Journal of System Simulation

Volume 28 | Issue 2 Article 17

8-17-2020

PHY Security Transmission Based on Antenna Selection and Artificial Noise

Deng Dan
1. Guangzhou Panyu Polytechnic, Guangzhou 511483, China;;

Wang Wei
1. Guangzhou Panyu Polytechnic, Guangzhou 511483, China;;

Zhao Ming
2. University of Science and Technology of China, Hefei 230027, China;

PHY Security Transmission Based on Antenna Selection and Artificial Noise

Abstract

Abstract: *A physical-layer security enhancement scheme based on antenna selection and artificial noise (ASAN) was proposed. In broadcast phase, the Relay node selected the optimal antenna subset, and transmitted the beamforming matrix and artificial noise vector simultaneously.* Simulation results show that the ASAN scheme outperforms classical beamforming scheme. Compared with beamforming scheme, the proposed scheme shows about 2.5dB gain in ergodic secrecy capacity when antenna number of Relay is three, and 3dB gain when the antenna number is six. Specifically, the combined selection criterion shows the similar curve compared with the one-direction criterion, in which the Relay only needs the channel information on Alice.

Keywords

artificial noise, analog network coding, physical-layer security, secrecy capacity

Recommended Citation

Deng Dan, Wang Wei, Zhao Ming. PHY Security Transmission Based on Antenna Selection and Artificial Noise[J]. Journal of System Simulation, 2016, 28(2): 376-383.

第 28 卷第 2 期 系统仿真学报© Vol. 28 No. 2
2016 年 2 月 Journal of System Simulation Feb., 2016

联合天线选择和人工噪声的安全传输技术

邓单[1]，王伟[1]，赵明[2]
(1. 广州番禺职业技术学院，广东 广州 511483；2. 中国科学技术大学，安徽 合肥 230027)

摘要：针对模拟网络编码系统(Analog Network Coding, ANC)，*提出联合天线选择与人工噪声(Antenna Selection and Artificial Noise，ASAN)的物理层安全传输方案。在 ANC 系统的广播阶段，中继结点从接收天线集合中优选出部分天线子集；基于优选天线子集，从联合等效信道矩阵中推导出波束成形矩阵与人工噪声向量。针对 ASAN 技术方案，提出了适合不同场景的天线选择方案并进行仿真分析。*仿真结果表明：当 Relay 结点天线数为 3 时，相比于经典的波束成形方案，ASAN 方案表现出的性能增益约为 2.5dB；当天线数目配置为 6 时，性能增益约为 3dB。特别地，联合优选准则与简化的单向选择准则具有接近的性能曲线，而单向选择准则算法的复杂度可减半。

关键词：人工噪声；模拟网络编码；物理层安全；安全容量
中图分类号：TN802 文献标识码：A 文章编号：1004-731X (2016) 02-0376-08

PHY Security Transmission Based on Antenna Selection and Artificial Noise

Deng Dan[1], *Wang Wei*[1], *Zhao Ming*[2]
(1. Guangzhou Panyu Polytechnic, Guangzhou 511483, China; 2. University of Science and Technology of China, Hefei 230027, China)

Abstract: *A physical-layer security enhancement scheme based on antenna selection and artificial noise (ASAN) was proposed. In broadcast phase, the Relay node selected the optimal antenna subset, and transmitted the beamforming matrix and artificial noise vector simultaneously.* Simulation results show that the ASAN scheme outperforms classical beamforming scheme. Compared with beamforming scheme, the proposed scheme shows about 2.5dB gain in ergodic secrecy capacity when antenna number of Relay is three, and 3dB gain when the antenna number is six. Specifically, the combined selection criterion shows the similar curve compared with the one-direction criterion, in which the Relay only needs the channel information on Alice.

Keywords: artificial noise; analog network coding; physical-layer security; secrecy capacity

引言

物理层网络编码(Physical-layer network coding，PNC)的概念与技术方案最初分别由 Zhang[1]和 Popovski[2]独立提出，随后成为无线通信领域的研究热点。Katti[3]提出更为通用化的网络编码策略：模拟网络编码(Analog Network Coding, ANC)。在 ANC 系统中，中继结节将接收到的信号线性叠加，简单放大再进行转发；合法结点在本地将自身发射信号部分从接收信号中抵消，从而可以获得有用信号部分。ANC 系统由于其实现简单而被广泛研究。

无线通信系统传输介质天然的广播特性导致窃听者可以轻易接收到网络中的发射信号。安全传输技术的目标是在减少窃听用户泄露信息量的前

收稿日期：2014-10-21 修回日期：2014-12-11；
基金项目：国家高技术研究发展计划(2012AA011402)；广东省教育科学教育信息技术研究专项课题(13JXN042)；
作者简介：邓单(1981-)，男，湖北京山，博士，高工，研究方向为 MIMO、物理层安全；王伟(1972-)，男，陕西咸阳，博士，副教授，研究方向为信息安全；赵明(通讯作者 1976-)，男，安徽铜陵，博士，讲师，研究方向无线通信技术，无线信道。

提下，尽量提高合法用户的有效传输速率。安全传输技术研究热点主要集中在波束成形技术，人工快速衰落技术以及人工噪声技术等若干领域。针对全向 MIMO 点对点 Relay 信道，文献[4-7]深入研究窃听结节的影响及其应对传输策略。其中，文献[4]提出广义天线选择合并算法(generalized selection combining，GSC)：合法结点通过选择最强的部分天线支路后，再进行 MRC 合并，该算法在系统性能与复杂度取得较好的平衡。文献[5]则证明了在两用户 MIMO 高斯广播信道场景中，若约束发射信号总功率，则线性预编码方法为最优发射机；且保密容量可由保密脏纸编码(Secret dirty paper coding，S-DPC)算法获得。文献[6]分析在大规模天线 MISO 条件下，使用线性预编码方法，根据不同的天线配比，部署不同的发射策略。文献[7]基于加权与灌水算法提出可以增强系统保密容量的优化算法。Mukherjee[8]还分析了多天线配置条件下 ANC 系统在物理层攻击结节下的脆弱性。更多的文献[9-13]提出多种基于预编码(precoding-based)和人工噪声(artificial-noise-based，AN-based)的技术策略。国内也有相关文献[14-15]详细研究基于合法用户信道的零空间而设计的随机波束算法，在不影响合法用户信噪比前提下，能降低窃听信道的等效链路质量。

经典的人工噪声方案是将人工噪声信号空间设计于合法结节等效信道的零空间中。此时人工噪声只会对非法窃听结节造成干扰，而不会对合法结节的接收信号产生任何影响。然而，目前还没有文献针对网络编码系统地研究物理层安全传输技术实现方案。

本文针对模拟网络编码系统，提出基于天线选择与人工噪声(Antenna Selection and Artificial Noise Based，ASAN)的物理层安全传输技术方案。在 ANC 系统的广播阶段(Broadcast phase，BC phase)，中继结点从接收天线集合中优选出部分天线子集；基于优选天线子集，从联合等效信道矩阵中推导出波束成形矩阵与人工噪声向量。我们提出了适合不同场景的天线选择方案并进行仿真分析。仿真结果表明：相比于经典的波束成形方案，ASAN 方案表现出明显的性能增益。

1 系统模型与假设

考虑具有 4 个结节的网络编码系统，如图 1 所示。系统中包括两个合法结节：Alice 与 Bob，以及中继(Relay)结点和窃听(eavesdropper，Eve)结点。合法结节 Alice 与 Bob 无直接通信链路，但可以通过 Relay 结点进行双向通信。Alice，Bob 与 Relay 结节配置多天线，其天线数目分别为：N_A, N_B, N_R。Eve 结点只配置单天线，即 $N_E=1$。在模拟网络编码系统发射过程中，系统可按照发射特点分为两个阶段：多址接入阶段(multiple access phase，MAC phase)与广播阶段(broadcast phase，BC phase)。在 MAC 阶段，两个合法结点 Alice 与 Bob 同时向 Relay 结点发送信号。在 BC 阶段，Relay 结点经过线性合并与简单放大后，将信号向两个源结点广播。随后，两个源结点首先从接收信号中将自身发射信号抵消，并从抵消后的信号中恢复出对方结点的信息。由于无线通信系统的开放性，在两个阶段中，窃听结点可以接收到所有信号，但不会主动发射任何信号。

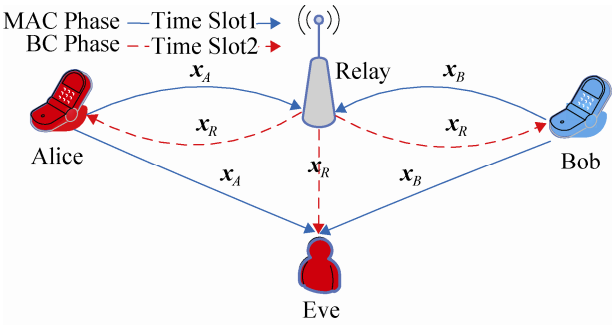

图 1 模拟网络编码系统模型

假设 ANC 系统发射信号带宽远小于信道相干带宽，即准静态平坦衰落信道模型。Alice/Bob 到 Relay 结点，Alice/Bob 到 Eve 结点之间的 MIMO 信道模型可描述如下：

第 28 卷第 2 期 系统仿真学报 Vol. 28 No. 2
2016 年 2 月 Journal of System Simulation Feb., 2016

$$\boldsymbol{H}_{AR} \in \mathbb{C}^{N_R \times N_A}, \boldsymbol{H}_{BR} \in \mathbb{C}^{N_R \times N_B}$$
$$\boldsymbol{H}_{AE} \in \mathbb{C}^{N_E \times N_A}, \boldsymbol{H}_{BE} \in \mathbb{C}^{N_E \times N_B} \quad (1)$$

式中各信道矩阵元素均为循环对称复高斯随机变量，并且其分布满足$\mathbb{CN}(0,1)$，并且信道矩阵之间相互独立不相关；信道衰落矩阵在一次 ANC 发射周期中保持恒定，且各发射周期之间对应的信道矩阵独立。

为简化系统复杂性，不失一般性，我们做如下假设：

A. 任意两个结点之间的信道衰落矩阵满足互易原则，即 $\boldsymbol{H}_{AR} \equiv \boldsymbol{H}_{RA}^T$

B. Alice/Bob 结点在在 MAC 阶段发射过程中，已知到 Relay 结点的信道衰落矩阵，但对 Eve 结点的信道未知。同样的假设也适用于 Relay 结点。

C. 对于 Relay 结点，天线选择的策略同时应用于发射天线与接收天线；即 Relay 在 MAC 阶段和 BC 阶段使用相同的天线子集。

2 ASAN 技术方案

在 MAC 阶段，Alice 与 Bob 同时向 Relay 结点发射无线信号；而 Eve 也可以同时对上述信号进行接收。此时，Relay/Eve 两结点的接收信号可描述为：

$$\boldsymbol{y}_R = \boldsymbol{H}_{AR}\boldsymbol{x}_A + \boldsymbol{H}_{BR}\boldsymbol{x}_B + \boldsymbol{n}_R \rightarrow$$
$$\boldsymbol{y}_E = \boldsymbol{H}_{AE}\boldsymbol{x}_A + \boldsymbol{H}_{BE}\boldsymbol{x}_B + \boldsymbol{n}_E \quad (2)$$

式中：$\boldsymbol{x}_A \in \mathbb{C}^{N_A \times 1}$，$\boldsymbol{x}_B \in \mathbb{C}^{N_B \times 1}$为合法结点 Alice/Bob 的发射信号向量；$\boldsymbol{n}_R \in \mathbb{C}^{N_R \times 1}$，$\boldsymbol{n}_E \in \mathbb{C}^{N_E \times 1}$ 为 Relay/Eve 结点在接收到的加性高斯白噪声(AWGN)向量，其分布分别为：$\boldsymbol{n}_R \sim CN(0, \sigma_R^2 \boldsymbol{I}_{N_R})$，$\boldsymbol{n}_E \sim CN(0, \sigma_E^2 \boldsymbol{I}_{N_E})$，其中 σ_R^2, σ_E^2 表示 Relay/Eve 结点上每根接收天线的平均噪声功率。Alice/Bob 结点的总发射功率满足如下功率限制：

$$P_A \triangleq Tr\{E[\mathbf{x}_A \mathbf{x}_A^\dagger]\}$$
$$P_B \triangleq Tr\{E[\mathbf{x}_B \mathbf{x}_B^\dagger]\} \quad (3)$$

为简化表述，Alice 与 Bob 为相互对称结点，我们可假设两结点以等功率发射信号，即 $P_A = P_B$。定义 Relay/Eve 结点两端的信噪比 SNR：

$$\overline{\gamma}_R \triangleq \frac{P_A}{\sigma_R^2}, \overline{\gamma}_E \triangleq \frac{P_A}{\sigma_E^2} \quad (4)$$

广播阶段，Relay 结点将从其 N_R 个天线中优选出天线子集，此天线子集中共有 $(N_A + N_B)$ 个元素。天线子集的接收信号为：

$$\boldsymbol{y}_R^s = \boldsymbol{H}_{AR}^s \boldsymbol{x}_A + \boldsymbol{H}_{BR}^s \boldsymbol{x}_B + \boldsymbol{n}_R^s \quad (5)$$

式中：$\boldsymbol{y}_R^s$ 表示从原始信号 $\boldsymbol{y}_R$ 中优选出的 $(N_A + N_B)$ 行的向量，类似表示同样适用于 $\boldsymbol{H}_{AR}^s$，$\boldsymbol{H}_{BR}^s$ 和 $\boldsymbol{n}_R^s$。详细的天线选择准则会在下一节内容中讨论。类似文献[13]中的方法，Relay 结点会分别推导出 BF 与 AN 信号，如下所示：

$$\boldsymbol{x}_R = \sqrt{\alpha_R \frac{P_R}{P_{RA}(N_A + N_B)}} \boldsymbol{W}_R \boldsymbol{y}_R^s + \sqrt{(1-\alpha_R)P_R}\boldsymbol{\eta}_R \quad (6)$$

式(6)中第 1 部分为波束成形(BF)信号部分，第 2 部分为人工噪声(AN)信号部分。BF 信号部分的波束方向与合法用户等效信道的特征值方向相匹配，可使用有用信号部分到达合法用户的等效信噪比最大化；AN 部分是由等效信道的零空间之基向量的线性组合构造而成，波束方向与合法用户等效信道相正交，即不影响有用信号的信噪比，又能以等效噪声形式降低窃听用户链路质量。其中，P_R 表示 Relay 结点的总发射功率，P_{RA} 表示 MAC 阶段 Relay 结点每个天线上的平均接收总功率，即 $P_{RA} \triangleq (P_A + P_B + \sigma_R^2)$. α_R 表示 AN 信号在总功率中功率分配因子。功率分配策略不在本文讨论内容之中，所以本文中假设功率分配因子固定 $\alpha_R = 0.5$。特别地，当 $\alpha_R = 1$ 时，人工噪声信号功率为 0，ASAN 策略退化为经典的 BF 策略。$\boldsymbol{W}_R \in \mathbb{C}^{N_R \times (N_A + N_B)}$ 表示 Relay 结点构造的波束成形矩阵，$\boldsymbol{\eta}_R \in \mathbb{C}^{N_R \times 1}$ 为 Relay 结点构造的人工噪声向量。为保证人工噪声不对合法结点通信造成不利影响，其设计必须保证同时与 $\boldsymbol{H}_{RB}/\boldsymbol{H}_{RA}$ 正交，即

$$\boldsymbol{H}_{RB}\boldsymbol{\eta}_R = 0, \ \boldsymbol{H}_{RA}\boldsymbol{\eta}_R = 0 \quad (7)$$

同时波束成形矩阵和人工噪声向量也必须满足正交关系：

$$\boldsymbol{W}_R^H \boldsymbol{\eta}_R = 0 \tag{8}$$

两者的总功率需要满足功率限制：

$$\boldsymbol{W}_R^H \boldsymbol{W}_R = \boldsymbol{I}, \boldsymbol{\eta}_R^H \boldsymbol{\eta}_R = \boldsymbol{I} \tag{9}$$

定义联合信道衰落矩阵如下：

$$\boldsymbol{H}_{ABR} \triangleq \begin{bmatrix} \boldsymbol{H}_{AR}^T \\ \boldsymbol{H}_{BR}^T \end{bmatrix} \in \mathbb{C}^{(N_A+N_B)\times N_R} \tag{10}$$

通过 SVD(singular value decomposition)分解，Relay 结点可间接推导出最优的 BF 矩阵 $\boldsymbol{W}_R$：

$$\boldsymbol{H}_{ABR} = \boldsymbol{U}_{ABR} \boldsymbol{\Lambda}_{ABR} \boldsymbol{V}_{ABR}^H \tag{11}$$

式中：$\boldsymbol{U}_{ABR} \in \mathbb{C}^{(N_A+N_B)\times(N_A+N_B)}$，$\boldsymbol{V}_{ABR} \in \mathbb{C}^{N_R \times N_R}$ a 均为酉阵；$\boldsymbol{\Lambda}_{ABR} \in \mathbb{C}^{(N_A+N_B)\times N_R}$ 为半对角矩阵。如果天线数目满足：$N_R > (N_A + N_B)$，则 $\boldsymbol{H}_{ABR}$ 存在零空间。最优波束成形矩阵 $\boldsymbol{W}_R$ 可从 $\boldsymbol{V}_{ABR}$ 的前 $(N_A + N_B)$ 个列向量中获得：

$$\boldsymbol{W}_R = [\boldsymbol{t}_1, \boldsymbol{t}_2, \cdots \boldsymbol{t}_{(N_A+N_B)}] \tag{12}$$

式中：$\boldsymbol{t}_i$ 表示矩阵 $\boldsymbol{V}_{ABR}$ 的第 i 个列向量；$\boldsymbol{\eta}_R$ 可通过 $\boldsymbol{V}_{ABR}$ 其他 $[N_R - (N_A + N_B)]$ 个列向量的线性组合来构造：

$$\boldsymbol{\eta}_R = \frac{1}{\sqrt{N_R - (N_A + N_B)}} \sum_{i=N_A+N_B+1}^{N_R} \boldsymbol{t}_i \beta_i \tag{13}$$

式中 β_i 为具有零均值，均匀相位分布，单位方差分布特性的独立复数随机变量。假设发射端与合法用户接收端均已知优选天线子集结果，则在 BC 阶段，Bob 结点的接收信号可表示为：

$$\begin{aligned} \boldsymbol{z}_B = \boldsymbol{H}_{RB}\boldsymbol{x}_R + \boldsymbol{n}_B = \\ \sqrt{\alpha_R \frac{P_R}{P_0}} \boldsymbol{H}_{RB} \boldsymbol{W}_R \boldsymbol{H}_{AR}^s \boldsymbol{x}_A + \\ \sqrt{\alpha_R \frac{P_R}{P_0}} \boldsymbol{H}_{RB} \boldsymbol{W}_R \boldsymbol{H}_{BR}^s \boldsymbol{x}_B + \\ \sqrt{\alpha_R \frac{P_R}{P_0}} \boldsymbol{H}_{RB} \boldsymbol{W}_R \boldsymbol{n}_R^s + \boldsymbol{n}_B \end{aligned} \tag{14}$$

式(14)中，第 1 部分为 Bob 接收到的经 Relay 结点转发的有用信号；第 2 部分为原先为 Bob 自身发射的经 Relay 结点转发的干扰信号；第 3~4 部分表示经由第 1 次转发和第 2 次接收所产生的噪声部分。其中，$\boldsymbol{n}_B \sim CN(0, \sigma_B^2 \boldsymbol{I}_{N_B})$ 为 Bob 结点接收到的噪声信号。定义总功率：$P_0 \triangleq P_{RA}(N_A + N_B)$。由于 Bob 结点拥有对其自身发射信号 $\boldsymbol{x}_B$ 的先验知识以及其等效信道衰落矩阵，接收信号 $\boldsymbol{z}_B$ 的第二部分可以通过干扰抵消技术进行消减，抵消之后的信号可表示为：

$$\begin{aligned} \boldsymbol{z}_B = \sqrt{\alpha_R \frac{P_R}{P_0}} \boldsymbol{H}_{RB} \boldsymbol{W}_R \boldsymbol{H}_{AR}^s \boldsymbol{x}_A + \\ \sqrt{\alpha_R \frac{P_R}{P_0}} \boldsymbol{H}_{RB} \boldsymbol{W}_R \boldsymbol{n}_R^s + \boldsymbol{n}_B \end{aligned} \tag{15}$$

对于 Bob 结点的系统容量可表示为：

$$C_B = \log_2[\det(\boldsymbol{K}_B^d + \boldsymbol{K}_B^n)] - \log_2[\det(\boldsymbol{K}_B^n)] \tag{16}$$

式中 2 个相关矩阵分别为信号相关矩阵与噪声/干扰相关矩阵，

$$\boldsymbol{K}_B^n = \alpha_R \frac{P_R}{P_0} \sigma_R^2 \boldsymbol{H}_{RB} \boldsymbol{H}_{RB}^H + \sigma_B^2 \boldsymbol{I}_{N_B} \tag{17}$$

式(17)中 $\boldsymbol{K}_B^n$ 表示对于 Bob 结点，其等效噪声的相关矩阵。经过 MAC 阶段与 BC 阶段两阶段的联合处理，$\boldsymbol{K}_B^n$ 由 2 部分构成。其中第 1 部分由 Relay 自身噪声功率及 Relay-Bob 信道矩阵构成；第 2 部分则由 Bob 结点自身接收噪声构成。

$$\boldsymbol{K}_B^d = \alpha_R \frac{P_A P_R}{N_A P_0} \boldsymbol{H}_{RB} \boldsymbol{W}_R \boldsymbol{H}_{AR}^s (\boldsymbol{H}_{RB} \boldsymbol{W}_R \boldsymbol{H}_{AR}^s)^H \tag{18}$$

式(18)中 $\boldsymbol{K}_B^d$ 表示 Bob 结点等效信道矩阵的相关函数；上述相关函数主要由 3 个结点互相之间的信道矩阵以及 BF 矩阵 $\boldsymbol{W}_R$ 决定：

$\Phi_A = E[\boldsymbol{x}_A \boldsymbol{x}_A^\dagger] = \frac{P_A}{N_A} \boldsymbol{I}_{N_A}$。

类似地，Alice 结点的接收信号可表示为：

$$\begin{aligned} \boldsymbol{z}_A = \sqrt{\alpha_R \frac{P_R}{P_0}} \boldsymbol{H}_{RA} \boldsymbol{W}_R \boldsymbol{H}_{BR}^s \boldsymbol{x}_B + \\ \sqrt{\alpha_R \frac{P_R}{P_0}} \boldsymbol{H}_{RA} \boldsymbol{W}_R \boldsymbol{n}_R^s + \boldsymbol{n}_A \end{aligned} \tag{19}$$

其系统容量表达式为：

$$C_A = \log_2[\det(\boldsymbol{K}_A^d + \boldsymbol{K}_A^n)] - \log_2[\det(\boldsymbol{K}_A^n)] \tag{20}$$

Alice/Bob 合法链路的容量为：$C_M = C_A + C_B$。

类似地，在广播阶段，窃听结点 Eve 的接收信号为：

第 28 卷第 2 期 系统仿真学报 Vol. 28 No. 2
2016 年 2 月 Journal of System Simulation Feb., 2016

$$\boldsymbol{z}_E = \boldsymbol{H}_{RE}\Big[\sqrt{\alpha_R \frac{P_R}{P_0}}\boldsymbol{W}_R(\boldsymbol{H}^s_{AR}\boldsymbol{x}_A + \boldsymbol{H}^s_{BR}\boldsymbol{x}_B + \boldsymbol{n}^s_R) + \sqrt{(1-\alpha_R)P_R}\boldsymbol{\eta}_R\Big] + \boldsymbol{n}_{E2} = \sqrt{\alpha_R \frac{P_R}{P_0}}\boldsymbol{H}_{RE}\boldsymbol{W}_R\boldsymbol{H}^s_{AR}\boldsymbol{x}_A + \sqrt{\alpha_R \frac{P_R}{P_0}}\boldsymbol{H}_{RE}\boldsymbol{W}_R\boldsymbol{H}^s_{BR}\boldsymbol{x}_B + \Big[\sqrt{\alpha_R \frac{P_R}{P_0}}\boldsymbol{H}_{RE}\boldsymbol{W}_R\boldsymbol{n}^s_R + \sqrt{(1-\alpha_R)P_R}\boldsymbol{H}_{RE}\boldsymbol{\eta}_R + \boldsymbol{n}_{E2}\Big] \quad (21)$$

式中：$\boldsymbol{n}_{E2} \sim CN(0, \sigma_E^2 \boldsymbol{I}_{N_E})$为 Eve 结点接收到的高斯噪声向量。联合公式(1)与(21)，Eve 结点在 2 个阶段的接收信号可进行联合整理为：

$$\begin{bmatrix} \boldsymbol{y}_E \\ \boldsymbol{z}_E \end{bmatrix} = \boldsymbol{H}_{ABE}\boldsymbol{x}_{AB} + \begin{bmatrix} \boldsymbol{n}_E \\ \overline{\boldsymbol{n}}_E \end{bmatrix} \quad (22)$$

式中：$\boldsymbol{x}_{AB} \triangleq \begin{bmatrix} \boldsymbol{x}_A \\ \boldsymbol{x}_B \end{bmatrix}$。

联合信道的等效衰落矩阵可表示为：

$$\boldsymbol{H}_{ABE} \triangleq \begin{bmatrix} \boldsymbol{H}_{AE} & \boldsymbol{H}_{BE} \\ \sqrt{\alpha_R \frac{P_R}{P_0}}\boldsymbol{H}_{RE}\boldsymbol{W}_R\boldsymbol{H}^s_{AR} & \sqrt{\alpha_R \frac{P_R}{P_0}}\boldsymbol{H}_{RE}\boldsymbol{W}_R\boldsymbol{H}^s_{BR} \end{bmatrix} \quad (23)$$

联合信号的等效噪声矩阵可表示为：

$$\overline{\boldsymbol{n}}_E \triangleq \sqrt{\alpha_R \frac{P_R}{P_0}}\boldsymbol{H}_{RE}\boldsymbol{W}_R\boldsymbol{n}^s_R + \sqrt{(1-\alpha_R)P_R}\boldsymbol{H}_{RE}\boldsymbol{\eta}_R + \boldsymbol{n}_{E2} \quad (24)$$

基于以上分析，Eve 信道的联合系统容量为：

$$C_E = \log_2[\det(\boldsymbol{K}^d_E + \boldsymbol{K}^n_E)] - \log_2[\det(\boldsymbol{K}^n_E)] \quad (25)$$

式中，信号相关矩阵分别为：$\boldsymbol{K}^d_E = \boldsymbol{H}_{ABE}\boldsymbol{\Phi}_{AB}\boldsymbol{H}_{ABE}$，$\Phi_{AB} \triangleq E[\mathbf{x}_{AB}\mathbf{x}^{\dagger}_{AB}] = \frac{P_A}{N_A}\boldsymbol{I}_{N_{AB}}$。

噪声相关矩阵表示为：

$$\boldsymbol{K}^n_E \triangleq \begin{bmatrix} \boldsymbol{K}^n_1 & 0 \\ 0 & \boldsymbol{K}^n_2 \end{bmatrix} \quad (26)$$

式（26）中，两个对角相关矩阵分别为 2 阶段的噪声相关矩阵：

$$\boldsymbol{K}^n_1 = \sigma_E^2 \boldsymbol{I}_{N_E} \quad (27)$$

$$\boldsymbol{K}^n_2 = [\alpha_R \frac{\sigma_R^2 P_R}{P_0} + 1 - \alpha_R]P_R\boldsymbol{H}_{RE}\boldsymbol{H}^H_{RE} + \sigma_E^2\boldsymbol{I}_{N_E} \quad (28)$$

ANC 系统的安全容量可表示为：

$$C_S = [C_A + C_B - C_E]^+ \quad (29)$$

特别地，本文还提出 2 种评估物理层安全的指标：安全容量截断概率和安全容量归 0 概率。2 个指标的定义分别如下：$P_{\text{out}} \triangleq P[C_S < C_{TH}]$ 以及 $P_0 \triangleq P[C_S = 0]$，式中，$C_{TH}$ 表示预定义的安全容量门限。

3 系统流程与天线选择准则

基于天线选择与人工噪声的物理层安全传输技术方案(ASAN)完整的处理流程如下：

Alice/Bob 同时进行正常的信号发射(MAC 阶段)；Relay 结点对 Alice/Bob 的信号进行接收，根据接收到的信号和天线选择准则进行最优子集选择；再根据公式(6)分别构造 BF 信号与 AN 信号，以广播方式向 Alice/Bob 结点进行发送(BC 阶段)；Alice/Bob 分别对 Relay 发射信号进行接收，在本地将自身信号部分进行抵消再解调恢复出对方发送的有用信息。基于 ASAN 技术方案，针对系统流程中最重要的天线选择模块，我们提出几种简化的天线选择准则。假设以安全容量最大化为优化目标，则公式(5)中最优的天线选择准则可表示为：

$$(A_R) = \arg\max_{(A_R)}\{C_S\} \quad (30)$$

式中：$A_R \in Z^{(N_A+N_B)}$ 表示优选天线子集。

最优选择准则需要把所有可能的天线子集遍历比较，其运算复杂度过于庞大。为减少 ASAN 方案的复杂度，提高其可实现性，我们提出几种简化的选择准则：

Sel-0: 无选择，即 $A_R = \{1, 2, \cdots (N_A + N_B)\}$

Sel-1: 单向选择准则

1) 计算 Alice/Relay 之间信道衰落矩阵 $\boldsymbol{H}_{AR}$ 每根天线的接收信号功率；

2) 根据各天线上接收功率进行降序排列；

3) 选择功率最大的前 $(N_A + N_B)$ 个天线作为

优选天线子集 A_R；

Sel-2: 联合优选准则

1) 分别计算 Alice/Relay 与 Bob/Relay 之间信道衰落矩阵 $\boldsymbol{H}_{AR}$ 和 $\boldsymbol{H}_{BR}$ 每根天线的接收信号功率；

2) 对两个矩阵各天线接收信号功率累加，根据各天线上接收功率进行降序排列；

3) 选择功率最大的前 (N_A+N_B) 个天线作为优选天线子集 A_R。

4 算法仿真与分析

为了对 ASAN 方案的性能进行定量分析，本节通过算法仿真，将 ASAN 方案与经典方案进行性能对比与分析。本文中使用 Matlab 作为仿真工具平台。不失一般性，我们假设 Eve 结点的 SNR 固定为 $\bar{\gamma}_E=10\text{ dB}, 5\text{ dB}$。为简化系统模型，并考虑到 Alice/Bob 的对称结构，我们假设两结点的发射功率与接收噪声功率相等，即公式(3)与(14)中 $P_A=P_B, \sigma_A^2=\sigma_B^2$。

首先，考虑 Alice/Bob/Eve 都是单天线配置，Relay 结点配置 3 根天线的系统模型。天线选择策略使用第 4 部分提出几种优选准则。当 Eve 结点的 SNR(公式 4)固定为 5 dB 时，其遍历安全容量曲线如图 2 所示。图中横坐标表示公式(4)中所示 Relay 结点处接收信号的平均 SNR，单位：dB；纵轴表示平均安全容量，即遍历安全容量。图中标注”No AN”表示经典的 BF 策略且不进行人工噪声加载(如公式(6)，(12)所示)，即 $\alpha_R=1$。由仿真结果易知，使用联合优选准则(Sel-2)方案的曲线性能最优，但其计算复杂度也最高。相比于经典 BF 策略(No AN)，联合优选准则方案提供增益 2.5 dB。相比于无选择(sel-0)方案，提供增益 1 dB。需要特别指出，联合优选准则方案(Sel-2)与单向选择方案(Sel-1)曲线性能接近，但联合优选准则方案计算复杂度需加倍。

由于联合优选准则方案(Sel-2)同时针对 Alice/Bob 2 个结点，基于天线接收功率排序进行天线子集选择。由于选择结果可使得合法链路的等效容量增加，从而间接使得系统的安全容量增大。Sel-2 方案的选择结果与最优的基于安全容量最大化方案最为接近，故其性能较其他方案为优，然而其计算复杂度也最大。单向选择方案(Sel-1)可以视为 Sel-2 方案的简化算法。Sel-1 只针对 ANC 系统中的单侧支路(如 Alice/Relay 链路)，选择发射结点中信道增益最大的天线子集，该算法复杂度比 Sel-2 减半，但性能与 Sel-2 性能曲线非常接近，可在复杂度与系统性能之间取得较好的折衷。

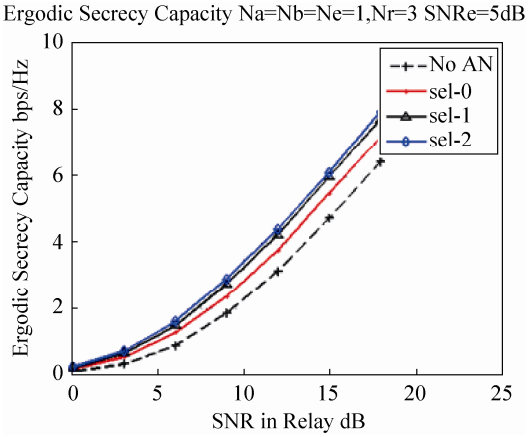

图 2 安全容量曲线(系统配置 Na=Nb=Ne=1,Nr=3 SNRe=5dB)

ANC 安全容量截断概率曲线如图 3 所示，图中横坐标表示公式(4)中所示 Relay 结点处接收信号的平均 SNR。截断容量定义如前文所示，其中门限预设为 $2N_A$ bps，式中 N_A 为 Alice 结点天线数目。类似地，由图中易知，相比于经典 BF 策略(No AN)，联合优选准则方案提供增益 2.5 dB。

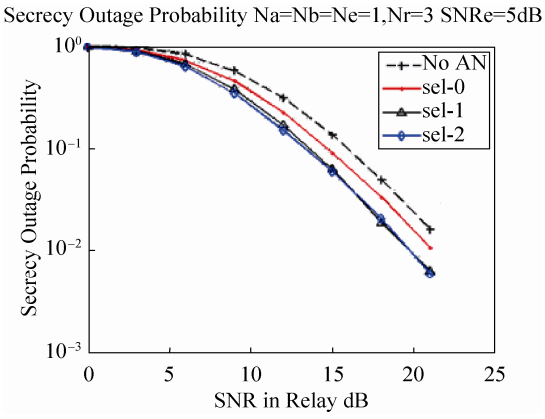

图 3 安全容量截断概率曲线
(系统配置 Na=Nb=Ne=1, Nr=3 SNRe=5dB)

第 28 卷第 2 期 系统仿真学报 Vol. 28 No. 2
2016 年 2 月 Journal of System Simulation Feb., 2016

同样的天线配置条件下，固定 Eve 结点的 SNR 为 10dB，其安全容量曲线与安全容量截断概率曲线分别如图 4~5 所示。可以看出，联合优选准则方案与单向选择准则相比于经典 BF 方案和无选择方案具有类似的性能增益。由图中可看到，联合优选准则相比于传统 BF 方案性能增益约 3 dB；相比于无选择方案，增益约 1 dB。

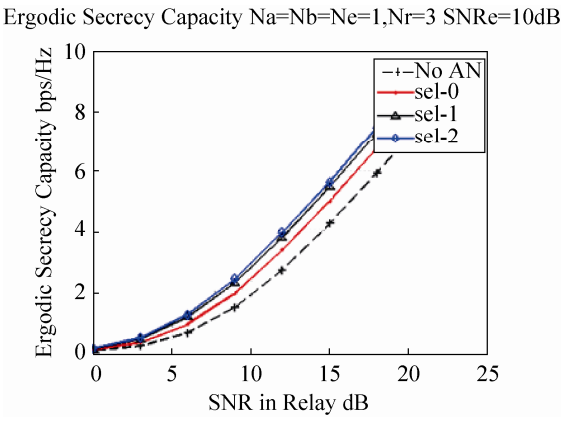

图 4 安全容量曲线
(系统配置 Na=Nb=Ne=1, Nr=3 SNRe=10dB)

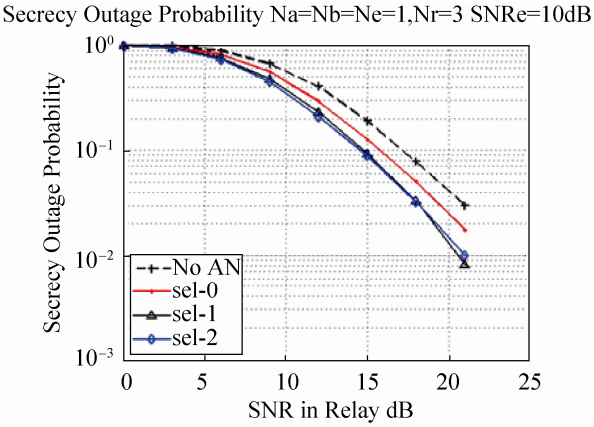

图 5 安全容量截断概率曲线
(系统配置 Na=Nb=Ne=1,Nr=3 SNRe=10dB)

5 结论

针对模拟网络编码系统(ANC)，本文提出联合天线选择与人工噪声(ASAN)的物理层安全传输方案。通过仿真分析，对 ASAN 方案中详细的天线选择方案进行了性能对比。仿真结果表明：ASAN 方案在系统复杂度与系统性能两方面可取得较好的平衡，为实用的 ANC 系统安全传输提供了有益的参考。同时，本文并未研究人工噪声与有用信号功率分配的方案及最优值，这也是未来研究工作的重要方向。

参考文献：

[1] S Zhang, S C Liew, P P Lam. Hot topic: physical-layer network coding [C]// 12th annual international conference on Mobile computing and networking, Los Angeles USA. USA: IEEE, 2006: 358-365.

[2] P Popovski, H Yomo. The anti-packets can increase the achievable throughput of a wireless multi-hop network [C]// Communications, 2006, IEEE International Conference on, Istanbul Turkey. USA: IEEE, 2006: 3885-3890.

[3] S Katti, S Gollakota, D Katabi. Embracing wireless interference: analog network coding [J]. ACM SIGCOMM Computer Communication Review (S0146-4833), 2007, 37(4): 397-408.

[4] L Chen, Y Yang, G Wei. Physical layer security enhancement with generalized selection diversity combining [C]// Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on (978-1-4673-6235-1), London UK. USA: IEEE, 2013: 518-521.

[5] S A A Fakoorian, A L Swindlehurst. On the Optimality of Linear Precoding for Secrecy in the MIMO Broadcast Channel [J]. IEEE Journal on Selected Areas in communication (S0733-8716), 2013, 31(9): 1701-1713.

[6] G Geraci, R Couille, J Yuan, et al. Large System Analysis of Linear Precoding in MISO Broadcast Channels with Confidential Messages [J]. Selected Areas in Communications, IEEE Journal on (S0733-8716), 2013, 31(9): 1660-1671.

[7] Q Li, M Hong, H-T Wai, et al. Transmit solutions for MIMO wiretap channels using alternating optimization [J]. Selected Areas in Communications, IEEE Journal on (S0733-8716), 2013, 31(9): 1714-1727.

[8] A Mukherjee, A L Swindlehurst. Securing multi-antenna two-way relay channels with analog network coding against eavesdroppers [C]// Signal Processing Advances in Wireless Communications (SPAWC), 2010 IEEE Eleventh International Workshop on, Marrakech Morocco. USA: IEEE, 2010: 1-5.

[9] S Goel, R Negi. Guaranteeing secrecy using artificial noise [J]. Wireless Communications, IEEE Transactions on (S1536-1276), 2008, 7(6): 2180-2189.

（下转第 387 页）

