基于安全保护域的增强型多点协作传输机制

黄开枝[①] 王 兵[*①] 许晓明[①②] 康小磊[①] 张 波[①]
[①](国家数字交换系统工程技术研究中心 郑州 450002)
[②](解放军理工大学通信工程学院 南京 210007)

摘 要：现有针对异构蜂窝网多点协作安全传输的研究集中于增强主信道质量以提升安全性，然而多基站协作又使基站和窃听者之间的平均距离变近，网络的安全性受限于距离协作基站较近的窃听者。针对该问题，该文提出一种基于安全保护域的增强型多点协作传输机制。然后，理论分析了用户的连接中断概率、安全中断概率以及安全吞吐量。进一步，以最大化安全吞吐量为目标，优化协作微基站的发射功率以及有用信息功率分配比例系数。仿真结果表明，相比于传统的多点协作安全传输机制，在存在严重安全威胁(窃听者密度较大)的场景下，所提机制可以实现非零系统安全吞吐量；在存在较小安全威胁(窃听者密度较小)的场景下，系统安全吞吐量最大可提升 76.1%。

关键词：异构蜂窝网；物理层安全；安全保护域；多点协作传输机制；人工噪声
中图分类号： TN92 **文献标识码**： A **文章编号**：1009-5896(2018)01-0108-08
DOI: 10.11999/JEIT170478

An Enhanced Coordinated Multipoint Transmission Policy Based on Secrecy Guard Zone

HUANG Kaizhi[①] WANG Bing[①] XU Xiaoming[①②] KANG Xiaolei[①] ZHANG Bo[①]
[①](*National Digital Switching System Engineering & Technological Research Center*, *Zhengzhou* 450002, *China*)
[②](*College of Communications Engineering*, *PLA University of Science and Technology*, *Nanjing* 210007, *China*)

Abstract: The existing researches on Coordinated Multi-Point transmission (CoMP) secure transmission in heterogeneous cellular networks mainly focus on improving the quality of the main channel to enhance security. However, CoMP also makes the average distance between base station and eavesdropper close which makes the security threat more severe. Based on secrecy guard zone, an enhanced CoMP policy is proposed in this paper. Then, the connection outage probability, secrecy outage probability and secrecy throughput are analyzed. Furthermore, the transmission power and power allocation factor are designed very carefully to maximize the secrecy throughput. Simulation results show that compared with conventional CoMP policy, the proposed policy can not only achieve non-zero secrecy throughput when faced with severe security threats (i.e. for larger eavesdropper density), but also improve the secrecy throughput of 76.1% at most when faced with small security threats (i.e. for smaller eavesdropper density).

Key words: Heterogeneous cellular networks; Physical layer security; Secrecy guard zone; Coordinated Multi-Point transmission (CoMP); Artificial noise

1 引言

异构蜂窝网络通过在宏基站的覆盖区域内合理部署低功率的微基站和微微基站，可以显著提升资源利用率与网络容量，成为 5G 网络部署的重要形态之一[1,2]。然而，无线信道的广播特性和动态接入机制的开放性，使得异构蜂窝网络容易受到恶意节点的攻击和窃听；此外，异构蜂窝网拓扑结构的动态变化、终端在各层网络切换时需要密钥信息的频繁扩展和搜索，给密钥的分发和管理提出了挑战[3]。因此，亟需挖掘异构蜂窝网中各层的统一属性以保证信息传输安全。近些年兴起的物理层安全技术利用无线信道特性解决信息安全问题，为保证异构蜂窝网络信息传输安全开辟了一条新途径。

目前，异构蜂窝网物理层安全的研究主要集中于性能分析[4]、信号处理[5–10]、资源管理[11]等方面。考虑异构蜂窝网中站点部署的随机性以及窃听者的隐匿性，已有学者借助于随机几何理论开展了相关

收稿日期：2017-05-17；改回日期：2017-08-23；网络出版：2017-11-01
*通信作者：王兵 wangbing_xd@163.com
基金项目：河南省科技攻关计划(152102210013)，国家 863 计划项目(2015AA01A708)，国家自然科学基金(61701538, 61171108, 61471396)
Foundation Items: The Program for Science and Technology Development of Henan Province (152102210013), The National 863 Program of China (2015AA01A708), The National Natural Science Foundation of China (61701538, 61171108, 61471396)

物理层安全的研究[4,6−10]。针对基站非协作的场景，文献[4]利用泊松点过程对 k 层异构蜂窝网中基站、用户和窃听者位置进行建模，分析了用户的安全覆盖概率和平均安全速率。为防止用户接入平均接收信号增益较低的基站，文献[8]通过设计一种门限值机制对用户的连接中断概率、安全中断概率，以及网络整体的安全吞吐量进行了分析。进一步，文献[9]对采用大规模 MIMO 技术提升异构蜂窝网物理层安全性能进行了初步探索。上述基站非协作的场景中，典型用户在接收服务基站信号的同时会受到其他基站的严重干扰，使用户的信干噪比受限。针对该不足，多点协作传输(Coordinated Multi-Point transmission, CoMP)技术以其在缓解蜂窝网中层间、层内干扰，提高终端接收信号功率方面的优势应运而生[12]。考虑系统的安全性，文献[13]将多点协作技术和方向调制结合，对小规模、确定性网络中不同调制方式对安全性能的影响进行了分析。进一步，考虑网络拓扑的随机性，文献[10]利用多点协作传输技术增强了主信道质量，相比于无多点协作机制的网络安全性能增益得到了提升。然而多基站协作也使得窃听者和协作基站之间的平均距离变近，系统的安全性受限于距离协作基站较近的窃听者。

针对该问题，本文在宏基站、微基站和窃听者都随机分布的异构蜂窝网络中，提出一种基于安全保护域的增强型多点协作传输机制：首先，根据用户侧平均接收信号增益确定协作微基站；然后，以微基站为中心建立安全保护域，判断安全保护域内是否存在窃听者；最后，根据安全保护域内是否存在窃听者，确定协作策略：存在窃听者，利用叠加编码[14]理论，微基站协作发送信息的同时发送人工噪声(Artificial Noise, AN)，否则微基站仅协作发送信息。本文通过分析用户的安全中断概率、连接中断概率以及安全吞吐量，对系统的安全性、可靠性以及有效性进行了评估。进一步以最大化微基站网络安全吞吐量为目标，优化了微基站的发射功率及有用信息功率分配因子。仿真结果表明，相比于传统多点协作机制[10]，所提机制在存在严重安全威胁(窃听者密度较大)的场景下可以实现正的安全吞吐量，在存在较小安全威胁(窃听者密度较小)的场景下，系统安全吞吐量最大可以提升 76.1%。

2　系统模型

多点协作异构蜂窝网络模型如图 1 所示，宏基站、微基站、和窃听者位置分别服从节点密度为 λ_m，λ_s 和 λ_e 的均匀泊松点过程(Homogeneous Poisson Point Process, HPPP)，分别记作 ϕ_m，ϕ_s 和 ϕ_e。考虑宏基站不协作，微基站协作场景。用户接收功率只有满足 $P||Y||^{-\alpha}>\tau$ 的微基站参与协作，可以求得参与协作的微基站距离典型用户的距离要满足 $D\le(P/\tau)^{1/\alpha}$。如图 1，仅以用户为中心半径为 D 的圆内基站参与协作。微基站和宏基站使用相同的频谱资源，噪声影响可以忽略[15]。假设所有节点都是单天线，无线信道之间相互独立均服从均值为 1 的准静态 Rayleigh 衰落，大尺度路径损耗因子为 α。考虑窃听者间不协作的被动窃听场景，网络的安全性能取决于接收信号功率最强的窃听者。考虑到码本设计及宏基站、窃听信道 CSI 获知的困难性，本文使用固定安全信息速率 R_s [8]传输保密信息。

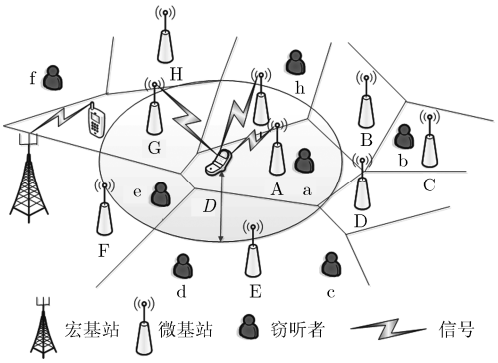

图 1 多点协作异构蜂窝网络模型

针对上述模型，现有多点协作安全传输的研究[10]从增强主信道的信道质量出发，利用多基站协作缓解干扰的同时提升用户接收功率，进而提升安全性。然而，多基站协作也使得窃听者和基站之间的平均距离变近，当协作微基站附近存在窃听者时，网络的整体安全性能将降低。如图 1 所示，协作微基站 A 很近的范围内就存在窃听者 a，窃听者会从基站 A 截获更强的保密信号，导致安全性能降低。

为对抗距离基站较近的窃听者，有学者引入了安全保护域[14,16−20]的思想，即假设基站可以感知一定范围内是否存在窃听者(感知方法可以分为金属检测、X 光检测、增强的热检测、本振信号检测等)。针对非协作传输场景，为提升系统的安全频谱效率和安全能量效率，Xu 等人[19]中假设只有在安全保护域内不存在窃听者时次用户才发送有用信息。ZHOU 等人[16]中假设保护域内存在窃听者时基站静默或者以全功率发送人工噪声，以系统吞吐量的降低换取了安全性的提升。可见，上述研究均通过引入安全保护域提升了系统安全性能，但如何在保证异构蜂窝网多点协作传输的同时，联合安全保护域和人工噪声的思想对抗距离基站较近的窃听者有待进一步研究。

针对上述问题，本文设计了一种基于安全保护域的增强型多点协作传输机制：以微基站为中心建

立安全保护域，判断安全保护域内是否存在窃听者。若存在窃听者，微基站在协作发送信息的同时发送人工噪声，以降低异构蜂窝网多点协作传输中距离协作微基站较近的窃听者带来的安全性能损失。

3 基于安全保护域的增强型多点协作传输机制

该机制主要分为以下 3 个步骤，具体实现如图 2 所示。

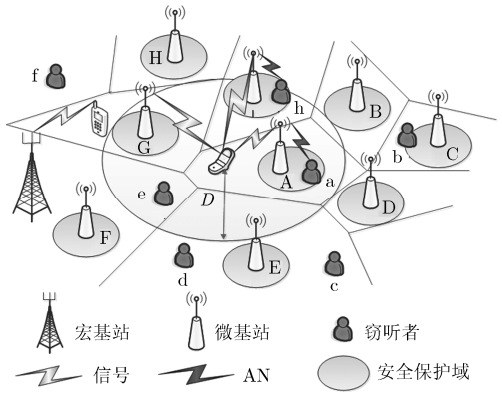

图 2 基于安全保护域的多点协作传输模型

步骤 1 协作微基站确定。根据用户侧平均接收信号增益确定协作微基站。为避免用户接入接收功率较低的微基站，借鉴文献[10]中的门限值机制，设定功率门限值 τ，用户接收功率只有满足 $P||Y||^{-\alpha}>\tau$ 的微基站参与协作，可以求得参与协作的微基站距离典型用户的距离要满足 $D\le(P/\tau)^{1/\alpha}$。另外，考虑协作微基站可以消除其他非协作微基站的干扰信号[15]。

步骤 2 安全保护域建立。基于安全保护域的思想[14,16–20]，以微基站为中心，d 为半径建立安全保护域，判断安全保护域内是否存在窃听者。为表述方便，将安全保护域内不存在窃听者的微基站称为第 1 类微基站(如图 2 中微基站 B)，否则，称为第 2 类微基站(如图 2 中微基站 A)。第 1 类微基站的位置分布记为 ϕ_s^1，其节点密度为 $\lambda_s^1=\lambda_s\exp\left(-\pi\lambda_e d^2\right)$，其中指数项表示任意一个微基站的安全保护域内无窃听者的概率。由于安全保护域的存在，ϕ_s^1 实际上不再为 HPPP，但文献[17]的研究表明存在安全保护域时发送节点的位置分布仍然近似服从 HPPP。第 2 类微基站的位置分布记为 ϕ_s^2，其节点密度为 $\lambda_s^2=\lambda_s\left[1-\exp\left(-\pi\lambda_e d^2\right)\right]$。

步骤 3 多点协作传输。安全保护域内若存在窃听者，运用叠加编码[14]理论，微基站以 kP_S 协作发送信息的同时，以 $(1-k)P_S$ 发送 AN，其中 k 为有用信息信号的功率分配比例系数；若不存在窃听者，微基站以功率 P_S 协作发送信息。

特别地，安全保护域并不是意味该基站服务的用户绝对安全，而是通过发送 AN 干扰窃听者，提升用户的安全性。另外，文献[10]中多点协作传输机制相当于本文中有用信息信号的功率分配比例系数 $k=1$ 时的特殊情况。

令 P_M 和 P_S 分别表示宏基站和微基站的功率，$\left\|Y_{a,b}\right\|$ 表示节点 a 和 b 之间的距离，$h_{a,b}$ 为均值为 0，方差为 1 的复高斯随机信道变量。因此，典型宏基站用户 v_0 接入宏基站 u_0 时接收到信号的信干比(Signal to Interference Ratio, SIR)为 SIR_m

$$=\frac{P_M\left\|Y_{u_0,v_0}\right\|^{-\alpha}\left|h_{u_0,v_0}\right|^2}{\sum\limits_{y\in\phi_m/\{u_0\}}P_M\left\|Y_{y,v_0}\right\|^{-\alpha}\left|h_{u_0,v_0}\right|^2+\sum\limits_{z\in\phi_s}P_S\left\|Y_{z,v_0}\right\|^{-\alpha}\left|h_{z,v_0}\right|^2} \tag{1}$$

令 $q=1,2$ 分别表示第 1 类微基站和第 2 类微基站，$m_{q|(q=1,2)}$ 表示参与协作的第 q 类基站的个数为 m_q，P_q 表示参与协作的第 q 类基站的功率。$\left\|r_{q,t}\right\|$ 表示第 q 类微基站中第 t 个微基站距离典型微基站用户的距离，假设用户可以消除其他基站发送的 AN，典型微基站用户 v_1 接收到信号的 SIR 为

$$\mathrm{SIR}_s=\frac{\left|\sum\limits_{q=1}^{2}\sum\limits_{t=1}^{m_q}\sqrt{P_q}\right|\left|r_{q,t}\right|^{-\alpha/2}\left|h_{q,t}\right|^2}{\sum\limits_{y\in\phi_m}P_M\left\|Y_{y,v_1}\right\|^{-\alpha}\left|h_{y,v_1}\right|^2} \tag{2}$$

考虑窃听者同时窃听两类协作微基站，取二者中的较大者作为窃听者的 SIR 。窃听节点 e_1 从第 1 类微基站 u_1 中窃听到的信号 SIR 为

$$\mathrm{SIR}_e^1=\frac{P_S\left\|Y_{u_1,e_1}\right\|^{-\alpha}\left|h_{u_1,e_1}\right|^2}{\sum\limits_{y\in\phi_m}P_M\left\|Y_{y,e_1}\right\|^{-\alpha}\left|h_{y,e_1}\right|^2+\sum\limits_{z\in\phi_s/\{u_1\}}P_S\left\|Y_{z,e_1}\right\|^{-\alpha}\left|h_{z,e_1}\right|^2} \tag{3}$$

类似地，窃听节点 e_2 从第 2 类微基站 u_2 中窃听到的信号 SIR 为

$$\mathrm{SIR}_e^2=\frac{kP_S\left\|Y_{u_2,e_2}\right\|^{-\alpha}\left|h_{u_2,e_2}\right|^2}{\sum\limits_{y\in\phi_m}P_M\left\|Y_{y,e_2}\right\|^{-\alpha}\left|h_{y,e_2}\right|^2+\sum\limits_{z\in\phi_s/\{u_2\}}P_S\left\|Y_{z,e_2}\right\|^{-\alpha}\left|h_{z,e_2}\right|^2+(1-k)P_S\left\|Y_{u_2,e_2}\right\|^{-\alpha}\left|h_{u_2,e_2}\right|^2} \tag{4}$$

故窃听者从两类微基站中接收到的信号 SIR 为

$$\mathrm{SIR}_e = \max\left(\max_{e_1\in\Phi_e/B(u_1,d)}\left(\mathrm{SIR}_e^1\right),\ \max_{e_2\in\Phi_e}\left(\mathrm{SIR}_e^2\right)\right) \quad (5)$$

4　性能分析

本节将对宏基站网络和微基站网络的连接中断概率(Connection Outage Probability, COP)，以及微基站网络的安全中断概率(Secrecy Outage Probability, SOP)进行求解。进一步结合 COP 和 SOP 对宏基站网络的可靠性、微基站网络的可靠性和安全性进行评估。最后，给出微基站网络安全吞吐量的理论表达式。

4.1 连接中断概率

4.1.1 宏基站用户的 COP　定义宏基站用户的连接中断 SIR 门限值为 $\theta_{\mathrm{co},m}=2^{R_t}-1$，其中 R_t 表示宏基站的信息传输速率，因此典型宏基站用户的 COP 可以表示为

$$P_{\mathrm{co},m} = 1-\mathbb{P}\left(\mathrm{SIR}_m > \theta_{\mathrm{co},m}\right) \quad (6)$$

命题 1　典型宏基站用户的 COP 为

$$P_{\mathrm{co},m}=1-\lambda_m\Big/\left[c_0\theta_{\mathrm{co},m}^{2/\alpha}\left(\lambda_m+\left(P_S/P_M\right)^{2/\alpha}\lambda_s\right)+\lambda_m\right] \quad (7)$$

其中，$c_0=\Gamma(1+2/\alpha)\Gamma(1-2/\alpha)$，$\lambda_m$ 和 λ_s 分别为宏微基站的密度。

由式(7)可以发现，$P_{\mathrm{co},m}$ 是关于 P_S 的增函数，为保证宏基站用户的可靠性，设定宏基站用户链路可靠性能约束 $P_{\mathrm{co},m}\le\delta_m$，可得 P_S 的上界为

$$\begin{aligned}P_S &\le P_{S,\mathrm{UB}_1}\\ &= P_M\left[\delta_m\lambda_m\Big/\left(\lambda_s\left(1-\delta_m\right)c_0\theta_{\mathrm{co},m}^{2/\alpha}\right)-\lambda_m/\lambda_s\right]^{\alpha/2}\end{aligned} \quad (8)$$

4.1.2 微基站用户的 COP　本节首先对微基站用户的连接概率进行分析，然后由连接概率和 COP 的定义 $P_{\mathrm{co},s}=1-P_{\mathrm{cov}}$，得到典型微基站用户的 COP。定义微基站用户 SIR 门限值为 $\theta_{\mathrm{co},s}=2^{R_t}-1$。由前节可知，微基站只有满足 $D\le\left(P/\tau\right)^{1/\alpha}$ 才可以参与协作。因此，有 $M_q=m_q$ 个微基站参与协作的概率为

$$\mathbb{P}\left(M_q=m_q\right)=\frac{\left(\pi\lambda_s^qD_q^2\right)^{m_q}}{m_q!}\exp\left(-\pi\lambda_s^qD_q^2\right) \quad (9)$$

由前文知 $r_{q,t}$ 为第 q 类微基站中第 t 个基站与典型用户间的距离，$r_{q,t}$ 在 D_q 内服从均匀分布，其概率密度函数为 $f_{r_{q,t}}\left(r_{q,t}\right)=2r_{q,t}/D_q^2$。用 $\boldsymbol{r}_q=\left[r_{q,1},r_{q,2},\cdots,r_{q,M_q}\right]$ 表示微基站和典型用户的距离矢量。由于 $r_{q,t}$ 的独立性，$\boldsymbol{r}_q$ 中元素的联合概率密度函数为

$$f_{\boldsymbol{r}_{q,t}}=\left(2^{m_q}\prod_{t=1}^{m_q}r_{q,t}\right)\Big/D_q^{2m_q},\quad 0\le r_{q,t}\le D_q \quad (10)$$

典型微基站用户的连接概率可以表示为

$$\begin{aligned}P_{\mathrm{cov}} &= \mathbb{P}\left(\mathrm{SIR}_s>\theta_{\mathrm{co},s}\right)=\sum_{m_1=0}^{\infty}\sum_{m_2=0}^{\infty}\mathbb{P}\left(M_1=m_1\right)\\ &\quad\cdot\mathbb{P}\left(M_2=m_2\right)P^c_{|\{m_1,m_2\}}\end{aligned} \quad (11)$$

命题 2　$P^c_{|\{m_1,m_2\}}$ 表示 m_1 个第 1 类微基站和 m_2 个第 2 类微基站参与协作时可以提供的覆盖概率，其表达式为

$$\begin{aligned}P^c_{|\{m_1,m_2\}}=&\int_{\boldsymbol{r}_1}\int_{\boldsymbol{r}_2}\exp\left(-\pi c_0\left(\frac{\theta_{\mathrm{co},s}P_M}{\sum_{q=1}^{2}\sum_{t=1}^{m_q}P_q\left\|r_{q,t}\right\|^{-\alpha}}\right)^{2/\alpha}\lambda_m\right)\\ &\cdot f_{\boldsymbol{r}_1}f_{\boldsymbol{r}_2}\mathrm{d}\boldsymbol{r}_1\mathrm{d}\boldsymbol{r}_2\end{aligned} \quad (12)$$

进一步可以得到典型微基站用户的连接概率为

$$\begin{aligned}P_{\mathrm{cov}} &= \exp\left\{-\pi\left(\lambda_s^1D_1^2+\lambda_s^2D_2^2\right)\right\}\\ &\quad\cdot\sum_{\{m_1=0\}}^{\infty}\sum_{\{m_2=0\}}^{\infty}\left[\frac{\left(\pi\lambda_s^1D_1^2\right)^{m_1}\left(\pi\lambda_s^2D_2^2\right)^{m_2}}{m_1!\,m_2!}P^c_{|\{m_1,m_2\}}\right]\end{aligned} \quad (13)$$

进一步，可以得到典型微基站用户的 COP 为

$$P_{\mathrm{co},s}=1-P_{\mathrm{cov}} \quad (14)$$

综合考虑式(12)-式(14)可以发现，$P_{\mathrm{co},s}$ 是一个关于 P_S 和 k 的减函数。给定 P_S，k 存在一个满足典型微基站用户链路可靠性约束 $P_{\mathrm{co},s}<\delta_s$ 的下界 $k\ge k_{\mathrm{LB}}=F_1\left(P_S\right)$，其中函数 $F_1(\bullet)$ 表示方程 $P_{\mathrm{co},s}\left(x,P_S\right)=\delta_s$ 的解；同理，给定 k，P_s 存在一个满足典型微基站用户链路可靠性约束 $P_{\mathrm{co},s}<\delta_s$ 的下界 $P_S\ge P_{S,\mathrm{LB}}=F_2\left(k\right)$，其中函数 $F_2(\bullet)$ 表示方程 $P_{\mathrm{co},s}\left(x,k\right)=\delta_s$ 的解。

由宏基站用户的 COP 表达式(7)和微基站用户的 COP 表达式(14)可以发现，宏基站用户的可靠性和微基站用户的可靠性之间存在关于 P_S 的折中关系。

4.2 安全中断概率

本节通过 SOP 对微基站网络的安全性能进行评估，SOP 表示至少存在一个窃听节点造成安全中断事件的概率。同样，定义微基站用户安全中断 SIR 门限值为 $\theta_{\mathrm{so},s}=2^{R_t-R_s}-1$，因此典型微基站用户的 SOP 为窃听者分别窃听第 1 类微基站和第 2 类微基站获得的最大 SIR_e 大于 $\theta_{\mathrm{so},s}$ 的概率，即

$$\begin{aligned}P_{\mathrm{so},s} &= \mathbb{P}\left\{\max\left(\max_{e_1\in\Phi_e/B(u_1,d)}\left(\mathrm{SIR}_e^1\right),\max_{e_2\in\Phi_e}\left(\mathrm{SIR}_e^2\right)\right)>\theta_{\mathrm{so},s}\right\}\\ &= 1-\mathbb{P}\left(\max_{e_1\in\Phi_e/B(u_1,d)}\left(\mathrm{SIR}_e^1\right)<\theta_{\mathrm{so},s}\right)\\ &\quad\cdot\mathbb{P}\left(\max_{e_2\in\Phi_e}\left(\mathrm{SIR}_e^2\right)<\theta_{\mathrm{so},s}\right)\triangleq 1-P^1P^2\end{aligned} \quad (15)$$

首先计算 P^1：

$$P^1=\mathbb{P}\left(\max_{e_1\in\Phi_e/B(u_1,d)}\frac{P_S\left\|Y_{u_1,e_1}\right\|^{-\alpha}\left|h_{u_1,e_1}\right|^2}{I_M\left(e_1\right)+I_S\left(e_1\right)}<\theta_{\mathrm{so},s}\right)$$

$$=\mathbb{E}_{\phi_m}\left\{\mathbb{E}_{\phi_s}\left\{\mathbb{E}_{\phi_e}\left\{\prod_{e_1\in\Phi_e/B(u_1,d)}\left(1-\mathbb{P}\left(\frac{P_S\left\|Y_{u_1,e_1}\right\|^{-\alpha}\left|h_{u_1,e_1}\right|^2}{I_M\left(e_1\right)+I_S\left(e_1\right)}>\theta_{\mathrm{so},s}\mid\phi_e,\phi_s,\phi_m\right)\right)\right\}\right\}\right\} \tag{16}$$

其中，$I_M(e_1)=\sum_{y\in\phi_m}P_M\left\|Y_{y,e_1}\right\|^{-\alpha}\left|h_{y,e_1}\right|^2$，$I_S(e_1)=\sum_{z\in\phi_s/\{u_1\}}P_S\left\|Y_{z,e_1}\right\|^{-\alpha}\left|h_{z,e_1}\right|^2$。

利用 PPP 生成函数，以及 Jensen 不等式可以得到 P^1 的理论下界：

$$P^1=\mathbb{E}_{\phi_m}\left\{\mathbb{E}_{\phi_s}\left\{\exp\left\{-\lambda_e\int_{R^2/B(u_1,d)}\mathbb{P}\left(\frac{P_S\left\|Y_{u_1,e_1}\right\|^{-\alpha}\left|h_{u_1,e_1}\right|^2}{I_M(e_1)+I_S(e_1)}>\theta_{\mathrm{so},s}\mid\phi_s,\phi_m\right)\mathrm{d}e_1\right\}\right\}\right\}$$

$$=\exp\left\{-\frac{\lambda_e\exp\left(-c_0\pi\theta_{\mathrm{so},s}^{2/\alpha}\left(\lambda_s+\left(P_M/P_S\right)^{2/\alpha}\lambda_m\right)d^2\right)}{c_0\theta_{\mathrm{so},s}^{2/\alpha}\left(\lambda_s+\left(P_M/P_S\right)^{2/\alpha}\lambda_m\right)}\right\} \tag{17}$$

类似地，可以得到 P^2 的下界：

$$P^2=\exp\left\{-\lambda_e\Big/\left[c_0\left(\theta_{\mathrm{so},s}/\left(k-(1-k)\theta_{\mathrm{so},s}\right)\right)^{2/\alpha}\left(\lambda_s+\left(P_M/P_S\right)^{2/\alpha}\lambda_m\right)\right]\right\} \tag{18}$$

由式(17)和式(18)，典型微基站用户的 SOP 上界为

$$P_{\mathrm{so},s}\le P_{\mathrm{so},s}^{\mathrm{UB}}=1-\exp\left\{-\frac{\lambda_e\exp\left(-c_0\pi\theta_{\mathrm{so},s}^{2/\alpha}\left(\lambda_s+\left(P_M/P_S\right)^{2/\alpha}\lambda_m\right)d^2\right)}{c_0\theta_{\mathrm{so},s}^{2/\alpha}\left(\lambda_s+\left(P_M/P_S\right)^{2/\alpha}\lambda_m\right)}\right.$$

$$\left.-\frac{\lambda_e}{c_0\left(\theta_{\mathrm{so},s}/\left(k-(1-k)\theta_{\mathrm{so},s}\right)\right)^{2/\alpha}\left(\lambda_s+\left(P_M/P_S\right)^{2/\alpha}\lambda_m\right)}\right\} \tag{19}$$

可以发现，$P_{\mathrm{so},s}$ 是关于 d 的减函数，这是因为保护域半径越大，存在窃听者的概率越大，微基站将会以更大的概率发送 AN。另外，$P_{\mathrm{so},s}$ 是关于 P_S 和 k 的增函数。满足微基站用户 SOP 门限值 ε_s 的条件下，给定 P_S，可以得到 k 的上界 k_{UB}；给定 k，可以得到 P_S 的另一个上界 P_{S,UB_2}。类似于对典型用户的分析，本节选择典型窃听者链路进行分析，精确的分析应该为遍历参与协作的每一个微基站，然后取其最大者作为窃听者获得的私密信息，故本文得到的是 SOP 的一个近似界。

由式(14)和式(19)可以发现，微基站用户的安全性和可靠性之间存在关于 P_S 和 k 的折中关系。

综合宏基站网络的 COP，微基站网络的 SOP, COP。P_S 和 k 不仅影响宏基站网络和微基站网络的可靠性折中关系，同时也影响微基站网络的安全性和可靠性折中关系，因此需要设计 P_S 和 k 使系统的整体性能最优。

4.3 安全吞吐量

为综合表征系统的安全性和可靠性，本文用安全吞吐量[18,21]对系统的整体性能进行评估，安全吞吐量为网络节点密度、可靠传输概率、安全传输概率和安全信息速率的乘积，即

$$\eta=\lambda_s\left(1-P_{\mathrm{co},s}\right)\left(1-P_{\mathrm{so},s}\right)R_s \tag{20}$$

为了优化传输机制，最大化微基站网络的安全吞吐量，需要在安全性能和可靠性能约束条件下对 P_S 和 k 进行优化：

$$\left.\begin{aligned}&\max_{P_S,k}\qquad\eta\\&\text{s.t.}\quad P_{\mathrm{co},m}<\delta_m,\quad P_{\mathrm{co},s}<\delta_s\\&P_{\mathrm{so},s}<\varepsilon_s,P_S\ge0,\ 0\le k\le1\end{aligned}\right\} \tag{21}$$

其中，δ_m 表示允许的最大宏基站用户的 COP，δ_s 和 ε_s 分别表示允许的最大微基站用户的 COP 和 SOP。δ_m，δ_s，ε_s 分别表征宏基站网络的可靠性能水平，微基站网络的可靠性能水平和安全性能水平。

进一步，结合式(12)、式(13)、式(14)和式(19)，η 可以进一步表示为

$$\eta=\lambda_s\left(1-P_{\mathrm{co},s}\right)\left(1-P_{\mathrm{so},s}\right)R_s=\lambda_s R_s\exp\left\{-\pi\left(\lambda_s^1D_1^2+\lambda_s^2D_2^2\right)\right\}\sum_{\{m_1=0\}}^{\infty}\sum_{\{m_2=0\}}^{\infty}\left[\frac{\left(\pi\lambda_s^1D_1^2\right)^{m_1}\left(\pi\lambda_s^2D_2^2\right)^{m_2}}{m_1!m_2!}P^c_{|\{m_1,m_2\}}\right]$$

$$\cdot\exp\left\{-\frac{\lambda_e\exp\left(-c_0\pi\theta_{\mathrm{so},s}^{2/\alpha}\left(\lambda_s+\left(P_M/P_S\right)^{2/\alpha}\lambda_m\right)d^2\right)}{c_0\theta_{\mathrm{so},s}^{2/\alpha}\left(\lambda_s+\left(P_M/P_S\right)^{2/\alpha}\lambda_m\right)}-\frac{\lambda_e}{c_0\left(\theta_{\mathrm{so},s}/\left(k-(1-k)\theta_{\mathrm{so},s}\right)\right)^{2/\alpha}\left(\lambda_s+\left(P_M/P_S\right)^{2/\alpha}\lambda_m\right)}\right\}\tag{22}$$

式(22)分别对 P_S 和 k 求导发现，很难精确地数学证明 η 关于 P_S 和 k 的凹凸性。由第 5 节中 η 关于 P_S 和 k 的仿真结果可以得到如下结论：对于函数 η，固定其中一个变量(P_S 或 k)，函数关于另一个变量(k 或 P_S)是拟凸的。

本文提出一种迭代算法求解最优的 P_S 和 k (表 1)。具体地，首先根据式(8)、式(14)和式(19)得到 P_S 和 k 满足安全性和可靠性要求的上下界，初始化最大迭代次数 M。每次迭代开始，在 $P_S[m-1]$ 给定的条件下利用二分法找到最优 $k[m]$。由前述可知这是一个拟凸优化问题，因此很容易获得 $k[m]$ 的解。然后在已知 $k[m]$ 的条件下利用二分法找到 $P_S[m]$。特别地，初始问题中可靠性约束和安全性约束使得 P_S 和 k 同时有界，所以效用函数 η 也存在上界，而不会随着迭代次数的增加而一直增加。当效用函数增益小于某个预先设定的门限值 δ 或者迭代次数达到 M 时，迭代终止。

表 1 最优发射功率 P_S^{opt} 和最优功率分配因子 k^{opt} 迭代算法

(1)初始化：$M, P_S[0]=P_{S,\mathrm{LB}}, k[0]=k_{\mathrm{LB}}|_{P_S}, \delta$，利用式(22)计算 $\eta[0]$；
(2)循环；
(a)对于固定的 $P_S[m-1]$，利用二分法得到最优的 $k[m]$；
(c)更新 $\eta[m]$；
(3)如果 $|\eta[m]-\eta[m-1]|<\delta$ 或者 $m=M$ 结束循环；
(4)返回 $P_S^{\mathrm{opt}}, k^{\mathrm{opt}}, \eta^{\mathrm{opt}}$。

本文所提迭代算法复杂度分析：在每次迭代中，通过二分法获得最优发射功率 P_S^{opt}，其计算复杂度为 $\mathcal{O}\left(\log_2\left(\min\left(P_{S,\mathrm{UB}_1},P_{S,\mathrm{UB}_2}\right)/\psi_{P_S}\right)\right)$[19]，其中 ψ_{P_S} 为发射功率的预设错误容忍度。同样，通过二分法获得最优功率分配比例系数 k^{opt}，其计算复杂度为 $\mathcal{O}\left(\log_2\left(k_{\mathrm{UB}}|_{P_S}/\psi_k\right)\right)$，其中 ψ_k 为功率分配比例系数的预设错误容忍度。故总的计算复杂度为 $M\left[\mathcal{O}\left(\log_2\left(\min\left(P_{S,\mathrm{UB}_1},P_{S,\mathrm{UB}_2}\right)/\psi_{P_S}\right)\right)+\mathcal{O}\left(\log_2\left(k_{\mathrm{UB}}|_{P_S}/\psi_k\right)\right)\right]$。

5　仿真验证与结果分析

本节将给出本文所提机制的仿真结果。首先给出了 $\theta_{\mathrm{co},m}$，$\theta_{\mathrm{co},s}$ 和 $\theta_{\mathrm{so},s}$ 不同取值条件下 P_S 以及 k 对系统安全性和可靠性的影响；其次研究了 P_S 和 k 对安全吞吐量 η 的影响；最后通过与传统的多点协作机制进行对比，对本文所提机制的优势进行了证明。如无特殊说明系统的预设参数如下 $P_M=40$ dBm，$P_S=35$ dBm, $\lambda_m=5\times10^{-4}$ nodes/m^2, $\lambda_s=10\times10^{-4}$ nodes/m^2, $\lambda_e=2\times10^{-4}$ nodes/m^2, $\delta_m=0.2$, $\delta_s=0.1$, $\varepsilon_s=0.2$, $d=10$ m。蒙特卡洛仿真次数为 10^6，仿真范围为半径为 1 km 圆形区域。

首先，分析 $\theta_{\mathrm{co},m}$，$\theta_{\mathrm{co},s}$ 和 $\theta_{\mathrm{so},s}$ 不同取值条件下 P_S 和 k 对系统安全性和可靠性的影响。图 3 给出了 $P_{\mathrm{co},m}$, $P_{\mathrm{co},s}$ 和 $P_{\mathrm{so},s}$ 随 P_S 变化的曲线图。可以发现 $P_{\mathrm{co},m}$ 和 $P_{\mathrm{so},s}$ 随着 P_S 增加而增加，而 $P_{\mathrm{so},s}$ 随着 P_S 的增加而减小。这表明 P_S 不仅引起了宏基站与微基站网络可靠性的相互折中，同时也引起了微基站网络可靠性和安全性的相互折中。另外可以发现 $P_{\mathrm{co},m}$ 和 $P_{\mathrm{co},s}$ 分别随着 $\theta_{\mathrm{co},m}$ 与 $\theta_{\mathrm{co},s}$ 的增大而减大，$P_{\mathrm{so},s}$ 随着 $\theta_{\mathrm{so},s}$ 的增大而减小，这是因为当用户的SIR 小于 $\theta_{\mathrm{co},s}$ 或者窃听者的SIR 大于 $\theta_{\mathrm{so},s}$ 时中断事件发生。

图 4 给出了 $\theta_{\mathrm{co},s}$ 和 $\theta_{\mathrm{so},s}$ 不同取值条件下微基站用户 $P_{\mathrm{co},s}$ 和 $P_{\mathrm{so},s}$ 随 k 变化的曲线图。需要指出的是，$P_{\mathrm{co},s}$ 随着 k 的增大而减小，这是因为越来越多的功率协作发送信息；而 $P_{\mathrm{so},s}$ 随着 k 增加而增加，这是因为随着 k 的增大，发送人工噪声的功率越来越小。特别地，$P_{\mathrm{so},s}$ 刚开始是直线是因为 k 很小时，第 2 类微基站以全功率发送噪声，因此中断概率中较大的是窃听第 1 类微基站的窃听者造成的，而第 1 类微基站的中断概率和 k 没有关系，故刚开始的曲线是直线。

然后，本文研究了 P_S 和 k 对安全吞吐量 η 的影响。图 5 给出了 k 取不同值时 η 关于 P_S 的增减性仿真，观察图 5 可以发现 η 关于 P_S 先增大后减小。图 6 给出了 P_S 取不同值时 η 关于 k 的增减性仿真，观察图 6 可以发现 η 关于 k 先增大后减小。综合上述仿真可以发现固定一个变量(P_S 或 k)，安全吞吐量 η 关于另一个变量(k 或 P_S)是拟凸的。

最后，为证明本文所提安全传输机制的优势，图 7 将本文机制与多点协作传输机制进行了比较。由图可知，本文所提机制优于多点协作传输机制，这是因为本文机制不仅引入了人工噪声策略，还优

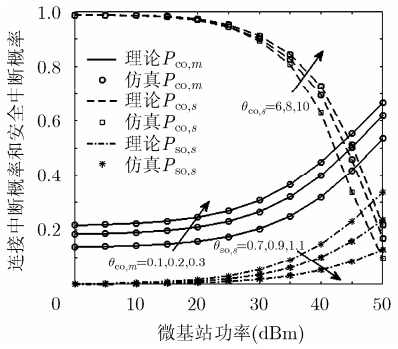

图 3 $P_{co,m}$, $P_{co,s}$ 和 $P_{so,s}$ 随微基站发射功率的变化

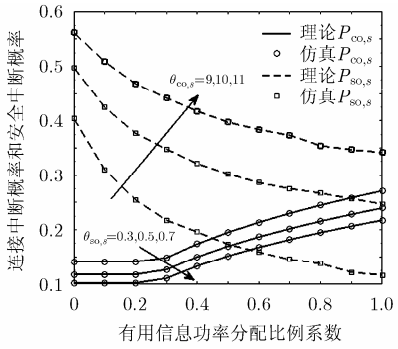

图 4 $P_{co,s}$ 和 $P_{so,s}$ 随有用信息功率分配比例系数的变化

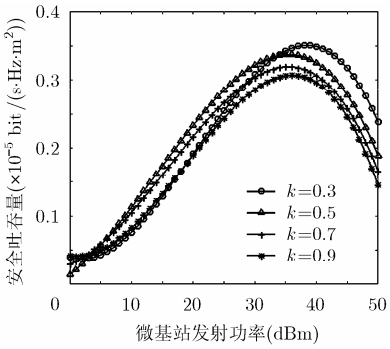

图 5 安全吞吐量随发射功率的变化

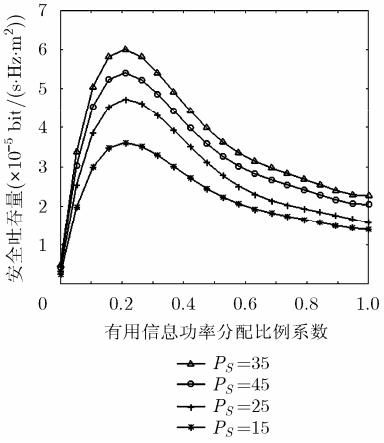

图 6 安全吞吐量随有用信息功率分配比例的变化

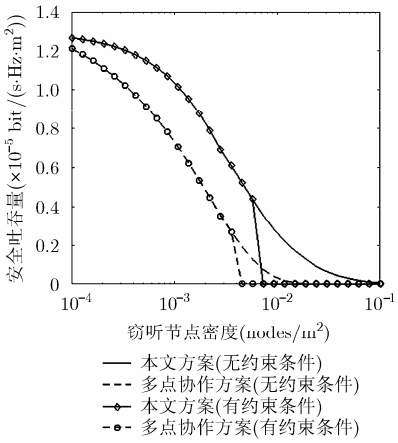

图 7 不同机制的安全吞吐量随窃听节点密度的变化

化了功率分配系数。通过与参考机制的对比，本文所提机制具有以下两种优势：首先是在存在严重安全威胁(λ_e 较大的情况)的场景下可以实现正的安全吞吐量，在存在较小安全威胁(λ_e 较小的情况)的场景下，系统安全吞吐量最大可以提升 76.1%。

6 结论

为对抗异构蜂窝网多点协作传输中距离协作微基站较近的窃听者，进一步提升系统的安全性。本文在宏基站、微基站和窃听者均随机分布的异构蜂窝网络中，提出了一种基于安全保护域的增强型多点协作传输机制，通过在安全保护域内发送 AN 干扰窃听者，提升系统的安全性。随后，本文通过分析用户的 COP, SOP 以及安全吞吐量，对系统的可靠性、安全性以及有效性进行了评估。最后，以最大化微基站网络安全吞吐量为目标，优化了微基站的发射功率以及有用信息功率分配比例系数。仿真结果表明，与传统多点协作安全传输机制相比，所提机制最大可以提升系统安全吞吐量 76.1%。

参 考 文 献

[1] WANG C X, HAIDER F, GAO X Q, *et al*. Cellular architecture and key technologies for 5G wireless communication networks[J]. *IEEE Communications Magazine*, 2014, 52(2): 122–130. doi: 10.1109/MCOM.2014.6736752.

[2] BOCCARDI F, HEATH R W, LOZANO A, *et al*. Five disruptive technology directions for 5G[J]. *IEEE Communications Magazine*, 2013, 52(2): 74–80. doi: 10.1109/MCOM.2014.6736746.

[3] YANG N, WANG L F, GERACI G, *et al*. Safeguarding 5G wireless communication networks using physical layer security[J]. *IEEE Communications Magazine*, 2015, 53(4): 20–27. doi: 10.1109/MCOM.2015.7081071.

[4] ZHONG Z H, PENG J H, LUO W Y, *et al*. A tractable approach to analyzing the physical-layer security in k-tier heterogeneous cellular networks[J]. *China Communications*, 2015, 12(s1): 166–173. doi: 10.1109/CC.2015.7386165.

[5] LÜ T J, GAO H, and YANG S S. Secrecy transmit beamforming for heterogeneous networks[J]. *IEEE Journal on Selected Areas in Communications*, 2015, 33(6): 1154–1170. doi: 10.1109/JSAC.2015.2416984.

[6] 钟智豪, 罗文宇, 彭建华. 多层异构蜂窝网协作传输和协作干扰机制的安全性能分析[J]. 中国科学: 信息科学, 2016, 46(1): 33–48. doi: 10.1360/N112015-00174.

[7] ZHONG Zhihao, LUO Wenyu, and PENG Jianhua. Secrecy performance analysis of cooperative transmission and cooperative jamming for multi-tier heterogeneous cellular networks[J]. *Science China Information Sciences*, 2016, 46(1): 33–48. doi: 10.1360/N112015-00174.

[8] WU H C, TAO X F, LI N, *et al*. Secrecy outage probability in multi-rat heterogeneous networks[J]. *IEEE Communications Letters*, 2016, 20(1): 53–56. doi: 10.1109/LCOMM.2015.2499748.

[9] WANG H M, ZHENG T X, YUAN J H, *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.

[10] QI X H, HUANG K Z, ZHONG Z H, *et al*. Physical layer security of multi-hop aided downlink MIMO heterogeneous cellular networks[J]. *China Communications*, 2016(S2): 120–130. doi: 10.1109/CC.2016.7833466.

[11] XU M, TAO X F, YANG F, *et al*. Enhancing secured coverage with CoMP transmission in heterogeneous cellular networks[J]. *IEEE Communications Letters*, 2016, 20(11): 2272–2275. doi: 10.1109/LCOMM.2016.2598536.

[12] GONG S Q, XING C W, FEI Z S, *et al*. Resource allocation for physical layer security in heterogeneous network with hidden eavesdropper[J]. *China Communications*, 2016, 13(3): 82–95. doi: 10.1109/CC.2016.7445504.

[13] XU M, TAO X F, YANG F, *et al*. On energy efficient design for dynamic CoMP transmission in k-tier heterogeneous cellular networks[J]. *China Communications*, 2016, 13(6): 147–153. doi: 10.1109/CC.2016.7513210.

[14] YUSUF M and ARSLAN H. Secure multi-user transmission using CoMP directional modulation[C]. IEEE Vehicular Technology Conference, Boston, USA, 2015: 1–2. doi: 10.1109/VTCFall.2015.7391131.

[15] CHAE S H, WAN C, LEE J H, *et al*. Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone[J]. *IEEE Transactions on Information Forensics and Security*, 2014, 9(10): 1617–1628. doi: 10.1109/TIFS.2014.2341453.

[16] HEATH R W, KOUNTOURIS M, and BAI T Y. Modeling heterogeneous network interference using Poisson point processes[J]. *IEEE Transactions on Signal Processing*, 2012, 61(16): 4114–4126. doi: 10.1109/TSP.2013.2262679.

[17] ZHOU X Y, GANTI R K, ANDREWS J G, *et al*. On the throughput cost of physical layer security in decentralized wireless networks[J]. *IEEE Transactions on Wireless Communications*, 2011, 10(8): 2764–2775. doi: 10.1109/TWC.2011.061511.102257.

[18] LIU W G, DING Z G, RATNARAJAH T, *et al*. On ergodic secrecy capacity of random wireless networks with protected zone[J]. *IEEE Transactions on Vehicular Technology*, 2016, 65(8): 1–5. doi: 10.1109/TVT.2015.2477315.

[19] XU X M, YANG W W, and CAI Y M. Secure transmission in the random CRNs with secrecy guard zone and artificial noise[J]. *Iet Communications*, 2016, 10(15): 1904–1913. doi: 10.1049/iet-com.2016.0117.

[20] XU X M, YANG W W, and CAI Y M. On the secure spectral-energy efficiency tradeoff in random cognitive radio networks[J]. *IEEE Journal on Selected Areas in Communications*, 2016, 34(10): 2706–2722. doi: 10.1109/JSAC.2016.2605901.

[21] MUKHERJEE A and SWINDLEHURST A L. Detecting passive eavesdroppers in the MIMO wiretap channel[C]. IEEE International Conference on Acoustics, Speech and Signal Processing, Kyoto, Japan, 2012: 2809–2812. doi: 10.1109/ICASSP.2012.6288501.

[22] YANG N, YAN S H, YUAN J H, *et al*. Artificial noise: transmission optimization in multi-input single-output wiretap channels[J]. *IEEE Transactions on Communications*, 2015, 63(5): 1771–1783. doi: 10.1109/TCOMM.2015.2419634.

黄开枝：　女，1973 年生，教授，博士生导师，研究方向为移动通信、物理层安全.

王　兵：　男，1992年生，硕士生，研究方向为移动通信、物理层安全.

许晓明：　男，1988年生，助理研究员，研究方向为移动通信、物理层安全.