

非理想信道下基于人工噪声的密集异构蜂窝网安全传输方案

许耘嘉^① 黄开枝^{*①} 李军^② 陈亚军^①

^①(国家数字交换系统工程技术研究中心 郑州 450002)

^②(中兴通讯股份有限公司 上海 200000)

摘要: 针对密集异构蜂窝网在非理想信道状态信息条件下的安全传输问题, 该文分析了人工噪声对通信的可靠性和安全性的影响, 在此基础上提出功率分配优化模型, 在不同信道估计精度条件下给出了最优的功率分配因子。首先, 考虑信道估计误差对合法信号传输以及人工噪声泄露的影响, 推导了典型通信链路的连通中断概率和安全中断概率。然后, 在安全性和可靠性约束条件下建立功率分配优化模型以最大化系统安全吞吐量, 并通过 K 维联合搜索算法得到每层网络的最优功率分配因子。最后, 仿真结果表明系统设置最优功率分配因子时, 人工噪声方案可提升约15%的安全吞吐量。

关键词: 密集异构蜂窝网; 物理层安全; 信道估计误差; 人工噪声

中图分类号: TN929.5

文献标识码: A

文章编号: 1009-5896(2018)10-2323-08

DOI: [10.11999/JEIT180003](https://doi.org/10.11999/JEIT180003)

Artificial Noise Aided Secure Transmission in Dense Heterogeneous Cellular Networks with Imperfect Channel State Information

XU Yunjia^① HUANG Kaizhi^① LI Jun^② CHEN Yajun^①

^①(National Digital Switching System Engineering & Technological Research Center, Zhengzhou 450002, China)

^②(Zhongxing Telecommunication Equipment Corporation, Shanghai 200000, China)

Abstract: To ensure secure transmission in dense heterogeneous cellular networks with imperfect Channel State Information (CSI), the influence of Artificial Noise (AN) on secure and reliable communication is analyzed, and a power split factor optimization model is presented to obtain the optimal value under different channel estimation accuracy. First, the connection outage probability and secrecy outage probability are deduced by considering the influence of channel estimation error on signal transmission and AN leakage. Then, a power split factor optimization model is presented, which maximizes the secrecy throughput subject to the security and reliability requirements. A K -dimensional search method is employed to solve the optimal power split factor of each tier. Finally, the numerical results verify that the AN transmission scheme with optimal power split factor can increase secrecy throughput by about 15%.

Key words: Dense heterogeneous cellular networks; Physical layer security; Channel estimation error; Artificial Noise (AN)

1 引言

密集异构蜂窝网通过在宏蜂窝小区中部署小型基站来提高系统的通信容量和覆盖范围^[1], 但由于无线通信的开放性使其面临信号在传输过程中被非

法窃听的问题。近年来, 物理层安全技术利用合法信道和窃听信道天然的信道差异来实现安全传输^[2], 成为解决密集异构蜂窝网安全通信问题的重要手段之一^[3]。其中, 研究广泛的人工噪声技术通过在合法信道的零空间发射噪声干扰, 在不影响合法信道的前提下降低窃听信道质量。文献^[4]首次将人工噪声方案用于保障安全通信。考虑节点随机分布的通信场景, 文献^[5]在Ad hoc网络中应用人工噪声来实现安全传输。在此基础上, 文献^[6]设计了

收稿日期: 2018-01-02; 改回日期: 2018-05-23; 网络出版: 2018-07-30

*通信作者: 黄开枝 huangkaizhi@tsinghua.org.cn

基金项目: 国家自然科学基金(61379006, 61401510, 61521003)

Foundation Items: The National Natural Science Foundation of China (61379006, 61401510, 61521003)

基于安全保护域的人工噪声方案,通过设置安全通信范围并设计人工噪声来实现安全通信。在多小区协作场景中,文献[7,8]通过多节点协作干扰制造人工噪声来实现安全传输。

上述文献均基于理想的信道假设,即发射端可得到准确的信道状态信息(Channel State Information, CSI)。实际中,由于信道估计误差等因素的影响,CSI难以准确地获取,因此考虑非理想CSI下的安全传输更符合实际。针对信道估计误差的问题,文献[9,10]分别针对窃听者随机分布以及干扰节点随机分布的系统,分析人工噪声方案的安全性能,为基于人工噪声的安全传输方案设计提供理论指导,但该分析仅针对干扰节点和窃听节点随机分布的系统,缺乏对所有通信节点均随机分布的考虑。点对点通信场景中,文献[11,12]针对中继协作系统,设计了人工噪声辅助波束成形的安全传输方案。文献[13]提出将人工噪声用于大规模MIMO (Multiple-Input Multiple-Output)系统,从而保证非理想CSI条件下的安全传输。但由于文献[11-13]仅考虑节点固定的通信场景,其算法扩展性受到密集异构蜂窝网拓扑结构的限制,因此需要针对节点随机动态部署的网络结构设计非理想CSI条件下的安全传输方案。

针对上述问题,本文针对存在信道估计误差的系统,分析了非理想CSI条件下人工噪声对安全可靠通信的影响,在此基础上给出功率分配优化模型,使系统在不同信道估计精度条件下得到最优的功率分配因子。首先,考虑信道估计误差对合法信号传输造成的波束偏移以及人工噪声泄露,推导了典型通信链路的连通中断概率和安全中断概率,在此基础上分析了功率分配因子对系统可靠性及安全性的影响。为优化系统性能,在安全性和可靠性约束条件下提出了功率分配优化模型以最大化系统安全吞吐量。通过 K 维联合搜索算法优化出每层网络的最优功率分配因子。仿真分析得出结论:应用人工噪声方案并设置最优功率分配因子时系统能提升约15%的安全吞吐量。

2 系统模型

在 K 层密集异构蜂窝网中,随机分布的基站、用户和窃听者均可建模为均匀泊松点过程(Homogeneous Point Process Positions, HPPPs) Φ_i , Φ_u 和 Φ_e ,其分布密度可分别表示为 λ_i , λ_u 和 λ_e 。不同层基站设置不同的发射功率、天线数量以及空间分布。以第 i 层第 m 个基站 B_{im} 为例,其发射功率设置为 P_i ,天线数量为 N_i 。用户和窃听者均配置单天线。同时考虑大尺度和小尺度衰落,其中大尺度衰落系数为 α , $\alpha > 2$ 。小尺度衰落为准静态瑞利衰落模型,信道增益服从独立同分布的零均值指数分布。

开放网络中用户可接入任意一层基站,但由于密集异构蜂窝网节点密集部署,用户接入效率受到影响。因此利用平均接收功率作为用户接入基站的衡量标准,假设接入门限分别为 τ_i ,仅当用户接收功率高于预设门限值 τ_i 时才可接入相应的发射基站,可表示为

$$P_i |x_i|^{-\alpha} > \tau_i \quad (1)$$

由于接入门限的设置是依据大尺度衰落确定的,因此可认为当用户距离基站的距离 x_i 小于备选半径 D_i 时可接入基站,其中 $D_i = (P_i/\tau_i)^{1/\alpha}$ 。也就是说,用户可接入的基站必须位于一个圆形区域 $(0, D_i]$ 内。在此范围内,合法用户接入接收功率最大的基站,则用户接入基站的连接概率 \mathcal{A}_i 以及用户到服务基站距离 X_i 的概率密度函数 $f_{X_i}(x)$ 可分别表示为^[14]

$$\begin{aligned} \mathcal{A}_i &= P\{P_{ri} > P_{rj} | x_i, \forall j \in K \setminus i\} \\ &= \lambda_i (P_i)^{2/\alpha} \left(1 - \exp \left(-\frac{\sum_{j \in K} \lambda_j (P_j)^{2/\alpha}}{-\pi \tau_i} \right) \right) \\ &\quad / \sum_{j=1}^K \lambda_j (P_j)^{2/\alpha} \end{aligned} \quad (2)$$

$$f_{X_i}(x) = 2\pi \lambda_i / \mathcal{A}_i \cdot x \exp \left\{ -\pi \sum_{j \in K} \lambda_j (P_j / P_i)^{2/\alpha} x^2 \right\} \quad (3)$$

在信道估计阶段,基站发射导频信号,用户通过接收到的导频信号对当前信道进行估计,不考虑反馈时延和量化误差,用户将信道估计值通过理想的回程链路反馈给基站。在信号传输阶段,基站通过反馈得到的当前CSI进行预编码,然后进行信号传输。由于密集异构蜂窝网节点随机密集部署,用户在估计信道时可能收到来自多个小区的导频信号引起信道估计误差。以 \mathbf{h}_{ui} 来表示合法信道的信道向量, $\tilde{\mathbf{h}}_{ui}$ 表示 \mathbf{h}_{ui} 的估计值,则估计信道与实际信道之间的关系可表示为^[10]

$$\mathbf{h}_{ui} = \tilde{\mathbf{h}}_{ui} + \mathbf{o}_i \quad (4)$$

其中, \mathbf{o}_i 表示信道估计误差, $\mathbf{o}_i \sim \mathcal{CN}(\mathbf{0}_{N_i}^T, (1-\rho_i)\mathbf{I}_{N_i})$ 。由于 $1-\rho_i$ 是估计误差的方差, ρ_i ($0 \leq \rho_i \leq 1$)越大信道估计误差越小,由此可将 ρ_i 看作信道估计精度, ρ_i 越大信道估计越准确。

3 性能分析

为防止窃听,基站通过在合法用户零空间发射人工噪声的方式,降低窃听信道容量同时不影响合法用户的通信。假设典型用户接入基站 B_{im} ,基站以功率 $\kappa_i P_i$ 发射信号,而以功率 $(1-\kappa_i) P_i$ 发射人工

噪声。由于基站依据估计CSI设计预编码矩阵，应用最大比合并的编码方式，编码矩阵可表示为 $\tilde{\mathbf{w}}_i = \tilde{\mathbf{h}}_{\text{ui}}^H / \|\tilde{\mathbf{h}}_{\text{ui}}\|$ 。此时用户的接收信号可表示为

$$y_{\text{ui}} = \sqrt{\kappa_i P_i} \mathbf{h}_{\text{ui}} \tilde{\mathbf{w}}_i s_{\text{ui}} x_i^{-\alpha/2} + \sqrt{(1 - \kappa_i) P_i / (N_i - 1)} \mathbf{h}_{\text{ui}} \tilde{\mathbf{U}}_i s_{\text{ui}} x_i^{-\alpha/2} + I_{\text{ui}} + n_{\text{ui}} \quad (5)$$

其中， s_{xi} 和 s_{ui} 分别表示私密信号和人工噪声。 $\tilde{\mathbf{U}}_i$ 表示人工噪声的方向向量，由于其方向位于估计信道零空间，因此 $\tilde{\mathbf{h}}_{\text{ui}}^H \tilde{\mathbf{U}}_i = \mathbf{0}$ 。 I_{ui} 表示合法用户接收到来自相邻小区的干扰， n_{ui} 是用户收到的零均值加性高斯白噪声。

由式(5)可知用户接收来自第*i*层基站的SINR γ_U^i 可表示为

$$\gamma_U^i = \left(\kappa_i P_i \|\tilde{\mathbf{h}}_{\text{ui}} \tilde{\mathbf{w}}_i\|^2 |X_i|^{-\alpha} \right) / \left(\kappa_i P_i \|\mathbf{o}_i \tilde{\mathbf{w}}_i\|^2 |X_i|^{-\alpha} + (1 - \kappa_i) P_i / (N_i - 1) \cdot \|\mathbf{o}_i \tilde{\mathbf{U}}_i\|^2 |X_i|^{-\alpha} + I_{\text{ui}} + \sigma_{\text{ui}}^2 \right) \quad (6)$$

其中， $i \in [1, K]$ ， $\|\tilde{\mathbf{h}}_{\text{ui}} \tilde{\mathbf{w}}_i\|^2 \sim \Gamma(N_i, \rho_i)$ 。 $\kappa_i P_i \cdot \|\mathbf{o}_i \tilde{\mathbf{w}}_i\|^2 |X_i|^{-\alpha}$ 和 $(1 - \kappa_i) P_i / (N_i - 1) \cdot \|\mathbf{o}_i \tilde{\mathbf{U}}_i\|^2 |X_i|^{-\alpha}$ 分别表示信道估计误差导致的信号偏移以及人工噪声泄露，其中 $\|\mathbf{o}_i \tilde{\mathbf{w}}_i\|^2 \sim \exp(1 - \rho_i)$ ， $\|\mathbf{o}_i \tilde{\mathbf{U}}_i\|^2 \sim \Gamma(N_i - 1, 1 - \rho)$ 。 $I_{\text{ui}} = \sum_{j=1}^K \sum_{j \in \Phi_j \setminus B_{\text{im}}} \left(\kappa_j P_j \|\mathbf{h}_{\text{uj}} \tilde{\mathbf{w}}_j\|^2 \cdot |Z_i|^{-\alpha} + (1 - \kappa_j) P_j / (N_j - 1) \cdot \|\mathbf{h}_{\text{uj}} \tilde{\mathbf{U}}_j\|^2 |Z_i|^{-\alpha} \right)$ 表示用户接收到来自小区间和小区内的干扰，其中 $\kappa_j P_j \|\mathbf{h}_{\text{uj}} \tilde{\mathbf{w}}_j\|^2 |Z_i|^{-\alpha}$ 表示来自干扰基站的信号， $(1 - \kappa_j) P_j / (N_j - 1) \cdot \|\mathbf{h}_{\text{uj}} \tilde{\mathbf{U}}_j\|^2 |Z_i|^{-\alpha}$ 表示来自干扰基站的人工噪声， \mathbf{h}_{uj} 是干扰基站到典型用户的信道向量， Z_i 为典型用户到干扰基站的距离。 σ_{ui}^2 表示用户接收到的高斯白噪声。

假设窃听者可准确估计信道。由于窃听者随机分布，考虑最危险(即窃听SINR最大)的情况，其接收SINR γ_E^i 可表示为

$$\gamma_E^i = \max_{e \in \Phi_e} \left\{ \left(\kappa_i P_i \|\mathbf{h}_{\text{ei}} \tilde{\mathbf{w}}_i\|^2 |Y_i|^{-\alpha} \right) / \left[(1 - \kappa_i) P_i / (N_i - 1) \cdot \|\mathbf{o}_i \tilde{\mathbf{U}}_i\|^2 |X_i|^{-\alpha} \cdot \|\mathbf{h}_{\text{ei}} \tilde{\mathbf{U}}_i\|^2 |Y_i|^{-\alpha} + I_{\text{ei}} + \sigma_{\text{ei}}^2 \right] \right\} \quad (7)$$

其中， $i \in [1, K]$ ， \mathbf{h}_{ei} 表示窃听信道向量， $\|\mathbf{h}_{\text{ei}} \tilde{\mathbf{w}}_i\|^2 \sim \exp(1)$ ， Y_i 表示服务基站到窃听者的距离。 $(1 - \kappa_i) P_i / (N_i - 1) \cdot \|\mathbf{h}_{\text{ei}} \tilde{\mathbf{U}}_i\|^2 |Y_i|^{-\alpha}$ 是窃听者接收到的人工噪声， $\|\mathbf{h}_{\text{ei}} \tilde{\mathbf{U}}_i\|^2 \sim \Gamma(N_i - 1, 1)$ 。 $I_{\text{ei}} = \sum_{j=1}^K \sum_{j \in \Phi_j \setminus B_{\text{im}}} \left(\kappa_j P_j \|\mathbf{h}_{\text{ej}} \tilde{\mathbf{w}}_j\|^2 |M_i|^{-\alpha} + (1 - \kappa_j) P_j / (N_j - 1) \cdot \|\mathbf{h}_{\text{ej}} \tilde{\mathbf{U}}_j\|^2 |M_i|^{-\alpha} \right)$ 表示窃听者接收到来自小区内和小区间的复杂干扰，其中 $\kappa_j P_j \|\mathbf{h}_{\text{ej}} \tilde{\mathbf{w}}_j\|^2 \cdot |M_i|^{-\alpha}$ 和 $(1 - \kappa_j) P_j / (N_j - 1) \cdot \|\mathbf{h}_{\text{ej}} \tilde{\mathbf{U}}_j\|^2 |M_i|^{-\alpha}$ 表示来自干扰基站的信号和人工噪声干扰，其中 \mathbf{h}_{ej} 表示干扰基站到窃听者的信道向量， M_i 表示干扰基站到窃听者的距离。 σ_{ei}^2 表示窃听者接收到的高斯白噪声。

由式(6)及式(7)可知信道估计误差引起波束偏移以及人工噪声泄露对用户及窃听者的接收SINR产生影响，同时由于密集异构蜂窝网通信节点随机密集部署的特点，导致难以直接分析功率分配因子以及信道估计精度对系统安全可靠性能的影响。因此本节通过推导连通中断概率和安全中断概率对系统的可靠性和安全性进行研究，并在此基础上给出可提升系统性能优化模型。

3.1 可靠性能分析

连通中断概率(Connection Outage Probability, COP)是衡量通信可靠性的重要指标。对于给定的连通中断阈值 R_b ，第*i*层基站的COP可表示为

$$P_{\text{co}}^i = \mathbb{P}(\log_2(1 + \gamma_U^i) \leq R_b) = \mathbb{P}\left(\|\tilde{\mathbf{h}}_{\text{ui}} \tilde{\mathbf{w}}_i\|^2 \leq \left(\mathbb{E}\left(\kappa_i P_i \|\mathbf{o}_i \tilde{\mathbf{w}}_i\|^2 + \frac{(1 - \kappa_i) P_i}{N_i - 1} \cdot \|\mathbf{o}_i \tilde{\mathbf{U}}_i\|^2\right) + (I_{\text{ui}} + \sigma_{\text{ui}}^2) x^\alpha\right) \frac{2^{R_b} - 1}{\kappa_i P_i}\right) \quad (8)$$

记 $\Theta_i = \left(\mathbb{E}\left(\kappa_i P_i \|\mathbf{o}_i \tilde{\mathbf{w}}_i\|^2 + \frac{(1 - \kappa_i) P_i}{N_i - 1} \cdot \|\mathbf{o}_i \tilde{\mathbf{U}}_i\|^2\right) + (I_{\text{ui}} + \sigma_{\text{ui}}^2) x^\alpha\right) \frac{2^{R_b} - 1}{\kappa_i P_i \rho_i}$ ， $\phi = 2^{R_b} - 1$ 。首先对 Θ_i 进行求解，由于 $\|\mathbf{o}_i \tilde{\mathbf{w}}_i\|^2 \sim \exp(1 - \rho_i)$ ， $\|\mathbf{o}_i \tilde{\mathbf{U}}_i\|^2 \sim \text{Gamma}(N_i - 1, 1 - \rho_i)$ ，可将 Θ_i 表示为 $\Theta_i = \left(P_i(1 - \rho_i) + (I_{\text{ui}} + \sigma_{\text{ui}}^2) x^\alpha\right) \frac{\phi}{\kappa_i P_i \rho_i}$ ，其均值可表示为 $\mathbb{E}(\Theta_i) = \frac{(1 - \rho_i) \phi}{\kappa_i \rho_i} + [\mathbb{E}(I_{\text{ui}}) + \sigma_{\text{ui}}^2] \frac{\phi x_i^\alpha}{\kappa_i P_i \rho_i}$ ，其中，

$$\begin{aligned} \mathbb{E}(I_{\text{ui}}) &= \sum_{j=1}^K \exp\left\{-2\pi\lambda_j \int_{D_j} \left[1 - \mathbb{E}\left(\kappa_j P_j \|\mathbf{h}_{\text{uij}} \tilde{\mathbf{w}}_j\|^2\right.\right.\right. \\ &\quad \left.\left.\left. \cdot z^{-\alpha} + \frac{(1-\kappa_j)P_j}{N_j-1} \|\mathbf{h}_{\text{uij}} \tilde{\mathbf{U}}_j\|^2 z^{-\alpha}\right)\right] z dz\right\} \\ &= \sum_{j=1}^K \left(2\pi\lambda_j P_j \rho_j (D_j)^{2-\alpha} / (\alpha-2)\right) \quad (9) \end{aligned}$$

将式(9)代入 $\mathbb{E}(\Theta_i)$ 可得

$$\begin{aligned} \mathbb{E}(\Theta_i) &= \frac{(1-\rho_i)\phi}{\kappa_i \rho_i} + \left(\sum_{j=1}^K \left(\frac{2\pi\lambda_j P_j \rho_j (D_j)^{2-\alpha}}{\alpha-2}\right)\right. \\ &\quad \left.+ \sigma_{\text{ui}}^2\right) \frac{\phi x^\alpha}{\kappa_i P_i \rho_i} \quad (10) \end{aligned}$$

定理 1 用户接入第*i*层基站后的COP可表示为

$$\begin{aligned} P_{\text{co}}^i &\stackrel{(a)}{=} 1 - \int_0^{D_i} \sum_{k=0}^{N_i-1} \mathbb{E}\left([\mathbb{E}(\Theta_i)]^k \exp\left(-\Theta_i/\rho_i\right)\right. \\ &\quad \left./\left(k! \rho_i^k\right)\right) f_{X_i}(x) dx \\ &= 1 - \int_0^{D_i} \sum_{k=0}^{N_i-1} [\mathbb{E}(\Theta_i)]^k \exp\left[-\left(P_i(1-\rho_i)\right.\right. \\ &\quad \left.\left.+ \sigma_{\text{ui}}^2 x^\alpha\right)\phi / \left(\kappa_i P_i \rho_i^2\right)\right] \mathcal{L}_{I_{\text{ui}}}(\varepsilon_i) / \left(k! \rho_i^k\right) \\ &\quad \cdot f_{X_i}(x) dx \quad (11) \end{aligned}$$

式(11)中(a)由Gamma分布的积累分布函数可得。 $\varepsilon_i = \phi x^\alpha / (\kappa_i P_i \rho_i^2)$, $\mathcal{L}_{I_{\text{ui}}}(\varepsilon_i)$ 表示干扰 I_{uij} 的拉普拉斯变换。定义 $\nu_i = P_j^I \left(\|\mathbf{h}_{\text{uij}} \tilde{\mathbf{w}}_j\|^2 + \varsigma_j \|\mathbf{h}_{\text{uij}} \tilde{\mathbf{U}}_j\|^2\right)$, 表示接入第*i*层BS的用户接收到的来自干扰基站的包括干扰信号和人工噪声的总干扰功率, 其中 $P_j^I = \kappa_j P_j$, $\varsigma_j = (1-\kappa_j) / [(N_j-1)\kappa_j]$ 。 ν_i 的概率分布函数可表示为^[5]

$$f_{\nu_i}(\iota) = \begin{cases} \frac{\iota^{N_j-1}}{(N_j-1)! (P_j^I \rho_j)^{N_j}} e^{-\frac{\iota}{\rho_j P_j^I}}, & \varsigma_j = 1 \\ \frac{(1-t\varsigma_j)^{1-N_j}}{(N_j-2)! \rho_j P_j^I} e^{-\frac{\iota}{\rho_j P_j^I}} \\ \quad \cdot \gamma\left(N_j-1, \frac{(1-\varsigma_j)\iota}{\varsigma_j \rho_j P_j^I}\right), & \text{其他} \end{cases} \quad (12)$$

定义 $\chi_j = \int_0^\infty e^{-\varepsilon_j \iota x^{-\alpha}} f_{\nu_i}(\iota) d\iota$, 则 $\mathcal{L}_{I_{\text{ui}}}(\varepsilon_i)$ 可表示为

$$\begin{aligned} \mathcal{L}_{I_{\text{ui}}}(\varepsilon_i) &= \mathbb{E}_{I_{\text{ui}}} \left\{ \exp\left(-\varepsilon_i \sum_{j=1}^K \sum_{j \in \Phi_j \setminus B_{\text{im}}} \nu_i \|x\|^{-\alpha}\right)\right\} \\ &= \prod_{j=1}^K \mathbb{E}_{\Phi_j} \left\{ \prod_{j \in \Phi_j \setminus B_{\text{im}}} \mathbb{E}_{\nu_i} \left\{ \exp(-\varepsilon_i \nu_i \|x\|^{-\alpha}) \right\} \right\} \\ &\stackrel{(a)}{=} \prod_{j=1}^K \exp\left(-2\pi\lambda_j \int_0^\infty (1-\chi_j) x dx\right) \quad (13) \end{aligned}$$

式中, (a)是由PPP的形成函数(Probability Generating Functional Lemma, PGFL)得到, χ_j 可表示为^[15]

$$\chi_j = \begin{cases} (1 + \varphi_j x^{-\alpha})^{-N_j}, & \varsigma_j = 1 \\ \frac{(1-\varsigma_j)^{1-N_j}}{1 + \varphi_j x^{-\alpha}} - \sum_{m=0}^{N_j-2} \frac{\varsigma_j (1-\varsigma_j)^{m+1-N_j}}{(1 + \varsigma_j \varphi_j x^{-\alpha})^{m+1}}, & \text{其他} \end{cases} \quad (14)$$

其中, $\varphi_j = \kappa_j P_j \rho_j \varepsilon_i = \phi x^\alpha / \rho_i$ 。

注意到功率分配因子和信道估计精度对COP均产生影响。由式(11)可知, COP与信道估计精度是负相关的, 这是由于信道估计精度越大, 估计误差越小, 此时系统更能实现可靠传输。换言之, 准确的信道估计能够降低COP, 是实现可靠通信的重要前提。

此外, COP随功率分配因子的增加而减小。由于功率分配因子反映了信号发射功率和人工噪声功率的关系, 功率分配因子越大意味着信号传输功率越大而人工噪声功率越小。一方面由于更大的信号功率本身对通信链路的可靠性提供有效增益; 另一方面, 由于信道估计误差的存在, 预设发射在合法信道零空间的人工噪声可能泄露到合法信道上, 此时增大功率分配因子, 人工噪声发射功率减小, 则泄露到合法信道的噪声功率减小, 通信链路的可靠性得到保证。

3.2 安全性能分析

安全中断概率(Security Outage Probability, SOP)是衡量通信安全性的重要指标。对于给定的安全中断阈值 R_s , 第*i*层基站的安全中断概率可表示为

$$P_{\text{so}}^i = \mathbb{P}(\log_2(1 + \gamma_E^i) > R_u^i - R_s) \quad (15)$$

为求解 P_{so}^i 的表达式, 将式(15)变形为 $P_{\text{so}}^i = 1 - \mathbb{F}_{\gamma_E}(2^{(R_u^i - R_s)} - 1)$, 其中 $\mathbb{F}_{\gamma_E}(\cdot)$ 表示窃听SINR的分布函数。 $R_U^i = \mathbb{E}\{\log_2(1 + \gamma_U^i)\}$ 表示合法用户的平均可达速率。由于难以得出 R_U^i 的精确表达式, 因此考虑计算用户平均可达速率的下界, 记为 $R_U^{L_i}$ 。依据Jensen不等式, 有

$$R_U^{L_i} = \log_2 \left(1 + \left[\mathbb{E} \left(\gamma_U^{i-1} \right) \right]^{-1} \right) \leq \mathbb{E} \{ \log_2 (1 + \gamma_U^i) \} \quad (16)$$

定理 2 信道估计误差条件下用户平均可达速率的下界为

$$\begin{aligned} R_U^{L_i} &= \log_2 \left(1 + \left[\mathbb{E} \left(\left(\kappa_i P_i \| \mathbf{o}_i \tilde{\mathbf{w}}_i \|^2 + \frac{(1-\kappa_i) P_i}{N_i - 1} \| \mathbf{o}_i \tilde{\mathbf{U}}_i \|^2 \right. \right. \right. \right. \\ &\quad \left. \left. \left. + (I_{\text{ui}} + \sigma_{\text{ui}}^2) |X_i|^\alpha / \left(\kappa_i P_i \| \tilde{\mathbf{h}}_{\text{ui}} \tilde{\mathbf{w}}_i \|^2 \right) \right) \right]^{-1} \right) \\ &= \log_2 \left(1 + \kappa_i P_i \rho_i N_i \left(P_i (1 - \rho_i) + \sum_{j=1}^K \left(2\pi \lambda_j \right. \right. \right. \\ &\quad \left. \left. \left. \cdot P_j \rho_j (D_j)^{2-\alpha} / (\alpha - 2) + \sigma_{\text{ui}}^2 \right) \right)^{-1} \right) \quad (17) \end{aligned}$$

将式(17)代入式(15)可得第*i*层的SOP。记 $\beta_i = 2^{R_i - R_s} - 1$, $\psi_i = \beta_i y^\alpha / P_i$, SOP的表达式可由定理3给出。

定理 3 用户接入第*i*层基站后的SOP可表示为

$$\begin{aligned} P_{\text{so}}^i &= 1 - \exp \left(-2\pi \lambda_e \exp \left(-\frac{(1-\kappa_i) \beta_i}{\kappa_i^2 P_i} \right) \right. \\ &\quad \left. \cdot \int_{D_i}^{\infty} \mathbb{E} \left[\exp \left(-\frac{I_{\text{ei}} + \sigma_{\text{ei}}^2}{\kappa_i P_i y^\alpha} \beta_i \right) \right] y dy \right) \\ &= 1 - \exp \left(-2\pi \lambda_e \exp \left(-\frac{(1-\kappa_i) \beta_i}{\kappa_i^2 P_i} \right) \right. \\ &\quad \left. \cdot \int_{D_i}^{\infty} \prod_{l=1}^K \mathcal{L}_{I_{\text{ei}}}(\psi_i) \exp \left(-\frac{\sigma_{\text{ei}}^2 \beta_i}{\kappa_i P_i y^\alpha} \right) y dy \right) \quad (18) \end{aligned}$$

与 I_{ui} 类似, I_{ei} 的拉普拉斯变换可表示为

$$L_{I_{\text{ei}}}(\psi_i) = \prod_{j=1}^K \exp \left(-2\pi \lambda_j \int_0^{\infty} (1 - \delta_j) x dx \right) \quad (19)$$

其中, δ_j 可表示为

$$\delta_j = \begin{cases} (1 + \vartheta_j x^{-\alpha})^{-N_j}, & s_j = 1 \\ \frac{(1 - s_i)^{1-N_j}}{1 + \vartheta_j x^{-\alpha}} - \sum_{m=0}^{N_j-2} \frac{s_i (1 - s_i)^{m+1-N_j}}{(1 + s_i \vartheta_j x^{-\alpha})^{m+1}}, & \text{其他} \end{cases} \quad (20)$$

其中, $\vartheta_j = \kappa_j P_j \psi_i$ 。

由式(18)可知, 功率分配因子和信道估计精度对SOP均产生影响。可以发现SOP与信道估计精度是负相关的, 这是由于信道估计精度越大, 人工噪声由于信道估计误差引起的泄露将减小, 合法信道容量得到提高, 而窃听信道容量维持不变, 因此SOP减小。

功率分配因子反映了信号功率和人工噪声功率的分配情况。由式(18)可知SOP与功率分配因子成正相关的关系。当功率分配因子增大时, 会有更多的发射功率分配给信号, 而更少的发射功率分配给人工噪声, 由此窃听信道的干扰变少, 窃听容量变大。因此增加功率分配因子将导致系统的安全性能下降, SOP增大。

3.3 优化分析

由上述分析可知在增大功率分配因子时存在一个SOP和COP的折中, 为综合考虑系统的可靠性和安全性, 需合理设置功率分配因子。以安全吞吐量(Secrecy throughput)来衡量系统的可靠性和安全性, 定义为保密信息安全可靠地从发射端传输到接收端的速率^[6]。第*i*层的安全吞吐量可表示为

$$\xi_i = \lambda_i (1 - P_{\text{co}}^i) (1 - P_{\text{so}}^i) R_s \quad (21)$$

各层功率分配因子通过影响SOP和COP对系统的安全吞吐量产生影响。图1给出了安全吞吐量和功率分配因子的关系。

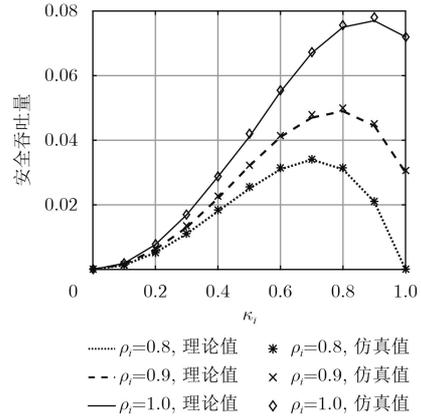


图1 安全吞吐量和功率分配因子的关系

可以发现, 安全吞吐量随着功率分配因子的增大而先增加后减小, 且存在一个最佳的功率分配因子使得系统的安全吞吐量达到最大值。因此, 为减小信道估计误差的影响, 在非理想情况下实现安全可靠传输, 设置合适的功率分配因子十分重要。为提升系统的安全可靠性能, 提出了功率分配因子优化模型, 在安全性和可靠性约束条件下最大化系统的安全吞吐量。由于用户对通信的安全可靠性需求大致相同, 因此假设各层的安全性和可靠性约束条件分别为 ∂_1 和 ∂_2 , 则上述优化问题可表示为

$$\left. \begin{aligned} \max_{\kappa_1, \dots, \kappa_K} \xi &= \sum_{i=1}^K \mathcal{A}_i \cdot \xi_i \\ \text{s.t.} \quad \text{C1: } &P_{\text{so}}^i \leq \partial_1, P_{\text{co}}^i \leq \partial_2, i = 1, 2, \dots, K \\ \text{C2: } &\partial_1 \in [0, 1], \partial_2 \in [0, 1] \\ \text{C3: } &\kappa_i \in [0, 1], i = 1, 2, \dots, K \end{aligned} \right\} \quad (22)$$

由于式(22)的优化问题难以直接求解,因此考虑通过搜索算法来求解最优功率分配因子 $\kappa_1^*, \kappa_2^*, \dots, \kappa_K^*$ 的数值解。依据安全可靠约束条件C1确定出算法的可行域 $(\kappa_1, \kappa_2, \dots, \kappa_K)$, 则最优值 $\kappa_1^*, \kappa_2^*, \dots, \kappa_K^*$ 是在可行域集合 $(\kappa_1, \kappa_2, \dots, \kappa_K)$ 内的, 可表示为

$$(\kappa_1^*, \kappa_2^*, \dots, \kappa_K^*) = \max_{\kappa_1, \kappa_2, \dots, \kappa_K} \xi(\kappa_1, \kappa_2, \dots, \kappa_K) \quad (23)$$

基于以上分析, 本文提出一种 K 维搜索算法来搜索 K 层网络的功率分配因子的最优数值解。算法如表1所示, 其中 $\kappa_1, \kappa_2, \dots, \kappa_K$ 的步长分别设置为 $\Delta\kappa_1, \Delta\kappa_2, \dots, \Delta\kappa_K$ 。

表1 功率分配因子最优值搜索算法

- (1) 输入: $K, \rho_i, \alpha_i, P_i, \lambda_i, \lambda_e, R_b, R_s, \partial_1, \partial_2, \Delta\kappa_1, \Delta\kappa_2, \dots, \Delta\kappa_K$;
- (2) 初始化: $C_1 = 1/\Delta\kappa_1, \dots, C_K = 1/\Delta\kappa_K, \xi^\circ = 0$;
- (3) for $c_i = 1 : C_i$ do
- (4) 计算 \mathcal{A}_i, P_{co}^i 和 P_{so}^i , 在约束条件 $P_{co}^i \leq \partial_1, P_{so}^i \leq \partial_2$ 下更新集合 $(\hat{\kappa}_1, \hat{\kappa}_2, \dots, \hat{\kappa}_K)$;
- (5) end for
- (6) 设置 Ω 为集合 $(\hat{\kappa}_1, \hat{\kappa}_2, \dots, \hat{\kappa}_K)$ 中的元素数量,
 $\Omega = \text{Card}(\hat{\kappa}_1), \text{Card}(\hat{\kappa}_2), \dots, \text{Card}(\hat{\kappa}_K)$
- (7) for $\omega = 1 : \Omega$ do
- (8) 将集合 $(\hat{\kappa}_1, \hat{\kappa}_2, \dots, \hat{\kappa}_K)$ 中的元素 $\kappa_1^\omega, \kappa_2^\omega, \dots, \kappa_K^\omega$ 代入式(21)计算 ξ ;
- (9) 当 $\xi > \xi^\circ$ 时, 令 $\xi^\circ = \xi, \kappa_1^* = \kappa_1^\omega, \kappa_2^* = \kappa_2^\omega, \dots, \kappa_K^* = \kappa_K^\omega$;
- (10) end for
- (11) 输出: 最优值 $\kappa_1^*, \kappa_2^*, \dots, \kappa_K^*$ 。

4 仿真分析

本节利用仿真分析验证人工噪声方案在非理想CSI下的有效性。以2层密集异构蜂窝网为例, 其网络半径为 $R_c = 500$ m, 其中部署有宏蜂窝基站(Macrocell Base Stations, MBSs)和微蜂窝基站(Picrocell Base Stations, PBSs), 其空间分布服从均匀PPP, 且分布密度分别为 $\lambda_1 = 1/\pi 500^2$ m⁻², $\lambda_2 = 5\lambda_1$ 。网络中的窃听者随机分布且分布密度为 $\lambda_e = 5\lambda_1$ 。仿真发射功率和路径衰落系数分别为 $P_1 = 20$ W, $P_2 = 2$ W和 $\alpha = 4$ 。保密信息传输速率为 $R_s = 0.1$ bit/(s·Hz)。

4.1 功率分配因子的影响

COP和功率分配因子的关系如图2所示, 图中COP的理论值和仿真值相一致, 说明理论分析的有效性。可观察到, COP随着功率分配因子的增加而降低。当 $\kappa_i = 0$ 时, 发射端不发射信号仅发射人工噪声, 因此COP的值约为1。由于 κ_i 反映了信号功率分配情况, 且 κ_i 的增加说明信号功率增加而

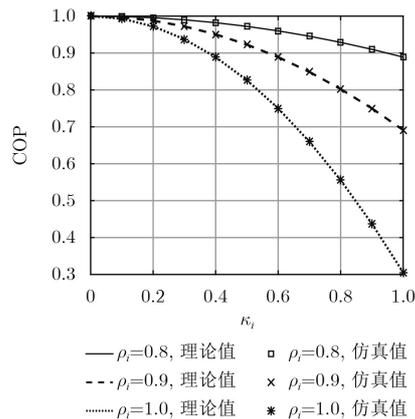


图2 COP与功率分配因子的关系

人工噪声功率减小, 因此通信的可靠性得到保证, COP下降。此外, 信道估计精度影响系统的COP, 比较 $\rho_i = 1$ 和 $\rho_i \neq 1$ 的曲线, 可见 $\rho_i = 1$ 对应的COP更低, 系统的可靠性更好。

SOP和功率分配因子的关系如图3所示, 可观察到, SOP随着功率分配因子的增加而增加。当 $\kappa_i = 0$ 时, 发射端不发射信号仅发射人工噪声, 因此SOP的值约为0, 系统不会出现安全中断。随着 κ_i 的增加, 人工噪声功率减小, 对窃听信道的人为干扰变小, 通信的安全性下降, SOP增加。因此提高功率分配因子会弱化系统的安全性能。

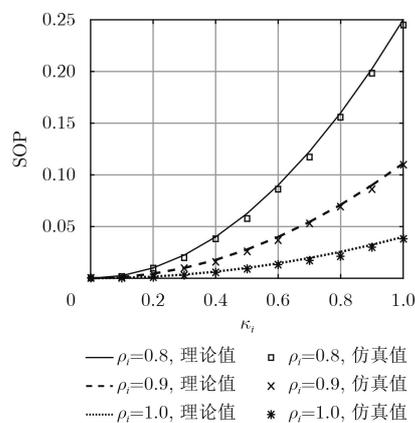


图3 SOP与功率分配因子的关系

4.2 信道估计精度的影响

图4给出了COP, SOP和安全吞吐量和信道估计精度的关系。设置 $\rho = \rho_1 = \rho_2$ 来研究信道估计精度的影响。显然COP和SOP随着 ρ 的提高而下降, 而安全吞吐量随着 ρ 的增加而增加。这是由于信道估计误差影响了正常通信, 当信道估计精度高时, 系统的可靠性和安全性均得到保证, 因此安全吞吐量得到提高。

比较 $\kappa_1=1.0, \kappa_2=1.0$; $\kappa_1=0.6, \kappa_2=0.6$ 和 $\kappa_1=0.4, \kappa_2=0.4$ 对应的曲线, 其中 $\kappa_1=1.0, \kappa_2=1.0$ 意味着系

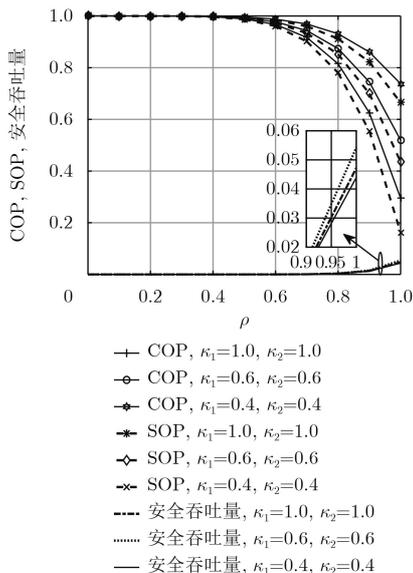


图4 COP, SOP和安全吞吐量与 ρ 的关系

统只发射信号而不发射人工噪声，其他两种情况是系统发射人工噪声的情况。观察曲线可以发现COP随着功率分配因子的减小而增加，SOP随着功率分配因子的减小而减小，因此人工噪声传输方案能够改善系统的安全性同时降低系统的可靠性，因此功率分配因子在安全性和可靠性之间存在折中。由图可见 $\kappa_1 = 0.6, \kappa_2 = 0.6$ 有最高的安全吞吐量，这是由于 $\kappa_1 = 0.6, \kappa_2 = 0.6$ 是 $\rho = 1.0$ 时的最佳功率分配因子，因此此时的安全吞吐量显然高于其他情况，可见当系统应用人工噪声方案且设置当前最优功率分配因子时可提升约15%的安全吞吐量。

图2-图4说明人工噪声方案可改变非理想信道条件下系统的安全可靠性能，实际中，功率分配因子的设置需根据不同的通信需求进行选择。此外，上述结果说明提升信道估计精度能够提升密集异构蜂窝网的性能。

4.3 微基站密度的影响

由于密集异构蜂窝网中基站的部署密度对系统性能产生重要影响，且宏基站和微基站的影响相似。为说明问题，仅考虑在宏蜂窝中部署微基站的情况。如图5所示为COP和SOP随微基站密度 λ_2 变化的关系，由图可知COP和SOP都随 λ_2 的增大而减小，这是由于微基站的部署使得系统中有更多的基站可为用户提供服务，因此合法信道容量得到提升。而 λ_2 的持续增加导致小区间干扰变复杂，限制了系统可靠性及安全性的持续改善，因此当 λ_2 增大到一定范围，COP和SOP的下降趋于平缓。

安全吞吐量和微基站密度及其信道估计精度的关系如图6所示，由图6可知系统的安全吞吐量是 λ_2 的增函数。当 $\lambda_2/\lambda_1 \leq 4$ 时， $\kappa_2 = 0.6$ 对应的安全

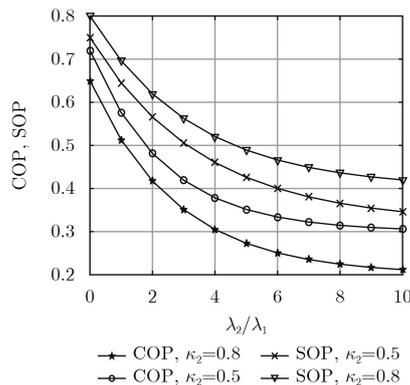


图5 COP和SOP和微基站密度的关系

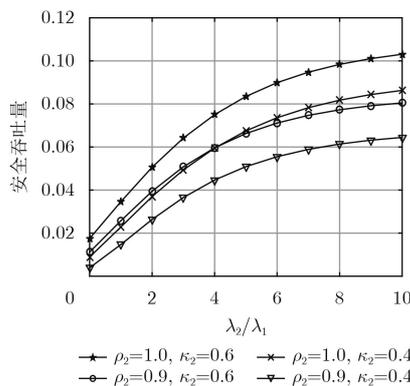


图6 安全吞吐量和微基站密度的关系

吞吐量大于 $\kappa_2 = 0.4$ 的情况，这是由于 $\kappa_2 = 0.6$ 是 $\rho_2 = 1.0$ 时的最佳功率分配因子，因此此时系统的安全吞吐量大于其他情况。当 $\lambda_2/\lambda_1 > 4$ 时， $\rho_2 = 0.9, \kappa_2 = 0.6$ 对应的安全吞吐量小于 $\rho_2 = 1.0, \kappa_2 = 0.4$ 对应的安全吞吐量，这是由于随着微基站密度的持续增加，信道估计误差引起的干扰不可忽视，因此此时部署信道估计能力强的微基站能得到更大的安全吞吐量。当微基站密度大于一定值以后，即 $\lambda_2/\lambda_1 > 6$ 时，系统的安全吞吐量增长趋于平缓，这是由于微基站的持续密集部署增大了系统间的干扰，影响系统性能。实际中，在宏蜂窝小区中部署微基站时需考虑基站的信道估计能力，部署的信道估计能力强的微基站能有效提升系统安全吞吐量。

5 结束语

本文分析了非理想CSI条件下人工噪声对密集异构蜂窝网安全可靠通信的影响，在此基础上给出功率分配因子优化模型，在不同信道估计精度条件下设置最优的功率分配因子。首先，考虑信道估计误差对合法信号传输以及人工噪声泄露的影响，分析了典型通信链路的可靠性和安全性。然后，为进一步优化系统性能，在安全性和可靠性约束条件下提出了功率分配因子优化模型，从而最大化系统安

全吞吐量。通过 K 维联合搜索算法优化出每层网络的最优功率分配因子。仿真分析了功率分配因子、信道估计精度、微基站密度以及天线数量对系统安全吞吐量的影响,得出结论人工噪声方案可改变非理想信道条件下系统的安全可靠性能,此外,提升信道估计精度能够提升密集异构蜂窝网的安全性能。

参考文献

- [1] YANG Xiaobin and FAPOJUWO A O. Coverage probability analysis of heterogeneous cellular networks in rician/rayleigh fading environments[J]. *IEEE Communications Letters*, 2015, 19(7): 1197–1200. doi: [10.1109/LCOMM.2015.2430346](https://doi.org/10.1109/LCOMM.2015.2430346).
- [2] BLOCH M and BARROS J. Physical-layer Security: From Information Theory to Security Engineering[M]. Cambridge: Cambridge University Press, 2011: 290–308. doi: [10.1017/CBO9780511977985](https://doi.org/10.1017/CBO9780511977985).
- [3] YANG Nan, WANG Lifeng, 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](https://doi.org/10.1109/MCOM.2015.7081071).
- [4] GOEL S and NEGI R. Guaranteeing secrecy using artificial noise[J]. *IEEE Transactions on Wireless Communication*, 2008, 7(6): 2180–2189. doi: [10.1109/TWC.2008.060848](https://doi.org/10.1109/TWC.2008.060848).
- [5] ZHANG Xi, ZHOU Xiangyun, and MCKAY M. Enhancing secrecy with multi-antenna transmission in wireless Ad hoc networks[J]. *IEEE Transactions on Information Forensics and Security*, 2013, 8(11): 1802–1814. doi: [10.1109/TIFS.2013.2279842](https://doi.org/10.1109/TIFS.2013.2279842).
- [6] CAI Yueming, XU Xiaoming, and YANG Weiwei. Secure transmission in the random cognitive radio networks with secrecy guard zone and artificial noise[J]. *IET Communications*, 2016, 10(15): 1904–1913. doi: [10.1049/iet-com.2016.0117](https://doi.org/10.1049/iet-com.2016.0117).
- [7] ZHONG Zhihao, LUO Wenyu, PENG Jianhua, et al. Secrecy performance analysis of cooperative transmission and cooperative jamming for multi-tier heterogeneous cellular networks[J]. *SCIENTIA SINICA Informationis China Information Sciences*, 2016, 46(1): 33–48. doi: [10.1360/N112015-00174](https://doi.org/10.1360/N112015-00174).
- [8] WANG Chao and WANG Huiming. Opportunistic jamming for enhancing security stochastic geometry modeling and analysis[J]. *IEEE Transactions on Vehicular Technology*, 2016, 65(12): 10213–10217. doi: [10.1109/TVT.2016.2536621](https://doi.org/10.1109/TVT.2016.2536621).
- [9] ZHENG Tongxing and WANG Huiming. Optimal power allocation for artificial noise under imperfect csi against spatially random eavesdroppers[J]. *IEEE Transactions on Vehicular Technology*, 2016, 65(10): 8812–8817. doi: [10.1109/TVT.2015.2513003](https://doi.org/10.1109/TVT.2015.2513003).
- [10] WANG Huiming, WANG Chao, ZHENG Tongxing, et al. Impact of artificial noise on cellular networks: A stochastic geometry approach[J]. *IEEE Transactions on Wireless Communications*, 2016, 15(11): 7390–7404. doi: [10.1109/TWC.2016.2601903](https://doi.org/10.1109/TWC.2016.2601903).
- [11] LI Si, LI Qiang, and SHAO Shihai. Robust secrecy beamforming for full-duplex two-way relay networks under imperfect channel state information[J]. *Science China Information Sciences*, 2018, 61(2): 022307. doi: [10.1007/S11432-017-9110-X](https://doi.org/10.1007/S11432-017-9110-X).
- [12] CAO Weifeng, ZOU Yulong, and YANG Zhen. Joint source-relay selection for improving wireless physical layer security[C]. 2016 IEEE Global Communications Conference, Singapore, 2017: 1–5. doi: [10.1109/GLOCOM.2016.7841935](https://doi.org/10.1109/GLOCOM.2016.7841935).
- [13] CAI Yunlong, SHI Qingjiang, CHAMPAGNE B, et al. Joint transceiver design for secure downlink communications over an amplify-and-forward MIMO relay[J]. *IEEE Transactions on Communications*, 2017, 65(9): 3691–3704. doi: [10.1109/TCOMM.2017.2708110](https://doi.org/10.1109/TCOMM.2017.2708110).
- [14] WANG Huiming, ZHENG Tongxing, YUAN Jinhong, et al. Physical layer security in heterogeneous cellular networks[J]. *IEEE Transactions on Communications*, 2016, 64(3): 1204–1219. doi: [10.1109/TCOMM.2016.2519402](https://doi.org/10.1109/TCOMM.2016.2519402).
- [15] GRADSHTEYN I, RYZHIK I, JEFFREY A, et al. Table of Integrals, Series, and Products[M]. New York, USA, Academic, 2007. doi: [10.2307/2007757](https://doi.org/10.2307/2007757).

许耘嘉: 女, 1993年生, 博士生, 研究方向为移动通信安全、物理层安全。

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

李 军: 男, 1981年生, 工程师, 研究方向为移动通信终端。