中国科学: 信息科学 2016 年 第 46 卷 第 1 期: 33–48
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
5G 移动通信专刊 · 论文

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

钟智豪, 罗文宇*, 彭建华, 黄开枝

国家数字交换系统工程技术研究中心, 郑州 450002
* 通信作者. E-mail: lwy_xd@163.com

收稿日期: 2015–08–06; 接受日期: 2015–11–30; 网络出版日期: 2015–12–29
国家自然科学基金 (批准号: 61401510)、国家自然科学基金委员会创新群体 (批准号: 61521003) 和国家高技术研究发展计划 (863 计划) (批准号: 2015AA01A708) 资助项目

摘要 多层异构蜂窝网安全威胁的特殊性, 是由其各层的不统一性和复杂、非计划的拓扑结构所引起的. 针对异构蜂窝网中的安全传输问题, 本文结合随机几何工具和物理层安全技术, 给出了 (1) 基站间无协作、仅宏基站参与协作和所有基站都参与协作的 3 种不同场景, (2) 协作基站与用户之间有/无信道测量的两种不同机制下的异构蜂窝网安全覆盖概率和平均安全速率的表达式. 并对服务基站用于发射人工噪声干扰的功率比例、协作功率中用于发射协作干扰的功率比例、安全速率门限、宏基站发射天线数和窃听者密度等不同参数对于用户安全性能所产生的影响进行了仿真分析. 以此为基础得出了在不同场景下, 以安全性能为导向的协作传输和协作干扰策略.

关键词 异构蜂窝网 物理层安全 安全传输 协作传输 协作干扰 随机几何

1 引言

近年来, 智能终端的普及和性能提升推动了无线数据业务的飞速发展. 然而, 追求大覆盖区域和同构业务优化的单层宏网络, 越来越难以承载指数级增长的数据流量. 旨在进一步提高用户体验速率的第五代移动通信系统 (5G) [1], 将朝着多层异构蜂窝网的方向发展 [2], 通过在宏蜂窝 (macrocell) 上叠加低功率的小蜂窝 (例如 Picocell、Femtocell 等), 提升空间资源的重用率和通信覆盖 [3,4].

关于异构蜂窝网的频谱管理 [5]、功率控制 [6]、多点协作 CoMP (coordinated multiple points) [7] 技术等方面涌现了许多研究成果, 如何利用随机几何解决异构蜂窝网问题也成为了研究热点之一 [8~10]. 然而, 异构蜂窝网的安全领域却鲜有问津.

无线通信因其天然的开放性和广播性特点, 使得窃听者能够很容易地通过无线信道进行非法接收. 传统的无线蜂窝网中, 广泛采用的安全技术是在上层进行密钥加密. 而密钥加密的安全性能是以高计算复杂度为代价的. 随着计算机技术的飞速发展, 以前看似无法实现的密码破译运算过程, 或许会变得很容易实现. 此外, 由于多层异构蜂窝网中小蜂窝部署的非计划性, 给密钥的安全传递和分发提出了极

引用格式: 钟智豪, 罗文宇, 彭建华, 等. 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. 中国科学: 信息科学, 2016, 46: 33–48, doi: 10.1360/N112015-00174

大的挑战. 小基站部署在较小的区域甚至家庭式环境中, 使得窃听者更易于攻击, 甚至能够获得存储在小基站上用于保护空中接口的安全密钥 [11].

根据 Wyner 提出的安全容量定义 [12], 只有当合法用户信道状态优于窃听者的情况下, 安全容量才不为零, 即合法用户才能够进行可靠的安全通信. 由于合法用户与窃听者的无线信道不可能完全相同, 利用两者信道特征的差异设计能够提升合法用户信道状态或恶化窃听者信道状态的物理层安全通信机制, 则能够有效提升合法用户的通信安全性能. 物理层安全技术, 是近年来兴起的利用无线信道的物理特性来保障通信安全的新方式. 相关领域的研究成果丰硕. 文献 [13] 中提出了研究单层宏蜂窝网络物理层安全问题的简便方法. 文献 [14] 中进一步研究了单层宏蜂窝网络中, 多个窃听者协作窃听的情况. 文献 [15] 中, 在考虑一个发射节点、一个接收节点和一个潜在窃听者的情况下, 提出了能够减少窃听者获得的有用信号能量的迫零波束成形策略. 文献 [16] 研究了多天线系统中的物理层安全传输算法. 文献 [17] 探讨了包含两个源节点、若干个中继节点和单个窃听者的场景下, 以安全性能为目标的中继选择和干扰策略. 文献 [18,19] 分析了多节点协作情况下的物理层安全问题. 文献 [20] 在包含单个宏基站与两个毫微微基站的场景下, 对波束成形安全传输策略进行了探究.

要想从根本上解决多层异构蜂窝网的安全问题, 需要利用无线信道特性这一各层统一属性, 从无线传输过程中构建多层异构蜂窝网络的安全体系. 物理层安全技术利用无线信道的多样性、时变性以及通信双方信道特征的唯一性和互易性来实现安全传输, 对窃听者没有计算能力的限制, 也无需在非计划性部署的小蜂窝网络中进行繁琐的密钥传递和分发. 因而, 相比于传统高层密钥加密的方式, 物理层安全技术更适合于解决异构蜂窝网的安全问题. 然而, 目前针对无线通信的物理层安全研究主要集中在传统的单层宏蜂窝网络方面, 或者只考虑少数几个节点的场景. 其主要原因是多层异构蜂窝网本身的系统复杂性, 以及小蜂窝部署的非计划性, 使得物理层安全研究在建模分析等方面存在较大的困难. 近年来, 随着研究者们对于利用随机几何方法分析无线网通信问题的不断探索, 人们对于随机几何工具的特性有了更深入的认识. 文献 [21] 中介绍了在基站和用户都是随机分布的网络中, 如何利用随机几何工具分析网络覆盖和数据速率的方法. 基于随机几何方法, 文献 [22] 提供了求解多层异构蜂窝网基本问题的方程. 根据文献 [23, 24] 中的结论, 利用 Poisson 点过程 PPP (Poisson point process) 对基站位置进行建模的方法, 相比于传统的网格模型, 前者更接近实际部署的网络.

受上述文献的启发, 本文旨在将物理层安全的研究推进到多层异构蜂窝网领域. 利用随机几何工具对多层异构蜂窝网进行建模, 研究不同的协作传输和协作干扰机制对安全传输性能的影响, 探索异构蜂窝网环境下综合安全性能更高的传输机制.

文中采用的符号说明如下: $\|\cdot\|$ 表示欧几里得范数, $|\cdot|$ 表示复数的模. $\mathbb{C}$ 表示复数域. $\bar{P}\{\cdot\}$ 表示概率, $\mathrm{E}\{\cdot\}$ 表示期望. $\{\cdot\}^+$ 表示 $\max\{\cdot, 0\}$. $\mathcal{CN}\left(\mu, \sigma^2\right)$ 表示均值为 μ, 方差为 σ^2 的复 Gauss 分布.

2 系统模型

考虑一个 K 层异构蜂窝网络, 各层代表一个具体的基站等级, 例如宏蜂窝基站 MBS (macrocell base station) 或微微蜂窝基站 PBS (picocell base station). 不同层的基站具有不同的发射功率、天线数和空间分布密度. 我们假定第 i 层基站位置的空间分布服从密度为 λ_i 的 PPP Φ_i, 基站个数为 n_i. 对于属于第 i 层的所有基站, 各基站的总发射功率为 P_i, 天线数为 N_i, 安全速率门限为 γ_i. 移动用户的位置分布服从密度为 λ_u 的独立 PPP Φ_u. 同样地, 窃听者的空间位置分布根据另一个密度为 λ_e 的独立 PPP Φ_e 得到, 令 n_e 代表窃听者个数. 其他相关变量如表 1 所示.

假定所有用户选择接收信号功率最强的基站作为服务基站. 假设服务基站通过信道测量能够获

表 1 主要变量

Table 1 Major variables

Variable	Description
s_o	The message signal intended for typical user, $\mathrm{E}\{\|s_o\|\}=1$
s_{im}	The message signal intended for user U_{im}, $i\in[1,K]$, $m\in[1,n_i]$, $\mathrm{E}\{\|s_{im}\|\}=1$
B_{im}	The m^{th} BS in the collection of the BSs in the i^{th} tier
$B_{c,k}$	The cooperative BS in the collection of the BSs in the k^{th} tier, $k\in[1,K]$
$\boldsymbol{x}_{im}$	The location of BS B_{im}
$\boldsymbol{h}_{im,o}$	The channel vector from the BS B_{im} to typical user
$\boldsymbol{h}_{im,e}$	The channel vector from the BS B_{im} to the most detrimental eavesdropper
$\boldsymbol{w}_o$	The precoding vector for the typical user's serving BS
$\boldsymbol{w}_{im}$	The precoding vector for the BS B_{im}
$\boldsymbol{z}_{jt}$	Artificial noise generated by the BS B_{jt}

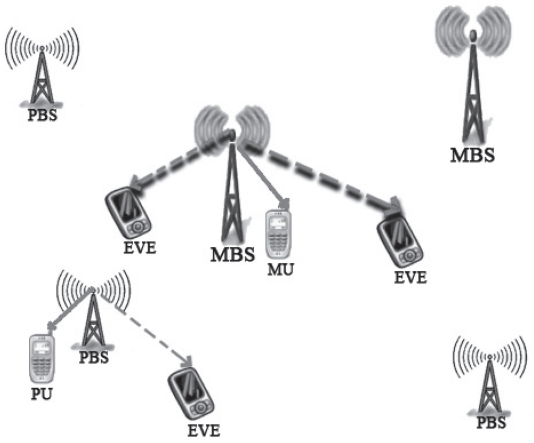

图 1 多层异构蜂窝网

Figure 1 Multi-tier heterogeneous cellular network

得用户的理想信道状态信息 CSI (channel state information), 并根据 CSI, 计算预编码向量 $\boldsymbol{w}$ 和生成人工噪声 $\boldsymbol{z}$. 人工噪声在用户信道的零空间内随机生成. 服务基站在向用户发送有用信号的同时, 以一定的功率发送人工噪声, 其中发送有用信号的功率和发送人工噪声的功率在服务基站总发射功率中所占比例分别为 P_T 和 P_I, 且满足约束 $P_T+P_I=1$. 由于人工噪声在用户信道的零空间内生成, 故对用户不产生干扰, 但能够恶化潜在窃听者的窃听信道, 降低窃听者的 SINR, 提升用户的安全性能.

图 1 中展示了一个如上述定义的两层异构蜂窝网的通信场景. 其中 MU 表示宏蜂窝用户, PU 表示微微蜂窝用户, EVE 表示窃听者, 实线箭头表示服务基站向用户发射的有用信号, 虚线箭头表示窃听者接收到的来自服务基站的信号. 紧贴虚线箭头的黑色虚线阴影表示人工噪声. 为了简便, 图 1 中仅展示了少数节点.

2.1 典型用户的 SINR

根据 Slivnyak 定理 [25], 可以考虑一个位于坐标原点的典型用户 o. 在前文所定义的网络下, 典型

用户接收到的信号为

$$\begin{aligned} y_o =&\sqrt{P_j P_T \|\boldsymbol{x}_{jt}\|^{-\alpha}}\boldsymbol{h}_{jt,o}\boldsymbol{w}_{jt}s_o + \sum_{i=1}^{K}\sum_{m=1,im\neq jt}^{n_i}\left(\sqrt{P_i P_T \|\boldsymbol{x}_{im}\|^{-\alpha}}\boldsymbol{h}_{im,o}\boldsymbol{w}_{im}s_{im}\right. \\ &\left.+\sqrt{P_i P_I \|\boldsymbol{x}_{im}\|^{-\alpha}}\boldsymbol{h}_{im,o}\boldsymbol{z}_{im}\right) + n_{to}, \end{aligned} \tag{1}$$

其中 $j \in [1,K]$, $t \in [1,n_j]$. $\alpha > 2$ 为路径损耗指数. $\boldsymbol{h}_{jt,o} \in \mathbb{C}^{1\times N_j}$ 和 $\boldsymbol{h}_{im,o} \in \mathbb{C}^{1\times N_i}$ 分别代表从基站 B_{jt} 到典型用户和从基站 B_{im} 到典型用户的信道向量, $\boldsymbol{h}_{jt,o}$ 和 $\boldsymbol{h}_{im,o}$ 独立且服从 Rayleigh 分布. $\boldsymbol{w}_{jt} \in \mathbb{C}^{N_j\times 1}$ 和 $\boldsymbol{w}_{im} \in \mathbb{C}^{N_i\times 1}$ 分别表示基站 B_{jt} 和 B_{im} 的预编码向量. $\boldsymbol{z}_{im} \in \mathbb{C}^{N_i\times 1}$ 为基站 B_{im} 发送的人工噪声. s_o 表示典型用户的服务基站发往典型用户的消息信号. 类似地, s_{im} 为基站 B_{im} 向其所服务的用户发送的消息信号. 随机变量 $n_{to} \sim \mathcal{CN}\left(0,\sigma^2\right)$ 表示典型用户处接收到的加性 Gauss 白噪声, 其中 σ^2 为恒定热噪声功率.

由此可得典型用户的 SINR 表达式为

$$\begin{aligned} \mathrm{SINR}_o\left(B_{jt}\right) &= \frac{P_j P_T \|\boldsymbol{x}_{jt}\|^{-\alpha}|\boldsymbol{h}_{jt,o}\boldsymbol{w}_{jt}|^2}{\sum_{i=1}^{K}\sum_{m=1,im\neq jt}^{n_i}\left(P_i P_T \|\boldsymbol{x}_{im}\|^{-\alpha}|\boldsymbol{h}_{im,o}\boldsymbol{w}_{im}|^2 + P_i P_I \|\boldsymbol{x}_{im}\|^{-\alpha}|\boldsymbol{h}_{im,o}\boldsymbol{z}_{im}|^2\right)+\sigma^2} \\ &= \frac{P_j P_T \|\boldsymbol{x}_{jt}\|^{-\alpha}|\boldsymbol{h}_{jt,o}\boldsymbol{w}_{jt}|^2}{I_o\left(B_{jt}\right)+\sigma^2}, \end{aligned} \tag{2}$$

其中 $I_o\left(B_{jt}\right) = \sum_{i=1}^{K}\sum_{m=1,im\neq jt}^{n_i} P_i\|\boldsymbol{x}_{im}\|^{-\alpha}\left(P_T|\boldsymbol{h}_{im,o}\boldsymbol{w}_{im}|^2 + P_I|\boldsymbol{h}_{im,o}\boldsymbol{z}_{im}|^2\right)$, $j \in [1,K]$, $t \in [1,n_j]$, 即 $B_{jt} \in \bigcup_{i=1}^{K}\Phi_i$. 为了便于表示, 令 $\Phi \triangleq \bigcup_{i=1}^{K}\Phi_i$.

2.2 窃听者的 SINR

假定网络中所有的窃听者均以典型用户为窃听目标, 则典型用户的通信安全性能主要由最危险的窃听者决定, 即所有窃听者当中, 窃听信道质量最好的窃听者. 为了方便, 除非特殊说明, 下文以 “窃听者” 代指最危险的窃听者. 类似于典型用户, 窃听者接收到的信号为

$$\begin{aligned} y_e =&\sqrt{P_j P_T \|\boldsymbol{x}_{jt}-\boldsymbol{x}_e\|^{-\alpha}}\boldsymbol{h}_{jt,e}\boldsymbol{w}_{jt}s_o + \sum_{i=1}^{K}\sum_{m=1,im\neq jt}^{n_i}\left(\sqrt{P_i P_T \|\boldsymbol{x}_{im}-\boldsymbol{x}_e\|^{-\alpha}}\boldsymbol{h}_{im,e}\boldsymbol{w}_{im}s_{im}\right. \\ &\left.+\sqrt{P_i P_I \|\boldsymbol{x}_{im}-\boldsymbol{x}_e\|^{-\alpha}}\boldsymbol{h}_{im,e}\boldsymbol{z}_{im}\right) + \sqrt{P_j P_I \|\boldsymbol{x}_{jt}-\boldsymbol{x}_e\|^{-\alpha}}\boldsymbol{h}_{jt,e}\boldsymbol{z}_{jt} + n_{te}, \end{aligned} \tag{3}$$

其中 $j \in [1,K]$, $t \in [1,n_j]$. $\boldsymbol{x}_e$ 表示窃听者的位置. $\boldsymbol{h}_{jt,e} \in \mathbb{C}^{1\times N_j}$ 和 $\boldsymbol{h}_{im,e} \in \mathbb{C}^{1\times N_i}$ 分别代表从基站 B_{jt} 到窃听者和从基站 B_{im} 到窃听者的信道向量. $\boldsymbol{z}_{jt} \in \mathbb{C}^{N_j\times 1}$ 为基站 B_{jt} 发送的人工噪声, 且满足 $\boldsymbol{h}_{jt,o}\cdot\boldsymbol{z}_{jt} = 0$. 随机变量 $n_{te} \sim \mathcal{CN}\left(0,\sigma^2\right)$ 表示窃听者处接收到的热噪声.

相应地, 窃听者的 SINR 表达式为

$$\mathrm{SINR}_e\left(B_{jt}\right) = \frac{P_j P_T \|\boldsymbol{x}_{jt}-\boldsymbol{x}_e\|^{-\alpha}|\boldsymbol{h}_{jt,e}\boldsymbol{w}_{jt}|^2}{I_e\left(B_{jt}\right)+P_j P_I\|\boldsymbol{x}_{jt}-\boldsymbol{x}_e\|^{-\alpha}|\boldsymbol{h}_{jt,e}\boldsymbol{z}_{jt}|^2+\sigma^2}, \tag{4}$$

其中 $I_e\left(B_{jt}\right) = \sum_{i=1}^{K}\sum_{m=1,im\neq jt}^{n_i} P_i\|\boldsymbol{x}_{im}-\boldsymbol{x}_e\|^{-\alpha}\left(P_T|\boldsymbol{h}_{im,e}\boldsymbol{w}_{im}|^2 + P_I|\boldsymbol{h}_{im,e}\boldsymbol{z}_{im}|^2\right)$, $B_{jt} \in \Phi$.

2.3 可达安全速率 R_{s}

可达安全速率定义为, 在保证窃听者无法获得保密信息的情况下, 用户所能得到的最大传输速率. 我们假定如下场景, 系统通过设置相应的安全速率门限 γ, 以保障合法用户的通信安全. 当且仅当合法用户获得的安全速率高于安全速率门限时, 服务基站才会向合法用户发送保密消息. 利用式 (2) 和 (4) 可得, 典型用户从基站 B_{jt} 获得的安全速率为

$$R_{\mathrm{s}}\left(B_{jt}\right)=\left\{\log_2\left(1+\mathrm{SINR}_o\left(B_{jt}\right)\right)-\max_{e\in\Phi_e}\left\{\log_2\left(1+\mathrm{SINR}_e\left(B_{jt}\right)\right)\right\}\right\}^+, \tag{5}$$

其中 $B_{jt}\in\Phi$.

相应地, 典型用户的可达安全速率为

$$R_{\mathrm{s}}=\begin{cases}\max\limits_{B_{jt}\in\Phi}R_{\mathrm{s}}\left(B_{jt}\right), & \max\limits_{B_{jt}\in\Phi}R_{\mathrm{s}}\left(B_{jt}\right)>\gamma_j,\\ 0, & \text{otherwise.}\end{cases} \tag{6}$$

3 异构蜂窝网安全传输的场景与协作机制

实际网络中, 并非所有的基站都一直处于活跃状态. 对于处于空闲状态的基站, 其全部发射功率都可以用于协助邻近的基站进行协作传输或协作干扰, 以提升邻基站的服务质量 QoS (quality of service). 类似地, 并非所有类型的数据业务都具有保密需要. 例如, 对于账号密码、网上金融交易等保密需求较高的保密型数据业务, 需要网络提供较高的通信安全保障. 而对于天气预报、推送广告等没有保密需要的公开型数据业务, 则无需耗费额外的代价去专门提升其通信安全性. 对于那些正在发送公开型数据业务的基站, 如果其所服务的用户对于数据速率的需求已经得到满足, 则该类型基站能够将一部分富余的发射功率 (例如原本规划用于在传输保密型数据业务时发送人工噪声的功率) 用于对邻近基站进行协作. 空闲基站和公开型数据业务的存在为协作安全传输提供了可能. 随着技术的进步, 资源进一步丰富, 为了提升 QoS, 未来的网络可能会部署大量的基站和热点, 使得网络中的大多数情况不再是一个基站服务多个用户, 而是多个基站服务一个用户. 这将为协作安全传输的应用提供广阔的舞台.

3.1 场景

为了对异构蜂窝网协作传输和协作干扰机制的安全性能进行较为全面的分析比较, 我们考虑 3 种不同的场景. 由于宏基站通常功率较大、性能较强, 我们假定所有场景中的宏基站均为多天线, 而小基站通常功率较低、性能受限. 我们考虑小基站、用户设备和窃听者设备均为单天线的情况.

3.1.1 场景 1: 无协作

场景 1 即传统的无协作场景. 用户在 K 层网络的所有基站中, 选择接收信号功率最强的基站作为服务基站. 系统中只有宏基站能够发射人工噪声. 宏基站根据所采用的安全传输机制, 将发射功率按照一定比例分为传输功率和干扰功率. 宏基站以传输功率对其所服务的用户发送有用信号, 同时以干扰功率在其所服务用户的信道零空间内发送人工噪声. 小基站由于仅有单天线, 无法在用户信道的零空间内发射人工噪声, 即无法发射不对合法用户产生影响的人工噪声. 故场景 1 中小基站不发射人工噪声, 小基站的全部发射功率都用于发射有用信号.

对于异构网络安全性能的分析评价, 主要基于两项指标: 安全覆盖概率 $\bar{P}_{\mathrm{sc}}$ 和平均安全速率 $\bar{R}_{\mathrm{s}}$. 安全覆盖概率定义为, 网络中一个任意位置的随机用户, 能够获得安全接入的概率, 亦即该用户从服务基站获得的安全速率高于安全门限的概率. 平均安全速率定义为, 系统中任意位置随机用户所能够获得的可达安全速率的数学期望.

定理1 对于场景 1 中随机选取的用户, 其安全覆盖概率为

$$\bar{P}_{\mathrm{sc}}=\sum_{j=1}^{K}\mathrm{E}\left\{\sum_{t=1}^{n_j}\mathbf{1}\left(R_{\mathrm{s}}\left(B_{jt}\right)>\gamma_j\right)\right\}. \tag{7}$$

证明 见附录 A.

命题1 对于场景 1 中随机选取的用户, 其平均安全速率为

$$\bar{R}_{\mathrm{s}}=\mathrm{E}\left\{\max_{B_{jt}\in\Phi}R_{\mathrm{s}}\left(B_{jt}\right)\middle|\bigcup_{B_{jt}\in\Phi}R_{\mathrm{s}}\left(B_{jt}\right)>\gamma_j\right\}. \tag{8}$$

证明 由式 (6) 结合定义可得.

3.1.2 场景 2: 仅宏基站参与协作

场景 2 的非协作部分与场景 1 相同. 场景 2 的协作部分中, 只有宏基站能够参与协作. 用户在除了服务基站以外的所有宏基站当中, 选择接收功率最强的宏基站作为协作基站. 协作基站用于协作的功率占该基站总发射功率的比例定义为 P_{co}, 令 K 层基站中的第 1 层代表宏基站, 则协作基站用于协作的发射功率为 $P_1\cdot P_{co}$.

3.1.3 场景 3: 所有基站都参与协作

场景 3 的非协作部分也与场景 1 相同. 场景 3 的协作部分中, 各层的所有基站都能够参与协作. 用户在除了服务基站以外的所有基站当中, 选择接收功率最强的基站作为协作基站, 当协作基站为 $B_{c,k}$ 时, 对应的协作功率为 $P_k\cdot P_{co}$.

3.2 协作机制

根据协作基站与典型用户之间是否进行信道测量, 可以将协作机制分为两大类, 协作基站无信道测量和协作基站有信道测量.

3.2.1 机制 1: 协作基站无信道测量

机制 1 即较为传统的机制, 协作基站与典型用户之间不进行信道测量, 即协作基站并不知道其与典型用户之间的 CSI. 因而无法根据 CSI 进行波束成形预编码, 也无法保证生成的人工噪声一定处于典型用户信道的零空间. 即此时协作基站向典型用户发送的协作传输预编码向量 $\boldsymbol{w}_{co}$ 和协作干扰人工噪声向量 $\boldsymbol{z}_{co}$ 均与典型用户的 CSI 无关.

类似于服务基站将发射功率分为有用信号传输功率和人工噪声干扰功率, 协作基站也将协作功率分为协作传输功率和协作干扰功率两个部分. 其中协作传输功率占协作功率的比例为 P_{coT}, 协作基站

$B_{c,k}$ 以功率 $P_k \cdot P_{co} \cdot P_{coT}$ 向典型用户发送有用信号. 相应地, 协作干扰功率占协作功率的比例为 P_{coI}, 满足 $P_{coT} + P_{coI} = 1$. 协作基站 $B_{c,k}$ 以功率 $P_k \cdot P_{co} \cdot P_{coI}$ 向典型用户发送人工噪声干扰.

采用机制 1 的情况下, 典型用户的 SINR 变为

$$\mathrm{SINR}_o{}'\left(B_{jt}\right) = \frac{\left|\sqrt{P_j P_T}\|\boldsymbol{x}_{jt}\|^{-\alpha/2}\boldsymbol{h}_{jt,o}\boldsymbol{w}_{jt} + \sqrt{P_k P_{co} P_{coT}}\|\boldsymbol{x}_{c,k}\|^{-\alpha/2}\boldsymbol{h}_{c,o}\boldsymbol{w}_{co}\right|^2}{I_o\left(B_{jt}\right) + P_k P_{co} P_{coI}\|\boldsymbol{x}_{c,k}\|^{-\alpha}\left|\boldsymbol{h}_{c,o}\boldsymbol{z}_{co}\right|^2 + \sigma^2}, \tag{9}$$

其中 $\boldsymbol{x}_{c,k}$ 表示协作基站的位置, $\boldsymbol{h}_{c,o} \in \mathbb{C}^{1\times N_k}$ 代表从协作基站到典型用户的信道向量, $\boldsymbol{w}_{co} \in \mathbb{C}^{N_k\times 1}$, 代表协作基站进行协作传输的预编码向量. 若处于场景 2, 则 $k = 1$. 若处于场景 3, 则 $k \in [1, K]$.

类似地, 窃听者的 SINR 变为

$$\mathrm{SINR}_e{}'\left(B_{jt}\right) = \frac{\left|\sqrt{P_j P_T}\|\boldsymbol{x}_{jt} - \boldsymbol{x}_e\|^{-\alpha/2}\boldsymbol{h}_{jt,e}\boldsymbol{w}_{jt} + \sqrt{P_k P_{co} P_{coT}}\|\boldsymbol{x}_{c,k} - \boldsymbol{x}_e\|^{-\alpha/2}\boldsymbol{h}_{\mathrm{c,e}}\boldsymbol{w}_{co}\right|^2}{I_e\left(B_{jt}\right) + P_j P_I\|\boldsymbol{x}_{jt} - \boldsymbol{x}_e\|^{-\alpha}\left|\boldsymbol{h}_{jt,e}\boldsymbol{z}_{jt}\right|^2 + P_k P_{co} P_{coI}\|\boldsymbol{x}_{c,k} - \boldsymbol{x}_e\|^{-\alpha}\left|\boldsymbol{h}_{\mathrm{c,e}}\boldsymbol{z}_{co}\right|^2 + \sigma^2}, \tag{10}$$

其中 k 的取值与典型用户相同, $\boldsymbol{h}_{\mathrm{c,e}} \in \mathbb{C}^{1\times N_k}$ 代表从协作基站到窃听者的信道向量.

推论1 在采用机制 1 的情况下, 对于场景 2 或场景 3 中随机选取的用户, 其安全覆盖概率为

$$\bar{P}_{\mathrm{sc}} = \sum_{j=1}^{K} \mathrm{E}\left\{\sum_{t=1}^{n_j} \mathbf{1}\left(R'_{\mathrm{s}}\left(B_{jt}\right) > \gamma_j\right)\right\}, \tag{11}$$

其中 $R'_{\mathrm{s}}\left(B_{jt}\right) = \left\{\log_2\left(1 + \mathrm{SINR}_o{}'\left(B_{jt}\right)\right) - \max_{e\in\Phi_e}\left\{\log_2\left(1 + \mathrm{SINR}_e{}'\left(B_{jt}\right)\right)\right\}\right\}^+$.

证明 由定理 1 结合式 (9) 和 (10) 可推得.

推论2 在采用机制 1 的情况下, 对于场景 2 或场景 3 中随机选取的用户, 其平均安全速率为

$$\bar{R}'_{\mathrm{s}} = \mathrm{E}\left\{\max_{B_{jt}\in\Phi} R'_{\mathrm{s}}\left(B_{jt}\right) \middle| \bigcup_{B_{jt}\in\Phi} R'_{\mathrm{s}}\left(B_{jt}\right) > \gamma_j\right\}. \tag{12}$$

证明 仿照推论 1, 根据命题 1 可推得.

3.2.2 机制 2: 协作基站有信道测量

机制 2 的条件相对较为苛刻, 要求协作基站与典型用户之间也要进行信道测量, 即协作基站能够知悉其与典型用户之间的理想 CSI. 因而当协作基站为宏基站 (即 $k = 1$) 时, 协作基站能够根据 CSI 进行波束成形预编码, 以及在典型用户信道的零空间内生成人工噪声. 机制二的其他基本情况与机制 1 类似.

采用机制 2 的情况下, 典型用户的 SINR 变为

$$\mathrm{SINR}_o{}''\left(B_{jt}\right) = \begin{cases} \mathrm{SINR}_o{}''\left(B_{jt}, \boldsymbol{x}_{c,1}\right), & k = 1, \\ \mathrm{SINR}_o{}'\left(B_{jt}\right), & k \neq 1, \end{cases} \tag{13}$$

其中

$$\mathrm{SINR}_o{}''\left(B_{jt}, \boldsymbol{x}_{c,1}\right) = \frac{\left|\sqrt{P_j P_T}\|\boldsymbol{x}_{jt}\|^{-\alpha/2}\boldsymbol{h}_{jt,o}\boldsymbol{w}_{jt} + \sqrt{P_k P_{co} P_{coT}}\|\boldsymbol{x}_{c,k}\|^{-\alpha/2}\boldsymbol{h}_{c,o}\boldsymbol{w}_{co}\right|^2}{I_o\left(B_{jt}\right) + \sigma^2}. \tag{14}$$

此时, 窃听者的 SINR 表达式与采用机制 1 的情况下相同. 仿照机制 1 中的步骤可得

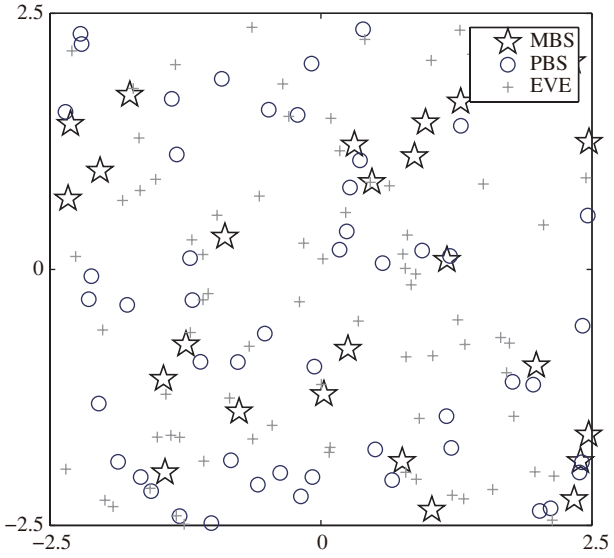

图 2　系统模型

Figure 2　System model

推论3　在采用机制 2 的情况下, 对于场景 2 或场景 3 中随机选取的用户, 其安全覆盖概率为

$$\bar{P}_{\mathrm{sc}}=\sum_{j=1}^{K}\mathrm{E}\left\{\sum_{t=1}^{n_j}\mathbf{1}\left(R''_{\mathrm{s}}\left(B_{jt}\right)>\gamma_j\right)\right\}, \tag{15}$$

其中 $R''_{\mathrm{s}}\left(B_{jt}\right)=\left\{\log_2\left(1+\mathrm{SINR}_o{}''\left(B_{jt}\right)\right)-\max_{e\in\Phi_e}\left\{\log_2\left(1+\mathrm{SINR}_e{}'\left(B_{jt}\right)\right)\right\}\right\}^{+}$.

证明　由定理 1 结合式 (10) 和 (13) 可推得.

推论4　在采用机制 2 的情况下, 对于场景 2 或场景 3 中随机选取的用户, 其平均安全速率为

$$\bar{R''}_{\mathrm{s}}=\mathrm{E}\left\{\max_{B_{jt}\in\Phi}R''_{\mathrm{s}}\left(B_{jt}\right)\middle|\bigcup_{B_{jt}\in\Phi}R''_{\mathrm{s}}\left(B_{jt}\right)>\gamma_j\right\}. \tag{16}$$

证明　由命题 1 结合推论 3 可推得.

4　仿真结果与分析

考虑一个如图 2 所示两层网络, 即 $K=2$. 第 1 层代表宏蜂窝层, 第 2 层代表小蜂窝层. 由于基站相较于用户具备更强大的性能, 部分基站间甚至可以建立有线连接, 故我们假定基站间的通信是安全的, 窃听者只窃听基站与移动用户间的通信. 基站间通信受窃听的情况留待在未来的工作中进行研究. 为了符合功率约束, 所有预编码向量 $\boldsymbol{w}$ 满足 $\|\boldsymbol{w}\|^2=1$. 类似地, 所有人工噪声 $\boldsymbol{z}$ 也满足 $\|\boldsymbol{z}\|^2=1$. 服务基站的预编码向量 $\boldsymbol{w}_{im}$ 满足 $\boldsymbol{w}_{im}=\boldsymbol{h}_{im,o}^{\mathrm{H}}$. 对于采用机制 1 的协作基站, 由于无法根据 CSI 进行波束成形, 其协作传输预编码向量中的所有元素均相等. 而对于采用机制 2 的协作基站, 其协作传输预编码向量 $\boldsymbol{w}_{co}$ 满足 $\boldsymbol{w}_{co}=\boldsymbol{h}_{c,o}^{\mathrm{H}}$, 协作基站为宏基站时, 生成的协作干扰人工噪声 $\boldsymbol{z}_{co}$ 满足 $\boldsymbol{h}_{c,o}\cdot\boldsymbol{z}_{co}=0$. 各层的安全速率门限 γ_i 均设为 γ. 路径损耗指数取 $\alpha=4$. 恒定热噪声功率设为 $\sigma^2=P_2/100$. 其他主

表 2 主要仿真参数

Table 2 Major simulation parameters

	λ_e	λ_2	P_1	P_I	γ (bit·s^{-1}·Hz^{-1})	N_1	P_{co}
Figure 3	$3\lambda_1$	$2\lambda_1$	$40P_2$	various	0.25	4	–
Figure 4	$3\lambda_1$	$2\lambda_1$	$40P_2$	various	0.25	4	–
Figure 5	$3\lambda_1$	$2\lambda_1$	$40P_2$	0.5	various	4	–
Figure 6	$3\lambda_1$	$2\lambda_1$	$40P_2$	0.5	0.25	various	–
Figure 7	$3\lambda_1$	$2\lambda_1$	$40P_2$	0.5	0.25	4	1
Figure 10	$3\lambda_1$	$2\lambda_1$	$40P_2$	0.5	0.25	4	1
Figure 8	$3\lambda_1$	$2\lambda_1$	$40P_2$	0.5	0.25	4	1
Figure 9	various	$2\lambda_1$	$40P_2$	0.5	0.25	4	1

要仿真参数如表 2 所示. 本节中各项仿真结果均通过 500000 次 (Monte Carlo) 仿真取得, 图 2 中展示了其中一次仿真中利用 PPP 得到的基站和窃听者位置分布情况.

4.1 无协作情况下的安全性能

对于不采用协作机制的场景 1, 我们主要关注服务基站自身发射的人工噪声干扰对安全覆盖概率和安全速率所产生的影响. 图 3 中展示了随着服务基站提高发射人工噪声的功率比例 (即 P_I), 平均安全速率和安全覆盖概率的变化情况, 其中, 左侧纵坐标对应平均安全速率, 右侧纵坐标对应安全覆盖概率. 从图 3 中能够明显看出, 平均安全速率和安全覆盖概率并不随着 P_I 的提高而单调增加或降低. 平均安全速率的峰值出现在 $P_I = 0.3$ 处, 即服务基站以 70% 的功率向合法用户发射有用信号, 以 30% 的功率发射人工噪声. 而安全覆盖概率的峰值出现在 $P_I = 0.6$ 处. 可见, 平均安全速率的峰值与安全覆盖概率的峰值位置并不相同. 这是由于, 在 $P_I = 0.3$ 时, 服务基站保持着较高的有用信号发射功率, 使得能够满足安全门限要求的用户都能够获得较高的数据速率. 而同时人工噪声功率也不算太低, 能够有效恶化窃听者的信道状态, 保障大部分合法用户的安全通信. 随着 P_I 继续提升, 由于用于发射有用信号的功率逐渐降低, 因而平均安全速率不可能一直增加, 而是开始随着有用信号功率的降低而逐渐降低. 在 $P_I = 0.6$ 时, 由于服务基站的大部分发射功率用于发射人工噪声, 因此窃听者的接收性能受到较大抑制. 绝大多数合法用户都能够获得安全覆盖. 但是由于发射人工噪声消耗了大部分的基站功率, 用于发送有用信号的功率较低, 即使没有窃听者存在, 合法用户获得的最高数据速率也比较有限. 因此, 虽然此时安全覆盖概率处于峰值, 平均安全速率却不及 $P_I = 0.3$ 的时候高. 当 P_I 在 0.6 以上继续提高时, 基站用于发射有用信号的功率越来越低, 即使没有窃听者存在, 部分合法用户获得的数据速率也低于安全速率门限, 因而安全覆盖概率逐渐降低.

由图 3 可以看出, P_I 范围在 $0 \sim 0.85$ 的时候, 网络中的整体平均安全速率处于宏蜂窝用户平均安全速率和小蜂窝用户平均安全速率之间, 且趋势与宏蜂窝用户平均安全速率基本一致. 这是由于宏基站功率较强, 承担了网络中的大部分负载, 因而主导了网络总体平均安全速率的走势. 宏蜂窝层的平均负载, 即满足安全门限条件的用户中, 由宏基站提供服务的用户比例, 如图 4 所示. 在 P_I 变化过程中, 小蜂窝用户的平均安全速率基本保持不变. 这是由于在场景 1 中并不存在协作, 宏基站发射的所有功率 (包括对宏基站用户发射的有用信号和人工噪声干扰), 对于小蜂窝用户而言都属于干扰. 因而小蜂窝用户受到的干扰程度并不随着 P_I 的改变而改变.

图 5 中展示了平均安全速率和安全覆盖概率随安全速率门限 γ 变化的情况. 明显地, 随着安全速

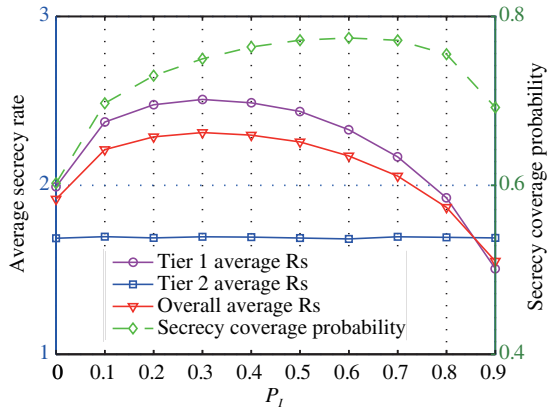

图 3 (网络版彩图) 场景 1 中平均安全速率/安全覆盖概率随人工噪声功率在发射功率中所占比例的变化曲线

Figure 3 (Color online) Average secrecy rate / secrecy coverage probability vs. the fraction of transmit power used for transmitting artificial noise under the Scenario-I

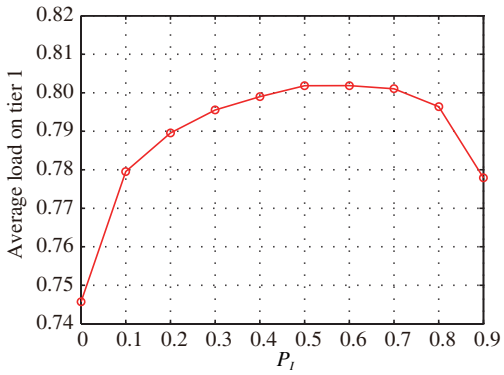

图 4 (网络版彩图) 场景 1 中宏蜂窝层的平均负载随人工噪声功率在发射功率中所占比例的变化曲线

Figure 4 (Color online) Average load on tier 1 vs. the fraction of transmit power used for transmitting artificial noise under the Scenario-I

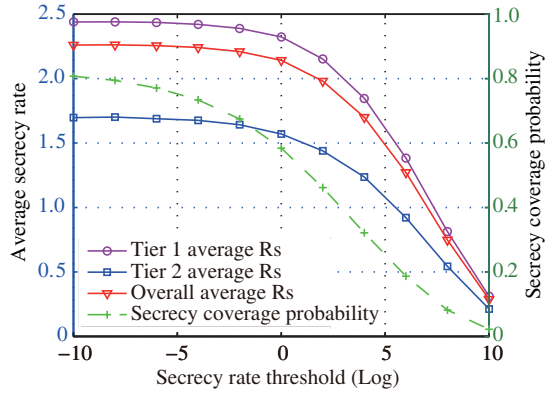

图 5 (网络版彩图) 场景 1 中平均安全速率/安全覆盖概率随安全速率门限的变化曲线

Figure 5 (Color online) Average secrecy rate / secrecy coverage probability vs. the secrecy rate threshold under the Scenario-I

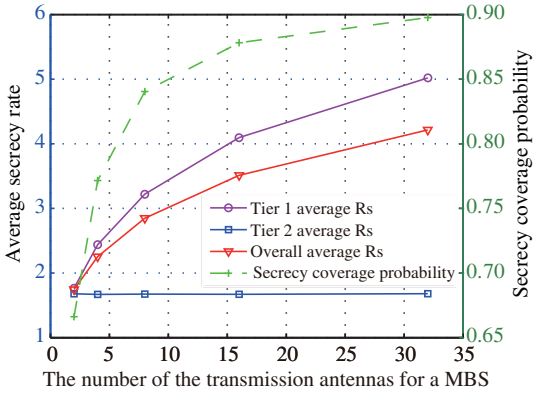

图 6 (网络版彩图) 场景 1 中平均安全速率/安全覆盖概率随宏基站发射天线数的变化曲线

Figure 6 (Color online) Average secrecy rate / secrecy coverage probability vs. the number of the transmission antennas for an MBS under the Scenario-I

率门限的提高, 平均安全速率和安全覆盖概率都单调下降. 但安全覆盖概率的下降速度明显快于平均安全速率的下降速度. 这是由于当安全速率门限提高的时候, 虽然满足安全门限要求 (能够与基站建立通信, 获得覆盖) 的用户数量减少了, 但是得到覆盖的用户都具有较高的安全速率. 因而平均安全速率的下降速度较慢.

图 6 反映了场景 1 中网络安全性能随宏基站发射天线数 N_i 的变化情况. 由图 6 中分别代表网络总体平均安全速率、宏蜂窝用户平均安全速率和小蜂窝用户平均安全速率的 3 条曲线可以看出, 宏基站发射天线数的增加只提升了宏蜂窝用户获得的安全性能, 小蜂窝用户的平均安全速率在这一过程中基本保持不变. 随着宏基站发射天线数的增加, 波束成形的指向性更好, 可供生成人工噪声的用户信道向量零空间的维度也更多, 因而宏蜂窝用户获得的安全性能也更好. 不过随着宏基站发射天线数的增

加, 通过增加天线数能够提供的安全性能增益变得越来越少, 表现为图 6 中平均安全速率和安全覆盖概率的增长趋势都逐渐趋缓.

4.2 协作情况下的安全性能

图 7 中对不同场景及不同机制下的平均安全速率进行了比较. 图 7 中横轴表示的是协作基站的协作功率中用户发射人工噪声的功率比例 P_{coI}. 对于场景 1 而言, 由于没有协作基站, 即相当于协作功率始终为 0. 对于采用机制 1 的场景, 由于协作基站发射的协作干扰人工噪声与典型用户的信道向量无关, 故这一部分协作干扰人工噪声功率, 在实际网络部署中可以用于向协作基站自身所服务的用户发送无需保密的公开型数据业务. 该数据业务的信号对于典型用户和以典型用户为目标的窃听者而言, 都相当于干扰.

从图 7 中可以明显看出, 就平均安全速率而言: 机制 2 优于机制 1, 即协作基站与典型用户之间有信道测量比没有信道测量获得的平均安全速率更高; 场景 2 优于场景 3, 即用户从协作基站获得的功率大小对安全性能的影响不及协作基站天线数目对安全性能的影响重要. 场景 2 中用户从服务基站以外的宏基站当中选择接收功率最强的基站作为协作基站, 而场景 3 中用户从服务基站以外的所有基站当中选择接收功率最强的基站作为协作基站, 这意味着场景 3 的用户获得的平均协作功率比场景 2 更高. 然而, 在场景 3 中, 当小基站作为协作基站时, 由于其仅具备单天线, 少量的协作功率提升并不足以弥补天线数减少对安全性能带来的影响 (天线数目对安全性能的影响参见图 6).

对于同样采用机制 1 的情况下, 我们注意到场景 2 中的平均安全速率基本上随着 P_{coI} 的增加而增加, 而场景 3 中平均安全速率基本上随着 P_{coI} 的增加而降低. 由于场景 3 中能够成为协作基站的基站集合包含的基站个数比场景 2 的更多, 场景 3 中协作基站到典型用户的平均距离 (由于涉及不同层基站发射功率不同, 此处我们讨论的距离为考虑接收功率相等情况下的加权距离) 比场景 2 中更近, 在窃听者密度保持不变的情况下, 这意味着场景 3 中的协作基站到窃听者的平均距离不变, 而缩短了到典型用户的平均距离. 这使得 P_{coI} 提升的时候, 协作干扰人工噪声对典型用户信道状态的恶化程度比对窃听者信道状态的恶化程度更显著. 因而导致了场景 3 中平均安全速率基本上随着 P_{coI} 的增加而降低. 其本质原理是, 当协作基站距离窃听者比距离典型用户更近的时候, 机制 1 的协作干扰对窃听者的影响更显著, 人工噪声对典型用户的安全性能产生正向增益. 反之 (即协作基站距离典型用户比距离窃听者更近的时候), 机制 1 的协作干扰对典型用户的影响更显著, 人工噪声对典型用户的安全性能产生负向增益.

对于采用机制 2 的情况下, 如图 7 所示, 场景 2 中的平均安全速率随 P_{coI} 的增加而单调下降. 这证明了在该场景中 (即窃听者密度相对而言不算特别高, 服务基站自身发射的人工噪声干扰已经为用户提供了相对较好的安全环境), 服务基站和协作基站都采用波束成形传输的情况下, 协作传输带来的安全增益大于协作干扰带来的安全增益. 这是由于此时协作基站通过波束成形使得协作传输具有指向性, 将协作功率用于协作传输能够显著提升安全性能. 而协作基站发射的协作干扰人工噪声虽然处于用户信道的零空间, 不会对典型用户产生干扰, 然而由于协作基站并不知悉窃听者的 CSI, 无法针对窃听者的信道向量生成具有指向性的人工噪声干扰, 因而此时将协作功率用于协作干扰带来的安全增益不及协作传输.

在采用机制 2 的场景 3 中, 平均安全速率不再随 P_{coI} 的增加而单调下降, 而是呈现先上升再下降的趋势. 如图 7 所示, 平均安全速率的最高峰位于 $P_{coI} = 0.4$ 处. 上升趋势的出现主要是受小蜂窝用户安全性能变化的影响. 如图 8 所示, 小蜂窝用户的平均安全速率和平均安全覆盖概率随 P_{coI} 的增加呈先上升后下降的趋势, 在 $P_{coI} = 0.5$ 附近取得峰值. 由于小基站作为服务基站时并不发射人工噪

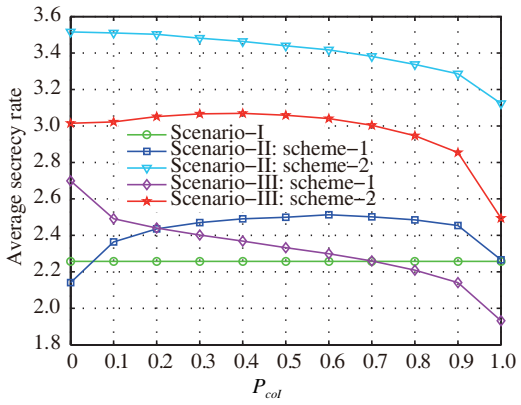

图 7 (网络版彩图) 不同场景下平均安全速率的比较

Figure 7 (Color online) Comparison of the average secrecy rates for different scenarios

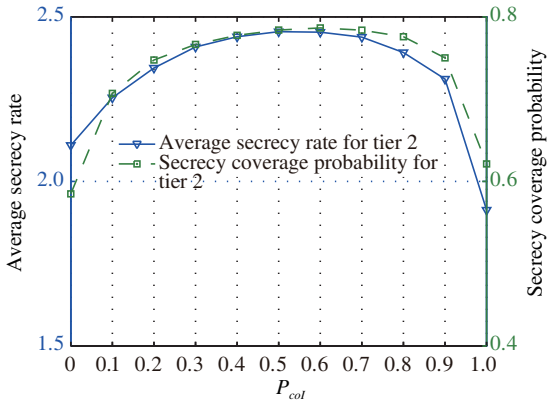

图 8 (网络版彩图) 采用机制 2 的情况下场景 3 中小蜂窝层的平均安全速率/安全覆盖概率随协作干扰功率在协作功率中所占比例的变化曲线

Figure 8 (Color online) Average secrecy rate / secrecy coverage probability for tier 2 vs. the fraction of cooperative power used for transmitting artificial noise under the Scenario-III with scheme-2

声干扰, 因而当小基站用户的协作基站在一定范围内提升发射协作干扰的功率比例 P_{coI} 时, 能够恶化窃听者的信道质量, 从而优化小基站用户的安全环境.

窃听者密度 λ_e 的改变也会改变平均安全速率随 P_{coI} 变化曲线的走势. 如图 9 所示, 在采用机制 2 的场景 2 中, 当窃听者密度升高后, 平均安全速率的峰值不再出现在 $P_{coI}=0$ 处, 而是移动到了 $P_{coI}=0.1$ 处. 类似地, 在采用机制 2 的场景 3 中, 随着窃听者密度的提升, 平均安全速率的峰值也从 $P_{coI}=0.3$ 处移动到了 $P_{coI}=0.5$ 处. 可见, 随着窃听者密度的增加, 协作基站需要提高用于发射协作干扰人工噪声的功率比例, 才能够使典型用户获得最佳的安全性能. 在图 9 中还能够明显看出, 随着窃听者密度的提升, 场景 3 中用户获得的平均安全速率明显下降了. 而场景 2 中由于协作基站均为宏基站, 采用机制 2 的情况下协作基站知悉用户的 CSI, 能够针对性地协传协扰, 因而在窃听者密度增加后, 用户平均安全速率的下降并不明显.

图 10 中对不同场景及不同机制下的安全覆盖概率进行了比较. 大多数特征与图 7 中平均安全速率的情况类似, 不再重复赘述. 主要区别在于, 在 P_{coI} 处于 $0\sim0.1$ 的范围内, 场景 3 的平均安全速率处于相对较高的位置, 而安全覆盖概率却处于相对较低的位置. 其主要原因是场景 3 中, 部分用户的协作基站为小基站. 小基站由于仅具有单根天线, 无论协作基站是否知悉典型用户的 CSI, 小基站发射的协作传输和协作干扰都与用户信道向量无关. 因而小基站协作时对用户安全性能的影响与采用机制 1 的场景 2 类似, 即如同协作基站不知道典型用户的 CSI. 如图 10 所示, 在 P_{coI} 处于 $0\sim0.1$ 的范围内场景 3 在两种机制下的安全覆盖概率走势与采用机制 1 的场景 2 中的安全覆盖概率走势基本一致. 之所以在 P_{coI} 处于 0 附近的时候, 小基站作为协作时, 平均安全速率相对较高, 而安全覆盖概率相对较低, 是因为此时协作小基站基本只发射没有指向性的有用信号, 不发射干扰, 即对于本身就达不到安全门限的用户而言, 安全性能并没有多少改善, 甚至反倒提升了部分窃听者获取有用信号的概率, 因而安全覆盖概率处于较低的水平. 不过较高的协作传输发射功率, 对于原本就能够达到安全门限的用户而言, 进一步提升了数据速率, 因而在安全覆盖概率较低的情况下依然具有相对较高的平均安全速率.

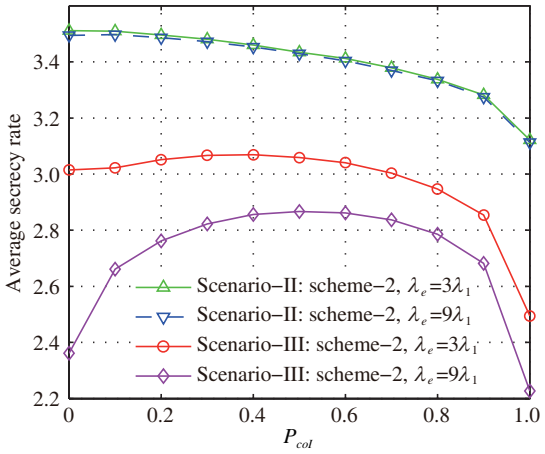

图 9　(网络版彩图) 采用机制 2 的情况下不同窃听者密度的平均安全速率比较

Figure 9　(Color online) Comparison of the average secrecy rates for different eavesdropper density with scheme-2

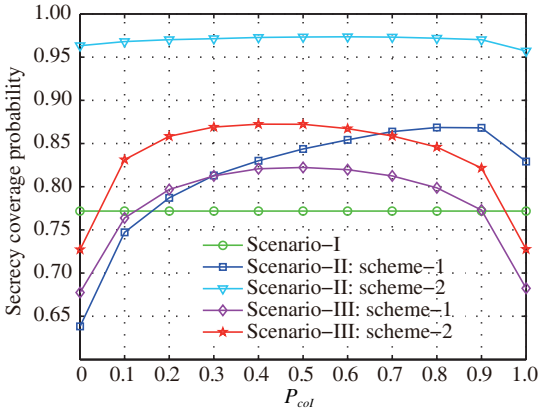

图 10　(网络版彩图) 不同场景下安全覆盖概率的比较

Figure 10　(Color online) Comparison of the secrecy coverage probabilities for different scenarios

4.3　安全性能为导向的协作功率分配策略

根据图 7 和 10 中各机制与场景 1 的比较, 可以归纳出不同场景下的协作功率分配指导策略. 如果受条件限制, 协作基站无法获悉协作基站与典型用户之间的 CSI 时, 即采取机制 1 的情况下, 在场景 2 中, 平均安全速率最高的协作功率分配策略将 60% 的协作功率用于发送协作干扰, 此时平均安全速率比无协作场景提升 10.95%. 兼顾安全覆盖概率的最优分配策略将 90% 的协作功率用于发送协作干扰, 此时平均安全速率比无协作场景提升 8.41%, 安全覆盖概率比无协作场景提升 12.47%. 在场景 3 中, 平均安全速率最高的协作功率分配策略将全部协作功率用于发送有用信号, 此时平均安全速率比无协作场景提升 19.02%. 兼顾安全覆盖概率的最优分配策略将 20% 的协作功率用于发送协作干扰, 此时平均安全速率比无协作场景提升 7.67%, 安全覆盖概率比无协作场景提升 3.18%.

如果协作基站能够获知协作基站与典型用户间的 CSI, 即采取机制 2 的情况下, 将大部分甚至全部的协作功率用于协作传输 (即发射有用信号) 能够获得更好的安全性能. 在场景 2 中, 平均安全速率最高的协作功率分配策略将全部协作功率用于发送有用信号, 此时平均安全速率比无协作场景提升 55.57%. 该分配方式也是兼顾安全覆盖概率的最优分配策略, 此时安全覆盖概率比无协作场景提升 24.83%. 在场景 3 中, 平均安全速率最高的协作功率分配策略将 40% 的协作功率用于发送协作干扰, 此时平均安全速率比无协作场景提升 35.96%, 该分配方式也是兼顾安全覆盖概率的最优分配策略, 此时安全覆盖概率比无协作场景提升 13.05%.

如果用户的安全环境较为恶劣 (例如窃听者密度较高时, 即图 9 所对应的情形) 的情况下, 应当适当提升协作干扰 (即发射人工噪声) 的功率比例, 以恶化窃听者的信道质量, 从而提升合法用户的安全性能, 保障安全覆盖概率.

5　结论

针对多层异构蜂窝网安全传输的问题, 本文利用随机几何工具进行建模, 对基站间无协作、仅宏

基站参与协作和所有基站都参与协作的 3 种不同场景开展分析. 对于有协作的两种场景, 根据协作基站与用户间无信道测量 (即协作基站并不知道用户与协作基站间的 CSI) 和协作基站与用户间有信道测量 (即协作基站知悉用户与协作基站间的 CSI) 两种不同机制, 进行分类研究, 给出了上述 3 种不同场景及两种不同机制情况下异构蜂窝网络中典型用户安全覆盖概率和平均安全速率的数学表达式. 并以此为基础, 在 3 种不同场景和两种不同机制情况下, 对服务基站用于发射人工噪声干扰的功率比例、协作功率中用于发射协作干扰的功率比例、安全速率门限、宏基站发射天线数和窃听者密度等不同参数对于用户安全性能的影响进行了仿真分析. 基于对不同场景和不同机制间的安全性能差异的分析比较情况, 给出了不同场景下能使用户获得最优安全性能的协作功率分配策略.

参考文献

1 You X H, Pan Z W, Gao X Q, et al. The 5G mobile communication: the development trends and its emerging key techniques. Sci Sin Inform, 2014, 44: 551–563 [尤肖虎, 潘志文, 高西奇, 等. 5G 移动通信发展趋势与若干关键技术. 中国科学: 信息科学, 2014, 44: 551–563]

2 Yang X B, Fapojuwo A O. Coverage probability analysis of heterogeneous cellular networks in rician/rayleigh fading environments. IEEE Commun Lett, 2015, 19: 1197–1200

3 Zhang X N, Tan Z H, Xu S Y, et al. Utility maximization based on cross-layer design for multi-service in macro-femto heterogeneous networks. IEEE Trans Wirel Commun, 2013, 12: 5607–5620

4 Samdanis K, Taleb T, Schmid S. Traffic offload enhancements for eUTRAN. IEEE Commun Surv Tut, 2012, 14: 884–896

5 Cao D, Zhou S, Niu Z. Improving the energy efficiency of two-tier heterogeneous cellular networks through partial spectrum reuse. IEEE Trans Wirel Commun, 2013, 12: 4129–4141

6 Liu J F, Zheng W, Li W, et al. Distributed uplink power control for two-tier femtocell networks via convex pricing. In: Proceedings of IEEE Wireless Communications and Networking Conference, Shanghai, 2013. 458–463

7 Xia P, Liu C H, Andrews J G. Downlink coordinated multi-point with overhead modeling in heterogeneous cellular networks. IEEE Trans Wirel Commun, 2013, 12: 4025–4038

8 Panahi F H, Ohtsuki T. Analytical modeling of cognitive heterogeneous cellular networks over Nakagami-m fading. EURASIP J Wirel Commun Netw, 2015, 1: 3628–3634

9 Deng N, Zhou W Y, Haenggi M. Heterogeneous cellular network models with dependence. IEEE J Sel Area Commun, 2015, 33: 2167–2181

10 Mirahsan M, Schoenen R, Yanikomeroglu H. HetHetNets: heterogeneous traffic distribution in heteogeneous wireless cellular networks. IEEE J Sel Area Commun, 2015, 33: 2252–2265

11 Cao J, Ma M, Li H, et al. A survey on security aspects for LTE and LTE-A networks. IEEE Commun Surv Tut, 2014, 16: 283–302

12 Wyner A D. The wire-tap channel. Bell Syst Tech J, 1975, 54: 1355–1367

13 Wang H, Zhou X Y, Reed M C. Physical layer security in cellular networks: a stochastic geometry approach. IEEE Trans Commun, 2013, 12: 2776–2787

14 Geraci G, Dhillon H S, Andrews J G, et al. Physical layer security in downlink multi-antenna cellular networks. IEEE Trans Commun, 2013, 62: 2006–2021

15 Zhu F C, Gao F F, Yao M L. Zero-forcing beamforming for physical layer security of energy harvesting wireless communications. EURASIP J Wirel Commun Netw, 2015

16 Ji J, Liu L, Jin L, et al. The physical layer security algorithm of MIMO system based on random reference. Sci Sin Inform, 2014, 44: 254–262 [吉江, 刘璐, 金梁, 等. 随机发送参考的多天线系统物理层安全传输算法. 中国科学: 信息科学, 2014, 44: 254–262]

17 Ibrahim D H, Hassan E S, El-Dolil S A. Relay and jammer selection schemes for improving physical layer security in two-way cooperative networks. Comput Secur, 2015, 50: 47–59

18 Luo M, Wang H M, Yin Q Y. Hybrid relaying and jamming for wireless physical layer security based on cooperative beamforming. Sci Sin Inform, 2013, 43: 445–458 [罗苗, 王慧明, 殷勤业. 基于协作波束形成的中继阻塞混合无线物

理层安全传输. 中国科学: 信息科学, 2013, 43: 445–458]
19 Deng H, Wang H M, Wang W J. Grouping cooperative jamming for wireless physical layer security. Sci Sin Inform, 2014, 44: 1482–1494 [邓浩, 王慧明, 王文杰. 基于多节点分组协作干扰的无线物理层安全传输. 中国科学: 信息科学, 2014, 44: 1482–1494]
20 Lv T J, Gao H, Yang S S. Secrecy transmit beamforming for heterogeneous networks. IEEE J Sel Area Commun, 2015, 33: 1154–1170
21 Andrews J G, Baccelli F, Ganti R K. A tractable approach to coverage and rate in cellular networks. IEEE Trans Commun, 2011, 59: 3122–3134
22 Dhillon H S, Ganti R K, Baccelli F, et al. Modeling and analysis of K-tier downlink heterogeneous cellular networks. IEEE J Sel Area Commun, 2012, 30: 550–560
23 Novlan T D, Ganti R K, Ghosh A, et al. Analytical evaluation of fractional frequency reuse for OFDMA cellular networks. IEEE Trans Wirel Commun, 2011, 10: 4294–4305
24 Novlan T D, Dhillon H S, Andrews J G. Analytical modeling of uplink cellular networks. IEEE Trans Wirel Commun, 2012, 12: 2669–2679
25 Chiu S N, Stoyan D, Kendall W S, et al. Stochastic Geometry and Its Applications. 3rd ed. New York: John Wiley & Sons Ltd, 2013. 48–51

附录 A 定理 1 证明

设 Ω 是概率为 $\bar{P}\{\Omega\}$ 的随机总体. 定义 $\mathbf{1}(\omega)$ 为 Ω 的指征函数, 即

$$\mathbf{1}(\omega)=\begin{cases}1, & \omega\in\Omega,\\ 0, & \omega\notin\Omega.\end{cases}\tag{A1}$$

则 $\bar{P}\{\mathbf{1}(\omega)=1\}=\bar{P}\{\Omega\}$, $\mathbf{1}(\Omega)$ 是随机变量的函数. 其数学期望为 $\mathrm{E}\{\mathbf{1}(\Omega)\}$. 有

$$\mathrm{E}\{\mathbf{1}(\Omega)\}=1\cdot\bar{P}\{\mathbf{1}(\omega)=1\}+0\cdot\bar{P}\{\mathbf{1}(\omega)=0\}=1\cdot\bar{P}\{\Omega\}+0\cdot\left(1-\bar{P}\{\Omega\}\right)=\bar{P}\{\Omega\}.\tag{A2}$$

于是有

$$\bar{P}_{\mathrm{sc}}=\bar{P}\left\{\bigcup_{B_{jt}\in\Phi}R_{\mathrm{s}}(B_{jt})>\gamma_j\right\}=\mathrm{E}\left\{\mathbf{1}\left(\bigcup_{B_{jt}\in\Phi}R_{\mathrm{s}}(B_{jt})>\gamma_j\right)\right\}.\tag{A3}$$

由于基站部署共有 K 层, 且各层的部署过程可以看作是相互独立, 即各层的指征函数

$$\mathbf{1}\left(\bigcup_{B_{jt}\in\Phi}R_{\mathrm{s}}(B_{jt})>\gamma_j\right),\tag{A4}$$

在 K 层的取值相互独立. 由于随机变量相互独立时, 和的期望等于期望的和, 结合式 (A4) 可得

$$\mathrm{E}\left\{\mathbf{1}\left(\bigcup_{B_{jt}\in\Phi}R_{\mathrm{s}}(B_{jt})>\gamma_j\right)\right\}=\mathrm{E}\left\{\sum_{j=1}^{K}\mathbf{1}\left(\bigcup_{B_{jt}\in\Phi_j}R_{\mathrm{s}}(B_{jt})>\gamma_j\right)\right\}=\sum_{j=1}^{K}\mathrm{E}\left\{\sum_{t=1}^{n_j}\mathbf{1}\left(R_{\mathrm{s}}(B_{jt})>\gamma_j\right)\right\}.\tag{A5}$$

Secrecy performance analysis of cooperative transmission and cooperative jamming for multi-tier heterogeneous cellular networks

Zhihao ZHONG, Wenyu LUO*, Jianhua PENG & Kaizhi HUANG

National Digital Switching System Engineering & Technological Research Center, Zhengzhou 450002*, China*
*E-mail: lwy_xd@163.com

Abstract The particularity of security threats for multi-tier heterogeneous cellular networks (HCNs) is caused by the nonuniformity between the tiers and the complex and unplanned topology. To promote the study of secrecy

transmission in HCNs, we utilize stochastic geometry tools and physical-layer security technologies to obtain the expressions for the secrecy coverage probability and average secrecy rate under different scenarios such as no cooperation, only macrocell base stations (MBSs) involved in cooperation, all base stations (BSs) involved in cooperation, and with/without channel measurements between the cooperative BSs and the mobile users. Furthermore, we simulate and analyze the influences on security performance caused by the fraction of transmit power used for transmitting artificial noise, the fraction of cooperative power used for transmitting artificial noise, the secrecy rate threshold, the number of transmission antennas for an MBS, and the eavesdropper density. Based on the simulation results, we propose a security-performance-oriented strategy for cooperative transmission and jamming in HCN.

Keywords heterogeneous cellular networks, physical layer security, secrecy transmission, cooperative transmission, cooperative jamming, stochastic geometry

Zhihao ZHONG was born in 1992. He received his B.E. in communication engineering from Nanjing University, Nanjing, China, in 2014. Currently he is an M.S. candidate at the National Digital Switching System Engineering & Technological Research Center. His research interests include physical layer security, heterogeneous cellular networks, and wireless mobile communication.

Wenyu LUO was born in 1982. He received his Ph.D. in communication engineering from the National Digital Switching System Engineering & Technological Research Center, Henan, China, in 2012. Currently he is a lecturer at the National Digital Switching System Engineering & Technological Research Center. His research interests include wireless physical layer security, heterogeneous cellular networks, cognitive radio, and signal processing.

Jianhua PENG was born in 1966. He received his M.S. in computer application in 1995. Currently he is a professor and doctoral supervisor as well as a deputy chief engineer at the National Digital Switching System Engineering & Technological Research Center, Henan, China. His major research interests include network switching, wireless mobile communication networks, and information secrecy.

Kaizhi HUANG was born in 1978. She received her Ph.D. in communication and information systems from Tsinghua University, Beijing, China. Currently she is a professor and supervisor of postgraduate students at the National Digital Switching System Engineering & Technological Research Center in Henan, China. Her major research interests include wireless mobile communication networks and information secrecy.