doi:10.11959/j.issn.1000-436x.2017009

基于用户配合的全双工蜂窝系统保密传输方案

康小磊，季新生，夏路，黄开枝
（国家数字交换系统工程技术研究中心，河南 郑州 450002）

摘 要：全双工人工噪声机制在干扰功率持续增加时性能提升受限，并且损失了双工增益。针对上述 2 个问题，提出一种基于用户配合的全双工蜂窝系统保密传输方案，半双工的用户上行发送的同时，与其配合的用户可以进行下行发送。蜂窝基站使用全双工技术实现配合用户的干扰消除，并且采用部分功率发送人工噪声干扰窃听者。在此基础上以最大化系统保密速率为目标，设计下行用户期望信号矢量与人工噪声波束矢量；并且利用一维线性搜索获得最优功率配比。仿真结果表明，参考 RS-ref 方法和 HD 方法，所提方法能获得的系统保密速率呈线性增长，并且能够获得全双工增益。

关键词：保密通信；同时同频全双工；用户配合；人工噪声；功率分配
中图分类号：TN925 **文献标识码**：A

Full duplex secret transmission scheme based on user cooperation

KANG Xiao-lei, JI Xin-sheng, XIA Lu, HUANG Kai-zhi
(China National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, China)

Abstract: Full-duplex artificial noise scheme can achieve a limited improvement while the interference power keeps increasing and the full-duplex gain is null. To solve these two problems, a full-duplex secure transmission scheme based on user cooperation was proposed, in which the full-duplex receiver used partial power to send artificial noise, and transmitted the downlink signal by the remaining power to the user who shared the same frequency. In order to maximize the system secrecy rate, the beam vector of the desired signal and the artificial noise were designed. Besides, the optimal power allocation factor was obtained by one-dimensional search simply. Simulation results show that compared with the RS-ref and HD methods, the proposed method can achieve an approximate linear growth in high power and can obtain the full-duplex gain.

Key words: secret communication, co-frequency co-time full duplex, user coordination, artificial noise, power allocation

1 引言

无线通信技术的蓬勃发展造成个人数据和信息进行愈加频繁和大范围的交互共享，因此，面临被窃听的安全问题越发突出。现有的基于人工噪声的物理层安全技术[1]通过无线信道特性实现对用户信号的天然保护，但是人工噪声技术需要发送方天线较多。显而易见地，未来蜂窝通信(5G)中大规模天线基站的使用将为人工噪声的利用带来巨大的机遇[2]。但是，受限于体积、功耗等因素，终端目前难以做到多天线，因此，蜂窝通信的上行安全问题已成为制约蜂窝系统安全性的关键所在。

蜂窝上行链路窃听问题可以建模为 SIMOME 模型，即发送方单天线，接收方和窃听方都为多天线，现有的大部分安全方案都集中于 MISOME[3~5]、MIMOME[6,7]等场景，而对于 SIMOME 场景，大多借助于外部节点的协作辅助达到类似的多天线效果[8,9]。文献[8]在完美信道状态信息假设下，研究

收稿日期：2016-05-28；**修回日期**：2016-11-18
基金项目：国家自然科学基金资助项目（No.61379006, No.61401510, No.61471396, No.61501516, No.61521003）；国家高技术研究发展计划（“863”计划）基金资助项目（No.2014AA01A704）
Foundation Items: The National Natural Science Foundation of China (No.61379006, No.61401510, No.61471396, No.61501516, No.61521003), The National High Technology Research and Development Program of China (863 Program) (No.2014AA01A704)

了各种不同协作转发策略下的保密速率。为了充分实现辅助节点的分布式干扰，避免集中处理带来的复杂度，文献[9]考虑了非协作场景下的外部节点辅助发送干扰的问题，采取机会干扰节点选择的方式，选择与合法信道逼近正交的干扰节点进行噪声转发，实现对 SIMO 链路的安全传输。虽然通过外部节点能够辅助实现 SIMO 系统的安全传输，但是针对移动蜂窝通信，外部节点的部署存在较大的困难，并且如果只为了发送干扰而存在则会受到极大的应用局限。

全双工技术的成熟为打破这种外部节点辅助的应用局限提供了可能，文献[10~13]从全双工的角度出发，研究了在不借助外部节点时候的安全传输问题。文献[10]首次提出了利用全双工接收机可以同时产生人工噪声来对抗外部窃听者，并从中断保密域指标上衡量系统安全性；文献[11]选取一根天线进行接收，其余天线发送人工噪声的方式实现 MIMOME 的安全传输，随后在文献[12]中进一步优化成接收方采用多天线接收，采用多天线发送人工噪声的方案，并且提出了天线分配和功率分配的优化算法。文献[13]则考虑 SIMO 场景下利用发送方产生人工噪声干扰窃听者的情况，并且详细分析了外部窃听者信道已知和未知情况、外部窃听者多天线和单天线等假设下的系统最优方案设计和相应算法。虽然上述方案都能够摆脱对外部辅助节点的依赖，但是存在以下 2 个共性问题：1) 根据保密速率的物理意义，当有用信号发送功率一定时，人工噪声对系统的保密速率提升是受限的，因此，全双工的接收方通过发送人工噪声对保密速率性能的提升有限，容易造成功率的浪费；2) 上述文献采用全双工技术的发送功能只是发送人工噪声，损失了双工增益，这对于未来移动通信需求来讲损失巨大。

针对这 2 个共性问题，本文提出一种基于用户上下行配合的全双工安全传输方案。首先，选取相互配合的 2 个半双工用户进行配对，配对用户上下行时隙颠倒，即在一个用户上行通信的同时，全双工接收机同时采用相同的频谱资源进行下行传输，服务另一个配合用户；然后，在配合用户的下行信号中添加人工噪声，让人工噪声位于该用户的零空间，避免对该用户的干扰；最后，寻找系统保密总速率与分配因子之间的关系，利用一维线性搜索获得最优功率配比。本文方案通过 2 个用户的配合首先能够将多余的功率服务于其他用户，不至于造成功率浪费，其次能够获得双工增益，为系统带来性能的提升。

命名规则及符号说明如下：外部窃听者用 Eve 表示，$(\cdot)^{-1}$、$(\cdot)^{\mathrm{T}}$ 和 $(\cdot)^{\mathrm{H}}$ 分别代表矩阵求逆、转置和共轭转置，$[\cdot]^{+}$ 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

系统模型如图 1 所示，用户是半双工模式，配备单天线；基站是全双工模式，配备多天线，其中，收发天线数分别为 M_{r} 和 M_{t}；当用户 1 与基站进行上行通信时，基站可以使用相同的频域资源与用户 2 进行下行通信[注1]，系统为 TDD 系统，即当前时隙与下一个时隙用户的上下行正好互换；外部窃听者 Eve 采用多天线 M_{e} 窃听。

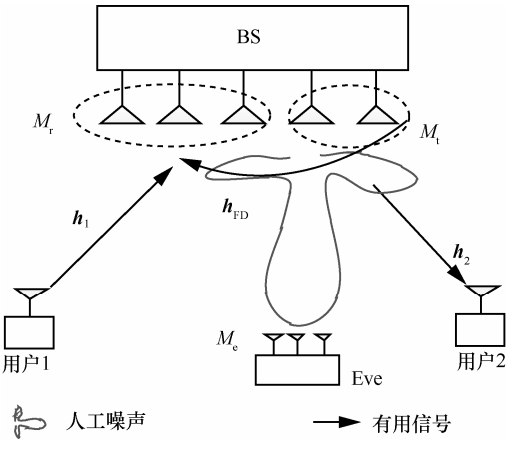


图 1　系统模型

由于 2 个时隙是对称的，因此，本文只需要考虑 1 个时隙上的安全机制即可。本文考虑第 1 时隙：用户 1 上行发送，用户 2 下行接收，此时在基站对用户 2 的下行信号中添加人工噪声。首先对接收信号首先进行分析，在第 1 时隙，基站收到来自用户 1 的上行信号 x_1，并同时受到双工干扰和信道噪声影响

$$y_{\mathrm{r}} = \boldsymbol{h}_1 x_1 + \boldsymbol{H}_{\mathrm{FD}} x_2 + n_{\mathrm{r}} \tag{1}$$

注1：本文假设系统已提前将上下行用户进行了配对，配对后的用户将使用相同资源，与其他用户互不干扰，因此只需考虑 1 对用户即可。

其中，$\boldsymbol{h}_1$ 为用户 1 到基站接收天线的信道向量参数，$\boldsymbol{H}_{\mathrm{FD}}$ 为基站发送天线到接收天线的双工干扰信道矩阵，x_2 为基站向用户 2 下行发送的信号，n_{r} 为背景白噪声。

用户 2 收到来自基站的下行信号，并且同时受到用户 1 的干扰和信道噪声的干扰为

$$y_2 = \boldsymbol{h}_2 \boldsymbol{x}_2 + h_{12} x_1 + n_2 \tag{2}$$

其中，$\boldsymbol{h}_2$ 为基站发送天线到用户 2 的信道向量参数，h_{12} 是用户 1 到用户 2 的干扰信道，n_2 为背景白噪声。假设 Eve 可以窃听到同频资源上的 2 个版本信号，即

$$y_{\mathrm{e}} = \boldsymbol{h}_{\mathrm{e}_1} x_1 + \boldsymbol{H}_{\mathrm{e}_2} x_2 + n_{\mathrm{e}} \tag{3}$$

其中，$\boldsymbol{h}_{\mathrm{e}_1}$ 为用户 1 到窃听者的信道向量参数，$\boldsymbol{H}_{\mathrm{e}_2}$ 为基站发送端到窃听者的信道矩阵。

在更加恶劣的情况，即合法用户无法区分 2 种信号，并且对窃听者是未知的，窃听者可以接近任一用户进行窃听。那么当窃听者接近任一用户进行窃听时，可以认为另一个用户的信号很小，考虑极端的话，认为窃听者可以有所选择地窃听想窃听的信号，屏蔽另一种信号。

基于物理层安全的保密速率定义为合法用户与 Eve 的互信息之间的差异，即 $I(x,y)-I(x,y_{\mathrm{e}})$，由信息论可知，最大值的获得与输入的分布有关。因此，本文通过衡量用户的可达保密速率来衡量安全性能。通过高斯信道容量可知，在第 1 时隙，用户 1 的上行可达保密速率 R_{s_1} 和用户 2 的下行可达保密速率 R_{s_2} 分别为

$$\begin{aligned} R_{s_1} &= I(x_1,y_{\mathrm{r}}) - I(x_1,y_{\mathrm{e}}) \\ &= \mathrm{lb}(1+SINR_{\mathrm{r}}) - \mathrm{lb}(1+SINR_{\mathrm{e}_1}) \leqslant C_{s_1} \end{aligned} \tag{4}$$

$$\begin{aligned} R_{s_2} &= I(x_2,y_2) - I(x_2,y_{\mathrm{e}}) \\ &= \mathrm{lb}(1+SINR_2) - \mathrm{lb}(1+SINR_{\mathrm{e}_2}) \leqslant C_{s_2} \end{aligned} \tag{5}$$

其中，式(4)和式(5)中 C_{s_1} 和 C_{s_2} 分别为用户 1 上行和用户 2 下行保密容量，*SINR* 表示信干噪比（signal to interference plus noise ratio）。

2.2 系统保密吞吐量

假设系统为频分复用系统，即用户对之间利用不同频段进行通信而避免用户间干扰，假设用户 1 与用户 2 使用的频段为 i，由式(4)和式(5)可知，在该段频谱资源上，系统的保密容量应由两用户的和速率性能决定，因此，本文定义此信道资源上系统可达保密速率为

$$R_{\Sigma}^{i} = R_{s_1} + R_{s_2} \tag{6}$$

若该蜂窝下存在 M 对相互配合的蜂窝用户，那么可定义整个蜂窝系统保密吞吐量为

$$T_s = \max \sum_{i=1}^{M} R_{\Sigma}^{i} \tag{7}$$

为了简化分析，本文暂不讨论更多用户对情况下的系统保密吞吐量问题，主要致力于系统保密速率的优化，即考虑 $\max R_{\Sigma}$。

3 方案设计

从式(4)和式(5)中还可以看出，下行信号可以借助基站多天线波束提升自身 *SINR*，但是上行信号只由单天线发送，因此很容易遭到抵近窃听。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，上行安全性很难得到保证，需要借助其他手段提升上行或恶化 Eve 的 *SINR* 来提升安全性能。

为此，基于文献[1]，本文在基站侧的下行信号中添加人工噪声，令 $x_2 = s_2 + \boldsymbol{z} = \boldsymbol{u}s + \boldsymbol{z}$，即蜂窝通信信号由 2 部分组成：期望信号 s_2 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 为期望传输的归一化有用信号。令人工噪声 $\boldsymbol{z}$ 对合法接收无影响（下文将讨论如何设计）。$\mathrm{E}\{|s_2|^2\} = \mathrm{tr}\{\boldsymbol{u}\boldsymbol{u}^{\mathrm{H}}\} = (1-\vartheta)p_d = p_s$ 为期望信号功率，ϑ 为功率分配因子；人工噪声信号功率为 $\mathrm{E}\{|\boldsymbol{z}|^2\} = p_z = \vartheta p_d$。同理，$\mathrm{E}\{|x_1|^2\} = p_u$，可以重写式(1)~式(3)为

$$y_{\mathrm{r}} = h_1 x_1 + \boldsymbol{H}_{\mathrm{FD}} \boldsymbol{u}s + n_{\mathrm{r}} \tag{8}$$

$$y_2 = h_2 \boldsymbol{u}s + h_{12} x_1 + n_2 \tag{9}$$

$$y_{\mathrm{e}} = \boldsymbol{h}_{\mathrm{e}_1} x_1 + \boldsymbol{H}_{\mathrm{e}_2} us + \boldsymbol{H}_{\mathrm{e}_2} z + n_{\mathrm{e}} \tag{10}$$

$\mathrm{E}\{|s_2|^2\} = \mathrm{tr}\{\boldsymbol{u}\boldsymbol{u}^{\mathrm{H}}\} = (1-\vartheta)P_0 = p_d$ 为期望信号功率，ϑ 为功率分配因子；人工噪声信号功率为 $\mathrm{E}\{|z|^2\} = p_z = \vartheta P_0$。同理，$\mathrm{E}\{|x_1|^2\} = p_u$，联立式(4)~式(10)可得

$$R_{s_1}=\mathrm{lb}\left(1+\frac{p_u\left\|\boldsymbol{h}_1\right\|^2}{\sigma_r^2+\left\|\boldsymbol{H}_{\mathrm{FD}}\boldsymbol{u}\right\|^2}\right)-\mathrm{lb}\left(1+\frac{\left\|\boldsymbol{h}_{\mathrm{e}_1}x_1\right\|^2}{\sigma_{\mathrm{e}}^2+\left\|\boldsymbol{H}_{\mathrm{e}_2}z\right\|^2}\right) \tag{11}$$

$$R_{s_2}=\mathrm{lb}\left(1+\frac{p_d\left\|\boldsymbol{h}_2\right\|^2}{\sigma_2^2+\left|h_{12}x_1\right|^2}\right)-\mathrm{lb}\left[1+\frac{p_d\left\|\boldsymbol{H}_{\mathrm{e}_2}\boldsymbol{u}s\right\|^2}{\sigma_{\mathrm{e}}^2+\left\|\boldsymbol{H}_{\mathrm{e}_2}z\right\|^2}\right] \tag{12}$$

3.1　人工噪声矢量设计

合法的接收有 2 部分：基站的上行接收和用户 2 的下行接收，为此，人工噪声的设计需要考虑 2 种情况，即对这 2 部分的干扰尽可能小，最简单的设计可参考文献[1]中的零陷成形，在 Eve 信道已知情况下可以建模为

$$\max_{\boldsymbol{u}}\left|\boldsymbol{h}_{E_1}\boldsymbol{z}\right|+\left|\boldsymbol{H}_{E_2}\boldsymbol{z}\right|$$
$$\text{s.t.}\begin{cases}\left|\boldsymbol{H}_{\mathrm{FD}}\boldsymbol{z}\right|=0\\ \left|\boldsymbol{h}_2\boldsymbol{z}\right|=0\\ p_s=\mathrm{tr}\{\boldsymbol{z}\boldsymbol{z}^{\mathrm{H}}\}=(1-\vartheta)P_0\end{cases} \tag{13}$$

为了保证合法用户的接收不受人工噪声影响，设计人工噪声 $\boldsymbol{z}$ 满足与合法用户信道正交，在此情况下寻求对 Eve 干扰最大的矢量 $\boldsymbol{z}$。但是，最为合理的假设是 Eve 信道状态信息未知，并且由于基站天线之间距离很近，想要做到零陷设计存在很大困难。本文考虑如下优化模型为

$$\min_{\boldsymbol{u}}\left|\boldsymbol{H}_{\mathrm{FD}}\boldsymbol{z}\right|$$
$$\text{s.t.}\begin{cases}\left|\boldsymbol{h}_2\boldsymbol{z}\right|=0\\ p_s=\mathrm{tr}\{\boldsymbol{z}\boldsymbol{z}^{\mathrm{H}}\}=(1-\vartheta)P_0\end{cases} \tag{14}$$

首先保证人工噪声位于用户 2 的接收零陷内，在此基础上最小化对基站全双工接收的干扰。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 $(M_{\mathrm{t}}-1)\times1$ 维的人工噪声向量，其元素相互独立，满足期望为 0，方差为 σ^2 的高斯分布。因此，有 $p_z=(M_{\mathrm{t}}-1)\sigma^2=\theta P_0$。

3.2　下行有用信号设计

如果不存在双工干扰，并且在只有一个用户情况下，文献[3]的定理 2 证明了当 Eve 信道已知时，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 $(\boldsymbol{I}_N+\boldsymbol{h}_{\mathrm{a}}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{a}},\ \boldsymbol{I}_N+\boldsymbol{H}_{\mathrm{e}}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{e}})$ 的最大广义特征值，其中，$\boldsymbol{h}_{\mathrm{a}}$ 和 $\boldsymbol{H}_{\mathrm{e}}$ 分别为基站到用户和到窃听者的信道状态。$\boldsymbol{u}_{\lambda_{\max}}$ 为 $\lambda_{\max}$ 所对应的广义特征向量；但是当 Eve 信道未知时，$\boldsymbol{u}$ 的设计只与合法用户有关。不同于文献[10]的是，本文的场景在考虑波束设计时还需要考虑尽量避免双工干扰的问题，因此，可以从 2 方面考虑：1) 以最大化用户 2 接收质量为目标；2) 以最小化双工干扰为目标。

针对第 1 种情况，首先保证双工干扰在信号层面能够得到第一步的消除，中文预编码设计原则可以建模如下

$$\max_{\boldsymbol{u}}\left|\boldsymbol{h}_2\boldsymbol{u}\right|$$
$$\text{s.t.}\begin{cases}\left|\boldsymbol{H}_{\mathrm{FD}}\boldsymbol{u}\right|=0\\ p_s=\mathrm{tr}\{\boldsymbol{u}\boldsymbol{u}^{\mathrm{H}}\}=(1-\vartheta)P_0\end{cases} \tag{15}$$

第 2 种情况，即无法在信号层面完全消除双工干扰，只能尽可能在满足下行传输的前提下有效减少双工干扰，由于 $\boldsymbol{h}_2\boldsymbol{u}\boldsymbol{u}^{\mathrm{H}}\ \boldsymbol{h}_2^{\mathrm{H}}\leqslant(1-\vartheta)P_0\left\|\boldsymbol{h}_2\right\|^2=(1-\vartheta)P_0\lambda_{\max}$，$\lambda_{\max}$ 为 $\boldsymbol{h}_2$ 的 2-范数（当 $\boldsymbol{h}_2$ 为矩阵时对应为最大奇异值），设定基站在用户 2 处接收功率受限于 γ_0，那么该问题可建模如下

$$\min_{\boldsymbol{u}}\left|\boldsymbol{H}_{\mathrm{FD}}\boldsymbol{u}\right|$$
$$\text{s.t.}\begin{cases}\left|\boldsymbol{h}_2\boldsymbol{u}\right|=\gamma_0\leqslant\lambda_{\max}\sqrt{(1-\vartheta)P_0}\\ p_s=\mathrm{tr}\{\boldsymbol{u}\boldsymbol{u}^{\mathrm{H}}\}=(1-\vartheta)P_0\end{cases} \tag{16}$$

与 3.1 节分析相同，现实中第 1 种情况比较难实现，在本文中以第 2 种优化模型为准设计用户波束矢量。

3.3　人工噪声与有用信号功率分配

为了获得最优的人工噪声与有用信号功率分配，本文给出如下定理。

定理 1　本文方案下系统总保密速率是人工噪声分配因子的凸函数。

证明　功率分配因子在 0~1 上连续，且由于对数函数的连续可导性，可知式(11)和式(12)在 0~1 上连续可导。为了重点分析保密总速率与人工噪声分配因子的关系，本文改写式(11)和式(12)，对于式(11)，可以认为本文方案下双工干扰足够小，所以 $\boldsymbol{H}_{\mathrm{FD}}\boldsymbol{u}\approx0$，式(11)的第 1 项与 θ 无关；第 2 项可以等价为 $\mathrm{lb}\left(1+\dfrac{B}{\sigma_{\mathrm{e}}^2+\theta P_0}\right)$，$\mathrm{lb}\left(1+\dfrac{B}{\sigma_{\mathrm{e}}^2+\theta P_0}\right)$ 的单调性与

$\mathrm{lb}\left(\frac{1}{\theta}\right)$是一致的，综上所述，式（11）的凹凸性等价于$R_{s_1} \propto A\mathrm{lb}(\theta)$，其中，$A$为常数；类似地，可得式(12)凹凸性等价于$R_{s_1} \propto B\mathrm{lb}(\theta)+C\mathrm{lb}(1-\theta)$，其中，$B$、$C$为常数。所以，$R_{\Sigma}=R_{s_1}+R_{s_1} \propto a\mathrm{lb}(\theta)+b\mathrm{lb}(1-\theta)$，其中，$a$、$b$分别为不为 0 的正数。对其求导可得$\frac{\partial R_{\Sigma}}{\partial \theta}=\frac{a}{\theta}+\frac{b}{1-\theta}$，$\frac{\partial^2 R_{\Sigma}}{\partial \theta^2}=\frac{-a(1-\theta)^2-b\theta^3}{(1-\theta)^2\theta^2}<0(\theta \neq 0)$，得证。

由于窃听者信道是未知的，并且总功率的不同都会导致常数的不同，因此最优的功率分配因子很难获得分析结果。不过幸运的是，本文已经得到了凸函数的结论，因此可以简单地通过一维线性搜索或二分法获得最优数值解。

4　数值结果

为了简化分析，本文假设所有信道服从复高斯分布，基站天线数为M_{r}=3，M_{t}=5，N_{e}=4。实验次数为 10 000。ζ=0.5，$\gamma_0=0.7\lambda_{\max}\sqrt{(1-\vartheta)P_0}$，在 Matlab2014 仿真环境中采用蒙特卡洛方法进行仿真。

设定用户 1 的发送功率为 20 dBm，基于用户配合的全双工传输方案（Cs-FD）与半双工下行传输方案（Cs-HD）的系统保密速率随人工噪声比例变化如图 2 所示，需要说明的是，为了对比合理，本文在仿真半双工时，将全部功率都交给接收端，并且利用全部天线对一个用户进行下行发送，在此基础上利用人工噪声方法计算半双工系统保密速率。从图 2 中可知，当全双工接收端功率为 10 dBm 时(总功率 30 dBm)，全双工方案性能在大多数情况下是差于半双工方案的，而随着接收端功率的增大，全双工方案优势逐渐大于半双工方案。上述结果与实际理论相符合：用户 2 接收到 2 个信号，一个是用户 1 的上行信号，一个是基站的下行信号，当接收端发送功率较小时，用户 2 受到用户 1 的上行干扰严重，造成用户 2 的下行速率低，因此会差于半双工下行传输；而当接收端功率足够大时，首先人工噪声功率也相应提升，对上行保密速率提升明显，并且下行功率的增大同样可以认为用户 2 收到的干扰成为次要因素，因此，全双工方案性能提升明显，并且优于半双工方案。此外还可以看出，随着接收机的功率变大，全双工方案下最优功率分配因子呈现减小趋势，这也说明了当上行功率一定时，人工噪声存在最优值，应该把剩余功率分配给用户 2 以提升用户 2 的保密速率才能整体提升系统保密速率，实现安全效率的提升。

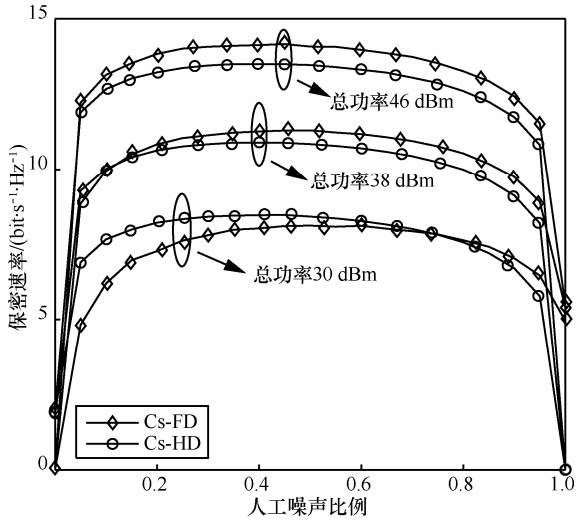


图 2　保密总速率随人工噪声比例变化

为了更加细节地验证单个用户的保密速率问题，本文给出了如图 3 所示的用户保密速率与发送功率之间的关系，其中，本文设定接收机下行发送总功率分别为：30 dBm、34 dBm、38 dBm。图 3 衡量了随着用户 1 上行发送功率变化情况下的用户 1 上行保密速率和用户 2 下行保密速率变化情况。从图 3 中可以看出，首先，随着上行功率的变化，用户 1 和用户 2 的保密速率呈现相反的变化结果，用户 1 肯定随自身发送功率的提升而提升，但是对用户 2 来说，用户 1 的上行信号完全是由于用户

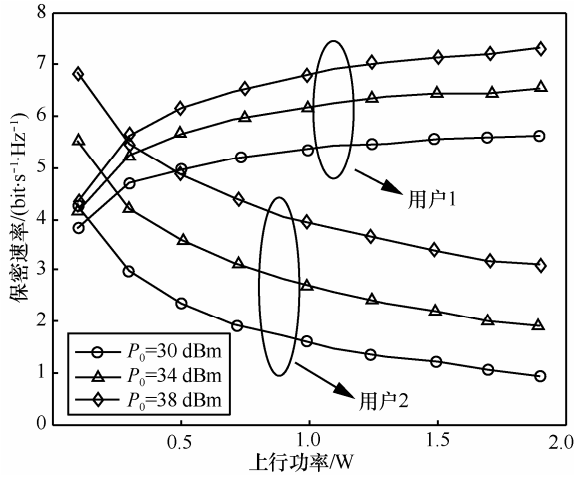


图 3　用户 1 和用户 2 的保密速率随上行功率变化情况

间配合而带来的干扰，只会对用户 2 带来损害，因此，用户 2 的性能是下降的。其次，当接收机总功率增大时，两用户的保密速率性能都有提升，这对于用户 2 来讲是必然的，对于用户 1，随着接收机功率的增大，人工噪声功率相应增大，因此会带来用户 1 保密速率的提升。

为了进一步对比本文方案的优势，图 4 给出了本文方案与半双工 HD 方法（Rs-HD-downlink）以及全双工人工噪声机制方案（Rs-ref[13]）的保密速率性能对比，从图 4 中可以看出，当上行功率一定时，文献[13]中的 Rs-ref 方法在额外提升全双工接收机的发送功率时对系统保密速率（需要注意的是，Rs-ref 方法只有上行保密速率）的提升十分有限，而本文方案将多余的功率分配给下行配合用户，能够极大地提升系统保密速率；而对比于半双工 HD 方法，在小功率域，本文方案由于存在较大干扰，因此性能不如半双工 HD 方法。不过当全双工接收机发送功率大于 14 dBm 时，本文方案已经全面优于半双工 HD 方法，并且在高功率域一直保持恒定优势，这部分增益就来自于全双工增益，可见本文方案也能够获得全双工增益的优势。此外，从图 4 中可以看出，本文方案和半双工都存在收敛特性，不随上行功率的变化而变化，这也是因为在下行发送功率足够大时，上行功率成为影响系统保密速率的次要因素。这里需要注意的是，本文仿真参考的 HD 方法只是针对上行保密速率，而半双工是针对下行保密速率，两者对功率的利用率差别很大，所以没有对比性。

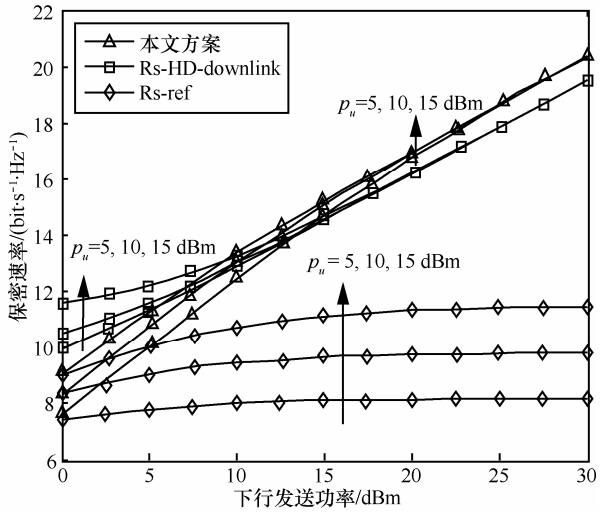


图 4　系统保密速率随下行功率变化情况

5　结束语

全双工接收机在物理层安全中应用能够摆脱系统对外部辅助节点的依赖，具有一定优势，但是现有方案存在性能提升受限和损失双工增益这 2 个问题。本文针对这 2 个问题，提出了一种基于用户配合的全双工安全传输方案，利用配对用户上下行时隙颠倒、接收端的多天线资源和全双工功能，在一个用户上行通信的同时，采用相同的频谱资源进行下行传输；然后在配合用户的下行信号中添加人工噪声，同时提升 2 个配合用户的保密速率；并且在此基础上利用一维线性搜索获得功率最优配比。本方案通过 2 个用户的配合，首先能够将多余的功率服务于其他用户，不至于造成功率浪费，其次还获得了全双工的双工增益，为系统带来性能的提升。在未来的工作中，将对多用户配合的全双工安全组网问题做进一步研究。

参考文献：

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

[2] 康小磊, 季新生, 黄开枝. 基于人工噪声辅助的D2D异构蜂窝安全通信方法[J]. 通信学报, 2015, 36(10): 149-156.
KANG X L, JI X S, HUANG K Z. Secure D2D heterogeneous cellular communication based on artificial noise assisted[J]. Journal on Communications, 2015, 36(10):149-156.

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

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

[5] WANG H M, ZHENG T, MU P. Secure MISO wiretap channels with multi-antenna passive eavesdropper via artificial fast fading[J]. IEEE Transactions on Wireless Communications, 2014, 14(1):5396-5401.

[6] KHISTI A, WORNELL G W. Secure transmission with multiple antennas—part II: The MIMOME wiretap channel[J]. IEEE Transactions on Information Theory, 2010, 56(11): 5515-5532.

[7] LI N, TAO X F, XU J. Ergodic secrecy sum-rate for downlink multi-user MIMO systems with limited CSI feedback[J]. IEEE Communications Letters, 2014,18(6): 969-972.

[8] 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.

[9] WANG C, WANG H M, XIA X G, et al. Uncoordinated jammer selection for securing SIMOME wiretap channels: a stochastic geometry approach[J]. IEEE Transactions on Wireless Communications, 2015,

14(5): 2596-2612.

[10] LI W, GHOGHO M, CHEN B, et al. Secure communication via sending artificial noise by the receiver: outage secrecy capacity/ region analysis[J]. IEEE Communications Letters, 2012, 16(10): 1628-1631.

[11] ZHOU Y, ZHU Y, LI F, et al. Securing communication via transmission of artificial noise by both sides: bipolar-beamforming optimization[J]. Mathematical Problems in Engineering, 2013, 18(5):708-716.

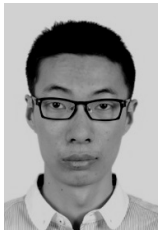
[12] ZHOU Y, XIANG Z Z, ZHU Y, et al. Application of full-duplex wireless technique into secure MIMO communication: achievable secrecy rate based optimization[J]. IEEE Signal Processing Letters, 2014, 21(7):804-808.

[13] ZHENG G, KRIKIDIS I, LI J,et al. Improving physical layer secrecy using full-duplex jamming receivers[J]. IEEE Transactions on Signal Process, 2013, 61(20): 4962-4974.

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。



夏路（1989-），男，安徽庐江人，国家数字交换系统工程技术研究中心助理研究员，主要研究方向为无线移动通信。

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。