

## 基于带内无线回程的 HetNets 安全性能研究

颌满刚<sup>1</sup>, 贾向东<sup>1,2</sup>, 周 猛<sup>1</sup>, 纪珊珊<sup>1</sup>, 焦金良<sup>1</sup>, 杨 正<sup>1</sup>

(1. 西北师范大学 计算机科学与工程学院, 兰州 730070; 2. 南京邮电大学 江苏省无线通信重点实验室, 南京 210003)

**摘 要:** 为解决当前异构网络物理层安全性能低下的问题, 提出一种带内全双工 (IB-FD) 无线回程方案。在大规模多入多出 (MIMO) 双层 HetNets 中, 宏蜂窝和小蜂窝通信链路受恶意窃听器窃听, 将无线回程信号作为宏蜂窝与小蜂窝通信的干扰信号, 以增强通信链路质量。借助随机几何与概率统计工具, 将网络节点分别建模为齐次泊松点过程, 研究宏蜂窝下行和小蜂窝上行传输的安全概率。研究表明, 在大规模 MIMO 双层 HetNets 中, 将 IB-FD 无线回程信号作为一种干扰信号, 宏蜂窝下行和小蜂窝上行链路的安全概率得到有效提高, 且物理层安全性能优于带外全双工无线回程方案。

**关键词:** 异构网络; 多入多出; 全双工; 带内回程; 安全概率

**中文引用格式:** 颌满刚, 贾向东, 周 猛, 等. 基于带内无线回程的 HetNets 安全性能研究[J]. 计算机工程, 2018, 44(5): 101-106.

**英文引用格式:** XIE Mangang, JIA Xiangdong, ZHOU Meng, et al. Research on Security Performance of HetNets Based on In-band Wireless Backhaul[J]. Computer Engineering, 2018, 44(5): 101-106.

## Research on Security Performance of HetNets Based on In-band Wireless Backhaul

XIE Mangang<sup>1</sup>, JIA Xiangdong<sup>1,2</sup>, ZHOU Meng<sup>1</sup>, JI Shanshan<sup>1</sup>, JIAO Jinliang<sup>1</sup>, YANG Zheng<sup>1</sup>

(1. College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China;

2. Wireless Communication Key Lab of Jiangsu Province, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

**[Abstract]** In order to solve the problem of low physical layer security performance in heterogeneous networks, an In-Band Full-Duplex (IB-FD) wireless backhaul scheme is proposed. In massive Multiple Input Multiple Output (MIMO) two-tier HetNets, macro and small cell links are eavesdropped by malicious eavesdroppers, and the wireless backhaul signal is regarded as the interference signal for macro and small cell communications to enhance communication link quality. By using the tool of stochastic geometry and probability statistics, we modeled the network elements as independent Poisson point processes, and investigate the secrecy probability of the macro cell downlinks and small cell uplinks. The presented results show that in massive MIMO HetNets, exploiting the IB-FD wireless backhaul signal as the interference can enhance the secrecy probabilities of both the macro and small cell transmission, and the in-band full-duplex backhaul mode outperforms the out-band Full-Duplex (FD) one.

**[Key words]** Heterogeneous Networks (HetNets); Multiple Input Multiple Output (MIMO); full duplex; in-band backhaul; security probability

**DOI:** 10.19678/j.issn.1000-3428.0046471

## 0 概述

大规模多入多出 (Multiple Input Multiple Output, MIMO)<sup>[1-3]</sup>、全双工 (Full-Duplex, FD)<sup>[4]</sup> 和异构网络 (Heterogeneous Networks, HetNets)<sup>[5-6]</sup> 是未来 5G 网络的 3 种关键技术, 三者的有效结合能够发挥各自优势, 并极大提高系统性能。然而, 随着小蜂窝网络的

大规模部署, 大量的回程数据需要反馈到核心网, 回程问题变得日趋重要<sup>[7]</sup>。

一般有 3 种小蜂窝回程解决方案, 即有线光纤连接方案, 微波或毫米波点对点定向无线传输方案和共享接入网频谱无线传输方案。在这 3 种回程传输方案中, 由于接入网无线电波的广播属性, 共享接入网频谱无线传输方案特别适合于非视距传输场

**基金项目:** 国家自然科学基金 (61261015, 61561043); 甘肃省属普通高校基本科研业务费专项资金“面向 5G 的 Massive MIMO 毫米波段信道建模及其估计”; 西北师范大学创新能力提升计划项目“面向毫米波的大规模 MIMO 异构网络方案设计及性能分析”。

**作者简介:** 颌满刚 (1990—), 男, 硕士研究生, 主研方向为移动通信; 贾向东, 副教授、博士后; 周 猛、纪珊珊、焦金良、杨 正, 硕士研究生。

**收稿日期:** 2017-03-22

**修回日期:** 2017-05-04

**E-mail:** jiaxd@nwnu.edu.cn

景,能够很好满足具有高大建筑物的市区无线通信需求,特别是带内(In-Band, IB)接入网频谱共享方案(蜂窝网链路和回程链路工作在同一频段)因其较高的频谱效率备受青睐<sup>[8]</sup>。同时,考虑到回程传输和接入网传输间的互干扰,在已有的文献中重点将回程传输看作无线接入网通信的一种障碍,即带内无线回程将使接入容量下降,误码率增加<sup>[9]</sup>。然而,当考虑到安全问题时,情况可能并非如此,由于回程传输对窃听者来讲是未知信号,可降低窃听信号信噪比,有利于提高网络的安全性能<sup>[10-12]</sup>。

基于上述考虑,本文建立一种基于带内无线回程的 FD 大规模 MIMO 双层 HetNets 模型。大规模 MIMO 宏蜂窝基站(Macro Cell Base Station, MBS)和单天线小蜂窝基站(Small Cell Base Station, SBS)均工作在带内回程模式,宏蜂窝和小蜂窝用户共享接入和回程链路频带资源,并受恶意窃听者的窃听。在该网络模型下,研究宏蜂窝下行和小蜂窝上行链路的安全概率。

## 1 网络模型及信道假设

如图 1 所示,FD 大规模 MIMO 双层 HetNets 由宏蜂窝用户终端(User Equipment, UE)、小蜂窝 UE 和窃听者(Eavesdropper, Eve)组成,小蜂窝覆盖在宏蜂窝之上减轻宏蜂窝负载。MBS 与 UE、UE 与 SBS、MBS 与 SBS 之间的链路分别为宏蜂窝下行、小蜂窝上行和回程链路。小蜂窝通过 MBS 连接到核心网,MBS 提供无线回程连接到小蜂窝,MBS 和 SBS 都工作在 FD 模式。MBS 配备了  $M_{Tx}$  个发送天线和  $M_{Rx}$  个接收天线,而 SBS 和 UE 均配备单天线。同时,假设一个 MBS 能够服务的最大 UE 数为  $N_m$ ,最大回程数  $N_n$ ,且满足  $\min(M_{Tx}, M_{Rx}) \gg N_n$  和  $\min(M_{Tx}, M_{Rx}) \gg N_m$ 。宏蜂窝和小蜂窝链路被恶意的 Eve 所窃听,Eve 只对宏蜂窝与小蜂窝的信号进行拦截和破译并不对其进行篡改。

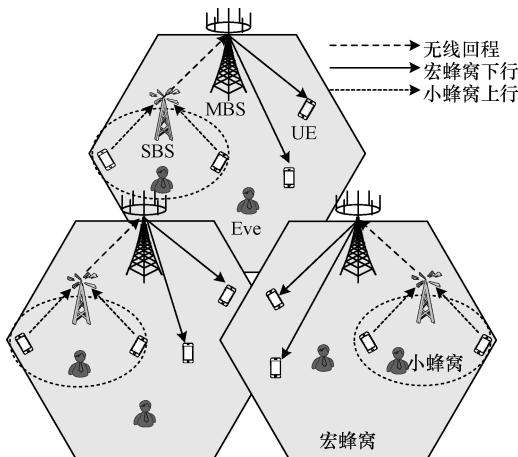


图 1 基于带内无线回程的全双工大规模 MIMO 双层 HetNets

MBS、SBS、UE 和 Eve 的空间拓扑结构都被建模为独立泊松点过程(Poisson Point Processes, PPPs)  $\Phi_M$ 、 $\Phi_S$ 、 $\Phi_{UE}$  和  $\Phi_{Ev}$ ,其强度分别为  $\lambda_M$ 、 $\lambda_S$ 、 $\lambda_{UE}$  和  $\lambda_{Ev}$ 。HetNets 中所有的无线信道相互独立,并且都经历路径损失和瑞利衰落。对于任意 2 个网络元素  $a$  和  $b$ ,分别用  $h_{ab}$  和  $r_{ab}$  表示小规模衰落信道功率增益和  $a$  与  $b$  之间的距离,路径损失表示为  $r_{ab}^{-\beta}$ ,  $\beta \in (\alpha_M, \alpha_S)$ ,其中,  $\alpha_M$  为宏蜂窝路径损失指数,  $\alpha_S$  为小蜂窝路径损失指数。此外,假设随机分布的 UE 只对应一个 SBS。根据 PPP 的性质<sup>[13]</sup>,定义一个新 PPP  $\tilde{\Phi}_{UE}$ ,表示与 SBS 对应的 UE 位置,显然  $\tilde{\Phi}_{UE}$  与  $\Phi_S$  有相同的强度。

同时,仅考虑宏蜂窝下行和小蜂窝上行传输,宏蜂窝与小蜂窝共享频谱。假设系统获得了可靠的信道状态信息,MBS 采用迫零接收和发送。有以下信号传输方案:对于小蜂窝上行,在相同的时频资源块,任一个 SBS 能够以功率  $P_{SB}$  发送回程数据到与其对应 MBS,同时接收距离最近 UE 以功率  $P_{UE}$  发送的数据。对于宏蜂窝下行,任一个 MBS 以功率  $P_{MB}$  发送数据到其对应的 UE,同时接收来自于 SBS 的回程数据。

## 2 安全概率分析

### 2.1 宏蜂窝下行链路安全概率

不失一般性,考虑任一宏蜂窝下行链路,宏蜂窝 UE 位于原点  $o$ ,MBS 位于点  $x$ 。那么,位于  $z$  点处的 Eve 接收到的信号与干扰噪声比(Signal to Interference Noise Ratio, SINR)表示为:

$$SINR_c^c(z) = \frac{\frac{P_{MB}}{\min(N_m, K_m)} h_{xz} r_{xz}^{-\alpha_M}}{I_A + I_{MBS}^{cc} + I_{SBS}^{cc} + I_{UE}^{cc}} \quad (1)$$

其中,信道功率增益满足  $h_{xz} \sim \exp(1)$ 。  $K_m$  为与 MBS 链接的 UE 数,其为一随机变量,可能会有  $K_m > N_m$ 。为了方便分析,将  $K_m$  近似为其平均值  $E\{K_m\} = \frac{\lambda_{UE}}{\lambda_M}$ ,  $E\{\cdot\}$  表示期望操作。同时,宏蜂窝

之间干扰为  $I_A = \frac{P_{MB}}{\min(N_m, K_m)} h_z r_{xz}^{-\alpha_M}$ ,小规模功率增益  $h_z \sim \Gamma(\min(N_m, K_m) - 1, 1)$ ,  $\Gamma(\cdot, \cdot)$  表示伽玛函数。  $I_{MBS}^{cc} = \sum_{l \in \Phi_M \setminus x} \frac{P_{MB}}{\min(N_m, K_m)} h_{lz} r_{lz}^{-\alpha_M}$  表示来自于 MBS 的干扰,对应的小规模衰落干扰信道增益为  $h_{lz} \sim \Gamma(\min(N_m, K_m), 1)$ 。  $I_{SBS}^{cc} = \sum_{i \in \Phi_S} P_{SB} h_{iz} r_{iz}^{-\alpha_S}$  是 SBS 回程传输的干扰,其信道功率增益为  $h_{iz} \sim \exp(1)$ 。  $I_{UE}^{cc} = \sum_{i \in \tilde{\Phi}_{UE}} P_{UE} h_{iz} r_{iz}^{-\alpha_M}$  为来自于 UE 的干扰,信道功率增益满足  $h_{iz} \sim \exp(1)$ 。

在被动 Eve 场景下,每一条链路都暴露于所有的 Eve。此时,只需考虑最恶意的 Eve,其拥有最强 SINR。那么,任一宏蜂窝下行链路的安全概率可以

表示为:

$$P_{\text{Sec}}^c(T_e^c) = \Pr\left\{\max_{z \in \Phi_{\text{UE}}} \text{SINR}_e^c(z) < T_e^c\right\} \quad (2)$$

其中,  $T_e^c$  是安全门限,借助随机几何,可得定理 1。

**定理 1** 在基于带内无线回程的全双工大规模 MIMO 双层 HetNets 中,任一宏蜂窝下行链路的安全概率可以表示为:

$$P_{\text{Sec}}^c(T_e^c) = \exp\left\{-2\pi\lambda_{\text{Ev}} \int_0^\infty \mathcal{L}_{I_{\text{MBS}}^{\text{ce}}}(s) \mathcal{L}_{I_{\text{SBS}}^{\text{ce}}}(s) \times \mathcal{L}_{I_{\text{UE}}^{\text{ce}}}(s) \frac{r}{(1+T_e^c)^{\min(N_m, K_m)-1}} dr\right\} \quad (3)$$

其中,  $s = \frac{T_e^c}{\tilde{P}_{\text{MB}} r^{-\alpha_M}}$ ,  $\tilde{P}_{\text{MB}} = \frac{P_{\text{MB}}}{\min(N_m, K_m)}$ 。  $\mathcal{L}_{I_{\text{MBS}}^{\text{ce}}}(s)$  和  $\mathcal{L}_{I_{\text{UE}}^{\text{ce}}}(s)$  是  $I_{\text{MBS}}^{\text{ce}}$ 、 $I_{\text{SBS}}^{\text{ce}}$  和  $I_{\text{UE}}^{\text{ce}}$  的拉普拉斯变换形式,分别表示为:

$$\mathcal{L}_{I_{\text{MBS}}^{\text{ce}}}(s) = \exp\left(-2\pi\lambda_{\text{M}} (\tilde{P}_{\text{MB}})^{\frac{2}{\alpha_M}} \sum_{k=1}^{\min(N_m, K_m)} \binom{\min(N_m, K_m)}{k} \times \frac{\Gamma(k-2/\alpha_M) \Gamma(\min(N_m, K_m)-k+2/\alpha_M)}{\Gamma(\min(N_m, K_m))}\right) \quad (4)$$

$$\mathcal{L}_{I_{\text{SBS}}^{\text{ce}}}(s) = \exp\left(\frac{-\pi\lambda_{\text{S}} (sP_{\text{SB}})^{\frac{2}{\alpha_S}}}{\sin(2/\alpha_M)}\right) \quad (5)$$

$$\mathcal{L}_{I_{\text{UE}}^{\text{ce}}}(s) = \exp\left(\frac{-\pi\lambda_{\text{S}} (sP_{\text{UE}})^{\frac{2}{\alpha_S}}}{\sin(2/\alpha_S)}\right) \quad (6)$$

证明:根据式(1)和定义  $I_A = \tilde{P}_{\text{MB}} h_z r_{xz}^{-\alpha_M}$ ,任一宏蜂窝下行链路的安全概率可以写成:

$$P_{\text{Sec}}^c(T_e^c) = \Pr\left\{\bigcap_{z \in \Phi_{\text{Ev}}} \text{SINR}_e^c(z) < T_e^c\right\} = \Pr\left\{\bigcap_{z \in \Phi_{\text{Ev}}} \frac{\tilde{P}_{\text{MB}} h_{xz} r_{xz}^{-\alpha_M}}{I_A^{\text{ce}} + I_{\text{MBS}}^{\text{ce}} + I_{\text{SBS}}^{\text{ce}} + I_{\text{UE}}^{\text{ce}}} < T_e^c\right\} = E_{\Phi_{\text{Ev}}}\left\{\prod_{z \in \Phi_{\text{Ev}}} \Pr\left\{\tilde{h}_z \leq \frac{T_e^c}{\tilde{P}_{\text{MB}} r_{xz}^{-\alpha_M}} \mid (I_{\text{MBS}}^{\text{ce}} + I_{\text{SBS}}^{\text{ce}} + I_{\text{UE}}^{\text{ce}})\right\}\right\} \quad (7)$$

其中,定义  $\tilde{h}_z = h_{xz} - T_e^c h_z$ ,且有  $h_z \sim \Gamma(\min(N_m, K_m) - 1, 1)$  和  $h_{xz} \sim \exp(1)$ ,可以得到  $\tilde{h}_z$  的累积分布函数  $F_{\tilde{h}_z}(y)$  表示为:

$$F_{\tilde{h}_z}(y) = \Pr\{(h_{xz} - T_e^c h_z) \leq y\} = E_{h_z}\{1 - e^{-(y+T_e^c h_z)}\} \quad (8)$$

根据  $h_z \sim \Gamma(\min(N_m, K_m) - 1, 1)$ ,  $h_z$  的概率密

$$\mathcal{L}_{I_{\text{MBS}}^{\text{ce}}}(s) = \exp\left(-2\pi\lambda_{\text{M}} \int_0^\infty \left[1 - \frac{1}{(1+s\tilde{P}_{\text{MB}} r^{-\alpha_M})^{\min(N_m, K_m)}}\right] r dr\right) = \exp\left\{-2\pi\lambda_{\text{M}} \sum_{k=1}^{\min(N_m, K_m)} \binom{\min(N_m, K_m)}{k} (s\tilde{P}_{\text{MB}})^k \times \int_0^\infty \frac{r^{-\alpha_M \cdot k+1}}{(1+s\tilde{P}_{\text{MB}} r^{-\alpha_M})^{\min(N_m, K_m)}} dr\right\} \quad (14)$$

以度函数可以写成:

$$f_w(w) = \frac{1}{\Gamma(\min(N_m, K_m) - 1)} w^{\min(N_m, K_m) - 2} e^{-w} \quad (9)$$

将式(9)代入式(8)得到:

$$F_{\tilde{h}_z}(y) = 1 - \frac{e^{-y}}{\Gamma(\min(N_m, K_m) - 1)} \cdot \int_0^\infty w^{\min(N_m, K_m) - 2} e^{-w(1+T_e^c)} dw = \frac{1 - e^{-y(1+T_e^c)^{1-\min(N_m, K_m)}}}{1 - e^{-y(1+T_e^c)^{1-\min(N_m, K_m)}}} \quad (10)$$

其中,  $(a)$  满足文献[14]中的式(3.381.4)。

将式(10)代入式(7),得到可实现的安全概率为:

$$P_{\text{Sec}}^c(T_e^c) = E_{\Phi_{\text{UE}}}\left\{\prod_{z \in \Phi_{\text{UE}}}\left[1 - \frac{1}{(1+T_e^c)^{\min(N_m, K_m)-1}} \times \exp\left(-\frac{T_e^c}{\tilde{P}_{\text{MB}} r_{xz}^{-\alpha_M}} (I_{\text{MBS}}^{\text{ce}} + I_{\text{SBS}}^{\text{ce}} + I_{\text{UE}}^{\text{ce}})\right)\right]\right\} = \exp\left(-2\pi\lambda_{\text{UE}} \int_0^\infty \exp\left(-\frac{T_e^c}{\tilde{P}_{\text{MB}} r_{xz}^{-\alpha_M}} (I_{\text{MBS}}^{\text{ce}} + I_{\text{SBS}}^{\text{ce}} + I_{\text{UE}}^{\text{ce}}) \times \frac{r}{(1+T_e^c)^{\min(N_m, K_m)-1}} dr\right)\right) \quad (11)$$

其中,  $(b)$  满足映射理论和 PPPs 的概率生成函数<sup>[15]</sup>。根据拉普拉斯变换的定义,可以得到式(3)。同时,根据  $I_{\text{MBS}}^{\text{ce}} = \sum_{l \in \Phi_{\text{M}} \setminus x} \tilde{P}_{\text{MB}} h_{lz} r_{lz}^{-\alpha_M}$  和  $h_{lz} \sim \Gamma(\min(N_m, K_m), 1)$ ,  $I_{\text{MBS}}^{\text{ce}}$  的拉普拉斯变换可以写为:

$$\mathcal{L}_{I_{\text{MBS}}^{\text{ce}}}(s) = E\{\exp(-s I_{\text{MBS}}^{\text{ce}})\} = \exp\left(-\lambda_{\text{M}} \int_{\mathbb{R}^2} (1 - E_{h_{lz}}\{\exp(-s\tilde{P}_{\text{MB}} h_{lz} r_{lz}^{-\alpha_M})\}) dr_{lz}\right) \quad (12)$$

其中,  $(c)$  满足文献[15]中的映射理论。根据  $h_{lz} \sim \Gamma(\min(N_m, K_m), 1)$ , 式(12)的积分项中期望可以写成:

$$E_{h_{lz}}\{\exp(-s\tilde{P}_{\text{MB}} h_{lz} r_{lz}^{-\alpha_M})\} = \int_0^\infty [\exp(-s\tilde{P}_{\text{MB}} r_{lz}^{-\alpha_M} x)] \cdot \frac{1}{\Gamma(\min(N_m, K_m))} x^{\min(N_m, K_m)-1} e^{-x} dx = (1 + s\tilde{P}_{\text{MB}} r_{lz}^{-\alpha_M})^{-\min(N_m, K_m)} \quad (13)$$

结合式(13)和式(12),得到:

为了计算式(14)中的积分项,使得  $x = r^{-\alpha_M}$ , 这样就有  $r = x^{-\frac{1}{\alpha_M}}$  和  $dr = \left(-\frac{1}{\alpha_M}\right)x^{-\frac{1}{\alpha_M}-1}dx$ , 式(14)中积分项可以写成:

$$A = \frac{1}{\alpha_M} \int_0^\infty \frac{x^{\frac{1}{\alpha_M}}}{(1 + s\tilde{P}_{MB}x)^{\min(N_m, K_m)}} x^{-\frac{1}{\alpha_M}-1} dx = \frac{1}{\alpha_M} (s\tilde{P}_{MB})^{-\left(k-\frac{2}{\alpha_M}\right)} B\left(k - \frac{2}{\alpha_M}, \min(N_m, K_m) - \left(k - \frac{2}{\alpha_M}\right)\right) \stackrel{(d)}{=} \frac{1}{\alpha_M} (s\tilde{P}_{MB})^{-\left(k - \frac{2}{\alpha_M}\right)} \cdot \frac{\Gamma\left(k - \frac{2}{\alpha_M}\right) \Gamma\left(\min(N_m, K_m) - k + \frac{2}{\alpha_M}\right)}{\Gamma(\min(N_m, K_m))} \quad (15)$$

其中, (d) 满足文献[14]中的式(3.194.3), 结合式(15)和式(14), 可以得到式(4)。

利用定义  $I_{SBS}^{cc} = \sum_{i \in \Phi_S} P_{SB} h_{jz} r_{jz}^{-\alpha_S}$  以及  $h_{jz} \sim \exp(1)$ ,  $I_{SBS}^{cc}$  的拉普拉斯变换  $\mathcal{L}_{I_{SBS}^{cc}}(s)$  可以有如下形式:

$$\mathcal{L}_{I_{SBS}^{cc}}(s) = E\{\exp(-s I_{SBS}^{cc})\} = \exp\left(-2\pi\lambda_S \int_0^\infty \left(1 - \frac{1}{1 + sP_{SB}r_{jz}^{-\alpha_S}}\right) r_{jz} dr_{jz}\right) \quad (16)$$

经过适当数学运算, 可以得到式(5)。利用类似方法可以得到式(6)。

定理1给出了任一宏蜂窝下行链路的安全概率, 清楚地呈现了网络参数对系统安全性能的影响。可以发现, 宏蜂窝下行链路的安全概率取决于  $I_{MBS}^{cc}$  和  $I_{UE}^{cc}$  以及  $I_{SBS}^{cc}$  的拉普拉斯变换。同时, 随着  $\lambda_S$  的增大, 系统的安全概率提高, 这是由于在式(1)中 SINR 随着  $\lambda_S$  的增大而减小。 $\lambda_{Ev}$  的增大也将降低系统安全概率  $P_{Sec}^c(T_c^e)$ , 这与实际网络模型相一致, 其原因是随着  $\lambda_{Ev}$  的增加, UE 间通信暴露给了更多的 Eve。此外, 随着 MBS 发送功率  $P_{MB}$  的增加, 安全概率  $P_{Sec}^c(T_c^e)$  降低, 系统安全概率  $P_{Sec}^c(T_c^e)$  还随着安全门限  $T_c^e$  的增大而增大。

## 2.2 小蜂窝上行链路安全概率分析

这部分主要研究小蜂窝下行链路安全概率。假设一 SBS 位于原点  $o$  与一个位于点  $y$  的 UE 通信。此时, 位于点  $v$  处的 Eve 从任一 UE 与其对应 SBS 通信过程中接收到的 SINR 可以表示为:

$$SINR_c^s(v) = \frac{P_{UE} h_{yv} r_{yv}^{-\alpha_S}}{I_{MBS}^{sc} + I_{SBS}^{sc} + I_{UE}^{sc}} \quad (17)$$

其中, 链路功率增益  $h_{yv} \sim \exp(1)$ , MBS 下行传输的干扰为  $I_{MBS}^{sc} = \sum_{l \in \Phi_M} \tilde{P}_{MB} h_{lv} r_{lv}^{-\alpha_M}$ ,  $h_{lv} \sim \Gamma(\min(N_m, K_m), 1)$ 。来自于 SBS 回程传输的干扰为  $I_{SBS}^{sc} = \sum_{i \in \Phi_S \setminus o} P_{SB} \cdot h_{jv} r_{jv}^{-\alpha_S}$ ,  $h_{jv} \sim \exp(1)$ 。来自于 UE 的干扰  $I_{UE}^{sc} =$

$$\sum_{i \in \tilde{\Phi}_{UE}} P_{UE} h_{iv} r_{iv}^{-\alpha_M}, h_{iv} \sim \exp(1)。$$

基于式(17), 考虑最恶意的 Eve 情形, 小蜂窝上行链路的安全概率可以定义为:

$$P_{Sec}^s(T_c^s) = \Pr\left\{\max_{v \in \Phi_{UE}} SINR_c^s(v) < T_c^s\right\} \quad (18)$$

其中,  $T_c^s$  为安全门限, 结合式(17)和式(18), 得到定理2。

**定理2** 在基于带内无线回程的全双工大规模 MIMO 双层 HetNets 中, 任一小蜂窝上行链路的安全概率可以表示为:

$$P_{Sec}^s(T_c^s) = \exp(-2\pi\lambda_{Ev} \int_0^\infty \mathcal{L}_{I_{MBS}^{sc}}(s_1) \mathcal{L}_{I_{SBS}^{sc}}(s_1) \mathcal{L}_{I_{UE}^{sc}}(s_1) r dr) \quad (19)$$

其中,  $s_1 = \frac{T_c^s}{P_{UE} r_{yv}^{-\alpha_S}}$ ,  $\mathcal{L}_{I_{MBS}^{sc}}(s_1)$ ,  $\mathcal{L}_{I_{SBS}^{sc}}(s_1)$  和  $\mathcal{L}_{I_{UE}^{sc}}(s_1)$  分别与式(4)~式(6)有相似形式。

证明: 将式(17)代入式(18), 得到:

$$P_{Sec}^s(T_c^s) = \Pr\left\{\max_{v \in \Phi_{UE}} \frac{P_{UE} h_{yv} r_{yv}^{-\alpha_S}}{I_{MBS}^{sc} + I_{SBS}^{sc} + I_{UE}^{sc}} < T_c^s\right\} = \exp\left(-2\pi\lambda_{Ev} \int_0^\infty \exp\left(-\frac{T_c^s}{P_{UE} r_{yv}^{-\alpha_S}} \cdot (I_{MBS}^{sc} + I_{SBS}^{sc} + I_{UE}^{sc})\right) r dr\right) \quad (20)$$

根据拉普拉斯变换的定义, 得到式(19)。

定理2表明, 利用回程干扰能够有效提高小蜂窝传输的安全性能。除了回程之外, 安全概率还随着强度  $\lambda_S$  和  $\lambda_{UE}$  的增加而增加。此外, 随着  $\lambda_M$  的增加, 小蜂窝传输的安全概率增大。

## 3 数值分析

本文对前面得到的安全概率进行数值分析。MBS 和 UE 之间的路径损失指数  $\alpha_M = 4$ , SBS 和 UE 之间路径损失指数  $\alpha_S = 3.5$ 。MBS、SBS 和 UE 的发送功率分别为  $P_{MB} = 10$  W,  $P_{SB} = 3$  W,  $P_{UE} = 1$  W。网络元素强度分别为  $\lambda_M = 0.4 \times 10^{-6}$ ,  $\lambda_S = 2 \times 10^{-6}$ ,  $\lambda_{UE} = 10 \times 10^{-6}$  以及  $\lambda_{Ev} = 6 \times 10^{-6}$ , 安全门限值  $T_c^e = T_c^s = 0.5$ 。

图2研究了在不同  $\lambda_S$  下 MBS-UE 下行和 UE-SBS 上行链路的安全概率。图2(a)给出了 MBS-UE 下行链路安全概率与  $\lambda_{Ev}$  的关系, 而图2(b)则给出了 UE-SBS 上行链路安全概率与  $\lambda_{Ev}$  的关系。观察图2可以发现, MBS-UE 和 UE-SBS 链路的安全概率随着  $\lambda_{Ev}$  的增加逐渐降低, 这是因为随着  $\lambda_{Ev}$  的增大, 通信链路暴露给更多的 Eve, 导致系统的安全性能降低。显然, 得到的结果与实际网络模型相一致。同时, 比较图2(a)和图2(b), 不难发现, 对于任一给定的  $\lambda_{Ev}$ , MBS-UE 比 UE-SBS 链路有更高的安全概率, 这也就是说, 在提出的 HetNets 模型中, 宏蜂窝比小蜂窝传输更为安全。对此有以下解释: 在

HetNets 中, MBS 配备了大规模 MIMO, 并采用了迫零预处理方案, 由于受到了巨大波束赋形增益的影响, MBS-UE 链路中任一 UE 接收到的 SINR 得到极大提高。同时, 图 2(a) 和图 2(b) 对带内全双工 (IB-FD) 和带外全双工 (OB-FD) 2 种模式做了比较, 结果表明, HetNets 在 IB-FD 模式下的性能要优于 OB-FD 模式, 这是由于 IB-FD 模式充分利用了回程干扰。此外, 随着  $\lambda_s$  增大, 系统安全性能提高, IB-FD 与 OB-FD 的安全概率间隙减小。

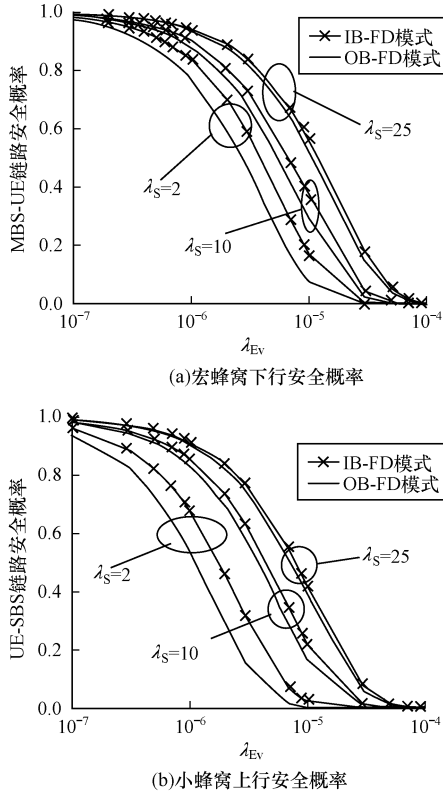


图2 宏蜂窝下行和小蜂窝上行链路的安全概率

为了进一步研究网络参数对系统安全性能的影响, 图 3(a) 研究了 MBS-UE 链路安全概率与  $\lambda_{UE}$  和  $\lambda_s$  的关系, 而图 3(b) 研究了  $\lambda_M$  和  $\lambda_s$  对 UE-SBS 链路的联合影响。观察可以发现 MBS-UE 和 UE-SBS 链路的安全性能随着  $\lambda_M$ 、 $\lambda_{UE}$  以及  $\lambda_s$  的增大而提高。图 4 研究了在不同安全限值  $T_e^c$  下, MBS-UE 链路安全概率与  $\lambda_M$  的关系。研究结果表明, 在  $T_e^c$  相对较小的情况下,  $\lambda_M$  取较小值时, 系统安全性能随着  $\lambda_M$  的增加而提高;  $\lambda_M$  取值较大时, 安全性能将逐渐降低。然而, 在  $T_e^c$  相对较大的情况下, 当  $\lambda_M$  较小时, 系统的安全概率趋近于一个常数; 仅当  $\lambda_M$  相对较大时, 随着  $\lambda_M$  的增大, 系统的安全概率急剧降低。对此有以下解释: 在  $T_e^c$  较小的情况下, 当  $\lambda_M$  相对较小时,  $\lambda_M$  的增大将会引发 Eve 接收信号干扰的增大, 从而引发 Eve 接收到 SINR 降低, 系统安全性能提高。然而, 当  $\lambda_M$  相对较大时, 分配给每一个 UE 的功率急剧减小, Eve 接收到的干扰信号功率急剧减小, 其接收到的

SINR 增大, 因此, 系统的安全性能随着  $\lambda_M$  的增加而降低。当  $T_e^c$  取值相对较大时, 根据式 (2) 不难发现当  $T_e^c$  较小时, 其对系统的安全概率有较大的影响。

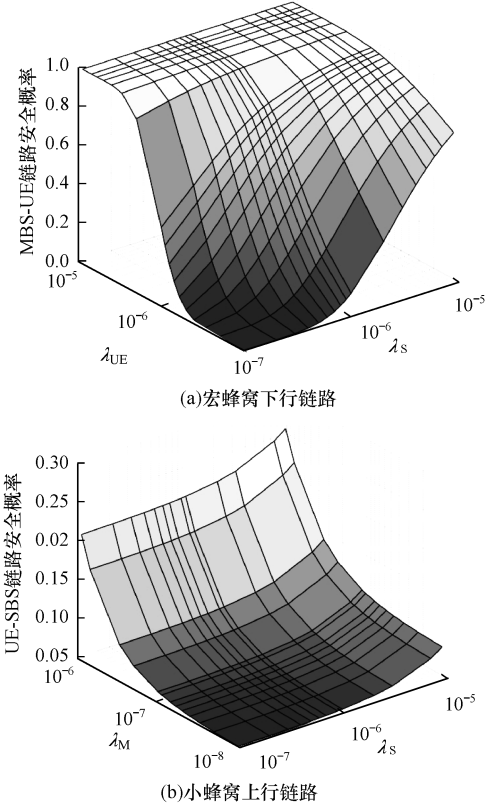


图3 宏蜂窝下行和小蜂窝上行安全概率与  $\lambda_s$  和  $\lambda_{UE}$  (或  $\lambda_M$ ) 的关系

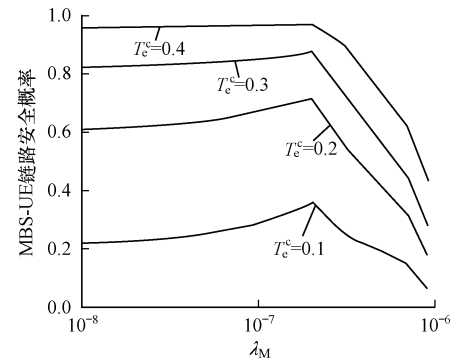


图4 宏蜂窝下行链路安全概率与不同安全门限的关系

## 4 结束语

本文提出一种带内全双工无线回程方案。在大规模 MIMO 双层异构网络中, 将回程信号作为宏蜂窝和小蜂窝通信链路的干扰信号, 分别研究宏蜂窝下行和小蜂窝上行链路的安全概率。实验结果表明, 利用带内全双工无线回程可以有效提高系统的安全性能, 且带内模式优于带外模式。今后将通过采用随机几何方法, 借助凸优化理论, 针对异构网络覆盖性能展开研究, 以达到网络覆盖性能的最优化。

## 参考文献

- [1] LU Lu, LI G, SWINDLEHURST A, et al. An overview of massive MIMO: benefits and challenges [J]. IEEE Journal of Selected Topics in Signal Processing, 2014, 8(5):742-758.
- [2] 邓鹏飞, 王 丹, 贾向东. 全双工大规模 MIMO AF 中继系统频谱与能量效率研究[J]. 计算机工程, 2016, 42(5):139-145.
- [3] 颜满刚, 贾向东, 周 猛. 基于大规模 MIMO 和 D2D 技术的混合网络能量效率研究[J]. 信号处理, 2017, 33(1):53-61.
- [4] JIA Xiangdong, DENG Pengfei, YANG Longxiang, et al. Spectrum and energy efficiencies for multiuser pairs massive MIMO systems with full-duplex amplify-and-forward relay[J]. IEEE Access, 2015, 3:1907-1918.
- [5] KAMEL M, HAMOUDA W, YOUSSEF A. Ultra-dense networks: a survey [J]. IEEE Communications Surveys & Tutorials, 2016, 18(4):2522-2545.
- [6] WANG Huiming, ZHENG Tongxing, YUAN Jinlong, et al. Physical layer security in heterogeneous cellular network [J]. IEEE Transactions on Communications, 2016, 64(3):1204-1219.
- [7] GE Xiaohu, CHENG Hui, GUIZANI M, et al. 5G wireless backhaul networks: challenges and research advances[J]. IEEE Network, 2014, 28(6):6-11.
- [8] LI Boyu, ZHU Dengkui, LIANG Ping. Small cell in-band wireless backhaul in massive MIMO systems: a cooperation of next-generation techniques [J]. IEEE Transactions on Wireless Communications, 2015, 14(12):7057-7066.
- [9] SHARMA A, GANTI R, MILLETH J. Joint backhaul-access analysis of full duplex self-backhauling heterogeneous networks [J]. IEEE Transactions on Wireless Communications, 2017, 16(3):1727-1740.
- [10] TABASSUM H, SAKR A, HOSSAIN E. Analysis of massive MIMO-enabled downlink wireless backhauling for full-duplex small cells [J]. IEEE Transactions on Communications, 2016, 64(6):2354-2369.
- [11] YANG H, GERACI G, QUEK T. Energy efficient design of MIMO heterogeneous networks with wireless backhaul [J]. IEEE Transactions on Wireless Communications, 2016, 15(7):4914-4927.
- [12] TABASSUM H, SAKR A, HOSSAIN E. Massive MIMO-enabled wireless backhauls for full-duplex small cells [C]//Proceedings of 2015 IEEE Global Communications Conference. Washington D. C., USA: IEEE Press, 2015:1-6.
- [13] CHIU S, STOYAN D, KENDALL W, et al. Stochastic geometry and its applications [M]. West Sussex, UK: John Wiley & Sons, 2013.
- [14] GRADSHTEYN I, RYZHIK I. Table of integrals, series and products [M]. Burlington, USA: Academic Press, 2007.
- [15] HAENGGI M, GANTI R. Interference in large wireless networks [M]. Notre Dame, USA: Now Publishers Inc., 2009.
- [8] EUM S, NAKAUCHI K, MURATA M, et al. CATT: potential based routing with content caching for ICN [C]//Proceedings of ACM Proceedings of the ICN Workshop on Information-centric Networking. New York, USA: ACM Press, 2012:49-54.
- [9] WANG Yu, XU Mingwei, FENG Zhen. Hop-based probabilistic caching for information-centric networks [C]//Proceedings of IEEE Global Communications Conference. Washington D. C., USA: IEEE Press, 2013:2102-2107.
- [10] PSARAS I, CHAI W K, PAVLOU G. Probabilistic in-network caching for information-centric networks [C]//Proceedings of the ICN Workshop on Information-centric Networking. New York, USA: ACM Press, 2012:55-60.
- [11] CHAI W K, HE Diliang, PSARAS I, et al. Cache “less for more” in information-centric networks [J]. Computer Communications, 2013, 36(7):758-770.
- [12] LI Zhe, SIMON G. Time-shifted TV in content centric networks: the case for cooperative in-network caching [C]//Proceedings of ICC'11. Washington D. C., USA: IEEE Press, 2011:1-6.
- [13] SOURLAS V, PSARAS I, SAINO L, et al. Efficient hash-routing and domain clustering techniques for information-centric networks [J]. Computer Networks, 2016, 103:67-83.
- [14] CHO K, LEE M, PARK K, et al. Wave: popularity-based and collaborative in-network caching for content-oriented networks [C]//Proceedings of IEEE Computer Communications Workshops. Washington D. C., USA: IEEE Press, 2012:316-321.
- [15] BERNARDINI C, SILVERSTON T, FESTOR O. MPC: IEEE Popularity-based caching strategy for content centric networks [C]//Proceedings of IEEE International Conference on Communications. Washington D. C., USA: IEEE Press, 2013:3619-3623.
- [16] HU Xiaoyan, GONG Jian, CHENG Guang, et al. Enhancing in-network caching by coupling cache placement, replacement and location [C]//Proceedings of IEEE International Conference on Communications. Washington D. C., USA: IEEE Press, 2015:5672-5678.
- [17] 葛国栋, 郭云飞, 刘彩霞等. 命名数据网络中基于局部请求相似性的协作缓存路由机制 [J]. 电子与信息学报, 2015, 37(2):435-442.
- [18] JIA Zixiao, ZHANG Peng, HUANG Jiwei, et al. Modeling hierarchical caches in content-centric networks [C]//Proceedings of IEEE International Conference on Computer Communications and Networks. Washington D. C., USA: IEEE Press, 2013:1-7.
- [19] FENG Bohao, ZHOU Huachun, ZHANG Hongke, et al. A popularity-based cache consistency mechanism for information-centric networking [C]//Proceedings of Global Communications Conference. Washington D. C., USA: IEEE Press, 2016:1-6.

编辑 刘 冰

编辑 刘 冰

(上接第 100 页)