j\varphi} \times [\text{rand}(M, N) + j * \text{rand}(M, N)]$ , 其中  $d_{AB}$  为节点 A、B 间的距离,  $k$  为尺度衰减因子,  $\varphi$  为相位, 服从  $(0, 2\pi]$  上的均匀分布,  $M, N$  为对应信道的接收与发送天线数. 设  $N_B = 8, N_R = N_E = 4, \xi = 5$ . 每次试验中 Eve 在小区内随机布置 10000 次. 仿真图中 RsBC 与 RsR 分别为 ZF 方法下蜂窝链路及 D2D 链路的保密速率, RsBC2 与 RsR2 分别为 SVD 方法下蜂窝链路及 D2D 链路的保密速率, Rsproposed 为式(5)所确定的优化预编码方法下的系统保密速率.

令  $P_D = 10, P_B = 250, \alpha$  变化范围为  $(0:0.1:1)$ . 基于 ZF 分解法与 SVD 波束成型法下蜂窝链路及 D2D 链路的保密速率与 BS 发送功率分配因子  $\alpha$  间的关系如图 2 所示. 可见, 采用 ZF 方法时, 蜂窝链路保密速率随  $\alpha$  的增加持续下降, 而 D2D 链路保密速率则小幅增加, 最终高于蜂窝链路. 采用 SVD 方法时, 蜂窝链路保密速率始终高于 ZF 方法, 但 D2D 链路保密速率始终低于 ZF 方法. 仿真结果与理论推导相一致: SVD 方法是以 CU 接收功率最大为目标, 会对 Relay 的接收产生干扰; ZF 方法以不干扰 D2D 链路为目标, 但 CU 接收 SINR 较低, 因此 D2D 链路保密速率高于 SVD 方法, 蜂窝链路信道容量会大大降低.

令  $P_R = 100, P_C = 10, \beta$  变化范围为  $(0:0.05:1)$ , 蜂窝链路保密速率 RsCU、D2D 链路保密速率 RsD 与 Relay 发送功率分配因子  $\beta$  间关系如图 3 所示, BS 与 Relay 均采用 SVD 法发送期望信号. 当  $\beta$  增加时, 蜂窝链路保密速率有小幅增加, D2D 链路保密速率则先增加

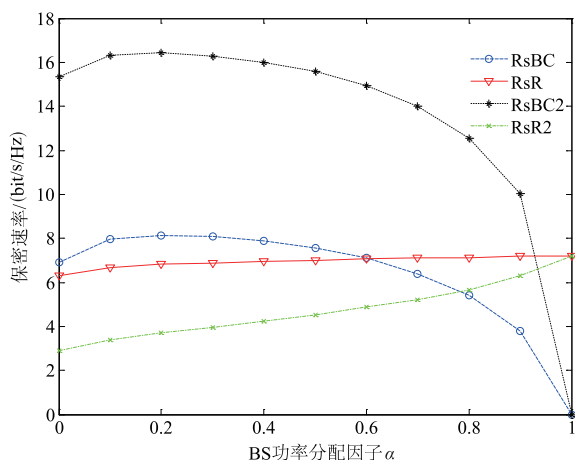


图 2 蜂窝链路与D2D链路保密速率随BS功率分配因子变化

后减少.这是由于当 $\beta$ 增加时,噪声功率增加,Eve受到的干扰增强.而Relay发送天线数少于BS发送天线数,因此Relay发送的人工噪声无法对准BS信道零空间,导致BS受到Relay的干扰,且变化较小,因此蜂窝链路保密速率小幅增加;而当噪声功率持续增大时,期望信号功率持续减小,D2D用户的接收信道速率随之下降,导致保密速率衰减,故D2D链路保密速率先增加后减小.

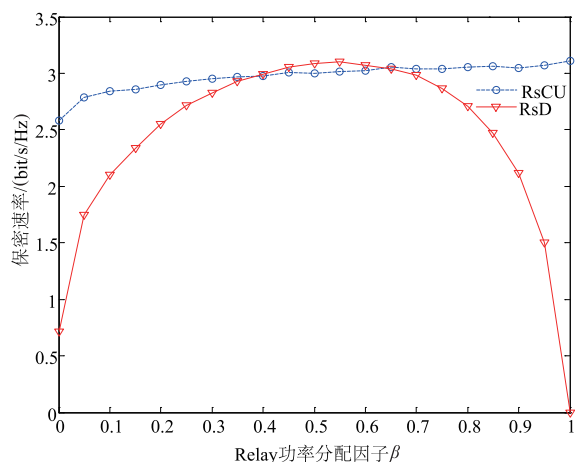


图 3 蜂窝链路与D2D链路保密速率随Relay功率分配因子变化

令 $\xi = 5, \phi_0 = 0.7\lambda_{\max}\sqrt{(1-\alpha)P_B}$ .图4给出(5)式所确定的优化预编码方法与SVD、ZF方法下的系统保密速率对比.系统保密速率由两条通信链路中保密速率最小者决定.可以看出,优化预编码方法在 $\alpha \leq 0.8$ 时性能较好,在 $\alpha > 0.8$ 时低于SVD方法,但始终优于ZF方法.这是由于在优化预编码方法与ZF方法下, $\alpha$ 的增加使蜂窝链路保密速率下降较快,系统保密速率由蜂窝链路决定;而在SVD方法下,D2D链路保密速率持续增加,同时蜂窝链路保密速率高于优化预编码方法,系统保密速率略高于优化预编码方法.但是,实际中BS

不可能将过多功率用于发送人工噪声,即 $\alpha \leq 0.8$ 始终成立,因此可以认为式(5)所确定的优化预编码方法性能更好.

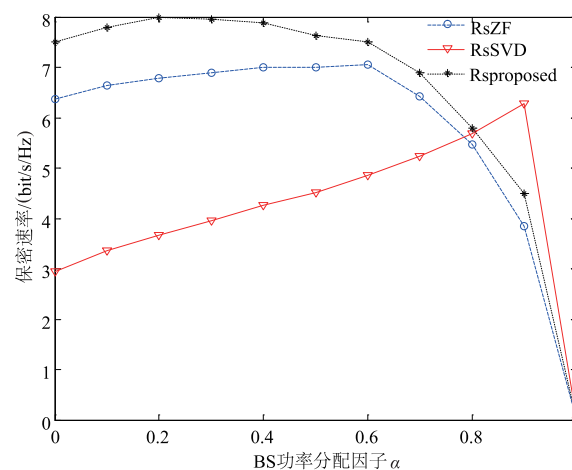


图 4 本文优化算法与传统方法下系统保密速率对比

## 5 结束语

本文研究了部署在蜂窝网络下中继D2D系统的通信过程,提出了一种基于蜂窝链路与D2D链路间相互辅助干扰窃听者的安全通信方法.利用基站与中继节点分别在两个阶段发送信号的特点以及多天线优势,在发送信号中添加人工噪声.针对SVD与ZF预编码方法不能同时兼顾两种链路安全性能的缺陷进行改进,设计期望信号与人工噪声预编码矩阵,实现了两种不同类型链路在正常通信的同时相互辅助干扰窃听者.同时对此过程中基站功率分配与D2D功率控制提出一种联合优化算法.整个通信过程的安全性能得到保障,同时性能较传统的SVD与ZF预编码方法有较大提升.但本文的研究场景仅包含一对D2D用户,未来将对多D2D用户场景下的安全问题进行研究.

## 参考文献

- [1] Doppler K, Rinne M, Cássio B. Device-to-device communication as an underlay to LTE-Advanced networks[J]. IEEE Transactions on Communications Magazine, 2009, 47(12): 42-49.
- [2] Chunguo Li, John M Cioffi, Luxi Yang. Optimal energy efficient joint power allocation for two-hop single-antenna relaying systems[J]. European Transactions on Telecommunications, 2014, 25(7): 745-751.
- [3] Chun G L, Xiang W, Lu X Y, Wei P Z. A joint source and relay power allocation scheme for a class of MIMO relay systems[J]. IEEE Transactions on Signal Processing, 2009, 57(12): 4852-4860.
- [4] Chun G L, Fan S, John M C, Lu X Y. Energy efficient MI-

- MO relay transmissions via joint power allocations [J]. IEEE Transactions on Circuits and Systems-II, 2014, 61 (7):531-535.
- [5] Chun G L, Hyun J Y, Fan S, John M C, Lu X Y. Multiuser overhearing for cooperative two-way multiantenna relays [J]. IEEE Transactions on Vehicular Technology, 2015, 65 (5):1-5.
- [6] Wang L, Peng T, Yang Y. Interference constrained D2D communication with relay underlying cellular networks [A]. IEEE International Conference on Vehicular Technology Conference [C]. Las Vegas: IEEE, 2013. 1-5.
- [7] Zheng W C, Su Z, Shi X S. Research on relay selection in device-to-device communications based on maximum capacity [A]. IEEE International Conference on Information Science, Electronics and Electrical Engineering [C]. Sapporo: Institute of Electrical and Electronics Engineers Inc, 2014. 1429-1434.
- [8] Vanganuru K, Ferrante S, Sternberg G. System capacity and coverage of a cellular network with D2D mobile relays [A]. IEEE Conference on Military Communications Conference [C]. Orlando: IEEE, 2012. 1-6.
- [9] Peng Y, Gao Q, Sun S. Discovery of device-device proximity; Physical layer design for D2D discovery [A]. IEEE International Conference on Communications in China-Workshops [C]. Xi'an: IEEE, 2013. 176-181.
- [10] YUE J, MA C, YU H, et al. Secrecy-based channel assignment for device-to-device communication; an auction approach [A]. IEEE International Conference on Wireless Communications & Signal Processing [C]. Hangzhou: IEEE, 2013. 1-6.
- [11] Yue J, Ma C, Yu H. Secrecy-based access control for device-to-device communication underlying cellular networks [J]. IEEE Transactions on Communications Letters, IEEE, 2013, 17(11):2068-2071.
- [12] Zhu D, Swindlehurst A L, Fakoorian S A A. Device-to-device communications; the physical layer security advantage [A]. IEEE International Conference on Acoustics, Speech and Signal Processing [C]. Florence: IEEE, 2014. 1606-1610.
- [13] Zhang H, Wang T, Song L. Radio resource allocation for physical-layer security in D2D underlay communications [A]. IEEE International Conference on Communications [C]. Sydney: IEEE, 2014. 2319-2324.
- [14] Yu X, Jing Y. SVD-based channel estimation for MIMO relay networks [A]. IEEE International Conference on Vehicular Technology Conference [C]. Québec City: IEEE, 2012. 1-5.
- [15] Li L, Wang J, Wu X. ZF beamforming performance analysis for multiuser spatial multiplexing with imperfect channel feedback [A]. IEEE International Conference on Wireless Communications, Networking and Mobile Computing [C]. Shanghai: IEEE, 2007. 869-872.
- [16] Goel S, Negi R. Guaranteeing secrecy using artificial noise [J]. IEEE Transactions on Wireless Communications, 2008, 7(6):2180-2189.
- [17] Li J, Petropulu A P. On ergodic secrecy rate for gaussian MISO wiretap channels [J]. IEEE Transactions on Wireless Communications, 2011, 10(4):1176-1187.

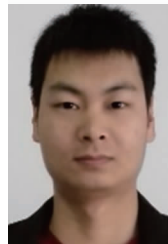
#### 作者简介



朱 宸 男, 1990 年 12 月生, 河南南召人, 国家数字交换系统工程技术研究中心博士生, 研究方向为无线通信网络与物理层安全。  
E-mail: zhuchen007X@outlook.com



黄开枝 女, 1973 年 9 月生, 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, 研究方向为无线通信网络与物理层安全。  
E-mail: huangkaizhi@tsinghua.org.cn



康小磊 男, 1986 年 12 月生, 陕西咸阳人, 术研究中心博士生, 研究方向为无线通信网络与物理层安全。  
E-mail: yiranniao001@163.com

钟 州 男, 1982 年 10 月生, 河南郑州人, 国家数字交换系统工程技术研究中心讲师, 博士, 研究方向为无线通信网络与物理层安全。