非理想情况下 K 层密集异构蜂窝网的安全性能分析

黄开枝 许耘嘉* 丁大钊 戚晓慧 陈亚军
(国家数字交换系统工程技术研究中心 郑州 450002)

摘 要：密集异构蜂窝网络节点布置的随机性、动态性、复杂性等特点，导致实际场景中该系统的安全性能受非理想信道估计的影响更严重，然而目前对该系统安全性能的研究主要集中于理想场景，缺乏在非理想场景中的研究。针对这一问题，该文从密集异构蜂窝网自身结构及实际部署的特点出发，分析了信道估计存在误差时系统的安全性能。首先基于随机几何对系统建模，推导了非理想情况下 K 层密集异构蜂窝网的安全中断概率；然后分析了部分参数对系统安全性能的影响；最后，通过仿真验证了理论推导的有效性。

关键词：密集异构蜂窝；物理层安全；信道估计误差；安全中断概率
中图分类号：TN92 **文献标识码**：A **文章编号**：1009-5896(2017)10-2456-08
DOI: 10.11999/JEIT161376

Secrecy Performance Analysis of K-tier Dense Heterogeneous Cellular Networks with Imperfect Channel State Information

HUANG Kaizhi XU Yunjia DING Dazhao QI Xiaohui CHEN Yajun
(*National Digital Switching System Engineering & Technological Research Center*, *Zhengzhou* 450002, *China*)

Abstact: Due to the characteristics of random, dynamic, and complex arrangement of dense heterogeneous cellular network nodes, the secrecy performance of the system is more seriously affected by the non-ideal channel estimation in the actual communication scenario. However, the research on the secrecy performance analysis of the dense heterogeneous cellular network mainly focuses on the ideal scene, but never involves non-ideal scene. To solve this problem, this paper considers the characteristics and actual deployment of the system, and analyzes the secrecy performance of the system when there exist channel estimation errors. First, based on stochastic geometry, the security outage probability of K-tier dense heterogeneous cellular networks is deduced. Then the influence of partial parameters on system security performance is analyzed. Finally, the validity of theoretical derivation is verified by simulation.

Key words: Dense heterogeneous cellular networks; Physical layer security; Channel estimation errors; Security outage probability

1 引言

移动互联网的快速发展驱使移动蜂窝网的结构向密集异构组网方式发展，其随机部署和“泛在接入”的特点在提升通信系统性能的同时也使得信息更容易遭受到窃听。受系统结构的影响，传统高层加密算法计算复杂度大大增加；且不同类型基站的计算能力不同，小型基站处理能力有限，也使得传统加密算法应用于密集异构蜂窝网时面临挑战。作为传统安全手段的重要补充，物理层安全利用无线信道的“唯一性”、“互易性”等“指纹特性”来保障系统的通信安全，使安全通信无需受制于系统的计算能力，更适合解决密集异构蜂窝网中的窃听问题[1−3]。

目前，业界在异构蜂窝网的物理层安全建模分析、传输方案设计等方面取得了一定进展。文献[4]将物理层安全技术引入密集异构蜂窝网，定义了衡量全局网络保密性能的安全指标。文献[5]在多制式接入通信网络模型中分析了系统的物理层安全性能。在此基础上，文献[6−8]利用随机几何工具分别针对异构蜂窝网[6]、传感网[7]、认知蜂窝网[8]等网络结构设计了保障系统安全通信的传输方案。但上述文献中所设计的传输方案都是基于发送端已知完整且准确的信道状态信息 CSI(Chanel State Information)。由于密集异构网络中基站分布随机且覆盖范围相互重叠，用户接收到的导频信号极易受到干扰，影响 CSI 的估计精度；此外，小型基站占

收稿日期：2016-12-16；改回日期：2017-04-07；网络出版：2017-05-26
*通信作者：许耘嘉 136564061@qq.com
基金项目：国家 863 计划项目(2015AA01A708)，国家自然科学基金(61379006, 61401510, 61521003)
Foundation Items: The National 863 Program of China (2015AA01A708), The National Natural Science Foundation of China (61379006, 61401510, 61521003)

有的资源以及计算处理能力均无法与宏基站相提并论[9]，导致基站难以实时处理用户回传的 CSI。因此密集异构蜂窝网容易出现 CSI 获取不准确等问题，进而对传输算法设计和系统安全性能产生影响。

相对密集异构蜂窝网，在传统蜂窝网中安全性能分析及波束成形[10,11]、人工噪声[12]等传输方案被广泛研究。由于密集异构蜂窝网节点随机部署的特点使节点之间的距离不再固定，且单个节点极易收到来自相邻小区基站的干扰，使得上述传统蜂窝网中的建模和分析方法不再适用，因此需要从密集异构蜂窝网的特点入手来开展研究。目前信道估计不理想在密集异构蜂窝网中的研究较少，由于系统本身十分复杂，各层各条链路都可能出现信道估计不准确的情况，因此密集异构蜂窝网在非理想情况下的建模分析存在较大的困难。而安全性能分析作为后续工作的基础，是研究非理想情况下密集异构蜂窝网的安全传输算法设计的重要前提，因此研究信道估计不理想时密集异构蜂窝网的物理层安全，首先需要对其安全性能进行分析。

针对以上需求，本文从密集异构蜂窝网自身结构及实际部署的特点出发，分析了非理想信道估计条件下系统的安全性能。利用随机几何工具推导了信道估计存在误差时 K 层密集异构蜂窝网的安全中断概率与信道估计精度的关系式。然后分析了信道估计精度、微基站分布密度、窃听者密度、中断门限以及基站天线数量等系统参数对系统安全性能的影响。最后通过仿真验证了理论推导的有效性，以及在不同估计精度条件下各参数对安全中断概率的影响，发现当信道由完全精确估计下降到完全不准确估计时系统的安全性能下降达到 60%～80%。

2　系统描述

在 K 层密集异构蜂窝网络中，不同层基站分别设置不同的发射功率、路径损耗系数、天线数和空间分布密度等参数。假设第 i 层基站服从密度为 λ_i 的 2 维泊松点过程(Possion Pointed Process, PPP)，用 Φ_i 表示。对于第 i 层所有基站的发射功率均为 P_i 且配备 N_i 根天线。系统中用户和窃听者分别服从参数为 λ_u 和 λ_e 的 PPP 分布，用 Φ_u 和 Φ_e 表示，二者接收天线数量均为 1。

开放网络中用户可以选择任意一层基站接入。假设用户选择提供最大接收功率 P_r 的基站接入，则用户接入第 i 层第 m 个基站 B_{im} 的概率 $\mathcal{A}_i$，及用户到基站 B_{im} 的距离 X 的概率密度函数可分别表示为[13]

$$\mathcal{A}_i = 2\pi\lambda_i\int_0^{\infty} x\exp\left\{-\pi\sum_{j=1}^{K}\lambda_j\left(\frac{P_j}{P_i}\right)^{2/a_j}x^{2a_i/a_j}\right\}\mathrm{d}x \tag{1}$$

$$f_{X_i}(x)=\frac{2\pi\lambda_i}{\mathcal{A}_i}x\exp\left\{-\pi\sum_{j=1}^{K}\lambda_j\left(\frac{P_j}{P_i}\right)^{2/a_j}x^{2a_i/a_j}\right\} \tag{2}$$

在信道估计阶段，基站在每个时隙发射导频信号，用户接收导频信号对当前信道进行估计，并将估计值通过理想的回程链路反馈给基站，随后基站以此为依据设计传输阶段的预编码矩阵。由于各层基站随机分布且覆盖范围相互重叠，因此用户可以接收到来自多个相邻基站发出的导频信号。复杂的干扰导致信道估计受到影响，这使得非理想信道估计在密集异构蜂窝网中极易发生。用 $\tilde{\boldsymbol{h}}_{\mathrm{ui}}$ 表示合法信道 $\boldsymbol{h}_{\mathrm{ui}}$ 的估计值，二者关系可表示为[14]

$$\boldsymbol{h}_{\mathrm{ui}} = \sqrt{\rho_i}\tilde{\boldsymbol{h}}_{\mathrm{ui}} + \sqrt{1-\rho_i}\boldsymbol{n}_i \tag{3}$$

其中，$\boldsymbol{n}_i$ 表示估计误差，并假设每路误差 $\boldsymbol{n}_i \sim \mathcal{CN}(0, \boldsymbol{I}_{N_i})$，$\rho_i\,(0 \le \rho_i \le 1)$ 是信道估计精度的度量，ρ_i 越大信道估计越准确，当 ρ_i=1 时信道估计完全准确。

3　非理想情况下的安全性能分析

不同于传统蜂窝结构，密集异构蜂窝网节点随机分布的特点导致难以直接得出信道估计精度与接收信干噪比(Signal to Interference plus Noise Ratio, SINR)的关系，因此本节首先利用随机几何工具，在密集异构蜂窝网中建立信道估计误差条件下的安全模型，推导了信道估计精度与安全中断概率的关系式；然后，在此基础上分析了部分参数对系统安全性能的影响。

3.1 安全模型建立

仅考虑目标小区信道估计非理想，根据 Slivnyak 定理，以一个典型用户为例，建立非理想情况下的安全模型。在信号传输阶段，基站 B_{im} 根据接收到的 CSI 估计值进行预编码，预编码矩阵为 $\widetilde{\boldsymbol{w}}_i = \tilde{\boldsymbol{h}}_{\mathrm{ui}}^{\mathrm{H}}\big/\big\|\tilde{\boldsymbol{h}}_{\mathrm{ui}}\big\|$。同时考虑大尺度衰落和小尺度衰落，其中大尺度路径衰落系数为 $\alpha_i > 2$，小尺度衰落服从准静态瑞利衰落。则合法用户的接收 SINR 可表示为

$$\mathrm{SINR}_{\mathrm{U}}^{i} = \frac{P_i\rho_i\left\|\tilde{\boldsymbol{h}}_{\mathrm{ui}}\right\|^2|X_i|^{-\alpha_i}}{P_i(1-\rho_i)\left\|\boldsymbol{n}_i\widetilde{\boldsymbol{w}}_i\right\|^2|X_i|^{-\alpha_i}+I_{\mathrm{ui}}+{\sigma_u}^2} \tag{4}$$

其中，$i \in [1,K]$，$\left\|\tilde{\boldsymbol{h}}_{\mathrm{ui}}\right\|^2 \sim \mathrm{gamma}(N_i,1)$，$\alpha_i$ 为第 i 层的路径损耗指数。$P_i(1-\rho_i)\left\|\boldsymbol{n}_i\widetilde{\boldsymbol{w}}_i\right\|^2|X_i|^{-\alpha_i}$ 表示信道估计误差导致的接收干扰，$\left\|\boldsymbol{n}_i\widetilde{\boldsymbol{w}}_i\right\|^2 \sim \exp(1)$。$I_{\mathrm{ui}} = \sum_{j=1}^{K}\sum_{B_{\mathrm{jt}}\in\Phi_j\setminus B_{\mathrm{im}}}P_j\left\|\boldsymbol{h}_{\mathrm{uj}}\right\|^2|Z_j|^{-\alpha_j}$ 表示用户接收

到的来自除服务基站 B_{im} 外的同层及层间基站干扰之和，$\boldsymbol{h}_{\mathrm{uj}}$ 表示干扰基站与用户之间的信道向量，$\left\|\boldsymbol{h}_{\mathrm{uj}}\right\|^2 \sim \exp(1)$，$Z_j$ 表示干扰基站到用户的距离，σ_u^2 表示用户收到加性高斯白噪声的噪声功率。

假设窃听者被动窃听且可以准确估计窃听信道，由于非联合窃听，因此考虑系统最差情况即 SINR 最大的窃听链路的性能，其等价 SINR 可表示为

$$\mathrm{SINR}_{\mathrm{E}}^{i}=\max_{e\in\Phi_e}\left\{\frac{P_i\left\|\boldsymbol{h}_{\mathrm{ei}}\widetilde{\boldsymbol{w}}_i\right\|^2\left|Y_i\right|^{-\alpha_i}}{I_{\mathrm{ei}}+{\sigma_e}^2}\right\} \tag{5}$$

其中，$i\in[1,K]$，$\left\|\boldsymbol{h}_{\mathrm{ei}}\widetilde{\boldsymbol{w}}_i\right\|^2\sim\exp(1)$，$Y_i$ 表示窃听者到服务基站的距离。$I_{\mathrm{ei}}=\sum_{j=1}^{K}\sum_{B_{\mathrm{jt}}\in\Phi_j\setminus B_{\mathrm{im}}}P_j\cdot\left\|\boldsymbol{h}_{\mathrm{ej}}\right\|^2\left|M_j\right|^{-\alpha_j}$ 表示窃听者收到的层间干扰和同层干扰，$\boldsymbol{h}_{\mathrm{ej}}$ 表示干扰基站与窃听者之间的信道向量，$\left\|\boldsymbol{h}_{\mathrm{ej}}\right\|^2\sim\exp(1)$，$M_j$ 表示干扰基站到窃听者的距离，σ_e^z 表示窃听者收到加性高斯白噪声的噪声功率。

3.2 安全中断概率

安全中断概率(Security Outage Probability, SOP)是指当用户的平均可达速率小于预设安全中断门限时，通信将不再安全而出现中断。第 i 层的 SOP 可表示为[15]

$$P_{\mathrm{out}}^{i}(R_i)=\mathbb{P}(R_{\mathrm{S}}^{i}<R_i) \tag{6}$$

将式(6)变形为[16]

$$P_{\mathrm{out}}^{i}(R_i)=\begin{cases}1-\mathbb{F}_{\mathrm{SINR}_{\mathrm{E}}^{i}}(2^{(R_{\mathrm{U}}^{i}-R_i)}-1), & 0<\rho_i<1\\ 1, & \rho_i=0\end{cases} \tag{7}$$

其中，$\mathbb{F}_{\mathrm{SINR}_{\mathrm{E}}^{i}}(\cdot)$ 表示窃听第 i 层用户的窃听者的接收信干噪比 $\mathrm{SINR}_{\mathrm{E}}^{i}$ 的分布函数，由 Jensen 不等式有[16]

$$\mathbb{E}\left\{\log_2\left(1+\mathrm{SINR}_{\mathrm{U}}^{i}\right)\right\}\geq\log_2\left(1+\left[\mathbb{E}\left(\mathrm{SINR}_{\mathrm{U}}^{i\,-1}\right)\right]^{-1}\right) \tag{8}$$

记 $R_{\mathrm{U}}^{L_i}=\log_2\left(1+\left[\mathbb{E}\left(\mathrm{SINR}_{\mathrm{U}}^{i\,-1}\right)\right]^{-1}\right)$ 为用户平均可达速率的下界，有

定理 1 信道估计非理想时，合法用户的平均可达速率下界 $R_U^{L_i}$ 为

$$R_{\mathrm{U}}^{L_i}=\begin{cases}\log_2\left(1+\left[\dfrac{\left(1-\rho_i\right)P_i+\displaystyle\int_0^{\infty}\left(\sum_{j=1}^{K}2\pi\lambda_jP_j\left(M_j\right)^{2-\alpha_j}\Big/\left(\alpha_j-2\right)+\sigma^2\right)x^{\alpha_i}f_{X_i}(x)\mathrm{d}x}{N_i\rho_iP_i}\right]^{-1}\right), & 0<\rho_i\leq1\\ 0, & \rho_i=0\end{cases} \tag{9}$$

证明 由 $R_{\mathrm{U}}^{L_i}$ 定义可知需首先计算 $\mathbb{E}\left(\mathrm{SINR}_{\mathrm{U}}^{i\,-1}\right)$，有：

$$\begin{aligned}\mathbb{E}\left(\mathrm{SINR}_{\mathrm{U}}^{i\,-1}\right)=&\left[\mathbb{E}\left(P_i\left(1-\rho_i\right)\left\|\boldsymbol{n}_i\widetilde{\boldsymbol{w}}_i\right\|^2\right)\right.\\&\left.+\int_0^{\infty}\left(\mathbb{E}\left(I_{\mathrm{ui}}\right)+{\sigma_u}^2\right)x^{\alpha_i}f_{X_i}(x)\mathrm{d}x\right]\\&\Big/\mathbb{E}\left(P_i\rho_i\left\|\widetilde{\boldsymbol{h}}_{\mathrm{ui}}\right\|^2\right)\end{aligned} \tag{10}$$

其中，

$$\mathbb{E}\left(\rho_iP_i\left\|\widetilde{\boldsymbol{h}}_{\mathrm{ui}}\right\|^2\right)=\frac{\rho_iP_i}{(N_i-1)!}\int_0^{\infty}\left\{\varsigma^{N_i}\mathrm{e}^{-\varsigma}\right\}\mathrm{d}\varsigma=N_i\rho_iP_i \tag{11}$$

$$\begin{aligned}\mathbb{E}\left[P_i\left(1-\rho_i\right)\left\|\boldsymbol{n}_i\widetilde{\boldsymbol{w}}_i\right\|^2\right]&=\left(1-\rho_i\right)P_i\int_0^{\infty}\left\{\iota\mathrm{e}^{-\iota}\right\}\mathrm{d}\iota\\&=\left(1-\rho_i\right)P_i\end{aligned} \tag{12}$$

$$\begin{aligned}\mathbb{E}\left(I_{\mathrm{ui}}\right)&=\mathbb{E}_{\Phi_j,\boldsymbol{h}_{\mathrm{uj}}}\left[\sum_{j=1}^{K}\sum_{B_{\mathrm{jt}}\in\Phi_j\setminus B_{\mathrm{im}}}P_j\left\|\boldsymbol{h}_{\mathrm{uj}}\right\|^2\left|Z_j\right|^{-\alpha_j}\right]\\&=\sum_{j=1}^{K}\sum_{B_{\mathrm{jt}}\in\Phi_j\setminus B_{\mathrm{im}}}\int_0^{\infty}\left\{\left\|\boldsymbol{h}_{\mathrm{uj}}\right\|^2>\left|Z_j\right|^{\alpha_j}P_j^{-1}t\right\}\mathrm{d}t\\&=\sum_{j=1}^{K}\left(\frac{2\pi\lambda_jP_j\left(D_j\right)^{2-\alpha_j}}{\alpha_j-2}\right)\end{aligned} \tag{13}$$

其中，$D_j=(P_j/P_i)^{1/\alpha_j}X_i^{\alpha_i/\alpha_j}$，由于用户接入接收功率最大的基站，即 $P_{\mathrm{ri}}>\max_{j,j\neq i}P_{\mathrm{rj}}$，可得第 j 层干扰基站距离用户应满足条件 $D_j>(P_j/P_i)^{1/\alpha_j}X_i^{\alpha_i/\alpha_j}$。将式(10)、式(11)、式(12)及式(13)代入式(8)可得 R_{U}^{L}，定理 1 得证。

定理 2 用户接入第 i 层的安全中断概率 $P_{\mathrm{out}}^{i}(R_i)$ 为

$$P_{\mathrm{out}}^{i}(R_i)=\begin{cases}1-\exp\left(-2\pi\lambda_e\displaystyle\int_0^{\infty}K\left(R_{\mathrm{U}}^{L_i}-R_i,\,y\right)y\mathrm{d}y\right), & 0<\rho_i\leq1\\ 1, & \rho_i=0\end{cases} \tag{14}$$

其中，

$$\begin{aligned}&K\left(R_{\mathrm{U}}^{L_i}-R_i,\,y\right)\\&=\prod_{j=1}^{K}\exp\left(-2\pi\lambda_j\right.\\&\quad\cdot\left.\int_0^{\infty}\left(1-\frac{1}{\left(2^{\left(R_{\mathrm{U}}^{L_i}-R_i\right)}-1\right)P_jy^{\alpha_i}z^{-\alpha_j}/P_i+1}\right)z\mathrm{d}z\right)\\&\quad\cdot\exp\left(-\frac{{\sigma_e}^2\left(2^{\left(R_{\mathrm{U}}^{L_i}-R_i\right)}-1\right)}{P_iy^{-\alpha_i}}\right)\end{aligned} \tag{15}$$

证明　窃听者不联合窃听，因此考虑最危险的窃听者，其接收 SINR 的分布函数可表示为

$$\mathbb{F}_{\mathrm{SINR}_{\mathrm{E}}^{i}}(\gamma)=\mathbb{E}\left\{\prod_{e\in\Phi_e}\mathbb{P}\left[\left\|\boldsymbol{h}_{\mathrm{ei}}\widetilde{\boldsymbol{w}}_i\right\|^2\le\frac{I_{\mathrm{ei}}+{\sigma_e}^2}{P_i\left|Y_i\right|^{-\alpha_i}}\gamma\right]\right\}$$
$$=\exp\left(-2\pi\lambda_e\int_0^{\infty}K(\gamma,y)\,y\mathrm{d}y\right)\tag{16}$$

其中，

$$K(\gamma,y)=\mathbb{E}\left[\exp\left(-\frac{\sum_{B_{\mathrm{jt}}\in\Phi_j\setminus B_{\mathrm{im}}}P_j\left\|\boldsymbol{h}_{\mathrm{ej}}\right\|^2|Z|^{-\alpha_i}+{\sigma_e}^2}{P_i\left|Y_i\right|^{-\alpha_i}}\gamma\right)\right]$$
$$=\prod_{j=1}^{K}\exp\left(-2\pi\lambda_j\int_0^{\infty}\left(1-\frac{1}{\gamma P_j y^{\alpha_i}z^{-\alpha_j}/P_i+1}\right)z\mathrm{d}z\right)$$
$$\cdot\exp\left(-\frac{{\sigma_e}^2\gamma}{P_i y^{-\alpha_i}}\right)\tag{17}$$

将式(9)、式(16)及式(17)代入式(7)即可得第 i 层的安全中断概率，定理 2 得证。

由于系统接入第 i 层基站的接入概率为 $\mathcal{A}_i$，则 K 层密集异构蜂窝网络系统的安全中断概率 P_{out} 可表示为

$$P_{\mathrm{out}}=\sum_{i=1}^{K}\mathcal{A}_iP_{\mathrm{out}}^{i}\left(R_i\right)\tag{18}$$

由式(18)可知，用户接入第 i 层蜂窝网时的 SOP 受该层的信道估计精度 ρ_i、窃听者分布密度 λ_e、安全中断门限 R_i 等参数的影响，接下来分析相关参数及其影响。

3.3 安全中断概率影响因素分析

3.3.1 信道估计精度 $\boldsymbol{\rho_i}$　ρ_i 直接影响用户的平均可达速率 $R_{\mathrm{U}}^{L_i}$，当安全中断门限一定时，SOP 随 $R_{\mathrm{U}}^{L_i}$ 的增加单调递减。因此通过研究 ρ_i 与 $R_{\mathrm{U}}^{L_i}$ 的关系来研究 ρ_i 与 SOP 的关系。

推论 1 平均可达速率 $R_{\mathrm{U}}^{L_i}$ 随 ρ_i 的变化单调递增。当 $0\le\rho_i\le1$ 时，有

$$\frac{\partial R_{\mathrm{U}}^{L_i}}{\partial\rho_i}=\frac{\left(N_i-1\right)}{\ln(2)\cdot\left[\left(N_i-1\right)\rho_i+\vartheta+P_i\right]}\tag{19}$$

其中，$\vartheta=\int_0^{\infty}\left(\mathbb{E}\left(I_{\mathrm{ui}}\right)+\sigma^2\right)x^{\alpha_i}f_{X_i}(x)\mathrm{d}x$。由于 $0\le\rho_i\le1$ 且 $N_i>1$，因此 $\dfrac{\partial R_{\mathrm{U}}^{L_i}}{\partial\rho_i}>0$。

由式(19)可知，当 $0\le\rho_i\le1$ 时第 i 层合法用户的平均可达速率随着该层信道估计精度 ρ_i 的变化单调递增。当 $\rho_i=1$，$R_{\mathrm{U}}^{L_i}$ 可达最大值；当 $\rho_i=0$ 时，$R_{\mathrm{U}}^{L_i}=0$。这是由于信道估计精度提高时信号的波束能更精确地对准合法用户，因此 $R_{\mathrm{U}}^{L_i}$ 提高。由于 $P_{\mathrm{out}}^{i}\left(R_i\right)$ 随 $R_{\mathrm{U}}^{L_i}$ 的变化单调递减，因此 ρ_i 增加时 $P_{\mathrm{out}}^{i}\left(R_i\right)$ 减小。由式(18)可知，各层 SOP 和接入概率 $\mathcal{A}_i$ 决定了系统的 SOP，每层网络的信道估计精度 ρ_i 以概率 $\mathcal{A}_i$ 影响整个系统的安全性能。因此，同时改善每层网络的估计精度能更高效地提升系统的安全性能。

3.3.2 窃听者密度 $\boldsymbol{\lambda_e}$、安全中断门限 $\boldsymbol{R_i}$　λ_e，R_i 等参数直接影响系统的安全性能，在非理想场景中，这种影响还与 ρ_i 有关，因此研究非理想情况下 λ_e，R_i 与 $P_{\mathrm{out}}^{i}\left(R_i\right)$ 的关系。

推论 2 $P_{\mathrm{out}}^{i}\left(R_i\right)$ 随 λ_e 的变化单调递减。当 $0<\rho_i\le1$ 时，有

$$\frac{\partial P_{\mathrm{out}}^{i}\left(R_i\right)}{\partial\lambda_e}=2\pi\int_0^{\infty}K\left(R_{\mathrm{U}}^{L_i}-R_i,y\right)y\mathrm{d}y$$
$$\cdot\exp\left(-2\pi\lambda_e\int_0^{\infty}K\left(R_{\mathrm{U}}^{L_i}-R_i,\,y\right)y\mathrm{d}y\right)\tag{20}$$

由于 $\exp(\cdot)>0$，$K\left(R_{\mathrm{U}}^{L_i}-R_i,y\right)=\prod_{j=1}^{K}\exp(\cdot)>0$，因此 $\dfrac{\partial P_{\mathrm{out}}^{i}\left(R_i\right)}{\partial\lambda_e}>0$。

推论 3 $P_{\mathrm{out}}^{i}\left(R_i\right)$ 随 R_i 的变化单调递减。当 $0<\rho_i\le1$ 时，有

$$\frac{\partial P_{\mathrm{out}}^{i}\left(R_i\right)}{\partial R_i}=2\pi\lambda_e\exp\left(-2\pi\lambda\int_0^{\infty}\frac{\partial K\left(R_{\mathrm{U}}^{L_i}-R_i,y\right)}{\partial R_i}y\mathrm{d}y\right)\tag{21}$$

由于 $\exp(\cdot)>0$，因此 $\dfrac{\partial P_{\mathrm{out}}^{i}\left(R_i\right)}{\partial R_i}>0$。

由式(20)，式(21)可知，当 $0<\rho_i\le1$ 时，无论信道估计准确与否，λ_e 和 R_i 的提高必然使 $P_{\mathrm{out}}^{i}\left(R_i\right)$ 增大。此外，ρ_i 也会改变 λ_e，R_i 对系统性能的影响。同等程度地增加 λ_e，信道估计非理想的系统安全性能必然劣于理想情况。这是由于合法信道估计不准确导致信号波形无法对准合法用户，用户的平均可达速率变小，且未对准的波束泄露到合法信道以外的空间，窃听者密度越大波束泄露到窃听信道空间的概率越大，因此相对于理想信道估计，非理想信道估计系统更容易受到窃听者密度变化的影响。

类似地，以同样程度增大 R_i，信道估计非理想的系统安全性能必然劣于理想情况。这是由于 R_i 增加时，用户只有相应地提高平均可达速率才能保证安全通信不会中断，而非理想信道估计使用户的平均可达速率反而变小，SOP 更高。因此相对于理想信道估计，非理想信道估计系统更容易受到安全中断门限的影响。

3.3.3 基站天线数量 $\boldsymbol{N_i}$　增加 N_i 将提升安全性能，而非理想场景中，N_i 不仅带来分集增益，也使系统更容易受信道估计误差的影响，因此分析 N_i 与

$P_{\text{out}}^{i}(R_i)$的关系。

推论 4 $P_{\text{out}}^{i}(R_i)$随N_i的变化单调递减。当$0 \le \rho_i \le 1$时，有

$$\frac{\partial R_{\text{U}}^{L_i}}{\partial N_i} = \frac{\rho_i P_i}{\ln(2)\left[\rho_i P_i N_i + (1-\rho_i)P_i + \vartheta\right]} \tag{22}$$

其中，$\vartheta = \int_0^{\infty}\left(\mathbb{E}(I_{\text{ui}}) + \sigma^2\right)x^{\alpha_i} f_{X_i}(x)\mathrm{d}x$。由于$0 \le \rho_i \le 1$，因此$\dfrac{\partial R_{\text{U}}^{L_i}}{\partial N_i} > 0$。

由于$R_{\text{U}}^{L_i}$随着N_i的变化单调增加且$P_{\text{out}}^{i}(R_i)$随$R_{\text{U}}^{L_i}$的变化单调递减，因此$P_{\text{out}}^{i}(R_i)$随N_i的变化单调递减。由式(22)可知，当$0 \le \rho_i \le 1$时，增加N_i均会导致 SOP 减小。这是由多天线增益带来的系统安全性能提升。而对比理想和非理想的情况，前者的多天线增益优于后者，这是由于增加天线数量虽然带来了分集增益，但由于信道估计不理想，天线数量的增加也使得非理想的因素增加，系统更容易受到信道估计非理想的影响。因此，非理想信道估计会严重影响多天线的分集增益。

4 仿真分析

本节利用 Matlab 仿真验证了部分系统参数对安全性能的影响。以两层密集异构蜂窝网为例，分别用宏蜂窝基站和微蜂窝基站表示，其中宏基站部署 20 根天线，微基站部署 5 根天线，路径衰落系数$\alpha = 3$，其余主要参数配置如表 1 所示。

表 1 主要仿真参数

图号	参数								
	ρ_1	ρ_2	R_1 (bit/(s·Hz))	R_2 (bit/(s·Hz))	λ_1	λ_2	λ_e	P_1 (W)	P_2 (W)
图1	–	–	2	1	0.01	0.05	0.06	20	2
图2	0.5/1	0.5/1	2	1	0.01	0.05	–	20	2
图3	0.8/1	0.8/1	–	–	0.01	0.05	0.03	20	2
图4	–	–	2	1	0.01	–	0.03	20	2

4.1 信道估计精度对系统性能的影响

图 1 给出了信道估计精度与各层以及系统 SOP 的关系，从两个角度入手：(1)仅改变微基站信道估计精度；(2)同时改变宏基站和微基站信道估计精度，以 SOP 为指标研究信道估计精度对系统安全性能的影响。其中，横坐标表示信道估计精度，纵坐标表示安全中断概率。

4.1.1 微基站信道估计精度 ρ_2 假设宏基站能够准确估计信道，即ρ_1=1。通过改变ρ_2，研究单层基站信道估计精度改变对系统安全性能的影响。如图 1(a)所示，当$\rho_2 = 0$时，微蜂窝层的 SOP 接近 1，几乎无法正常通信；但由于此时宏基站准确估计信道，其安全性能较好；因此系统的 SOP 居于宏/微蜂窝层的 SOP 之间。随着微基站的信道估计精度提高，信道估计越准确，系统的 SOP 下降，微蜂窝层的安全性能提高，宏蜂窝的安全性能并不会受到ρ_2的影响。当$\rho_2 = 0.9$时，系统及各层的 SOP 交于一点。可从式(18)看出，当宏/微蜂窝的 SOP 相等时，系统以概率 1 接入两层蜂窝中的任意一层。从图中可以看出仅微基站的信道估计精度从 0 变为 1 系统的安全性能提升约 60%。

4.1.2 宏、微基站信道估计精度 ρ_1, ρ_2 单层及系统的 SOP 随ρ_1, ρ_2变化的情况如图 1(b)所示，在信道估计精度ρ_1, ρ_2均从 0 变化到 1 的过程中，信道估计越来越准确，单层及系统的 SOP 均不断下降。从图中可以看出同时改变宏、微基站的信道估计精度，系统的安全性能提升约 80%。

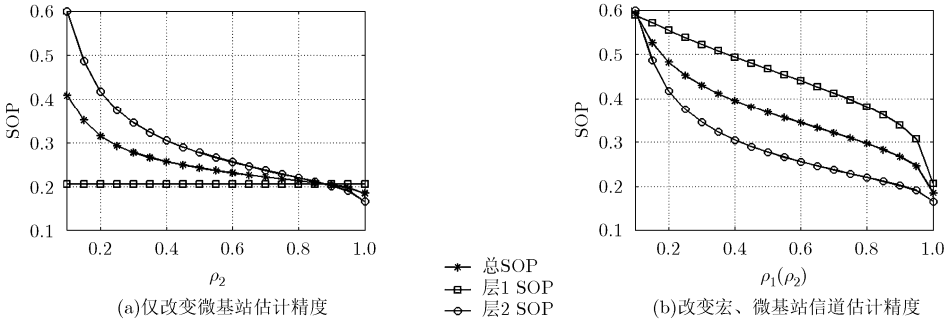

图 1 不同信道估计精度条件下的安全中断概率

4.2 窃听者密度对系统性能的影响

图 2 给出了在信道估计理想及非理想条件下窃听者分布密度与各层及系统的 SOP 的关系。由图可知，λ_e 的增加必然提高 SOP，且 SOP 的增长速率随着 λ_e 的增加逐渐变缓。这是由于初始阶段增加 λ_e 时，系统中不断出现有更大 $\mathrm{SINR}_{\mathrm{E}}^{i}$ 的窃听者，因此此时 SOP 上升速率较快；随着 λ_e 的继续增加，系统中继续出现有更大 $\mathrm{SINR}_{\mathrm{E}}^{i}$ 的窃听者的概率减小，因此 SOP 上升速率变缓。

此外，不同信道估计对系统的安全性能产生不同的影响。在 λ_e 一定的情况下，理想信道估计相对于估计精度为 0.5 的系统安全性能最大提升了约 40%，因此准确的信道估计是保证安全通信的重要前提。

4.3 安全中断门限设置对系统性能的影响

图 3 给出了在信道估计理想及非理想条件下，安全门限与各层及系统的 SOP 的关系。如图 3 所示，无论发射端天线数量的多少，系统及两层蜂窝网的 SOP 均随安全门限的增大而增大。比较不同信道估计精度对安全性能的影响，可以发现信道估计非理想的系统对安全门限更敏感，SOP 上升速率比理想系统更快。

安全门限一定时，同样程度地增加天线数量，信道估计非理想的系统安全性能提升较小。这是由于天线数量的增加虽然带来了分集增益，但对于信道估计不理想的系统，天线数量的增加也使得系统更容易受信道估计非理想的影响，且估计精度越低这种影响越明显。

4.4 微基站分布密度对系统性能的影响

将微基站部署在宏蜂窝小区内，可以卸载宏蜂窝巨大的业务量提升系统处理能力，同时微基站的加入对系统的安全性能也将产生影响。图 4 给出了不同信道估计精度情况下的微基站分布密度与各层以及系统 SOP 的关系。从以下 3 个角度讨论信道估计精度对系统安全性能的影响：(1)宏/微基站信道估计精度相同；(2)宏基站信道估计精度高于微基站；(3)宏基站信道估计精度低于微基站。

4.4.1 宏/微基站信道估计精度相同 $\rho_1=\rho_2$　图 4(a) 给出了 $\rho_1=\rho_2$ 时，系统及各层 SOP 随 λ_2 的变化情况。如图所示，系统的 SOP 随着 λ_2 的增加而减小，这是由于用户可以通过接入控制来选择接入的基站，λ_2 的增加使用户可选的服务基站更多，系统的安全性能得到提升。因此在各层信道估计误差相同时，增加微基站密度能够提升系统的安全性能。

随着 λ_2 的提高，系统安全性能提升的速率减慢，当 λ_2 较大时系统的 SOP 趋于平缓。一方面，这是由于微基站数量的增多给用户提供了更大的选择空间，从而提升系统安全性能；另一方面，这又给相邻小区引入了干扰，λ_2 越高干扰越严重。干扰同时影响合法用户和窃听者，当前环境中合法用户受到

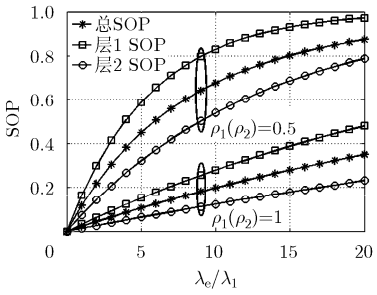

图 2 不同窃听者分布密度时的安全中断概率

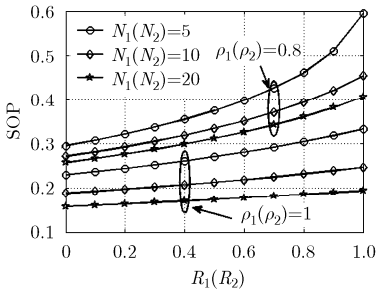

图 3 不同安全中断门限时的安全中断概率

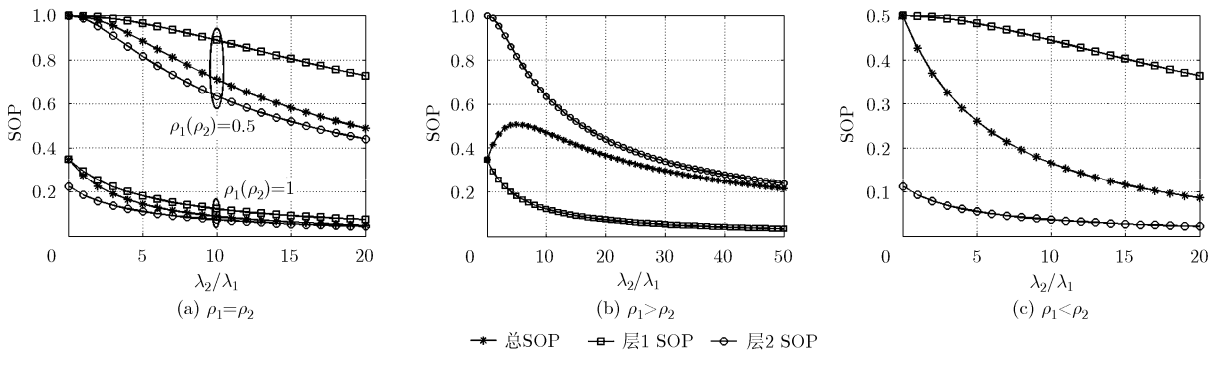

图 4 不同微基站密度时的安全中断概率

的影响小于窃听者，但这种优势随着干扰的增大不断减弱。因此 SOP 虽然不断下降，但是下降的速率越来越缓慢。

4.4.2 宏基站信道估计精度高于微基站 $\rho_1 > \rho_2$ 图 4(b)给出了 $\rho_1 > \rho_2$，且 ρ_1=1, ρ_2=0.5 时，系统及各层的 SOP 与 λ_2 的关系。如图所示，单层 SOP 随 λ_2 的增加而下降，这是由于微基站的增加使用户可选择的服务基站变多，单个用户的安全性能得到保证。而系统的 SOP 却出现先上升后下降的情况，这是由微基站信道估计不准确造成的：初始阶段 λ_2 的增加使用户能够接入微基站，但却受到信道估计不准确的影响，系统的 SOP 反而升高；继续增加 λ_2，系统 SOP 逐渐下降趋于平缓。因此在 $\rho_1 > \rho_2$ 时，单纯增加微基站密度不一定能提升系统安全性能。

4.4.3 宏基站信道估计精度低于微基站 $\rho_1 < \rho_2$ 图 4(c)给出了 $\rho_1 < \rho_2$，且 ρ_1=0.5，ρ_2=1 时，系统及各层的 SOP 与 λ_2 的关系。从图中可以看出，各层及系统的 SOP 均随着 λ_2 的增加而下降。因此在 $\rho_1 < \rho_2$ 时，增加微基站密度能够有效地提升系统安全性能。

综上可知，当微基站信道估计精度不低于宏基站的估计精度，即 $\rho_1 \le \rho_2$ 时，在宏蜂窝中部署微基站可以提升系统安全性能。

5 结束语

本文针对 K 层密集异构蜂窝网在信道估计存在误差时的系统安全性能展开研究，从密集异构蜂窝网自身结构及实际部署的特点出发，分析了非理想信道估计条件下系统的安全性能。利用随机几何工具推导了 K 层密集异构蜂窝网的安全中断概率与信道估计精度的关系式，然后分析了窃听者分布密度、微基站分布密度、安全门限、天线数量等参数对系统安全性能的影响。仿真验证了理论推导的有效性，发现当信道由完全精确估计下降到完全不准确估计时，系统的安全性能下降可达 60%~80%，系统几乎不能正常通信。在此基础上，以安全中断概率为指标对比了不同信道估计精度对系统参数设置的影响，及其给安全性能带来的变化。讨论了在宏蜂窝中部署不同信道估计精度的微基站对系统安全性能的影响，得出结论当 $\rho_1 \le \rho_2$ 时，在宏蜂窝中部署微基站可以提升系统安全性能。

参 考 文 献

[1] XIE B, KUMAR A, ZHAO D, *et al*. On secure communication in integrated heterogeneous wireless networks [J]. *International Journal of Information Technology Communications & Convergence,* 2010, 1(1): 4–23. doi: 10.1504/IJITCC.2010.035224.

[2] VALERO M, SANG S J, ULUAGAC A S, *et al*. Di-Sec: A distributed security framework for heterogeneous wireless sensor networks[C]. Proceedings of IEEE INFOCOM, 2012, 131(5): 585–593. doi: 10.1109/INFCOM.2012.6195801.

[3] BLOCH M and BARROS J. Physical-layer Security: From Information Theory to Security Engineering[M]. Cambridge University Press, 2011: 290–308. doi: 10.1017/CBO9780511977985.

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

[5] WU Huici, TAO Xiaofeng, LI Na, *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.

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

[7] DENG Yansha, WANG Lifeng, ELKASHLAN M, *et al*. Physical layer security in three-tier wireless sensor networks: A stochastic geometry approach[J]. *IEEE Transactions on Information Forensics & Security*, 2016, 11(6): 1128–1138. doi: 10.1109/TIFS.2016.2516917.

[8] XU Xiaoming, YANG Weiwei, CAI Yueming, *et al*. 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.

[9] TING A, CHIENG D, KWONG K H, *et al*. Dynamic backhaul sensitive network selection scheme in LTE-WiFi wireless HetNet[C]. IEEE International Symposium on Personal Indoor and Mobile Radio Communications, 2013: 3061–3065. doi: 10.1109/PIMRC.2013.6666672.

[10] MUKHERJEE A and SWINDLEHURST A L. Robust beamforming for security in MIMO wiretap channels with imperfect CSI[J]. *IEEE Transactions on Signal Processing*, 2011, 59(1): 351–361. doi: 10.1109/TSP.2010.2078810.

[11] PEI Minyan, WEI Jibo, WONG Kai-Kit, *et al*. Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI[J]. *IEEE Transactions on Wireless*

Communications, 2012, 11(2): 544–549. doi: 10.1109/TWC.2011.120511.110567.

[12] LIAO Weicheng, CHANG Tsunghua, MA Wingkin, *et al*. QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach [J]. *IEEE Transactions on Signal Processing*, 2011, 59(3): 1202–1216. doi: 10.1109/TSP.2010.2094610.

[13] JO H S, SANG Y J, XIA P, *et al*. Heterogeneous cellular networks with flexible cell association: A comprehensive downlink SINR analysis[J]. *IEEE Transactions on Wireless Communications*, 2011, 11(10): 3484–3495. doi: 10.1109/TWC.2012.081612.111361.

[14] CHEN Xiaoming. 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.

[15] GERBRACHT S, SCHEUNERT C and JORSWIECK E A. Secrecy outage in MISO systems with partial channel information[J]. *IEEE Transactions on Information Forensics & Security*, 2012, 7(2): 704–716. doi: 10.1109/TIFS.2011.2181946.

[16] DENG Yansha, WANG Lifeng, WONG K, *et al*. Safeguarding massive MIMO aided hetnets using physical layer security[C]. International Conference on Wireless Communications & Signal Processing, Nanjing, China, 2015: 1544–1566.

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.

许耘嘉：　女，1993 年生，硕士生，研究方向为移动通信、物理层安全.

丁大钊：　男，1979 年生，工程师，研究方向为通信与信息系统.