基于人工噪声预编码的多天线中继安全性能分析

赵 睿*①② 贺玉成①② 周 林① 谢维波①
①(华侨大学厦门市移动多媒体通信重点实验室 厦门 361021)
②(西安电子科技大学 ISN 国家重点实验室 西安 710071)

摘 要：为提升存在窃听者的中继网络的安全性能，在多天线放大转发中继端采用人工噪声预编码(ANP)和特征波束形成(EB)安全传输策略，推导了 ANP 和 EB 的可达安全速率(EASR)闭合表达式。在中继配置大规模天线时，推导了 ANP 的 EASR 下界，并在高信噪比和低信噪比情况下研究了渐近性能。分析和仿真结果显示，在中高信噪比区域，ANP 相比于 EB 可获得显著的性能增益，而在低信噪比区域，EB 优于 ANP。当信噪比增加时，EB 的 EASR 接近一个与第 1 跳无关的常数。在高信噪比区域，ANP 的最优功率分配方案是将一半左右的功率分配给人工噪声。

关键词：物理层安全；放大转发中继；人工噪声；遍历可达安全速率
中图分类号：TN92 **文献标识码**：A **文章编号**：1009-5896(2016)10-2575-07
DOI: 10.11999/JEIT160053

Secrecy Performance Analysis of Multiple-antenna Relay Systems with Artificial Noise Precoding

ZHAO Rui①② HE Yucheng①② ZHOU Lin① XIE Weibo①
①(*Xiamen Key Laboratory of Mobile Multimedia Communications*, *Huaqiao University*, *Xiamen* 361021, *China*)
②(*The State Key Laboratory of Integrated Services Networks*, *Xidian University, Xi'an* 710071, *China*)

Abstract: To improve the secrecy performance of relay networks in the presence of one eavesdropper, the Artificial Noise Precoding (ANP) and Eigen-Beamforming (EB) secure transmission schemes are appilied at the multiple-antenna amplify-and-forward relay, and the new tight closed-form expressions of the Ergodic Achievable Secrecy Rate (EASR) for two schemes are derived. The lower bound of the EASR for ANP is derived with a large antenna array at the relay, and its corresponding asymptotic performance is investigated in the high SNR and low SNR regimes to show valuable intrinsic insights. Analysis and Simulation results show that, in the moderate-to-high SNR regime, ANP achieves remarkable performance gain over EB, while in the low SNR regime, EB outperforms ANP. Moreover, in the high SNR regime, it is optimal to allocate around half of total power to artificial noise for ANP.

Key words: Physical layer security; Amplify-and-forward relay; Artificial noise; Ergodic Achievable Secrecy Rate (EASR)

1 引言

中继系统物理层安全中的物理层安全问题近年来已成为研究热点。通过利用协作中继，学者们提出了多种基于协作的策略来增强无线安全性从而对抗窃听攻击，比如：协作波束形成技术、中继选择技术和协作加扰技术(CJ)[1–7]。在多中继系统中，协作波束形成和中继选择通过合理分配中继的加权因子和发送功率，可显著提升安全容量。CJ 通过发送加扰信号(即人工噪声)显著降低了窃听者的接收 SNR，且能保证期望信号的接收质量，已成为一种高效的传输策略。

当多天线中继发送加扰信号时，中继作为辅助者使用人工噪声预编码(ANP)技术干扰窃听者，通过将人工噪声的波束方向对准合法信道的正交子空间中，将有用信号转发至目的端，从而增强安全性能[8,9]。文献[10]首次提出 ANP 技术来提升多天线发送端的典型搭线信道的安全容量。文献[11]和文献[12]提出了最优功率分配(PA)策略以最大化平均安全速率。学者们还针对特定中继系统研究了 ANP 技术的安全性能。在解码转发(DF)中继系统中，文献[8]针对已知和未知信道状态信息(CSI)两种情况

收稿日期：2016-01-13；改回日期：2016-06-20；网络出版：2016-08-26
*通信作者：赵睿 rzhao@hqu.edu.cn
基金项目：国家自然科学基金(61401165, 61302095, 61271383)，福建省自然科学基金(2015J01262, 2014J01243)
Foundation Items: The National Natural Science Foundation of China (61401165, 61302095, 61271383), The Natural Science Foundation of Fujian Province (2015J01262, 2014J01243)

分别提出了 ANP 的最优波束形成和功率分配策略。在放大转发(AF)中继系统中，文献[9]给出了遍历安全容量(ESC)和安全中断概率(SOP)的渐近性分析。在无加扰信号和存在直达目的端和窃听者链路的情况下，文献[13]分析了 AF 中继系统的安全速率可达性。然而，现有的研究没有给出当 ANP 应用在 AF 中继系统的遍历安全容量和最优 PA 解。

本文旨在探索多天线中继在保障安全通信方面的潜力，推导了包含一对收发端、一个窃听者和一个 AF 中继的两跳系统的遍历可达安全速率(EASR)表达式。考虑两种安全传输策略，ANP 和特征波束形成(EB)[14]，其中 EB 可在无加扰情况下最大化合法信道容量，可作为 ANP 方案的参考基准方案。与传统的中继策略相比，本文中的传输方案在目的端和窃听端信干噪比中引入了额外的与噪声相关的随机变量，从而增加了 EASR 闭合表达式的推导难度，也使得文献[15]中的有用信息与噪声的功率分配方案无法运用到本文系统中。本文针对任意中继天线数情况，推导了 ANP 和 EB 策略的 EASR 闭合表达式，从而极大降低了系统设计的复杂度，并揭示了 ANP 相比于 EB 的性能优势。进一步，针对大规模中继天线数情况，本文利用简化的渐近表达式推导了 ANP 策略的最优功率分配因子，采用所提功率分配方案可进一步提升 ANP 策略的 EASR 性能。

2 系统模型和安全传输策略

本节给出 ANP 和 EB 安全传输策略的系统模型和传输策略。

2.1 系统模型

考虑一个两跳 AF 中继安全通信系统，如图 1 所示，其中一对合法信源和信宿节点(A 和 B)借助一个中继 R 相互通信，同时中继 R 也需要保障所传输信息不被窃听节点 E 窃听。中继配置 N 根天线，所有其他节点均配置单天线，这种天线配置可应用在多种实际通信场景，比如两个距离相隔较远的低复杂度 D2D 或 M2M 设备借助一个高级多天线设备(如基站)相互交换信息。假设 A 与 B 之间无直达链路。由于窃听者总是试图窃听所有可能的信息，所以假设 A 与 E 之间存在直达链路。所有节点均工作在半双工模式。

所有信道均建模为 Rayleigh 衰落信道。中继和目的端可获得两跳合法信道的完全 CSI。如果 ANP 策略均采用最优功率分配以最大化遍历可达安全速率，合法节点需要获知与合法节点相关的统计 CSI，最优功率分配方案将在下文探讨。本文采用固定增益 AF 中继，可获得与可变增益中继类似的性能并使系统易于分析。A 与 R 的发送功率记为 P 和 P_{r}。A 与 R, R 与 B, R 与 E 以及 A 与 E 之间的信道分

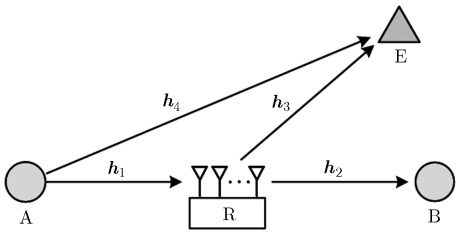

图 1 两跳多天线中继安全通信系统传输模型

别记为 $\boldsymbol{h}_1=[h_{1,1}h_{1,2}\ \cdots\ h_{1,N}]^{\mathrm{T}}$，$\boldsymbol{h}_2=[h_{2,1}\ h_{2,2}\ \cdots\ h_{2,N}]^{\mathrm{T}}$，$\boldsymbol{h}_3=[h_{3,1}\ h_{3,2}\ \cdots\ h_{3,N}]^{\mathrm{T}}$ 与 h_4，其中 $\boldsymbol{h}_1$，$\boldsymbol{h}_2$ 和 $\boldsymbol{h}_3$ 中每个元素为零均值方差为 Ω_1，Ω_2 和 Ω_3 的独立同分布(i.i.d.)复高斯随机变量，$\boldsymbol{h}_4$ 服从均值为零方差为 Ω_4 的 i.i.d.复高斯分布。信道 $\boldsymbol{h}_1$，$\boldsymbol{h}_2$，$\boldsymbol{h}_3$ 和 $\boldsymbol{h}_4$ 互相独立。信道方差 Ω_i 可进一步建模为大尺度衰落的形式，即：$\Omega_i=1/d_i^{n_i}$，其中 d_i 为距离，n_i 为大尺度衰落因子。

2.2 人工噪声预编码(ANP)

在 ANP 策略中，多天线中继节点同时发送信息信号与噪声。在第 1 时隙中，A 发送 x 至 R, R 和 E 端的接收信号可分别表示为

$$\boldsymbol{y}_{\mathrm{r}}=\sqrt{P}\boldsymbol{h}_1x+\boldsymbol{n}_{\mathrm{r}} \tag{1}$$

$$y_{\mathrm{e}}=\sqrt{P}\boldsymbol{h}_4x+n_{\mathrm{e}} \tag{2}$$

其中，x 为 i.i.d.复高斯信号，功率限制为 $\mathbb{E}[|x|^2]=P$，其中 P 为 A 的发送功率，$\boldsymbol{n}_{\mathrm{r}}$ 为 R 的加性白高斯噪声(AWGN)，且 $\mathbb{E}[\boldsymbol{n}_{\mathrm{r}}^{\mathrm{H}}\boldsymbol{n}_{\mathrm{r}}]=N_0\boldsymbol{I}_N$，$n_{\mathrm{e}}$ 为 E 的 AWGN，方差为 N_0。为了最大化中继节点的接收 SNR，中继采用最大比合并(MRC)接收方案。MRC 合并器为 $\boldsymbol{u}_1=\boldsymbol{h}_1^{\mathrm{H}}/\|\boldsymbol{h}_1\|$，其中 $\|\cdot\|$ 为欧氏范数。中继接收机的输出可表示为

$$\hat{y}_{\mathrm{r}}=\boldsymbol{u}_1\boldsymbol{y}_{\mathrm{r}}=\sqrt{P}\,\|\boldsymbol{h}_1\|x+\frac{\boldsymbol{h}_1^{\mathrm{H}}\boldsymbol{n}_{\mathrm{r}}}{\|\boldsymbol{h}_1\|} \tag{3}$$

当中继采用 ANP 策略来提升安全性能时，R 端的发送信号包含有用信息 $\hat{y}_{\mathrm{r}}$ 和人工噪声 $\boldsymbol{v}$。由于中继可获知 $\boldsymbol{h}_2$ 的全部 CSI 而无法获知 $\boldsymbol{h}_3$ 的 CSI，中继发送信号的设计可参照文献[10]，可设计如式(4)：

$$\boldsymbol{x}_{\mathrm{r}}=\boldsymbol{w}_1\tilde{y}_{\mathrm{r}}+\boldsymbol{W}_2\boldsymbol{v} \tag{4}$$

其中，$\tilde{y}_{\mathrm{r}}=\beta_1\tilde{y}_{\mathrm{r}}$，$\beta_1$ 为 AF 中继的功率放大因子，$\tilde{y}_{\mathrm{r}}$ 的方差记为 $\sigma_{\tilde{y}_{\mathrm{r}}}^2$，$\boldsymbol{w}_1$ 为发送波束形成向量，为最大化目的端接收 SNR 可设计成与第 2 跳信道 $\boldsymbol{h}_2$ 匹配，即：$\boldsymbol{w}_1=\boldsymbol{h}_2/\|\boldsymbol{h}_2\|$；$\boldsymbol{W}_2$ 为 $\boldsymbol{h}_2$ 的零空间的正交基，即：$\boldsymbol{W}_2=\mathrm{null}(\boldsymbol{w}_1)$，且 $\boldsymbol{W}_2\in\mathbb{C}^{N\times(N-1)}$；向量 $\boldsymbol{v}\in\mathbb{C}^{(N-1)\times1}$ 的每个元素为 i.i.d.复高斯随机变量，方差为 σ_v^2。ρ 为有用信息功率与总功率的比值，由于发送功率在 $N-1$ 个人工噪声元素中均分，则有 $\sigma_{\tilde{y}_{\mathrm{r}}}^2=\rho P_{\mathrm{r}}$ 和 $\sigma_v^2=\dfrac{1-\rho}{N-1}P_{\mathrm{r}}$。固定增益中继的放大因子 β_1 可计算

如下：$\beta_1^2=\rho P_{\mathrm{r}}/\left(P\mathbb{E}\left[\|\boldsymbol{h}_1\|^2\right]+\mathbb{E}\left[\boldsymbol{h}_1^{\mathrm{H}}\boldsymbol{n}_{\mathrm{r}}/\|\boldsymbol{h}_1\|\right]\right)$。在第 2 时隙，中继将信号转发给目的端。B 和 E 的接收信号为

$$y_{\mathrm{b}}=\boldsymbol{h}_2^{\mathrm{H}}\boldsymbol{x}_{\mathrm{r}}+n_{\mathrm{b}}=\beta_1\sqrt{P}\,\|\boldsymbol{h}_1\|\|\boldsymbol{h}_2\|x+\beta_1\frac{\boldsymbol{h}_1^{\mathrm{H}}\boldsymbol{n}_{\mathrm{r}}}{\|\boldsymbol{h}_1\|}\|\boldsymbol{h}_2\|+n_{\mathrm{b}} \tag{5}$$

$$\begin{aligned}y_{\mathrm{e}}&=\boldsymbol{h}_3^{\mathrm{H}}\boldsymbol{x}_{\mathrm{r}}+n_{\mathrm{e}}=\beta_1\sqrt{P}\frac{\boldsymbol{h}_3^{\mathrm{H}}\boldsymbol{h}_2}{\|\boldsymbol{h}_2\|}\|\boldsymbol{h}_1\|x\\&\quad+\beta_1\frac{\boldsymbol{h}_3^{\mathrm{H}}\boldsymbol{h}_2}{\|\boldsymbol{h}_2\|}\frac{\boldsymbol{h}_1^{\mathrm{H}}\boldsymbol{n}_{\mathrm{r}}}{\|\boldsymbol{h}_1\|}+\boldsymbol{h}_3^{\mathrm{H}}\boldsymbol{W}_2\boldsymbol{v}+n_{\mathrm{e}}\end{aligned} \tag{6}$$

其中，n_{b} 为零均值方差 N_0 的 AWGN。为最大化接收 SNR，窃听者采用 MRC 策略合并两个时隙的信号。经过代数运算 B 和 E 端的 SINR 可分别表示为

$$\gamma_{\mathrm{b,ANP}}=\frac{\beta_1^2\gamma_1 g_1 g_2}{\beta_1^2 x_1 g_2+1} \tag{7}$$

$$\gamma_{\mathrm{e,ANP}}=\frac{\beta_1^2\gamma_1 x_2 g_1}{\beta_1^2 x_1 x_2+a g_3+1}+\gamma_1 g_4 \tag{8}$$

其中，$\gamma_1=\dfrac{P}{N_0}$，$a\triangleq\dfrac{1-\rho}{N-1}\gamma_2$，$\gamma_2=\dfrac{P_{\mathrm{r}}}{N_0}$，$x_1\triangleq\dfrac{\left|\boldsymbol{h}_1^{\mathrm{H}}\boldsymbol{n}_{\mathrm{r}}\right|^2}{N_0\|\boldsymbol{h}_1\|^2}$，$x_2\triangleq\dfrac{\left|\boldsymbol{h}_3^{\mathrm{H}}\boldsymbol{h}_2\right|^2}{\|\boldsymbol{h}_2\|^2}$，$g_1\triangleq\|\boldsymbol{h}_1\|^2$，$g_2\triangleq\|\boldsymbol{h}_2\|^2$，$g_3\triangleq\left\|\boldsymbol{h}_3^{\mathrm{H}}\boldsymbol{W}_2\right\|^2$，$g_4\triangleq|h_4|^2$。因为 g_1，g_2 和 g_3 均服从伽马分布，即：$g_1\sim\Gamma(N,\Omega_1)$，$g_2\sim\Gamma(N,\Omega_2)$，$g_3\sim\Gamma(N-1,\Omega_3)$，且有 $\mathbb{E}[g_1]=N\Omega_1$，$\mathbb{E}[g_2]=N\Omega_2$，$\mathbb{E}[g_3]=(N-1)\Omega_3$。注意到 g_4 服从均值为 Ω_4 的指数分布，即：$g_4\sim\exp(1/\Omega)_4$。由于 $\boldsymbol{h}_1$，$\boldsymbol{n}_{\mathrm{r}}$，$\boldsymbol{h}_2$ 和 $\boldsymbol{h}_3$ 相互独立，x_1 服从均值为 1 的指数分布，即：$x_1\sim\exp(1)$，x_2 服从均值 Ω_3 的指数分布，即：$x_2\sim\exp(1/\Omega_3)$。因此 $\beta_1^2=\rho\gamma_2/(\gamma_1 N\Omega_1+1)$。

2.3 特征波束形成(EB)

当功率分配因子 ρ 设为 1 时，ANP 策略就成为 EB 策略(也称为 MRC/MRT)，其中中继端的接收和发送波束形成向量分别与第 1 跳信道和第 2 跳信道向量匹配，不使用干扰信号。B 和 E 端的 SINR 可表示为

$$\gamma_{\mathrm{b,EB}}=\frac{\beta_3^2\gamma_1 g_1 g_2}{\beta_3^2 x_1 g_2+1} \tag{9}$$

$$\gamma_{\mathrm{e,EB}}=\frac{\beta_3^2\gamma_1 x_2 g_1}{\beta_3^2 x_1 x_2+1}+\gamma_1 g_4 \tag{10}$$

其中，β_3 为 EB 策略的功率归一化系数，$\beta_3^2=\dfrac{\gamma_2}{\gamma_1 N\Omega_1+1}$。

在无窃听者的简单 3 节点(A，R 和 B)系统中，EB 为最优中继处理矩阵[14]，尽管在所考虑的系统中从安全性的角度来看，EB 可能不是最优的策略。ANP 策略需要相对复杂的中继端处理或 A，B 间同步，而 EB 策略仅需在中继端进行简单的预编码操作，复杂度大为降低。

3　遍历安全容量分析

在本节中，将分析 ANP 和 EB 策略的遍历安全容量。遍历安全容量定义为可达平均安全通信速率的最大值[16]，在块衰落信道中可表示为

$$\mathbb{E}[C_{\mathrm{s}}]=\mathbb{E}\left[\left[C_{\mathrm{b}}-C_{\mathrm{e}}\right]^+\right] \tag{11}$$

其中，$[x]^+\triangleq\max\{0,x\}$，$C_{\mathrm{b}}$ 与 C_{e} 分别为信源至目的端和信源至窃听端的互信息，$[C_{\mathrm{b}}-C_{\mathrm{e}}]^+$ 为安全容量。在本文模型中，C_{b} 和 C_{e} 可分别表示为 $C_{\mathrm{b}}=0.5\log_2(1+\gamma_{\mathrm{b}})$ 和 $C_{\mathrm{e}}=0.5\log_2(1+\gamma_{\mathrm{e}})$，其中 γ_{b} 和 γ_{e} 为目的端和窃听端的 SINR。然而，对于本文的传输模型，式(11)的准确闭合表达式难以获得。进而，本文关注式(11)的下界的分析，可表示为

$$\mathbb{E}[C_{\mathrm{s}}]\ge\left[\mathbb{E}[C_{\mathrm{b}}]-\mathbb{E}[C_{\mathrm{e}}]\right]^+\triangleq\overline{C}_{\mathrm{s}} \tag{12}$$

其中，下界 $\left[\mathbb{E}[C_{\mathrm{b}}]-\mathbb{E}[C_{\mathrm{e}}]\right]^+$ 记为 $\overline{C}_{\mathrm{s}}$，也称为遍历可达安全速率(EASR)，由于使用固定增益 AF 中继，EASR 与遍历安全容量式(11)相比是次优的。在下文将通过仿真验证基于式(12)所推导的 EASR 与确切的遍历安全容量式(11)是非常吻合的。接下来我们通过分析 $\mathbb{E}[C_{\mathrm{b}}]$ 和 $\mathbb{E}[C_{\mathrm{e}}]$ 来推导任意天线数情况下 ANP 和 EB 策略的 EASR 的闭合表达式。

3.1 人工噪声预编码(ANP)

对于 ANP 策略，以下引理给出了 $\mathbb{E}[C_{\mathrm{b,ANP}}]$ 的闭合表达式。

引理 1　ANP 策略下合法信道的遍历容量为

$$\mathbb{E}\left[C_{\mathrm{b,ANP}}\right]=\begin{cases}\dfrac{\beta_1^2\Omega_2}{2\Gamma(N)\ln 2}\left\{\left((1-\gamma_1\Omega_1)^{-N}-1\right)\tilde{I}-\gamma_1\Omega_1\displaystyle\sum_{m=0}^{N-1}\frac{\left((1-\gamma_1\Omega_1)^{m-N}-1\right)}{m!}\mathrm{G}_{3,1}^{1,3}\left(\beta_1^2\gamma_1\Omega_1\Omega_2\,\middle|\,\begin{matrix}-N,-m,0\\0\end{matrix}\right)\right\}, & \gamma_1\ne\dfrac{1}{\Omega_1}\\[2ex]\dfrac{\beta_1^2\Omega_2}{2\Gamma(N)\ln 2}\left\{\displaystyle\sum_{m=0}^{N-1}\frac{1}{m!}\mathrm{G}_{3,1}^{1,3}\left(\beta_1^2\Omega_2\,\middle|\,\begin{matrix}-N,-m,0\\0\end{matrix}\right)+\frac{1}{N\Gamma(N)}\mathrm{G}_{3,1}^{1,3}\left(\beta_1^2\Omega_2\,\middle|\,\begin{matrix}-N,-N,0\\0\end{matrix}\right)-\tilde{I}\right\}, & \gamma_1=\dfrac{1}{\Omega_1}\end{cases} \tag{13}$$

其中，$\mathrm{G}_{p,q}^{m,n}\left(z\middle|\begin{matrix}a_1,\ldots,a_p\\b_1,\ldots,b_q\end{matrix}\right)$ 为 Meijer's G 函数[17]，$\tilde{I}\triangleq\mathrm{G}_{3,1}^{1,3}\left(\beta_1^2\Omega_2\middle|\begin{matrix}-N,0,0\\0\end{matrix}\right)$。$\Gamma(n)=(n-1)!$ 为关于实数 n

的伽马函数。

证明过程略。

通过仔细分析发现，由于缺少式(8)的 CDF，所以无法获得 $\mathbb{E}\left[C_{\mathrm{e,ANP}}\right]=\frac{1}{2\ln 2}\mathbb{E}\left[\ln\left(1+\gamma_{\mathrm{e,ANP}}\right)\right]$ 的闭合表达式。于是我们在以下引理中给出 $\mathbb{E}\left[C_{\mathrm{e,ANP}}\right]$ 的上界表达式。

引理 2 ANP 策略下窃听信道的遍历容量的上界为

$$\begin{aligned}\mathbb{E}\left[C_{\mathrm{e,ANP}}\right]\le&\frac{1}{2\ln 2}\ln\Big(\beta_1^2\gamma_1 N\Omega_1\Omega_3+\beta_1^2\Omega_3\\&+a(N-1)\Omega_3+1+\beta_1^2\gamma_1\Omega_3\Omega_4+\gamma_1\Omega_4\\&+a\gamma_1(N-1)\Omega_3\Omega_4\Big)\\&+-\frac{1}{2\ln 2}\ln\Big(1+e^{\ln\beta_1^2-2\nu+\ln\Omega_3}\\&+e^{\ln a+\psi(N-1)+\ln\Omega_3}\Big)\end{aligned}\tag{14}$$

其中，$\nu=0.5772$ 为欧拉常数[17]，$\psi(x)$ 为欧拉 psi 函数[17](也称为 Digamma 函数)。

证明过程略。

至此，通过合并式(12)，式(13)和式(14)可得 ANP 策略的 EASR 下界的闭合表达式。

3.2 特征波束形成(EB)

将式(13)中的 β_1 替换成 β_3，并将 ρ 设置成 1，即可得 EB 策略中 $\mathbb{E}[C_{\mathrm{b}}]$ 的解析表达式。要获得 EB 中 $\mathbb{E}[C_{\mathrm{e}}]$ 的准确闭合表达式(记为 $\mathbb{E}\left[C_{\mathrm{e,EB}}\right]$)很困难，所以我们给出当 $\gamma_{\mathrm{RE}}/\gamma_{\mathrm{AE}}\to\infty$ 时 $\mathbb{E}\left[C_{\mathrm{e,EB}}\right]$ 的渐近表达式。

引理 3 当 $\gamma_{\mathrm{RE}}/\gamma_{\mathrm{AE}}\to\infty$ 时，EB 策略中窃听信道的遍历容量的下界可近似表示为

$$\mathbb{E}\left[C_{\mathrm{e,EB}}\right]\gtrsim\begin{cases}\dfrac{\beta_3^2\Omega_3}{2\ln 2}\Bigg\{\Big(\big(1-\gamma_1\Omega_1\big)^{-N}-1\Big)\hat{I}\\\quad-\displaystyle\sum_{k=0}^{N-1}\frac{\gamma_1\Omega_1\Big(\big(1-\gamma_1\Omega_1\big)^{k-N}-1\Big)}{k!}\\\quad\cdot\mathrm{G}_{3,1}^{1,3}\left(\beta_3^2\gamma_1\Omega_1\Omega_3\,\middle|\,\begin{matrix}-1,-k,0\\0\end{matrix}\right)\Bigg\},\ \gamma_1\ne\dfrac{1}{\Omega_1}\\\dfrac{\beta_3^2\Omega_3}{2\ln 2}\Bigg\{\displaystyle\sum_{k=0}^{N-1}\frac{1}{k!}\mathrm{G}_{3,1}^{1,3}\left(\beta_3^2\Omega_3\,\middle|\,\begin{matrix}-1,-k,0\\0\end{matrix}\right)\\\quad+\dfrac{1}{N\Gamma(N)}\mathrm{G}_{3,1}^{1,3}\left(\beta_3^2\Omega_3\,\middle|\,\begin{matrix}-1,-N,0\\0\end{matrix}\right)-\hat{I}\Bigg\},\\\quad\gamma_1=\dfrac{1}{\Omega_1}\end{cases}\tag{15}$$

其中，$\hat{I}\triangleq\mathrm{G}_{3,1}^{1,3}\left(\beta_3^2\Omega_3\,\middle|\,\begin{matrix}-1,0,0\\0\end{matrix}\right)$。

证明 当 $\gamma_{\mathrm{RE}}/\gamma_{\mathrm{AE}}\to\infty$，EB 策略中窃听信道的遍历容量的近似下界为

$$\mathbb{E}\left[C_{\mathrm{e,EB}}\right]\gtrsim\frac{1}{2\ln 2}\Big(\mathbb{E}\left[\ln(1+X)\right]-\mathbb{E}\left[\ln(1+Y)\right]\Big)\tag{16}$$

其中，$X\triangleq\beta_3^2x_1x_2+\beta_3^2\gamma_1x_2g_1$ 和 $Y\triangleq\beta_3^2x_1x_2$。采用类似于引理 1 的推导方法，可得式(15)。限于空间，详细推导过程省略。

结合式(12)，式(13)和式(15)可得 EB 策略在 $\gamma_{\mathrm{RE}}/\gamma_{\mathrm{AE}}\to\infty$ 和高 SNR 时的 EASR 的近似上界表达式。在本文中，高 SNR 是指 SNR 大于 20 dB 的情况。

定理 1 当 $\gamma_{\mathrm{RE}}/\gamma_{\mathrm{AE}}\to\infty$ 时，在高 SNR($\gamma_1\gg1$，$\gamma_2\gg1$ 且对于某固定 η 有 $\gamma_1/\gamma_2=\eta$)，AF 多天线中继的 EB 策略的 EASR 可近似为

$$\begin{aligned}\overline{C}_{\mathrm{s,EB}}\Big|_{\gamma_1\gg1,\gamma_2\gg1,\frac{\gamma_1}{\gamma_2}=\eta}\approx&\frac{1}{2\ln 2}\Bigg[\Bigg(\frac{\Omega_3}{N\eta}\mathrm{G}_{3,1}^{1,3}\left(\frac{\Omega_3}{N\eta}\,\middle|\,\begin{matrix}-1,0,0\\0\end{matrix}\right)\\&-\frac{\Omega_2}{N\eta\Gamma(N)}\mathrm{G}_{3,1}^{1,3}\left(\frac{\Omega_2}{N\eta}\,\middle|\,\begin{matrix}-N,0,0\\0\end{matrix}\right)\\&+\psi(N)+\ln\left(\frac{\Omega_2}{\Omega_3}\right)+\nu\Bigg)\Bigg]^{+}\end{aligned}\tag{17}$$

证明 将式(9)和式(10)代入式(12)中，EB 在高信噪比时的 EASR 可近似为

$$\overline{C}_{\mathrm{s,EB}}\Big|_{\gamma_1\gg1,\gamma_2\gg1,\frac{\gamma_1}{\gamma_2}=\eta}\approx\frac{1}{2\ln 2}\left[\mathbb{E}\left[\ln\left(\frac{g_2\left(x_1x_2+N\eta\right)}{x_2\left(x_1g_2+N\eta\right)}\right)\right]\right]^{+}\tag{18}$$

通过类似于引理 1 的推导方法，式(18)可表示成闭合形式(17)。 证毕

注 1： 由式(17)可见，随着 SNR 增大，EB 的 EASR 受限于一常数，该常数仅与 N，η，Ω_2 和 Ω_3 有关，并不随 γ_1 或 γ_2 而增长。

4 大规模天线中继的遍历可达安全速率分析

上节所推导的解析表达式极大地降低了所提传输策略的 EASR 的计算复杂度。大规模 MIMO 相比于传统 MIMO 技术具有巨大的性能增益和简化的收发机技术，已成为下一代无线通信系统最具潜力的技术之一[17,18]。在本节，为了便于分析 ANP 策略，我们考虑 $\gamma_{\mathrm{RE}}/\gamma_{\mathrm{AE}}$ 趋于无穷的情况，针对大规模天线中继，分析 ANP 策略的渐近 EASR 性能，进而得到最优功率分配系数。

对于 ANP 策略，当中继天线数趋于无穷，即 $N\to\infty$，有定理 2。

定理 2　当 $N\to\infty$ 时，ANP 策略的遍历可达安全速率的近似下界为

$$\overline{C}_{\text{s,ANP}} \gtrapprox \frac{1}{2\ln 2}\left[\ln\left(\frac{\rho\gamma_1\gamma_2 N+\rho\gamma_2+\gamma_1}{\gamma_2+1}\cdot\frac{(1-\rho)\gamma_2+1}{\rho\gamma_2+\gamma_1}\right)\right]^+ \tag{19}$$

能获得最大 EASR 的最优功率分配因子为

$$\rho^*=\begin{cases}-\dfrac{\gamma_1}{\gamma_2}+\dfrac{\gamma_1}{\gamma_2}\sqrt{\dfrac{N(1+\gamma_1+\gamma_2)}{1+N\gamma_1}}, & \varphi>0\\ 1, & \varphi\le 0\end{cases} \tag{20}$$

其中，$\varphi=\dfrac{\gamma_2^2}{\gamma_1^2}+\dfrac{N\gamma_2^2}{\gamma_1}+\dfrac{2\gamma_2}{\gamma_1}+N\gamma_2+1-N$。

证明过程略。

基于定理 2 中的结论，我们在下列两个推论中给出高SNR和低SNR情况下的最优功率分配策略。在本文中，低 SNR 是指 SNR 小于−5 dB 的情况。

推论 1　当 $N\to\infty$ 时，在高 SNR 情况下（$\gamma_1\gg 1$，$\gamma_2\gg 1$，$\gamma_1/\gamma_2=\eta$），ANP 策略能取得最大 EASR 的最优功率分配系数为

$$\rho^*=\sqrt{\eta^2+\eta}-\eta \tag{21}$$

证明　对于高SNR和大 N 的情况，可得 $\varphi>0$，通过渐近近似，式(21)可由式(20)获得。　　证毕

从推论 1 可见，ρ^* 是一个仅与 η 相关的常数，如果 $\eta=1$ 则 $\rho^*=0.41$。

推论 2　当 $N\to\infty$ 时，在低 SNR 情况下（$\gamma_1\ll 1$，$\gamma_2\ll 1$，$\gamma_1/\gamma_2=\eta$），ANP 策略能取得最大 EASR 的最优功率分配系数为 $\rho^*=1$。

证明　当 $N\to\infty$ 时，在低 SNR 时，式(19)可近似为

$$\overline{C}_{\text{s,ANP}}\Big|_{\gamma_1\ll 1,\gamma_2\ll 1,\frac{\gamma_1}{\gamma_2}=\eta}^{N\to\infty}\approx\frac{1}{2\ln 2}\ln\left(\frac{\rho\gamma_1 N+\rho+\eta}{\rho+\eta}\right) \tag{22}$$

定义 $f(\rho)\triangleq\ln\left(\dfrac{\rho\gamma_1 N+\rho+\eta}{\rho+\eta}\right)$。因为 $f(\rho)$ 相对于 ρ 的一阶偏导为 $\dfrac{\partial f(\rho)}{\partial\rho}=\dfrac{\eta\gamma_1 N}{(\eta+\rho)(\eta+\rho+\gamma_1 N\rho)}>0$，$f(\rho)$ 是关于 ρ 的增函数，因此通过设定 $\rho=1$ 可使 $\overline{C}_{\text{s,ANP}}|_{N\to\infty}$ 最大化。　　证毕

注 2：从推论 2 可得出如下结论：当 $N\to\infty$ 时，在低 SNR 情况下，EB 策略的 EASR 性能优于 ANP 策略。对于任意 N 的情况，也有相同结论，推导如下。此时有 $\beta_1^2\approx\rho\gamma_2$ 和 $a\approx 0$，通过使用 $\lim\limits_{x\to 0}\ln(1+x)\approx x$，从式(7)，式(8)和式(12)可得：

$$\overline{C}_{\text{s,ANP}}\Big|_{\gamma_1\ll 1,\gamma_2\ll 1,\frac{\gamma_1}{\gamma_2}=\eta}\approx\frac{\rho}{2\ln 2}\left[\mathbb{E}\left[\gamma_1\gamma_2 g_1 g_2-\gamma_1\gamma_2 x_2 g_1\right]\right]^+ \tag{23}$$

式 (23) 与 ρ 成正比。因此，当 $\rho=1$ 时，$\overline{C}_{\text{s,ANP}}\Big|_{\gamma_1\ll 1,\gamma_2\ll 1,\frac{\gamma_1}{\gamma_2}=\eta}$ 可取得最大值。

5　仿真结果与讨论

在本节，两种安全传输策略的遍历可达安全速率性能和上文推导的解析表达式将通过 Monte Carlo 仿真加以验证。在所有仿真中，设 $\gamma_1=\gamma_2$。为仿真 $\gamma_{\text{RE}}/\gamma_{\text{AE}}\to\infty$ 的情况，设 $\Omega_i=1/d_i^{n_i}$（$i=1,2,3$）中的 $d_i=2$ m，$n_i=2$，$d_4=4$ m，$n_4=4$。平均值由 10^6 次 Monte Carlo 仿真获得。在图 2 和图 3 中，通过合并式(12)，式(13)和式(14)可得到 ANP 的 EASR 下界的解析曲线，通过合并式(12)，式(13)和式(15)可得到 EB 的 EASR 近似上界的解析曲线。

在图 2 中，所推导 ANP 和 EB 的 EASR 的闭合表达式与仿真 ESC(即：式(11)的 Monte Carlo 仿真值)进行了比较，参数设置：$\rho=0.5$，$d_2=d_3=2$ 和 $N=10$。d_1 的值分别设为 1 和 2。仿真结果显示所推导的 ANP 的下界很紧，EB 近似上界在整个感兴趣的 SNR 区域内与仿真结果吻合。对于两种 d_1 情

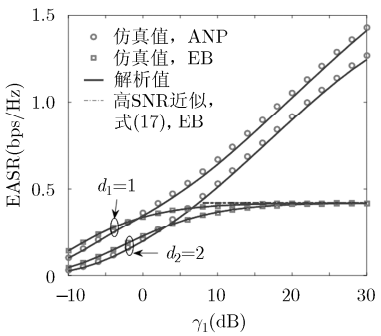

图 2　$d_1=1$ 和 $d_1=2$ 情况下 ANP 和 EB 的 EASR 曲线

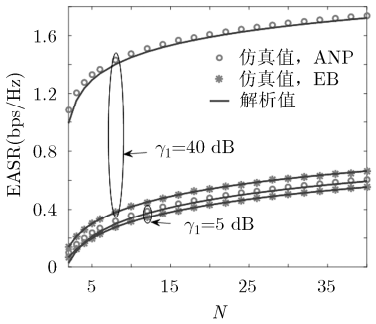

图 3　$\gamma_1=5$ dB 和 $\gamma_1=40$ dB 情况下 ANP 和 EB 的 EASR 曲线

况，EB 的 EASR 的高 SNR 近似(即：式(17))与 Monte Carlo 仿真值完全吻合。ANP 的 EASR 随着 γ_1 而增大，而 EB 的 EASR 在高 SNR 区域保持恒定，验证了定理 1。在低 SNR 区域，EB 比其他方案性能优越，验证了推论 2。在高 SNR 情况下，当 d_1 减小(即 Ω_1 增加)，EB 的 EASR 趋于一常数，验证了注 1 的正确性，而 ANP 的 EASR 增加显著。综上所述，当 d_1 减小(即 Ω_1 增加)，ANP 和其他策略的差距增大，意味着在高 SNR 时，第 1 跳信道增益对 ANP 的 EASR 的影响超过对 EB 的影响。

图 3 给出了分别在 $\gamma_1 = 5$ dB 和 $\gamma_1 = 40$ dB 时天线数 N 对两种策略的 EASR 的影响。仿真条件：$\rho = 0.5$ 和 $d_1 = d_2 = d_3 = 2$。我们可以看到，在两种 SNR 区域，随着 N 的增加，两种策略的 EASR 增加，且解析曲线与仿真结果吻合。总之，在大规模天线中继安全通信系统中，ANP 策略的 EASR 性能显著优于其他两种策略。

图 4 给出了 $N = 100$ 时 ANP 的 EASR 随功率分配(PA)因子的变化曲线。在图 4 中，近似下界式(19)与 Monte Carlo 仿真结果吻合良好，尤其是在中低 SNR 区域和大多数高 SNR 区域。因此，从相应的 EASR 解析表达式推导最优 PA 因子是合理的。从两图中还可见，在低 SNR 区域，最优 PA 因子等于 1，验证了推论 2。

图 5 给出了所提最优 PA 策略、等 PA 策略和仿真最优 PA 策略的 ANP 的 Monte Carlo 仿真的 EASR 性能比较。仿真最优 PA 指的是在 $0 < \rho \le 1$ 范围内搜索步长 $\Delta = 0.01$ 时通过遍历搜索获得的最优 PA 系数，可视为准确的最优 PA 策略。等 PA 策略是指 PA 系数为定值 0.5。在图 5 中，对于 ANP 策略，当采用所提最优 PA 策略时，我们为不同的 SNR 采用合适的 PA 方案，即：对于 $\gamma_1 = 20$ dB，采用式(21)，对于 $\gamma_1 = 10$ dB 和 $\gamma_1 = 0$ dB，采用式(20)，对于 $\gamma_1 = -10$ dB 和 $\gamma_1 = -20$ dB，采用 $\rho = 1$。从图 5 可见，所提最优 PA 策略的 EASR 在全部 SNR 区域和全部 N 区域与准确的最优 PA 策略的 EASR 吻合良好，即使是对于小 N 值也吻合良好。在低 SNR 区域，所提 PA 策略明显优于等 PA 策略，在高 SNR 区域，等 PA 策略的 EASR 也能够与准确的最优值相匹配，因为在这种情况下所提 PA 系数 $\rho = 0.41$，与 $\rho = 0.5$ 相近。

6 结论

本文研究了存在一个窃听节点的多天线 AF 中继传输系统的遍历安全容量。研究并分析了两种安全传输策略：ANP 和 EB，并推导了新的 EASR 的闭合表达式，可用来高效地评价任意中继天线数时的系统性能。当中继配置大规模天线时，针对高 SNR 和低 SNR 区域进行了渐近性分析，并基于渐近表达式给出了近似最优功率分配因子的闭合解。解析结果显示 ANP 在中高 SNR 区域的性能显著优于 EB 策略，而在低 SNR 区域，采用等功率分配时 EB 优于 ANP。EB 的 EASR 不能随着发送功率无限增加，而是趋近于一个与第一跳信道增益独立的常数。在高 SNR 区域，建议在 ANP 策略中将一半左右的功率分配给人工噪声。仿真结果验证了理论分析结果。

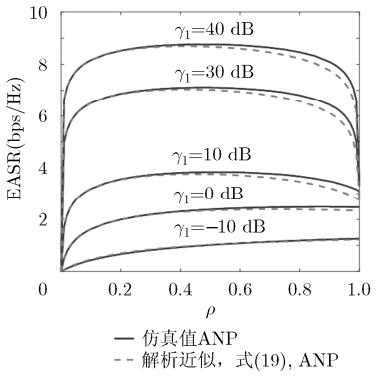

图 4 ANP 的 EASR 的 Monte Carlo 仿真结果和近似下界比较

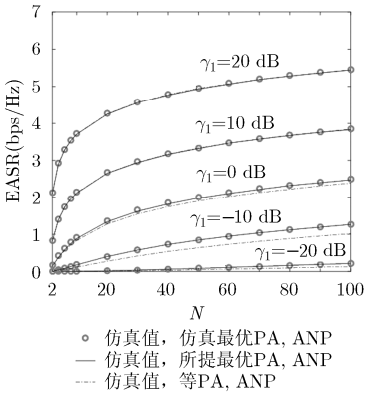

图 5 ANP 的 Monte Carlo 仿真 EASR 的仿真最优 PA 方案、所提最优 PA 方案和等 PA 方案比较

参 考 文 献

[1] WANG H M, LIU F, and XIA X G. Joint source-relay precoding and power allocation for secure amplify-and-forward MIMO relay networks[J]. *IEEE Transactions on Information Forensics and Security*, 2014, 9(8): 1240–1250. doi: 10.1109/TIFS.2014.2327480.

[2] FAN L S, LEI X, DUONG T Q, *et al*. Secure multiuser communications in multiple amplify-and-forward relay networks[J]. *IEEE Transactions on Communications*, 2014, 62(9): 3299–3310. doi: 10.1109/TCOMM.2014.2345763.

[3] LIN H X, ZHAO R, HE Y C, *et al*. Secrecy performance of transmit antenna selection with outdated CSI for MIMO relay systems[C]. IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 2016: 2516–2521.

[4] YUAN Y, ZHAO R, LIN H X, *et al*. Secrecy outage probability of cognitive decode-and-forward relay networks[C]. IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 2016: 3167–3172.

[5] ZHAO R, HUANG Y M, WANG W, *et al*. Ergodic secrecy capacity of dual-hop multiple-antenna AF relaying systems[C]. IEEE Global Communications Conference (GLOBECOM), San Diego, USA, Dec. 2015: 1–6. doi: 10.1109/GLOCOM.2015.7417212.

[6] LAI L and GAMAL H E. The relay–eavesdropper channel: Cooperation for secrecy[J]. *IEEE Transactions on Information Theory*, 2008, 54(9): 4005–4019. doi: 10.1109/TIT.2008.928272.

[7] LIN M, GE J, YANG Y, *et al*. Joint cooperative beamforming and artificial noise design for secrecy sum rate maximization in two-way AF relay networks[J]. *IEEE Communications Letters*, 2014, 18(2): 380–383. doi: 10.1109/LCOMM.2013.121713.132262.

[8] HUANG J. Cooperative jamming for secure communications in MIMO relay networks[J]. *IEEE Transactions on Signal Processing*, 2011, 59(10): 4871–4884. doi: 10.1109/TSP.2011.2161295.

[9] DING Z, PENG M, and CHEN H H. A general relaying transmission protocol for MIMO secrecy communications[J]. *IEEE Transactions on Communications*, 2012, 60(11): 3461–3471. doi: 10.1109/TCOMM.2012.081012.110236.

[10] GOEL S and NEGI R. Guaranteeing secrecy using artificial noise[J]. *IEEE Transactions on Wireless Communications*, 2008, 7(6): 2180–2189. doi: 10.1109/TWC.2008.060848.

[11] TSAI S H and POOR H V. Power allocation for artificial-noise secure MIMO precoding systems[J]. *IEEE Transactions on Signal Processing*, 2014, 62(13): 3479–3493. doi: 10.1109/TSP.2014.2329273.

[12] XIONG Q, GONG Y, LIANG Y C, *et al*. Achieving secrecy of MISO fading wiretap channels via jamming and precoding with imperfect channel state information[J]. *IEEE Wireless Communications Letters*, 2014, 3(4): 357–360. doi: 10.1109/LWC.2014.2317194.

[13] AKHTAR A, BEHNAD A, and WANG X. On the secrecy rate achievability in dual-hop amplify-and-forward relay networks[J]. *IEEE Wireless Communications Letters*, 2014, 3(5): 493–496. doi: 10.1109/LWC.2014.2349514.

[14] MUNOZ-MEDINA O, VIDAL J, and AGUSTIN A. Linear transceiver design in nonregenerative relays with channel state information[J]. *IEEE Transactions on Signal Processing*, 2007, 55(6): 2593–2604. doi: 10.1109/TSP.2006.890913.

[15] PARK K H, WANG T, and ALOUINI M S. On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming[J]. *IEEE Journal on Selected Areas in Communications*, 2013, 31(9): 1741–1750. doi: 10.1109/JSAC.2013.130908.

[16] BLOCH M, BARROS J, RODRIGUES M R D, *et al*. Wireless information-theoretic security[J]. *IEEE Transactions on Information Theory*, 2008, 54(6): 2515–2534. doi: 10.1109/TIT.2008.921908.

[17] GRADSHTEYN I S and RYZHIK I M. Table of Integrals, Series, and Products [M]. New York: Academic Press, 2007: 1–20.

[18] JIN S, LIANG X, WONG K K, *et al*. Ergodic rate analysis for multipair massive MIMO two-way relay networks[J]. *IEEE Transactions on Wireless Communications*, 2015, 14(3): 1480–1491. doi: 10.1109/TWC.2014.2367503.

赵　睿：男，1980 年生，副教授，研究方向为无线通信信号处理、协作通信和物理层安全.

贺玉成：男，1964 年生，教授，研究方向为无线通信、信道编码、协作无线通信等.

周　林：男，1982 年生，讲师，研究方向为无线通信、信道编码和编码调制技术.