有限字符输入系统的物理层安全传输条件

崔 波* 刘 璐 金 梁
(国家数字交换系统工程技术研究中心 郑州 450002)

摘 要：针对无线数字通信系统中人工噪声方法可被多天线窃听者破解的问题，该文提出有限字符输入下物理层安全传输的一个充分条件，并以此为指导设计了一种类符号人工噪声方法。分析表明，人工噪声方法下，有限字符输入信号和窃听者无噪接收信号之间的等效信道是一个离散有噪无损信道(Discrete Noisy Lossless Channel, DNLC)。由于 DNLC 输入信号的可逆性为窃密提供了必要条件，窃听者通过增加天线可使窃听信道容量达到合法用户的信道容量上限，致使系统的保密互信息为零，因此破坏输入信号的可逆性是有限字符输入下物理层安全传输的一个充分条件。类符号人工噪声方法满足这一充分条件，可以保证物理层安全传输，仿真结果也表明了该方法的有效性。

关键词：无线通信；无线物理层安全；有限字符；人工噪声；离散有噪无损信道；类符号人工噪声
中图分类号：TN92 **文献标识码**： A **文章编号**：1009-5896(2014)06-1441-07
DOI: 10.3724/SP.J.1146.2013.01321

Physical Layer Security Transmission Condition for Finite Alphabet Input System

Cui Bo Liu Lu Jin Liang
(*National Digital Switching System Engineering & Technological Research Center*, *Zhengzhou* 450002, *China*)

Abstract: Addressing the problem that the artificial noise method can be cracked by the eavesdropper with multiple antennas in wireless communication systems, a sufficient condition is proposed for secure physical layer transmission with finite alphabet inputs. Under this guideline, a signal-like artificial noise method is designed to ensure the system security transmission. Analysis reveals that the equivalent channel between the finite alphabet input and the eavesdropper's noise-free output is a Discrete Noisy Lossless Channel (DNLC). Since the reversibility of the input under a DNLC provides the necessary condition for eavesdropping, the eavesdropper can augment its antennas to successfully squeeze out the secure information, nullifying the system's secrecy mutual information. As a result, destroying the reversibility of the input signal becomes a sufficient condition for the secure physical layer transmission with finite alphabet inputs. The signal-like artificial noise method satisfies the sufficient condition, which can ensure the secure physical layer transmission. Simulation results demonstrate the efficacy of this method.

Key words: Wireless communication; Wireless physical-layer security; Finite alphabet; Artificial noise; Discrete Noisy Lossless Channel (DNLC); Signal-like artificial noise

1 引言

无线信道的时变性、随机性和差异性是其区别于有线信道的重要特征，也是无线物理层安全传输的研究基础。1975 年，Wyner[1]提出了搭线窃听加密模型，首次讨论信道对系统安全性的作用，并引入了保密容量来衡量系统安全性能。文献[2,3]将该模型扩展到广播信道和加性高斯噪声情况。2009 年，Liang 等人[4]总结了已有的不同应用场景下的搭线窃听模型。搭线窃听加密模型为无线物理层安全传输提供了较好的解决思路，但要求合法用户的信道质量优于第三方用户。

为了给合法用户创造信道质量优势，现有研究一般采用多天线技术。其中，当系统已知窃听信道信息时，Khisti 等人[5,6]通过广义奇异值分解(Singular Value Decomposition, SVD)等方法获取正的保密容量。当系统未知窃听信道信息时，Goel 等人[7]提出人工噪声方法，Li 等人[8]提出天线阵列随机加权法以获取正的保密容量。吴等人[9]基于阵列信号处理理论，发现文献[7,8]中的两种方法实质相同，均利用波束成形技术[5]在合法用户方向的波束中发送保密信息，保证合法用户接收性能；而在其它波束中发送空域干扰，降低窃听者的信噪比(Signal to Noise Ratio, SNR)。并据此建立了基于空域加扰物理层安全传输的统一数学模型，将上述两种安全方

2013-08-28 收到，2013-12-05 改回
国家自然科学基金(61171108)资助课题
*通信作者：崔波 eeeicuibo@163.com

法容纳到同一系统框架下。由于人工噪声方法不用假设已知窃听信道信息，已经在许多新的场景中得到应用[10,11]。

上述基于信息论的物理层安全研究通常假设高斯输入，原因是高斯输入具有最佳的理论效果并且分析计算简便。对于实际数字通信中的有限字符输入系统，现有的相关研究集中于最大化信道互信息[12−14]，而很少利用信息论讨论无线物理层安全传输[9,15,16]。文献[9]从阵列信号处理角度出发，指出多输入单输出多天线窃听(Multiple-Input Single-Output Multiple-Antenna Eavesdropper, MISOME)系统存在安全问题，并给出一种 MUSIC-like 窃密算法。文献[15,16]假设已知多输入多输出多天线窃听(Multiple-Input Multiple-Output Multiple-antenna Eavesdropper, MIMOME)系统的窃听信道参数，通过预线性编码或广义 SVD 等方法获取正的保密互信息。然而，上述研究没有基于信息论严格分析安全传输的条件，本文针对该问题展开相关研究，为有限字符输入系统的物理层安全传输设计提供一定的指导。

当输入信号的调制类型确定时，有限字符输入系统的合法信道存在容量上限[12,13]。论文首先从信息论角度严格证明窃听者可以通过增加窃听天线改善窃听信道质量，让窃听信道容量达到该上限，致使系统的保密互信息趋于零。进一步研究发现，在人工噪声方法中，将有限字符输入信号作为输入，将窃听者的无噪(观测噪声)接收信号作为输出，所经等效信道是一个 DNLC[17]。该特性与高斯输入存在本质不同，并且 DNLC 下输入信号具有可逆性，为窃密提供了必要条件。在此基础上，利用有限字符输入信号和高斯分布的空域干扰的分布规律差异，窃听者可以无损地或以较小误码率重构输入信号。从几何角度来看，窃听者的无噪接收信号位于多个不同的平面或超平面上[18]，而这些(超)平面与输入信号间存在一一对应关系，验证了 DNLC 下输入信号的可逆性。

反之，在不能限制窃听信道质量的前提下，破坏输入信号的可逆性则是有限字符输入系统的物理层安全传输的充分条件。在此指导下，论文最后提出使用类符号人工噪声方法，通过发送与输入信号分布相同的空域干扰，致使窃听者无法区分信号和干扰，实现系统安全传输。从几何角度来看，输入符号和空域干扰经过 DNLC 后将位于某个(超)平面体的顶点上，由于窃听者未知合法信道信息，无法判定各个输入符号对应哪些顶点，因此无法恢复输入信号。

后文论述中，$\mathbb{C}$，$\mathbb{E}(\cdot)$，$\|\cdot\|$ 和 $\Re\{\cdot\}$ 分别表示复空间，数学期望，2 范数和复数实部。$\mathcal{CN}(a,b)$ 表示均值为 a，方差为 b 的复高斯分布。

2 问题描述

2.1 MISO 系统模型及其信道互信息

考虑某 MISOME 系统，发送方(Alice)配备 N_a ($N_a>1$)根天线；合法用户(Bob)配备 N_b ($N_b=1$) 根天线；窃听者(Eve)配备 N_e ($N_e>1$)根天线，不发送信号，只进行被动接收，并且不知道 Alice 到 Bob 的合法信道信息。Bob 接收天线上的观测噪声 $\boldsymbol{v}_b(n)\sim\mathcal{CN}(0,\sigma_b^2)$，Eve 接收天线上的噪声 $\boldsymbol{v}_e(n)\in\mathbb{C}^{N_e\times 1}$，服从 $\mathcal{CN}(\boldsymbol{0},\sigma_e^2\boldsymbol{I}_{N_e})$。

Alice 到 Bob 的合法信道可以表示为 N_a 维向量：

$$\boldsymbol{h}_b^{\mathrm{H}}=[h_1,h_2,\cdots,h_{N_a}] \tag{1}$$

Alice 到 Eve 的窃听信道可以表示为 $N_e\times N_a$ 的矩阵。

$$\boldsymbol{H}_e=\begin{bmatrix} h_{11}, & h_{12}, & \cdots, & h_{1N_a}\\ h_{21}, & h_{22}, & \cdots, & h_{2N_a}\\ \vdots & \vdots & & \vdots\\ h_{N_e1}, & h_{N_e2}, & \cdots, & h_{N_eN_a}\end{bmatrix} \tag{2}$$

假设信道分块衰落，在一个数据帧内信道是准静态的，不同数据帧之间信道增益系数独立同分布。

Alice 利用波束形成技术[5]在时刻 n 发送信号矢量 $(\boldsymbol{h}_b/\|\boldsymbol{h}_b\|)s(n)$，Bob 和 Eve 的接收信号分别为

$$\boldsymbol{y}_b(n)=\|\boldsymbol{h}_b\|s(n)+\boldsymbol{v}_b(n) \tag{3}$$

$$\boldsymbol{y}_e(n)=\boldsymbol{H}_e\frac{\boldsymbol{h}_b}{\|\boldsymbol{h}_b\|}s(n)+\boldsymbol{v}_e(n) \tag{4}$$

发送信号在 Bob 处同相叠加，使得 Bob 接收信号的能量比 Eve 的更加集中，但是 Bob 仅有 1 根接收天线，天线数比 Eve 少。为了合理比较两者的接收效果，假设所有的信道增益系数均为标准复高斯随机变量，即 $h_k\sim\mathcal{CN}(0,1)$，$k=1,2,\cdots,N_a$，$h_{ij}\sim\mathcal{CN}(0,1)$，$i=1,2,\cdots,N_e$，$j=1,2,\cdots,N_a$。Bob 和 Eve 接收信号的 SNR 分别定义为

$$\mathrm{SNR}_b\triangleq\mathbb{E}_{\boldsymbol{h}_b}\left[\frac{\|\boldsymbol{h}_b s(n)\|^2}{\sigma_b^2}\right] \tag{5}$$

$$\mathrm{SNR}_e\triangleq\mathbb{E}_{\boldsymbol{H}_e,\boldsymbol{h}_b}\left[\frac{\|\boldsymbol{H}_e\boldsymbol{h}_b s(n)\|^2}{\|\boldsymbol{h}_b\|^2\sigma_e^2}\right] \tag{6}$$

将窃听信道简记为 $\boldsymbol{h}_e=\boldsymbol{H}_e(\boldsymbol{h}_b/\|\boldsymbol{h}_b\|)$，$\boldsymbol{h}_e\in\mathbb{C}^{N_e}$ 且服从 $\mathcal{CN}(\boldsymbol{0},\boldsymbol{I}_{N_e})$。Eve 的接收信号及其 SNR 可以简化为

$$\boldsymbol{y}_e(n)=\boldsymbol{h}_e s(n)+\boldsymbol{v}_e(n) \tag{7}$$

$$\mathrm{SNR}_e \triangleq \mathbb{E}_{\boldsymbol{h}_e}\left[\frac{\left\|\boldsymbol{h}_e s(n)\right\|^2}{\sigma_e^2}\right] \tag{8}$$

其中，$\mathbb{E}_{\boldsymbol{h}_e}$ 表示 $\mathbb{E}_{\boldsymbol{H}_e,\boldsymbol{h}_b}$。假设所有信道参数对 Bob 和 Eve 都是公开的，得到 Alice-Bob 和 Alice-Eve 条件平均互信息为

$$\begin{aligned}&\mathcal{I}(s;\boldsymbol{y}_b \mid \boldsymbol{h}_b)\\&=\log_2 M-\frac{1}{M}\\&\cdot\sum_{m=1}^{M}\mathbb{E}_{\boldsymbol{v}_b}\left\{\log_2\sum_{k=1}^{M}\exp\left[-\frac{\left\|\boldsymbol{h}_b\right\|(s_m-s_k)+\boldsymbol{v}_b\right|^2-\left|\boldsymbol{v}_b\right|^2}{\sigma_b^2}\right]\right\}\end{aligned} \tag{9}$$

$$\begin{aligned}&\mathcal{I}(s;\boldsymbol{y}_e \mid \boldsymbol{h}_e)\\&=\log_2 M-\frac{1}{M}\\&\cdot\sum_{m=1}^{M}\mathbb{E}_{\boldsymbol{v}_e}\left\{\log_2\sum_{k=1}^{M}\exp\left[-\frac{\left\|\boldsymbol{h}_e(s_m-s_k)+\boldsymbol{v}_e\right\|^2-\left\|\boldsymbol{v}_e\right\|^2}{\sigma_e^2}\right]\right\}\end{aligned} \tag{10}$$

在不引起歧义时，计算式(9)和式(10)的平均互信息省略了时间标记。进一步，得到 Alice-Bob 和 Alice-Eve 统计平均互信息为

$$\begin{aligned}&\mathcal{I}(s;y_b)\\&=\mathbb{E}_{\boldsymbol{h}_b}\left[\mathcal{I}(s;y_b \mid \boldsymbol{h}_b)\right]=\log_2 M-\mathbb{E}_{\boldsymbol{h}_b}\\&\cdot\left\{\frac{1}{M}\sum_{m=1}^{M}\mathbb{E}_{\boldsymbol{v}_b}\left[\log_2\sum_{k=1}^{M}\exp\left(-\frac{\left\|\boldsymbol{h}_b\right\|(s_m-s_k)+\boldsymbol{v}_b\right|^2-\left|\boldsymbol{v}_b\right|^2}{\sigma_b^2}\right)\right]\right\}\end{aligned} \tag{11}$$

$$\begin{aligned}&\mathcal{I}(s;\boldsymbol{y}_e)\\&=\mathbb{E}_{\boldsymbol{h}_e}\left[\mathcal{I}(s;y_b \mid \boldsymbol{h}_e)\right]=\log_2 M-\mathbb{E}_{\boldsymbol{h}_e}\\&\cdot\left\{\frac{1}{M}\sum_{m=1}^{M}\mathbb{E}_{\boldsymbol{v}_e}\left[\log_2\sum_{k=1}^{M}\exp\left(-\frac{\left\|\boldsymbol{h}_e(s_m-s_k)+\boldsymbol{v}_e\right\|^2-\left\|\boldsymbol{v}_e\right\|^2}{\sigma_e^2}\right)\right]\right\}\end{aligned} \tag{12}$$

Alice-Bob 和 Alice-Eve 统计平均互信息的上限均为 $\log_2 M$ bit/(s·Hz)。

2.2 系统保密互信息

根据广播系统保密互信息的定义[2]，定义上述 MISOME 系统的保密互信息为

$$\mathcal{C}_s \triangleq \left[\mathcal{I}(s;\boldsymbol{y}_b)-\mathcal{I}(\boldsymbol{x};\boldsymbol{y}_e)\right]^+ \tag{13}$$

其中，$[x]^+=\max(0,x)$。针对上述系统，定理 1 表明了保密互信息与收发天线数之间的数值关系，为分析系统保密互信息提供了理论依据。

定理 1　Alice 采用波束形成技术发送信号，且 Bob 和 Eve 的噪声水平一致，即 $\sigma_b^2=\sigma_e^2$。在互信息未饱和前，保密互信息由天线数 N_e 和 N_a 决定。

$$\left.\begin{aligned}&\mathcal{C}_s>0, \quad N_e<N_a\\&\mathcal{C}_s=0, \quad N_e\geq N_a\end{aligned}\right\} \tag{14}$$

证明　首先证明 $N_e=N_a$ 的情况。分别重写 $\mathcal{I}(s;\boldsymbol{y}_b \mid \boldsymbol{h}_b)$ 和 $\mathcal{I}(s;\boldsymbol{y}_e \mid \boldsymbol{h}_e)$ 为

$$\begin{aligned}&\mathcal{I}(s;\boldsymbol{y}_b \mid \boldsymbol{h}_b)\\&=\log_2 M-\frac{1}{M}\\&\cdot\sum_{m=1}^{M}\mathbb{E}_{\boldsymbol{v}_b}\left\{\log_2\sum_{k=1}^{M}\exp\left[-\left(\left\|\boldsymbol{h}_b\right\|^2\left|s_m-s_k\right|^2\right.\right.\right.\\&\left.\left.\left.+2\Re\left\{\boldsymbol{v}_b^{\mathrm{H}}\left\|\boldsymbol{h}_b\right\|(s_m-s_k)\right\}\right)\Big/\sigma_b^2\right]\right\}\end{aligned} \tag{15}$$

$$\begin{aligned}&\mathcal{I}(s;\boldsymbol{y}_e \mid \boldsymbol{h}_e)\\&=\log_2 M-\frac{1}{M}\sum_{m=1}^{M}\mathbb{E}_{\boldsymbol{v}_e}\left\{\log_2\sum_{k=1}^{M}\exp\left[-\left(\left\|\boldsymbol{h}_e\right\|^2\right.\right.\right.\\&\left.\left.\left.\cdot\left|s_m-s_k\right|^2+2\Re\left\{\boldsymbol{v}_e^{\mathrm{H}}\boldsymbol{h}_e(s_m-s_k)\right\}\right)\Big/\sigma_e^2\right]\right\}\end{aligned} \tag{16}$$

其中，$\Re\{\boldsymbol{v}_b^{\mathrm{H}}\left\|\boldsymbol{h}_b\right\|(s_m-s_k)\}$ 和 $\Re\{\boldsymbol{v}_e^{\mathrm{H}}\boldsymbol{h}_e(s_m-s_k)\}$ 是零均值实高斯随机变量，协方差分别为 $\left\|\boldsymbol{h}_b\right\|^2\left|s_m-s_k\right|^2\cdot\sigma_b^2/2$ 和 $\left\|\boldsymbol{h}_e\right\|^2\left|s_m-s_k\right|^2\sigma_e^2/2$。由于 $\sigma_b^2=\sigma_e^2$ 且 $\boldsymbol{h}_b$ 和 $\boldsymbol{h}_e$ 分布相同，根据式(15)和式(16)，Alice-Bob 和 Alice-Eve 统计平均互信息也将相同，即 $\mathcal{I}(s;\boldsymbol{y}_b)=\mathcal{I}(s;\boldsymbol{y}_e)$。根据式(13)，得到 $\mathcal{C}_s=0$。

若 $N_e>N_a$，将配备 N_e 根接收天线的 Alice-Eve 统计平均互信息表示为 $\mathcal{I}_{N_e}(s;\boldsymbol{y}_e)$。将配备 N_a 和 N_e 根接收天线的 Alice-Bob 统计平均互信息分别表示为 $\mathcal{I}_{N_a}(s;\boldsymbol{y}_b)$ 和 $\mathcal{I}_{N_e}(s;\boldsymbol{y}_b)$。由于波束形成的作用，Bob 配备 N_e 根接收天线的接收质量比配备 N_a 根接收天线的更好，所以在互信息未饱和前，$\mathcal{I}_{N_e}(s;\boldsymbol{y}_b)>\mathcal{I}_{N_a}(s;\boldsymbol{y}_b)$。由 $N_e=N_a$ 情况下的互信息关系可得 $\mathcal{I}_{N_e}(s;\boldsymbol{y}_b)=\mathcal{I}_{N_e}(s;\boldsymbol{y}_e)$。因此，在互信息未饱和前，$\mathcal{I}_{N_e}(s;\boldsymbol{y}_e)>\mathcal{I}_{N_a}(s;\boldsymbol{y}_b)$。根据式(13)得到 $\mathcal{C}_s=0$。

若 $N_e<N_a$，同理可证 $\mathcal{I}_{N_e}(s;\boldsymbol{y}_e)<\mathcal{I}_{N_a}(s;\boldsymbol{y}_b)$，根据式(13)得到 $\mathcal{C}_s>0$。　证毕

由此可见，在有限字符输入的 MISOME 系统中，当 Eve 各子信道的质量与 Bob 的子信道质量相当时，即使 Bob 采用了波束成形等技术，只要 Eve 配备了足够的窃听天线，其整体接收效果理论上可以达到甚至超越 Bob 的接收效果，致使系统保密互信息为 0。

图 1 所示为 Alice-Bob 和 Alice-Eve 统计平均互信息仿真结果。仿真采用 BPSK 信号；$N_a=4$，$N_b=1$，$N_e=3,4,5$；所有的信道增益系数均是标准复高斯随机变量。图 1 中每个点代表 10^6 次 Monte-

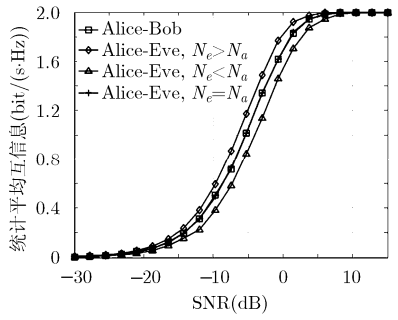

图 1 Alice-Bob 和 Alice-Eve 统计平均互信息

Carlo 仿真平均值，其中，信道和噪声各进行10^3次 Monte-Carlo 仿真。在互信息未饱和前的很大 SNR 范围内，Alice-Eve 在同一 SNR 下的统计平均互信息大小顺序是按照 N_e 大小排列的。特别地，当 $N_e = N_a = 4$ 时，Alice-Bob 和 Alice-Eve 统计平均互信息的仿真结果基本一致。

因此，从信息论分析和统计平均互信息仿真结果来看，有限字符输入的 MISOME 系统存在安全隐患。

3 有限字符输入下 MISOME 系统的安全性分析

针对 MISOME 系统下人工噪声方法，利用信息论的知识分析人工噪声方法的几何意义和窃密算法，挖掘出有限字符输入下 MISOME 系统的物理层安全传输条件。

3.1 信号接收过程的 Markov 链表示

在人工噪声方法中，Alice 发送信号包括两部分，即 $(\boldsymbol{h}_b/\|\boldsymbol{h}_b\|)s(n)+\boldsymbol{h}_b^{\perp}\boldsymbol{u}(n)$。第 1 部分 $(\boldsymbol{h}_b/\|\boldsymbol{h}_b\|)\cdot s(n)$ 表示发送给 Bob 的有用信号；第 2 部分 $\boldsymbol{h}_b^{\perp}\boldsymbol{u}(n)$ 表示对 Bob 零空间发送的空域干扰，不影响 Bob 但影响 Eve 接收。其中，$s(n)\in\mathcal{S}$，字符集 $\mathcal{S}$ 定义为 $\mathcal{S}\triangleq\{s_1,s_2,\cdots,s_M\}$；$\boldsymbol{h}_b^{\perp}=[\boldsymbol{\beta}_1,\boldsymbol{\beta}_2,\cdots,\boldsymbol{\beta}_{N_a-1}]$ 表示 $\boldsymbol{h}_b$ 的规范正交补空间，对 $\boldsymbol{h}_b$ 进行 SVD 可得到 $\boldsymbol{h}_b=\boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\mathrm{H}}$ 和 $\boldsymbol{U}=[(\boldsymbol{h}_b/\|\boldsymbol{h}_b\|),\boldsymbol{\beta}_1,\boldsymbol{\beta}_2,\cdots,\boldsymbol{\beta}_{N_a-1}]$。此时 Bob 和 Eve 的接收信号分别为

$$y_b(n)=\|\boldsymbol{h}_b\|s(n)+\boldsymbol{v}_b(n)=x_b(n)+\boldsymbol{v}_b(n) \tag{17}$$

$$\begin{aligned}\boldsymbol{y}_e(n)&=\boldsymbol{H}_e\frac{\boldsymbol{h}_b}{\|\boldsymbol{h}_b\|}s(n)+\boldsymbol{H}_e\boldsymbol{h}_b^{\perp}\boldsymbol{u}(n)+\boldsymbol{v}_e(n)\\&=\boldsymbol{x}_e(n)+\boldsymbol{v}_e(n)\end{aligned} \tag{18}$$

其中，$x_b(n)=\|\boldsymbol{h}_b\|s(n)$ 和 $\boldsymbol{x}_e(n)=\boldsymbol{H}_e(\boldsymbol{h}_b/\|\boldsymbol{h}_b\|),s(n)+\boldsymbol{H}_e\boldsymbol{h}_b^{\perp}\boldsymbol{u}(n)$ 分别表示 Bob 和 Eve 的无噪接收信号。若信道 $\boldsymbol{h}_b$ 存在测量误差，波束形成的增益将下降，同时空域干扰的能量将部分落在合法信道上，影响合法用户的接收性能以及对窃听者的干扰效果。因此，实际系统要求信道的测量误差较小，这里为讨论简便假设 Alice 精确已知 $\boldsymbol{h}_b$。

将 Bob 和 Eve 的信号接收过程表示为 Markov 链形式。对于 Bob，其 Markov 链为

$$s(n)\leftrightarrow x_b(n)\rightarrow\boldsymbol{y}_b(n) \tag{19}$$

其中，$s(n)\leftrightarrow x_b(n)$ 表示输入信号可逆，可从 $x_b(n)$ 中无损恢复 $s(n)$。因此，该 Markov 链可以缩短为 $s(n)\rightarrow\boldsymbol{y}_b(n)$。对于 Eve，其 Markov 链为

$$s(n)\rightarrow\boldsymbol{x}_e(n)\rightarrow\boldsymbol{y}_e(n) \tag{20}$$

3.2 离散有噪无损信道及其几何含义

DNLC 的定义[17]为：信道的 1 个输入对应多个输出，而且每个输入所对应的输出值不重合。根据 DNLC 的定义，式(20)中 $s(n)\rightarrow\boldsymbol{x}_e(n)$ 间的等效信道是一个 DNLC。如图 2 所示，输入 1 个符号 s_m，对应输出 $\boldsymbol{x}_e(n)=\boldsymbol{H}_e(\boldsymbol{h}_b/\|\boldsymbol{h}_b\|)s_m+\boldsymbol{H}_e\boldsymbol{h}_b^{\perp}\boldsymbol{u}(n)$ 在不同时刻 n 有不同的值，但不同输入符号 s_m 对应的输出值是不重合的，验证了该结论。

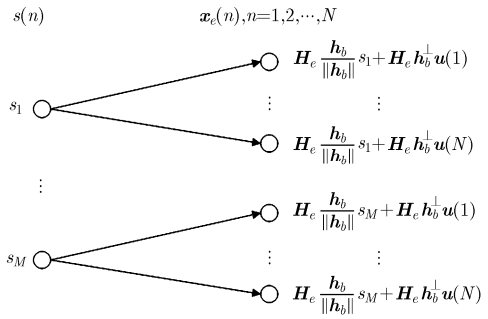

图 2 人工噪声方法等效信道的输入输出关系图

对于 Bob 的信号接收过程 $s(n)\rightarrow y_b(n)$ 而言，系统实际也是让合法信道逼近 DNLC，进而从包含噪声的接收信号 $y_b(n)$ 中无损地或以较小误码率恢复出输入信号 $s(n)$。考虑到 $\mathcal{I}(s;y_b)=H(s)-H(s\mid y_b)$，系统为了让合法信道逼近 DNLC，要求 $H(s\mid y_b)\rightarrow 0$，所以 SNR_b 较高。当窃听信道质量与合法信道质量相当时，可以认为 SNR_e 也较高，此时 $H(s\mid\boldsymbol{y}_e)\rightarrow 0$ 且 $\mathcal{I}(s;\boldsymbol{y}_e)\rightarrow H(s)$。因此，在合法信道努力逼近 DNLC 的同时，Eve 通过增加天线也可使窃听信道逼近 DNLC。

在 DNLC 的作用下，Eve 的无噪接收信号 $\boldsymbol{x}_e(n)$ 表现出“有限”的几何特征：$\boldsymbol{x}_e(n)$ 位于有限的(超)平面[18]，$\boldsymbol{H}_e(\boldsymbol{h}_b/\|\boldsymbol{h}_b\|)s_m$ 是这些(超)平面的几何中心，因此不同(超)平面对应不同的输入信号 s_m。

图 3 所示的是人工噪声方法下 Eve 无噪接收信号的仿真图。为了显示直观，以 BPSK 信号为例，天线数 $N_a=N_e=3$，且限定各信道增益系数为实

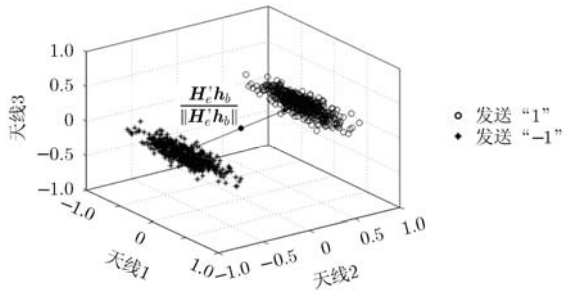

图 3　Eve 的无噪接收信号

高斯随机变量。此时，BPSK 的 2 个星座点分别对应了 2 个不同的平面。窃听者可以根据接收信号所处平面判断出输入符号，且可以计算出平面的法线方向 $\boldsymbol{H}_e^{\dagger}\boldsymbol{h}_b/\ ||\boldsymbol{H}_e^{\dagger}\boldsymbol{h}_b||$。因此，虽然 Eve 未知 $\boldsymbol{h}_b$，但仍然可以窃密，验证了 DNLC 下输入信号的可逆性。当天线数 N_a, N_e 增加，或者信道增益系数为复数时，接收信号的星座点将服从超平面分布。

3.3 人工噪声方法的窃密算法分析

由于 DNLC 下输入信号是可逆的，表示为 $s(n) \leftrightarrow \boldsymbol{x}_e(n)$，Eve 在窃听信道容量的保证下利用 MUSIC-like 窃密算法[9]可从 $\boldsymbol{x}_e(n)$ 中恢复出发送信号 $s(n)$。

累积 K ($K > N_a$)个符号，得到 $\boldsymbol{X}_e = [\boldsymbol{x}_e(n), \boldsymbol{x}_e(n+1),\cdots,\boldsymbol{x}_e(n+K-1)]$, $\boldsymbol{X}_e \in \mathbb{C}^{N_e\times K}$ 可改写为

$$\boldsymbol{X}_e = \boldsymbol{H}_e\left[\frac{\boldsymbol{h}_b}{\|\boldsymbol{h}_b\|}, \boldsymbol{h}_b^{\perp}\right]\begin{bmatrix} s(n), s(n+1),\cdots,s(n+K-1) \\ \boldsymbol{u}(n), \boldsymbol{u}(n+1),\cdots,\boldsymbol{u}(n+K-1)\end{bmatrix} \tag{21}$$

对 $\boldsymbol{X}_e$ 进行 SVD，得到

$$\boldsymbol{X}_e = [\boldsymbol{U}_s, \boldsymbol{U}_n]\begin{bmatrix}\boldsymbol{\Sigma}_s & \\ & \boldsymbol{0}\end{bmatrix}\begin{bmatrix}\boldsymbol{V}_s^{\mathrm{H}} \\ \boldsymbol{V}_n^{\mathrm{H}}\end{bmatrix} \tag{22}$$

当 $\boldsymbol{H}_e$ 列满秩时，$\boldsymbol{X}_e$ 的秩最大为 N_a，经过简单推导可得 $[s(n), s(n+1),\cdots,s(n+K-1)]$ 与噪声子空间 $\boldsymbol{V}_n$ 正交。利用该正交关系和输入信号的有限字符特性，遍历搜索可得 $s(n), s(n+1),\cdots,s(n+K-1)$,1 次遍历的搜索规模为 M^{K+1}。

考虑观测噪声时，MUSIC-like 算法的具体步骤可参照文献[9]。通过人工噪声方法可以看出，由于 DNLC 下 $s(n) \leftrightarrow \boldsymbol{x}_e(n)$ 成立，即使 Eve 未知 $\boldsymbol{h}_b$ 仍然可以窃密。由此可见，破坏输入信号的可逆性是有限字符输入 MISOME 系统安全传输的充分条件。

4　有限字符输入下 MIMOME 系统的安全性分析

对于 MIMOME 系统($N_a, N_b, N_e > 1$)的物理层安全传输，现有研究通常假设 Alice 已知 Bob 和 Eve 的信道参数[15,16]。实际上，Alice 很难获取 Eve 的信道参数，甚至不知道 Eve 是否存在。因此，Alice 更容易做到最大化合法信道互信息，特别地，波束形成正是 MISO 信道的互信息最大化方法。同 MISOME 系统一样，若窃听子信道和合法子信道质量相当，窃听者则可以配备更多天线实现窃听。

MIMOME 系统通常发送多流信号[12−16]。令 $\boldsymbol{s}(n) = [s_1(n), s_2(n),\cdots,s_{N_b}(n)]^{\mathrm{T}}$，表示 Alice 的发送符号向量。其中，$s_j(n), 1 \le j \le N_b$，表示第 j 个数据流的符号，$\boldsymbol{s}(n)$ 各符号独立同分布。Alice 在线性预编码的基础上采用人工噪声方法时，Bob 和 Eve 的接收信号分别为

$$\boldsymbol{y}_b(n) = \boldsymbol{H}_b\boldsymbol{P}\boldsymbol{s}(n) + \boldsymbol{v}_b(n) \tag{23}$$

$$\boldsymbol{y}_e(n) = \boldsymbol{H}_e\boldsymbol{P}\boldsymbol{s}(n) + \boldsymbol{H}_e\boldsymbol{H}_b^{\perp}\boldsymbol{u}(n) + \boldsymbol{v}_e(n) \tag{24}$$

其中，$\boldsymbol{H}_b \in \mathbb{C}^{N_b\times N_a}$ 是 Alice-Bob 信道矩阵；$\boldsymbol{P} \in \mathbb{C}^{N_a\times N_b}$ 是线性预编码矩阵；$\boldsymbol{v}_b(n) \in \mathbb{C}^{N_b\times 1}$ 表示 Bob 接收天线上的噪声，服从 $\mathcal{CN}(\boldsymbol{0}, \sigma_b^2\boldsymbol{I}_{N_b})$。

将 Bob 和 Eve 的信号接收过程分别表示为 Markov 链形式：

$$\boldsymbol{s}(n) \leftrightarrow \boldsymbol{x}_b(n) \rightarrow \boldsymbol{y}_b(n) \tag{25}$$

$$\boldsymbol{s}(n) \rightarrow \boldsymbol{x}_e(n) \rightarrow \boldsymbol{y}_e(n) \tag{26}$$

其中，$\boldsymbol{x}_b(n)=\boldsymbol{H}_b\boldsymbol{P}\boldsymbol{s}(n), \boldsymbol{x}_e(n)=\boldsymbol{H}_e\boldsymbol{P}\boldsymbol{s}(n)+\boldsymbol{H}_e\boldsymbol{H}_b^{\perp}\boldsymbol{u}(n)$; $\boldsymbol{s}(n) \leftrightarrow \boldsymbol{x}_b(n)$ 表示 $\boldsymbol{s}(n)$ 可从 $\boldsymbol{x}_b(n)$ 中无损恢复。根据定义，$\boldsymbol{s}(n) \rightarrow \boldsymbol{x}_e(n)$ 的等效信道也是 DNLC，所以 MIMOME 系统中也存在 $\boldsymbol{s}(n) \leftrightarrow \boldsymbol{x}_e(n)$。

由于发送信号的维度较高，很难用超平面方法直观反映出 Alice-Eve 的 DNLC。但是利用 MUSIC-like 窃密算法可以从 $\boldsymbol{x}_e(n)$ 中无损恢复出 $\boldsymbol{s}(n)$，同样可以验证 DNLC 下输入信号的可逆性。类似式(21)，将 K ($K > N_a$)个连续符号向量累积成矩阵 $\boldsymbol{X}_e = [\boldsymbol{x}_e(n), \boldsymbol{x}_e(n+1),\cdots,\boldsymbol{x}_e(n+K-1)]$，对 $\boldsymbol{X}_e$ 进行 SVD。利用 $\boldsymbol{s}(n)$ 与噪声子空间的正交关系，并基于 $\boldsymbol{s}(n)$ 的有限字符特性，同样可以搜索出 $\boldsymbol{s}(n)$。因为 1 次遍历搜索可以获得全部的符号组合，所以 1 次遍历的搜索规模仍为 M^{K+1}。

至此，论文得出如下结论：对于有限字符输入系统，在无法限制窃听信道质量的前提下，破坏输入信号的可逆性是系统安全传输的充分条件。

5　类符号人工噪声方法

以上述结论为指导，提出类符号人工噪声方法保证有限字符输入系统的安全传输。本节以 MISOME 系统为例，令 Alice 往 Bob 的零空间中发送与 $s(n)$ 分布相同的空域干扰，使 Eve 无法恢复输入信号，进而实现物理层安全传输。

具体而言，在类符号人工噪声方法中，Alice 发送符号组合 $(\boldsymbol{h}_b/\|\boldsymbol{h}_b\|)s(n) + \boldsymbol{h}_b^{\perp}\boldsymbol{u}_s(n)$。其中，$\boldsymbol{u}_s(n) \in \mathbb{C}^{N_a-1}$ 表示发送到 $\boldsymbol{h}_b$ 零空间 $\boldsymbol{h}_b^{\perp}$ 的类符号空域干

扰，不影响 Bob 但影响 Eve 接收，并且 $\boldsymbol{u}_s(n)$ 各元素与 $s(n)$ 源自同一字符集 $\mathcal{S}$。Bob 和 Eve 的接收信号分别为

$$\boldsymbol{y}_b(n)=\|\boldsymbol{h}_b\|s(n)+v_b(n) \tag{27}$$

$$\begin{aligned}\boldsymbol{y}_e(n)&=\boldsymbol{H}_e\frac{\boldsymbol{h}_b}{\|\boldsymbol{h}_b\|}s(n)+\boldsymbol{H}_e\boldsymbol{h}_b^{\perp}\boldsymbol{u}_s(n)+\boldsymbol{v}_e(n)\\&=\boldsymbol{x}_e(n)+\boldsymbol{v}_e(n)\end{aligned} \tag{28}$$

其中，$\boldsymbol{x}_e(n)=\boldsymbol{H}_e(\boldsymbol{h}_b/\|\boldsymbol{h}_b\|)s(n)+\boldsymbol{H}_e\boldsymbol{h}_b^{\perp}\boldsymbol{u}_s(n)$。将发送信号表示为

$$\left[\frac{\boldsymbol{h}_b}{\|\boldsymbol{h}_b\|},\boldsymbol{\beta}_1,\boldsymbol{\beta}_2,\cdots,\boldsymbol{\beta}_{N_a-1}\right]\begin{bmatrix}s(n)\\\boldsymbol{u}_s(n)\end{bmatrix} \tag{29}$$

此时在 Eve 看来，$(\boldsymbol{h}_b/\|\boldsymbol{h}_b\|)$ 与 $\boldsymbol{\beta}_1,\boldsymbol{\beta}_2,\cdots,\boldsymbol{\beta}_{N_a-1}$ 的作用完全等价，并且 $s(n)$ 与 $\boldsymbol{u}_s(n)$ 各元素的分布规律相同。考虑到 Eve 未知 $\boldsymbol{h}_b$，在没有其它先验知识时，Eve 的最佳解调效果是恢复出包含 $s(n)$ 和 $\boldsymbol{u}_s(n)$ 的 N_a 个有限字符序列，但是无法判定哪个字符序列对应 $s(n)$。

本质上，类符号人工噪声方法和高斯输入下的人工噪声方法的原理相同。在高斯输入下，高斯分布的空域干扰和输入信号由于分布相同而无法区分；在有限字符输入下，类符号人工噪声和输入信号也是由于分布相同而无法区分。因此，类符号人工噪声方法使 Eve 无法准确恢复 $s(n)$，可以实现系统的安全传输。从几何角度来看，$\boldsymbol{x}_e(n)$ 落在多个(超)平面上，且这些(超)平面构成一个(超)平面体[18]，$\boldsymbol{x}_e(n)$ 位于该(超)平面体的顶点上。

图 4 所示的是类符号人工噪声方法下 Eve 无噪接收信号的示意图。为了显示直观，以 BPSK 信号为例，天线数 $N_a=N_e=3$，且限定各信道增益系数为标准实高斯随机变量。此时，BPSK 的 2 个星座点分别位于两个相互平行的四边形的顶角上，且这 8 个点又对应了一个平行六面体的 8 个顶点。由于 Eve 未知 $\boldsymbol{h}_b$，在没有其它先验知识的前提下，Eve 不能准确判断各平面所对应的输入符号，也无法准确判断法线方向 $\boldsymbol{H}_e^{\dagger}\boldsymbol{h}_b/\ ||\boldsymbol{H}_e^{\dagger}\boldsymbol{h}_b||$。当天线数 N_a,N_e 增加，或者信道增益系数为复数时，接收信号的星座点将服从超平面体分布。

在 MISOME 系统中，Alice 分别采用高斯分布的人工噪声方法[7]和类符号人工噪声方法进行安全传输；Eve 采用 MUSIC-like 算法进行窃密，并选择幅度最高的“伪峰”搜索输入符号[9]，其信号解调的误码率如图 5 所示。仿真选择天线数 $N_a=3$，$N_b=1$，$N_e=2,3$ 或 4。各信道增益系数为随机产生的标准复高斯随机变量。信号功率占总功率的1/3，空域干扰的功率在 Bob 的零空间均匀分布。MUSIC-like 算法的累积符号长度 $K=9$。另外，为便于 Eve 窃听方便，选择 BPSK 输入信号。图 5 中每个点代表 1000 次 Monte-Carlo 仿真的平均值。

图 5 中，总体而言，随着 SNR 的提高，两种安全传输方法表现出的性能差异逐渐增大。Alice 采用高斯分布的人工噪声方法时，Eve 的误码率逐渐减小；而 Alice 采用类符号人工噪声方法时，Eve 的误码率始终保持在较高水平。由此可见，类符号人工噪声方法可以保证系统的安全传输。另外，高斯分布的人工噪声方法中，由于各子信道质量相当，天线数对窃听效果起到了决定性的影响。如图 5 所示，当 $N_e\geq N_a$ 时，窃听者利用 MUSIC-like 算法获得了较低的误码率。

由于 Eve 仍然可能获得多个字符序列，其中一个序列对应完整的 $s(n)$，只是不能确定是哪一个字符序列。当 Eve 获得其它的先验知识时，仍然有可能判断出 $s(n)$。本质上，类符号人工噪声方法所能做到的只是让窃听者无法分辨出有用信号和人工噪声，仍然没有改变等效信道是 DNLC 这一事实，因此对输入信号可逆性的破坏程度是有限的。

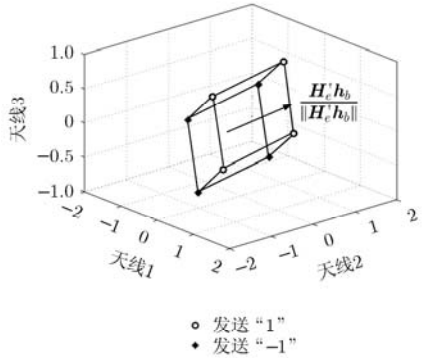

图 4 类符号人工噪声方法的无噪接收信号

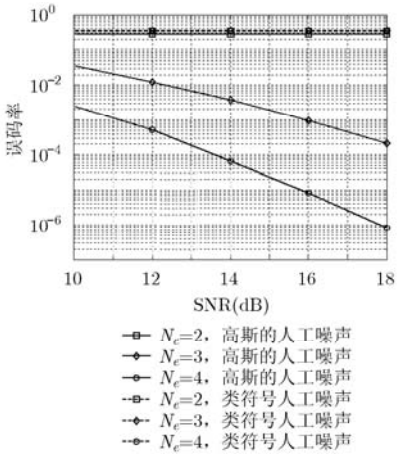

图 5 不同传输方法下 Eve 信号接收的误码率

6　结束语

在对有限字符输入下 MISOME 系统的保密互信息进行计算的基础上，分析有限字符输入的 MISOME 和 MIMOME 系统，发现窃听者无噪接收下的等效信道是一个 DNLC。由于 DNLC 下输入信号具有可逆性，为窃密提供了必要条件，致使高斯分布的人工噪声方法无法保证有限字符输入系统的安全性。通过对人工噪声方法的几何含义及其窃密算法的反向分析，指出物理层安全传输的充分条件是破坏有限字符输入信号的可逆性，并提出了类符号人工噪声方法保证物理层安全传输。由于类符号人工噪声方法对输入信号的可逆性破坏程度有限，寻找更大程度地破坏输入信号的可逆性仍然是个开放问题。

参 考 文 献

[1] Wyner A D. The wire-tap channel[J]. *The Bell System Technical Journal*, 1975, 54(8): 1355–1387.

[2] Csiszár I and Körner J. Broadcast channels with confidential messages[J]. *IEEE Transactions on Information Theory*, 1978, 24(3): 339–348.

[3] Cheong-Leung-Yan S K and Hellman M E. The Gaussian wire-tap channel[J]. *IEEE Transactions on Information Theory*, 1978, 24(4): 451–456.

[4] Liang Y, Poor H V, and Shamai S. Information theoretic security[J]. *Foundations and Trends in Communications and Information Theory*, 2009, 5(4/5): 355–580.

[5] Khisti A and Wornell G W. Secure transmission with multiple antennas I: the MISOME wiretap channel[J]. *IEEE Transactions on Information Theory*, 2010, 56(7): 3088–3104.

[6] Khisti A and Wornell G W. Secure transmission with multiple antennas II: the MIMOME wiretap channel[J]. *IEEE Transactions on Information Theory*, 2010, 56(11): 5515–5532.

[7] Goel S and Negi R. Guaranteeing secrecy using artificial noise [J]. *IEEE Transactions on Wireless Communications*, 2008, 7(6): 2180–2189.

[8] Li X, Hwu J, and Ratazzi E P. Using antenna array redundancy and channel diversity for secure wireless transmissions[J]. *Journal of Communications*, 2007, 2(3): 24–32.

[9] 吴飞龙, 王文杰, 王慧明, 等. 基于空域加扰的保密无线通信统一数学模型及其窃密方法[J]. 中国科学: 信息科学, 2012, 42(4): 483–492.
Wu Fei-long, Wang Wen-jie, Wang Hui-ming, *et al.*. A unified mathematical model for spatial scrambling based secure wireless communication and its wiretap method[J]. *CHINA SCIENCE Information Sciences*, 2012, 42(4): 483–492.

[10] Li Q and Ma W. Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization[J]. *IEEE Transactions on Signal Processing*, 2013, 61(10): 2704–2717.

[11] Qin H, Sun Y, Chang T, *et al.*. Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs[J]. *IEEE Transactions on Wireless Communications*, 2013, 12(6): 2717–2729.

[12] Zeng W, Xiao C, and Lu J. A low-complexity design of linear precoding for MIMO channels with finite-alphabet inputs[J]. *IEEE Wireless Communications Letters*, 2012, 1(1): 38–41.

[13] Zeng W, Xiao C, Wang M, *et al.*. Linear precoding for finite-alphabet inputs over MIMO fading channels with statistical CSI[J]. *IEEE Transactions on Signal Processing*, 2012, 60(6): 3134–3148.

[14] Wang M, Zheng Y R, Xiao C, *et al.*. A low complexity algorithm for linear precoder design with finite alphabet inputs[C]. Proceedings of Military Communications Conference, Orlando, FL, 2012: 1–5.

[15] Wu Y, Xiao C, Ding Z, *et al.*. Linear precoding for finite-alphabet signaling over MIMOME wiretap channels[J]. *IEEE Transactions on Vehicular Technology*, 2012, 61(6): 2599–2612.

[16] Bashar S, Ding Z, and Xiao C. On secrecy rate analysis of MIMO wiretap channels driven by finite-alphabet input[J]. *IEEE Transactions on Communications*, 2012, 60(12): 3816–3825.

[17] 傅祖芸. 信息论: 基础理论与应用[M]. 北京: 电子工业出版社, 2001: 91–93.

[18] Hansen L K and Xu G. A hyperplane-based algorithm for the digital co-channel communications problem[J]. *IEEE Transactions on Information Theory*, 1997, 43(5): 1536–1548.

崔　波：　男，1985 年生，博士生，研究方向为无线通信安全、盲信号处理.

刘　璐：　男，1988 年生，博士生，研究方向为无线通信安全.

金　梁：　男，1969 年生，教授，博士生导师，主要研究方向为无线通信、阵列信号处理.