doi:10.3969/j.issn.1001-893x.2014.02.014
引用格式:段明义,黄继海,吉江. MISO 的普适性人工噪声保密容量[J]. 电讯技术,2014,54(2):189-194. [DUAN Ming-yi,HUANG Ji-hai,JI Jiang. Secrecy Capacity Analysis of General MISO System with Artificial Noise[J]. Telecommunication Engineering,2014,54(2):189-194.]

MISO 的普适性人工噪声保密容量*

段明义[1],黄继海[1,**],吉　江[2]

(1. 中州大学 信息工程学院,郑州 450044;2. 国家数字交换系统工程技术研究中心,郑州 450002)

摘　要:当 MISO(Multi Input Single Output)系统存在的加性人工噪声服从一般分布时,系统保密容量讨论难度较大。为推导一般意义多天线系统下的保密容量,引入了信道等效特征的概念。利用信道特征阐明了人工噪声方法的物理概念,并推导出了具有普适性的人工噪声方法保密容量上下限,进一步结合熵功率,推导出 AWGN 信道下的保密容量解析式。理论分析和仿真得出,通过人工噪声可使平均保密容量增大,从而提高 MISO 系统的安全性。

关键词:MISO 系统;保密容量;物理层安全;人工噪声
中图分类号:TN918　　**文献标志码**:A　　**文章编号**:1001-893X(2014)02-0189-06

Secrecy Capacity Analysis of General MISO System with Artificial Noise

DUAN Ming-yi[1],HUANG Ji-hai[1],JI Jiang[2]

(1. Information Engineering College,Zhongzhou University,Zhengzhou 450044, China;
2. National Digital Switching System Engineering Technological R&D Center,Zhengzhou 450002,China)

Abstract: When the artificial noise in multi-input single-output(MISO) follows general distribution, the security capacity is hard to be calculated. To deduce the secrecy capacity of general multi-antenna system, this paper presents an equivalent channel characteristic model. This model is used to describe intrinsically how the artificial noise method makes the wireless communication more safe. And the upper/lower limit of secrecy capacity is deduced. Then, with the entropy power, the analytic expression of secrecy capacity in AWGN channel is deduced. The theoretic and simulation analysis show that in a power limited system, the artificial methods can increase the average secrecy capacity and improve the security of MISO system.

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。1949 年,Shannon 首次讨论了具有一般性意义的加密系统,并提出实现完美加密的条件是第三方用户收到的信号与原始发送信息相互独立[1],但其中并未将信道纳入考虑。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[2]。在文献[3]中,按照接线窃听模型 I. Csiszár and J. Köner 推导出广播信道情况下授权用户的保密容量,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[2]和[3]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[4]讨论了存在加性高斯噪声情况下的接线窃听模型,并给出

*　**收稿日期**:2013-09-04;**修回日期**:2013-12-02　Received date:2013-09-04;Revised date:2013-12-02
基金项目:河南省科技厅科技攻关项目(122102210142)
Foundation Item: Key Technologies R&D Program of Science and Technology Department, Henan Province(No. 122102210142)
**　**通讯作者**:huangjihai@sina.com　**Corresponding author**: huangjihai@sina.com

了此时的保密容量,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。文献[5]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。

随着无线安全研究的不断发展,近几年出现了几种新的物理层加密方法[6-7],这些方法通过改变一些信道特征,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,通过改变信道特征可以使授权用户获得可观的保密容量。其中,文献[7]是一类利用 MISO(Multi-Input Singl-Output)系统多天线发射人工噪声来实现物理层加密,并给了高斯类型人工噪声的生成方法和 AWGN 信道中的保密容量;文献[8]对加性人工噪声方法在衰落环境下的保密容量进行了讨论;文献[9]中讨论的是如何根据信道状况动态分配发射功率的问题。对于一般性的 MISO 系统模型,所引入的人工噪声服从任意分布时,现有 MISO 系统中利用人工噪声实现物理层安全的保密容量讨论较少。而只有分析得到系统的保密容量,才能设计合适的安全编码实现信息的安全传输[1]。

本文从 MISO 系统发射人工噪声的物理层加密方法入手,将加入人工噪声的过程看作是改变了信道的传输特性。随后提出等效信道特征模型,并在此模型的基础上,借助于传统信息论中的熵功率,推导出具有普适性的利用加性人工噪声实现 MISO 系统安全的保密容量上下限,并在随后的仿真与分析中得到结论:当总发射功率受限时,通过人工噪声的方式,本质上是在等效信道的主信号能量和人工噪声能量二维空间内提高了平均保密容量,从而提高系统的整体安全性。

2 基于等效信道的 MISO 加密系统

首先建立 MISO 的系统模型。设 MISO 系统的发射端有 M 根天线,$M\geqslant 2$;接收端有 1 根天线。若定义发射端 M 根天线上的发射信号为

$$\boldsymbol{x}=[x_1 \quad x_2 \quad \cdots \quad x_M]^{\mathrm{T}}$$

其中的元素独立同分布。发送端的 M 根天线到授权用户端天线的信道特征向量为

$$\boldsymbol{h_b}=[h_{b,1},h_{b,2},\cdots,h_{b,M}]^{\mathrm{T}}$$

到第三方用户端天线的信道特征向量为

$$\boldsymbol{h_e}=[h_{e,1},h_{e,2},\cdots,h_{e,M}]^{\mathrm{T}}$$

其中,$h_{b,i}=A_i\cdot e^{j\phi_i}$,$h_{e,i}=E_i\cdot e^{j\varphi_i}$,$i=1,2,\cdots,M$,$A_i$ 和 E_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 和 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,所以授权用户和第三方用户单根天线接收的信号为

$$y_B=\boldsymbol{h}_b^{\mathrm{T}}\cdot\boldsymbol{X}+n_B=\sum_{i=1}^{M}A_i\cdot e^{\sqrt{-1}\cdot\phi_i}\cdot x_i+n_B,$$

$$y_E=\boldsymbol{h}_e^{\mathrm{T}}\cdot\boldsymbol{X}=\sum_{i=1}^{M}E_i\cdot e^{\sqrt{-1}\cdot\varphi_i}\cdot x_i+n_E \qquad (1)$$

其中,$y_B\in\boldsymbol{Y_B}$,$y_E\in\boldsymbol{Y_E}$,n_B 和 n_E 表示单根接收天线上的加性噪声,x_i 为第 i 根发射天线发送的信号,$x_i\in\boldsymbol{X}$。

图 1 是发射端将信源数据 $\boldsymbol{X}$ 送往加密系统 $\boldsymbol{G}$,经过加密后发送到无线信道中。同前所述,到授权用户的无线信道特征向量为 $\boldsymbol{h_b}$,到第三接收方的无线信道特征向量为 $\boldsymbol{h_e}$;授权用户接收到的信号为 y_B,第三方用户收到的信号为 y_E。

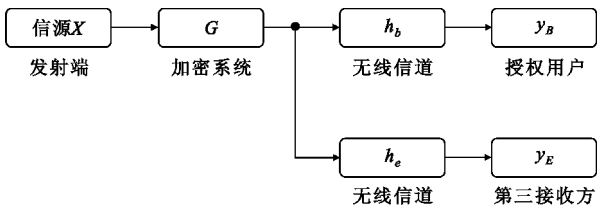


图 1 MISO 系统物理层加密结构

Fig. 1 The physical layer encryption structure of MISO system

为使加密系统与后续的 $\boldsymbol{h_b}$ 和 $\boldsymbol{h_e}$ 分别形成新的信道特征(等效信道特征),加密系统可表示为

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

所以在加密后授权用户的等效信道特征 $\boldsymbol{H_B}$ 为

$$\boldsymbol{G}\cdot\boldsymbol{h_b}=\boldsymbol{H_B},\boldsymbol{G}\cdot\boldsymbol{h_e}=\boldsymbol{H_E} \qquad (3)$$

其中,$\boldsymbol{H_B}=[h_{B,1},\cdots,h_{B,M}]^{\mathrm{T}}$,$\boldsymbol{H_E}=[h_{E,1},\cdots,h_{E,M}]^{\mathrm{T}}$。

$$y_B=\boldsymbol{h}_b^{\mathrm{T}}\cdot\boldsymbol{G}^{\mathrm{T}}\cdot\boldsymbol{X}+n_B=\boldsymbol{H}_{\boldsymbol{B}}^{\mathrm{T}}\cdot\boldsymbol{X}+n_B$$

$$y_E=\boldsymbol{h}_e^{\mathrm{T}}\cdot\boldsymbol{G}^{\mathrm{T}}\cdot\boldsymbol{X}+n_E=\boldsymbol{H}_E^{\mathrm{T}}\cdot\boldsymbol{X}+n_E \qquad (4)$$

与文献[7]类似,令 M 根天线上的 S 根发射人工噪声,即

$$x_i=x_{\mathrm{rand}},i=M-S+1,M-S+2,\cdots,M \qquad (5)$$

为防止窃听发送信号 $\boldsymbol{X}$ 被分为有用信号和噪声信号两部分,令 $\boldsymbol{G}=\boldsymbol{G}_1+\boldsymbol{G}_2$,其中 $\boldsymbol{G}_1=[\boldsymbol{g}_1^{(1)},\ \boldsymbol{g}_2^{(1)},\ \cdots,\ \boldsymbol{0}]^{\mathrm{T}}$ 用于传输有用信号部分,当 $i\neq 1,2,\cdots,M-s$ 时,$\boldsymbol{g}_i^{(1)}=\boldsymbol{0}$;而 $\boldsymbol{G}_2=[\boldsymbol{0},\ \boldsymbol{0},\ \cdots,\ \boldsymbol{g}_M^{(2)}]$ 用于传输人工噪声部分,当 $i=1,2,\cdots,M-s$ 时,$\boldsymbol{g}_i^{(2)}=\boldsymbol{0}$。此时,由式(7)可得授权用户的接收信号为

$$y_B=\boldsymbol{h}_b^{\mathrm{T}}\cdot\boldsymbol{G}_1^{\mathrm{T}}\cdot\boldsymbol{X}+\boldsymbol{h}_b^{\mathrm{T}}\cdot\boldsymbol{G}_2^{\mathrm{T}}\cdot\boldsymbol{X}+n_B \qquad (6)$$

从式(6)中可知,$\boldsymbol{h}_b^{\mathrm{T}} \cdot \boldsymbol{G}_2^{\mathrm{T}} \cdot \boldsymbol{X}$ 项表示人工噪声项,当此项为零时,Bob 端收到的信号信噪比较高。所以对于任意的 $\boldsymbol{X}$,应该有 $\boldsymbol{h}_b^{\mathrm{T}} \cdot \boldsymbol{G}_2^{\mathrm{T}} = \boldsymbol{0}$,即 $\boldsymbol{G}_2$ 的所有行向量属于 $\boldsymbol{h}_b$ 的垂直空间。所以有

$$y_B = \boldsymbol{h}_b^{\mathrm{T}} \cdot \boldsymbol{G}_1^{\mathrm{T}} \cdot \boldsymbol{X} + n_B,$$
$$y_E = \boldsymbol{h}_e^{\mathrm{T}} \cdot \boldsymbol{G}_1^{\mathrm{T}} \cdot \boldsymbol{X} + \boldsymbol{h}_e^{\mathrm{T}} \cdot \boldsymbol{G}_2^{\mathrm{T}} \cdot \boldsymbol{X} + n_E \quad (7)$$

通过保持加密系统中的 $\boldsymbol{G}_1$ 与 $\boldsymbol{h}_b$ 同向,而同时动态地随机产生式(7)中的 $\boldsymbol{G}_2$,最终在第三方的信道中引入更多的噪声。

3　利用等效特征加密的保密容量

根据式(11),整个加密传输过程可等效为图 2 中所示,原始信息 $\boldsymbol{M}$ 经过编码器后输出为 $\boldsymbol{X}$。经过利用等效信道特征进行加密的加密系统后传输到信道中,信道中存在自然加性噪声 $\boldsymbol{n}_B$ 和 $\boldsymbol{n}_E$,以及加密系统中通过等效信道特征产生的人工加性噪声 $\boldsymbol{h}_e^{\mathrm{T}} \cdot \boldsymbol{G}_2^{\mathrm{T}} \cdot \boldsymbol{X}$。

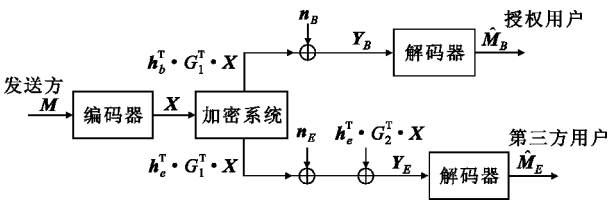


图 2　利用加性 MISO 加密系统的等效原理图

Fig. 2 The equivalent schematic of MISO encryption system using additive artificial noise

图 2 所示的模型本质上属于接线窃听模型,因此该模型的保密容量可由文献[3]中方法求得。保密容量为

$$C_s = \max_{P_X P_{YZ|X}} [I(X;Y) - I(X;Z)] \quad (8)$$

为讨论当人工噪声 $\boldsymbol{G}_2$ 服从任意分布时 MISO 系统的保密容量,假设 $\boldsymbol{X}$ 的功率为 δ_X^2,加性信道噪声 $n_B(k) \sim N(\mu_B, \delta_B^2)$,Eve 的加性信道噪声 $n_E(k) \sim N(\mu_E, \delta_E^2)$,令 $\sigma_{Y_B}^2$ 为信息 $\boldsymbol{Y}_B$ 的熵功率,$\sigma_{Y_E}^2$ 为信息 $\boldsymbol{Y}_E$ 的熵功率,$\sigma_{X_B}^2$ 为信息 $\boldsymbol{h}_b^{\mathrm{T}} \cdot \boldsymbol{G}_1^{\mathrm{T}} \cdot \boldsymbol{X}$ 的熵功率,$\sigma_{X_E}^2$ 为信息 $\boldsymbol{h}_e^{\mathrm{T}} \cdot \boldsymbol{G}_1^{\mathrm{T}} \cdot \boldsymbol{X}$ 的熵功率,$\sigma_{n_B}^2$ 为 $\boldsymbol{n}_B$ 的熵功率,$\sigma_{n_E}^2$ 为 $\boldsymbol{n}_E + \boldsymbol{h}_e^{\mathrm{T}} \cdot \boldsymbol{G}_2^{\mathrm{T}} \cdot \boldsymbol{X}$ 的熵功率[10]。

为使式(8)的信道容量最大化,首先讨论 $\boldsymbol{I}(\boldsymbol{Y}_B; \boldsymbol{X})$ 和 $\boldsymbol{I}(\boldsymbol{Y}_E; \boldsymbol{X})$ 的取值范围。在式(7)中 $\boldsymbol{X}$ 与噪声 $\boldsymbol{n}_B$ 和 $\boldsymbol{n}_E$ 相互独立,则根据加性信道特点可得

$$\boldsymbol{I}(\boldsymbol{Y}_B; \boldsymbol{X}) = H(\boldsymbol{Y}_B) - H(\boldsymbol{Y}_B | \boldsymbol{X}) = H(\boldsymbol{Y}_B) - H(\boldsymbol{n}_B) \quad (9)$$

$$\boldsymbol{I}(\boldsymbol{Y}_E; \boldsymbol{X}) = H(\boldsymbol{Y}_E) - H(\boldsymbol{h}_e^{\mathrm{T}} \cdot \boldsymbol{G}_2^{\mathrm{T}} \cdot \boldsymbol{X} + \boldsymbol{n}_E) \quad (10)$$

则按照文献[10]的定理 15 可知:

$$\sigma_{X_B}^2 + \sigma_{n_B}^2 \leqslant \sigma_{Y_B}^2 \leqslant \| \boldsymbol{H}_B \|^2 \delta_X^2 + \delta_B^2,$$
$$\sigma_{X_E}^2 + \sigma_{n_E}^2 + \sigma_{n_{E1}}^2 \leqslant \sigma_{Y_E}^2 \leqslant \| \boldsymbol{H}_E \|^2 \delta_X^2 + \delta_E^2 \quad (11)$$

若信号带宽为 W,利用熵功率表示式(9)和式(10)的互信息,可得

$$\boldsymbol{I}(\boldsymbol{Y}_B; \boldsymbol{X}) = W \operatorname{lb} 2\pi \mathrm{e} \sigma_{Y_B}^2 - W \operatorname{lb} 2\pi \mathrm{e} \sigma_{n_B}^2,$$
$$\boldsymbol{I}(\boldsymbol{Y}_E; \boldsymbol{X}) = W \operatorname{lb} 2\pi \mathrm{e} \sigma_{Y_E}^2 - W \operatorname{lb} 2\pi \mathrm{e} \sigma_{n_E}^2 \quad (12)$$

将式(11)分别代入到式(12)中可分别得到两个互信息的范围:

$$W \operatorname{lb} \frac{\sigma_{X_B}^2 + \sigma_{n_B}^2}{\sigma_{n_B}^2} \leqslant \boldsymbol{I}(\boldsymbol{Y}_B; \boldsymbol{X}) \leqslant W \operatorname{lb} \frac{\| H_B \|^2 \delta_X^2 + \delta_B^2}{\sigma_{n_B}^2} \quad (13)$$

$$W \operatorname{lb} \frac{\sigma_{X_E}^2 + \sigma_{n_E}^2}{\sigma_{n_E}^2} \leqslant \boldsymbol{I}(\boldsymbol{Y}_E; \boldsymbol{X})$$
$$\boldsymbol{I}(\boldsymbol{Y}_E; \boldsymbol{X}) \leqslant W \operatorname{lb} \frac{\| \boldsymbol{h}_e^{\mathrm{T}} \cdot \boldsymbol{G}_1^{\mathrm{T}} \|^2 \cdot \delta_X^2 + \| \boldsymbol{h}_e^{\mathrm{T}} \cdot \boldsymbol{G}_2^{\mathrm{T}} \|^2 \delta_X^2 + \delta_E^2}{\sigma_{n_E}^2} \quad (14)$$

由于 $\| \boldsymbol{h}_e^{\mathrm{T}} \cdot \boldsymbol{G}_1^{\mathrm{T}} \|^2 \cdot \delta_X^2 + \| \boldsymbol{h}_e^{\mathrm{T}} \cdot \boldsymbol{G}_2^{\mathrm{T}} \|^2 \delta_X^2 = \| \boldsymbol{H}_E \|^2 \delta_X^2$,所以第三方的互信息的范围为

$$W \operatorname{lb} \frac{\sigma_{X_E}^2 + \sigma_{n_E}^2}{\sigma_{n_E}^2} \leqslant \boldsymbol{I}(\boldsymbol{Y}_E; \boldsymbol{X}) \leqslant W \operatorname{lb} \frac{\| \boldsymbol{H}_E \|^2 \delta_X^2 + \delta_E^2}{\sigma_{n_E}^2} \quad (15)$$

结合式(13)和式(15)可得

$$\boldsymbol{I}(\boldsymbol{Y}_B; \boldsymbol{X}) - \boldsymbol{I}(\boldsymbol{Y}_E; \boldsymbol{X}) \leqslant W \operatorname{lb} \left(\frac{(\| H_B \|^2 \delta_X^2 + \delta_B^2) \cdot \sigma_{n_E}^2}{\sigma_{n_B}^2 (\sigma_{X_E}^2 + \sigma_{n_E}^2)} \right) \quad (16)$$

式(16)中的熵功率满足如下公式:

$$\begin{cases} \sigma_{n_B}^2 \leqslant \delta_B^2, \sigma_{n_E}^2 \leqslant \delta_E^2 + \delta_{E1}^2 \\ \sigma_{X_B}^2 \leqslant \boldsymbol{H}_B^2 \delta_X^2, \sigma_{X_E}^2 \leqslant \boldsymbol{H}_E^2 \delta_X^2 \end{cases} \quad (17)$$

其中,$\delta_{E1}^2 = \| \boldsymbol{h}_e^{\mathrm{T}} \cdot \boldsymbol{G}_2^{\mathrm{T}} \|^2 \delta_X^2$,同时当且仅当各方差对应的变量服从正态分布时,式(16)中的等号成立。下面讨论式(16)右端的最大取值问题,从而最终可得保密容量 C_s。若令

$$Q(\sigma_{X_E}^2, \sigma_{n_E}^2) = \frac{\| \boldsymbol{H}_B \|^2 \delta_X^2 + \delta_B^2}{\delta_B^2} \cdot \frac{\sigma_{n_E}^2}{\sigma_{X_E}^2 + \sigma_{n_E}^2} = \frac{\| \boldsymbol{H}_B \|^2 \delta_X^2 + \delta_B^2}{\delta_B^2} \cdot \left(1 - \frac{\sigma_{X_E}^2}{\sigma_{X_E}^2 + \sigma_{n_E}^2} \right) \quad (18)$$

从式(18)右端可看出,$Q(\sigma_{X_E}^2, \sigma_{n_E}^2)$ 是 $\sigma_{n_E}^2$ 的增函数,再根据式(17),当 $\boldsymbol{h}_e^{\mathrm{T}} \cdot \boldsymbol{G}_2^{\mathrm{T}} \cdot \boldsymbol{X}$ 均服从正态分布时,$\sigma_{n_E}^2 = \delta_E^2 + \delta_{E1}^2$,此时 $Q(\sigma_{X_E}^2, \sigma_{n_E}^2)$ 达到最大值。

而由于 $\sigma_{X_E}^2$ 表示 $\boldsymbol{h}_e^{\mathrm{T}} \cdot \boldsymbol{G}_1^{\mathrm{T}} \cdot \boldsymbol{X}$ 的熵功率,按照文献[10]中对熵功率的定义有

$$\sigma_{X_E}^2 = \frac{1}{2\pi \mathrm{e}} \mathrm{e}^{2 \cdot H(\boldsymbol{h}_e^{\mathrm{T}} \cdot \boldsymbol{G}_1^{\mathrm{T}} \cdot \boldsymbol{X})}, \quad \sigma_{X_B}^2 = \frac{1}{2\pi \mathrm{e}} \mathrm{e}^{2 \cdot H(\boldsymbol{h}_b^{\mathrm{T}} \cdot \boldsymbol{G}_1^{\mathrm{T}} \cdot \boldsymbol{X})} \quad (19)$$

为讨论式(19)中的熵功率,首先给出如下的引理。

引理:设有随机变量 x,并且随机变量 $z = \lambda \cdot x$,

其中 λ 为常数,则信息熵 $H(z)=H(x)+\mathrm{lb}(\lambda)$。

证明:因为若 x 的概率密度函数为 $f(x)$,则 z 的概率密度函数为 $f(z/\lambda)/\lambda$。

所以

$$H(z)=\int -\frac{1}{\lambda}\cdot f(z/\lambda)\cdot \mathrm{lb}\left(\frac{1}{\lambda}\cdot f(z/\lambda)\right)\mathrm{d}z=$$
$$\int -\frac{1}{\lambda}\cdot f(\lambda\cdot x/\lambda)\cdot \mathrm{lb}\left(\frac{1}{\lambda}\cdot f(\lambda\cdot x/\lambda)\right)\mathrm{d}(\lambda\cdot x)=$$
$$\int -f(x)\cdot \mathrm{lb}(f(x))\mathrm{d}x+\int f(x)\cdot \mathrm{lb}(\lambda)\mathrm{d}x=$$
$$H(x)+\mathrm{lb}(\lambda)$$

从而引理得证。

由于信道特征 $\boldsymbol{h}_b$、$\boldsymbol{h}_e$ 与发送的信息 $\boldsymbol{G}_1^{\mathrm{T}}\cdot\boldsymbol{X}$ 相互独立,所以根据引理可得

$$H(\boldsymbol{h}_b^{\mathrm{T}}\cdot\boldsymbol{G}_1^{\mathrm{T}}\cdot\boldsymbol{X})=\mathrm{lb}(\|\boldsymbol{h}_b\|^2)+H(\boldsymbol{G}_1^{\mathrm{T}}\cdot\boldsymbol{X}),$$
$$H(\boldsymbol{h}_e^{\mathrm{T}}\cdot\boldsymbol{G}_1^{\mathrm{T}}\cdot\boldsymbol{X})=\mathrm{lb}(\|\boldsymbol{h}_e\|^2)+H(\boldsymbol{G}_1^{\mathrm{T}}\cdot\boldsymbol{X}) \quad (20)$$

所以对于(19)式分别有

$$\sigma_{X_E}^2=\frac{1}{2\pi\mathrm{e}}\cdot\mathrm{e}^{2\cdot\mathrm{lb}(\|h_b\|)+2H(\boldsymbol{G}_1^{\mathrm{T}}\cdot\boldsymbol{X})}=\frac{\|\boldsymbol{h}_b\|^2}{2\pi\mathrm{e}}\cdot\mathrm{e}^{2H(\boldsymbol{G}_1^{\mathrm{T}}\cdot\boldsymbol{X})},$$
$$\sigma_{X_B}^2=\frac{1}{2\pi\mathrm{e}}\cdot\mathrm{e}^{2\cdot\mathrm{lb}(\|h_e\|)+2H(\boldsymbol{G}_1^{\mathrm{T}}\cdot\boldsymbol{X})}=\frac{\|\boldsymbol{h}_e\|^2}{2\pi\mathrm{e}}\cdot\mathrm{e}^{2H(\boldsymbol{G}_1^{\mathrm{T}}\cdot\boldsymbol{X})} \quad (21)$$

由于对于固定的信道特征 $\boldsymbol{h}_b$、$\boldsymbol{h}_e$,$\boldsymbol{h}_b^{\mathrm{T}}\cdot\boldsymbol{G}_1^{\mathrm{T}}\cdot\boldsymbol{X}$ 与 $\boldsymbol{h}_e^{\mathrm{T}}\cdot\boldsymbol{G}_1^{\mathrm{T}}\cdot\boldsymbol{X}$ 有相同的分布,且熵功率的形式相似,所以令 $Q'(\sigma_{X_B}^2,\sigma_{X_E}^2,\sigma_{n_E}^2)=\frac{\sigma_{X_B}^2+\delta_B^2}{\delta_B^2}\cdot\frac{\sigma_{n_E}^2}{\sigma_{X_E}^2+\sigma_{n_E}^2}$,则根据式(17)和式(18),可知当 $\sigma_{X_B}^2=\|\boldsymbol{H}_B\|^2\delta_X^2$ 时,

$$Q'(\delta_{X_B}^2,\sigma_{X_E}^2,\sigma_{n_E}^2)=Q(\sigma_{X_E}^2,\sigma_{n_E}^2) \quad (22)$$

将式(21)代入到 $Q'(\sigma_{X_B}^2,\sigma_{X_E}^2,\sigma_{n_E}^2)$ 可得

$$Q'(\sigma_{X_B}^2,\sigma_{X_E}^2,\sigma_{n_E}^2)=\frac{\|\boldsymbol{h}_b\|^2\cdot\mathrm{e}^{2H(\boldsymbol{G}_1^{\mathrm{T}}\cdot\boldsymbol{X})}+2\pi\mathrm{e}\delta_B^2}{2\pi\mathrm{e}\delta_B^2}\cdot 2\pi\mathrm{e}\sigma_{n_E}^2/(\|\boldsymbol{h}_e\|^2\cdot\mathrm{e}^{2H(\boldsymbol{G}_1^{\mathrm{T}}\cdot\boldsymbol{X})}+2\pi\mathrm{e}\sigma_{n_E}^2) \quad (23)$$

在式(23)中,信道特征的模相同,即 $\|\boldsymbol{h}_b\|^2=\|\boldsymbol{h}_e\|^2$。根据式(18)的分析,$\sigma_{n_E}^2=\delta_E^2$,并且在接线窃听模型中有假设 $\delta_E^2\geqslant\delta_B^2$,所以 $Q'(\sigma_{X_B}^2,\sigma_{X_E}^2,\delta_E^2)$ 是 $H(\boldsymbol{G}_1^{\mathrm{T}}\cdot\boldsymbol{X})$ 的增函数。另外,又由于发射端的总发射功率受限,所以当向量 $\boldsymbol{G}_1^{\mathrm{T}}\cdot\boldsymbol{X}$ 中的元素服从高斯分布时,式(23)达到最大值[10],此时

$$Q'(\delta_{X_B}^2,\delta_{X_E}^2,\sigma_{n_E}^2)=Q(\delta_{X_E}^2,\sigma_{n_E}^2) \quad (24)$$

所以有如下定理成立。

定理一:若噪声 $\boldsymbol{n}_B$ 和 $\boldsymbol{n}_E$ 均服从正态分布,则当 $\boldsymbol{X}$ 和 $\boldsymbol{h}_e^{\mathrm{T}}\cdot\boldsymbol{G}_2^{\mathrm{T}}\cdot\boldsymbol{X}$ 均服从正态分布时图 2 所示的模型的保密容量为

$$C_s=C_{\mathrm{AB}}-C_{\mathrm{AE}}=W\cdot\mathrm{lb}\left(\frac{\|\boldsymbol{H}_B\|^2\delta_X^2+\delta_B^2}{\delta_B^2}\right)-W\cdot\mathrm{lb}\left(\frac{\|\boldsymbol{H}_E\|^2\delta_X^2+\delta_E^2}{\|\boldsymbol{h}_e^{\mathrm{T}}\cdot\boldsymbol{G}_2^{\mathrm{T}}\|^2\delta_X^2+\delta_E^2}\right) \quad (25)$$

其中,Alice 和 Bob 间的信道容量为

$$C_{\mathrm{AB}}=W\cdot\mathrm{lb}\left(\frac{\boldsymbol{H}_B^2\delta_X^2+\delta_B^2}{\delta_B^2}\right)$$

Alice 和 Eve 间的信道容量

$$C_{\mathrm{AE}}=W\cdot\mathrm{lb}\left(\frac{\|\boldsymbol{H}_E\|^2\delta_X^2+\delta_E^2}{\|\boldsymbol{h}_e^{\mathrm{T}}\cdot\boldsymbol{G}_2^{\mathrm{T}}\|^2\delta_X^2+\delta_E^2}\right)。$$

4 仿真与分析

为利用文中提出的等效信道特征模型揭示普适性加性人工噪声算法的安全性本质,对算法依照前述模型的结构进行仿真。令信道特征向量的模 $\|\boldsymbol{h}_b\|^2=\|\boldsymbol{h}_e\|^2=1$,式(25)可展开为

$$C_s=W\cdot\mathrm{lb}\left(\frac{\|\boldsymbol{h}_b\|^2\cdot\|\boldsymbol{G}_1\|^2\cdot\delta_X^2+\delta_B^2}{\delta_B^2}\cdot\frac{\|\boldsymbol{h}_e\|^2\cdot\|\boldsymbol{G}_2\|^2\cdot\cos^2\beta\cdot\delta_X^2+\delta_E^2}{\|\boldsymbol{h}_e\|^2\cdot\|\boldsymbol{G}\|^2\cdot\cos^2\alpha\cdot\delta_X^2+\delta_E^2}\right) \quad (26)$$

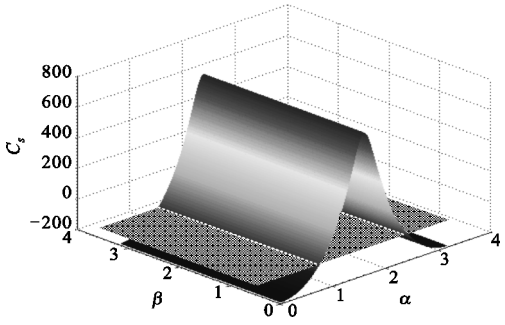
其中,α 是 $\boldsymbol{h}_e$ 与 $\boldsymbol{G}_1$ 的夹角,为主信号能量夹角;β 是 $\boldsymbol{h}_e$ 与 $\boldsymbol{G}_2$ 的夹角,为人工噪声能量夹角。通常情况下,由于第三接收方为配合状态,信道特征向量 $\boldsymbol{h}_e$ 未知,所以这两个角度无法测定。

首先按照表 1 中所示的参数设置进行仿真。由于此时 $\|\boldsymbol{G}_2\|^2=0$ mW,即在系统中未加入人工噪声项 $\boldsymbol{h}_e^{\mathrm{T}}\cdot\boldsymbol{G}_2^{\mathrm{T}}\cdot\boldsymbol{X}$,仿真过程等同于根据授权用户的信道特征方向做预均衡,此时可以观测出单独由预均衡所提供的系统安全性能。仿真中,在[0,π]之间遍历加密系统 $\boldsymbol{G}$ 与第三方信道特征 $\boldsymbol{h}_e$ 的两个夹角 α 和 β,并求出所有角度取值下的保密容量 C_s,最终的仿真结果如图 3 所示。

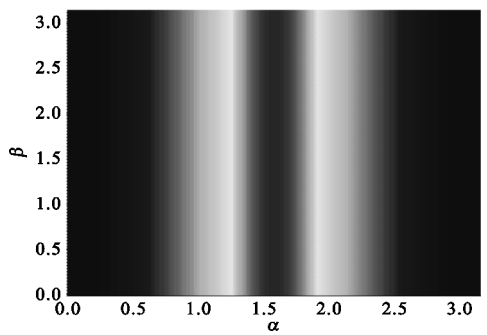
表 1 第一组仿真的参数设置情况

Table 1 The simulation parameters of the first set

参数	取值
δ_X^2/mW	50
δ_E^2/mW	2
δ_B^2/mW	4
$\|\boldsymbol{G}_1\|^2$/mW	2
$\|\boldsymbol{G}_2\|^2$/mW	0
W/Hz	200



(a) C_s 的三维分布图



(b) C_s 分布的俯视图

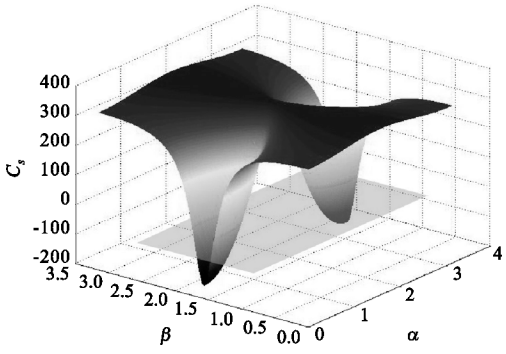
图 3　第一组仿真的保密容量分布图
Fig. 3 The secrecy capacity distribution of the first group of simulation

从图 3(a)中可以看出，由于 $\| \boldsymbol{G}_2 \|^2 = 0$ mW，C_s 只与 α 有关，并且当第三方的信道特征 $\boldsymbol{h}_e$ 与授权用户的信道特征 $\boldsymbol{h}_b$ 正交时，即 $\alpha = \pi/2$ 时，系统达到最大的保密容量。而当 $\boldsymbol{h}_e$ 与 $\boldsymbol{h}_b$ 的夹角较小，即两个信道特征较为相似时 C_s 迅速下降(如图 3(a)中所示)。由于在第一组仿真中，授权用户信道的加性噪声高于第三方用户($\delta_B^2 > \delta_E^2$)，所以在图 3(a)所示的水平平面以下，有 $C_s \leqslant 0$。这表示第三方用户可以收到任何授权用户接收到的信息，导致整个系统无法实现安全通信。另外，$\boldsymbol{h}_e$ 的信道情况在未知的情况下无法保证 α 的取值，而对应于俯视图 3(b)，只有中间 $1 \leqslant \alpha \leqslant 2.14$ 的部分可有效地进行安全通信，所以安全性无法得到保障。

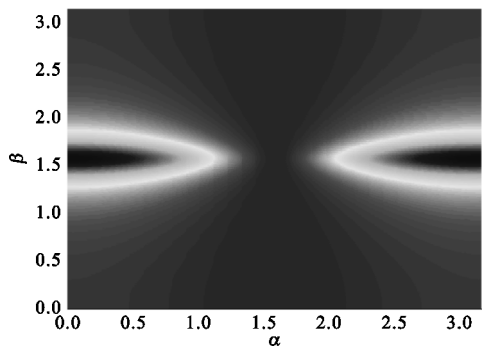
第二组仿真中引入了人工噪声，即 $\| \boldsymbol{G}_2 \|^2 > 0$，具体的参数见表 2。此时可以观测出通过人工噪声和预均衡两方面提供的系统安全性，最终得到的 C_s 随 α 和 β 的分布如图 4 所示。

表 2　第二组仿真的参数设置情况
Table 2 The simulation parameters of the second set

参数	取值
δ_X^2/mW	5
δ_E^2/mW	2
δ_B^2/mW	4
$\| \boldsymbol{G}_1 \|^2$/mW	2
$\| \boldsymbol{G}_2 \|^2$/mW	18
$\boldsymbol{W}$/Hz	200



(a) C_s 的三维分布图



(b) C_s 分布的俯视图

图 4　第二组仿真的保密容量分布图
Fig. 4 The secrecy capacity distribution of the second group of simulation

从图 4(a)中可以看出，$C_s > 0$ 的区域远大于图 3(a)中的分布区域。通过引入人工噪声，使得安全通信对 α 和 β 的取值要求降低。图 4(b)表示得更为明显，只有在左中以及右中两片深色锥形区域里 $C_s < 0$，其余绝大部分区域可以保证授权用户可安全地接收到发射端传输的信息。对比图 3(a)和图 4(a)的峰值可知，由于第二组仿真中将总发射功率(即 $\| \boldsymbol{G} \|^2 \cdot \delta_X^2$)中的一部分用于发射人工噪声，从而导致图 4(a)的峰值小于图 3(a)中的峰值。

第三组仿真主要用于观察平均意义下的 C_s，所以首先假设 α 和 β 服从均匀分布，其次取不同的噪声 n_E 功率 $\delta_E^2 \in (0.1, 100)$ mW 来观察平均保密容量 $\bar{C}_s$，其函数表示式为

$$\bar{C}_s = \frac{1}{\pi^2} \int_0^{\pi} \int_0^{\pi} C_s(\alpha, \beta) \, \mathrm{d}\alpha \mathrm{d}\beta \tag{27}$$

如表 3 中所示，δ_X^2 分别取 5 mW、50 mW、100 mW得到 3 条 $\bar{C}_s$ 性能曲线。图 5 的横坐标为 δ_B^2/δ_E^2，用来衡量两个信道的噪声大小。从图 5 中可以看出从平均意义上看，$\bar{C}_s$ 均大于 0，即通过引入人工噪声可以有效提高系统的保密容量。另外，随着 δ_X^2 变大，$\bar{C}_s$ 的增幅逐渐降低。

表 3 第三组仿真的参数设置情况

Table 3 The simulation parameters of the third set

参数	取值一	取值二	取值三
δ_X^2/mW	5	50	100
δ_E^2/mW	0.1 ~ 100	0.1 ~ 100	0.1 ~ 100
δ_B^2/mW	4	4	4
$\|\boldsymbol{G}_1\|^2$/mW	2	2	2
$\|\boldsymbol{G}_2\|^2$/mW	18	18	18
$\boldsymbol{W}$/Hz	200	200	200

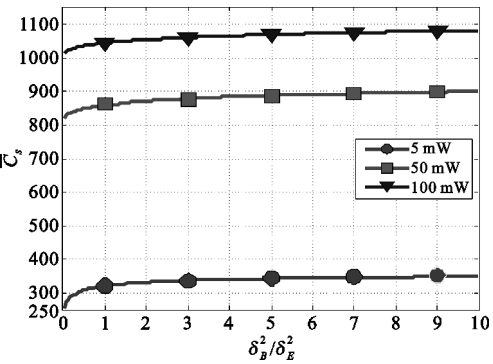


图 5 第三组仿真的保密容量对比曲线图

Fig. 5 Secrecy capacity comparison of the third group simulation

5 结束语

本文通过建立信道特征的概念分析了一般 MISO 系统中人工噪声方法的保密容量,并将加入人工噪声归结为改变信道的原始信道特征,从而导致噪声授权用户和第三方用户的等效信道特征不一致:一是授权用户的等效信道特征稳定,便于接收;二是第三方的等效信道特征随机变化。随后对传统的接线窃听模型进行扩展,并结合熵功率推导出在加性高斯噪声情况下,当服从任意分布时,人工噪声方式的 MISO 系统保密容量 。在实际中,将本文的结论结合安全信道编码可实现一般意义下 MISO 系统的信息安全传输。在后续研究中,需要将文中的结论推广到 MIMO 系统中,讨论更广范围多天线系统的安全性能。

参考文献:

[1] Shannon C E. Communication theory of secrecy systems [J]. Bell System Technical Journal, 1949, 28(4):656-715.

[2] Lin Tong, Huang Kaizhi, Luo Wenyu. A Multicarrier-based Physical Layer Security Scheme for the Multicast Systems [J]. Journal of Electronics & Information Technology, 2013, 35(6):1338-1343.

[3] Csiszar I, Koner J. Broadcast channels with confidential messages [J]. IEEE Transactions on Information Theory, 1978, 24(5):339-348.

[4] Shiu Yi-Sheng, Chang Shih-Yu, Wu Hsiao-Chun, et al. Physical layer security in wireless networks: a tutorial [J]. IEEE Wireless Communications, 2011, 18(4):66-74.

[5] Liang Yingbin, Vincent P H, Shamai S. Information Theoretic Security [M]// Foundations and Trends in Communications and Information Theory. Boston: Now Publishers Inc., 2008: 355-580.

[6] Tahir M. Wireless physical layer security using channel state information [C]// Proceedings of 2010 International Conference on Computer and Communication Engineering. Kuala, Lumpur: IEEE, 2010: 1-5.

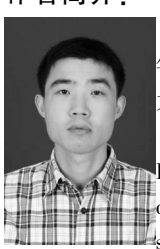
[7] 吉江,金梁,黄开枝. 基于人工噪声的 MISO 保密容量分析[J]. 通信学报,2012,33(10): 138-142.
JI Jiang, JIN Liang, HUANG Kai-zhi. Secrecy capacity analysis of MISO system with artificial noise [J]. Journal on Communications, 2012, 33(10):138-142. (in Chinese)

[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] Zhou X. Physical layer security with artificial noise: secrecy capacity and optimal power allocation [C]// Proceedings of 2009 International Conference on Signal Processing and Communication Systems. Omaha, NE: IEEE, 2009: 1-5.

[10] Shannon C E. A Mathematical Theory of Communication [J]: Bell System Technical Journal, 1948, 27(6-10): 379-423, 623-656.

作者简介:



段明义(1978—),男,河南郑州人,2006 年获工学硕士学位,现为讲师,主要研究方向为计算机网络、数据库、数据挖掘;

DUAN Ming-yi was born in Zhengzhou, Henan Province, in 1978. He received the M. S. degree in 2006. He is now a lecturer. His research concerns computer network, database and data mining.

Email: duanmingyi@126.com

黄继海(1977—),男,河南濮阳人,硕士,讲师,主要研究方向为计算机网络、分布式计算等;

HUANG Ji-hai was born in Puyang, Henan Province, in 1977. He is now a lecturer with the M. S. degree. His research concerns computer network and distributed computing.

Email: huangjihai@sina.com

吉 江(1983—),男,河南南乐人,2012 年获工学博士学位,主要研究方向为无线通信、计算机网络、信号处理。

JI Jiang was born in Nanle, Henan Province, in 1983. He received the Ph. D. degree in 2012. His research concerns wirless communication, computer network and signal processing.