利用人工噪声提高合法接收者性能的物理层安全方案

雷维嘉*　林秀珍　杨小燕　谢显中
(重庆邮电大学移动通信技术重庆市重点实验室　重庆　400065)

摘　要：该文研究在采用波束赋形和人工噪声的物理层安全方案中利用人工噪声提高合法接收端性能。发送端根据发送符号和信道系数，判断人工噪声是否对合法接收端的信号检测有益，并针对有益噪声和无益噪声分别设计不同的噪声波束赋形矢量。通过利用有益噪声，在不改变窃听端接收信噪比的条件下，合法接收端的信噪比有较明显的提高。对误比特率和保密容量进行理论分析和仿真，结果显示，与传统的人工噪声方案相比，所提方案可提高合法接收端的性能，改善保密容量。

关键词：物理层安全；误比特率；人工噪声；保密容量
中图分类号：TN925　　**文献标识码**：A　　**文章编号**：1009-5896(2016)11-2887-06
DOI: 10.11999/JEIT160054

Physical Layer Security Scheme Exploiting Artificial Noise to Improve the Performance of Legitimate User

LEI Weijia　LIN Xiuzhen　YANG Xiaoyan　XIE Xianzhong
(*Chongqing Key Laboratory of Mobile Communications Technology*, *Chongqing University of Posts and Telecommunications*, *Chongqing* 400065, *China*)

Abstract: A physical layer security scheme is studied, which employs the advantage of artificial noise to improve the performance of legitimate user for multiple antenna systems using beamforming technology and artificial noise. Based on the transmitted symbols and channel coefficients, the sender determines whether or not the artificial noises are beneficial to the signal detection at the legitimate receiver. Then, beamforming vectors are designed accordingly. By taking advantage of useful noise, the signal to noise ratio at the legitimate receiver is improved effectively while that at the illegal receiver will remain the same. The bit error rate and the secrecy capacity are analyzed and simulated. The results demonstrate that the proposed scheme can improve the performance of the legal receiver and enhance secrecy capacity.

Key words: Physical layer security; Bit error rate; Artificial noise; Secrecy capacity

1　引言

由于无线通信系统中传输媒介的开放性、无线终端的移动性和网络结构的不稳定性，传输的可靠性和安全性面临严峻的考验。研究表明，除传统的高层的加密方式外，安全传输也可以通过物理层安全技术来解决。作为上层加密方法的一种补充或代替技术，物理层安全技术是在底层利用无线信道的多径、互易性、空间唯一性等特征提高系统的安全性，其理论基础是 Shannon 建立的信息论安全模型[1]。

随着多天线技术的快速发展，利用多天线实现物理层安全成为一个学术界的研究热点。利用多根发送天线提供的空间自由度可抑制窃听者的信号接收质量[2−4]。目前常用的抑制窃听者信号接收质量的技术主要有两类，一类是对发送信号进行波束赋形[5]，将发射信号对准合法用户的方向，同时降低窃听端的接收信号功率；另一类是人为产生噪声对窃听者进行干扰。

使用人工噪声(Artificial Noise, AN)来提高物理层安全性能首先是由文献[6]提出的，此后很多学者对人工噪声方案进行了广泛的研究。按照发送端获得窃听信道状态信息(Eavesdropper's Channel State Information, ECSI)的 3 种情况，人工噪声的设计方案有较大的不同。在发送端能获得完美的 ECSI 的情况下，文献[7]以安全中断概率为指标，讨论了人工噪声与信号的最优功率分配方案。当发送

收稿日期：2016-01-13；改回日期：2016-05-12；网络出版：2016-07-19
*通信作者：雷维嘉　leiwj@cqupt.edu.cn
基金项目：国家自然科学基金(61471076, 61301123)，重庆市基础与前沿研究计划(cstc2015jcyjA40047)，长江学者和创新团队发展计划(IRT1299)，重庆市科委重点实验室专项经费
Foundation Items: The National Natural Science Foundation of China (61471076, 61301123), The Chongqing Research Program of Basic Research and Frontier Technology (cstc2015jcyjA40047), The Program for Changjiang Scholars and Innovative Research Team in University (IRT1299), The Special Fund of Chongqing Key Laboratory (CSTC)

端仅能获得部分或不准确的 ECSI 时，则需要考虑人工噪声方案的鲁棒性问题。针对多输入单输出(Multiple-input Single-Output, MISO)窃听信道模型，在 ECSI 存在误差情况下，通过设计发送信号和人工噪声的协方差矩阵，文献[8~10]依次解决了最大化遍历保密容量问题，合法接收端服务质量约束条件下发送端功率最小化问题以及最小化中断概率等问题。在发送端完全未知 ECSI 情况下，通常的设计方法是使 AN 各向同性，均匀分布在合法信道的零空间[11]，这样，在保证不干扰合法接收端的情况下，劣化窃听端接收的信号[11]。如文献[12]提出了一种双向中继网络中的两阶段零空间波束赋形方案，通过中继加入人工噪声来改善双向中继传输系统的安全性能；文献[13]提出了一种 MISO 模型下基于人工噪声辅助的波束赋形传输技术，在保密容量和中断概率联合约束下，实现最大化保密信息吞吐量的目标。

现有的应用人工噪声的方案中，一般都要求人工噪声不对合法接收者造成干扰，也就是在合法接收者处人工噪声的功率为 0，相应地人工噪声也就不会对合法接收者的接收有任何帮助。实际上，在特定的情况下，人工噪声对合法接收者而言有可能是有益的。在使用人工噪声的方案中，发送端是可以根据合法信道的状态信息和人工噪声，判断出到达合法接收端的人工噪声是否对其信号检测有益。本文从合法接收者利用有益人工噪声的角度出发，对基于信号波束赋形和人工噪声的物理层安全传输方案进行研究，利用波束赋形技术使有益人工噪声能提高合法接收端性能。具体思路为：发送端根据当前发送符号和信道系数，判断人工噪声是否对合法接收端信号检测有益。如果有益，采用全向的人工噪声波束赋形，使合法接收者也能收到人工噪声，提高检测性能；如果有害，则采用将人工噪声置于合法信道零空间的波束赋形，避免对合法接收者产生干扰。对于窃听者，由于人工噪声和合法信道的随机特性，其无法判断发送者使用了哪种波束赋形方案，人工噪声仍然能很好地保护保密信息。

本文的结构如下：第 2 节建立系统模型，给出信号波束赋形和人工噪声方案；第 3 节针对二进制相移键控(Binary Phase Shift Keying, BPSK)、四相移键控(Quadrature Phase Shift Keying, QPSK)调制方式，具体分析系统的误比特率、保密容量等性能；第 4 节对所提方案进行数值仿真和分析；最后一节对全文进行总结。

注：本文中使用的符号的说明如下。$||\boldsymbol{a}||$表示向量 $\boldsymbol{a}$ 的 2-范数；$\mathrm{diag}(\boldsymbol{a})$表示以向量 $\boldsymbol{a}$ 的元素为对角元素的对角矩阵；$\arg(\bullet)$ 表示复数的角度，$\mathrm{Re}(\bullet)$ 表示取复数的实部，$|\bullet|$ 表示复数的模；$\Leftrightarrow$ 表示等价；$\mathcal{CN}(\mu, \sigma^2)$表示服从均值为 μ、方差为 σ^2 的复高斯分布；$\mathrm{E}(\bullet)$ 表示对随机变量取均值。$\boldsymbol{I}_N$ 表示 $N\times N$ 阶单位阵。

2 系统模型

考虑一个包括源节点 S，一个目的节点 D 和单个窃听节点 E 的无线网络模型，其中源节点具有 N 根天线(N>1)，目的节点和窃听节点均为单天线节点。我们采用联合波束赋形和人工噪声的方案，对承载信息的信号和人工噪声使用不同的赋形矢量。标量 x 表示在一个传输时隙内要传输的符号，具有单位功率，即 $\mathrm{E}\{|x|^2\}=1$。另外，为了符号的书写方便，省略时间下标。$\boldsymbol{z}=[z_1, z_2, \cdots, z_N]^{\mathrm{T}}$ 表示随机生成的 N 维人工噪声矢量，且 $z_i \sim C\mathcal{N}(0,\ 1)$, i=1,2,$\cdots$,N。

在发送端，发送信号表示为

$$x_{\mathrm{t}} = \sqrt{P_{\mathrm{s}}}\boldsymbol{w}_1 x + \sqrt{P_{\mathrm{z}}/N}\boldsymbol{W}_2\boldsymbol{z} \tag{1}$$

其中，$\boldsymbol{w}_1$ 为信号的波束赋形矢量，$\boldsymbol{w}_1=[w_{11}, w_{12}, \cdots, w_{1N}]^{\mathrm{T}}$，$\boldsymbol{W}_2$ 为噪声的波束赋形矩阵，满足 $\boldsymbol{W}_2^{\mathrm{H}}\boldsymbol{W}_2 = \boldsymbol{I}_N$。$P_{\mathrm{s}}$ 是发送信号功率，P_{z} 是发送人工噪声功率。

假设窃听节点是被动节点，发送端未知自己到窃听节点的信道状态，在此状况下，我们以最大化接收端的接收功率为目标，设计信息的波束赋形矢量 $\boldsymbol{w}_1$，易得

$$\boldsymbol{w}_1 = \boldsymbol{h}/\|\boldsymbol{h}\| \tag{2}$$

其中，$\boldsymbol{h} \triangleq [h_{\mathrm{D},1}, h_{\mathrm{D},2}, \cdots, h_{\mathrm{D},N}]^{\mathrm{T}}$ 是 S-D 的信道增益矢量。

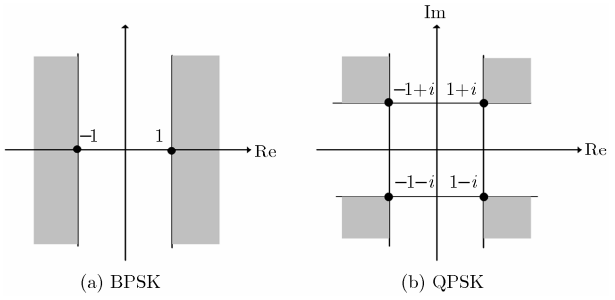
目的节点和窃听节点接收到的信号分别为

$$\begin{aligned} y_{\mathrm{D}} &= \boldsymbol{h}^{\mathrm{H}}x_{\mathrm{t}} + n_{\mathrm{D}} = \sqrt{P_{\mathrm{s}}}\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}_1 x \\ &\quad + \sqrt{P_{\mathrm{z}}/N}\boldsymbol{h}^{\mathrm{H}}\boldsymbol{W}_2\boldsymbol{z} + n_{\mathrm{D}} \end{aligned} \tag{3}$$

$$\begin{aligned} y_{\mathrm{E}} &= \boldsymbol{g}^{\mathrm{H}}x_{\mathrm{t}} + n_{\mathrm{E}} = \sqrt{P_{\mathrm{s}}}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_1 x \\ &\quad + \sqrt{P_{\mathrm{z}}/N}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}_2\boldsymbol{z} + n_{\mathrm{E}} \end{aligned} \tag{4}$$

式中，$\boldsymbol{g} \triangleq [g_{\mathrm{E},1}, g_{\mathrm{E},2}, \cdots, g_{\mathrm{E},N}]^{\mathrm{T}}$ 是 S-E 的信道增益矢量，$n_{\mathrm{D}} \sim \mathcal{CN}(0, \sigma_{\mathrm{D}}^2)$，$n_{\mathrm{E}} \sim \mathcal{CN}(0, \sigma_{\mathrm{E}}^2)$分别是目的节点和窃听节点处的复加性高斯白噪声。

人工噪声有可能对接收端的信号检测和判决是有利的。图 1 所示为 BPSK, QPSK 调制方式的星座图。当人工噪声使得接收信号向着阴影区域移动时，人工噪声有利于接收端作出正确的判决。为了有效地利用人工噪声，设计两种人工噪声波束赋形矩阵：(1) $\boldsymbol{W}_{21}=\mathrm{diag}(\boldsymbol{w}_{21})=\boldsymbol{I}_N$，即 $N\times N$ 的单位矩阵，$\boldsymbol{w}_{21}$ 为元素全为 1 的 N 维单位矢量；(2) $\boldsymbol{W}_{20}$ 则是主信道零空间的投影矩阵，即满足 $\boldsymbol{h}^{\mathrm{H}}\boldsymbol{W}_{20}=0$。采用 $\boldsymbol{W}_{21}$ 时，接收端能接收到人工噪声，而采用 $\boldsymbol{W}_{20}$ 时不会。人工噪声的波束赋形矩阵可表示为



(a) BPSK　　(b) QPSK

图 1 BPSK, QPSK 星座图中有益噪声的区域

$$\boldsymbol{W}_2=\begin{cases}\boldsymbol{W}_{21}, & k=1\\ \boldsymbol{W}_{20}, & k=0\end{cases} \tag{5}$$

其中，k 为波束赋形矩阵的选择开关，当人工噪声有利时为 1，选择 $\boldsymbol{W}_{21}$，否则为 0，选择 $\boldsymbol{W}_{20}$。

将 $\boldsymbol{w}_1$ 和 $\boldsymbol{W}_2$ 表达式代入式(3)，式(4)中，接收端和窃听者接收到的信号可改写为

$$y_{\mathrm{D}}=\begin{cases}\sqrt{P_{\mathrm{s}}}\,\|\boldsymbol{h}\|x+\sqrt{P_{\mathrm{z}}/N}\boldsymbol{h}^{\mathrm{H}}\boldsymbol{z}+n_{\mathrm{D}}, & k=1\\ \sqrt{P_{\mathrm{s}}}\,\|\boldsymbol{h}\|x+n_{\mathrm{D}}, & k=0\end{cases} \tag{6}$$

$$y_{\mathrm{E}}=\begin{cases}\sqrt{P_{\mathrm{s}}}\dfrac{\boldsymbol{g}^{\mathrm{H}}\boldsymbol{h}}{\|\boldsymbol{h}\|}x+\sqrt{\dfrac{P_{\mathrm{z}}}{N}}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{z}+n_{\mathrm{E}}, & k=1\\ \sqrt{P_{\mathrm{s}}}\dfrac{\boldsymbol{g}^{\mathrm{H}}\boldsymbol{h}}{\|\boldsymbol{h}\|}x+\sqrt{\dfrac{P_{\mathrm{z}}}{N}}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}_{20}\boldsymbol{z}+n_{\mathrm{E}}, & k=0\end{cases} \tag{7}$$

3　性能分析

3.1 BPSK 调制

3.1.1 误码率分析　发送端采用 BPSK 调制方式时，即 $x\in\{+1,-1\}$。发送端采用单位矢量的人工噪声加权矢量 $\boldsymbol{w}_{21}$，接收端接收到的人工噪声为

$$z_{\mathrm{D}}=\sqrt{P_{\mathrm{z}}/N}\boldsymbol{h}^{\mathrm{H}}\boldsymbol{W}_{21}\boldsymbol{z}=\left|\sqrt{P_{\mathrm{z}}/N}\boldsymbol{h}^{\mathrm{H}}\boldsymbol{z}\right|\mathrm{e}^{\mathrm{j}\theta_{z1}} \tag{8}$$

其中，$\theta_{z1}=\arg(\boldsymbol{h}^{\mathrm{H}}\boldsymbol{z})$ 为接收人工噪声的相位。当 $x=+1$，$-\pi/2<\theta_{z1}<\pi/2$ (即 $\mathrm{Re}(\boldsymbol{h}^{\mathrm{H}}\boldsymbol{z})>0$)时，或 $x=-1$，$\pi/2<\theta_{z1}<3\pi/2$ (即 $\mathrm{Re}(\boldsymbol{h}^{\mathrm{H}}\boldsymbol{z})<0$)时，人工噪声对接收端的判决有利，否则有害。因此，发送端人工噪声赋形矢量开关的选择为

$$k=\begin{cases}1, & x\,\mathrm{Re}\left(\boldsymbol{h}^{\mathrm{H}}\boldsymbol{z}\right)>0\\ 0, & \text{其它}\end{cases} \tag{9}$$

由于 $\boldsymbol{h}$ 和 $\boldsymbol{z}$ 的相位都是在$-\pi$~$+\pi$间均匀分布，因此有利的人工噪声取值概率为 1/2，也即 $p(k=1)=p(k=0)=1/2$。

当 k=1 时，式(6)中第 2 项可以看作是信号部分(对判断发送信号有利)。接收端对接收信号的实部进行检测，信号平均功率为

$$\begin{aligned}\overline{P}_{\mathrm{sD1\_b}}&=\mathrm{E}\left(\mathrm{Re}\left(\sqrt{P_{\mathrm{s}}}\,\|\boldsymbol{h}\|x+\sqrt{P_{\mathrm{z}}/N}\boldsymbol{h}^{\mathrm{H}}\boldsymbol{z}\right)^2\right)\\ &=NP_{\mathrm{s}}+\frac{P_{\mathrm{z}}}{2}+2\sqrt{\frac{P_{\mathrm{s}}P_{\mathrm{z}}N}{\pi}}\end{aligned} \tag{10}$$

其中，功率下标“_b”表示 BPSK 调制方式，下同。

接收端噪声平均功率 $\overline{P}_{\mathrm{nD\_b}}=0.5\sigma_{\mathrm{D}}^2$，由此可得接收端的平均信噪比为

$$\overline{\gamma}_{1\_\mathrm{b}}=\overline{P}_{\mathrm{sD1\_b}}/\overline{P}_{\mathrm{nD\_b}}=\frac{2NP_{\mathrm{s}}}{\sigma_{\mathrm{D}}^2}+\frac{P_{\mathrm{z}}}{\sigma_{\mathrm{D}}^2}+\frac{4}{\sigma_{\mathrm{D}}^2}\sqrt{\frac{P_{\mathrm{s}}P_{\mathrm{z}}N}{\pi}} \tag{11}$$

当 k=0 时，接收端的信号功率为

$$\overline{P}_{\mathrm{sD0\_b}}=\mathrm{E}\left(\mathrm{Re}\left(\sqrt{P_{\mathrm{s}}}\,\|\boldsymbol{h}\|x\right)^2\right)=NP_{\mathrm{s}} \tag{12}$$

对于接收端，各天线发送信号根据信道系数进行了加权，与采用多接收天线并采用最大比值合并方式相当，根据文献[14]，误比特率为

$$p_{\mathrm{e}}=\left(\frac{1-\mu}{2}\right)^N\sum_{l=0}^{N-1}\binom{N-1-l}{l}\left(\frac{1+\mu}{2}\right)^l \tag{13}$$

其中，$\mu=\sqrt{\overline{\gamma}/(1+\overline{\gamma})}$，$\overline{\gamma}$ 为平均比特信噪比。对于本文方案，平均误比特率为 k=0 和 1 时的误比特率的平均：

$$\begin{aligned}\overline{p}_{\mathrm{eD\_b}}&=\overline{p}_{\mathrm{eD\_1}}p(k=1)+\overline{p}_{\mathrm{eD\_0}}p(k=0)\\ &=\frac{1}{2}\left(\frac{1-\mu_1}{2}\right)^N\sum_{l=0}^{N-1}\binom{N-1-l}{l}\left(\frac{1+\mu_1}{2}\right)^l\\ &\quad+\frac{1}{2}\left(\frac{1-\mu_0}{2}\right)^N\sum_{l=0}^{N-1}\binom{N-1-l}{l}\left(\frac{1+\mu_0}{2}\right)^l\end{aligned} \tag{14}$$

其中，$\mu_1=\sqrt{\dfrac{\overline{\gamma}_{1\_\mathrm{b}}/N}{1+\overline{\gamma}_{1\_\mathrm{b}}/N}}$，$\mu_0=\sqrt{\dfrac{\overline{\gamma}_{0\_\mathrm{b}}/N}{1+\overline{\gamma}_{0\_\mathrm{b}}/N}}$，$\overline{p}_{\mathrm{eD\_1}}$ 和 $\overline{p}_{\mathrm{eD\_0}}$ 分别是 k=1 和 0 时的平均误比特率。

对窃听端而言，信号功率与 k 取值无关，考虑最坏的情况：窃听端不仅已知 $\boldsymbol{g}$，而且可以知道 $\boldsymbol{w}_1$，即窃听端可以进行正确的相位校正。此时，平均接收功率为

$$\overline{P}_{\mathrm{sE\_b}}=\mathrm{E}\left(\mathrm{Re}\left(\frac{\left(\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_1\right)^*}{\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_1\right|}\sqrt{P_{\mathrm{s}}}\frac{\boldsymbol{g}^{\mathrm{H}}\boldsymbol{h}}{\|\boldsymbol{h}\|}x\right)^2\right)=P_{\mathrm{s}} \tag{15}$$

而噪声功率为人工噪声功率与信道噪声功率之和。

$$\begin{aligned}\overline{P}_{\mathrm{nE\_b}}&=\mathrm{E}\left(\mathrm{Re}\left(\frac{\left(\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_1\right)^*}{\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_1\right|}\sqrt{\frac{P_{\mathrm{z}}}{N}}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{z}+n_{\mathrm{E}}\right)^2\right)\\ &=\mathrm{E}\left(\mathrm{Re}\left(\frac{\left(\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_1\right)^*}{\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_1\right|}\sqrt{\frac{P_{\mathrm{z}}}{N}}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}_{20}\boldsymbol{z}+n_{\mathrm{E}}\right)^2\right)\\ &=\frac{P_{\mathrm{z}}}{2}+\frac{\sigma_{\mathrm{E}}^2}{2}\end{aligned} \tag{16}$$

窃听端的平均信噪比为

$$\overline{\gamma}_{\mathrm{E\_b}}=\overline{P}_{\mathrm{sE\_b}}/\overline{P}_{\mathrm{nE\_b}}=\frac{2P_{\mathrm{s}}}{\sigma_{\mathrm{E}}^2+P_{\mathrm{z}}} \tag{17}$$

对窃听信道，信号增益为多个复高斯变量乘积的和，分析起来比较复杂，很难得到平均误比特率的闭式解，窃听信道性能将在第 4 节通过仿真的方

式说明。

3.1.2 保密容量分析 把 BPSK 调制器、解调器与信道一起看作是一个广义的 2 输入 2 输出的离散信道，主信道和窃听信道瞬时转移概率矩阵为

$$\boldsymbol{P}_{u\_\mathrm{b}}=\begin{bmatrix}1-p_{u\_\mathrm{b}} & p_{u\_\mathrm{b}}\\ p_{u\_\mathrm{b}} & 1-p_{u\_\mathrm{b}}\end{bmatrix} \tag{18}$$

式中，下标 u 取 D 或 E，对应合法信道或窃听信道，本节和下节中符号下标 u 的含义相同。$p_{u\_\mathrm{b}}=Q(\sqrt{2\gamma_{u\_\mathrm{b}}})$ 表示合法接收端或窃听端瞬时误比特率，γ_{u_b} 表示瞬时比特信噪比，上述信道转移矩阵具有对称性，为 2 元离散对称信道，则合法信道与窃听信道的瞬时信道容量可表示为

$$\begin{aligned}C_{u\_\mathrm{b}}&=\log_2 2-H\left(p_{u\_\mathrm{b}},1-p_{u\_\mathrm{b}}\right)\\&=1-H\left(Q\left(\sqrt{2\gamma_{u\_\mathrm{b}}}\right),1-Q\left(\sqrt{2\gamma_{u\_\mathrm{b}}}\right)\right)\end{aligned} \tag{19}$$

其中，$H(p_1,p_2,\cdots,p_d)$ 表示概率分布为 $\{p_1,p_2,\cdots,p_d\}$ 的离散变量的熵。

遍历保密容量为

$$\begin{aligned}C_{\mathrm{s\_b}}&=\mathrm{E}\left(\left[C_{\mathrm{D}}-C_{\mathrm{E}}\right]^{+}\right)=\frac{1}{2}\mathrm{E}\left(\left(C_{\mathrm{D1}}-C_{\mathrm{E1}}\right)^{+}\right)\\&\quad+\frac{1}{2}\mathrm{E}\left(\left(C_{\mathrm{D0}}-C_{\mathrm{E0}}\right)^{+}\right)\end{aligned} \tag{20}$$

其中，$[x]^{+}=\max(x,0)$，即当窃听信道信道容量大于合法信道信道容量时，保密容量为零。$C_{\mathrm{D}i}$ 和 $C_{\mathrm{E}i}(i=0,1)$ 表示对应 k 取 i 时瞬时保密容量。

3.2 QPSK 调制

3.2.1 误码率分析 设发送端信号采用 QPSK 调制方式，即 $x\in\{\pm1/\sqrt{2},\pm i/\sqrt{2}\}$，且等概分布。当接收端接收到人工噪声的相位在发送信号相位的 $\pm\pi/4$ 范围内时，人工噪声有利于接收端作出正确的判决。噪声赋形矢量选择开关取值为

$$k=\begin{cases}1, & \arg(x)-\pi/4\ \le\arg\left(\boldsymbol{h}^{\mathrm{H}}\boldsymbol{z}\right)\\ & \qquad\le\arg(x)+\pi/4\\ 0, & \text{其它}\end{cases} \tag{21}$$

由于 $\boldsymbol{h}$ 和 $\boldsymbol{z}$ 的相位在$-\pi$~$+\pi$间均匀分布，因此 $p(k=1)=1/4$。

对合法接收端，当 k=1 时，接收功率为

$$\begin{aligned}\overline{P}_{\mathrm{sD1\_q}}&=\mathrm{E}\left(\left|\sqrt{P_{\mathrm{s}}}\,\|\boldsymbol{h}\|x+\sqrt{P_{\mathrm{z}}/N}\boldsymbol{h}^{\mathrm{H}}\boldsymbol{z}\right|^2\right)\\&=\mathrm{E}\left(\left|\sqrt{P_{\mathrm{s}}}\,\|\boldsymbol{h}\|x\right|^2\right)+P_{\mathrm{z}}/N\cdot\mathrm{E}\left(\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{z}\right|^2\right)\\&\quad+\sqrt{P_{\mathrm{s}}P_{\mathrm{z}}/N}\mathrm{E}\left(\|\boldsymbol{h}\|x\cdot\boldsymbol{h}^{\mathrm{H}}\boldsymbol{z}\right)\\&\quad+\sqrt{P_{\mathrm{s}}P_{\mathrm{z}}/N}\mathrm{E}\left(\|\boldsymbol{h}\|x\cdot\left(\boldsymbol{h}^{\mathrm{H}}\boldsymbol{z}\right)^{*}\right)\\&=NP_{\mathrm{s}}+P_{\mathrm{z}}+4\sqrt{\frac{P_{\mathrm{s}}P_{\mathrm{z}}N}{2\pi}}\end{aligned} \tag{22}$$

其中，功率下标“_q”表示 QPSK 调制方式，下同。

接收端信道噪声功率 $\overline{P}_{\mathrm{nD\_q}}=\sigma_{\mathrm{D}}^2$，由此可得接收端信噪比为

$$\overline{\gamma}_{1\_\mathrm{q}}=\overline{P}_{\mathrm{sD1\_q}}/\overline{P}_{\mathrm{nD\_q}}=\frac{NP_{\mathrm{s}}}{\sigma_{\mathrm{D}}^2}+\frac{P_{\mathrm{z}}}{\sigma_{\mathrm{D}}^2}+\frac{4}{\sigma_{\mathrm{D}}^2}\sqrt{\frac{P_{\mathrm{s}}P_{\mathrm{z}}N}{2\pi}} \tag{23}$$

当 k=0 时，接收功率与 BPSK 调制方式相同：$\overline{P}_{\mathrm{sD0\_q}}=NP_{\mathrm{s}}$，噪声功率 $\overline{P}_{\mathrm{nD\_q}}=\sigma_{\mathrm{D}}^2$，接收端信噪比为

$$\overline{\gamma}_{0\_\mathrm{q}}=\overline{P}_{\mathrm{sD0\_q}}\big/\overline{P}_{\mathrm{nD\_q}}=\frac{NP_{\mathrm{s}}}{\sigma_{\mathrm{D}}^2} \tag{24}$$

与采用 BPSK 调制时类似，对合法信道，平均误比特率为

$$\begin{aligned}\overline{p}_{\mathrm{eD\_q}}&=\overline{p}_{\mathrm{eD\_1}}p(k=1)+\overline{p}_{\mathrm{eD\_0}}p(k=0)\\&=\frac{1}{4}\left(\frac{1-\mu_1}{2}\right)^N\sum_{l=0}^{N-1}\binom{N-1-l}{l}\left(\frac{1+\mu_1}{2}\right)^l\\&\quad+\frac{3}{4}\left(\frac{1-\mu_0}{2}\right)^N\sum_{l=0}^{N-1}\binom{N-1-l}{l}\left(\frac{1+\mu_0}{2}\right)^l\end{aligned} \tag{25}$$

式(25)中，$\mu_1=\sqrt{\dfrac{\overline{\gamma}_{1\_\mathrm{q}}/(2N)}{1+\overline{\gamma}_{1\_\mathrm{q}}/(2N)}}$，$\mu_0=\sqrt{\dfrac{\overline{\gamma}_{0\_\mathrm{q}}/(2N)}{1+\overline{\gamma}_{0\_\mathrm{q}}/(2N)}}$。

对窃听端而言，接收功率与 k 取值无关，即

$$\begin{aligned}\overline{P}_{\mathrm{sE\_q}}&=\mathrm{E}\left(\left(\frac{\left(\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_1\right)^{*}}{\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_1\right|}\sqrt{P_{\mathrm{s}}}\frac{\boldsymbol{g}^{\mathrm{H}}\boldsymbol{h}}{\|\boldsymbol{h}\|}x\right)\left(\frac{\left(\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_1\right)^{*}}{\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_1\right|}\sqrt{P_{\mathrm{s}}}\frac{\boldsymbol{g}^{\mathrm{H}}\boldsymbol{h}}{\|\boldsymbol{h}\|}x\right)^{*}\right)\\&=P_{\mathrm{s}}\end{aligned} \tag{26}$$

$$\begin{aligned}\overline{P}_{\mathrm{nE\_q}}&=\mathrm{E}\left(\left(\frac{\left(\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_1\right)^{*}}{\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_1\right|}\sqrt{\frac{P_{\mathrm{z}}}{N}}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{z}+n_{\mathrm{E}}\right)\right.\\&\quad\left.\cdot\left(\frac{\left(\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_1\right)^{*}}{\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_1\right|}\sqrt{\frac{P_{\mathrm{z}}}{N}}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{z}+n_{\mathrm{E}}\right)^{*}\right)\\&=\mathrm{E}\left(\left(\frac{\left(\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_1\right)^{*}}{\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_1\right|}\sqrt{\frac{P_{\mathrm{z}}}{N}}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}_{20}\boldsymbol{z}+n_{\mathrm{E}}\right)\right.\\&\quad\left.\cdot\left(\frac{\left(\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_1\right)^{*}}{\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_1\right|}\sqrt{\frac{P_{\mathrm{z}}}{N}}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}_{20}\boldsymbol{z}+n_{\mathrm{E}}\right)^{*}\right)\\&=P_{\mathrm{z}}+\sigma_{\mathrm{E}}^2\end{aligned} \tag{27}$$

窃听端信噪比为

$$\overline{\gamma}_{\mathrm{E\_q}}=\overline{P}_{\mathrm{sE\_q}}\big/\overline{P}_{\mathrm{nE\_q}}=\frac{P_{\mathrm{s}}}{\sigma_{\mathrm{E}}^2+P_{\mathrm{z}}} \tag{28}$$

3.2.2 保密容量分析 把 QPSK 调制器、解调器与信道一起看作为一个广义的 4 输入、4 输出的离散信道，合法信道和窃听信道的瞬时转移矩阵可以表示为

$$\boldsymbol{P}_{u\_\mathrm{q}}=\begin{bmatrix} Y^2 & p_{u\_\mathrm{q}}Y & p_{u\_\mathrm{q}}Y & p_{u\_\mathrm{q}}^2 \\ p_{u\_\mathrm{q}}Y & Y^2 & p_{u\_\mathrm{q}}^2 & p_{u\_\mathrm{q}}Y \\ p_{u\_\mathrm{q}}Y & p_{u\_\mathrm{q}}^2 & Y^2 & p_{u\_\mathrm{q}}Y \\ p_{u\_\mathrm{q}}^2 & p_{u\_\mathrm{q}}Y & p_{u\_\mathrm{q}}Y & Y^2 \end{bmatrix} \tag{29}$$

式中，$Y=1-p_{u\_\mathrm{q}}$，$p_{u\_\mathrm{q}}=Q(\sqrt{2\gamma_{u\_\mathrm{q}}})$ 分别表示 QPSK 调制方式下合法接收端与窃听端对应的瞬时误比特率，γ_{u_q} 表示合法接收端或窃听端的瞬时比特信噪比。合法信道和窃听信道的转移矩阵都具有对称性，因此是 4 元离散对称信道，瞬时信道容量为

$$C_{u\_\mathrm{q}}=\log_2 4-H\left(\left(1-p_{u\_\mathrm{q}}\right)^2,p_{u\_\mathrm{q}}\left(1-p_{u\_\mathrm{q}}\right),p_{u\_\mathrm{q}}\left(1-p_{u\_\mathrm{q}}\right),p_{u\_\mathrm{q}}^2\right) \tag{30}$$

遍历保密容量为

$$C_{\mathrm{s}\_\mathrm{q}}=\mathrm{E}\left(\left(C_{\mathrm{D}}-C_{\mathrm{E}}\right)^+\right)=\frac{1}{4}\mathrm{E}\left(\left(C_{\mathrm{D1}}-C_{\mathrm{E1}}\right)^+\right)+\frac{3}{4}\mathrm{E}\left(\left(C_{\mathrm{D0}}-C_{\mathrm{E0}}\right)^+\right) \tag{31}$$

$C_{\mathrm{D}i}$和 $C_{\mathrm{E}i}(i$=0,1)表示对应 k取 i时的瞬时保密容量。

4　仿真结果

在仿真中，合法信道和窃听信道是独立同分布的平坦瑞利衰落信道，信道增益服从均值为 0、方差为 1 的独立复高斯分布；目的节点和窃听节点的噪声功率均为 $\sigma_{\mathrm{D}}^2=\sigma_{\mathrm{E}}^2$=0 mW，仿真中定义信噪比为源端的发送信号功率 P_{s}与噪声功率的比值，功率分配因子 a定义为源端的发送信号功率 P_{s} 与总功率 P 的比值，即 $P_{\mathrm{s}}=aP$，$P_{\mathrm{z}}=(1-a)P$。图例中合法信道表示为“LC”，窃听信道记为“EC”。

图 2 和图 3 分别是 BPSK, QPSK 平均误比特率仿真结果，a=0.2，天线数目 N=4，合法接收端和窃听端均采用最大似然译码。从仿真结果曲线可以看出，合法接收者误比特率的仿真结果与理论分析结果一致。与传统人工噪声方案比较，本文提出的方案在保证窃听信道误比特率基本不变的条件下，降低了主信道误比特率。对比图 2 和图 3 可知，相同条件下，BPSK 误比特率改善效果优于 QPSK，这是因为对于 BPSK 调制方式，k 取 1 概率更大，即人工噪声对判决有益的概率更大，接收端接收到的信号平均功率更大。注意到在窃听者误比特率的仿真中，我们考虑了最坏的情况，即窃听端不仅已知窃听信道的信道增益 $\boldsymbol{g}$，而且可以知道发送端的信号波束赋形矢量 $\boldsymbol{w}_1$，其据此对接收信号进行正确的相位校正。实际上，窃听者很难获得 $\boldsymbol{w}_1$，此时其误比特率在整个仿真的信噪比范围内都约为 0.5。

图 4 和图 5 分别是是采用 BPSK, QPSK 调制时保密容量随功率分配因子 a 变化的仿真结果，发送端总功率固定为 P=1 mW，发送天线数 N 为 3 和 5。保密容量由 30000 次独立的蒙特卡洛仿真结果取平均得到，下同。从图 4 和图 5 可以看出，相同条件下，本文方案得到的保密容量始终大于传统方案下的保密容量。在 P 和 N 一定的条件下，随着 a 增大，保密容量先增大后减小，并且两种方案的差异越来越小。该结果表明，信号和人工噪声功率的分配影响可获得的保密容量，存在一个最佳的功率分配方案使保密容量最大。当 a 较小时，发送人工噪声的功率较多，本文方案利用有利的人工噪声使合法接收者的性能改善较大，而随着 a 的增大，人工噪声 P_{z}逐渐减小，本文方案对合法接收端信噪比的改善作用也逐渐减小，因此对保密容量的提升也相应减小。

图 6 和图 7 分别是采用 BPSK, QPSK 调制方式时，在最优的功率分配因子下，保密容量随发送总功率 P 变化的仿真结果。发送天线数目 N 为 3 和 4。从图中可以看出，当采用最优的功率分配因子时，保密容量随发送端功率的增大和发送天线数目的增加而提高，本文方案的性能始终优于传统方案。

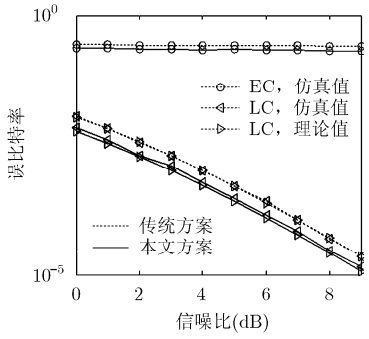


图 2 误比特率随信噪比的变化，BPSK

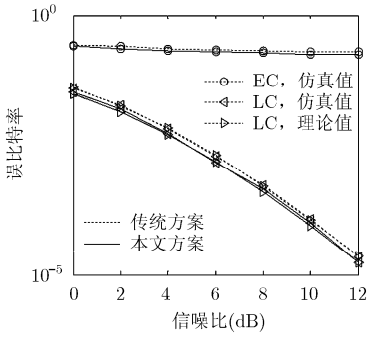


图 3 误比特率随信噪比的变化，QPSK

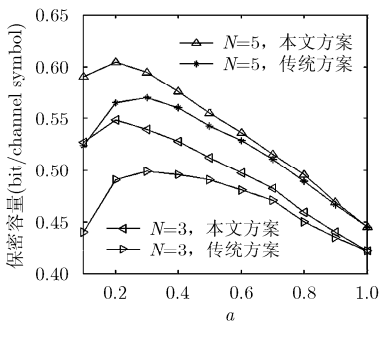


图 4 保密容量 C_{s}与 a, N 的关系，BPSK 调制

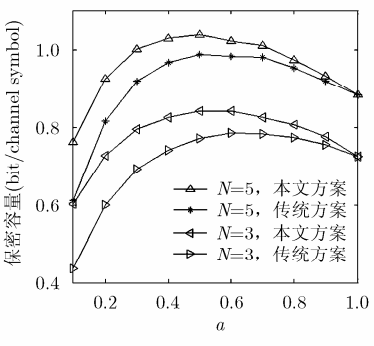


图 5 保密容量 C_s 与 a, N 的关系，QPSK 调制

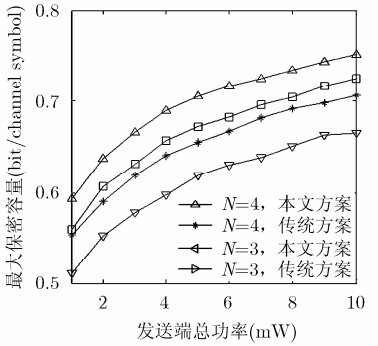


图 6 保密容量与 N, P 的关系，BPSK 调制

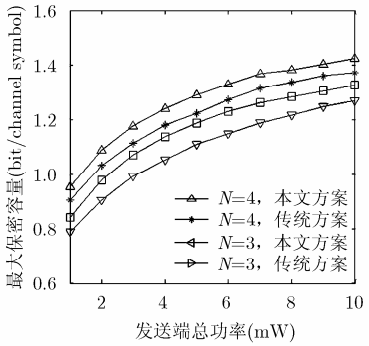


图 7 保密容量与 N, P 的关系，QPSK 调制

5 结束语

本文对未知 ECSI 情况下的 MISO 系统中采用信号波束赋形和人工噪声的物理层安全传输方案进行研究，提出了一种人工噪声新方案。在发送端，联合考虑合法信道的状态信息和人工噪声具体取值，判断到达合法接收端的人工噪声是否对其信号检测有利，并由此将人工噪声划分为有益噪声与无益噪声两类，采用不同的波束赋形方案。人工噪声有益时，采用全向波束赋形矢量，人工噪声可改善合法接收者的检测性能；而当人工噪声为无益噪声时，则利用波束赋形使其处于合法信道零空间，人工噪声不对合法接收者产生干扰。结合特定的 BPSK 和 QPSK 调制方式，给出了人工噪声是否有益的判别规则，分析了对应的误比特率和保密容量。分析和仿真结果表明，通过利用有利的人工噪声，相比较传统的人工噪声方案，本方案中合法接收者的性能有较为明显的提升，安全性能得到改善。

参 考 文 献

[1] SHANNON C E. Communication theory of secrecy system[J]. *Bell System Technical Journal*, 1949, 28(4): 656–710. doi: 10.1002/j.1538-7305.1949.tb00928.x.

[2] HONG W Y P, LAN P C, and KUO C C J. Enhancing physical-layer secrecy in multi-antenna wireless systems: an overview of signal processing approaches[J]. *IEEE Signal Processing Magazine*, 2013, 30(5): 29–40. doi: 10.1109/MSP.2013.2256953.

[3] CHEN X, ZHONG C, YUEN C, *et al*. Multi-antenna relay aided wireless physical layer security[J]. *IEEE Communications Magazine*, 2015, 53(12): 40–46. doi: 10.1109/MCOM.2015.7355564.

[4] CHEN X and LEI L. Energy-efficient optimization for physical layer security in multi-antenna downlink networks with QoS guarantee[J]. *IEEE Communications Letters*, 2013, 17(4): 637–640. doi: 10.1109/LCOMM.2013.022713.130029.

[5] MA H and MA P. Beamforming design of decode-and- forward cooperation for improving wireless physical layer security[C]. 2013 15th International Conference on Advanced Communication Technology (ICACT), PyeongChang, 2013: 41–49.

[6] NEGI R and GOEL S. Secret communication using artificial noise[C]. IEEE Vehicular Technology Conference (VTC-2005-Fall), Dallas, USA, 2005: 1906–1910. doi: 10.1109/VETECF.2005.1558439

[7] CHAE S H, CHOI W, LEE J H, *et al*. Enhanced secrecy in stochastic wireless networks: artificial noise with secrecy protected zone[J]. *IEEE Transactions on Information Forensics and Security*, 2014, 9(10): 1617–1627. doi: 10.1109/TIFS.2014.2341453.

[8] GREBRACHT S, WOLF A, and JORSWIECK E A. Beamforming for fading wiretap channels with partial channel information[C]. International Workshop on Smart Antennas, Bremen, Germany, 2010: 394–401. doi: 10.1109/WSA.2010.5456398.

[9] HUANG J and SWINDLEHURST A L. Robust secure transmission in MISO channels based on worst-case optimization[J]. *IEEE Transactions on Signal Processing*, 2012, 60(4): 1696–1707. doi: 10.1109/TSP.2011.2182344.

[10] GREBRACHT S, SCHEUNERT C, and JORSWIECK E A. Secrecy outage in MISO systems with partial channel information[J]. *IEEE Transactions on Information Forensics and Security*, 2012, 7(2): 704–716. doi: 10.1109/TIFS. 2011.2181946.

[11] HU F, GAO F, ZHANG T, *et al*. Physical-layer security for full-duplex communications with self-interference mitigation[J]. *IEEE Transactions on Wireless Communications*, 2016, 15(1): 329–340. doi: 10.1109/TWC. 2015.2472527.

[12] YANG Y, SUN C, ZHAO H, *et al*. Algorithms for secrecy guarantee with null space beamforming in two-way relay networks[J]. *IEEE Transactions on Signal Processing*, 2014, 62(8): 2111–2126. doi: 10.1109/TSP.2014.2303942.

[13] ZHANG X, ZHOU X, MCKAY M R, *et al*. Arti cial-noise-aided secure multi-antenna transmission with limited feedback[J]. *IEEE Transactions on Wireless Communications*, 2015, 14(5): 2742–2754. doi: 10.1109/ICASSP.2014.6854346.

[14] SIMON M K and ALOUIION M S. Digital Communication over Fading Channels[M]. New York: John Wiley & Sons, Inc., 2000: 265–267.

雷维嘉： 男，1969 年生，博士生，教授，主要研究方向为无线通信和移动通信技术.

林秀珍： 女，1990 年生，硕士生，研究方向为无线通信和物理层安全.

杨小燕： 女，1990 年生，硕士生，研究方向为物理层安全.