人工噪声策略的临界信噪比和功率分配研究

邓浩[1]，王慧明[2]
（1. 河南大学物理与电子学院，河南 开封 450004；2. 西安交通大学电子与信息工程学院，陕西 西安 710049）

摘 要：给出了多输入单输出窃听链路中人工噪声策略安全性能的统一分析。通过对私密信号和人工噪声之间最优功率分配的研究，发现人工噪声策略不是在所有情况下都能有效提升系统的安全性，同时给出了人工噪声工作的临界信噪比。此外，基于保密速率的下界得出了适应任意信噪比的功率分配表达式，据此推导出了未知窃听用户统计信道信息情况下的功率分配结果。仿真结果显示，相对于平均功率分配策略，所提功率分配方案可以有效增大系统的保密速率。

关键词：物理层安全；人工噪声；保密速率；最优功率分配
中图分类号：TN919.3
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019114

Research on critical SNR and power allocation of artificial noise assisted secure transmission

DENG Hao[1], WANG Huiming[2]
1. School of Physics and Electronics, Henan University, Kaifeng 450004, China
2. School of Electronics and Information Engineering , Xi'an Jiaotong University, Xi'an 710049, China

Abstract: A comprehensive performance analysis of artificial noise (AN) assisted secure transmission in multiple-input single-output (MISO) wiretap channels was presented. It was shown that the AN scheme did not always improve the security, and provided an exact signal-to-noise ratio (SNR) threshold below which AN did not work. An explicit result of the optimal power allocation (OPA) using the lower bound to the ergodic secrecy rate (ESR) was presented and the OPA for the worst case without the knowledge of the eavesdropper's relative distance was also provided. Simulations demonstrate that the proposed power allocation result achieves a higher ESR than the equal one.

Key words: physical layer security, artificial noise, secrecy rate, optimal power allocation

1 引言

随着移动无线通信技术及应用领域的快速演进和拓展，由无线广播的固有特性引发的窃听问题日趋凸显，使安全问题成为了制约其发展的重要瓶颈之一。众所周知，无线信号在传输过程中，一方面要经历无线信道畸变带来的衰落，另一方面在接收机端还会受到噪声的影响，这意味着合法无线链路和窃听无线链路之间存在着很大的差异性。具体而言，这种差异性最典型的体现就是合法用户端和窃听用户端获得的接收信噪比不同。那么，如何利用信道之间的差异性来保障无线通信系统的安全，现有的物理层安全研究在一定程度上给出了答案。

物理层安全的出发点是利用无线信道的随机性和差异性保障无线信号的安全传输，随之而来的一系列信号处理技术均是利用无线通信的空域资源最大化主信道和窃听信道之间的差异性[1]，其中，

收稿日期：2018–12–26；**修回日期**：2019–04–15
基金项目：国家自然科学基金资助项目（No.61640005, No.61671364）；陕西省青年科技新星基金资助项目（No. 2015KJXX-01）
Foundation Items: The National Natural Science Foundation of China (No.61640005, No.61671364), The Young Talent Support Fund of Science and Technology of Shaanxi Province (No.2015KJXX-01)

人工噪声策略因不需要窃听用户信道信息的特性，在多输入多输出（MIMO, multiple-input multiple-output）安全传输中得到了广泛关注。人工噪声策略首次由 Goel 等[2]在 2008 年提出，其基本思路为基站首先采用波束成形技术对发射的私密信号进行聚焦，来降低私密信号能量在非期望方向的泄露，同时在主信道的正交方向发送人工噪声以干扰窃听用户。需要指出的是，在主信道以外的其他方向以相同功率发送各向同性人工噪声显然不是最优的策略。Lin 等[3]指出通过联合优化设计私密信号与人工噪声的协方差矩阵，在主信道方向上也发射人工噪声反而可以额外提升保密速率。吉江等[4]证明了人工噪声服从高斯分布时系统达到了最大保密容量。在安全中断约束条件下，Wang 等[5]证明了零空间发射人工噪声是最优策略。

不同于基于人工噪声的安全传输策略，Li 等[6]开辟了利用天线阵列冗余的另一条思路，即通过随机选择各发射天线的权系数，使合法接收端等效信道在一个数据帧内保持不变，而窃听用户的等效信道则随着码元变换而快速变化，因此称这种方法为人造快衰落策略；Wang 等[7]首次从理论上给出了人造快衰落策略的可达保密速率，并剖析了人造快衰落策略和基于人工噪声的安全传输策略各自的优劣。

由于发射人工噪声需要消耗系统的部分功率，在系统功率受限的情况下，人工噪声和私密信号之间的最优功率分配是一个重要问题，并得到了广泛研究[3,5,7-16]。大部分研究者主要从各态历经保密速率（ESR, ergodic secrecy rate）[3,8,10-13]和安全中断概率[5,9,14]这 2 个角度分析人工噪声策略在不同场景下的最优功率分配问题。在信道信息不理想的情况下，如信道估计有误差或主信道存在相关性等情况下，人工噪声策略的安全性也得到了部分研究者的关注[14-16]。需要指出的是，上述最优功率分配的结果都基于已知窃听用户瞬时信道信息或统计信道信息的假设，但实际上很难获取静默窃听用户的信道信息，甚至无法确定窃听用户的存在。当发射端如基站无法知晓窃听用户信道信息时，上述最优功率分配结果将不再适用。显然，这种情况下的功率分配依然是一个需要研究的问题，更重要的是，部分研究者[9-11]指出，当通信系统工作在低信噪比时，人工噪声策略会失效。也就是说，在低信噪比区域，人工噪声策略将不是最优的策略，因此，存在一个临界信噪比，当接收信噪比低于临界值时，人工噪声策略不再有效，而这个临界值尚未在研究文献中得到全面讨论和分析。当然这并不意味着，当系统工作在低信噪比区域时，就不存在提升安全性的物理层技术。此时，通过波束成形[11]/预编码[17]、天线选择[18]、定向调制[19]等信号处理技术或利用多用户增益[20]改善合法用户端的接收信噪比，同样可以有效保障无线通信系统的安全性。此外，很多文献中的信道模型都没有考虑大尺度衰落。一般情况下，合法接收用户和窃听用户的大尺度衰落有很大差异，所接收的信噪比也会有很大的差异，这显然会严重影响人工噪声策略的性能。针对相对距离对人工噪声安全性能的影响，也较少有文献给出系统的分析。

在移动通信系统中，基站一般都配置多天线，而由于体积及成本的限制，移动终端大多配置单天线，因此移动通信系统是一种典型的 MISO（multipe-input single-output）场景。本文选择 MISO 窃听信道作为研究对象，给出了人工噪声策略的统一性能分析。首先，本文推导了人工噪声工作的临界信噪比，并展开了定性分析，讨论了系统可达保密速率不为零的条件；然后，在人工噪声策略的情况下，给出了已知窃听用户统计信道信息和未知信道信息这 2 种情况下最优功率分配的明确表达式；最后，采用蒙特卡洛仿真证实了本文的理论结果。

2　系统模型和问题描述

假设 MISO 窃听链路包括一个配置 $N_{\mathrm{t}} \geqslant 2$ 根天线的基站、一个配置单天线的合法用户和一个配置单天线窃听用户。基站至合法用户及窃听用户的信道分别建模为 $r_{\mathrm{D}}^{-\frac{c}{2}}\boldsymbol{h} \in \mathbb{C}^{N_{\mathrm{t}}\times 1}$ 和 $r_{\mathrm{E}}^{-\frac{c}{2}}\boldsymbol{g} \in \mathbb{C}^{N_{\mathrm{t}}\times 1}$，其中，$r_{\mathrm{D}}$ 和 r_{E} 分别表示合法用户与窃听用户和基站之间的距离；$\boldsymbol{h}$ 和 $\boldsymbol{g}$ 分别表示基站至合法用户和窃听用户之间的小尺度衰落信道向量且均服从复高斯分布 $\mathrm{CN}(\boldsymbol{0}, \boldsymbol{I}_{N_{\mathrm{t}}})$；常数 c 表示路径衰减因子，取值一般在 2~4 之间。不失一般性，假设系统中所有节点的噪声是均值为 0 和方差为 δ^2 的复高斯白噪声。

在物理层安全的研究中，通常假设系统已知窃听用户的统计信道信息，甚至是瞬时信道信息，但对一个静默的窃听用户而言，由于不会发射任何信号，因此很难估计其瞬时信道信息。由于本文主要研究相对距离对人工噪声安全性能的影响关系，故先假设已知窃听用户的统计信道信息，同时也考虑

未知窃听用户统计信道信息情况下的最优功率分配问题。当窃听用户的统计信道信息已知时，移动通信系统可以得到合法用户和窃听用户相对距离的先验知识，描述该相对距离的指标定义为 $\theta \triangleq \left(\frac{r_{\mathrm{E}}}{r_{\mathrm{D}}}\right)^{-c}$。显然，当$\theta>1$时，意味着窃听用户到基站的距离比合法用户到基站的距离更近，窃听用户可以获得来自基站更高的接收信噪比；反之，当$\theta<1$时，合法用户距离基站更近，能获得来自基站更高的接收信噪比。

如前所述，人工噪声策略的基本思想就是利用多天线带来的空域自由度选择性地干扰潜在窃听用户，同时通过波束成形构建一个最佳的合法用户等效信道。由于发射私密信号权向量的改变不会影响窃听用户接收信噪比的大小，最佳的波束成形权向量必然是主信道的信道方向向量；由于不知晓窃听用户的瞬时信道信息，则人工噪声权矩阵无法利用此信道信息进行优化设计，在不干扰合法用户的前提下，该权矩阵应该由主信道的零空间生成。由此可知，人工噪声策略的发射信号为[8,11-12]

$$\boldsymbol{x}=\sqrt{P\alpha}\boldsymbol{w}s+\sqrt{P\beta}\boldsymbol{F}\boldsymbol{z} \tag{1}$$

其中，s表示待发射的私密信号且平均功率满足$\mathbb{E}\{|s|^2\}=1$；$\boldsymbol{w}=\frac{\boldsymbol{h}}{\|\boldsymbol{h}\|}$表示信号波束成形向量；$\boldsymbol{z}\in\mathbb{C}^{(N_{\mathrm{t}}-1)\times 1}$表示待发射的人工噪声向量且服从复高斯分布$\mathrm{CN}(\boldsymbol{0},\boldsymbol{I}_{N_{\mathrm{t}}-1})$，$\boldsymbol{F}\in\mathbb{C}^{N_{\mathrm{t}}\times(N_{\mathrm{t}}-1)}$表示人工噪声权矩阵，由于人工噪声不能干扰合法用户，显然其必须满足$\boldsymbol{h}^{\mathrm{H}}\boldsymbol{F}=\boldsymbol{0}$；参数$\alpha$和$\beta$分别表示分配给私密信号和每一个正交方向上人工噪声的功率比例系数，且满足$\beta=\frac{1-\alpha}{N_t-1}$，则人工噪声总的功率分配比例为$1-\alpha$。在上述信号设计策略下，式(1)中的发射信号$\boldsymbol{x}$的功率满足$\mathbb{E}\{\|\boldsymbol{x}\|^2\}=P$。从式(1)可以看出，每一根发射天线上的信号既包括私密信号，也包括人工噪声。经过信道传输后，合法用户和窃听用户的接收信号分别表示为

$$y_{\mathrm{D}}=\sqrt{P\alpha}r_{\mathrm{D}}^{-\frac{c}{2}}\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}s+n_{\mathrm{D}} \tag{2}$$

$$y_{\mathrm{E}}=\sqrt{P\alpha}r_{\mathrm{E}}^{-\frac{c}{2}}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}s+\sqrt{P\beta}r_{\mathrm{E}}^{-\frac{c}{2}}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{F}\boldsymbol{z}+n_{\mathrm{E}} \tag{3}$$

其中，n_{D}，n_{E}分别表示合法用户和窃听用户服从均值为0和方差为δ^2的高斯白噪声。由式(2)和式(3)可知，合法用户和窃听用户的接收信噪比为

$$\begin{aligned}\Gamma_{\mathrm{D}}&=\rho\alpha X,\\ \Gamma_{\mathrm{E}}&=\frac{\rho\theta\alpha Y}{\rho\theta\beta Z+1}\end{aligned} \tag{4}$$

其中，为表示方便，分别定义$\rho\triangleq\frac{Pr_{\mathrm{D}}^{-c}}{\delta^2}$，$X\triangleq\|\boldsymbol{h}\|^2$，$Y\triangleq\|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\|^2$和$Z\triangleq\|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{F}\|^2$。因信道矢量$\boldsymbol{h}$和$\boldsymbol{g}$中的元素均为复高斯变量，则有$X\sim\chi^2_{2N_t}$，$Y\sim\chi^2_2$，$Z\sim\chi^2_{2(N_t-1)}$，其中，$\chi^2_{2N}$表示自由度为$2N$的卡方分布。

由于窃听用户的瞬时信道信息未知，本文利用各态历经保密速率作为人工噪声策略安全性能的衡量指标。基于文献[11]关于ESR的定义，人工噪声策略的可达各态历经保密速率为

$$R_s=\left\{\mathbb{E}\left[\log(1+\rho\alpha X)\right]-\mathbb{E}\left[\log\left(1+\frac{\rho\theta\alpha Y}{1+\rho\theta\beta Z}\right)\right]\right\}^+ \tag{5}$$

其中，非线性运算符$\{\cdot\}^+$定义为$\{\cdot\}^+=\max(0,\cdot)$，$\mathbb{E}(x)$表示随机变量$x$的期望。若无特殊说明，本文采用的对数底为自然数e。

本文接下来的目标就是寻找最优的功率分配因子α^*，以使系统获得最大的ESR（ergodic secrecy rate）。由式(5)可知，最优功率分配α^*的值依赖于统计信道信息，一旦发射天线数和相对距离确定，便可以得到α^*的具体值。在每一次信道实现时，都以该固定比例在私密信号和人工噪声之间分配功率。需要注意的是，最优的功率分配结果包含2种特殊情况，具体如下。

1) $\alpha^*=1$，由窃听用户的接收信噪比可知，在发射功率很小时，若$\rho\to 0$，则$\rho\theta\beta Z\ll 1$成立，故满足$\rho\theta\beta Z+1\approx 1$，此时人工噪声无法对窃听用户产生干扰，显然最佳的策略是将所有的功率全部用于发射私密信号，也就是说此时不发射人工噪声是最优的选择。

2) $\alpha^*=0$，这种情况下分配给私密信号的最优功率为0，说明此时系统无法获得正的保密速率，即系统无法实现安全通信。因此，当满足$0<\alpha^*<1$时，发射人工噪声有益于安全通信。

3 人工噪声策略的工作临界信噪比及安全通信的存在条件

本节将会证实人工噪声策略并不是在所有情况下都能提升系统的可达各态历经保密速率，并给出了人工噪声策略的临界信噪比。此外，还将讨论

系统达到正保密速率的条件。

令 $R' \triangleq \dfrac{\partial R_s}{\partial \alpha}$ 及 $R'' \triangleq \dfrac{\partial^2 R_s}{\partial \alpha^2}$，具体表达式为

$$R' = \mathbb{E}\left[\frac{\rho X}{1+\rho\alpha X}\right] - \frac{1}{N_{\mathrm{t}}-1}\mathbb{E}\left[\frac{\rho\theta Z}{1+\rho\theta\beta Z}\right] - \mathbb{E}\left[\frac{\rho\theta Y - \dfrac{\rho\theta Z}{N_{\mathrm{t}}-1}}{1+\rho\theta\beta Z+\rho\theta\alpha Y}\right] \tag{6}$$

$$R'' = -\mathbb{E}\left[\frac{(\rho X)^2}{(1+\rho\alpha X)^2}\right] - \frac{1}{(N_{\mathrm{t}}-1)^2}\cdot \mathbb{E}\left[\frac{(\rho\theta Z)^2}{(1+\rho\theta\beta Z)^2}\right] - \mathbb{E}\left[\frac{(\rho\theta Z)^2+(\rho\theta Y)^2}{(1+\rho\theta\alpha Y+\rho\theta\beta Z)^2}\right] \tag{7}$$

由式(7)可知，R_s 是关于变量 α 的上凸函数，因此，系统保密速率 R_s 一定在区间 $[0,1]$ 内有最大值。显然，当满足 $R'|_{\alpha=1} \geqslant 0$ 时，R_s 在区间 $[0,1]$ 内随着 α 的增大而增大，则最大的保密速率在 $\alpha^* = 1$ 时获得。如前文所述，这种情况下人工噪声策略会失效，由此可知满足不等式 $R'|_{\alpha=1} \geqslant 0$ 的信噪比的解则为人工噪声策略工作的临界信噪比。而当满足 $R'|_{\alpha=0} \leqslant 0$ 时，R_s 在区间 $[0,1]$ 内是变量 α 的单调递减函数，则最大的保密速率在 $\alpha^* = 0$ 时获得，在这种情况下，系统无法达到正的保密速率，由 $R'|_{\alpha=0} \leqslant 0$ 可以得到系统安全通信的存在条件。3.1 节和 3.2 节将具体研究上述 2 种情况。当同时满足 $R'|_{\alpha=0} > 0$ 和 $R'|_{\alpha=1} < 0$ 时，最优功率分配因子满足 $0 < \alpha^* < 1$，此时发射人工噪声可以提升系统的安全性，对应的最优功率分配结果将在第 4 节进行讨论。

3.1　人工噪声工作临界信噪比

令 $\Delta_1(\rho) \triangleq R'|_{\alpha=1}$，经过化简可知最优功率分配解为 $\alpha^* = 1$ 的条件为

$$\Delta_1(\rho) = \mathbb{E}\left[\frac{1+\rho\theta}{1+\rho\theta Y}\right] - \mathbb{E}\left[\frac{1}{1+\rho X}\right] - \rho\theta \geqslant 0 \tag{8}$$

根据式(18)，人工噪声策略工作临界信噪比的求解可由定理 1 给出。

定理 1　当满足 $N_{\mathrm{t}} \leqslant \theta$ 时，临界信噪比满足 $\rho_0 = 0$，即人工噪声策略始终提升了系统的保密速率；当满足 $N_{\mathrm{t}} > \theta$ 时，临界信噪比是方程 $\Delta_1(\rho) = 0$ 的唯一非零解，如式(9)所示。

$$\Delta_1(\rho) = \frac{1+\rho\theta}{\rho\theta}\mathrm{e}^{\frac{1}{\rho\theta}}E_1\left(\frac{1}{\rho\theta}\right) - \frac{1}{\rho}\mathrm{e}^{\frac{1}{\rho}}E_{N_{\mathrm{t}}}\left(\frac{1}{\rho}\right) - \rho\theta \tag{9}$$

其中，$E_k(x) = \int_1^\infty \dfrac{\mathrm{e}^{-xt}}{t^k}\mathrm{d}t$ 表示指数积分函数。

证 明　首先将 $\Delta_1(\rho)$ 改写为 $\Delta_1(\rho) \triangleq \Delta_{11}(\rho) - \Delta_{12}(\rho)$ 的形式，$\Delta_{11}(\rho)$ 和 $\Delta_{12}(\rho)$ 的表达式分别为

$$\Delta_{11}(\rho) \triangleq \mathbb{E}\left[\frac{1+\rho\theta}{1+\rho\theta Y}\right] - \rho\theta$$

$$\Delta_{12}(\rho) \triangleq \mathbb{E}\left[\frac{1}{1+\rho X}\right] \tag{10}$$

则方程 $\Delta_1(\rho) = 0$ 的解为曲线 $\Delta_{11}(\rho)$ 和 $\Delta_{12}(\rho)$ 的交点。求 $\Delta_{11}(\rho)$ 和 $\Delta_{12}(\rho)$ 关于变量 ρ 的一阶偏导数可得

$$\frac{\partial\Delta_{11}(\rho)}{\partial\rho} = \theta\left(\mathbb{E}\left[\frac{1}{1+\rho\theta Y}\right]-1\right) - \mathbb{E}\left[\frac{\theta y(1+\rho\theta)}{(1+\rho\theta Y)^2}\right] \leqslant 0$$

$$\frac{\partial\Delta_{12}(\rho)}{\partial\rho} = -\mathbb{E}\left[\frac{X}{(1+\rho X)^2}\right] \leqslant 0 \tag{11}$$

式(11)证实了 $\Delta_{11}(\rho)$ 和 $\Delta_{12}(\rho)$ 是关于变量 ρ 的递减函数。又因式 $\Delta_{11}(\rho=\infty) = -\infty < \Delta_{12}(\rho=\infty) = 0$ 和式 $\Delta_{11}(\rho=0) = \Delta_{12}(\rho=0) = 1$ 成立，说明：1)曲线 $\Delta_{11}(\rho)$ 和 $\Delta_{12}(\rho)$ 在 $\rho = 0$ 时相交；2) 如果曲线 $\Delta_{11}(\rho)$ 和 $\Delta_{12}(\rho)$ 在 $\rho > 0$ 时存在第二个交点，必须满足 $\Delta_{11}(\rho)$ 随着变量 ρ 变小的过程中首先衰减比 $\Delta_{12}(\rho)$ 慢继而比 $\Delta_{12}(\rho)$ 快。若 $\dfrac{\partial\Delta_{12}\rho}{\partial\rho|_{\rho=0}} > \dfrac{\partial\Delta_{11}\rho}{\partial\rho|_{\rho=0}}$，即 $N_{\mathrm{t}} \leqslant \theta$ 时，$\Delta_{11}(\rho)$ 的函数值一直小于 $\Delta_{12}(\rho)$，则 $\Delta_{11}(\rho)$ 和 $\Delta_{12}(\rho)$ 仅在 $\rho = 0$ 处有唯一的交点，这证明了定理 1 的前半部分。而当 $N_{\mathrm{t}} > \theta$ 时，曲线 $\Delta_{11}(\rho)$ 和 $\Delta_{12}(\rho)$ 在 $\rho > 0$ 时有且仅存在一个交点，则方程 $\Delta_1(\rho_0) = 0$ 有唯一非零非负解。进一步对式(8)化简可得

$$\Delta_1(\rho) = \int_0^\infty \frac{(1+\rho\theta)\mathrm{e}^{-z}}{1+\rho\theta z}\mathrm{d}z - \int_0^\infty \frac{\mathrm{e}^{-x}x^{N_{\mathrm{t}}-1}}{(1+\rho x)(N_{\mathrm{t}}-1)!}\mathrm{d}x - \rho\theta =$$

$$\frac{1+\rho\theta}{\rho\theta}\mathrm{e}^{\frac{1}{\rho\theta}}E_1\left(\frac{1}{\rho\theta}\right) - \int_0^\infty \frac{\mathrm{e}^{-x}x^{N_{\mathrm{t}}-1}}{\rho(N_{\mathrm{t}}-1)!}\mathrm{d}\ln(1+\rho x) - \rho\theta \overset{(a)}{=}$$

$$\frac{1+\rho\theta}{\rho\theta}\mathrm{e}^{\frac{1}{\rho\theta}}E_1\left(\frac{1}{\rho\theta}\right) + \int_0^\infty \frac{\ln(1+\rho x)\mathrm{e}^{-x}x^{N_{\mathrm{t}}-2}}{\rho(N_{\mathrm{t}}-2)!}\mathrm{d}x - \int_0^\infty \frac{\ln(1+\rho x)\mathrm{e}^{-x}x^{N_{\mathrm{t}}-1}}{\rho(N_{\mathrm{t}}-1)!}\mathrm{d}x - \rho\theta \overset{(b)}{=}$$

$$\frac{1+\rho\theta}{\rho\theta}\mathrm{e}^{\frac{1}{\rho\theta}}E_1\left(\frac{1}{\rho\theta}\right) - \frac{1}{\rho}\mathrm{e}^{\frac{1}{\rho}}E_{N_{\mathrm{t}}}\left(\frac{1}{\rho}\right) - \rho\theta \tag{12}$$

其中，步骤(a)利用了分部积分，步骤(b)来自文献[21]中式(21)的结果。证毕。

定理 1 仅证明了当 $\rho > \rho_0$ 时，基站发射人工噪声才能提升系统的保密速率。虽然定理 1 没有给出临界信噪比 ρ_0 的具体表达式，但由定理 1 的证明过程可知，$\Delta_1(\rho)$ 和 $\Delta_2(\rho)$ 均是关于变量 ρ 的减函数，则很容易通过二分法得到 ρ_0 的数值解。如 $\frac{r_{\mathrm{E}}}{r_{\mathrm{D}}}=2$，即当窃听用户到基站的距离是合法用户到基站距离的 2 倍时，假设路径衰减因子为 $c=3.5$，则基站天线数为 8 和 16 这 2 种情况下的临界信噪比均约为 $\rho_0 \approx 12\ \mathrm{dB}$。这验证了在某些场景中，即便在一般信噪比时，人工噪声策略就失效了。由 $\rho \triangleq \frac{P r_{\mathrm{D}}^{-c}}{\delta^2}$ 定义可知，$\rho \leqslant \rho_0$ 意味着发射功率满足 $P \leqslant P_0 \triangleq \rho_0 r_{\mathrm{D}}^{c} \delta^2$，也就是说，临界信噪比决定了临界发射功率，该临界功率决定了基站是否发射人工噪声。需要指出的是，$N_{\mathrm{t}} \leqslant \theta$ 只有当满足 $\theta > 2$ 时才成立，此时窃听用户至基站的距离相对合法用户更近，其接收信噪比相对更高，故发射人工噪声可有效干扰窃听用户，从而提升系统的安全速率。此外，定理 1 既适用于大规模天线的场景，也适用于一般天线数目的场景，因此定理 1 的结论具有普适性。

3.2 安全通信的存在条件

令 $\Delta_2(\rho, N_t, \theta) \triangleq R'|_{\alpha=0}$，类似于定理 1 的证明过程，最优功率分配为 $\alpha^*=0$ 的条件为

$$\Delta_2(\rho, N_{\mathrm{t}}, \theta) = \rho N_{\mathrm{t}} - \rho\theta \mathbb{E}\left[\frac{1}{1+\frac{\rho\theta Z}{N_{\mathrm{t}}-1}}\right] = \rho N_{\mathrm{t}} - (N_{\mathrm{t}}-1)\mathrm{e}^{\frac{N_{\mathrm{t}}-1}{\rho\theta}} E_{N_{\mathrm{t}}-1}\left(\frac{N_{\mathrm{t}}-1}{\rho\theta}\right) \leqslant 0 \tag{13}$$

则系统正保密速率存在的条件为 $\Delta_2(\rho, N_{\mathrm{t}}, \theta) > 0$。利用 Jensen 不等式，可知式(13)满足

$$\Delta_2(\rho, N_{\mathrm{t}}, \theta) < \Delta_{2,\mathrm{hi}}(\rho, N_{\mathrm{t}}, \theta) = \rho N_{\mathrm{t}} + \frac{1}{1+\rho\theta} - 1 \tag{14}$$

显然，当 $\Delta_{2,\mathrm{hi}}(\rho, N_{\mathrm{t}}, \theta) < 0$ 时，必定有 $\Delta_2(\rho, N_{\mathrm{t}}, \theta) < 0$。式(14)显示当窃听用户距离基站很近且基站的发射功率较低时，系统无法保障安全通信的存在。一般而言，在 5G 通信系统或未来的移动通信系统中，基站配备了大规模天线阵列，即使边界上的用户也有较高的接收信噪比，此时基于多天线发射的零空间投影的人工噪声，即使对近距离的窃听端也有明显的抑制，人工噪声策略可以保证安全通信的存在。

4 人工噪声工作情况下的最优功率分配

如前所述，当同时满足 $R'|_{\alpha=0} > 0$ 和 $R'|_{\alpha=1} < 0$ 时，人工噪声策略可有效地提升系统的安全性能，对应的最大保密速率在 $R'=0$ 时获得。然而，很难通过求解方程 $R'=0$ 得到最优功率分配 α^* 的闭式表达式。前述已证实 R_s 是关于变量 α 的上凸函数，则 α^* 同样可以利用 ESR 的表达式通过二分法得到数值解，因此，得到一个 ESR 的闭式表达式是非常有意义的。人工噪声策略下系统的 ESR 由定理 2 给出。

定理 2 在 MISO 窃听链路中，系统可达各态历经保密速率为

$$R_s = \left\{ \mathrm{e}^{\frac{1}{\rho\alpha}} \sum_{k=1}^{N_{\mathrm{t}}} E_k\left(\frac{1}{\rho\alpha}\right) - \left(\frac{\alpha}{\beta}\right)^{N_{\mathrm{t}}-2} I_1\left(\frac{1}{\rho\theta\alpha}, \frac{\alpha}{\beta}, N_{\mathrm{t}}-2\right) \right\}^{+} \tag{15}$$

其中，$I_1(\cdot,\cdot,\cdot)$ 的表达式为

$$I_1(a,b,n) = \int_0^{\infty} \frac{\mathrm{e}^{-ax}}{(1+x)(b+x)^n} \mathrm{d}x = \begin{cases} \sum_{k=1}^{n-1} \frac{(k-1)!(-a)^{n-k-1}}{(n-1)!} + \frac{(-a)^{n-1}}{(n-1)!} \mathrm{e}^{a} E_1(a), & b=1 \\ \sum_{k=1}^{n} \frac{(-1)^{k-1}}{(1-b)^k} \mathrm{e}^{ab} I_2(a,b,k-n-1) + \frac{\mathrm{e}^{a} E_1(a)}{(b-1)^n}, & b \neq 1 \end{cases} \tag{16}$$

$I_2(\cdot,\cdot,\cdot)$ 的表达式为

$$I_2(a,b,n) = \int_b^{\infty} t^m \mathrm{e}^{-at} \mathrm{d}t = \begin{cases} \mathrm{e}^{ab} \sum_{k=0}^{n} \frac{n! b^k}{k! a^{n-k+1}}, & n \geqslant 0 \\ E_1(ab), & n=-1 \\ \frac{(-a)^{-n-1}}{(-n-1)!} \left(E_1(ab) - \mathrm{e}^{-ab} \sum_{k=0}^{-n-2} \frac{(-1)^k k!}{(ab)^{k+1}} \right), & n \leqslant -2 \end{cases} \tag{17}$$

证明 利用文献[21]中式(21)的结果，很容易推导出式(15)中第一部分。接下来，重点给出式(15)第二部分的证明。令 $T \triangleq \frac{\rho\theta\alpha Y}{1+\rho\theta\beta Z}$，其累积概率分布函数为

$$\mathrm{F}_T(t) = \mathbb{P}\{T \leqslant t\} = \mathbb{P}\left\{\rho\theta\alpha Y \leqslant t(1+\rho\theta\beta Z)\right\} = \int_0^{\frac{t(1+\rho\theta\beta z)}{\rho\theta\alpha}} \mathrm{e}^{-y} \mathrm{d}y \int_0^{\infty} \frac{\mathrm{e}^{-z} z^{N_{\mathrm{t}}-2}}{(N_{\mathrm{t}}-2)!} \mathrm{d}z = 1 - \frac{\mathrm{e}^{-\frac{t}{\rho\theta\alpha}}}{\left(1+\frac{\beta}{\alpha}t\right)^{N_{\mathrm{t}}-2}} \tag{18}$$

利用上述累积概率分布函数，可求得 $\ln(1+T)$ 的期望，如式(19)所示。

$$\mathbb{E}_T\{\ln(1+T)\}=\int_0^{\infty}\frac{1-\mathrm{F}_T(t)}{1+t}\mathrm{d}t=\left(\frac{\alpha}{\beta}\right)^{N_\mathrm{t}-2}\int_0^{\infty}\frac{\mathrm{e}^{-\frac{t}{\rho\theta\alpha}}}{(1+t)\left(\frac{\alpha}{\beta}+t\right)^{N_\mathrm{t}-2}}\mathrm{d}t=\left(\frac{\alpha}{\beta}\right)^{N_\mathrm{t}-2}I_1\left(\frac{1}{\rho\theta\alpha},\frac{\alpha}{\beta},N_\mathrm{t}-2\right)\tag{19}$$

综合上述结果，定理 2 证毕。

虽然利用上述定理可以得到最优功率分配 α^* 的数值解，但是其无法为系统的特性提供更多有益的结论。为更具体地分析相对距离对最优功率的影响，将利用 ESR 的下界给出最优功率分配的具体结果。特别需要指出的是，利用该结论可以推导出未知窃听用户统计信道信息的功率分配结果。对式(5)利用 Jensen 不等式，可得

$$R_s\geqslant R_{s,\mathrm{lo}}\triangleq\left\{\mathbb{E}\left[\ln(1+\rho\alpha X)\right]+\left[\ln(1+\rho\theta\beta Z)\right]-\ln\left(1+\rho\theta\right)\right\}^{+}\tag{20}$$

$R_{s,\mathrm{lo}}$ 关于变量 α 的一阶偏导为

$$\frac{\partial R_{s,\mathrm{lo}}}{\partial\alpha}=\mathbb{E}\left[\frac{\rho X}{1+\rho\alpha X}\right]-\frac{1}{N_\mathrm{t}-1}\mathbb{E}\left[\frac{\rho\theta Z}{1+\rho\theta\beta Z}\right]=\frac{1}{(N_\mathrm{t}-1)\beta}\mathbb{E}\left[\frac{1}{1+\rho\theta\beta Z}\right]-\frac{1}{\alpha}\mathbb{E}\left[\frac{1}{1+\rho\alpha X}\right]+\frac{1-2\alpha}{\alpha(1-\alpha)}=\frac{(N_\mathrm{t}-1)}{\rho\theta(1-\alpha)^2}\mathrm{e}^{\frac{N_\mathrm{t}-1}{\rho\theta(1-\alpha)}}E_{N_\mathrm{t}-1}\left(\frac{N_\mathrm{t}-1}{\rho\theta(1-\alpha)}\right)-\frac{1}{\rho\alpha^2}\mathrm{e}^{\frac{1}{\rho\alpha}}E_{N_\mathrm{t}}\left(\frac{1}{\rho\alpha}\right)+\frac{1-2\alpha}{\alpha(1-\alpha)}\tag{21}$$

当人工噪声策略工作时，最优的功率分配 α^* 近似为方程 $\frac{\partial R_{s,\mathrm{lo}}}{\partial\alpha}=0$ 的解。利用文献[22]中关于指数积分函数的不等式 $\frac{1}{(x+k)}<\mathrm{e}^x\,\mathrm{E}_k(x)\leqslant\frac{1}{(x+k-1)}$，式(21)可进一步得出如式(22)所示的结果。

$$\frac{1}{(1-\alpha^*)(1+\rho\theta(1-\alpha^*))}+\frac{1-2\alpha^*}{\alpha^*(1-\alpha^*)}\leqslant\frac{1}{\alpha^*+\rho(\alpha^*)^2(N_\mathrm{t}-1)}\tag{22}$$

式(22)化简可得

$$\alpha^*\geqslant\alpha^*_{\mathrm{lower}}=\frac{1}{2}-\frac{1}{2\rho(N_\mathrm{t}-1)}+\frac{1}{2\rho\theta}\tag{23}$$

式(23)给出了一个最优功率分配的下界。虽然是下界，但是从后续的仿真中看到，这个下界获得的保密速率与通过二分法搜索得到的最大保密速率几乎完全一样。这说明，$\alpha^*_{\mathrm{lower}}$ 是最优功率分配一个非常好的选择，原因在于其给出了人工噪声策略一个适应任意信噪比的功率分配的具体表达式。需要指出的是，大部分文献给出的都是低信噪比和高信噪比区域这 2 种特殊情况下的功率分配结果。观察式(23)可以得出以下 3 个结论。

1) 当 θ 变大时，即窃听用户距离基站更近时，$\alpha^*_{\mathrm{lower}}$ 变小，意味着基站应该为人工噪声分配更多的功率。

2) 当 N_t 变大时，即基站天线数增多时，$\alpha^*_{\mathrm{lower}}$ 变大，意味着基站应该为信号分配更多的功率。

3) 当 $\theta<N_\mathrm{t}-1$ 时，$\alpha^*_{\mathrm{lower}}$ 随着发射功率增大而减小；反之则随发射功率增大而增大。

其中，结论 1) 和结论 2)是非常直观的，当窃听用户距离基站更近，则窃听用户获得私密信号的接收信噪比更大，基站必然应该分配更多的功率发射人工噪声以干扰窃听用户。当基站天线数变多时，其干扰窃听用户的自由度变大，对窃听用户的干扰程度也更严重，此时选择分配更多的功率给私密信号也是非常合理的。结论 3)的重要性在于，式(23)建立了相对距离与天线数之间的桥梁，也就是说基站可以利用多天线带来的空间自由度抗衡近距离窃听用户的侦听。综合上述 3 个结论，式(23)比较系统地展示了相对距离对人工噪声策略安全性能的影响。

在式(23)的推导过程中假设 θ 已知，也就是说已知窃听用户的统计信道信息。而在窃听用户的统计信道信息无法获取时，也就是说未知 θ，此时也就无法根据式(23)中计算最优的功率分配。这种情况下最优的选择是考虑最坏的情况，即认为窃听用户的距离足够近使 $\theta\to\infty$ 成立，从而得到了未知窃听用户统计信道信息下的功率分配结果为

$$\alpha^*\geqslant\alpha^*_{\mathrm{worst}}=\frac{1}{2}-\frac{1}{2\rho(N_\mathrm{t}-1)}\tag{24}$$

文献[10-11]的结论指出，在高信噪比的情况下，平均功率分配是一个渐进最优的策略。式(24)

证实了这个结论。但是，需要指出的是，式(24)给出了比文献[10-11]更具一般性的结论。从第 5 节的仿真结果中也可看到，利用式(24)中的功率分配方案系统会获得更高的保密速率。

5 仿真结果

本节利用数值仿真结果以验证前述理论结果，假设系统中合法用户和窃听用户都经历准静态平衰落，仿真中所有的数值结果均来自 10 000 次独立蒙特卡洛实验。

图 1 是临界信噪比随相对距离变化的关系曲线，其中 $\frac{r_{\mathrm{E}}}{r_{\mathrm{D}}}$ 的范围为 $[1/2,\ 2]$。首先，从图 1 中可以看出，临界信噪比均随着 $\frac{r_{\mathrm{E}}}{r_{\mathrm{D}}}$ 的变大而增大。注意到，$\frac{r_{\mathrm{E}}}{r_{\mathrm{D}}}$ 变大意味着窃听用户距离基站的距离相对于合法用户更远，则窃听用户私密信号的接收信噪比将变小且人工噪声的干扰程度也随之下降，在这种情况下，发射人工噪声无法改善安全性能。其次，当 $\frac{r_{\mathrm{E}}}{r_{\mathrm{D}}}=2$ 时，也就是说窃听用户距离基站的距离是合法用户距离 2 倍时，当路径衰减因子 $c=2$ 时，临界信噪比 $\rho_0\approx 7$ dB；而当路径衰减因子 $c=3.5$ 时，临界信噪比 $\rho_0\approx 12$ dB。这进一步证实了在一般信噪比场景下，人工噪声策略就无法改善系统的安全性能了。最后，图 1 也验证了基站发射天线数对临界信噪比的影响，在发射功率较大时，天线数对临界信噪比的影响较小；而当发射功率较小时，天线数增大带来的功率增益的影响使得临界信噪比变大。

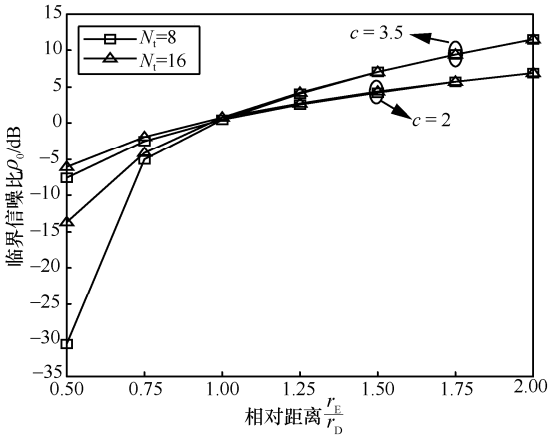


图 1 临界信噪比与相对距离的关系

为分析最优功率分配对安全性能的影响，图 2 给出了在不同功率分配策略下的保密速率曲线。其中，$c=3.5$，$N_t=4$，$r_{\mathrm{D}}=3r_{\mathrm{E}}$。图 2 中考虑了 4 种不同的功率分配策略，第一种是最优策略，即基于式(15)的二分搜索结果；第二种是式(23)给出的结果；第三种是式(24)给出的结果；第四种是文献[8,10]中给出的高信噪比情况下的平均分配策略。图 2 显示第二种和第三种策略获得的保密速率几乎完全等于最优功率分配的结果，这更充分显示了式(23)和式(24)结果的意义。同时可以看出，当基站未知窃听用户的统计信道信息时，式(24)中的功率分配可获得相对平均功率分配策略更高的保密速率。当发射信噪比变大时，上述 4 种策略的保密速率趋近于相同。分析式(23)和式(24)可知，当 $\rho\to\infty$ 时，$\alpha^*_{\mathrm{lower}}$ 和 $\alpha^*_{\mathrm{worst}}$ 均会趋近于 $\frac{1}{2}$。这再次验证了私密信号和人工噪声之间平均分配功率在高信噪比的时候是一个渐进最优的策略。所不同的是，本文的结论更具有一般性，适用于任意的信噪比和不同的相对距离关系。

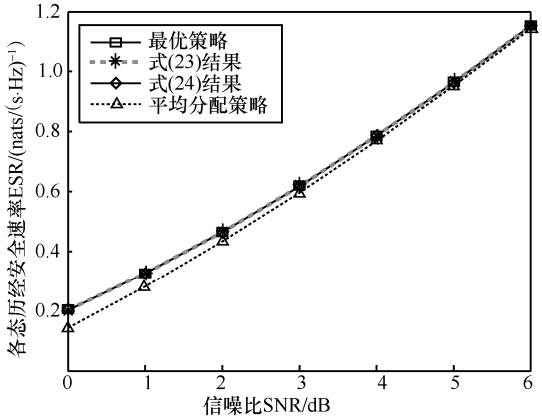


图 2 不同功率分配策略下 ESR 与信噪比的关系

6 结束语

本文研究了 MISO 信道中的安全传输问题，给出了人工噪声策略安全性能分析的统一框架，并从理论到仿真讨论了人工噪声工作的临界信噪比。研究发现，该临界信噪比受相对距离、基站发射天线数、路径衰减因子的影响，结果显示在一些场景下，甚至在一般信噪比（如 $\rho\leqslant 12$ dB）时，基站发射人工噪声都无法提升系统的保密速率。此外，本文还给出了适应任意信噪比的最优功率分配的具体表达式，并据此推导了未知窃听用户统计信道信息时的功率分配结果。仿真实验

验证了所提算法相对于平均分配策略系统可获得更高的保密速率。

参考文献:

[1] LIU Y, CHEN H H, WANG L. Physical layer security for next generation wireless networks: theories, technologies, and challenges[J]. IEEE Communications Surveys & Tutorials, 2017, 19(1): 347-376.

[2] GOEL S, NEGI R. Guaranteeing secrecy using artificial noise[J]. IEEE Transactions on Wireless Communications, 2008, 7(6): 2180-2189.

[3] LIN P H, LAI S H, LIN S C, et al. On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels[J]. IEEE Journal on Selected Areas in Communications, 2012, 31(9): 1728-1740.

[4] 吉江, 金梁, 黄开枝. 基于人工噪声的 MISO 保密容量分析[J]. 通信学报, 2012, 33(10): 138-142.
JI J, JIN L, HUANG K Z. Secrecy capacity analysis of MISO system with artificial noise [J]. Journal on Communications, 2012, 33(10):138-142.

[5] WANG B, MU P, LI Z. Artificial-noise-aided beamforming design in the MISOME wiretap channel under the secrecy outage probability constraint[J]. IEEE Transactions on Wireless Communications, 2017, 16(11): 7207-7220.

[6] LI X, HWU J, RATAZZI E P. Using antenna array redundancy and channel diversity for secure wireless transmissions[J]. Journal of Communications, 2007, 2(3): 24-32.

[7] WANG H M, ZHENG T, MU P. Secure MISO wiretap channels with multi-antenna passive eavesdropper via artificial fast fading[J]. IEEE Transactions on Wireless Communications, 2014, 14(1): 5396-5401.

[8] ZHOU X，MCKAY M R. Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation[J]. IEEE Transactions on Vehicular Technology, 2010, 59(8): 3831-3842.

[9] GERBRACHT S, SCHEUNERT C, JORSWIECK E A. Secrecy outage in MISO systems with partial channel information[J]. IEEE Transactions on Information Forensics & Security, 2012, 7(2): 704-716.

[10] DENG H, WANG H M, GUO W, et al. Secrecy transmission with a helper: to relay or to jam[J]. IEEE Transactions on Information Forensics & Security, 2014, 10(2): 293-307.

[11] TSAI S H，POOR H V. Power allocation for artificial-noise secure MIMO precoding systems[J]. IEEE Transactions on Signal Processing, 2014, 62(13): 3479-3493.

[12] YUN S, IM S, KIM I M, et al. On the secrecy rate and optimal power allocation for artificial noise assisted MIMOME channels[J]. IEEE Transactions on Vehicular Technology, 2018, 67(4): 3098-3113.

[13] LI N, TAO X, WU H, et al. Large-system analysis of artificial-noise-assisted communication in the multiuser downlink: ergodic secrecy sum rate and optimal power allocation[J]. IEEE Transactions on Vehicular Technology, 2016, 65(9): 7036-7050.

[14] ZHENG T X, WANG H M. Optimal power allocation for artificial noise under imperfect CSI against spatially random eavesdroppers[J]. IEEE Transactions on Vehicular Technology, 2016, 65(10): 8812-8817.

[15] HU J, CAI Y, YANG N, et al. Artificial-noise-aided secure transmission scheme with limited training and feedback overhead[J]. IEEE Transactions on Wireless Communications, 2017, 16(1): 193-205.

[16] YAN S, ZHOU X, YANG N, et al. Artificial-noise-aided secure transmission in wiretap channels with transmitter-side correlation[J]. IEEE Transactions on Wireless Communications, 2016, 15(12): 1536-1276.

[17] GERACI G, EGAN M, YUAN J, et al. Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding[J]. IEEE Transactions on Communications, 2012, 60(11):3472-3482.

[18] YANG N, YEOH P L, ELKASHLAN M, et al. Transmit antenna selection for security enhancement in MIMO wiretap channels[J]. IEEE Transactions on Communications, 2013, 61(1):144-154.

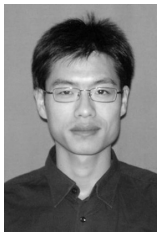
[19] HU J, YAN S, SHU F, et al. Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays[J]. IEEE Access, 2016, 5: 1658-1667.

[20] DENG H, WANG H M, YUAN J, et al. Secure communication in uplink transmissions: user selection and multiuser secrecy gain[J]. IEEE Transactions on Communications, 2016, 64(8):3492-3506.

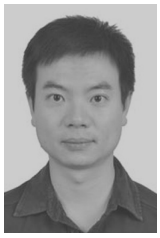
[21] SHIN H, LEE J H. Capacity of multiple-antenna fading channels: spatial fading correlation, double scattering, and keyhole[J]. IEEE Transactions on Information Theory, 2003, 49(10): 2636-2647.

[22] ABRAMOWITZ M, STEGUN I A. Handbook of mathematical functions[M]. New York: Dover Publications, 1970.

[作者简介]



邓浩（1982− ），男，湖北恩施人，博士，河南大学副教授、硕士生导师，主要研究方向为物理层安全、阵列信号处理。



王慧明（1983− ），男，江苏溧阳人，博士，西安交通大学教授、博士生导师，主要研究方向为高效安全的无线通信技术。