doi:10.11959/j.issn.1000-436x.2015044

有限字符输入的空间调制物理层安全传输方法

崔波，刘璐，李翔宇，金梁
(国家数字交换系统工程技术研究中心，河南 郑州 450002)

摘 要：针对有限字符输入系统的无线物理层安全传输问题，提出了一种空间调制安全传输方法。该方法以信息论为基础，利用多输入多输出（MIMO, multiple-input multiple-output）系统的接收天线索引承载信息，通过切换接收天线随机化窃听者的等效信道，保证物理层安全传输。首先分析了该空间调制传输系统中合法用户和窃听者的不同接收性能。然后计算出安全传输系统的保密互信息，指出获取正的保密互信息的 2 个充分条件。最后给出信道互信息的估计算法，并利用有限字符集的对称性进一步降低了计算复杂度。理论分析和数据仿真验证了该安全传输方法的可行性和有效性。

关键词：无线物理层安全；空间调制；有限字符集；多输入多输出多天线窃听；信息论
中图分类号：TN92 **文献标识码**：A

Physical-layer security transmission method based on spatial modulation with finite alphabet inputs

CUI Bo, LIU Lu, LI Xiang-yu, JIN Liang
(National Digital Switching System Engineering & Technological Research Center, Zhengzhou 450002, China)

Abstract: Addressing the problem of wireless physical layer security transmission for finite alphabet input systems, a spatial modulation secure transmission method is proposed. On the basis of information theory, the method utilizes the receive antenna indices of multiple-input multiple-output (MIMO) system to bear information, and randomizes the eavesdropper's equivalent channel by switching the receive antennas, which can guarantee physical layer security transmission. First, the different receiving performances of the legitimate user and eavesdropper are analyzed in the spatial modulation secure transmission system. Second, the mutual information and secrecy mutual information of the transmission system are calculated, and two sufficient conditions that ensure positive secrecy mutual information are pointed out. Finally, an estimation algorithm of mutual information is provided. Moreover, the symmetry of finite alphabet set is exploited to decrease the computational complexity. Theoretical analysis and numerical simulation results verify the availability of the security transmission method.

Key words: wireless physical-layer security; spatial modulation; finite alphabet set; multiple-input multiple-output multiple-antenna eavesdropper (MIMOME); information theory

1 引言

基于信息论的物理层安全传输技术是当前无线通信领域的研究热点[1~7]。该技术旨在保证合法用户相比窃听者具有一定的信道质量优势[1]，通常在多天线技术的基础上通过线性预编码[2,3]和人工噪声等方法[4~6]产生可用的（正的）保密互信息。但是实际通信系统很难获取窃听信道信息，甚至不能确定窃听者存在与否，导致安全传输机制区分合法用户和窃听者的能力不足。另外，数字调制系统的有限字符集特性也给予窃听者一定的便利。吴[7]等已经发现，对于有限字符输入下采用人工噪声方法的多输入单输出（MISO, multiple-input single-output）系统，多天线窃听者可以利用穷举方法

收稿日期：2013-09-02；**修回日期**：2014-03-27
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)

进行窃密。

空间调制传输技术是当前无线通信领域的另一个研究热点[8~11]。该技术利用收发天线的索引承载信道调制符号信息，在传输幅度/相位调制（APM, amplitude/phase modulation）信号的基础上增加了一维信息承载的方式[8]，主要包括空间移位键控[9]、正交空分复用[10]和信息导引信道跳变[11]等调制方式。空间调制传输利用了收发双方不同天线对应信道间的差异性，由于合法信道和窃听信道各自内部差异性的分布规律不同，所以该技术区分合法用户和窃听者的能力较强。将它与物理层安全传输技术相结合，可以增强后者的安全传输性能。

基于空间调制，Guan[12]等针对 MISO 系统提出一种随机切换发送天线的安全传输方法。该方法假设只能有一个单天线的窃听者，且精确已知窃听者的瞬时信道信息，无法满足实际需求。本质上，MISO 系统中发送天线的切换是标量信道的切换，而标量信道只有一维的空间维度，不同标量信道间不具备足够的差异。因此，切换 MISO 系统发送天线不能实现信道随机化的效果。

针对上述问题，本文提出基于 MIMO 系统的空间调制物理层安全传输方法。该方法首先将传输信号分为 APM 信号和信道调制信号 2 部分。然后将 MIMO 系统分解为多个 MISO 子系统，并利用各个子系统传输 APM 信号，所以 APM 信号是在向量信道上传输的。在传输 APM 信号的基础上，系统将信道调制符号映射为不同的预处理权值，激活合法用户的不同接收天线。合法用户在解调 APM 信号的同时，将被激活天线的索引映射回信道调制信号，完成联合天线检测和信号解调。

相比于 MISO 系统，基于 MIMO 系统的空间调制物理层安全传输方法通过扩大系统规模，换取了系统安全性能的极大提高。一方面，基于 MIMO 系统的安全传输方法切换了向量信道。由于向量信道间存在足够的差异性，发送方可有效区分合法用户和窃听者。当系统随机切换接收天线时，窃听者被激活的天线索引不同于合法用户的，从而对发送信息产生疑义，窃听行为被抑制。另一方面，即使窃听者获得系统的调制参数，可以对系统发送信号进行盲搜索，然而由于窃听者的搜索规模与 MIMO 系统接收天线数而呈指数关系[8]，致使窃听者搜索信号的难度极大。论文通过计算系统的互信息和保密互信息，指出获取正的保密互信息的 2 个充分条件，并分析充分条件的成立基础，论证了传输方法的安全性。

后文论述中，C 、E(•) 、Tr(•) 和R(•) 分别表示复数空间、数学期望、迹和复数实部。$\{x\}^+ = \max(x,0)$ 。

2　空间调制安全传输系统模型

2.1　传输系统模型与方法

考虑 MIMOME 系统，发送方（Alice）配备 N_a 根发射天线，合法用户（Bob）配备 N_b 根接收天线，窃听者（Eve）配备 N_e 根接收天线（也可以假设存在多个联合的单天线 Eve）。Alice-Bob 信道矩阵为 $\boldsymbol{H}_b = \left[h_{i,j}\right]$，$\boldsymbol{H}_b \in C^{N_b \times N_a}$，$h_{i,j}$ 表示 Alice 第 j 根发送天线和 Bob 第 i 根接收天线间的信道增益系数。类似地，Alice-Eve 信道矩阵为 $\boldsymbol{H}_e \in C^{N_e \times N_a}$ 。

由于无线信道特征的差异性，一般情况下 $\boldsymbol{H}_b$ 与 $\boldsymbol{H}_e$ 不同。因此，当 Alice 发送信号时，Bob 和 Eve 被激活的天线不同。如图 1 所示，假设某时刻 Alice 激活了 Bob 的第 1 根接收天线，对 Eve 而言，可能被激活了第 2 根接收天线，也有可能被激活了 0 根或多根天线。

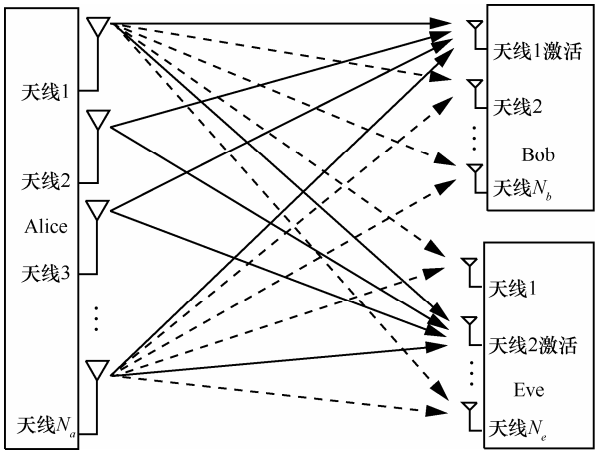

图 1　空间调制物理层安全传输模型

基于 MIMOME 系统的上述特性，本文提出一种空间调制物理层安全传输方法。如图 2 所示，Alice 一次发送 $p+q$ bit 的信息块，包含 p bit 的信道调制符号和 q bit 的 APM 符号。其中，$N_b = 2^p$，$M = 2^q$ 。Alice 将信道调制符号映射为不同的预处理权值以激活 Bob 的不同接收天线，同时在该信道上传输 APM 符号。Bob 检测到被激活的天线，将对应索引映射回信道调制符号，并解调该信道上传输的 APM 符号。

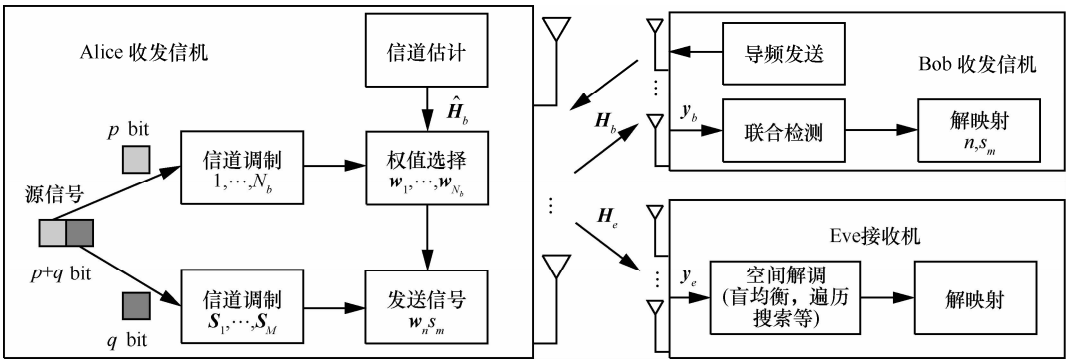

图 2 空间调制物理层安全传输方案

在发送信息块中，p bit 的信道调制符号映射为接收天线的索引，q bit 的 APM 符号源自有限字符集 $S=\{s_1,s_2,\cdots,s_M\}$。以 $N_b=4$ 和二进制相移键控（BPSK, binary phase shift keying）调制符号的组合为例说明信息块的组成形式。如表 1 所示，4 根接收天线的索引承载 2 bit 信道调制符号，BPSK 调制承载 1 bit APM 符号，总共发送 3 bit 二进制符号。

表 1 空间调制传输的信息映射关系

信息块	天线索引	BPSK 调制符号
000	1	+1
001	1	−1
010	2	+1
011	2	−1
100	3	+1
101	3	−1
110	4	+1
111	4	−1

假设 Alice 采用“迫零”方式激活 Bob 的接收天线[13]，将信道调制符号映射为预处理权值 $\boldsymbol{w}_n$，激活 Bob 的第 n 根接收天线，则 Bob 的接收信号为

$$\begin{aligned}\boldsymbol{y}_b&=\boldsymbol{H}_b\boldsymbol{W}\boldsymbol{e}_n s_m+\boldsymbol{v}_b\\&=[\cdots,\ 0,\ s_m,\ 0,\ \cdots]^{\mathrm{T}}+\boldsymbol{v}_b\end{aligned}\tag{1}$$

其中，$\boldsymbol{H}_b\boldsymbol{W}=\boldsymbol{C}$，$\boldsymbol{C}$ 是所有元素为正数的对角阵，文中为推导简便令 $\boldsymbol{C}=\boldsymbol{I}_{N_b}$；$\boldsymbol{e}_n\in C^{N_b\times 1}$ 是单位向量，第 n 个元素为 1，其余元素为 0；定义 $\boldsymbol{w}_n\triangleq\boldsymbol{W}\boldsymbol{e}_n$；$s_m$ 是源自 S 的 APM 符号；$\boldsymbol{v}_b\in C^{N_b\times 1}$ 是 Bob 接收天线上的观测噪声，服从 $\mathrm{CN}(\boldsymbol{0},\sigma_b^2\boldsymbol{I}_{N_b})$。

对 $\boldsymbol{H}_b$ 进行奇异值分解（SVD, singular value decomposition），设计系统的预处理权值 $\boldsymbol{w}_n$。$\boldsymbol{H}_b$ 的 SVD 为

$$\boldsymbol{H}_b=\boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\mathrm{H}}\tag{2}$$

其中，$\boldsymbol{U}\in C^{N_b\times N_b}$ 和 $\boldsymbol{V}\in C^{N_a\times N_a}$ 分别表示左右奇异矩阵；$\boldsymbol{\Sigma}\in C^{N_b\times N_a}$ 为奇异值形成的对角阵。假设 $\boldsymbol{H}_b$ 满秩，当 $N_a>N_b$ 时，式(2)可写为

$$\boldsymbol{H}_b=\boldsymbol{U}[\boldsymbol{D}\ \ \boldsymbol{O}][\boldsymbol{V}_0\ \boldsymbol{V}_1]^{\mathrm{H}}\tag{3}$$

其中，$\boldsymbol{D}\in C^{N_b\times N_b}$ 是非零的奇异值构成的对角阵；$\boldsymbol{V}_1\in C^{N_a\times(N_a-N_b)}$ 的列向量组成 $\boldsymbol{H}_b$ 零空间的基。设计预处理权值 $\boldsymbol{w}_n$ 为

$$\begin{aligned}\boldsymbol{w}_n&=[\boldsymbol{V}_0\ \ \boldsymbol{V}_1]\begin{bmatrix}\boldsymbol{D}^{-1}\boldsymbol{U}^{\mathrm{H}}\boldsymbol{e}_n\\ \boldsymbol{r}\end{bmatrix}\\&=\boldsymbol{V}_0\boldsymbol{D}^{-1}\boldsymbol{U}^{\mathrm{H}}\boldsymbol{e}_n+\boldsymbol{V}_1\boldsymbol{r}\end{aligned}\tag{4}$$

其中，$\boldsymbol{r}\in C^{N_a-N_b}$ 是独立于信源的随机加扰向量，服从 $\mathrm{CN}(\boldsymbol{0},\boldsymbol{I}_{N_a-N_b})$。

定义预编码矩阵

$$\begin{aligned}\boldsymbol{W}&\triangleq\boldsymbol{V}_0\boldsymbol{D}^{-1}\boldsymbol{U}^{\mathrm{H}}\left[\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_{N_b}\right]+\boldsymbol{V}_1[\boldsymbol{r},\cdots]\\&=\boldsymbol{W}_0+\boldsymbol{W}_1\end{aligned}\tag{5}$$

$\boldsymbol{W}\in C^{N_a\times N_b}$ 由 2 部分组成：$\boldsymbol{W}_0=\boldsymbol{V}_0\boldsymbol{D}^{-1}\boldsymbol{U}^{\mathrm{H}}$，每个列向量表示不同的预处理权值，与信道调制符号一一对应；$\boldsymbol{W}_1=\boldsymbol{V}_1[\boldsymbol{r},\cdots]$，处于 $\boldsymbol{H}_b$ 的零空间，即 $\boldsymbol{H}_b\boldsymbol{W}_1=0$，不影响 Bob，却会使 Eve 的接收信号随机快变，抑制 Eve 截获信号，从而提高系统安全性，其中，$[\boldsymbol{r},\cdots]$ 表示不同时刻的 N_b 个随机加扰向量组成的矩阵。特别地，当 $N_a=N_b$ 时，预编码矩阵退化为 $\boldsymbol{W}=\boldsymbol{H}_b^{-1}$，Alice 仍然可以执行空间调制传输，但不能再对 Eve 主动实施空域加扰。

Bob 的接收信号可简写为

$$\boldsymbol{y}_b = \boldsymbol{H}_b\boldsymbol{w}_n s_m + \boldsymbol{v}_b = \boldsymbol{h}_n s_m + \boldsymbol{v}_b \tag{6}$$

其中，$\boldsymbol{h}_n \triangleq \boldsymbol{H}_b\boldsymbol{w}_n$ 是 Bob 的等效接收信道。Eve 的接收信号可简写为

$$\begin{aligned}\boldsymbol{y}_e &= \boldsymbol{H}_e\boldsymbol{W}_0\boldsymbol{e}_n s_m + \boldsymbol{H}_e\boldsymbol{V}_1\boldsymbol{r} + \boldsymbol{v}_e \\ &= \boldsymbol{g}_n s_m + \boldsymbol{H}_e\boldsymbol{V}_1\boldsymbol{r} + \boldsymbol{v}_e\end{aligned} \tag{7}$$

其中，$\boldsymbol{g}_n \triangleq \boldsymbol{H}_e\boldsymbol{W}_0\boldsymbol{e}_n$ 是 Eve 的等效接收信道；$\boldsymbol{v}_e$ 是 Eve 端的观测噪声，服从 $\mathrm{CN}(\boldsymbol{0},\sigma_e^2\boldsymbol{I}_{N_e})$；$\boldsymbol{u}=\boldsymbol{H}_e\boldsymbol{V}_1\boldsymbol{r}+\boldsymbol{v}_e$ 是 Eve 的总噪声，服从 $\mathrm{CN}(\boldsymbol{0},\ \boldsymbol{H}_e\boldsymbol{V}_1\boldsymbol{V}_1^{\mathrm{H}}\boldsymbol{H}_e^{\mathrm{H}}+\sigma_e^2\boldsymbol{I}_{N_e})$。

2.2　系统的有限字符输入

虽然在信息论安全中，高斯输入通常具有最佳的理论效果，但是实际数字通信系统的调制方式属于有限字符集范畴，与高斯输入系统性能迥异[14~17]，因此文中重点针对有限字符输入系统进行安全传输设计。

常用的数字调制方式有 PSK，脉冲幅度调制（PAM, pulse amplitude modulation）和正交幅度调制（QAM, quadrature amplitude modulation）等。假设 M 维调制信号满足均匀分布，各星座点分布概率为 $1/M$，其分布形式如下。

MPSK: $s_m \in \left\{\exp\left(\mathrm{j}2\pi m/M + \mathrm{j}\phi\right)\right\}$，$\phi$ 是任意的随机相位。

MPAM: $s_m \in \left\{(2m-1-M)\Big/\sqrt{M^2-1}\right\}$。

MQAM: 若 M 为偶数，该调制则可以分解为 2 个相互正交的 $\sqrt{M}$-PAM，各占一半的功率。M 非整数平方时不支持这种分解，但是这种情况很少出现。

有限字符集存在一些特殊性质。首先，有限字符集满足对称性，$|s_m|=|s_{M-m}|$ 且 $\sum_{m=1}^{M} s_m = 0$。其次，MPSK 调制信号在此基础上还满足循环对称性，$|s_m|=\left|s_{\mathrm{mod}(m+1)}\right|$ 且 $s_{\mathrm{mod}(m+2)}/s_{\mathrm{mod}(m+1)} = s_{\mathrm{mod}(m+1)}/s_m$，$\mathrm{mod}(\cdot)$ 表示模 M 运算。

2.3　系统的接收性能

设置系统发送功率为 P，功率分配因子为 α，表示 Alice 分配 αP 功率用于发送有用信号。考虑到功率约束

$$\mathrm{Tr}(\boldsymbol{W}^{\mathrm{H}}\boldsymbol{W}) \leqslant P \tag{8}$$

预编码矩阵可改写为

$$\boldsymbol{W} = \sqrt{\frac{\alpha P N_b}{\mathrm{Tr}(\boldsymbol{D}^{-2})}}\boldsymbol{V}_0\boldsymbol{D}^{-1}\boldsymbol{U}^{\mathrm{H}} + \sqrt{\frac{(1-\alpha)P}{N_a-N_b}}\boldsymbol{V}_1\boldsymbol{R} \tag{9}$$

记 $\lambda = \sqrt{\dfrac{\alpha P N_b}{\mathrm{Tr}(\boldsymbol{D}^{-2})}}$，则 Bob 的接收信号可重写为

$$\boldsymbol{y}_b = \lambda\boldsymbol{e}_n s_m + \boldsymbol{v}_b \tag{10}$$

其信噪比（SNR, signal to noise ratio）为 $\dfrac{\alpha P N_b}{\sigma_b^2\mathrm{Tr}(\boldsymbol{D}^{-2})}$。

Bob 采用最大似然（ML, maximum likelihood）解码方法

$$(\hat{n},\ \hat{m}) = \arg\min_{\boldsymbol{e}_n, s_m}\left\|\boldsymbol{y}_b - \lambda\boldsymbol{e}_n s_m\right\|^2 \tag{11}$$

令 $\boldsymbol{e}_n s_m = \boldsymbol{r}_{n,m}$，定义成对错误概率（PEP, pairwise error probability）为

$$PEP \underset{(n,m)\neq(n_2,m_2)}{\triangleq} \Pr(\boldsymbol{r}_{n,m} \to \boldsymbol{r}_{n_2,m_2}) \tag{12}$$

表示将第 n 根接收天线及其符号 s_m 被检测为第 n_2 根天线及符号 s_{m_2} 的概率。其中，$(n,m)\neq(n_2,m_2)$ 表示 $n=n_2$ 和 $m=m_2$ 不同时成立。将 $\boldsymbol{y}_b = \lambda\boldsymbol{e}_n s_m + \boldsymbol{v}_b$ 代入式(12)，展开得到 Bob 的 *PEP*。

$$\begin{aligned}PEP &= \Pr\left(\left\|\boldsymbol{y}_b - \lambda\boldsymbol{e}_n s_m\right\|^2 > \left\|\boldsymbol{y}_b - \lambda\boldsymbol{e}_{n_2} s_{m_2}\right\|^2\right) \\ &= \Pr\left\{\mathrm{R}\left[\boldsymbol{v}_b^{\mathrm{H}}(\boldsymbol{e}_n s_m - \boldsymbol{e}_{n_2} s_{m_2})\right] > \frac{\lambda}{2}\left\|\boldsymbol{e}_n s_m - \boldsymbol{e}_{n_2} s_{m_2}\right\|^2\right\}\end{aligned} \tag{13}$$

其中，

$$\mathrm{R}\left[\boldsymbol{v}_b^{\mathrm{H}}(\boldsymbol{e}_n s_m - \boldsymbol{e}_{n_2} s_{m_2})\right] \sim \begin{cases}\mathrm{CN}\left(0, \sigma_b^2\dfrac{\left|s_m - s_{m_2}\right|^2}{2}\right), & n = n_2 \\ \mathrm{CN}\left(0, \sigma_b^2\dfrac{|s_m|^2 + \left|s_{m_2}\right|^2}{2}\right), & n \neq n_2\end{cases} \tag{14}$$

继续推导得到

$$PEP = \begin{cases}Q\left(\dfrac{\lambda\left|s_m - s_{m_2}\right|}{\sqrt{2}\sigma_b}\right), & n = n_2 \\ Q\left(\dfrac{\lambda\sqrt{|s_m|^2 + \left|s_{m_2}\right|^2}}{\sqrt{2}\sigma_b}\right), & n \neq n_2\end{cases} \tag{15}$$

其中，$Q(x)=\frac{1}{\sqrt{2\pi}}\int_x^{\infty}\mathrm{e}^{-t^2/2}\,\mathrm{d}t$ 表示 Gaussian-Q 函数。在 $n=n_2$ 时，联合检测退化为传统的 APM 解调。

以平均成对错误概率（APEP, average pairwise error probability）作为接收性能的衡量指标

$$\begin{aligned}APEP&=\mathrm{E}\left[\Pr(\boldsymbol{r}_{n,m}\to\boldsymbol{r}_{n_2,m_2})\right]\\&=\frac{1}{N_bM(N_bM-1)}\sum_{n=1}^{N_b}\sum_{m=1}^{M}\sum_{\substack{n_2=1\\(n,m)\neq(n_2,m_2)}}^{N_b}\sum_{m_2=1}^{M}P(\boldsymbol{r}_{n,m}\to\boldsymbol{r}_{n_2,m_2})\end{aligned}\tag{16}$$

将式(15)代入式(16)，得到 Bob 的 *APEP* 理论值。由于 Eve 的接收模型较为复杂，本文只得到其 ML 解码的 *APEP* 仿真值。

3 空间调制物理层安全传输系统的安全性分析

本节推导出安全传输系统的保密互信息，给出获取正的保密互信息的充分条件，并分析该条件的成立基础，论证系统传输的安全性。

3.1 空间调制安全传输系统的保密互信息

由式(6)分别得到 $\boldsymbol{y}_b$ 的条件分布概率为

$$p(\boldsymbol{y}_b\mid\boldsymbol{h}=\boldsymbol{e}_n,s=s_m)=\frac{1}{(\pi\sigma_b^2)^{N_b}}\exp\left(-\frac{\left\|\boldsymbol{y}_b-\boldsymbol{e}_ns_m\right\|^2}{\sigma_b^2}\right)\tag{17}$$

其边缘分布概率为

$$p(\boldsymbol{y}_b\mid\boldsymbol{h}=\boldsymbol{e}_n)=\frac{1}{M}\sum_{m=1}^{M}\frac{1}{(\pi\sigma_b^2)^{N_b}}\exp\left(-\frac{\left\|\boldsymbol{y}_b-\boldsymbol{e}_ns_m\right\|^2}{\sigma_b^2}\right)\tag{18}$$

$$p(\boldsymbol{y}_b\mid s=s_m)=\frac{1}{N_b}\sum_{n=1}^{N_b}\frac{1}{(\pi\sigma_b^2)^{N_b}}\exp\left(-\frac{\left\|\boldsymbol{y}_b-\boldsymbol{e}_ns_m\right\|^2}{\sigma_b^2}\right)\tag{19}$$

$$p(\boldsymbol{y}_b)=\frac{1}{N_bM}\sum_{n=1}^{N_b}\sum_{m=1}^{M}\frac{1}{(\pi\sigma_b^2)^{N_b}}\exp\left(-\frac{\left\|\boldsymbol{y}_b-\boldsymbol{e}_ns_m\right\|^2}{\sigma_b^2}\right)\tag{20}$$

已知发送信号 s 时，等效接收信道 $\boldsymbol{h}$ 和接收信号 $\boldsymbol{y}_b$ 间的条件平均互信息为

$$I(\boldsymbol{h};\boldsymbol{y}_b\mid s)=\frac{1}{N_bM}\sum_{n=1}^{N_b}\sum_{m=1}^{M}\int_{\boldsymbol{y}_b}\frac{1}{(\pi\sigma_b^2)^{N_b}}\exp\left(-\frac{\left\|\boldsymbol{y}_b-\boldsymbol{e}_ns_m\right\|^2}{\sigma_b^2}\right)\cdot\mathrm{lb}\frac{\exp\left(-\dfrac{\left\|\boldsymbol{y}_b-\boldsymbol{e}_ns_m\right\|^2}{\sigma_b^2}\right)}{\displaystyle\sum_{n_2=1}^{N_b}\exp\left(-\frac{\left\|\boldsymbol{y}_b-\boldsymbol{e}_{n_2}s_m\right\|^2}{\sigma_b^2}\right)}\mathrm{d}\boldsymbol{y}_b\tag{21}$$

将 $\boldsymbol{y}_b=\boldsymbol{e}_ns_m+\boldsymbol{v}_b$ 代入式(21)，得到

$$I(\boldsymbol{h};\boldsymbol{y}_b\mid s)=\mathrm{lb}N_b-\frac{1}{N_bM}\sum_{n=1}^{N_b}\sum_{m=1}^{M}\cdot\mathrm{E}_{\boldsymbol{v}_b}\left[\mathrm{lb}\sum_{n_2=1}^{N_b}\exp\left(-\frac{\left\|(\boldsymbol{e}_n-\boldsymbol{e}_{n_2})s_m+\boldsymbol{v}_b\right\|^2-\left\|\boldsymbol{v}_b\right\|^2}{\sigma_b^2}\right)\right]\tag{22}$$

$$I(s;\boldsymbol{y}_b)=\mathrm{lb}M-\frac{1}{N_bM}\sum_{n=1}^{N_b}\sum_{m=1}^{M}\cdot\mathrm{E}_{\boldsymbol{v}_b}\left[\mathrm{lb}\frac{\displaystyle\sum_{n_2=1}^{N_b}\sum_{m_2=1}^{M}\exp\left(-\frac{\left\|\boldsymbol{d}_n+\boldsymbol{v}_b\right\|^2}{\sigma_b^2}\right)}{\displaystyle\sum_{n_2=1}^{N_b}\exp\left(-\frac{\left\|(\boldsymbol{e}_n-\boldsymbol{e}_{n_2})s_m+\boldsymbol{v}_b\right\|^2}{\sigma_b^2}\right)}\right]\tag{23}$$

其中，$\boldsymbol{d}_n=\boldsymbol{e}_ns_m-\boldsymbol{e}_{n_2}s_{m_2}$，当 $m_2=m$ 且 $n_2=n$ 时，$\boldsymbol{d}_n=\boldsymbol{0}$。

把 $\boldsymbol{y}_b$ 与 s、$\boldsymbol{h}$ 间的互信息 $I(s,\boldsymbol{h};\boldsymbol{y}_b)$ 作为合法信道的互信息，并根据互信息链式法则

$$I(s,\boldsymbol{h};\boldsymbol{y}_b)=I(\boldsymbol{h};\boldsymbol{y}_b\mid s)+I(s;\boldsymbol{y}_b)\tag{24}$$

得到

$$I(s,\boldsymbol{h};\boldsymbol{y}_b)=\mathrm{lb}N_bM-\frac{1}{N_bM}\sum_{n=1}^{N_b}\sum_{m=1}^{M}\cdot\mathrm{E}_{\boldsymbol{v}_b}\left[\mathrm{lb}\sum_{n_2=1}^{N_b}\sum_{m_2=1}^{M}\exp\left(-\frac{\left\|\boldsymbol{d}_n+\boldsymbol{v}_b\right\|^2-\left\|\boldsymbol{v}_b\right\|^2}{\sigma_b^2}\right)\right]\tag{25}$$

当 *SNR* 趋于无穷大时，σ_b^2 趋于 0，$I(s,\boldsymbol{h}_b;\boldsymbol{y}_b)$ 趋于上限 $\mathrm{lb}N_bM$。

当 $N_a=N_b$ 时，Alice 将无法发送空域干扰，$\boldsymbol{u}$ 退化为 $\boldsymbol{v}_e$，此时窃听信道的互信息 $I(s,\boldsymbol{g};\boldsymbol{y}_e)$ 为

$$I(s,\boldsymbol{g};\boldsymbol{y}_e)=\mathrm{lb}N_bM-\frac{1}{N_bM}\sum_{n=1}^{N_b}\sum_{m=1}^{M}\cdot\mathrm{E}_{\boldsymbol{v}_e}\left[\mathrm{lb}\sum_{n_2=1}^{N_b}\sum_{m_2=1}^{M}\exp\left(-\frac{\left\|\boldsymbol{d}_e+\boldsymbol{v}_e\right\|^2-\left\|\boldsymbol{v}_e\right\|^2}{\sigma_e^2}\right)\right]\tag{26}$$

其中，$\boldsymbol{d}_e = \boldsymbol{g}_n s_m - \boldsymbol{g}_{n_2} s_{m_2}$。当 *SNR* 趋于无穷大时，$I(s,\boldsymbol{g}_e;\boldsymbol{y}_e)$ 也趋于上限 $\mathrm{lb}N_bM$。

根据广播信道中保密互信息的定义[18]，定义空间调制安全传输系统的保密互信息为

$$I_s \triangleq \left\{ I(s,\boldsymbol{h};\boldsymbol{y}_b) - I(s,\boldsymbol{g};\boldsymbol{y}_e) \right\}^+ \tag{27}$$

由于 Alice 掌握信息发送的主动权并且能够获取 $\boldsymbol{h}$ 的估计值，式(27)中 $I(s,\boldsymbol{h};\boldsymbol{y}_b)$ 容易趋近上限，因此获取正的 I_s 的关键在于减少 $I(s,\boldsymbol{g};\boldsymbol{y}_e)$。

3.2　正的保密互信息的充分条件分析

当空域干扰为 0 时，$I(s,\boldsymbol{g};\boldsymbol{y}_e)$ 和 $I(s,\boldsymbol{h};\boldsymbol{y}_b)$ 具有相同的理论上限，表面上看系统并不具备正的保密互信息。但是空间调制安全传输技术恶化了 Eve 的接收，甚至会出现下面 2 种情况：Eve 错误检测所有的接收天线或错误解调所有的接收信号。下面将说明，在合法信道互信息趋于上限时，实现或逼近上述 2 种情况可以减少 $I(s,\boldsymbol{g};\boldsymbol{y}_e)$，为有限字符输入系统获取正的保密互信息提供了 2 个充分条件[12]。

当 Eve 错误检测所有天线时，将把检测到的各个 $\boldsymbol{g}_n$ 等效视为同一天线增益，即 $\boldsymbol{g}_n = \boldsymbol{g}_{n_2}$。将 $\boldsymbol{g}_n = \boldsymbol{g}_{n_2}$ 代入 $I(s,\boldsymbol{g};\boldsymbol{y}_e)$，得到

$$I(s,\boldsymbol{g};\boldsymbol{y}_e) = \mathrm{lb}N_bM - \frac{1}{N_bM}\sum_{n=1}^{N_b}\sum_{m=1}^{M}\cdot \mathrm{E}_{\boldsymbol{v}_e}\left\{ \mathrm{lb}\sum_{n_2=1}^{N_b}\sum_{m_2=1}^{M}\exp\left[-\frac{\left\| \boldsymbol{g}_{n_2}(s_m - s_{m_2}) + \boldsymbol{v}_e \right\|^2 - \left\| \boldsymbol{v}_e \right\|^2}{\sigma_e^2} \right] \right\} \tag{28}$$

其上限是 $\mathrm{lb}M$。当 *SNR* 较高时，$I(s,\boldsymbol{h};\boldsymbol{y}_b)$ 和 $I(s,\boldsymbol{g};\boldsymbol{y}_e)$ 同时趋于上限，根据式(27)得到 I_s 趋于 $\mathrm{lb}N_b$。

当 Eve 错误判断所有符号时，将把解调的各个 s_m 等效视为同一符号，即 $s_m = s_{m_2}$。将 $s_m = s_{m_2}$ 代入 $I(s,\boldsymbol{g};\boldsymbol{y}_e)$，得到

$$I(s,\boldsymbol{g};\boldsymbol{y}_e) = \mathrm{lb}N_bM - \frac{1}{N_bM}\sum_{n=1}^{N_b}\sum_{m=1}^{M}\cdot \mathrm{E}_{\boldsymbol{v}_e}\left\{ \mathrm{lb}\sum_{n_2=1}^{N_b}\sum_{m_2=1}^{M}\exp\left[-\frac{\left\| (\boldsymbol{g}_n - \boldsymbol{g}_{n_2}) s_{m_2} + \boldsymbol{v}_e \right\|^2 - \left\| \boldsymbol{v}_e \right\|^2}{\sigma_e^2} \right] \right\} \tag{29}$$

其上限是 $\mathrm{lb}N_b$。当 *SNR* 较高时，$I(s,\boldsymbol{h};\boldsymbol{y}_b)$ 和 $I(s,\boldsymbol{g};\boldsymbol{y}_e)$ 同时趋于上限，根据式(27)得到 I_s 趋于 $\mathrm{lb}M$。

当 Eve 错误检测所有接收天线且错误解调所有接收信号，根据式(26)可知 $I(s,\boldsymbol{g};\boldsymbol{y}_e)$ 为 0。当 *SNR* 较高时，$I(s,\boldsymbol{h};\boldsymbol{y}_b)$ 趋于上限，由式(27)得到 I_s 趋于 $\mathrm{lb}M$。

因此，当合法信道互信息趋于上限时，实现或逼近上述 2 个充分条件可以保证系统的安全传输。下面分别从高阶统计量和二阶统计量的角度说明，在空间调制安全传输方法中上述 2 个充分条件均能成立，从而有效抑制 Eve 的窃听行为。

1) Eve 无法通过高阶统计量实现窃听

先考虑最不利的情况，即空域干扰为 0。现有的 Bussgang、超指数和倒谱等盲均衡算法均需要得到稳定的高阶统计量，并且需要几百甚至更多的符号才能获得转换矩阵 $\boldsymbol{G} \in C^{N_b \times N_e}$ 以实现

$$\boldsymbol{G}\boldsymbol{y}_e = \boldsymbol{G}\left(\boldsymbol{H}_e \boldsymbol{w}_n s_m + \boldsymbol{v}_e \right) = \boldsymbol{e}_n s_m + \boldsymbol{G}\boldsymbol{v}_e \tag{30}$$

从而等效接收到和 Bob 相同的信号，恢复发送符号和信道调制符号。（当 $\boldsymbol{H}_e$ 可逆时，$\boldsymbol{G} = \boldsymbol{H}_b \boldsymbol{H}_e^{-1}$；否则 $\boldsymbol{G} = \boldsymbol{H}_b \boldsymbol{H}_e^{\dagger}$，$\boldsymbol{H}_e^{\dagger}$ 表示伪逆）。由于等效的窃听信道在不断切换，Eve 的接收信号不具备稳定的高阶统计特征，无法通过高阶统计量实现窃听。加上空域干扰后，Eve 的窃听难度进一步增加。

2) Eve 无法通过二阶统计量实现窃听

MUSIC-like 算法是一种典型的基于二阶统计量的窃密算法[7]。该算法假设 Eve 已经获取信号调制类型参数等先验信息，对每 K（$K > N_a N_b$）个符号进行一次 SVD 和遍历搜索，所需要的符号数最少。由于每个符号 $\boldsymbol{e}_n s_m$ 对应 N_bM 种可能形式，因此一次遍历的搜索规模为 $(N_bM)^K$。以 QPSK 输入的 4 发 4 收 MIMO 系统为例，Eve 一次遍历的搜索规模是 $16^5 \approx 10^6$。随着信号调制阶数和天线规模的增大，搜索规模将呈指数增加，计算复杂度极为庞大。因此，Eve 也无法通过二阶统计量实时窃听。进一步，当空间调制传输系统采用更为灵活的软激活方式时，接收信号不再是 $\boldsymbol{e}_n s_m$ 的形式，将不具备有限字符特性，致使 Eve 无法利用符号遍历的方法窃听。

对于非符号遍历的二阶统计量方法，则需要通过二阶统计量估计出信道信息或构造均衡器后才能恢复输入信号，一般情况下，比 MUSIC-like 算法所需符号数更多。但是空间调制安全传输技术使得 Eve 的等效接收信道随机快变，致使 Eve 无法正

确估计二阶统计量，窃听失败。

另外，对 Bob 所有天线上的接收信号求和，可以将 N_a 发 N_b 收的 MIMO 空间调制安全传输系统等价为 N_aN_b 发 1 收的 MISO 人工噪声系统，信道则由 $N_b\times N_a$ 的 $\boldsymbol{H}_b=\left[h_{i,j}\right]$ 变为 $N_bN_a\times 1$ 的 $\boldsymbol{h}_b^{\mathrm{H}}=\left[h_{1,1},\cdots,h_{1,N_a},\cdots,h_{N_b,1},\cdots,h_{N_b,N_a}\right]$，Alice 每次使用全部的 N_aN_b 根天线发送信号和空域干扰，并且该MISO系统可以纳入文献[7]中的基于空域加扰的保密无线通信统一数学模型。由于该 MISO 系统的发送天线数是 MIMO 系统发送天线数的 N_b 倍，窃听者需要配备更多的窃听天线才能窃听。因此，相比于 MISO 人工噪声系统，空间调制安全传输技术提高了对窃听者的装备要求。

4 空间调制传输系统的互信息估计

基于 MIMO 信道的互信息下界[19,20]，本节推导出空间调制传输系统互信息下界的一般形式，并选择适当参数的下界对信道互信息进行估计。另外，利用有限字符集的对称特性，进一步降低互信息估计的计算复杂度。

4.1 一般形式的互信息下界

Zeng[19]等发现有限字符输入下 MIMO 信道互信息存在一个下界，该下界舍弃一个常数项后与互信息理论值很接近，适用于各种信道条件和调制类型。基于下界估计信道互信息可以避免互信息计算中繁琐的 Monte Carlo 仿真，在许多优化算法中得到了应用[2,20,21]。空间调制传输系统也存在类似的互信息下界可用于估计互信息，下面的定理给出了它的一般形式。

定理 1 有限字符输入的空间调制传输系统的信道互信息存在下界

$$I_L^{\alpha}(s,\boldsymbol{h};\boldsymbol{y}_b)=\mathrm{lb}N_bM-\left[(1+\alpha)\mathrm{lbe}-\mathrm{lb}(1+\alpha)\right]N_b-\frac{1}{M}\sum_{m=1}^{M}\mathrm{lb}\sum_{n_2=1}^{N_b}\sum_{m_2=1}^{M}\exp\left(-\frac{1+\alpha}{2+\alpha}\frac{\left\|\boldsymbol{d}_1\right\|^2}{\sigma_b^2}\right)\tag{31}$$

其中，$\boldsymbol{d}_1=\boldsymbol{e}_1s_m-\boldsymbol{e}_{n_2}s_{m_2}$，$\alpha\geqslant -1$。

证明 式(25)中的信道互信息可以分解成下面的形式。

$$\begin{aligned}I_L^{\alpha}(s,\boldsymbol{h};\boldsymbol{y}_b)=\mathrm{lb}N_bM-\mathrm{E}_{\boldsymbol{v}_b}\left[\mathrm{lb}\exp\left(\frac{1+\alpha}{\sigma^2}\left\|\boldsymbol{v}_b\right\|^2\right)\right]-\frac{1}{N_bM}\sum_{n=1}^{N_b}\sum_{m=1}^{M}\mathrm{E}_{\boldsymbol{v}_b}\cdot\\ \left\{\mathrm{lb}\sum_{n_2=1}^{N_b}\sum_{m_2=1}^{M}\exp\left[-\frac{\left\|\boldsymbol{d}_n\right\|^2+\boldsymbol{d}_n^{\mathrm{H}}\boldsymbol{v}_b+\boldsymbol{v}_b^{\mathrm{H}}\boldsymbol{d}_n+(1+\alpha)\left\|\boldsymbol{v}_b\right\|^2}{\sigma_b^2}\right]\right\}\end{aligned}\tag{32}$$

式(32)等号右侧的第 2 项等于 $-(1+\alpha)N_b\mathrm{lbe}$。由于 $\mathrm{lb}(x)$ 是凹函数，利用 Jensen 不等式先对等式右侧第 3 项的变量 $\boldsymbol{v}_b$ 求期望，得到第 3 项的下界为

$$\begin{aligned}&-\frac{1}{N_bM}\sum_{n=1}^{N_b}\sum_{m=1}^{M}\mathrm{lbE}_{\boldsymbol{v}_b}\left\{\sum_{n_2=1}^{N_b}\sum_{m_2=1}^{M}\exp\left[-\frac{\left\|\boldsymbol{d}_n\right\|^2+\boldsymbol{d}_n^{\mathrm{H}}\boldsymbol{v}_b+\boldsymbol{v}_b^{\mathrm{H}}\boldsymbol{d}_n+(1+\alpha)\left\|\boldsymbol{v}_b\right\|^2}{\sigma_b^2}\right]\right\}\\ &=-\frac{1}{N_bM}\sum_{n=1}^{N_b}\sum_{m=1}^{M}\mathrm{lb}\int_{\boldsymbol{v}_b}\sum_{n_2=1}^{N_b}\sum_{m_2=1}^{M}\exp\left(-\frac{1+\alpha}{2+\alpha}\frac{\left\|\boldsymbol{d}_n\right\|^2}{\sigma_b^2}-\frac{2+\alpha}{\sigma_b^2}\left\|\frac{\boldsymbol{d}_n}{2+\alpha}+\boldsymbol{v}_b\right\|^2\right)\mathrm{d}\boldsymbol{v}_b\\ &=N_b\mathrm{lb}(2+\alpha)-\frac{1}{N_bM}\sum_{n=1}^{N_b}\sum_{m=1}^{M}\mathrm{lb}\sum_{n_2=1}^{N_b}\sum_{m_2=1}^{M}\exp\left(-\frac{1+\alpha}{2+\alpha}\frac{\left\|\boldsymbol{d}_n\right\|^2}{\sigma_b^2}\right)\end{aligned}\tag{33}$$

式(33)中，当 $n=n_2$ 时，$\left\|\boldsymbol{d}_n\right\|^2=\left|s_m-s_{m_2}\right|^2$；当 $n\neq n_2$ 时，$\left\|\boldsymbol{d}_n\right\|^2=\left|s_m\right|^2+\left|s_{m_2}\right|^2$，因此不同的 n 对求和的作用相同。不失一般性，令 $n=1$，式(33)可简化为

$$N_b\mathrm{lb}(2+\alpha)-\frac{1}{M}\sum_{m=1}^{M}\mathrm{lb}\sum_{n_2=1}^{N_b}\sum_{m_2=1}^{M}\exp\left(-\frac{1+\alpha}{2+\alpha}\frac{\left\|\boldsymbol{d}_1\right\|^2}{\sigma_b^2}\right)\tag{34}$$

结合式(33)和式(34)可得式(31)。

特别地，当 $\alpha=0$ 时，该下界与 Zeng 等的形式是一致的；当 $\alpha=-1$ 时，下界恒为 0。

舍弃式(31)等号右侧第 2 项 $-[(1+\alpha)\mathrm{lbe}-\mathrm{lb}(1+\alpha)]N_b$，剩余部分记为 $\hat{I}_L^{\alpha}(s,\boldsymbol{h};\boldsymbol{y}_b)$。仿真产生 2 发 2 收和 4 发 4 收的信道矩阵，矩阵元素相互独立且服从 CN(0,1)。信号输入类型为 BPSK，QPSK 和

4-PAM 等。在[−15,30] dB 的 SNR 段，每隔 1 dB 设置一个样本点，以10^4次 Monte Carlo 仿真平均值作为互信息的理论值，比较不同信道条件下$\hat{I}_L^{\alpha}(s,\boldsymbol{h};\boldsymbol{y}_b)$仿真值与理论值之差的标准差。综合比较发现在$\alpha=-0.27$附近时得到的标准差最小，相对于其他$\alpha$，$\hat{I}_L^{-0.27}(s,\boldsymbol{h};\boldsymbol{y}_b)$总体上最接近$I(s,\boldsymbol{h};\boldsymbol{y}_b)$的理论值。

4.2　有限字符集对称性的应用

因为

$$\left\|\boldsymbol{d}_1\right\|^2=\begin{cases}\left|s_m-s_{m_2}\right|^2=\left|e_{m,m_2}\right|^2, & n_2=1\\ \left|s_m\right|^2+\left|s_{m_2}\right|^2, & n_2\neq 1\end{cases} \tag{35}$$

其中，符号差$e_{m,m_2}=s_m-s_{m_2}$，所以输入信号在式(31)中总是以$\left|e_{m,m_2}\right|^2$和$\left|s_m\right|^2+\left|s_{m_2}\right|^2$的形式出现，可以利用有限字符集的对称性进一步简化式(31)的计算量。

基于有限字符集的对称性，将S划分成如下 2 个子集

$$S=\left[S_1\ \ S_2\right] \tag{36}$$

其中，$S_1=[s_1\cdots s_{M/2}]$，$S_2=[s_{M/2+1}\cdots s_M]$。当$n_2=1$，$1\leqslant m\leqslant M/2$且$1\leqslant m_2\leqslant M$时，$s_m\in S_1$且$e_{m,m_2}$满足

$$\left|e_{m,m_2}\right|^2=\left|e_{M/2+m,\mathrm{mod}(M/2+m_2)}\right|^2 \tag{37}$$

$\left\|\boldsymbol{d}_1\right\|^2=\left|e_{m,m_2}\right|^2$，式(31)中$m$和$M/2+m$项对求和的贡献相同，对$m$的相关求和项可以减少到一半，即$M/2$项。当$n_2\neq 1$时，由于$\left|s_m\right|=\left|s_{M-m}\right|$且$\left\|\boldsymbol{d}_1\right\|^2=\left|s_m\right|^2+\left|s_{m_2}\right|^2$，式(31)中对$m$的相关求和项也可以减少到一半。综合比较，式(31)中可对m从 1 到$M/2$求和，然而将求和结果乘以 2，因此互信息估计算法的计算量减半。

对 MPSK 调制而言，其有限字符集在对称性的基础上还存在循环对称性。当$n_2=1$，$m=1$且$1\leqslant m_2\leqslant M$时，根据 2.2 节中 MPSK 的分布形式，$e_{m,m_2}$满足

$$\left|e_{1,m_2}\right|^2=\left|e_{2,\mathrm{mod}(m_2+1)}\right|^2=\cdots=\left|e_{M,\mathrm{mod}(m_2+M-1)}\right|^2 \tag{38}$$

由于$\left\|\boldsymbol{d}_1\right\|^2=\left|e_{m,m_2}\right|^2=\left|e_{1,m_2}\right|^2$，对$m$的相关求和项可以减少至 1 项。当$n_2\neq 1$时，由于$\left|s_m\right|=\left|s_{\mathrm{mod}(m+1)}\right|$且$\left\|\boldsymbol{d}_1\right\|^2=\left|s_m\right|^2+\left|s_{m_2}\right|^2$，对$m$的相关求和项也可以减少至 1 项。综合比较，式(31)中令$m=1$即可，然后将求和结果乘以M，因此互信息估计的计算量减少到原来的$1/M$。

5　数据仿真结果

对空间调制物理层安全传输方法进行仿真分析，验证传输方案的可行性。仿真图中每个 *APEP* 点对应 10^5 个接收符号的仿真结果的平均值，每个互信息点对应 10^4 次 Monte Carlo 仿真结果的平均值。随机生成 Alice 到 Bob 和 Eve 的信道矩阵，各信道增益系数是相互独立的标准复高斯随机变量。

图 3 所示为空间调制安全传输的接收 *APEP*。仿真选择$N_a=6$，$N_b=2$，$N_e=N_b$，输入信号的调制类型为 BPSK。Bob 和 Eve 均采用 ML 解码方法，功率分配因子$\alpha=1$和 0.5，分别表示发送的空域扰动功率为 0 和占总功率的一半。由图可见，Eve 的 *APEP* 始终稳定在一个常数值，且比 Bob 高数个量级。其中，Bob 在$\alpha=1$且 *SNR* 为 12 dB 时，由于仿真所用符号数不足，得到的 *APEP* 为 0，该点在图 3 中没有体现出来。

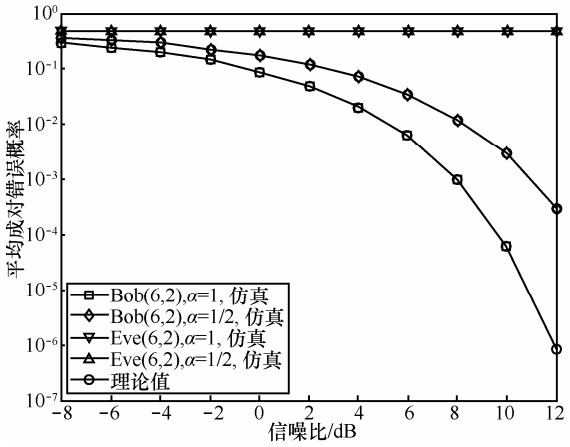

图 3　空间调制安全传输系统的 *APEP*

图 4 所示为空间调制传输系统的合法信道互信息。实线代表不同信道条件下的 Monte Carlo 仿真值，虚线代表基于下界的估计值。仿真选择$N_a=4$，$N_b=1$，2 和 4，输入信号的调制类型为 BPSK 和 QPSK。比较不同N_b下信道互信息的估计精度，随着N_b的增大，得到互信息估计值逐渐偏离 Monte Carlo 仿真值，可见接收天线数对互信息的近似方法有一定负面影响。不过这种偏离表现出一定的规律性，一般在互信息趋近$\mathrm{lb}N_bM$前的一段 *SNR* 范围内，互信息估计值有一点偏大。

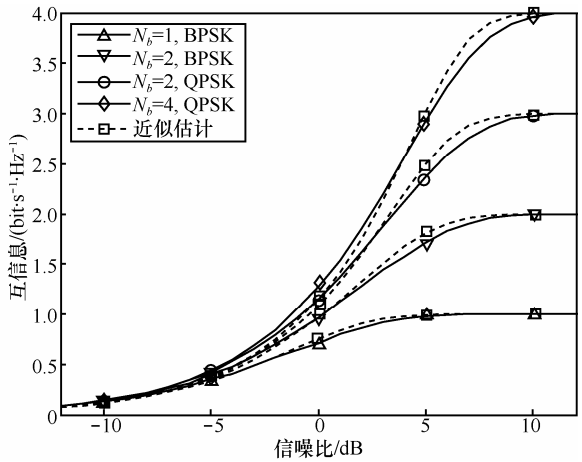

图 4 空间调制安全传输系统的合法信道互信息

图 5 是空间调制传输系统的保密互信息。仿真选择 $N_a=4$， $N_b=4$， $N_e=4$，输入信号调制类型为 BPSK。图中给出了 Eve 满足 2 个安全充分条件时的系统保密互信息。当 $s_m=s_{m_2}$ 成立且 *SNR* 较高时，保密互信息趋于 1 bit/(s·Hz)；当 $\boldsymbol{g}_n=\boldsymbol{g}_{n_2}$ 成立且 *SNR* 较高时，保密互信息趋于 2 bit/(s·Hz)；当 2 个充分条件都成立且 *SNR* 较高时，保密互信息趋于 3 bit/(s·Hz)。

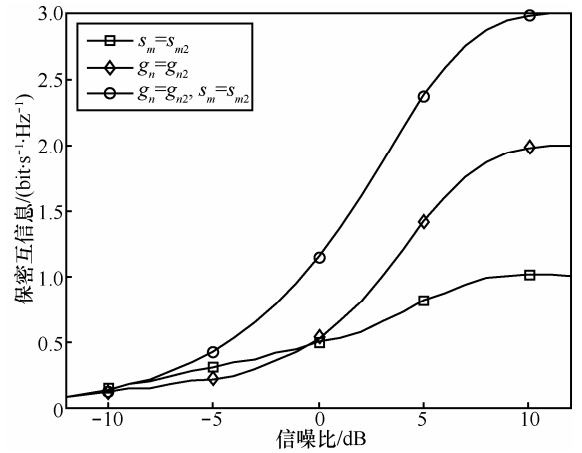

图 5 空间调制安全传输系统的保密互信息

6 结束语

本文以有限字符输入的 MIMO 系统为对象，结合空间调制技术提出了一种无线物理层安全传输方法。该方法以 MIMO 接收天线索引承载信道调制信息，通过切换向量信道随机化窃听者的等效接收信道，恶化了窃听者的接收质量，从而保障了信息的安全传输。基于信息论，计算了该安全传输系统的保密互信息，给出了系统安全的充分条件，并分析了空间调制传输方法下该充分条件的成立基础，论证了安全传输系统的可行性。仿真结果也验证了所提安全传输方法的可行性。下一步，除迫零激活方式外，需要研究更加灵活的软激活方式。

参考文献：

[1] BASHAR S, XIAO C, DING Z. On secrecy rate analysis of MIMO wiretap channels driven by finite-alphabet input[J]. IEEE Transactions on Communications, 2012, 60(12): 3816-3825.

[2] 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.

[3] 罗文宇,金梁, 黄开枝等. γ 约束均方误差下的无线信道加密方法[J]. 电子学报, 2010, 40(7): 1289-1297.
LUO W Y, JIN L, HUANG K Z, *et al*. A wireless channel encryption method with γ mean square error[J]. Atca Electronica Sinica, 2010, 40(7): 1289-1297.

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

[5] 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.

[6] 李桥龙, 金梁. 基于最小信息泄漏的线性随机化实现物理层安全传输[J]. 通信学报, 2013, 34(7): 42-48.
LI Q L, JIN L. Linear randomization with lowest information leakage for physical layer secure transmission[J]. Journal on Communications, 2013, 34(7): 42-48.

[7] 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 F L, WANG W J, WANG H M, *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.

[8] MESLEH R, HAAS H, SINANOVIC S, *et al*. Spatial modulation[J]. IEEE Transactions on Vehicular Technology, 2008, 57(4): 2228 -2241.

[9] DI RENZO M, DE LEONARDIS D, GRAZIOSI F, *et al*. Space shift keying (SSK-) MIMO with practical channel estimates[J]. IEEE Transactions on Wireless Communications, 2012, 60(4): 998-1012.

[10] SIGDEL S, KRZYMIEŃ W A. Antenna and user subset selection in downlink multiuser orthogonal space-division multiplexing[J]. Wireless Personal Communications, 2010, 52(1): 227-240.

[11] YANG Y, AISSA S. Information guided channel hopping with an arbitrary number of transmit antennas[J]. IEEE Communications Letters, 2012, 16(10): 1552-1555.

[12] GUAN X, CAI Y, YANG W. On the mutual information and precoding

for spatial modulation with finite alphabet[J]. IEEE Wireless Communications Letters, 2013, 2(4): 383-386.

[13] LI Q. Information-guided randomization for wireless physical layer secure transmission[A]. IEEE Milicom[C]. Orlando, FL, 2012.1-6.

[14] GUO D, SHAMAI S, VERDÚ S. Mutual information and minimum mean-square error in Gaussian channels[J]. IEEE Transactions on Information Theory, 2005, 51(4): 1261-1282.

[15] PALOMAR D P, VERDÚ S. Gradient of mutual information in linear vector Gaussian channels[J]. IEEE Transactions on Information Theory, 2006, 52(1): 141-154.

[16] LOZANO A, TULINO A M, VERDÚ S. Optimum power allocation for parallel Gaussian channels with arbitrary input distributions[J]. IEEE Transactions on Information Theory, 2006, 52(7):3033-3051.

[17] PÉREZ-CRUZ F, RODRIGUES M R D, VERDÚ S. MIMO Gaussian channels with arbitrary inputs: optimal preceding and power allocation[J]. IEEE Transactions on Information Theory, 2010, 56(3): 1070-1084.

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

[19] ZENG W, XIAO C, LU J. A low-complexity design of linear preceding for MIMO channels with finite-alphabet inputs[J]. IEEE Communications Letters, 2012, 1(1):38-41.

[20] ZENG W, XIAO C, WANG M, *et al*. Linear preceding for finite-alphabet inputs over MIMO fading channels with statistical CSI[J]. IEEE Transactions on Signal Processing, 2012, 60(6): 3134-3148.

[21] WANG M, ZHENG Y R, XIAO C, *et al*. A low complexity algorithm for linear precoder design with finite alphabet inputs[A]. IEEE Milicom[C]. Orlando, FL, 2012.1-5.

作者简介：

崔波（1985-），男，安徽长丰人，国家数字交换系统工程技术研究中心博士生，主要研究方向为物理层安全、盲信号处理等。

刘璐（1988-），男，安徽宿州人，国家数字交换系统工程技术研究中心博士生，主要研究方向为物理层安全。

李翔宇（1987-），男，河南淮阳人，国家数字交换系统工程技术研究中心博士生，主要研究方向为物理层安全。

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，主要研究方向为物理层安全、通信信号处理和阵列信号处理等。