多用户大规模 MIMO 自适应安全传输策略

金 梁 宋昊天* 钟 州 许晓明
(国家数字交换系统工程技术研究中心 郑州 450002)

摘 要：大规模 MIMO 系统采用空分多址可以提高系统吞吐量，同时利用多用户下行信号的相互协作可以对窃听者造成叠加干扰，带来了天然的安全增益。但目前该系统的物理层安全研究仍采用传统的人工噪声方案，忽略了多用户信号干扰带来的安全增益，造成严重的功率浪费。针对这一问题，该文分析了多用户信号干扰对系统可达平均安全速率和平均安全能效的影响，给出了系统的最佳接入用户区间。研究发现，在系统接入用户数较少和用户数较多时，系统安全能力较弱，针对此分别提出了 N 波束加扰和基于用户位置的用户调度的自适应安全传输策略。最后通过仿真验证了理论推导和所提策略的有效性，利用该文所提策略，能够保证系统天然安全能力不足时的安全通信。

关键词：大规模 MIMO；物理层安全；多用户；自适应安全传输
中图分类号： TN92 **文献标识码**： A **文章编号**：1009-5896(2018)06-1468-08
DOI: 10.11999/JEIT170974

Adaptive Secure Transmission Strategy for Multiuser Massive MIMO

JIN Liang SONG Haotian ZHONG Zhou XU Xiaoming
(*National Digital Switching System Engineering & Technological Research Center*, *Zhengzhou* 450002, *China*)

Abstact: Massive MIMO system using Space Division Multiple Access (SDMA) can improve system throughput, and the use of multi-user downlink signal collaboration can cause superimposed interference to the eavesdropper, bringing a natural security gain. However, the physical layer security research of the system still adopts the traditional artificial noise scheme to improve the system security, ignoring the safety gain caused by the multi-user signal interference, resulting in serious power waste. In response to this problem, the impact of multi-user signal interference on the system achievable average security rate and average safety energy efficiency is analyzed in this paper, and the optimal interval of access users is given. The research shows that the system security capability is weak when the number of access users is small or large. Therefore, an adaptive secure transmission strategy to transmit N scrambling beams and user scheduling based on user location is proposed respectively. Finally, the effectiveness of the theoretical derivation and the proposed strategy is verified through the simulation. By using the proposed strategy, the secure communication can be guaranteed when the system's natural security capability is insufficient.

Key words: Massive MIMO; Physical layer security; Muti-users; Adaptive secure transmission

1 引言

由于无线信道的开放性，信息安全一直是无线通信的重要问题。近些年，物理层安全从信息论的角度为无线通信提供了新的安全保障。特别是在下一代移动通信中，基站端配备大规模 MIMO，天线数的增多，除了带来更高的数据传输速率、可靠性和更低的用户间干扰外，也为物理层安全的应用提供了新的契机[1]。

在大规模 MIMO 系统中，随着基站天线数的增多，热噪声和用户间干扰的影响逐渐变小。系统利用线性预编码，可以同时同频地服务更多的用户，而来自系统外部的窃听者在窃听目标用户时，则会收到发送给其他用户信号的叠加干扰。这一模型与人工噪声模型非常类似，因此多用户信号为系统的安全性能提升带来了天然的增益。当前大多数大规模 MIMO 物理层安全的研究利用传统的人工噪声和线性预编码[2,3]，或者利用功率控制[4]来保障通信安全，以此得到系统安全性能的下界。这种做法忽

收稿日期：2017-10-17；改回日期：2018-01-16；网络出版：2018-03-23
*通信作者：宋昊天 476657937@qq.com
基金项目：国家 863 计划项目(2015AA01A708)，国家自然科学基金(61471396, 61701538, 61601514, 61501516, 61521003)
Foundation Items: The National 863 Program of China (2015AA01A708), The National Natural Science Foundation of China (61471396, 61701538, 61601514, 61501516, 61521003)

略了系统的多用户干扰带来的安全增益，造成大量的功率浪费[5]。

目前已经有研究利用多用户下行信号干扰窃听者，提升系统安全性能。文献[6]利用正交随机波束成形和用户窃听者的信干比反馈，通过选择对窃听者干扰最大的波束，提升系统安全性，并推导了平均安全和速率的闭合表达式。文献[7]在此基础上，分析了高低信噪比情况下使系统安全性能最高的最佳接入用户数。然而传统多用户 MIMO 系统基站端天线数较少，系统可以同时服务的用户数少，对窃听者影响有限，且小尺度衰落对用户的信干噪比影响较大，需要花费大量的资源进行信干噪比反馈。而在大规模 MIMO 系统中，随着天线数增多，小尺度衰落和热噪声对用户的影响渐渐消失，因此基于传统 MIMO 系统的结论已经不再适用。在大规模 MIMO 两层异构网络中，文献[8]考虑了配备了大规模 MIMO 的宏基站用户信号和单天线微基站用户信号干扰对系统安全中断概率的影响，但是该文重点研究了微基站密度对系统安全性能的影响，忽略了宏基站用户数量变化的影响。文献[8]的结论说明合法用户通过配合可以在窃听端造成多路信息相互干扰，且窃听者无法消除这种干扰。然而，当前对于大规模 MIMO 系统中用户信号干扰对窃听者影响的研究还未见诸报道，更没有基于此提出相适应的安全传输策略。

针对以上问题，本文以单小区下行大规模 MIMO 通信系统为例，利用随机几何工具对用户和窃听者的位置、数量进行建模。首先，推导了用户的可达平均安全速率，之后给出了系统的平均安全能效；然后，基于上述分析，提出基于接入用户数的自适应安全传输策略，在保证用户安全通信的同时实现系统功率效率最大化；最后，仿真验证了理论推导的有效性，以及本文安全策略带来的系统安全性能的增益。研究发现大规模 MIMO 系统具有天然的安全传输特性，利用本文所提安全策略，能够保证系统在用户数较少或者用户数过多情况下天然安全能力不足时的安全通信。

2　系统模型描述

单小区下行大规模 MIMO 通信系统模型如图 1 所示，配备 M 根天线的基站同时同频地服务 K 个单天线用户，所有用户均匀地分布在外径为 R 内径为 r_0 的服务范围内，用 Φ_k 表示。同样配备单天线的窃听者独立隐蔽地窃听被服务用户的信息，在全空间内服从密度为 λ_e 的 2 维 PPP(Poisson Point Process)分布，用 Φ_e 表示。

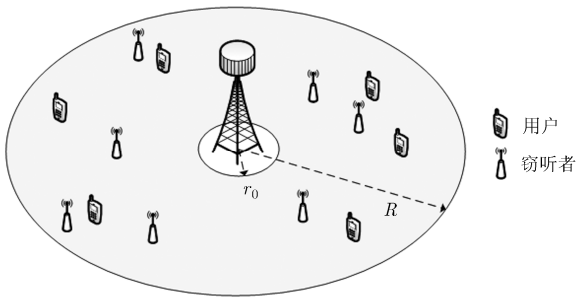

图 1 单小区下行大规模 MIMO 通信系统

在 TDD 模式下，用户发送上行导频信号，大规模 MIMO 基站通过导频信号进行信道估计，利用信道互易性获得下行信道矩阵。假设信道相干时间长度为 T，其中发送上行导频的时间长度为 τ，则同时同频接入基站的用户数 $K \le \tau \le T$。假设基站到 K 个用户的信道矩阵为 $\boldsymbol{G} = \boldsymbol{D}^{1/2}\boldsymbol{H}$，其中，$\boldsymbol{D} = \mathrm{diag}\{\beta_1, \beta_2, \cdots, \beta_k\}$ 是大尺度衰落矩阵，衰落系数 $\beta = \xi d^{-\alpha}$，等于阴影衰落 ξ 和路径衰落 $d^{-\alpha}$ 的乘积，并且 $10\lg\xi \sim \mathcal{N}\left(0, \sigma_{\mathrm{SF}}^2\right)$，$\alpha$ 是路径衰落因子，$\boldsymbol{H} = \left[\boldsymbol{h}_1^{\mathrm{T}}\, \boldsymbol{h}_2^{\mathrm{T}} \cdots \boldsymbol{h}_k^{\mathrm{T}}\right]^{\mathrm{T}} \in \boldsymbol{C}^{K\times M}$ 是小尺度衰落矩阵，其元素 $h_{km} \sim \mathcal{CN}(0,1)(k = 1,2,\cdots,K; m = 1,2,\cdots,M)$ 是独立同分布的复高斯随机变量。同样地，每个窃听者的信道向量可以表示为 $\boldsymbol{g}_e = \sqrt{\beta_e}\boldsymbol{h}_e$。假设基站可以获得精确的用户 CSI(Channel State Information)，但是无法获得窃听者的 CSI。

假设基站端使用 ZFBF(Zero-Forcing Beam-Forming)向每个用户发送一束等功率的信息流，此时每个用户只能接收到发送给自己的信号，而无法成为系统内部的潜在窃听者。基站端的预编码矩阵为

$$\boldsymbol{W} = [\boldsymbol{w}_1, \boldsymbol{w}_2, \cdots, \boldsymbol{w}_k] = \frac{\boldsymbol{H}^{\mathrm{H}}\left(\boldsymbol{H}\boldsymbol{H}^{\mathrm{H}}\right)^{-1}}{\left\|\boldsymbol{H}^{\mathrm{H}}\left(\boldsymbol{H}\boldsymbol{H}^{\mathrm{H}}\right)^{-1}\right\|} \tag{1}$$

此时每个用户和窃听者接收信号为

$$y_k = \sqrt{\beta_k}\boldsymbol{h}_k\boldsymbol{w}_k\sqrt{p_k}s_k + n_k \tag{2}$$

$$y_e = \sqrt{\beta_e}\boldsymbol{h}_e\boldsymbol{w}_k\sqrt{p_k}s_k + \sqrt{\beta_e}\boldsymbol{h}_e\sum_{j=1\neq k}^{K}\boldsymbol{w}_j\sqrt{p_j}s_j + n_e \tag{3}$$

其中，s_k 是发送给每个用户的信号，满足 $\mathrm{E}\left[\left|s_k\right|^2\right] = 1$，$p_k$ 是每束信号的功率，总发送功率满足 $P_T \ge \sum_{k=1}^{K} p_k$。$n_k \sim \mathcal{CN}\left(0, \sigma_k^2\right)$ 和 $n_e \sim \mathcal{CN}\left(0, \sigma_k^2\right)$ 分别是用户和窃听端的加性高斯白噪声，方差分别为 σ_k^2 和 σ_e^2。

值得说明的是，本文之所以假设用户在服务区域内服从均匀分布，是为了确定同时同频接入系统

的用户数量，而窃听者服从 PPP 分布是为了增加窃听者位置及数量的不确定性，使结果更符合实际条件。本文以单小区为例展开分析，其结论可以为多小区大规模 MIMO 系统提供参考。

3 基于接入用户数的大规模 MIMO 安全传输策略

由于大规模 MIMO 系统中用户和窃听者的数目、位置随机性较高，导致其安全性能较难分析。本节利用随机几何工具，建立大规模 MIMO 系统下多用户多窃听者安全模型，通过对用户的可达安全速率、系统安全能量效率的分析，得到系统安全性能随接入用户数的变化趋势，并依据此提出基于接入用户数的安全传输策略。

3.1 安全模型建立

假设所有信道经历准静态瑞利衰落，由式(2)可得第 k 个用户的接收 SNR 为

$$\mathrm{SNR}_k = \left|\boldsymbol{h}_k\boldsymbol{w}_k\right|^2 \theta_k \tag{4}$$

其中，第 k 个用户到基站的信道增益是 $\left|\boldsymbol{h}_k\boldsymbol{w}_k\right|^2 \sim \Gamma(M-K+1,1)$ [9]，$\theta_k = \dfrac{p_k\beta_k}{\sigma_k^2}$ 表示基站单天线时用户 k 的平均接收信噪比。

考虑系统最差的情况，即 SINR(Signal to Interference plus Noise Ratio)最大的窃听链路性能，由式(3)可得最危险的窃听者接收 SINR 为

$$\mathrm{SINR}_k^e = \max_{e\in\Phi_e}\left\{\frac{\left|\boldsymbol{h}_e\boldsymbol{w}_k\right|^2}{\theta_e^{-1}+\sum\limits_{l=1\neq k}^{K}\left|\boldsymbol{h}_e\boldsymbol{w}_l\right|^2}\right\} \tag{5}$$

其中，最危险窃听者与基站间的信道增益是 $\left|\boldsymbol{h}_e\boldsymbol{w}_k\right|^2 \sim \exp(1)$，小区内其他用户信号对窃听者干扰的信道增益是 $\sum_{l=1\neq k}^{K}\left|\boldsymbol{h}_e\boldsymbol{w}_l\right|^2 \sim \Gamma(K-1,1)$ [10]，$\theta_e = \dfrac{p_k\beta_e}{\sigma_e^2}$ 表示基站单天线时窃听者的平均接收信噪比。

3.2 可达平均安全速率下界

为了保证系统内每个用户的安全通信，首先分析合法用户的可达平均安全速率。假设信道服从高斯分布，且输入信息 $s\sim\mathcal{CN}(0,1)$ 时，用户 k 的可达平均安全速率为[11]

$$R_k^s = \left[R_k - R_k^e\right]^+ \tag{6}$$

其中，$R_k = \dfrac{T-\tau}{T}\mathrm{E}\left\{\log_2(1+\mathrm{SNR}_k)\right\}$ 是用户的可达平均速率，$R_k^e = \dfrac{T-\tau}{T}\mathrm{E}\left\{\log_2(1+\mathrm{SINR}_k^e)\right\}$ 是窃听者的平均窃听速率，$[x]^+ \triangleq \max(0,x)$。在本文分析中假设导频 τ 与接入用户数 K 相等。

引理 1 在瑞利慢衰落信道下，配备 M 根天线的基站使用 ZFBF，同时同频地为服从 Φ_k 分布的 K 个用户服务时，用户 k 的可达平均速率下界为

$$R_k^L = \frac{T-\tau}{T}\log_2\left[1+(M-K)\theta_T\right] \tag{7}$$

其中，平均区域 SNR 为

$$\theta_T = \frac{p_k}{\sigma_k^2}\frac{\alpha+2}{2}\frac{R^2-r_0^2}{R^{\alpha+2}-r_0^{\alpha+2}}\exp\left[-\frac{1}{2}\left(\frac{\ln 10}{10}\sigma_{\mathrm{SF}}\right)^2\right] \tag{8}$$

证明 在多用户场景中，很难获得每个用户的精确可达平均速率。根据凸优化理论可知，函数 $\log_2\left(1+x^{-1}\right)$ 为关于变量 x 的凸函数。根据 Jensen 不等式可得

$$\mathrm{E}\left\{\log_2(1+x^{-1})\right\} \geq \log_2\left(1+\mathrm{E}^{-1}(x)\right) \tag{9}$$

应用式(9)，可得可达平均速率的下界为

$$R_k^L = \frac{T-\tau}{T}\log_2\left(1+\mathrm{E}^{-1}\left(\mathrm{SNR}_k{}^{-1}\right)\right) \tag{10}$$

结合式(4)可得

$$\begin{aligned}\mathrm{E}\left(\mathrm{SNR}_k{}^{-1}\right) &= \mathrm{E}^{-1}\left(\left|\boldsymbol{h}_k\boldsymbol{w}_k\right|^2\right)\mathrm{E}\left(\theta_k^{-1}\right)\\ &= \frac{\sigma_k^2}{p_k}\mathrm{E}^{-1}\left(\left|\boldsymbol{h}_k\boldsymbol{w}_k\right|^2\right)\mathrm{E}\left(d_k^{\alpha}\right)\mathrm{E}\left(\xi_k^{-1}\right)\end{aligned} \tag{11}$$

$\mathrm{E}^{-1}\left(\left|\boldsymbol{h}_k\boldsymbol{w}_k\right|^2\right)$，$\mathrm{E}\left(d_k^{\alpha}\right)$ 和 $\mathrm{E}\left(\xi_k^{-1}\right)$ 的计算方法和文献[11]中的相同，将 3 个期望值代入式(11)即可得 R_k^L。引理 1 得证。

引理 2 当存在服从 Φ_e 分布的窃听者时，对于 K 个被服务用户中的目标用户 k，最危险窃听者的可达平均速率为

$$\begin{aligned}R_k^e &= \frac{T-\tau}{T}\mathrm{E}\left\{\log_2(1+\mathrm{SINR}_k^e)\right\}\\ &= \frac{T-\tau}{T}\frac{1}{\ln 2}\int_0^{\infty}\frac{1-F_{\mathrm{SINR}^e}(\gamma)}{1+\gamma}\mathrm{d}\gamma\end{aligned} \tag{12}$$

其中，窃听者接收 SINR 的分布函数

$$\begin{aligned}F_{\mathrm{SINR}^e}(\gamma) = \exp\Bigg\{&-2\pi\lambda_e\frac{1}{(1+\gamma)^{K-1}}\frac{\Gamma(2/\alpha)}{\alpha}\\ &\cdot\left(\frac{p_k}{\sigma_e^2\gamma}\right)^{2/\alpha}\exp\left[2\left(\frac{\ln 10}{10}\frac{\sigma_{\mathrm{SF}}}{\alpha}\right)^2\right]\Bigg\}\end{aligned} \tag{13}$$

证明 假设窃听者独立地窃听合法用户的信息，对于目标用户 k，其安全下界由能力最强即链路 SINR 最大的窃听者的窃听性能决定。则最危险窃听者的 SINR 分布函数为

$$F_{\mathrm{SINR}^{\mathrm{e}}}(\gamma)=P\left(\max_{e\in\Phi_e}\left\{\frac{\left|\boldsymbol{h}_e\boldsymbol{w}_k\right|^2}{\theta_e^{-1}+\sum_{l=1\neq k}^{K}\left|\boldsymbol{h}_e\boldsymbol{w}_l\right|^2}\right\}\le\gamma\right)\overset{\mathrm{a}}{=}\mathrm{E}\left\{\prod_{e\in\Phi_e}P\left[\left|\boldsymbol{h}_e\boldsymbol{w}_k\right|^2\le\gamma\left(\theta_e^{-1}+g_l\right)\right]\right\}\overset{\mathrm{b}}{=}\mathrm{E}\left\{\prod_{e\in\Phi_e}\mathrm{E}\left[1-\exp\left(-\gamma\theta_e^{-1}-\gamma g_l\right)\right]\right\}$$

$$\overset{\mathrm{c}}{=}\exp\left\{-2\pi\lambda_e\mathrm{E}\left(e^{-\gamma g_l}\right)\int_0^{\infty}\mathrm{E}\left[\exp\left(\frac{-\gamma\sigma_e^2y^{\alpha}}{p_k\xi_e}\right)\right]y\mathrm{d}y\right\}\overset{\mathrm{d}}{=}\exp\left\{-2\pi\lambda_e\cdot L_{g_l}(\gamma)\cdot\frac{\Gamma\left(\frac{2}{\alpha}\right)}{\alpha}\left(\frac{p_k}{\sigma_e^2\gamma}\right)^{\frac{2}{\alpha}}\mathrm{E}\left(\xi_e^{\frac{2}{\alpha}}\right)\right\}\tag{14}$$

其中，(a)根据概率论得到，$g_l=\sum_{l=1\neq k}^{K}\left|\boldsymbol{h}_e\boldsymbol{w}_l\right|^2$ 是服从 $\Gamma(K-1,1)$ 的随机变量，(b)根据指数分布的分布函数求得，(c)根据 PPP 分布的概率母函数得到，(d)中 $L_{g_l}(\gamma)$ 是随机变量 g_l 的拉普拉斯反变换，$\mathrm{E}\left(\xi_e^{2/\alpha}\right)$ 的求法和引理 1 相同，将结果代入式(14)，引理 2 得证。

基于以上分析，本文得到大规模 MIMO 系统中用户可达平均安全速率的下界。

定理 1　对于大规模 MIMO 多用户多窃听者场景，考虑多用户信号干扰对窃听者的影响时，用户 k 的可达平均安全速率的下界为

$$R_k^{sL}=\left[R_k^L-R_k^e\right]^+\tag{15}$$

其中，R_k^L 为用户 k 可达平均速率下界，由引理 1 给出。R_k^e 为窃听用户 k 的窃听者中 SINR 最强的窃听者的平均窃听速率，由引理 2 给出。

3.3 平均安全能效下界

可达平均安全速率衡量了单个用户通信的安全性能，然而对于完整的多用户通信系统，使系统内单个用户安全速率最高的传输策略未必是最佳的，因为能量效率也是衡量系统性能的重要指标。现有的文献为了提高用户可达平均安全速率，多利用人工噪声来恶化窃听者的接收信干噪比，大量的功率被用来生成人工噪声，造成了严重的功率浪费。为保证用户合法通信的同时，实现系统功率效率的最大化，本节以安全能效为衡量标准，研究大规模 MIMO 下行通信系统的安全性能。

系统安全能效定义为系统安全谱效与总消耗功率的比值[12]。其中系统的平均安全谱效为所有用户平均可达安全速率的和，可以表示为

$$\mathrm{SSE}=\sum_{k=1}^{K}R_k^s\tag{16}$$

总消耗功率为

$$P_t=p_0+\sum_{k=1}^{K}\frac{p_k}{\varepsilon}+\sum_{t=1}^{3}\left(K^{t-1}\left(\Delta_t+M\Lambda_t\right)\right)\tag{17}$$

其中，p_0 为大规模天线基站的静态硬件功率消耗，ε 为功率放大器的效率系数，参数 Δ_t 和 Λ_t 由收发链路、编解码、信道估计以及预编码等过程的功率消耗决定。

定理 2　对于大规模 MIMO 多用户多窃听者场景，考虑多用户信号干扰对窃听者的影响时，系统的平均安全能效下界为

$$\mathrm{SEE}^L=\mathrm{SSE}^L/P_t\tag{18}$$

其中，$\mathrm{SSE}^L=\sum_{k=1}^{K}R_k^{sL}$ 为系统的平均安全谱效下界。

式(15)和式(18)对接入用户数 K 分别求导发现，很难精确地数学证明 R_k^{sL} 和 SEE^L 关于 K 的凹凸性。从物理含义角度出发，当接入用户数较少时，窃听者接收到的非目标用户的信号干扰较小，可达窃听速率较高，此时应该以保证目标用户的 R_k^{sL} 为目的设计安全传输策略。当接入用户数增多时，窃听者的窃听能力因多用户信号干扰而受限，用户的可达平均安全速率下界 R_k^L 成为安全性能的限制因素，并且当用户数增长到发射天线数时，R_k^L=0。此时为了提高资源利用率，应该控制接入用户数，以最优的 SEE^L 为目的设计调度策略。

3.4 基于接入用户数的自适应安全传输策略

经过以上分析发现，基站端通过联合预编码，可以消除合法用户处其他用户信号的干扰，使其无法成为系统的内部窃听者。而来自系统外的窃听者由于没有参与协作，会受到发送给其他用户信息流的叠加干扰，窃听性能受到限制。因此接入系统的用户数量对系统的安全性能有很大的影响，需要针对不同的接入用户数实施对应的安全策略。本节首先给出了最佳的用户接入区间；之后，针对接入用户数较少的情况给出了 N 波束加扰策略，针对请求接入用户数较多的情况给出了基于用户位置的用户调度策略；最后给出了自适应安全传输策略的详细实施步骤。

3.4.1 最佳接入用户区间分析　图 2 是不同接入用户数时，用户、最强窃听者的可达平均速率和该用户的可达平均安全速率的变化曲线，假设基站配备

64 根天线，同时同频为均匀分布在内径为 50 m 外径为 500 m 的圆环上的用户服务，窃听者独立地窃听目标用户，系统参数如下：$\alpha=3.8$，$\sigma_{\mathrm{SF}}=8$，$T=128$，$\sigma_k^2=\sigma_e^2=-70$ dB，$p_k=2$ W。

观察图 2 曲线变化趋势可得，当接入系统的用户数较少时，最危险窃听者可以取得较高的可达平均速率。这是由于当用户数较少时，窃听者受到的多用户干扰较小，而最危险窃听者拥有信道优势，最终导致系统的可达平均安全速率较低。因此系统存在一个最佳接入用户数的最小值 $K_{\min}^{\mathrm{opt}}$，使得 $R_k^{sL}\geq R_{\mathrm{th}}$，$R_{\mathrm{th}}$ 为安全速率门限值。

请求接入的用户数大于 $K_{\min}^{\mathrm{opt}}$ 时，发射给用户的信号对窃听者的干扰已经使系统的安全性能满足需求，无需使用任何安全手段即可保障合法用户的安全通信。

图 3 是不同数量接入用户时，系统的可达平均安全能效下界的变化曲线。仿真条件和图 2 相同，其余系统参数如下：$p_0=4$，ε=0.38，$\Delta_1=4.8$，$\Delta_2=0$，$\Delta_3=2.08\times10^{-8}$，$\Lambda_1=1$，$\Lambda_2=9.5\times10^{-8}$，$\Lambda_3=6.25\times10^{-8}$。

当请求接入的用户数继续增加，此时窃听者受其他用户信号的干扰，窃听性能已经非常弱了，而受到系统总自由度的约束，每个合法用户的平均自由度下降，当接入用户数增大到某一门限时，用户的可达平均速率下降，最终导致可达平均安全速率下降。并且随着接入用户数的继续增多，系统的总功率消耗增加，导致系统的平均安全能效急速下降，因此从系统的功率效率的角度出发，存在一个最佳的接入用户数的最大值 $K_{\max}^{\mathrm{opt}}$，使系统的平均安全能效最优，如图 3 所示。

给定系统参数，若窃听者密度已知，则可以通过 1 维线性搜索求解出最佳用户接入区间 $\left[K_{\min}^{\mathrm{opt}},K_{\max}^{\mathrm{opt}}\right]$，即

$$K_{\max}^{\mathrm{opt}}=\underset{K\in\{1,2,\cdots,M\}}{\arg\max}\ \mathrm{SEE}^L \tag{19}$$

$$K_{\min}^{\mathrm{opt}}=\min_{R_k^{sL}\geq R_{\mathrm{th}}}K,K\in\{1,2,\cdots,M\} \tag{20}$$

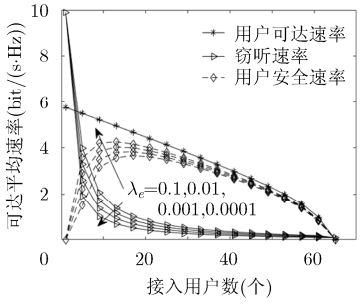

图 2 不同接入用户数时可达平均速率

3.4.2 *N* 波束加扰策略 当请求接入用户数少于 $K_{\min}^{\mathrm{opt}}$ 时，用户的安全通信受到威胁，此时需要使用人工噪声来提高系统的安全性能，即在合法用户信道零空间上发射 N 个加扰波束，使 $R_k^{sL}\geq R_{\mathrm{th}}$。此时，合法用户的接收信噪比未改变，而窃听者接收信噪比变为

$$\mathrm{SINR}_k^{e^*}=\max_{e\in\Phi_e}\left\{\frac{\left|\boldsymbol{h}_e\boldsymbol{w}_k\right|^2}{\theta_e^{-1}+\sum_{i=1}^{N}\left|\boldsymbol{h}_e\boldsymbol{w}_i\right|^2+\sum_{l=1\neq k}^{K}\left|\boldsymbol{h}_e\boldsymbol{w}_l\right|^2}\right\} \tag{21}$$

式中，$\sum_{i=1}^{N}\left|\boldsymbol{h}_e\boldsymbol{w}_i\right|^2\sim\Gamma(N,1)$ 是加扰波束对窃听者的干扰，$\boldsymbol{w}_i$ 是加扰波束的发射权值，从合法用户信道的零空间中选取。此时用户 k 的可达平均安全速率下界为

$$\begin{aligned}R_k^{sL^*}=&R_k^L-\frac{T-\tau}{T}\frac{1}{\ln 2}\\&\cdot\int_0^{\infty}\left[\left\{1-\exp\left\{-2\pi\lambda_e\frac{1}{(1+\gamma)^{K+N-1}}\right.\right.\right.\\&\left.\left.\left.\cdot\frac{\Gamma(2/\alpha)}{\alpha}\left(\frac{p_k}{\sigma_e^2\gamma}\right)^{2/\alpha}\exp\left[2\left(\frac{\ln 10}{10}\frac{\sigma_{SF}}{\alpha}\right)^2\right]\right\}\right\}\\&\left.\Big/(1+\gamma)\right]\mathrm{d}\gamma\end{aligned} \tag{22}$$

分析式(13)和式(22)可得，加扰波束和下行用户信号对窃听者的干扰效果相同。因此当 $K_{\min}^{\mathrm{opt}}-1=K+N-1$ 时，$R_k^{sL}\geq R_{\mathrm{th}}$。所以加扰波束数 N 为

$$N=K_{\min}^{\mathrm{opt}}-K \tag{23}$$

值得说明的是，本文场景中每个加扰波束功率和发送给每个合法用户的信号功率都是相等的，这样即使窃听者使用例如串行干扰消除等技术，也无法将目标用户的信号分离出来。

3.4.3 基于用户位置的用户调度策略 当请求接入的用户数大于 $K_{\max}^{\mathrm{opt}}$ 时，应进行用户调度，使接入用户数等于最佳用户数。对于大规模 MIMO 基站而

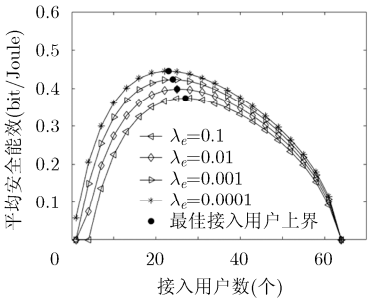

图 3 不同接入用户数时系统的平均安全能效

言，当发射天线数 $M\to\infty$ 时，$\dfrac{\boldsymbol{H}^{\mathrm{H}}\boldsymbol{H}}{M}\approx I_K$。此时用户的信道增益主要来源于大尺度衰落，而与小尺度衰落无关[13]，因此传统的基于瞬时 CSI 的调度策略在大规模 MIMO 系统中的作用会十分有限。因此本文提出基于位置的安全调度策略，当请求接入用户数大于 $K_{\max}^{\mathrm{opt}}$ 时，选择距离近的 $K_{\max}^{\mathrm{opt}}$ 个用户作为活跃用户同时被基站服务。假设被选择的 K 个用户到基站的距离按升序排列依次为 $d_1,d_2,\cdots,d_K$，则第 k 个用户的距离 d_k 的期望为[14]

$$\mathrm{E}^{*}\left(d_k^{\alpha}\right)=r_0^{\alpha}\,{}_2F_1\left(k,-\frac{\alpha}{2};Q+1;1-\frac{R^2}{r_0^2}\right)\tag{24}$$

其中，${}_2F_1(\bullet)$ 表示高斯超几何函数，Q 表示请求接入用户数，代入可得系统的平均安全能效下界为

$$\begin{aligned}\mathrm{SEE}^{L^*}=\Bigg\{&\frac{T-\tau}{T}\log_2\Bigg\{1+(M-K)\frac{p_k}{\sigma_k^2}\\&\cdot\frac{K}{\sum\limits_{k}^{K}r_0^{\alpha}\,{}_2F_1\left(k,-\frac{\alpha}{2};Q+1;1-\frac{R^2}{r_0^2}\right)}\\&\cdot\exp\left[-\frac{1}{2}\left(\frac{\ln 10}{10}\sigma_{\mathrm{SF}}\right)^2\right]\Bigg\}-R_k^e\Bigg\}\Big/P_t\end{aligned}\tag{25}$$

综上所述，本文所提自适应安全传输策略实现步骤如表 1 所示。

4　仿真分析

本节利用 Matlab 仿真给出了所提策略对安全性能的影响。首先，分析了窃听者密度对系统天然安全增益和所提安全策略的影响；然后，在用户数较少的情况下，研究了本文所提 N 波束加扰策略对用户可达安全速率和安全能效的增益，并与传统零空间均匀加扰进行了对比；最后，在用户数较多的情况下，对比了传统方案、随机调度策略和本文所提的位置调度策略的安全能效增益，再次对本文所提策略的优势进行了证明。以单小区大规模 MIMO 基站为例，基站端配备 $M=64$ 根天线，用户和窃听者配备单天线，路径衰落系数 $\alpha=3.8$，阴影衰落标准差 $\sigma_{\mathrm{SF}}=8$ dB，相干时间的符号数 $T=128$ 个，其中导频个数 τ 与接入的用户数相等，外径 $R=500$ m，内径 $r_0=50$ m，噪声功率 $\sigma_k^2=\sigma_e^2=-70$ dBm，发射功率 $p_k=2$ W，$p_0=4$ W，门限值 $R_{\mathrm{th}}=2$ bit/(s·Hz)，如无特殊说明，窃听者密度 $\lambda_e=10^{-2}$，ε=0.38，$\Delta_1=4.8$，$\Delta_2=0$，$\Delta_3=2.08\times10^{-8}$，$\Lambda_1=1$，$\Lambda_2=9.5\times10^{-8}$，$\Lambda_3=6.25\times10^{-8}$ [15]。

表 1 基于接入用户数的自适应安全传输策略

步骤 1　请求接入用户发送反向导频，基站进行信道估计；
步骤 2　基站计算出最佳接入用户区间$\left[K_{\min}^{\mathrm{opt}},\ K_{\max}^{\mathrm{opt}}\right]$，计算方法由式(19)和式(20)给出；
步骤 3　判断请求接入数 Q 是否在$\left[K_{\min}^{\mathrm{opt}},\ K_{\max}^{\mathrm{opt}}\right]$内： (a)若是，系统天然安全性可以满足用户需求； (b)若不是，至下一步；
步骤 4　判断 $Q<K_{\min}^{\mathrm{opt}}$： (a)若是，发送 N 个加扰波束，N 由式(23)给出； (b)若不是，将 Q 个用户按距离排序，选择距离最近的 $K_{\max}^{\mathrm{opt}}$ 个用户进行服务。

4.1　系统对窃听者密度的鲁棒性

当请求接入用户数过多时要根据 $K_{\max}^{\mathrm{opt}}$ 进行用户调度，而 $K_{\max}^{\mathrm{opt}}$ 的大小与系统参数以及小区内窃听者密度有关。如果窃听者密度已知，则可以离线计算出 $K_{\max}^{\mathrm{opt}}$ 的大小，然后将请求接入用户按到基站距离进行升序排列，选择前 $K_{\max}^{\mathrm{opt}}$ 个接入系统，这极大地降低了调度策略的复杂度。然而基站已知窃听者密度这一假设在实际中很难实现。图 4 显示了不同接入用户数时窃听者密度对用户通信安全性能的影响。如图 4 所示，当接入用户数较少时，窃听者密度变化对通信安全性能影响比较显著，因此需要施加其他的安全技术来保障安全通信。当接入用户数增多时，窃听者密度变化对安全性能影响逐渐变小，且安全性能较高，无需任何安全技术即可实现安全通信。同时当用户数高于 $K_{\max}^{\mathrm{opt}}$ 时，窃听者密度变化的影响已经可以忽略不计，因此可以作为一个已知量，来进行 $K_{\max}^{\mathrm{opt}}$ 的离线计算。

4.2　*N* 波束加扰策略性能分析

当用户数低于 $K_{\max}^{\mathrm{opt}}$ 时，仅靠系统的天然安全增益无法满足用户安全通信的需求，此时需要使用空域加扰来提高用户通信的安全性能，加扰波束的数量可以根据用户的安全需求以及系统状态来决定。图 5 显示了当用户数较少时，无加扰波束、传统零空间均匀加扰和本文所提方案的系统安全速率变化曲线。从图中可以看出，当不发送加扰波束时，用户的可达安全速率下界低于门限值，不满足用户的安全需求。此时，利用本文所提方案，发送 N 个加扰波束，即可实现通信安全。当用户数高于 $K_{\max}^{\mathrm{opt}}$ 时，系统天然安全增益可以满足安全需求，无需任何安全技术。结合 4.1 节的结论，随着用户数提升，系统对窃听者密度的鲁棒性增强，此时可以根据系统参数及门限值 R_{th} 离线的计算出 $K_{\max}^{\mathrm{opt}}$ 和加扰波束数量 N 的经验值。传统方案多不考虑系统的天然安全增益，利用系统冗余的自由度和功率在用户信道零空间均匀加扰，通过控制功率分配系数来达到最佳的系统安全性能。该做法的确可以为系统带来更高

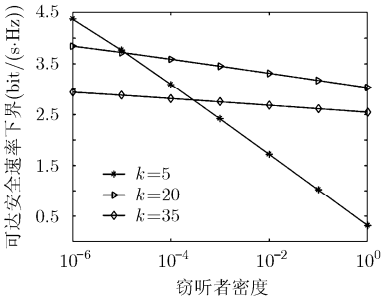

图 4 窃听者密度对用户可达平均安全速率的影响

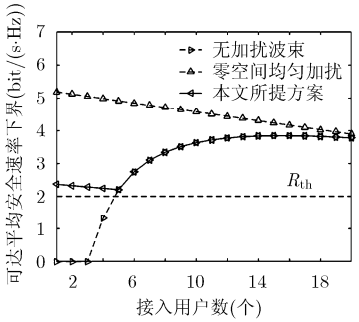

图 5 加扰波束数量对用户可达安全速率的影响

的平均安全速率，但是大量的功率被用来发射干扰，造成系统的平均安全能效较低，如图 6 所示。本文所提方案根据用户需求和系统状态，在利用系统天然安全增益的基础上发送定量的干扰，可以实现较高的功率效率。

4.3 安全调度策略性能分析

图 7 给出了当请求接入用户数高于 $K_{\max}^{\rm opt}$ 时，不使用安全调度策略、使用随机调度和本文所提基于位置的调度策略的系统平均安全能效。如图 7 所示，当不进行用户调度，仅靠系统天然安全增益时，受平均自由度的限制，系统平均安全能效随接入用户数增加而减小，当请求接入用户数高于发射天线数时，平均安全能效变为零。而传统方案由于不考虑系统天然安全增益，平均安全能效一直处于较低水平，特别是当用户数接近发射天线数时，系统冗余自由度减少，加扰效果降低，系统安全能效趋于零。若使用调度策略，由于瞬时 CSI 的影响降低，大规模 MIMO 系统多使用随机调度策略，即随机的调度 $K_{\max}^{\rm opt}$ 个用户接入系统，此时系统能够维持无调度策略时的安全能效最优情况。而使用本文所提调度策略时，从请求接入用户集合中选取距离基站最近的 $K_{\max}^{\rm opt}$ 个用户接入系统，减少了用户信号的路径损耗，可以获得更高的安全能效，并且随着备选用户数的增多，系统的平均安全能效会持续上升，为系统带来了更高的功率效率。

5 结束语

本文主要研究了配备大规模 MIMO 的基站下行并发信号对系统安全性能的影响。研究表明，基站端通过适当的预编码，可以在消除合法用户间干扰的同时对潜在的窃听者造成多路信息相互干扰的效果，该安全效果寄生于系统正常通信之中，是大规模 MIMO 的天然内生安全。之后通过分析用户的可达平均安全速率和系统的平均安全能效，针对系统内生安全能力不足的情况，提出了相应的安全传输策略。仿真结果表明，所提安全传输策略可以在保证用户安全通信的同时提高系统的功率效率。

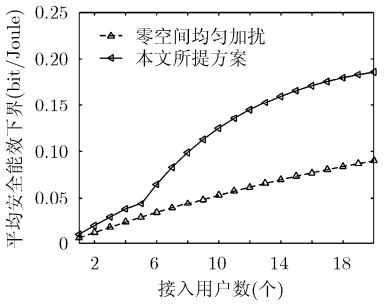

图 6 安全能效对比

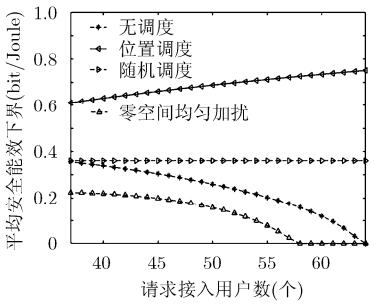

图 7 安全调度策略对系统安全能效的影响

参 考 文 献

[1] RUSEK F, PERSSON D, LAU B K, *et al*. Scaling up MIMO: Opportunities and challenges with very large arrays[J]. *IEEE Signal Processing Magazine*, 2013, 30(1): 40–60. doi: 10.1109/MSP.2011.2178495.

[2] ZHU Jun, SCHOBER R, and BHARGAVA V K. Secure transmission in multicell massive MIMO systems[J]. *IEEE Transactions on Wireless Communications*, 2014, 13(9): 4766–4781. doi: 10.1109/TWC.2014.2337308.

[3] ZHU Jun, SCHOBER R, and BHARGAVA V K. Linear precoding of data and artificial noise in secure massive MIMO systems[J]. *IEEE Transactions on Wireless Communications*, 2016, 15(3): 2245–2261. doi: 10.1109/TWC.2015.2500578.

[4] ZHU Jun and WEI Xu. Securing massive MIMO via power scaling[J]. *IEEE Communications Letters*, 2016, 20(5): 1014–1017. doi: 10.1109/LCOMM.2016.2532328.

[5] ZHONG Zhihao, PENG Jianhua, HUANG Kaizhi, *et al*. Secrecy spectrum and secrecy energy efficiency in massive MIMO enabled hetnets[J]. *KSII Transactions on Internet & Information Systems*, 2017, 11(2): 628–649. doi: 10.3837/tiis.2017.02.002.

[6] KRIKIDIS I and OTTERSTEN B. Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling[J]. *IEEE Signal Processing Letters*, 2013, 20(2): 141–144. doi: 10.1109/LSP.2012.2234109.

[7] CHEN Xiaoming and ZHANG Yu. Mode selection in MU-MIMO downlink networks: A physical-layer security perspective[J]. *IEEE Systems Journal*, 2017, 11(2): 1128–1136. doi: 10.1109/JSYST.2015.2413843.

[8] DENG Yansha, WANG Lifeng, WONG K K, *et al*. Safeguarding massive MIMO aided hetnets using physical layer security[C]. Wireless Communications & Signal Processing, Nanijing, China, 2015: 1–5. doi: 10.1109/WCSP.2015.7341120.

[9] ZHAO Long, ZHENG Kan, LONG Hang, *et al*. Performance analysis for downlink massive MIMO system with ZF precoding[J]. *Transactions on Emerging Telecommunications Technologies*, 2014, 25(12): 1219–1230. doi: 10.1002/ett.2745.

[10] 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.

[11] OGGIER F and HASSIBI B. The secrecy capacity of the MIMO wiretap channel[J]. *IEEE Transactions on Information Theory*, 2011, 57(8): 4961–4972. doi: 10.1109/TIT.2011.2158487.

[12] BJORNSON E, SANGUINETTI L, HOYDIS J, *et al*. Designing multi-user MIMO for energy efficiency: When is massive MIMO the answer?[C]. Wireless Communications and Networking Conference, Istanbul, Turkey, 2014: 242–247. doi: 10.1109/WCNC.2014.6951974.

[13] MARZETTA T L. Noncooperative cellular wireless with unlimited numbers of base station antennas[J]. *IEEE Transactions on Wireless Communications*, 2010, 9(11): 3590–3600. doi: 10.1109/TWC.2010.092810.091092.

[14] LIU Haijing, GAO Hui, YANG Shaoshi, *et al*. Low-complexity downlink user selection for massive MIMO systems[J]. *IEEE Systems Journal*, 2017, 11(2): 1072–1083. doi: 10.1109/JSYST.2015.2422475.

[15] HE Anqi, WANG Lifeng, ELKASHLAN M, *et al*. Spectrum and energy efficiency in massive MIMO enabled hetnets: A stochastic geometry approach[J]. *IEEE Communications Letters*, 2015, 19(12): 2294–2297. doi: 10.1109/LCOMM.2015.2493060.

金　梁：男，1969年生，教授，博士生导师，研究方向为移动通信技术、阵列信号处理、物理层安全.

宋昊天：男，1993年生，硕士，研究方向为移动通信、物理层安全.

钟　州：男，1982年生，讲师，研究方向为移动通信、物理层安全.

许晓明：男，1988年生，助理研究员，研究方向为移动通信、物理层安全.