基于联盟博弈的多小区下行链路保密协作算法

李明亮 郭云飞 黄开枝*
(国家数字交换系统工程技术研究中心 郑州 450000)

摘 要：考虑一个存在多窃听者的多小区下行链路蜂窝网络，协作小区通过在选定的子载波上执行协作波束赋形，利用小区间干扰抑制窃听者，实现安全传输。在窃听者位置未知的情况下，推导了下行链路保密连接概率的闭式表达式。在此基础上，将下行链路建模为博弈参与者，该文提出一种基于联盟博弈的多小区下行链路保密协作算法，以保密连接概率为效用函数，通过设计联盟加入和退出规则，实现了下行链路对子载波的高效选择和保密协作联盟的自组织生成。理论和仿真分析表明所提算法能够形成稳定的联盟结构，并且所提算法的保密性能优于传统的联盟协作算法。

关键词：无线通信；物理层安全；联盟博弈；多小区协作
中图分类号：TN92 **文献标识码**：A **文章编号**：1009-5896(2017)06-1271-07
DOI: 10.11999/JEIT160969

Coalition Game Based Secrecy Downlink Cooperation Algorithm in Multi-cell Networks

LI Mingliang GUO Yunfei HUANG Kaizhi
(*National Digital Switching System Engineering & Technological R&D Center*, *Zhengzhou* 450000, *China*)

Abstract: This paper studies physical layer security of the multi-cell cellular networks, where the base stations need to perform cooperation beamforming in selected subcarriers to secure the downlink communication, and eavesdroppers with random location are interfered by inter-cell interference. Firstly, the approximation for the secrecy connection probability with uncertained locations of eavesdroppers is obtained. Then a distributed coalition game based cooperation algorithm is proposed to maximize the secrecy connection probability of downlinks. Specifically, the downlink is modeled as game player, whose payoff is the secrecy connection probability in the selected coalition, the join and quit rules of coalitions are designed to make downlinks self-organizing form cooperative coalition and achieve the effective subcarrier allocation. Moreover, the convergence of the proposed coalition formation game is proved, theoretical analysis and simulation results show that the proposed algorithm can form a stable coalitional structure and results in a notable secure performance advantage relative to the traditional cooperation algorithms.

Key words: Wireless communication; Physical layer security; Coalition game; Multi-cell cooperation

1 引言

为了适应未来移动通信高速增长的通信需求，蜂窝网络逐步向密集化和自组织化部署的方向发展，密集化部署在提高网络频谱效率的同时，导致网络的干扰管理更加复杂；自组织化部署在拓展组网便利性的同时，进一步开放了网络的接入权限，导致网络的保密通信受到威胁。目前，保障蜂窝网络安全传输的手段依然是高层的密钥加密机制，但是密钥的管理和分发存在一定的安全隐患。与此同时，基于无线信道特征的物理层安全传输技术为蜂窝网络安全提供了新思路。

物理层安全技术基于合法用户信道和窃听信道的差异性，在空域、时域、频域等多个通信维度，发送具有目标选择性的干扰，为合法用户构造优势通信条件，限制非授权用户的窃听行为，从而保障安全通信。文献[1]首次提出在空域构造人工噪声恶化窃听者的接收信号质量，保障通信安全。文献[2]针对下行链路多用户 MIMO 系统，通过协作干扰者发送人工噪声干扰潜在窃听者，并推导了最优的联合波束赋形发射方案。当已知窃听者瞬时信道状态信息时，文献[3]研究了多天线协作中继系统的遍历可达保密速率。文献[4]通过多小区的资源调度将小区间干扰转化为网络的保密增益，并研究了多小区

收稿日期：2016-09-26；改回日期：2017-02-22；网络出版：2017-04-14
*通信作者：黄开枝 huangkaizhi@tsinghua.org.cn
基金项目：国家 863 计划项目(SS2015AA011306)，国家自然科学基金(61379006)
Foundation Items: The National 863 Program of China (SS2015AA 011306), The National Natural Science Foundation of China (61379006)

波束和发射功率的联合优化方案。当窃听者瞬时信道状态信息不准确时，文献[5]研究了多小区下行链路波束赋形的保密性能，并推导了遍历保密速率的表达式。当窃听者的位置分布服从泊松点过程时，文献[6,7]分析了认知无线电网络的保密传输性能。文献[8]分析了多跳网络中译码转发中继的保密性能。上述文献对蜂窝网络的保密协作传输性能进行了定量分析，但并未考虑网络如何形成保密协作关系。

在多小区网络中，基站间的协作行为受到诸如基站相对位置关系，信道状态等多方面因素的制约，联盟博弈[9]研究博弈参与人如何形成协作联盟及形成联盟后协作收益如何分配等问题。文献[10]首次利用联盟博弈构造了多节点保密协作博弈模型，提出了一种基于 TDMA 的保密协作联盟形成博弈算法。在此基础上，文献[11]利用联盟形成博弈的性质对节点动态行为进行建模，并分析了动态行为对保密性能的影响。文献[12]从窃听者的角度出发，将恶意干扰中继的协作问题建模为效用不可转移的联盟博弈，分析了窃听者如何加入或脱离联盟，以达到最佳的窃听效果。文献[13]对友好中继的协作行为进行了建模分析，基于联盟形成博弈设计了中继的身份选择机制和协作联盟形成算法。文献[14]利用联盟形成博弈进一步研究了认知无线电场景下，利用主次用户间干扰保障安全传输的多节点协作问题。文献[15]研究了将 D2D 链路干扰转化为蜂窝链路保密增益的联盟协作算法。通过分析上述文献可发现，现有基于联盟博弈的物理层安全协作研究均需要协作节点之间交互保密信息，并且假设窃听者的瞬时信道状态和位置已知。当网络自组织部署时，窃听者的位置和信道状态信息难以获得，辨别接入网络通信节点的身份变得更加困难，此时，在基站间交换保密信息进行协作传输是不安全的。

针对上述问题，本文利用 CoMP 协同赋形技术[16]实现多小区基站的保密协作，在减少保密信息扩散的同时，避免了对其余下行链路的干扰。在此基础上，将窃听者的位置分布建模为泊松点过程，推导了基于 CoMP 协同赋形技术的下行链路保密连接概率的闭式表达式；与此同时，综合考虑网络的子载波分配和协作关系形成问题，将下行链路建模为博弈参与者，并以保密连接概率为效用函数，将多小区下行链路的保密协作建模为效用不可转移的联盟形成博弈，提出一种基于联盟博弈的多小区下行链路保密协作算法。该算法以通信子载波为索引对协作联盟进行划分，通过设计协作联盟的加入和退出规则，实现了下行链路自组织的协作联盟划分和子载波分配。理论分析证明了所提算法的收敛性，仿真结果表明所提算法的保密性能优于传统协作算法。

2 系统模型

如图 1 所示，考虑一个由 N 个微小区组成的多小区 MISO 下行链路系统，令 $\mathcal{P}=\{1,2,\cdots,N\}$ 表示所有基站的位置集合，每个基站装备 M 根天线，系统采用 OFDMA 的多址方式，通信频带被划分为 I 个正交的子载波信道，各个子载波信道是相互独立的块衰落信道。系统中存在单天线窃听者试图对合法用户的下行链路通信进行窃听，其位置分布服从密度为 λ_e 的泊松点过程 Φ_e [17]。当基站小区密集部署时，相邻小区间的干扰将急剧增大，小区边缘用户的信道质量将严重恶化，这给小区用户的保密通信带来了安全隐患。

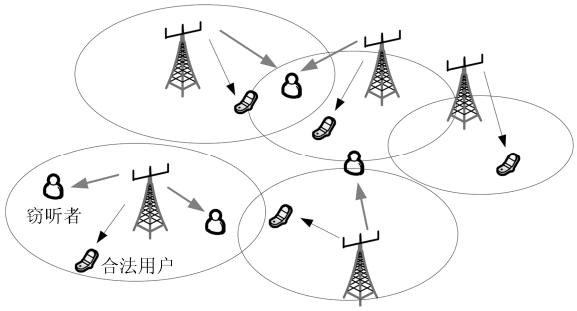

图 1 多小区下行保密传输模型

为了抑制用户间干扰和提升保密性能，基站能够协作进行 CoMP 波束赋形，令 $\pi_{\mathcal{P}}=\{S_1,S_2,\cdots,S_I\}$ 表示在各个子载波上形成的协作组划分的集合，在第 i 个子载波上，当 $|S_i|$ 个基站组成协作组 $S_i\in\pi_{\mathcal{P}}$ 执行联合波束赋形时，子载波 i 上目标用户 n 和窃听者 e 的接收信号可分别表示为

$$y_n^i=\sqrt{P_n}\,r_{n,n}^{-\alpha/2}\boldsymbol{h}_{n,n}^i\boldsymbol{w}_n^i x_n^i+\sum_{q\neq n,q\in S_i}\sqrt{P_q}\,r_{n,q}^{-\alpha/2}\boldsymbol{h}_{n,q}^i\boldsymbol{w}_q^i x_q^i+N_n^i \tag{1}$$

$$y_e^i=\sqrt{P_n}\,r_{e,n}^{-\alpha/2}\boldsymbol{g}_{e,n}^i\boldsymbol{w}_n^i x_n^i+\sum_{q\neq n,q\in S_i}\sqrt{P_q}\,r_{e,q}^{-\alpha/2}\boldsymbol{g}_{e,q}^i\boldsymbol{w}_q^i x_q^i+N_e^i \tag{2}$$

其中，$\boldsymbol{h}_{n,q}^i,\boldsymbol{g}_{e,q}^i$ 分别表示子载波 i 上 $1\times M$ 维的基站 $q\in\mathcal{P}$ 到用户 n 和到窃听者 e 的信道状态向量，$\boldsymbol{w}_n^i$ 表示子载波 i 上基站 n 的发射波束赋形向量，P_n 表示基站 n 的发射功率，x_n^i 表示子载波 i 上发送给用户 n 的保密信号，N_n^i,N_e^i 表示子载波 i 上用户 n 和窃听者 e 的均值为 0、方差为 σ^2 的加性高斯白噪声。

CoMP 技术按照传输方式不同，可分为联合处理技术和协同赋形技术。当窃听者位置未知时，在基站间交互保密信息是不安全的，可能导致保密信

息的传播范围扩大。为了保证保密通信，基站应当在保证合法链路传输质量的基础上，降低对其余用户的干扰，并且尽可能缩小保密信号的传播范围，这与协同赋形 CoMP[16]的实现方式是相似的。

定义 1　满足上述约束的基站 n 的波束构造可表示为

$$\left.\begin{aligned}&\max\left|\boldsymbol{h}_{n,n}^{i}\boldsymbol{w}_{n}^{i}\right|\\&\text{s.t.}\quad \boldsymbol{h}_{q,n}^{i}\boldsymbol{w}_{n}^{i}=0,\forall q\neq n,q\in S_i\\&\qquad\left\|\boldsymbol{w}_{n}^{i}\right\|=1\end{aligned}\right\}\tag{3}$$

由定义 1 可知，基站 n 的波束赋形向量建立在其余协作用户信道状态构成的补矩阵 $\boldsymbol{H}_{n}^{i}=\left[\left(\boldsymbol{h}_{1,n}^{i}\right)^{\mathrm{H}},\cdots,\left(\boldsymbol{h}_{n-1,n}^{i}\right)^{\mathrm{H}},\left(\boldsymbol{h}_{n+1,n}^{i}\right)^{\mathrm{H}},\cdots,\left(\boldsymbol{h}_{|S_i|,n}^{i}\right)^{\mathrm{H}}\right]^{\mathrm{H}},n\in S_i$ 的零空间上。对 $\boldsymbol{H}_{n}^{i}$ 进行 SVD 分解，令 $\boldsymbol{V}_{n}^{i}$ 表示右奇异值矩阵中奇异值为 0 的向量构成的矩阵。由此可以得到，在子载波 i 上基站 n 的波束赋形向量：$\boldsymbol{w}_{n}^{i}=\dfrac{1}{\left\|\boldsymbol{h}_{n,n}^{i}\right\|}\left(\boldsymbol{V}_{n}^{i}\right)\left(\boldsymbol{V}_{n}^{i}\right)^{\mathrm{H}}\left(\boldsymbol{h}_{n,n}^{i}\right)^{\mathrm{H}}$。

此时，用户的保密信息仅仅局限在当前服务小区内传输，避免了协作引起的保密信息扩散；并且，由式(3)可知，$\boldsymbol{w}_{n}^{i}$ 建立在其余用户的零空间上，避免了对其余用户下行链路通信的干扰。在子载波 i 上目标用户 n 和窃听者 e 的接收 SINR 可分别表示为

$$\mathrm{SINR}_{n}^{i}=\frac{P_n r_{n}^{-\alpha}\left|\boldsymbol{h}_{n,n}^{i}\boldsymbol{w}_{n}^{i}\right|^{2}}{\sigma^{2}}\tag{4}$$

$$\mathrm{SINR}_{e}^{i}=\frac{P_n r_{e,n}^{-\alpha}\left|\boldsymbol{g}_{e,n}^{i}\boldsymbol{w}_{n}^{i}\right|^{2}}{I_{S_i}+\sigma^{2}}\tag{5}$$

其中，$I_{S_i}=\sum_{q\neq n,q\in S_i}P_q r_{e,q}^{-\alpha}\left|\boldsymbol{g}_{e,q}^{i}\boldsymbol{w}_{q}^{i}\right|^{2}$ 表示协作组内其余基站对窃听者的干扰，由于系统内存在多个窃听者窃听，因此目标用户 n 的保密速率[1]可表示为

$$R_{n}^{i}=\left[\log_2\left(1+\mathrm{SINR}_{n}^{i}\right)-\max_{e\in\Phi_e}\log_2\left(1+\mathrm{SINR}_{e}^{i}\right)\right]^{+}\tag{6}$$

由于窃听信道的瞬时信道状态未知，网络无法获取精确的保密速率指标，因此本文以保密连接概率 $\mathbb{P}_{\mathrm{r}}\{R_{n}^{i}\geq R_{n}^{\mathrm{thr}}\}$ 为指标衡量下行链路的保密性能。

定理 1　当协作组内基站到窃听者的距离近似相等时，在子载波 i 上，下行链路 n 的保密连接概率可表示为

$$\mathbb{P}_{\mathrm{r}}\left\{R_{n}^{i}\geq R_{n}^{\mathrm{thr}}\right\}=\exp\left(-2\pi\lambda_e\prod_{q\neq n,q\in S_i}\left(1+\gamma_i P_q\right)^{-1}\cdot\int_0^{\infty}\exp\left(-\frac{\gamma_i\sigma^{2}}{r_{e,n}^{-\alpha}}\right)r_{e,n}\mathrm{d}r_{e,n}\right)\tag{7}$$

其中，R_{n}^{thr} 表示下行链路 n 的保密速率需求，$\gamma_i=\left(1+\mathrm{SNIR}_{n}^{i}\right)2^{-R_{n}^{\mathrm{thr}}}-1$。

证明　当多个下行链路形成协作组进行保密传输时，由式(6)得，在子载波 i 上，基站 n 的保密连接概率可表示为

$$\begin{aligned}\mathbb{P}_{\mathrm{r}}\left\{R_{n}^{i}\geq R_{n}^{\mathrm{thr}}\right\}&=\mathbb{P}_{\mathrm{r}}\left(\max_{e\in\Phi_e}\left(\mathrm{SINR}_{e}^{i}\right)\leq\gamma_i\right)\\&=\mathbb{P}_{\mathrm{r}}\left(\max_{e\in\Phi_e}\left\{\frac{\left|\boldsymbol{g}_{e,n}^{i}\boldsymbol{w}_{n}^{i}\right|^{2}r_{e,n}^{-\alpha}P_n}{I_{S_i}+\sigma^{2}}\right\}\leq\gamma_i\right)\\&=E_{\Phi_e}\left[\prod_{e\in\Phi_e}\mathbb{P}_{\mathrm{r}}\left(\left|\boldsymbol{g}_{e,n}^{i}\boldsymbol{w}_{n}^{i}\right|^{2}\leq\frac{\gamma_i\left(I_{S_i}+\sigma^{2}\right)}{r_{e,n}^{-\alpha}}\right)\right]\end{aligned}\tag{8}$$

由泊松点过程的性质[18]可得，式(8)可进一步化简为

$$\begin{aligned}&\mathbb{P}_{\mathrm{r}}\left\{R_{n}^{i}\geq R_{n}^{\mathrm{thr}}\right\}\\&=\exp\left(-2\pi\lambda_e\int_0^{\infty}\left(1-E_{I_{S_i}}\left[\mathbb{P}_{r}\left(\left|\boldsymbol{g}_{e,n}^{i}\boldsymbol{w}_{n}^{i}\right|^{2}\leq\frac{\gamma_i\left(I_{S_i}+\sigma^{2}\right)}{r_{e,n}^{-\alpha}}\right)\right]\right)r_{e,n}\mathrm{d}r_{e,n}\right)\end{aligned}\tag{9}$$

由于 $\boldsymbol{w}_{n}^{i}$ 与 $\boldsymbol{g}_{e,n}^{i}$ 相互独立，假设 $h_{e,n}^{i}\triangleq\left|\boldsymbol{g}_{e,n}^{i}\boldsymbol{w}_{n}^{i}\right|^{2}\sim\exp(1)$[17]，因此，

$$\mathbb{P}_{\mathrm{r}}\left(h_{e,n}^{i}\leq\frac{\gamma_i\left(I_{S_i}+\sigma^{2}\right)}{r_{e,n}^{-\alpha}}\right)=1-\exp\left(-\frac{\gamma_i\left(I_{S_i}+\sigma^{2}\right)}{r_{e,n}^{-\alpha}}\right)\tag{10}$$

代入式(9)可得，

$$\begin{aligned}&\mathbb{P}_{\mathrm{r}}\left\{R_{n}^{i}\geq R_{n}^{\mathrm{thr}}\right\}\\&=\exp\left(-2\pi\lambda_e\int_0^{\infty}E_{I_{S_i}}\left[\exp\left(-\frac{\gamma_i\left(I_{S_i}+\sigma^{2}\right)}{r_{e,n}^{-\alpha}}\right)\right]r_{e,n}\mathrm{d}r_{e,n}\right)\end{aligned}\tag{11}$$

其中，

$$\begin{aligned}&E_{I_{S_i}}\left[\exp\left(-\frac{\gamma_i\left(I_{S_i}+\sigma^{2}\right)}{r_{e,n}^{-\alpha}}\right)\right]\\&=E_{h_{e,q}^{i}}\left[\exp\left(-\frac{\gamma_i\sum\limits_{q\neq n,q\in S_i}P_q h_{e,q}^{i}r_{e,q}^{-\alpha}}{r_{e,n}^{-\alpha}}\right)\right]\exp\left(-\frac{\gamma_i\sigma^{2}}{r_{e,n}^{-\alpha}}\right)\\&=\exp\left(-\frac{\gamma_i\sigma^{2}}{r_{e,n}^{-\alpha}}\right)\prod_{q\neq n,q\in S_i}E_{h_{e,q}^{i}}\left[\exp\left(-\frac{\gamma_i P_q h_{e,q}^{i}r_{e,q}^{-\alpha}}{r_{e,n}^{-\alpha}}\right)\right]\end{aligned}\tag{12}$$

由于 $h_{e,q}^{i}\triangleq\left|\boldsymbol{g}_{e,q}^{i}\boldsymbol{w}_{q}^{i}\right|^{2}\sim\exp(1)$，因此，式(12)中，

$$E_{h_{e,q}^i}\left[\exp\left(-\frac{\gamma_i P_q h_{e,q}^i r_{e,q}^{-\alpha}}{r_{e,n}^{-\alpha}}\right)\right]=\left(1+\frac{\gamma_i P_q r_{e,q}^{-\alpha}}{r_{e,n}^{-\alpha}}\right)^{-1} \tag{13}$$

将式(12)，式(13)代入式(11)得

$$\begin{aligned}&\mathbb{P}_{\mathrm{r}}\left\{R_n^i\geq R_n^{\mathrm{thr}}\right\}\\&=\exp\left(-2\pi\lambda_e\int_0^{\infty}\prod_{q\neq n,q\in S_i}\left(1+\frac{\gamma_i P_q r_{e,q}^{-\alpha}}{r_{e,n}^{-\alpha}}\right)^{-1}\right.\\&\left.\cdot\exp\left(-\frac{\gamma_i\sigma^2}{r_{e,n}^{-\alpha}}\right)r_{e,n}\mathrm{d}r_{e,n}\right)\end{aligned} \tag{14}$$

令 $\Delta_{n,q}$ 表示基站 n 和基站 q 到窃听者 e 的距离差，式中 $\gamma_i P_q r_{e,q}^{-\alpha}/r_{e,n}^{-\alpha}$ 可表示为

$$\begin{aligned}\frac{\gamma_i P_q r_{e,q}^{-\alpha}}{r_{e,n}^{-\alpha}}&=\gamma_i P_q\left(\frac{r_{e,n}}{r_{e,q}}\right)^{\alpha}=\gamma_i P_q\left(\frac{r_{e,n}}{r_{e,n}+\Delta_{n,q}}\right)^{\alpha}\\&=\gamma_i P_q\left(1-\frac{\Delta_{n,q}}{r_{e,n}+\Delta_{n,q}}\right)^{\alpha}\end{aligned} \tag{15}$$

当 $r_{e,n}\gg\Delta_{n,q}$ 时，即各个基站到窃听者的绝对距离远远大于各个基站到窃听者的相对距离时，$\gamma_i P_q r_{e,q}^{-\alpha}/r_{e,n}^{-\alpha}\approx\gamma_i P_q$，代入式(14)，定理 1 得证。

这一条件适用于协作组内基站密集部署，距离窃听者较远的场景，此时可认为协作组内基站到窃听者的距离近似相等，在这一情况下也不需知道窃听者的具体位置。

观察式(4)-式(7)可发现，各个基站如何形成协作组，以及如何为各个协作组分配子载波将直接决定系统的保密性能。令 $\Pi(\mathcal{P})$ 表示集合 $\mathcal{P}$ 的划分结构集合，贝尔数 $\mathcal{B}_{\mathcal{P}}=\sum_{i=1}^{I}S(\mathcal{P},i)$ 表示 $\Pi(\mathcal{P})$ 中集合划分 $\pi_{\mathcal{P}}$ 的数目，其中 $S(\mathcal{P},k)$ 表示将 $\mathcal{P}$ 划分为 i 个子集合时可能的组合数目。$\mathcal{B}_{\mathcal{P}}$ 将随子载波数目和用户数目呈几何级增长，这使得集中式的最优化资源分配算法的计算复杂度急剧增大，并且在密集网络中，微小区基站趋向于个人化部署，具有一定的自私属性，这进一步增加了集中式资源分配算法的实现难度。联盟博弈是一种分析博弈参与者如何形成协作关系的数学工具，本文利用联盟博弈对各个基站的协作过程进行分析。

3 基于联盟形成博弈的下行链路保密资源分配

本节利用联盟形成博弈分析下行链路的保密协作问题，首先将下行链路定义为联盟博弈的参与者，每个博弈参与者寻求组成最优的协作组及子载波实现各自的保密传输。

3.1 下行链路联盟博弈

定义 2 令二元组 $(\mathcal{P},\boldsymbol{v})$ 表示联盟博弈，其中，$\mathcal{P}$ 表示博弈参与者集合，$\boldsymbol{v}:S_i\rightarrow\mathbb{R}^{S_i}$ 表示联盟划分函数，$\boldsymbol{v}(S_i)$ 是联盟成员效用函数向量的闭凸集合。

下行链路 n 在子载波 i 上的效用函数：

$$v(n,S_i)=\begin{cases}\mathbb{P}_{\mathrm{r}}\left\{R_n^i\geq R_n^{\mathrm{thr}}\right\}, & n\in S_i,\ |S_i|\leq M\\0, & n\notin S_i\end{cases} \tag{16}$$

其中，第 1 个条件表示下行链路 n 参与联盟 S_i 的获得收益，第 2 个条件表示下行链路 n 不参与联盟 S_i 的收益。由式(7)知，提出的联盟博弈是效用不可转移的，联盟 S_i 的效用 $\boldsymbol{v}(S_i)$ 可表示为

$$\begin{aligned}\boldsymbol{v}(S_i)=\Big\{\Big|\boldsymbol{v}(S_i)\in R^{|S_i|}\Big|\boldsymbol{v}(S_i)=\big(&v(1,S_i),\\&v(2,S_i),\cdots,v\big(|S_i|,S_i\big)\big)\Big\}\end{aligned} \tag{17}$$

联盟博弈关注联盟参与者是否会形成相互分割的联盟结构，当任意增大联盟规模均能够提高联盟内参与者的收益时，该联盟博弈是超可加的，此时联盟成员会相互协作形成唯一的联盟协作组，而不会形成相互分割的联盟结构。

在所提的联盟形成博弈中，为了避免对其余协作用户的干扰，下行链路的波束赋形向量 $\boldsymbol{w}_n^i$ 必须在其余用户信道的零空间上进行构造，因此，联盟成员的数目不能多于基站的天线数目，所提的联盟博弈会形成多个相互分离的联盟协作组，下面介绍多个下行链路如何自组织地形成协作联盟。

3.2 下行链路联盟形成算法

在联盟博弈的过程中，每个下行链路根据自身的保密性能需求和当前所处联盟提供的保密增益，综合选择所要加入或退出的联盟，通过联盟的多轮分裂合并，形成稳定的保密联盟划分。

定义 3 令 $\mathcal{R}=\{R_1,R_2,\cdots,R_l\}$, $\mathcal{S}=\{S_1,S_2,\cdots,S_m\}$ 表示子集 $\mathcal{A}\subset\mathcal{P}$ 的两个划分结构，即 $\bigcup_{j=1}^{m}S_j=\mathcal{A},\bigcup_{j=1}^{m}R_j=\mathcal{A}$。$\mathcal{S}\rhd\mathcal{R}$ 表示相对于联盟划分结构 $\mathcal{R}$，博弈参与者偏好于以联盟划分结构 $\mathcal{S}$ 形成协作关系。

根据联盟博弈的群体理性原则[9]，下行链路参与协作的前提是自身的保密效用不因协作而降低，并且至少有一个用户的效用因为协作而有所提高，联盟协作组才有可能成立。因此，博弈参与者的偏好关系可表示为

$$\left.\begin{aligned}&\forall n\in\mathcal{A},\mathcal{S}\rhd\mathcal{R}\Leftrightarrow v(n,\mathcal{S})\geq v(n,\mathcal{R})\\&\exists n\in\mathcal{A},\mathcal{S}\rhd\mathcal{R}\Leftrightarrow v(n,\mathcal{S})>v(n,\mathcal{R})\end{aligned}\right\} \tag{18}$$

与文献[14]不同，在提出的博弈模型中，除了需要对协作组进行划分外，还需对每个联盟使用的子载波进行分配，最终所形成的联盟划分中的联盟个数与子载波数目相同，因此，本文利用子载波索引

对联盟划分结构进行编号，与此同时，为了建模便利，引入虚拟子载波 0，用来容纳无法在其余子载波上获得服务的用户。所提的联盟划分结构可表示为 $\mathcal{S}=\{S_0,S_1,\cdots,S_I\}$，其中，$S_0$ 表示无法获得服务的下行链路集合，$\forall n\in S_0, v\left(n,S_0\right)=0$。$S_i,1\le i\le I$ 表示子载波 i 上形成的保密协作联盟。

根据上述联盟偏好属性，所提联盟博弈的联盟形成规则可表示为

$$\left.\begin{aligned}&\forall n\in S_i,m\in S_j,n\ne m,\\&\text{if } v\left(n,S_j\bigcup\{n\}\right)>v\left(n,S_i\right)\text{ and}\\&\quad v\left(m,S_j\bigcup\{n\}\right)\ge v\left(m,S_j\right)\\&\text{Joining}:\ S_j=S_j\bigcup\{n\}\\&\text{Quitting}:S_i=S_i\setminus\{n\}\end{aligned}\right\}\tag{19}$$

该形成规则表明当下行链路所在联盟提供的保密增益小于其他联盟时，下行链路选择跳出当前联盟，并加入新的具备更高保密增益的联盟进行协作。为了形成稳定联盟划分结构，假设当某个联盟成员正在形成联盟结构时，联盟内其余成员保持当前的协作状态[19]。

3.3 算法实现及复杂度分析

各个微小区基站能够通过控制信道获取各个子载波上相邻小区的位置、功率以及用户数等信息，并通过信道估计获取协作组内用户的信道状态信息。在获取相邻小区的信息后，基站能够将用户身份信息设置为下行链路标识，通过控制信道与相邻基站进行博弈交互操作，启动各个下行链路的协商过程。按照式(18)所示的联盟形成规则，在载波数一定的情况下，算法的复杂度主要取决于各个微小区基站的协商次数决定，在初始条件下，每个微小区需要与所有的相邻小区进行协商，总协商次数为 $N(N+1)/2$，算法的复杂度为 $o(N^2)$。但是随着算法的执行，当微小区选择到合适的联盟时，则不再参与联盟形成过程，算法的复杂度会逐渐降低，并收敛为稳定的联盟结构。提出的联盟博弈流程如表 1 所示。

表 1 联盟博弈流程

步骤 1	初始化，t=0，所有的下行链路初始时刻均处在虚拟子载波 0，网络被划分为初始联盟结构 $\pi_{\mathcal{P}}^0=\{S_0\}$, $S_0=\mathcal{P}$；
步骤 2	基于现有联盟划分结构 $\pi_{\mathcal{P}}^t$，下行链路 $n\in S_i$, $0\le i\le I$ 随机选择要加入的潜在保密协作联盟 $S_j, j\ne i$，依据式(7)和式(17)计算加入联盟 S_j 后能够取得的潜在收益 $v\left(n,S_j\bigcup\{n\}\right)$；
步骤 3	下行链路 n 对比现有联盟提供的保密增益 $v(n,S_i)$，当满足式(19)时，下行链路 n 脱离 S_i，加入联盟 S_j，否则下行链路 n 继续留在当前联盟 S_i。博弈形成新的联盟结构 $\pi_{\mathcal{P}}^{t+1}$；
步骤 4	当所有下行链路均不改变联盟划分结构，即 $\pi_{\mathcal{P}}^{t+1}=\pi_{\mathcal{P}}^t$ 时，联盟博弈形成稳定的联盟划分结构，博弈结束，所有下行链路按照 $\pi_{\mathcal{P}}^{t+1}$ 确定的协作关系进行保密通信。否则，联盟没有形成稳定的联盟结构，令 t=t+1，跳转到步骤 2。

引理　一个集合划分 $\pi_{\mathcal{P}}=\{S_1,S_2,\cdots,S_I\}$ 是 $\mathbb{D}_{hp}$ 稳定的[20]，当且仅当具备如下条件时：

(1)对于任意的 $i\in\{1,2,\cdots,I\}$ 和任意的划分 $\{R_1,R_2,\cdots,R_m\}$ of $S_i\in\pi_{\mathcal{P}}$，均有 $\{R_1,R_2,\cdots,R_m\}\not\rhd S_i$。

(2)对于任意的 $i\in\{1,2,\cdots,I\}$，均有

$$\bigcup_{i\in\{1,2,\cdots,I\}}\not\trianglerighteq\{S_i\mid i\in\{1,2,\cdots,I\}\}$$

上述两个条件分别给出了联盟形成博弈在分裂和合并两个方向上的稳定性约束。

定理 2　以任意的联盟划分结构为初始状态，提出的联盟形成博弈是 $\mathbb{D}_{hp}$ 稳定的，即能够收敛于稳定的联盟划分结构。

证明　在本文设计的博弈规则中，加入和退出的过程分别对应引理中的两个条件，博弈参与者的每次行动均会产生新的集合划分结构，博弈过程可表示为 $\pi_{\mathcal{P}}^0\to\pi_{\mathcal{P}}^1\to\cdots\to\pi_{\mathcal{P}}^t\to\pi_{\mathcal{P}}^{t+1}$，观察式(19)可发现，博弈参与者的博弈趋势是退出低收益的联盟并加入高收益的联盟，因此 $\pi_{\mathcal{P}}^{t+1}\rhd\pi_{\mathcal{P}}^t, t\ge1$，由于集合划分结构被子载波数限制并且参与博弈的成员数量是有限的，因此经过有限轮迭代，各个博弈参与者的效用达到稳定值，此时任何的加入和退出行动均不会带来效用的提升，所提的联盟博弈能够收敛于稳定的联盟划分结构。　　证毕

4　仿真分析

本节对提出的算法(CCA)进行仿真，假设无线信道的小尺度衰落服从均值为 0，方差为 1 的瑞利衰落，大尺度路径衰落因子 $\partial=2$，下行链路的保密速率需求 $R_n^{\text{thr}}=1\ \text{bit/(s}\cdot\text{Hz)}$，与此同时，为简化分析，假设基站到合法用户的距离 $r_{e,n}=10\ \text{m}$。在仿真中与随机协作算法(RCA)、贪婪协作算法(GCA)进行性能对比，其中在随机协作算法中，各条下行链路随机选择子载波形成协作联盟进行保密通信，在贪婪协作算法中，各条下行链路按照优先级依次选择最优的子载波形成协作联盟进行保密通信。利用蒙特卡洛方法进行 10000 次独立实验，并求解各次实验结果的均值。

设置 $P_n/\sigma^2=18\ \text{dB}$，窃听者的分布密度 $\lambda_e=1$，基站数目 $N=10$，下行链路平均连接概率随子载波数目的变化曲线如图 2 所示，随着天线数

目增加，所提算法的平均保密连接概率优于贪婪协作算法和随机协作算法。并且随着子载波数目的增大，所提算法和贪婪协作算法的平均保密连接概率均逐渐变大，而随机联盟协作算法的平均连接概率逐渐减小，这是由于子载波数目增多提高了频域信道的丰富性，在所提算法与贪婪算法中，每条下行链路有更大的机会选择到优势联盟进行协作通信，而随机协作算法没有联盟择优过程，子载波数目增多反而降低了下行链路形成协作联盟的机会。

设置窃听者的分布密度 $\lambda_e = 1$，子载波数目 $I = 10$，天线数目 $M = 4$，下行链路平均连接概率随基站数目的变化曲线如图 3 所示，随着基站数目和发射功率的增加，所提算法的保密连接概率逐渐增大并且优于对比算法，这是由于在所提算法中，联盟形成的过程是下行链路相互选择和相互匹配的过程，基站数目增加，增大了下行链路匹配到最优协作联盟的机会。

设置 $P_n / \sigma^2 = 18$ dB，子载波数目 $I = 10$，天线数目 $M = 4$，下行链路平均连接概率随窃听者分布密度的变化曲线如图 4 所示，随着窃听者密度增大，所提算法的平均保密连接概率逐渐下降，但仍然优于对比算法。定义所有用户完成一轮博弈策略选择为一次算法迭代，平均迭代次数随基站数目的变化曲线如图 5 所示，经过大约 3 次左右的迭代，所提算法能够形成稳定的联盟划分结构，迭代次数多于贪婪算法，这说明所提算法通过牺牲部分算法效率换来了下行链路系统的保密性能提升。

5 结论

本文在窃听者瞬时信道状态和位置未知的情况下，针对多小区下行链路的保密协作问题，提出一种基于联盟博弈的多小区下行链路保密协作算法，利用 CoMP 协同赋形技术在降低小区间干扰的同时，防止保密信息扩散。在此基础上，将下行链路建模为联盟博弈参与者，建立以保密连接概率为效用的联盟博弈模型，通过设计加入和退出规则，实现了下行链路自组织的高效子载波分配和保密协作联盟形成，理论分析表明所提方法具有收敛性，仿真结果表明所提算法的保密性能优于传统的联盟协作算法。

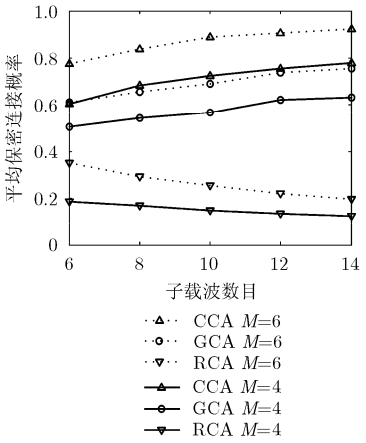

图 2 平均保密连接概率随子载波数目变化趋势

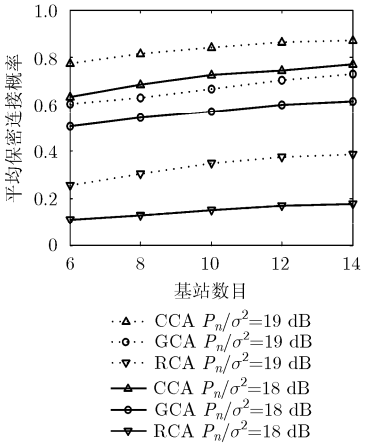

图 3 平均保密连接概率随基站数目变化趋势

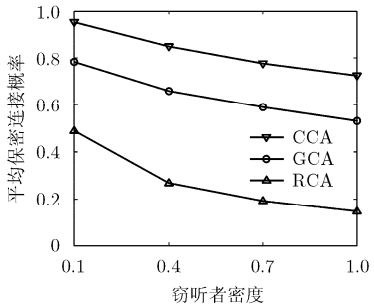

图 4 平均保密连接概率随窃听者密度变化趋势

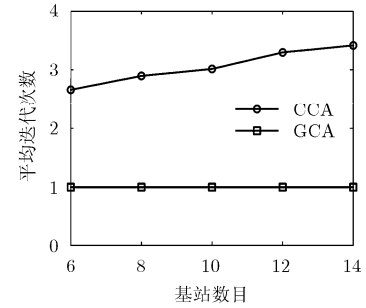

图 5 迭代次数随基站数目变化趋势

参 考 文 献

[1] GOEL S and NEGI R. Guaranteeing secrecy using artificial noise[J]. *IEEE Transactions on Wireless Communications*, 2008, 7(6): 2180–2189. doi: 10.1109/TWC.2008.060848.

[2] JEONG S, LEE K, HUH H, *et al*. Secure transmission in downlink cellular network with a cooperative jammer[J].

IEEE Wireless Communications Letters, 2013, 2(4): 463–466. doi: 10.1109/WCL.2013.052813.130272.

[3] ZHAO Rui, HUANG Yongming, WANG Wei, *et al*. Ergodic achievable secrecy rate of multiple-antenna relay systems with cooperative jamming[J]. *IEEE Transactions on Wireless Communications*, 2016, 15(4): 2537–2551. doi: 10.1109/TWC.2015.2504526.

[4] CEPHELI O, DARTMANN G, KARABULUT G, *et al*. Beamforming aided interference management for improved secrecy in multicell environments[C]. Proceedings of 20th European Wireless Conference, Barcelona, 2014: 1–6.

[5] CHEN Xiaoming and CHEN H. Physical layer security in multi-cell MISO downlinks with incomplete CSI — A unified secrecy performance analysis[J]. *IEEE Transactions on Signal Processing*, 2014, 62(23): 6286–6297. doi: 10.1109/TSP.2014.2362890.

[6] ZHU Fengchao and YAO Minli. Improving physical-layer security for crns using sinr-based cooperative beamforming[J]. *IEEE Transactions on Vehicular Technology*, 2016, 65(3): 1835–1841. doi: 10.1109/TVT.2015.2412152.

[7] XU X, HE B, YANG W, *et al*. Secure transmission design for cognitive radio networks with poisson distributed eavesdroppers[J]. *IEEE Transactions on Information Forensics and Security*, 2016, 11(2): 373–387. doi: 10.1109/TIFS.2015.2500178.

[8] YAO J, FENG S, ZHOU X, *et al*. Secure routing in multihop wireless Ad-hoc networks with decode-and-forward relaying [J]. *IEEE Transactions on Communications*, 2016, 64(2): 753–764. doi: 10.1109/TCOMM.2015.2514094.

[9] SAAD W, HAN Z, DEBBAH M, *et al*. Coalitional game theory for communication networks[J]. *IEEE Signal Processing Magazine*, 2009, 26(5): 77–97. doi: 10.1109/MSP.2009.000000.

[10] SAAD W, HAN Z, BASAR T, *et al*. Physical layer security: Coalitional games for distributed cooperation[C]. 7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, Seoul, 2009: 1–8. doi: 10.1109/WIOPT.2009.5291619.

[11] HOU Lijun and FU Xiaomei. Physical layer security with dynamic behaviour cooperator based on coalitional game[J]. *IET Communications*, 2014, 8(8): 1258–1264. doi: 10.1049/iet-com.2013.0274.

[12] ZHANG Rongqing, SONG Lingyang, HAN Zhu, *et al*. Distributed coalition formation of relay and friendly jammers for secure cooperative networks[C]. IEEE International Conference on Communications, Kyoto, 2011: 1–6. doi: 10.1109/icc.2011.5962513.

[13] CAO Yang and WEI Jiaolong. Distributed coalition formation for selfish relays and eavesdroppers in wireless networks: A job-hopping game[C]. International Conference on Wireless Communications & Signal Processing, Huangshan, 2012: 1–6. doi: 10.1109/WCSP.2012.6542873.

[14] ZHANG Hang, WANG Tianyu, SONG Linyang, *et al*. Interference improves PHY security for cognitive radio networks[J] *IEEE Transactions on Information Forensics and Security*, 2016, 11(3): 609–620. doi: 10.1109/TIFS.2015.2500184.

[15] ZHANG Rongqing, CHENG Xiang, and YANG Liuqing. Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks[J]. *IEEE Transactions on Wireless Communications*, 2016, 15(8): 5651–5663. doi: 10.1109/TWC.2016.2565579.

[16] 3GPP TR 36.819. Coordinated multi-point operation for LTE physical layer aspects[S]. 2011.

[17] WANG Huiming, ZHENG Tongxing, YUAN Jinhong, *et al*. Physical layer security in heterogeneous cellular networks[J]. *IEEE Transactions on Communications,* 2016, 64(3): 1204–1219. doi: 10.1109/TCOMM.2016.2519402.

[18] DHILLON H S, GANTI R K, BACCELLI F, *et al*. Modeling and analysis of K-tier downlink heterogeneous cellular networks[J]. *IEEE Journal on Selected Areas in Communications*, 2012, 30(3): 550–560. doi: 10.1109/JSAC.2012.120405.

[19] SUDARSHAN G, DUSIT N, MEHDI B, *et al*. Dynamic coalition formation for network MIMO in small cell networks [J]. *IEEE Transactions on Wireless Communications*, 2013, 12(10): 5360–5372. doi: 10.1109/TWC.2013.090513.130516.

[20] APT K R and WITZEL A. A generic approach to coalition formation[J]. *International Game Theory Review*, 2009, 11(3): 347–367.

李明亮：　男，1988 年生，博士生，研究方向为物理层安全.
郭云飞：　男，1963 年生，教授，研究方向为网络空间安全.
黄开枝：　女，1973 年生，教授，研究方向为移动通信安全.