doi:10.3969/j.issn.1000-436X.2012.10.018

基于人工噪声的 MISO 保密容量分析

吉江，金梁，黄开枝
（国家数字交换系统工程技术研究中心，河南 郑州 450002）

摘 要：对 MISO 系统的发射功率分配和噪声形成方法进行讨论。首先建立 MISO 系统的人工噪声模型，将人工噪声等效为加性信道噪声，指出当人工噪声服从高斯分布是具有最大保密容量，并给出其保密容量表达式。然后在总发射功率受限的条件下，利用向量空间投影的方法推导保密容量最佳的功率分配方案。最后采用 Box-Muller 变换方法结合向量空间投影给出最佳功率分配方法下服从高斯分布的人工噪声生成方法。

关键词：MISO 系统；保密容量；物理层安全；人工噪声
中图分类号：TN919.3 **文献标识码**：A **文章编号**：1000-436X(2012)10-0138-05

Secrecy capacity analysis of MISO system with artificial noise

JI Jiang, JIN Liang, HUANG Kai-zhi
((National Digital Switching System Engineering & Technological Research Center, Zhengzhou 450002, China)

Abstract: Adding artificial noise in the MISO system was an effective method to improve the security. The transmit power allocation and artificial noise generation was mainly discussed. An artificial noise model of MISO system was presented, in which the artificial noise was regarded as additive channel noise. It was proven that when the artificial noise was distributed on Gaussian distribution, the secrecy capacity of MISO system was maximized, and the expression of this secrecy capacity was deduced. Considering the transmit power constraint and using the vector space projection method, The optimum power allocation is obtained. Given a power allocation, the artificial noise is generated by Box-Muller transformation, which was distributed on Gaussian distribution. And with the vector projection method, the artificial noise meets the optimum power allocation.

Key words: MISO system; secrecy capacity; physical layer security; artificial noise

1 引言

无线信道的时变特性、随机特性和差异性是区别于有线信道的重要特征，也是无线通信物理层加密的研究重点。1975 年 Wyner 提出了接线窃听加密模型，首次讨论信道对系统安全性的影响，并引入了保密容量来衡量系统安全性能[1]。在文献[2]中，按照接线窃听模型 I. Csiszár 和 J. Kōner 推导出广播信道情况下的保密容量为

$$C_s = \max_{P_X P_{YZ|X}} \left[I(X;Y) - I(X;Z) \right] \quad (1)$$

其中，X 为发送信息；Y 为授权用户接收的信息；Z 为第三方用户接收的信息。通过式（1）可计算出当发送端与授权用户通信时，第三方完全无法截获的前提下授权用户的最大信道容量为 C_s。文献[1]和文献[2]的研究引发了利用信息论讨论各种场景接线窃听模型的热潮。文献[3]讨论了存在加性高斯噪声情况下的接线窃听模型，并给出了此时的保密

收稿日期：2011-06-07；**修回日期**：2012-04-08
基金项目：国家自然科学基金资助项目（61171108）
Foundation Item: The National Natural Science Foundation of China (61171108)

容量，由于 AWGN（adding gaussian white noise）在无线通信研究中的基础地位，接线窃听模型随后被进一步发展。2008 年，文献[4]对已有的接线窃听模型下不同应用场景的保密容量、安全信道编码方式等方面做了总结。接线窃听模型为无线物理层加密提供了较好的解决思路，但其要求授权用户的信道质量好于第三方用户。

随着无线安全研究的不断发展，近几年出现的利用 MISO 系统多天线发射人工噪声来实现物理层加密的方法[5]较好地解决了上述问题。该方法通过在与授权用户信道特征正交的空间内发射噪声，降低第三方的接收信号质量，从而可以提高保密容量。所以即使第三方用户端的信号信噪比高于授权用户端的信号信噪比，通过发射人工噪声可以使授权用户获得可观的保密容量。同时文献[5]中给出了在 AWGN 信道中的保密容量下限。文献[6]随后对其在衰落环境下的保密容量进行了讨论。文献[7]中讨论的是如何根据衰落信道状况动态分配多根发射天线上的功率。事实上，影响系统安全性的一个重要问题是当发射总功率一定时，如何分配人工噪声和传输信息的功率从而使得系统保密容量最大，并且利用该分配方法如何生成人工噪声。

针对此问题，文中首先建立基于人工噪声的 MISO 物理层安全系统模型，在系统分析后，将人工噪声等效成为第三方用户的接收信号引入了加性的噪声。随后根据信息论相关原理，功率受限的条件下，高斯分布具有最大信息熵，所以人工噪声的分布为高斯分布时系统具有最大保密容量。由于发送端的总发射功率一定，文中对功率在信息和人工噪声间的分配进行了讨论，采用空间投影的分析方法可知，人工噪声物理层安全方法是在与授权用户信道特征向量正交的空间内引入噪声，从而只对与授权用户信道存在差异的接收方产生干扰，借助于信道特征向量的空间位置关系推导了最佳功率分配方案。在此基础上利用 Box-Muller 变换方法给出高斯加性人工噪声的具体生成方法。

2　基于人工噪声的 MISO 系统安全模型

2.1　MISO 系统模型

首先介绍 MISO 的系统模型，设 MISO 系统的发射端（后文用“Alice”表示）有 $M(M \geqslant 2)$根天线；授权用户（后文用“Bob”表示）有 1 根天线；第三接收方（后文用“Eve”表示）有 1 根天线。若定义 Alice 的 M 根天线上发射信号为 $\boldsymbol{X}=\left[x_1 \quad x_2 \quad \cdots \quad x_M\right]^{\mathrm{T}}$，其中的元素独立同分布。发送端的 M 根天线到 Bob 端天线的信道特征（信道状态）归一化向量为 $\boldsymbol{h}_{\mathrm{b}}=\left[h_{\mathrm{b},1}, h_{\mathrm{b},2}, \cdots, h_{\mathrm{b},M}\right]^{\mathrm{T}}$，其中，$h_{b,i}=A_i \mathrm{e}^{\mathrm{j}\phi_i}$，$i=1,2,\cdots,M$，$A_i$ 表示第 i 根发射天线传输到单根接收天线的信号幅度；ϕ_i 为第 i 根发射天线传输到单根接收天线的信号相角值；所以 Bob 单根天线接收的信号为

$$y_{\mathrm{B}}=\boldsymbol{h}_{\mathrm{b}}^{\mathrm{T}} \boldsymbol{X}+n_{\mathrm{B}}=\sum_{i=1}^{M} A_i \mathrm{e}^{\sqrt{-1}\cdot\phi_i} x_i+n_{\mathrm{B}} \tag{2}$$

其中，n_{B} 表示单根接收天线上的高斯加性噪声；x_i 为第 i 根发射天线发送的信号，是 $\boldsymbol{X}$ 中的元素。发送端的 M 根天线到第三方用户端天线的信道特征归一化向量为 $\boldsymbol{h}_{\mathrm{e}}=\left[h_{\mathrm{e},1}, h_{\mathrm{e},2}, \cdots, h_{\mathrm{e},M}\right]^{\mathrm{T}}$，其中，$h_{e,i}=E_i \mathrm{e}^{\mathrm{j}\varphi_i}$，即第三方的接收信号为

$$y_{\mathrm{E}}=\boldsymbol{h}_{\mathrm{e}}^{\mathrm{T}} \boldsymbol{X}=\sum_{i=1}^{M} E_i \cdot \mathrm{e}^{\sqrt{-1}\cdot\varphi_i} \cdot x_i+n_{\mathrm{E}} \tag{3}$$

其中，E_i 表示第 i 根发射天线传输到接收天线的信号幅度；φ_i 为第 i 根发射天线传输到接收天线的信号相角值；n_{E} 表示接收天线上的高斯加性噪声；x_i 为第 i 根发射天线发送的信号。

2.2　MISO 系统物理层安全模型

后文所用的物理层安全模型可描述如下：首先 Alice 将信源数据 $\boldsymbol{X}$ 送往加密系统 $\boldsymbol{G}$，经过加密后发送到无线信道中。按照前述，Alice 与 Bob 的无线信道特征向量为 $\boldsymbol{h}_{\mathrm{b}}$，与 Eve 的无线信道特征向量为 $\boldsymbol{h}_{\mathrm{e}}$；Bob 接收到的信号为 y_{B}，第三方用户收到的信号为 y_{E}。为使加密系统与后续的 $\boldsymbol{h}_{\mathrm{b}}$ 和 $\boldsymbol{h}_{\mathrm{e}}$ 分别形成新的信道特征（等效信道特征），加密系统可表示为

$$\boldsymbol{G}=\begin{bmatrix} g_{(1,1)} & g_{(1,2)} & \cdots & g_{(1,M)} \\ g_{(2,1)} & g_{(2,2)} & \cdots & g_{(2,M)} \\ & & \ddots & \\ g_{(M,1)} & g_{(M,2)} & \cdots & g_{(M,M)} \end{bmatrix} \tag{4}$$

所以加密后 Alice 与 Bob 之间的等效信道特征为 $\boldsymbol{G}\boldsymbol{h}_{\mathrm{b}}=\boldsymbol{H}_{\mathrm{B}}$，$\boldsymbol{H}_{\mathrm{B}}=\left[h_{\mathrm{B},1}, h_{\mathrm{B},2}, \cdots, h_{\mathrm{B},M}\right]$；则对于 Eve 有等效信道特征 $\boldsymbol{G}\boldsymbol{h}_{\mathrm{e}}=\boldsymbol{H}_{\mathrm{E}}$，其中，$\boldsymbol{H}_{\mathrm{E}}=[h_{\mathrm{E},1}, h_{\mathrm{E},2}, \cdots, h_{\mathrm{E},M}]$。此时 Bob 端接收天线的接收信号为

$$y_{\mathrm{B}} = \boldsymbol{h}_{\mathrm{b}}\boldsymbol{G}\boldsymbol{X} + n_{\mathrm{B}} = \boldsymbol{H}_{\mathrm{B}}\boldsymbol{X} + n_{\mathrm{B}} \tag{5}$$

Eve 接收天线的接收信号为

$$y_{\mathrm{E}} = \boldsymbol{h}_{\mathrm{e}}\boldsymbol{G}\ \boldsymbol{X} + n_{\mathrm{E}} = \boldsymbol{H}_{\mathrm{E}}\boldsymbol{X} + n_{\mathrm{E}} \tag{6}$$

事实上，现有物理层安全方案中的人工噪声可由加密系统 $\boldsymbol{G}$ 引入，所以有 $\boldsymbol{G} = \boldsymbol{G}_1 + \boldsymbol{G}_2$，其中，$\boldsymbol{G}_1$ 用于传输信息；$\boldsymbol{G}_2$ 用于为 Eve 端引入人工噪声，可用作承载人工噪声 R 来增加保密容量。为避免在 Bob 的接收信号中引入人工噪声，通常有 $\boldsymbol{G}_2\boldsymbol{h}_{\mathrm{b}}=\boldsymbol{0}$。根据式（4）、式（5）在引入人工噪声后 Bob 端接收天线的接收信号为

$$y_{\mathrm{B}} = \boldsymbol{h}_b\boldsymbol{G}_1\boldsymbol{X} + \boldsymbol{h}_{\mathrm{b}}\boldsymbol{G}_2\boldsymbol{R} + n_{\mathrm{B}} = \boldsymbol{h}_{\mathrm{b}}\boldsymbol{G}_1\boldsymbol{X} + n_{\mathrm{B}} \tag{7}$$

Eve 接收天线的接收信号为

$$y_{\mathrm{E}} = \boldsymbol{h}_{\mathrm{e}}\boldsymbol{G}_1\boldsymbol{X} + \boldsymbol{h}_{\mathrm{e}}\boldsymbol{G}_2\boldsymbol{R} + n_{\mathrm{E}} \tag{8}$$

从式（6）、式（7）可以看出，$\boldsymbol{G}_1$ 用于传送信息 X；而 $\boldsymbol{G}_2$ 承载人工噪声 R 只作用于 Eve 端，因此 Alice 的总发射功率 P_X 通过加密系统后分散在 2 部分中，第 1 部分为 $\boldsymbol{G}_1\boldsymbol{X}$，其中保留有信息 $\boldsymbol{X}$，令这一部分的功率为 $\left\|\boldsymbol{G}_1\boldsymbol{X}\right\|^2 = P_{X1}$；另外一部分为 $\boldsymbol{G}_2\boldsymbol{R}$，用于在 Eve 的信道中引入噪声，令这一部分的功率为 $\left\|\boldsymbol{G}_2\boldsymbol{X}\right\|^2 = P_{X2}$，功率满足 $P_X = P_{X1} + P_{X2}$。

所以后续讨论的保密容量为安全传输 X 的最大传输速率，$\boldsymbol{G}_2\boldsymbol{R}$ 为随机人工噪声向量。

按照上述描述，利用加性人工噪声提高物理层安全性的模型如图 1 所示，Alice 端的信息 S 经过编码器后变为 $\boldsymbol{X}+\boldsymbol{R}$，加密系统利用信道特征从其中分离出信息部分 $\boldsymbol{G}_1\boldsymbol{X}$ 和人工噪声部分 $\boldsymbol{G}_2\boldsymbol{R}$，其中人工噪声只在 Eve 端可以收到。所以需满足

$$\boldsymbol{G}_1\boldsymbol{R} = \boldsymbol{0},\ \ \boldsymbol{G}_2\boldsymbol{X} = \boldsymbol{0} \tag{9}$$

若令总发射功率为 $P_X = 1$，不考虑人工噪声 $\boldsymbol{G}_2\boldsymbol{R}$，当 $\boldsymbol{h}_{\mathrm{b}}\boldsymbol{G}_1\boldsymbol{X}$ 服从高斯分布时，文中的 MISO 系统可为高斯窃听信道模型，按照文献[3]中所述其保密容量为

$$C_{\mathrm{sec}} = \frac{1}{2}\left[\log(1+\frac{\left\|\boldsymbol{h}_{\mathrm{b}}\boldsymbol{G}_1\boldsymbol{X}\right\|^2}{\delta_{\mathrm{B}}^2}) - \log(1+\frac{\left\|\boldsymbol{h}_{\mathrm{e}}\boldsymbol{G}_1\boldsymbol{X}\right\|^2}{\delta_{\mathrm{E}}^2})\right] \tag{10}$$

按照图 1 所示引入加性人工噪声 $\boldsymbol{G}_2\boldsymbol{R}$ 后，由于在实际系统中人工噪声的功率受限，所以人工噪声项 $\boldsymbol{h}_{\mathrm{e}}\boldsymbol{G}_2\boldsymbol{R}$ 服从高斯分布时，系统具有最大安全容量。

结论 1 如果在式(7)和式(8)表示的加性人工噪声模型中，噪声 $\boldsymbol{n}_{\mathrm{B}}$ 和 $\boldsymbol{n}_{\mathrm{E}}$ 都服从正态分布，则当 $\boldsymbol{h}_{\mathrm{e}}\boldsymbol{G}_2\boldsymbol{R}$ 服从正态分布，并且与 $\boldsymbol{X}$ 相互独立时，系统达到最大安全信道容量

$$C'_{\mathrm{sec}} = \frac{1}{2}\log\left(\frac{\delta_{\mathrm{B}}^2 + \left\|\boldsymbol{h}_{\mathrm{b}}\boldsymbol{G}_1 X\right\|^2}{\delta_{\mathrm{B}}^2}\frac{\delta_{\mathrm{E}}^2 + \left\|\boldsymbol{h}_{\mathrm{e}}\boldsymbol{G}_2 R\right\|^2}{\delta_{\mathrm{E}}^2 + \left\|\boldsymbol{h}_{\mathrm{e}}\boldsymbol{G}_2 R\right\|^2 + \left\|\boldsymbol{h}_{\mathrm{e}}\boldsymbol{G}_1 X\right\|^2}\right) \tag{11}$$

3 发射功率的最优化讨论

下面讨论如何通过空间投影的方法设计加密系统，从而使得高斯噪声条件下，图 1 所示的 MISO 系统的人工噪声模型保密容量最大化。

由于 $\boldsymbol{G}_2\boldsymbol{R}$ 和 $\boldsymbol{G}_1\boldsymbol{X}$ 同为 $M\times 1$ 维向量。在式(11)中，由于随机矩阵 $\boldsymbol{G}_2$ 和 $\boldsymbol{h}_{\mathrm{b}}$ 的方向垂直。按照向量的投影计算可得

$$\begin{aligned}\left\|\boldsymbol{h}_{\mathrm{b}}\boldsymbol{G}_1\boldsymbol{X}\right\|^2 &= \left\|\boldsymbol{h}_{\mathrm{b}}\right\|^2\left\|\boldsymbol{G}_1\boldsymbol{X}\right\|^2\cdot\cos^2(\alpha_{\mathrm{b}})\\ &= \left\|\boldsymbol{h}_{\mathrm{b}}\right\|^2 P_{X1}\cos^2(\alpha_{\mathrm{b}})\end{aligned} \tag{12}$$

$$\begin{aligned}\left\|\boldsymbol{h}_{\mathrm{e}}\boldsymbol{G}_2\boldsymbol{R}\right\|^2 &= \left\|\boldsymbol{h}_{\mathrm{e}}\right\|^2\left\|\boldsymbol{G}_2\boldsymbol{R}\right\|^2\cos^2(\alpha_{\mathrm{e2}})\\ &= \left\|\boldsymbol{h}_{\mathrm{e}}\right\|^2 P_{X2}\cos^2(\alpha_{\mathrm{e2}})\end{aligned} \tag{13}$$

其中，$\alpha_{\mathrm{b}} = 0$ 为 $\boldsymbol{h}_{\mathrm{b}}$ 和 $\boldsymbol{G}_1\boldsymbol{X}$ 的夹角；α_{e2} 为 $\boldsymbol{h}_{\mathrm{e}}$ 和 $\boldsymbol{G}_2\boldsymbol{R}$ 的夹角；令 α_{e1} 为 $\boldsymbol{h}_{\mathrm{e}}$ 和 $\boldsymbol{G}_1\boldsymbol{X}$ 的夹角。

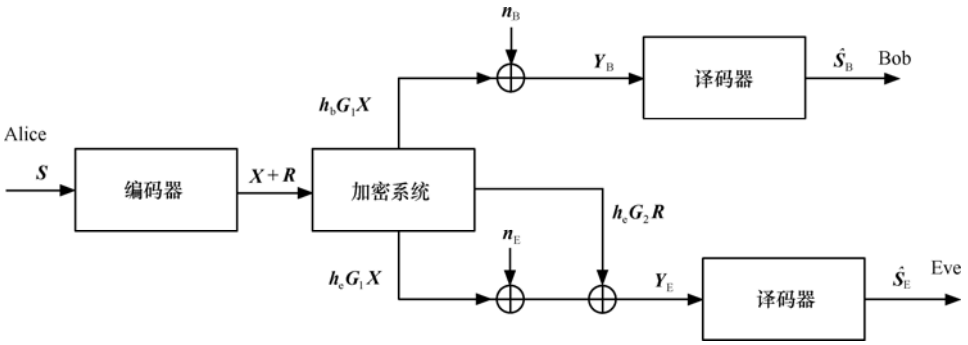

图 1 加性人工噪声系统模型

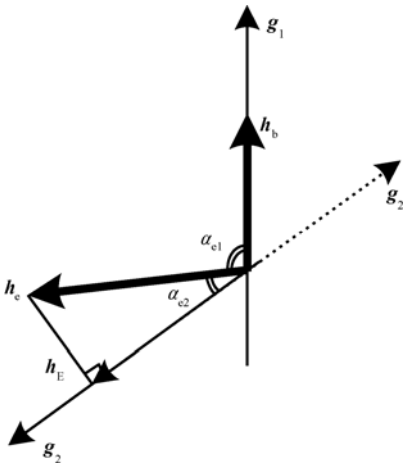

图 2　$\boldsymbol{G}_2\boldsymbol{R}$ 沿直线方向变化的投影示意

如图 2 所示，如果固定 $\boldsymbol{G}_2\boldsymbol{R}$ 的方向在 $\boldsymbol{g}_2$ 上，此时 α_{e2} 服从 $\alpha_{e2}\in\{\alpha,\alpha+\pi\}$ 的二项分布。则根据结论一可知当投影量 $\|\boldsymbol{G}_2\boldsymbol{R}\|^2\cos\alpha_{e2}$ 服从高斯分布时，可达到式(11)的最大保密容量。由于 $\|\boldsymbol{G}_2\boldsymbol{R}\|^2\cos\alpha_{e2}=P_{X2}\cos\alpha_{e2}$，所以当 α_{e2} 服从等概率的二项分布时，并且 $\|\boldsymbol{G}_2\boldsymbol{R}\|^2\cos\alpha_{e2}$ 服从高斯分布时。根据式(11)，此时保密容量为

$$C_{\text{sec}}=\frac{1}{2}\log\left(\frac{\delta_{\text{B}}^2+\|\boldsymbol{h}_{\text{b}}\|^2P_{X1}\cos^2(\alpha_{\text{b}})}{\delta_{\text{B}}^2}\cdot\frac{\delta_{\text{E}}^2+\|\boldsymbol{h}_{\text{e}}\|^2P_{X2}\cos^2(\alpha_{e2})}{\delta_{\text{E}}^2+\|\boldsymbol{h}_{\text{e}}\|^2P_{X2}\cos^2(\alpha_{e2})+\|\boldsymbol{h}_{\text{e}}\|^2P_{X1}\cos^2(\alpha_{\text{e1}})}\right)=\frac{1}{2}\log\frac{\left(\delta_{\text{B}}^2+K_1P_{x1}\right)\left(\delta_{\text{E}}^2+K_2P_{x2}\right)}{\delta_{\text{B}}^2\left(\delta_{\text{E}}^2+K_2P_{x2}+K_3P_{x1}\right)}\tag{14}$$

其中，$K_1=\|\boldsymbol{h}_{\text{b}}\|^2\cos^2\alpha_{\text{b}}$，$K_2=\|\boldsymbol{h}_{\text{e}}\|^2\cos^2\alpha_{e2}$，$K_3=\|\boldsymbol{h}_{\text{e}}\|^2\cos^2\alpha_{\text{e1}}$。通过系统中的随机变量 $\boldsymbol{G}_2$ 取得式(14)所示的保密容量，在 $\boldsymbol{G}_2$ 随机变化的同时 $\boldsymbol{G}_1$ 保持恒定。若 δ_X^2 分配功率为 P_{x1} 和 P_{x2}，式(14)中的 C_{sec} 取最大值。由于 $P_{x1}=\lambda\delta_X^2$，$P_{x2}=(1-\lambda)\delta_X^2$。所以只要求解式(14)满足

$$\frac{\partial C_{\text{sec}}(\lambda)}{\partial\lambda}=0\tag{15}$$

可以解出得到 λ，排除掉一个不符合取值范围的解后，最终得如下的解：

$$\lambda^*=\frac{\sqrt{K_1K_2}(\delta_{\text{E}}^2+K_2\delta_x^2)-\sqrt{K_3(\delta_{\text{E}}^2+K_2\delta_x^2)((K_2-K_3)\delta_{\text{B}}^2+K_1\delta_{\text{E}}^2+K_1K_2\delta_x^2)}}{\sqrt{K_1K_2}(K_2-K_3)\delta_x^2}\tag{16}$$

结论 2　当 MISO 系统加性人工噪声模型达到结论 1 的保密容量时，如果信息 $\boldsymbol{X}$ 的分配因子 $\lambda=\lambda^*$，则保密容量达到最大值

$$C_{\text{sec}}=\frac{1}{2}\log\frac{\left(\delta_{\text{B}}^2+K_1\lambda^*\delta_X^2\right)\left(\delta_{\text{E}}^2+K_2(1-\lambda^*)\delta_X^2\right)}{\delta_{\text{B}}^2\left(\delta_{\text{E}}^2+K_2(1-\lambda^*)\delta_X^2+K_3\lambda^*\delta_X^2\right)}\tag{17}$$

4　人工噪声的生成算法

事实上，由于 Eve 为第三方用户，其信道特征 $\boldsymbol{h}_{\text{e}}$ 往往未知，所以在式(16)中 $\boldsymbol{h}_{\text{e}}$、$\cos^2\alpha_{\text{e}}$ 和 $\cos^2\alpha_{e1}$ 未知，且保密容量 C_{sec} 是 $\cos\alpha_{\text{e}}$ 的增函数，所以如果固定 $\boldsymbol{G}_2$ 的方向则有可能 $\alpha_{\text{e}}\to90^\circ$，$\boldsymbol{h}_{\text{e}}$ 在其方向的投影趋近于 0，导致 $C_{\text{sec}}\to C_{\text{sec}}^{'}$，从而 C_{sec} 较小。

由于 $\boldsymbol{h}_{\text{e}}$ 未知，为获得平均意义下 $\boldsymbol{h}_{\text{e}}$ 在 $\boldsymbol{G}_2\boldsymbol{R}$ 方向上的投影值，需变化 $\boldsymbol{G}_2\boldsymbol{R}$ 的方向。由于 $\boldsymbol{h}_{\text{e}}$ 的未知性，可认为 $\boldsymbol{h}_{\text{e}}$ 在整个空间均匀分布。为此需要在与 $\boldsymbol{G}_1\boldsymbol{X}$ 垂直的空间内转动 $\boldsymbol{G}_2\boldsymbol{R}$，使 $\boldsymbol{G}_2\boldsymbol{R}$ 均匀地分布于整个平面方向。如图 3 所示，$\boldsymbol{g}_2^{(2)}$ 是 $\boldsymbol{h}_{\text{e}}$ 在与 $\boldsymbol{h}_{\text{b}}$ 垂直的平面上的投影方向，$\boldsymbol{g}_2^{(2)}$ 和 $\boldsymbol{h}_{\text{e}}$ 的夹角为 α。在第 t 时刻，用 $\boldsymbol{g}_2^{(2)}$ 表示 $\boldsymbol{G}_2\boldsymbol{R}$ 向量。$\boldsymbol{g}_2^{(2)}$ 与 $\boldsymbol{g}_2^{(2)}(t)$ 的夹角为 β。$\boldsymbol{h}_{\text{E}}$ 是 $\boldsymbol{h}_{\text{e}}$ 在 $\boldsymbol{g}_2^{(2)}(t)$ 上的投影，所以

$$\|\boldsymbol{h}_{\text{E}}\|=\boldsymbol{h}_{\text{e}}\boldsymbol{g}_2^{(2)}(t)=\|\boldsymbol{h}_{\text{e}}\|\cdot\|\boldsymbol{g}_2^{(2)}(t)\|\cos(\alpha)\cos(\beta)\tag{18}$$

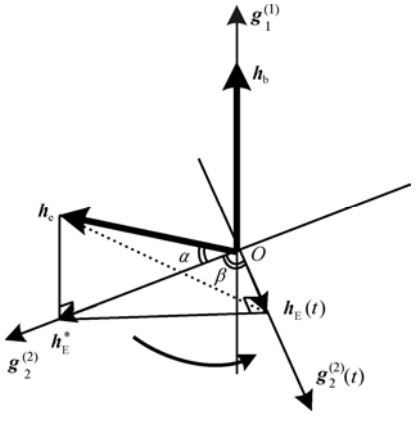

图 3　$\boldsymbol{G}_2$ 沿平面转动的投影示意

其中，由于 Eve 的信道特征向量 $\boldsymbol{h}_{\text{e}}$ 未知，可认为式(18)中的 α 服从均匀分布。按照结论 1 可知，当 $\boldsymbol{h}_{\text{e}}\boldsymbol{G}_2\boldsymbol{R}$ 服从高斯分布时，系统可以达到保密容量。代入式(18)可得

$$\boldsymbol{h}_{\mathrm{e}}\boldsymbol{G}_2\boldsymbol{R}=\boldsymbol{h}_{\mathrm{e}}\boldsymbol{g}_2^{(2)}(t)=\left\|\boldsymbol{h}_{\mathrm{e}}\right\|\cdot\left\|\boldsymbol{g}_2^{(2)}(t)\right\|\cos(\alpha)\cos(\beta) \quad (19)$$

对于每一个 Eve 来说，$\boldsymbol{h}_{\mathrm{e}}$ 和 α 为恒定值。所以需要设计 β 和 $\left\|\boldsymbol{g}_2^{(2)}(t)\right\|$ 的概率分布方式，从而使式(19)服从高斯分布。按照文献[8]中的 Box-Muller 变换方法，若相互独立的 U_1 和 U_2 均服从[0,1)的均匀分布。则令

$$\left\|\boldsymbol{g}_2^{(2)}(t)\right\|=\sqrt{-2\ln(U_2)} \quad (20)$$

$$\beta=2\pi U_1 \quad (21)$$

则 $\boldsymbol{h}_{\mathrm{e}}\boldsymbol{G}_2\boldsymbol{X}\sim\boldsymbol{N}\left(0,\ \left\|\boldsymbol{h}_{\mathrm{e}}\right\|^2\cos^2(\alpha)P_{x2}\right)$。结合结论 1 可以得到如下结论。

结论 3 如果第三方用户 Eve 一定，则当 $\left\|\boldsymbol{g}_2^{(2)}(t)\right\|$ 服从式(20)的分布、β 服从式(21)的分布时，系统有保密容量

$$C_{\mathrm{sec}}=\frac{1}{2}\log\left(\frac{\delta_{\mathrm{B}}^2+K_1P_{x1}}{\delta_{\mathrm{B}}^2}\frac{\delta_{\mathrm{E}}^2+K_4P_{x2}}{\delta_{\mathrm{E}}^2+K_4P_{x2}+K_5P_{x1}}\right) \quad (22)$$

其中，$K_1=\left\|\boldsymbol{h}_{\mathrm{b}}\right\|^2\frac{1}{M}\cos^2\alpha_{\mathrm{b}}$，$K_4=\left\|\boldsymbol{h}_{\mathrm{e}}\right\|^2\cos^2(\alpha)$，$K_5=\left\|\boldsymbol{h}_{\mathrm{e}}\right\|^2\sin^2(\alpha)$。

结论 4 当模型达到结论 3 的保密容量时，如果功率的分配因子 $\lambda=\lambda_1^*$，则保密容量达到最大值：

$$C_{\mathrm{sec}}=\frac{1}{2}\log\frac{\left(\delta_{\mathrm{B}}^2+K_1\lambda_1^*\delta_X^2\right)\left(\delta_{\mathrm{E}}^2+K_4(1-\lambda_1^*)\delta_X^2\right)}{\delta_{\mathrm{B}}^2\left(\delta_{\mathrm{E}}^2+K_4(1-\lambda_1^*)\delta_X^2+K_5\lambda_1^*\delta_X^2\right)} \quad (23)$$

此时

$$\lambda_1^*=\frac{\sqrt{K_1K_4}(\delta_{\mathrm{E}}^2+K_4\delta_x^2)-\sqrt{K_5(\delta_{\mathrm{E}}^2+K_4\delta_x^2)((K_4-K_5)\delta_{\mathrm{B}}^2+K_1\delta_{\mathrm{E}}^2+K_1K_4\delta_x^2)}}{\sqrt{K_1K_4}(K_4-K_5)\delta_x^2} \quad (24)$$

至此，当模型中能达到的最大的保密容量在式(22)中给出，并且当加密系统的 $\boldsymbol{G}_1$ 与 $\boldsymbol{h}_{\mathrm{b}}$ 同向且 $\boldsymbol{G}_2\boldsymbol{R}$ 按照式(20)和式(21)分布，同时此时的分配因子 $\lambda=\lambda_1^*$ 时，可以达到该保密容量。

5 结束语

本文对基于人工噪声的 MISO 物理层安全系统进行了深入分析，主要解决了人工噪声的功率分配问题和人工噪声最优化概率分布的生成问题。文中通过将人工噪声等效为加性信道噪声，指出当加性人工噪声项服从高斯分布时，系统具有最大的保密容量。随后推导出其保密容量表达式，以保密容量最大化为目标，给出了最佳功率分配方案。最后文中对人工噪声的方法进行讨论，利用 Box-Muller 变换方法产生符合系统保密容量最大化的加性人工噪声。

参考文献：

[1] WYNER A D. The wire-tap channel[J]. Bell Laboratory System Technology Journal, 1975, 54(8): 1355-1387.

[2] CSISZáR I, KöNER J. Broadcast channels with confidential messages[A]. IEEE Transactions on Information Theory[C]. 1978. 339-348.

[3] LEUNG S K, CHEONG Y, HELLMAN M E. The Gaussian wire-tap channel[A]. IEEE Transactions on Information Theory[C]. 1978. 451-456.

[4] LIANG Y, POOR H V, SHAMAI S. Information theoretic security[A]. Foundations and Trends in Communications and Information Theory[C]. 2008. 355-580.

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

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

[7] ZHOU X, MCKAY M R. Physical layer security with artificial noise: secrecy capacity and optimal power allocation[A]. International Conference Signal Processing and Communication Systems (ICSPCS 2009)[C]. 2009.

[8] BOX G E P, MERVIN E. A note on the generation of random normal deviates[J]. The Annals of Mathematical Statistics, 1958, 29(2): 610-611.

作者简介：

吉江（1983-），男，河南南乐人，国家数字交换系统工程技术研究中心博士生，主要研究方向为无线通信安全、超宽带通信。

金梁（1969-），男，北京人，国家数字交换系统工程技术研究中心教授、博士生导师，主要研究方向为阵列信号处理、数字通信。

黄开枝（1973-），女，安徽来安人，国家数字交换系统工程技术研究中心副教授、硕士生导师，主要研究方向为移动通信。