隐藏有限字符特性的跳空安全传输方法

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: 针对无线数字通信系统,从信息论角度推导了一个保障物理层安全传输的充分条件,并提出了一种隐藏有限字符特性的跳空安全传输方法.首先,在有限字符输入系统中,多天线窃听者具有离散有噪无损信道(Discrete Noisy Lossless Channel,DNLC)结构,可以恢复保密信号,致使人工噪声方法失效,因此破坏窃听者的DNLC结构是保证系统传输安全的一个充分条件.然后,利用无线信道特征的多样性和独特性,提出一种基于多输入多输出(Multiple Input Multiple Output,MIMO)系统的跳空安全传输方法,在传输信息的过程中随机切换收发天线并发送空域干扰,可以隐藏保密信号的有限字符特性并破坏窃听者的DNLC结构.最后,理论分析和仿真结果表明了该安全方法的有效性.

关键词: 无线物理层安全;有限字符;跳空;离散有噪无损信道;多输入多输出多天线窃听者
中图分类号: TN92 **文献标识码:** A **文章编号:** 0372-2112 (2015)05-0940-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.05.017

A Space Hopping Secure Transmission Method with Masked Characteristic of Finite Alphabets

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

Abstract: Addressing the wireless digital communication system, a sufficient condition to ensure the physical-layer security transmission is derived from the viewpoint of information theory, and a space hopping secure transmission method is proposed, which can mask the characteristic of finite alphabets. First, since the multi-antenna eavesdropper in the finite-alphabet-input system possesses the architecture of Discrete Noisy Lossless Channel (DNLC), it can reconstruct the secret signal and invalidate the artificial noise method. As a result, destroying the eavesdropper's DNLC architecture becomes a sufficient condition for ensuring the security of system transmission. Then, utilizing the diversity and uniqueness of wireless channel characteristics, a space hopping secure transmission method based on the Multiple Input Multiple Output (MIMO) system is proposed. It switches receiver/transmitter antennas and transmits spatial scrambling during the information transmission, which can mask the finite alphabet characteristic of the secret signal and destroy the eavesdropper's DNLC architecture. Finally, theoretical analysis and simulation results demonstrate the efficacy of the secure method.

Key words: wireless physical-layer security; finite alphabet; space hopping; discrete noisy noiseless channel (DNLC); multiple input multiple output multiple-antenna eavesdropper (MIMOME)

1 引言

基于信息论的物理层安全技术[1~4]通过开发无线信道的空域特征差异保障通信系统的安全.其中,Goel等人[1]提出的人工噪声方法具有代表性,该方法对合法信道进行强耦合,在未知窃听信道信息时仍能保证系统的安全性[2~4].目前,物理层安全技术的研究通常假设理想的高斯输入[1~4],该假设便于理论研究,但在实际中无法实现.实际的通信系统一般使用数字调制,所需传输的保密信号具备有限字符特性,为窃听者提供了窃密依据,致使人工噪声等安全方法失效[5].尽管如此,考虑到有限字符输入系统的高计算复杂度[6~10],还鲜有学者从信息论角度研究其物理层安全传输[11,12].

针对上述问题,本文从信息论角度证明,在有限字符输入系统中,多天线窃听者的信道互信息可以逼近系统的信道容量[8~10],致使系统的保密互信息趋于零.因此,在人工噪声方法中,保密信号与窃听者的无噪(观测噪声)接收信号之间可以等效为离散有噪无损信道(Di-

收稿日期:2013-11-17;修回日期:2014-07-10;责任编辑:蓝红杰
基金项目:国家自然科学基金(No.61171108)

screte Noisy Lossless Channel, DNLC)[13,14],该特点与高斯输入系统存在本质区别.从几何角度来看,窃听者的无噪接收信号位于不同的(超)平面上[15],而这些(超)平面与有限字符集的符号之间存在对应关系,致使保密信号有规律可循.而窃听者利用保密信号和空域干扰的分布规律差异,能以较小误码率甚至无损地恢复保密信号[5].反之,破坏窃听者的 DNLC 结构成为保证有限字符输入系统物理层安全传输的一个充分条件.

在此指导下,本文提出隐藏有限字符特性的跳空安全传输方法.该方法建立数字调制信号与合法用户天线索引之间的映射关系[16,17],将保密信号的内容实时映射为跳空图样,避免了跳空图样的分发.在信号传输时,系统快速切换 MIMO 系统的收发天线,根据跳空图样向指定的接收天线发送保密信号,并往该天线对应信道的零空间发送空域干扰.因此,该方法可以扩展信号的空间谱[18],隐藏保密信号的有限字符特性并破坏窃听者的 DNLC 结构,从而保证系统的安全性.最后,基于信息论,本文分别从二阶统计量和高阶统计量的角度论证该方法的安全性.

2　问题描述

2.1　系统模型

考虑有限字符输入的多输入多输出多天线窃听者(Multiple Input Multiple Output Multiple-antenna Eavesdropper, MIMOME)系统,发送方(Alice)、合法用户(Bob)和窃听者(Eve)配备的天线数分别为 $N_a>1$、$N_b\geq 1$ 和 $N_e>1$.当 $N_b=1$ 时,系统退化为多输入单输出多天线窃听者(Multiple Input Single Output Multiple-antenna Eavesdropper, MISOME)系统.Eve 仅被动接收,不发送信号.假设无线信道为富散射信道,且分块衰落,即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.将 Alice 到 Bob 的合法信道和 Alice 到 Eve 的窃听信道分别表示为 $N_b\times N_a$ 的矩阵 $\boldsymbol{H}_b=[h_{b,ij}]$ 和 $N_e\times N_a$ 的矩阵 $\boldsymbol{H}_e=[h_{e,ij}]$.

假设 $N_a\geq N_b$,系统发送多流的保密信号 $s(n)\in\mathbb{R}^{N_b\times 1}$,Bob 和 Eve 的接收信号分别为

$$\boldsymbol{y}_b(n)=\boldsymbol{H}_b\boldsymbol{P}\boldsymbol{s}(n)+\boldsymbol{v}_b(n) \tag{1}$$

$$\boldsymbol{y}_e(n)=\boldsymbol{H}_e\boldsymbol{P}\boldsymbol{s}(n)+\boldsymbol{v}_e(n) \tag{2}$$

其中,预编码矩阵 $\boldsymbol{P}\in\mathbb{R}^{N_a\times N_b}$;信号向量 $\boldsymbol{s}(n)=[s_1(n),s_2(n),\cdots,s_{N_b}(n)]^{\mathrm{T}}$,$s_j(n)\in\mathcal{S}$,表示第 j 个数据流的符号,各符号间相互独立;有限字符集定义为 $\mathcal{S}=\{s_1,s_2,\cdots,s_M\}$;Bob 的观测噪声 $\boldsymbol{v}_b\in\mathbb{R}^{N_b\times 1}$,服从复高斯分布 $\mathcal{CN}(0,\sigma_b^2\boldsymbol{I}_{N_b})$,Eve 的观测噪声 $\boldsymbol{v}_e\in\mathbb{R}^{N_e\times 1}$,服从 $\mathcal{CN}(0,\sigma_e^2\boldsymbol{I}_{N_e})$;令 $\boldsymbol{x}_b(n)=\boldsymbol{H}_b\boldsymbol{P}\boldsymbol{s}(n)$ 表示 Bob 的无噪接收信号.

假设所有信道参数对 Bob 和 Eve 均公开,得到 Alice-Bob 和 Alice-Eve 的条件平均互信息[7]为

$$\mathcal{I}(\boldsymbol{s};\boldsymbol{y}_b\mid\boldsymbol{H}_b)=N_b\log_2 M-\frac{1}{M^{N_b}}\sum_{m=1}^{M^{N_b}}\mathbb{E}_{\boldsymbol{v}_b}\left[\log_2\sum_{k=1}^{M^{N_b}}\exp\left(-\frac{\|\boldsymbol{H}_b\boldsymbol{P}\boldsymbol{e}_{mk}+\boldsymbol{v}_b\|^2-\|\boldsymbol{v}_b\|^2}{\sigma_b^2}\right)\right] \tag{3}$$

$$\mathcal{I}(\boldsymbol{s};\boldsymbol{y}_e\mid\boldsymbol{H}_e)=N_b\log_2 M-\frac{1}{M^{N_b}}\sum_{m=1}^{M^{N_b}}\mathbb{E}_{\boldsymbol{v}_e}\left[\log_2\sum_{k=1}^{M^{N_b}}\exp\left(-\frac{\|\boldsymbol{H}_e\boldsymbol{P}\boldsymbol{e}_{mk}+\boldsymbol{v}_e\|^2-\|\boldsymbol{v}_e\|^2}{\sigma_e^2}\right)\right] \tag{4}$$

式中省略了信号的时间标识;$\mathbb{E}$表示数学期望;信号向量 $\boldsymbol{s}_m$ 的各个元素属于 $\mathcal{S}$ 且相互独立,信号向量差 $\boldsymbol{e}_{mk}=\boldsymbol{s}_m-\boldsymbol{s}_k$.进一步得到 Alice-Bob 和 Alice-Eve 的统计平均互信息分别为 $\mathcal{I}(\boldsymbol{s};\boldsymbol{y}_b)=\mathbb{E}_{\boldsymbol{H}_b}[\mathcal{I}(\boldsymbol{s};\boldsymbol{y}_b\mid\boldsymbol{H}_b)]$ 和 $\mathcal{I}(\boldsymbol{s};\boldsymbol{y}_e)=\mathbb{E}_{\boldsymbol{H}_e}[\mathcal{I}(\boldsymbol{s};\boldsymbol{y}_e\mid\boldsymbol{H}_e)]$.在广播信道下,定义上述 MIMOME 系统的保密互信息[11,12]为

$$C_s=[\mathcal{I}(\boldsymbol{s};\boldsymbol{y}_b)-\mathcal{I}(\boldsymbol{s};\boldsymbol{y}_e)]^+ \tag{5}$$

其中,$[x]^+=\max(0,x)$.

对 $\boldsymbol{H}_b$ 进行奇异值分解,得到

$$\boldsymbol{H}_b=\boldsymbol{U}_{\boldsymbol{H}_b}[\boldsymbol{\Sigma}_{\boldsymbol{H}_b}\ \boldsymbol{O}]\boldsymbol{V}_{\boldsymbol{H}_b}^{\mathrm{H}}=\boldsymbol{U}_{\boldsymbol{H}_b}[\boldsymbol{\Sigma}_{\boldsymbol{H}_b}\ \boldsymbol{O}][\boldsymbol{V}_1\ \boldsymbol{V}_2]^{\mathrm{H}} \tag{6}$$

令 $\boldsymbol{H}_b^{\perp}=\boldsymbol{V}_2^{\mathrm{H}}$ 表示 $\boldsymbol{H}_b$ 的零空间,$\boldsymbol{H}_b^{\perp}\in\mathbb{E}^{(N_a-N_b)\times N_a}$.最大化互信息的线性预编码矩阵[7]为 $\boldsymbol{P}=\boldsymbol{V}_1\boldsymbol{\Sigma}_P\boldsymbol{V}_P^H$,$P\in\mathbb{C}^{N_a\times N_b}$,且 $\boldsymbol{H}_b^{\perp}\boldsymbol{P}=\boldsymbol{O}$.其中,对角阵 $\boldsymbol{\Sigma}_P$ 和酉矩阵 $\boldsymbol{V}_P^{\mathrm{H}}$ 分别对输入信号进行功率分配和酉变换.

由于线性预编码的作用,Bob 接收天线上的信号能量比 Eve 的更加集中,但是 Eve 可能会配备更多的天线.为了综合比较两者的接收效果,假设所有信道增益系数都是标准复高斯随机变量,即 $h_{b,ij}\sim\mathcal{CN}(0,1)$,且 $h_{e,ij}\sim\mathcal{CN}(0,1)$.当 $N_b=1$ 时,存在引理 1[15];当 $N_b>1$ 时,存在定理 1(证明见附录).

引理 1　对于 MISOME 系统,假设 Alice 采用波束形成技术发送信号,且 Bob 和 Eve 的噪声功率一致,即 $\sigma_b^2=\sigma_e^2$.在互信息未饱和前,系统的保密互信息由天线数 N_e 和 N_a 决定:

$$\begin{cases}C_s>0, & \text{若 } N_e<N_a\\ C_s=0, & \text{若 } N_e\geq N_a\end{cases} \tag{7}$$

定理 1　对于 MIMOME 系统,假设 Alice 采用预编码矩阵 $\boldsymbol{P}=\boldsymbol{V}_1\boldsymbol{\Sigma}_P\boldsymbol{V}_P^{\mathrm{H}}$ 发送信号,且 Bob 和 Eve 的噪声功率一致,即 $\sigma_b^2=\sigma_e^2$.在互信息未饱和前,Eve 将天线数至多增加到 $N_e=N_aN_b$ 即可使 $C_s=0$.

因此,在有限字符输入系统中,当 Eve 与 Bob 的子信道质量相当时,即使 Bob 采用了预编码技术,只要 Eve 配备了足够多的天线,其接收效果理论上可以达到甚至超越 Bob,致使系统的保密互信息为 0.

2.2 离散有噪无损信道及其几何意义

在 $N_a > N_b$ 的 MIMO 系统中,人工噪声方法通过发送高斯分布的空域干扰实现安全传输.假设 Alice 精确已知合法信道信息,其发送信号为 $\boldsymbol{Ps}(n) + \boldsymbol{H}_b^{\perp}\boldsymbol{u}(n)$.其中,$\boldsymbol{H}_b^{\perp}\boldsymbol{u}(n)$表示空域干扰,$\boldsymbol{u}(n) \sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{I}_{N_a - N_b})$.此时,Bob 的接收信号不变,Eve 的接收信号变为

$$\boldsymbol{y}_e(n) = \boldsymbol{H}_e\boldsymbol{Ps}(n) + \boldsymbol{H}_e\boldsymbol{H}_b^{\perp}\boldsymbol{u}(n) + \boldsymbol{v}_e(n) \tag{8}$$

其中,令 $\boldsymbol{x}_e(n) = \boldsymbol{H}_e\boldsymbol{Ps}(n) + \boldsymbol{H}_e\boldsymbol{H}_b^{\perp}\boldsymbol{u}(n)$表示 Eve 的无噪接收信号.将 Bob 和 Eve 的信号接收过程分别表示为 Markov 链

$$\boldsymbol{s}(n) \leftrightarrow \boldsymbol{x}_b(n) \rightarrow \boldsymbol{y}_b(n) \tag{9}$$

$$\boldsymbol{s}(n) \rightarrow \boldsymbol{x}_e(n) \rightarrow \boldsymbol{y}_e(n) \tag{10}$$

其中,$\boldsymbol{s}(n) \leftrightarrow \boldsymbol{x}_b(n)$表示 $\boldsymbol{s}(n)$可从 $\boldsymbol{x}_b(n)$中无损恢复.

引入 DNLC 的定义:信道的一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[13].在上述系统中,对于保密信号 $\boldsymbol{s}_m$ 而言,由于 $\boldsymbol{H}_b^{\perp}\boldsymbol{P} = \boldsymbol{O}$ 且 $\boldsymbol{u}(n)$随机快变,$\boldsymbol{x}_e(n) = \boldsymbol{H}_e[\boldsymbol{Ps}_m + \boldsymbol{H}_b^{\perp}\boldsymbol{u}(n)]$在不同时刻 n 有不同值,并且不同 $\boldsymbol{s}_m$ 对应的输出值不重合,符合 DNLC 的定义.因此 $\boldsymbol{s}(n) \rightarrow \boldsymbol{x}_e(n)$间可以等效为一个 DNLC,存在 $\boldsymbol{s}(n) \leftrightarrow \boldsymbol{x}_e(n)$.

实际上,系统也需要让合法信道逼近 DNLC,才能从有噪接收信号 $\boldsymbol{y}_b(n)$中无损地或以较小误码率恢复保密信号 $\boldsymbol{s}(n)$.考虑到 $\mathcal{I}(\boldsymbol{s};\boldsymbol{y}_b) = H(\boldsymbol{s}) - H(\boldsymbol{s}|\boldsymbol{y}_b)$,系统为了让合法信道逼近 DNLC,要求 $H(\boldsymbol{s}|\boldsymbol{y}_b) \rightarrow 0$,意味着 Bob 接收信号的 SNR 较高.当窃听信道质量与合法信道质量相当时,可以认为 Eve 接收信号的 SNR 也较高,此时 $H(\boldsymbol{s}|\boldsymbol{y}_e) \rightarrow 0$ 且 $\mathcal{I}(\boldsymbol{s};\boldsymbol{y}_e) \rightarrow H(\boldsymbol{s})$.因此,根据定理 1 可知,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.

从几何角度分析 DNLC 可知,Eve 的无噪接收信号 $\boldsymbol{x}_e(n)$分布在有限的(超)平面[14]上.不同的(超)平面对应不同的保密信号 $\boldsymbol{s}_m$,这些(超)平面的法线是 $\frac{\boldsymbol{H}_e^{\dagger}\boldsymbol{h}_b}{\|\boldsymbol{H}_e^{\dagger}\boldsymbol{h}_b\|}$.如图 1 所示,选择单流的 MISOME 系统进行仿真验证.令 $N_a = N_e = 3$, $N_b = 1$;限定各信道增益系数和空域干扰为标准实高斯随机变量;输入信号调制类型为二进制相移键控(Binary Phase Shift Keying, BPSK),其字符集为$\{\pm 1\}$.

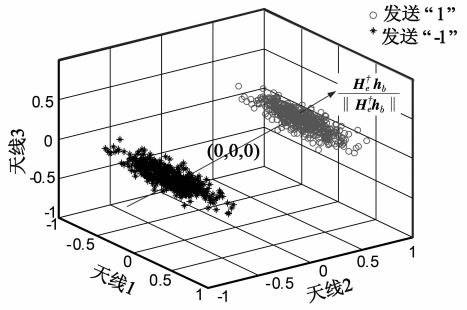

图1 Eve的无噪接收信号

在图 1 中,BPSK 信号的两个星座点分别对应两个不同的平面.当天线数 N_a, N_e 增加,数据流增多或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.对于分块衰落的信道,在一个数据帧内信道是准静态的,Eve 接收信号所在(超)平面的位置是固定的,信号的数字特征也是稳定的.因此,当一个数据帧内有足够的符号数时,Eve 可以统计出接收信号的数字特征,根据接收信号所处(超)平面判断出保密信号,因此 Eve 即使未知 $\boldsymbol{H}_b$ 也可以实现窃密.

对于多流发送信号,很难用几何方法直观反映出 Eve 无噪接收信道的 DNLC 结构,但是利用 MUSIC-like 窃密算法[5]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.

上述分析表明,人工噪声方法中的 Eve 具有 DNLC 结构,其接收信号表现出稳定的数字和几何特征,为窃听者提供攻击条件.因此,可以得到一个保证有限字符输入系统物理层安全的充分条件:破坏窃听者的 DNLC 结构.与保密互信息相比,该条件为无线数字通信系统提供了一个更为简捷的安全设计准则.

3 跳空安全传输系统

为破坏 Eve 的 DNLC 结构,本节结合有限字符特性和跳空通信技术提出一种新的安全方法:隐藏有限字符特性的跳空安全传输方法.

3.1 跳空安全传输系统模型

现有的跳空安全传输方法可以破坏窃听者的 DNLC 结构,但是需要预先分发跳空图样[18].隐藏有限字符特性的跳空安全传输方法可以避免跳空图样的预先分发,其单流的传输模型如图 2 所示,多流的情况可以进行类似扩展.

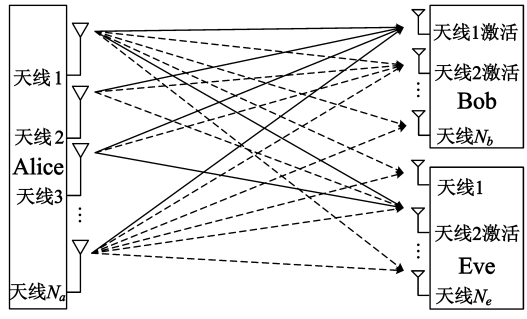

图2 跳空物理层安全传输模型

在图 2 中,Alice 同时发送保密信号和空域干扰,所经信道分别用实线和虚线表示.在某一时刻,Alice 根据跳空图样,向指定的 Bob 天线(如索引为 1 的天线,简记

为天线 1)对保密信号进行波束形成,向该天线对应信道的零空间发送空域干扰.此时,保密信号的能量将激活该天线,而空域干扰的能量则可能激活 Bob 的其余天线,如天线 2.由于无线信道特征的多样性和独特性,一般情况下 $\boldsymbol{H}_e$ 与 $\boldsymbol{H}_b$ 不同,在保密信号和空域干扰的共同作用下,Eve 可能被激活了某根天线,如 Eve 的天线 2,也可能被激活了 0 根或多根天线.

该模型的关键问题在于如何生成不用预先分发的跳空图样,并且保证 Bob 从多根可能被激活的天线中正确检测出指定天线.对此,所提方法建立数字调制信号与 Bob 接收天线索引之间的映射关系,将所传输的保密信号内容作为跳空图样,保证 Bob 正确选择接收天线进行解调.具体的系统传输方案如图 3 所示.

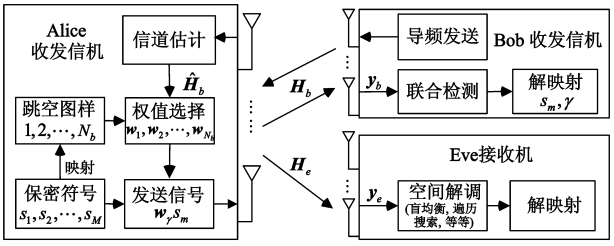

图3　跳空物理层安全传输方案图

首先,建立数字调制信号和 Bob 接收天线索引之间的映射关系.定义跳空图样集 $\Gamma=\{1,2,\cdots,N_b\}$,$\Gamma$ 同时也是 Bob 的接收天线索引集.考虑到接收天线数有限,可以假设 $N_b\leqslant M$.在映射过程中,Alice 将 $\log_2 M$ 比特的符号 $s_m(s_m\in S)$映射为$\log_2 N_b$ 比特的跳空图样 $\gamma(\gamma\in\Gamma)$.当 $N_b=M$ 时,s_m 与 γ 一一对应,即 $\gamma=m$.当 $N_b<M$ 时,s_m 下标 m 的模运算$\mathrm{mod}_{N_b}(m)$和 γ 对应,即 $\gamma=\mathrm{mod}_{N_b}(m)$,其中,$\mathrm{mod}_{N_b}(\cdot)$表示模 N_b 运算.此时,将出现多个符号对应同一天线索引的情况.表 1 所示为正交相移键控(Quadrature Phase Shift Keying,QPSK)符号 $s_m=\mathrm{e}^{\mathrm{j}\pi(2m-1)/4}$与跳空图样 γ 之间的映射关系:$\gamma=\mathrm{mod}_{N_b}(m)$,$N_b\leqslant 4$.

表 1　跳空安全传输的映射关系

序号 m	QPSK 符号	跳空图样 γ
1	$\mathrm{e}^{\mathrm{j}\frac{\pi}{4}}$	$\mathrm{mod}_{N_b}(1)$
2	$\mathrm{e}^{\mathrm{j}\frac{3\pi}{4}}$	$\mathrm{mod}_{N_b}(2)$
3	$\mathrm{e}^{\mathrm{j}\frac{5\pi}{4}}$	$\mathrm{mod}_{N_b}(3)$
4	$\mathrm{e}^{\mathrm{j}\frac{7\pi}{4}}$	$\mathrm{mod}_{N_b}(4)$

在上述映射关系下,Alice 对 Bob 的信息传输过程为:

(1)初始传输时刻时,跳空图样默认为 1.Alice 往 Bob 的天线 1 方向发送保密符号,往该天线对应信道的零空间发送空域干扰,并把该符号映射为新的跳空图样.对称地,Bob 选择天线 1 进行解调,并将解调出的符号映射为新的跳空图样.

(2)此后每次传输时,Alice 根据更新后的跳空图样,往 Bob 的指定接收天线方向发送保密符号,往该天线对应信道的零空间发送空域干扰,并把该保密符号映射为新的跳空图样.对称地,Bob 根据跳空图样,解调出指定接收天线上的保密符号,并把该符号映射为新的跳空图样.

图 4 所示为跳空图样的一个生成时序示例.其中,假设 Alice 发送 QPSK 信号,且 Bob 有 4 根接收天线.在时刻 1(初始时刻),跳空图样 γ 默认为 1,Alice 对 Bob 的天线 1 方向发送保密符号 $\mathrm{e}^{\mathrm{j}5\pi/4}$,对该天线对应信道的零空间发送空域干扰;相应地,Bob 对天线 1 上的信号进行解调.假设 Bob 解调正确得到符号 $\mathrm{e}^{\mathrm{j}5\pi/4}$,根据表 1 的映射关系,得到时刻 2 的跳空图样 $\gamma=3$.因此,在传输时刻 2,Alice 往 Bob 的天线 3 方向发送保密信号,往该天线对应信道的零空间发送空域干扰;相应地,Bob 对天线 3 上的信号进行解调.在传输时刻 3,4,…,依次进行类推.实际上,Bob 可以对实时接收的信号进行离线分析,也能解调出信号.

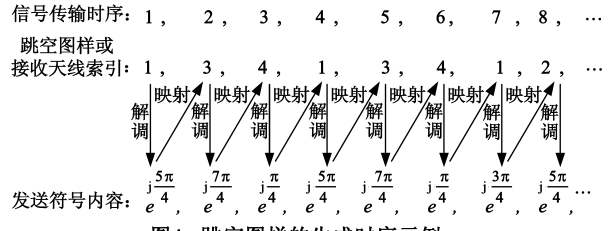

图4　跳空图样的生成时序示例

在传输过程中,Alice 根据跳空图样 γ,往 Bob 的天线 γ 方向 $\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma$ 发送信号 $\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma s(n)/\|\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma\|$,并往其零空间$(\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma)^{\perp}$发送空域干扰 $\boldsymbol{u}(n)$.Bob 的接收信号为

$$\boldsymbol{y}_b(n)=\boldsymbol{H}_b\frac{\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma}{\|\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma\|}\boldsymbol{s}(n)+\boldsymbol{H}_b(\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma)^{\perp}\boldsymbol{u}(n)+\boldsymbol{v}_b(n)\tag{11}$$

Eve 的接收信号为

$$\boldsymbol{y}_e(n)=\boldsymbol{H}_e\frac{\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma}{\|\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma\|}s(n)+\boldsymbol{H}_e(\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma)^{\perp}\boldsymbol{u}(n)+\boldsymbol{v}_e(n)\tag{12}$$

由式(11)和(12)可见,Bob 和 Eve 的接收信号中同时包含了保密信号和空域干扰.由于两者的分布规律不同,在未知跳空图样时,保密信号的有限字符特性将被有效隐藏,从而达到抑制窃听的目标.

由于 Alice 对 Bob 的指定接收天线进行波束形成,正常情况下 Bob 可以获得正确的接收天线索引 γ,其接收信号可重写为

$$y_b(n)=\boldsymbol{e}_\gamma^{\mathrm{H}}\boldsymbol{H}_b\frac{\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma}{\|\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma\|}s(n)+\boldsymbol{e}_\gamma^{\mathrm{H}}\boldsymbol{v}_b(n)$$
$$=\|\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma\|s(n)+v_b(n) \quad (13)$$

其中，$v_b(n)=\boldsymbol{e}_\gamma^{\mathrm{H}}\boldsymbol{v}_b(n)$，服从 $\mathcal{CN}(0,\sigma_b^2)$，式(13)保证了 Bob 的正常接收. 定义预处理向量

$$\boldsymbol{w}_\gamma(n)=\frac{\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma}{\|\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma\|}+(\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma)^{\perp}\boldsymbol{u}(n) \quad (14)$$

式(13)可简写为

$$y_b(n)=\boldsymbol{e}_\gamma^{\mathrm{H}}\boldsymbol{H}_b\boldsymbol{w}_\gamma s(n)+v_b(n) \quad (15)$$

3.2 跳空安全传输系统的接收性能

设置系统发送功率为 P，功率分配因子为 α，表示 Alice 分配 αP 功率用于发送信号 $s(n)$. 考虑到功率约束 $\mathbb{E}[\mathrm{Tr}(\boldsymbol{w}_\gamma(n)\boldsymbol{w}_\gamma^{\mathrm{H}}(n))]\leqslant P$，将发送信号重写为 $\sqrt{\alpha P}\frac{\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma}{\|\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma\|}+\sqrt{\frac{(1-\alpha)P}{N_a-1}}(\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma)^{\perp}\boldsymbol{u}(n)$. 其中，$\mathrm{Tr}(\cdot)$ 表示矩阵迹. 为了便于 Bob 解调，不失一般性，令 $\|\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma\|=1$，$\sqrt{\alpha P}=c$，则 Bob 的接收信号变为

$$y_b(n)=cs(n)+v_b(n) \quad (16)$$

考虑到跳空安全传输的累积误差，系统每传输 L 次重新进行初始化，将跳空图样默认为 $\gamma=1$，并且初始化前后的传输过程是相互独立的. Bob 采用最大似然(Maximum Likelihood，ML)准则解调信号. 当输入是 BPSK 和 QPSK 信号时，根据式(16)得到单个符号传输的误码率分别为

$$p_B=\frac{1}{2}\mathrm{erfc}\left(\frac{c}{\sigma_b}\right) \quad (17)$$

$$p_Q=1-\left[1-\frac{1}{2}\mathrm{erfc}\left(\frac{c}{\sqrt{2}\sigma}\right)\right]^2 \quad (18)$$

其中，$\mathrm{erfc}(x)=\frac{2}{\sqrt{\pi}}\int_x^\infty e^{-u^2}\mathrm{d}u$.

对于 BPSK 和 QPSK 输入，初始化后的首次传输误码率为 $p_1=p_B$ 或 p_Q，第 l 次传输的误码率分别为

$$p_l=(1-p_{l-1})p_B+p_{l-1}\frac{1}{2},1<l\leqslant L \quad (19)$$

$$p_l=(1-p_{l-1})p_Q+p_{l-1}\frac{3}{4},1<l\leqslant L \quad (20)$$

单个初始化间隔 L 内的平均误码率为

$$\bar{p}_e=\frac{1}{L}\sum_{l=1}^{L}p_l \quad (21)$$

由于每次初始化前后的传输过程相互独立，可以认为平均误码率 $\bar{p}_e$ 也是系统的整体误码率. 特别地，当 p_e 固定时，减小初始化间隔 L 可以减小累积误差，进而降低系统的整体误码率.

Eve 也采用 ML 准则解调信号，但是由于 Eve 的接收过程比较复杂，这里不再计算其误码率的理论值，后文通过仿真给出其误码率的估计值.

4 跳空物理层安全传输系统的安全性分析

本节推导出有限字符输入下跳空物理层安全传输系统的保密互信息，并说明该系统可以获取正的保密互信息，论证所提跳空传输方法的安全性.

4.1 跳空安全传输系统的保密互信息

根据式(16)得到 y_b 的条件分布概率与其分布概率分别为

$$p(y_b\mid s=s_m)=\frac{1}{\pi\sigma_b^2}\exp\left(-\frac{|y_b-cs_m|^2}{\sigma_b^2}\right) \quad (22)$$

$$p(y_b)=\frac{1}{M}\sum_{m=1}^{M}\frac{1}{\pi\sigma_b^2}\exp\left(-\frac{|y_b-cs_m|^2}{\sigma_b^2}\right) \quad (23)$$

式中省略了时间标识. 根据互信息定义，推导出 Alice-Bob 的平均互信息为

$$\mathcal{I}(s;y_b)=\log_2 M-\frac{1}{M}\sum_{m=1}^{M}\mathbb{E}_{v_b}\left[\log_2\sum_{k=1}^{M}\exp\left(-\frac{|ce_{mk}+v_b|^2-|v_b|^2}{\sigma_b^2}\right)\right] \quad (24)$$

其中，$e_{mk}=s_m-s_k$. 当 SNR 较高时，$\mathcal{I}(s;y_b)$ 趋于上限 $\log_2 M$bit/s/Hz.

先考虑最不利的情况，即 Eve 的空域干扰为 0. 此时 $\boldsymbol{y}_e=\boldsymbol{H}_e\boldsymbol{w}_\gamma s_m+\boldsymbol{v}_e$，得到 Alice-Eve 的统计平均互信息 $\mathcal{I}(s,\Gamma;\boldsymbol{y}_e)$ 为

$$\mathcal{I}(s,\Gamma;\boldsymbol{y}_e)=\log_2 N_b M-\frac{1}{N_b M}\sum_{\gamma=1}^{N_b}\sum_{m=1}^{M}\mathbb{E}_{\boldsymbol{v}_e}\left[\log_2\sum_{\gamma_2=1}^{N_b}\sum_{m_2=1}^{M}\exp\left(-\frac{\|d+\boldsymbol{v}_e\|^2-\|\boldsymbol{v}_e\|^2}{\sigma_e^2}\right)\right] \quad (25)$$

其中，$d=\boldsymbol{H}_e\boldsymbol{w}_\gamma s_m-\boldsymbol{H}_e\boldsymbol{w}_{\gamma_2}s_{m_2}$，$\mathcal{I}(s,\Gamma;\boldsymbol{y}_e)$ 将跳空图样作为互信息的一部分进行了重复统计. 去除重复统计的部分，$\mathcal{I}(s,\Gamma;\boldsymbol{y}_e)$ 的上限为 $\log_2 M$bit/s/Hz.

在广播信道下，定义跳空安全传输系统的保密互信息[11,12]为

$$C_s=[\mathcal{I}(s;y_b)-\mathcal{I}(s,\Gamma;\boldsymbol{y}_e)]^+ \quad (26)$$

由于 Alice 掌握信息发送的主动权并且能够获取信道的估计值 $\hat{\boldsymbol{H}}_b$，式(26)中 $\mathcal{I}(s;y_b)$ 容易趋近上限，因此最大化保密互信息的关键在于减少 $\mathcal{I}(s,\Gamma;\boldsymbol{y}_e)$.

4.2 跳空安全传输系统安全性分析

跳空安全传输方法通过随机化 Eve 的等效接收信道，恶化了 Eve 的信号接收效果，致使 Eve 不能正确检测天线和解调信号. 当 Eve 错误检测所有天线时，将把检测得到的不同 $\boldsymbol{w}_\gamma$ 等效视为同一天线增益，即 $\boldsymbol{w}_\gamma=\boldsymbol{w}_{\gamma_2}$. 当 Eve 错误判断所有符号时，将把解调得到的不同 s_m 等效视为同一符号，即 $s_m=s_{m_2}$. 将 $\boldsymbol{w}_\gamma=\boldsymbol{w}_{\gamma_2}$ 和 $s_m=s_{m_2}$ 代入式(25)，得到 Alice-Eve 的平均互信息 $\mathcal{I}(s,\Gamma;\boldsymbol{y}_e)=0$. 根据式(26)可知系统可以获得正的保密互信息，当 SNR 较高时，系统的保密

互信息趋于上限$\log_2 M$bit/s/Hz.下面分别从二阶统计量和高阶统计量的角度,说明跳空安全传输方法下 Eve 无法得到稳定的统计量,不能正确检测天线和解调信号,从而实现或逼近上述两个等式,保证了系统的安全性.

(1)Eve 无法通过二阶统计量实现窃密.

跳空安全传输系统通过随机切换 MIMO 收发天线,并对 Bob 的多个接收天线同时发送保密信号和空域干扰,掩藏了信号的有限字符特性.由于 Eve 无法获得跳空图样,其接收信号没有稳定的数字特征.从几何角度来看,Eve 的无噪接收信号不服从(超)平面分布.因此,Eve 的无噪接收信道不满足 DNLC 结构特点.对于利用符号遍历的二阶统计量方法,如 MUSIC-like 窃密算法而言,由于无法利用信号的有限字符特性,无法窃密.对于非符号遍历的二阶统计量方法而言,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,并且比 MUSIC-like 算法所需符号更多,但是跳空安全传输系统的信道在不断切换,窃听者无法获取准确的二阶统计量,无法窃密.

(2)Eve 无法通过高阶统计量实现窃密.

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 $G\in\mathbb{E}^{N_b\times N_e}$以实现

$$\boldsymbol{G}\boldsymbol{y}_e=\boldsymbol{G}(\boldsymbol{H}_e\boldsymbol{w}_\gamma s_m+\boldsymbol{v}_e)=\boldsymbol{e}_\gamma s_m+\boldsymbol{G}\boldsymbol{v}_e \tag{27}$$

从而等效接收到和 Bob 相同的信号,恢复跳空图样和保密符号.(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).即使空域干扰为 0 时,由于 Eve 的等效接收信道在不断切换,其接收信号不具备稳定的高阶统计特征,仍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.

5　数据仿真结果

对跳空安全传输方法进行仿真分析,验证方法的安全性.下面的仿真图中,每个平均误码率点对应10^6个接收符号的仿真结果平均值,每个平均互信息点对应10^3次 Monte Carlo 仿真结果的平均值.仿真中随机生成 Alice-Bob 和 Alice-Eve 的信道矩阵 $\boldsymbol{H}_b$ 和 $\boldsymbol{H}_e$,矩阵中各元素相互独立且服从 $\mathcal{CN}(0,1)$.为了便于计算平均误码率的理论值,调整矩阵系数使得 $\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma=\sqrt{N_b}\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma/\|\boldsymbol{H}_b^{\mathrm{H}}\boldsymbol{e}_\gamma\|$,$1\leqslant\gamma\leqslant N_b$.

图 5 所示为跳空安全传输系统接收信号平均误码率的仿真结果.设定天线数 $N_a=N_b=N_e=4$,输入信号的调制类型为 QPSK.功率分配因子 $\alpha=0.8$ 和 0.5.初始化间隔 $L=10$ 和 100.Bob 和 Eve 均采用 ML 解码方法.由图可见,Eve 的平均误码率始终稳定在一个常数值,约为 0.75,随着 SNR 的提高,Bob 的平均误码率快速下降,比 Eve 的平均误码率低数个量级.

另外,由图 5 仿真结果可知,初始化间隔对接收性能存在一定的影响,但是影响较小.$L=10$ 与 $L=100$ 时接收性能很接近.而功率分配因子对接收性能影响较大,$\alpha=0.8$ 和 $\alpha=0.5$ 时接收性能的差异比较明显.可见,发送空域干扰在实现安全的同时影响到了接收性能,需要合理分配功率.

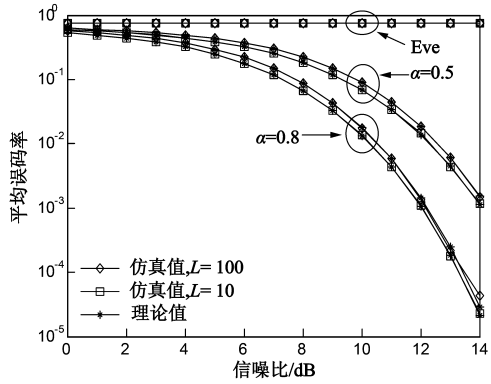

图5　跳空安全传输系统的误码率

图 6 所示为不同传输方法下 MUSIC-like 窃密算法的平均误码率.仿真对象分别是 4 发 2 收的 MIMO 跳空传输系统和采用人工噪声方法的 4 发 1 收 MISO 系统.两个系统的功率分配因子均分别设定为 $\alpha=0.8$ 和 0.5.初始化间隔设定为 $L=10$.考虑到 MUSIC-like 算法的复杂度很高,为便于 Eve 进行窃听,仿真选择信号调制类型为 BPSK.窃听天线数 $N_e=6$.MUSIC-like 算法的累积符号长度 $K=9$.

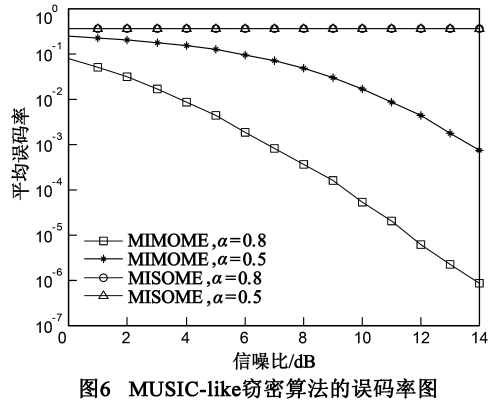

图6　MUSIC-like窃密算法的误码率图

图 6 中,随着 SNR 提高,MISO 人工噪声系统下 MUSIC-like 窃密算法的平均误码率下降很快,表明 MISO 人工噪声系统能被 MUSIC-like 算法窃密,存在安全隐患.但是,MIMO 跳空传输系统中,MUSIC-like 算法的平均误码率在各种 SNR 下均保持较高值,约为 0.25,表明了 MIMO 跳空传输方法的安全性.图 7 所示的是跳空安全传输的保密互信息.仿真选择天线数 $N_a=N_b=N_e=4$,

输入信号为单流的 QPSK,功率分配因子分别为 $\alpha=0.8$ 和 0.5,初始化间隔设定为 $L=10$. 在图 7 中,由于 Eve 无法正确检测天线和解调信号,系统保密互信息随着 SNR 的提高逐渐增大,并趋于上限 $\log_2 M=2$bit/s/Hz. 该仿真结果与图 5 相对应,在图 5 中,跳空传输系统的平均误码率随着 SNR 提高而逐渐降低.

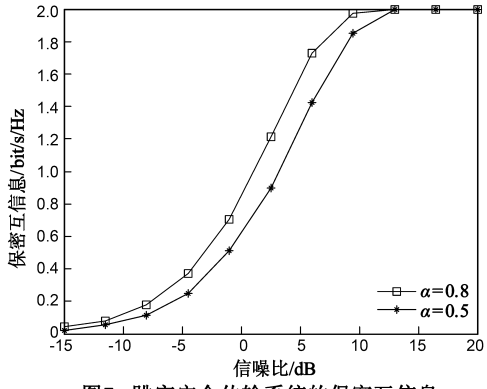

图7 跳空安全传输系统的保密互信息

6 结束语

针对 MIMO 无线数字通信系统,本文推导了一个保证物理层安全传输的充分条件,并结合有限字符特性和跳空传输技术,提出了一种新的物理层安全传输方法. 该方法建立了数字调制信号与合法用户接收天线索引之间的映射关系,以保密信号的内容为跳空图样,利用信号内容的随机性保证跳空图样的安全性. 并且,通过快速切换 MIMO 收发天线和发送空域干扰,随机化了窃听者的等效信道,隐藏了保密信号的有限字符特性,破坏了窃听者的 DNLC 结构,从而保障了信息的安全传输. 理论分析和仿真结果表明,跳空安全传输系统可以获得正的保密互信息,证明了该安全方法的有效性.

附录

定理 1 证明

令 $N_e=N_aN_b$,限定发送功率为 $\mathrm{Tr}(\boldsymbol{\Sigma}_P^2)=1$. 由于酉变换不改变互信息[7],Bob 的接收信号可以重写为

$$\tilde{\boldsymbol{y}}_b(n)=\boldsymbol{\Sigma}_H\boldsymbol{\Sigma}_P\boldsymbol{V}_P^{\mathrm{H}}\boldsymbol{s}(n)+\tilde{\boldsymbol{v}}_b(n) \tag{a1}$$

其中,$\tilde{\boldsymbol{y}}_b(n)=\boldsymbol{U}_H^{\mathrm{H}}\boldsymbol{y}_b(n)$,$\tilde{\boldsymbol{v}}_b(n)=\boldsymbol{U}_H^{\mathrm{H}}\boldsymbol{v}_b(n)$,并令 $\boldsymbol{V}_P^{\mathrm{H}}\boldsymbol{s}(n)=[\upsilon_1(n),\upsilon_2(n),\cdots,\upsilon_{N_b}(n)]^{\mathrm{T}}$. Eve 的接收信号可重写为

$$\boldsymbol{y}_e(n)=\boldsymbol{H}_e\boldsymbol{V}_1\boldsymbol{\Sigma}_P\boldsymbol{V}_P^{\mathrm{H}}\boldsymbol{s}(n)+\boldsymbol{v}_e(n) \tag{a2}$$

将式(a1)和(a2)代入式(3)和(4),得到 Bob 和 Eve 的互信息为

$$\mathcal{I}(\boldsymbol{s};\boldsymbol{y}_b\mid\boldsymbol{H}_b)=N_b\log_2 M-\frac{1}{M^{N_b}}\sum_{m=1}^{M^N}\mathbb{E}_{\tilde{\boldsymbol{v}}_b}\left[\log_2\sum_{k=1}^{M^{N_b}}\exp\left(-\frac{\|\boldsymbol{\Sigma}_{H_b}\boldsymbol{\Sigma}_P\boldsymbol{V}_P^{\mathrm{H}}\boldsymbol{e}_{mk}+\tilde{\boldsymbol{v}}_b\|^2-\|\tilde{\boldsymbol{v}}_b\|^2}{\sigma_b^2}\right)\right] \tag{a3}$$

$$\mathcal{I}(\boldsymbol{s};\boldsymbol{y}_e\mid\boldsymbol{H}_e)=N_b\log_2 M-\frac{1}{M^{N_b}}\sum_{m=1}^{M^{N_b}}\mathbb{E}_{\boldsymbol{v}_e}\left[\log_2\sum_{k=1}^{M^{N_b}}\exp\left(-\frac{\|\boldsymbol{H}_e\boldsymbol{V}_1\boldsymbol{\Sigma}_P\boldsymbol{V}_P^{H}\boldsymbol{e}_{mk}+\boldsymbol{v}_e\|^2-\|\boldsymbol{v}_e\|^2}{\sigma_e^2}\right)\right] \tag{a4}$$

直接计算式(a3)和(a4)复杂很高. 由于 Bob 和 Eve 具有分布相似的输入和观测噪声,可以利用等效的 SNR 统计值来比较两者的互信息.

定义 Bob 和 Eve 的等效 SNR 统计值分别为

$$\mathrm{SNR}_b=\frac{\mathbb{E}_{\boldsymbol{H}}\left\{\mathrm{Tr}\left[\boldsymbol{\Sigma}_H\boldsymbol{\Sigma}_P\boldsymbol{V}_P^{\mathrm{H}}\left(\sum_{m=1}^{M^{N_b}}\sum_{k=1}^{M^{N_b}}\boldsymbol{e}_{mk}\boldsymbol{e}_{mk}^{\mathrm{H}}\right)\boldsymbol{V}_P\boldsymbol{\Sigma}_P\boldsymbol{\Sigma}_{H_b}\right]\right\}}{\sigma_b^2}=\frac{\alpha\,\mathbb{E}_{\boldsymbol{H}}[\mathrm{Tr}(\boldsymbol{\Sigma}_H^2\boldsymbol{\Sigma}_P^2)]}{\sigma_b^2} \tag{a5}$$

$$\mathrm{SNR}_e=\frac{\mathbb{E}_{\boldsymbol{H}_e}\left\{\mathrm{Tr}\left[\boldsymbol{H}_e\boldsymbol{V}_1\boldsymbol{\Sigma}_P\boldsymbol{V}_P^{\mathrm{H}}\left(\sum_{m=1}^{M^{N_b}}\sum_{k=1}^{M^{N_b}}\boldsymbol{e}_{mk}\boldsymbol{e}_{mk}^{\mathrm{H}}\right)\boldsymbol{V}_P\boldsymbol{\Sigma}_P\boldsymbol{V}_1^{\mathrm{H}}\boldsymbol{H}_e^{\mathrm{H}}\right]\right\}}{\sigma_e^2}=\frac{\alpha\,\mathbb{E}_{\boldsymbol{H}_e}\{\mathrm{Tr}[(\boldsymbol{H}_e\boldsymbol{V}_1)^{\mathrm{H}}\boldsymbol{H}_e\boldsymbol{V}_1\boldsymbol{\Sigma}_P^2]\}}{\sigma_e^2} \tag{a6}$$

其中,$\sum_{m=1}^{M^{N_b}}\sum_{k=1}^{M^{N_b}}\boldsymbol{e}_{mk}\boldsymbol{e}_{mk}^{\mathrm{H}}=\alpha\boldsymbol{I}_N$,$\mathbb{E}_{\boldsymbol{H}}[\mathrm{Tr}(\boldsymbol{\Sigma}_{\boldsymbol{H}}^2)]=N_aN_b$,且 $\mathbb{E}_{\boldsymbol{H}_e}\{\mathrm{Tr}[(\boldsymbol{H}_e\boldsymbol{V}_1)^{\mathrm{H}}\boldsymbol{H}_e\boldsymbol{V}_1]\}=N_aN_b^2$. 由于 $\boldsymbol{\Sigma}_{\boldsymbol{H}}$ 的对角元素是按降序排列的,在 $\mathrm{Tr}(\boldsymbol{\Sigma}_{\boldsymbol{P}}^2)=1$ 的功率约束下,$\mathbb{E}[\mathrm{Tr}(\boldsymbol{\Sigma}_{\boldsymbol{H}}^2\boldsymbol{\Sigma}_{\boldsymbol{P}}^2)]\leqslant N_aN_b$. 由于 $\boldsymbol{H}_e\boldsymbol{V}_1$ 在各个方向上的分布规律相同,在 $\mathrm{Tr}(\boldsymbol{\Sigma}_{\boldsymbol{P}}^2)=1$ 的功率约束下,$\mathbb{E}\{\mathrm{Tr}[(\boldsymbol{H}_e\boldsymbol{V}_1)^{\mathrm{H}}\boldsymbol{H}_e\boldsymbol{V}_1]\boldsymbol{\Sigma}_{\boldsymbol{P}}^2\}=N_aN_b$. 将这两个数学期望值以及 $\sigma_b^2=\sigma_e^2$ 代入式(a5)和(a6),得到 $\mathrm{SNR}_b\leqslant\mathrm{SNR}_e$. 因此,在互信息未饱和($\mathcal{I}(s;\boldsymbol{y}_b\mid\boldsymbol{H}_b)<N_b\log_2 M$)前,可以认为 $\mathcal{I}(\boldsymbol{s};\boldsymbol{y}_b)\geq\mathcal{I}(\boldsymbol{s};\boldsymbol{y}_e)$,由式(5)可得 $C_s=0$.

参考文献

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

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

[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,2012,40(7):1289 – 1297.
Luo Wen-yu, Jin Liang, Huang Kai-zhi, et al. A wireless channel encryption method with γ mean square error[J]. Atca Elec-

tronica Sinica,2012,40(7):1289 – 1297.(in Chinese)
[4] 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.
[5] 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 forspatial scrambling based secure wireless communication and its wiretap method[J] Scientia Sinica Information,2012,42(4):483 – 492.(in Chinese)
[6] 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.
[7] Xiao C, Zheng Y R, Ding Z. Globally optimal linear precoders for finite alphabet signals over complex vector Gaussian channels[J]. IEEE Transactions on Signal Processing,2011,59(7):3301 – 3314.
[8] Pérez-Cruz F, Rodrigues M R D, Verdú S. MIMO Gaussian channels with arbitrary inputs: optimal precoding and power allocation[J]. IEEE Transactions on Information Theory, 2010, 56(3):1070 – 1084.
[9] 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.
[10] 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.
[11] Barshar 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.
[12] 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.
[13] 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.
[14] Hansen L K, Xu G. A hyperplane-based algorithm for the digital co-channel communications problem[J]. IEEE Transactions on Information Theory, 1997, 43 (5):1536 – 1548.
[15] 崔波,刘璐,金梁.有限字符输入系统的物理层安全传输条件[J].电子与信息学报,2014,36(6):1441 – 1447.
Cui Bo, Liu Lu, Jin Liang. Physical layer security transmission condition for finite alphabet input system[J]. Journal of Electronics & Information Technology, 2014, 36(6):1441 – 1447.(in Chinese)
[16] Mesleh R, Haas H, Sinanovic S, et al. Spatial modulation[J]. IEEE Transactions on Vehicular Technology, 2008, 57(4):2228 – 2241.
[17] Renzo M Di, Leonardis D De, Graziosi F, et al. Space shift keying (SSK-) MIMO with practical channel estimates[J]. IEEE Transactions on Wireless Communications. 2012, 60(4):998 – 1012.
[18] 殷勤业,贾曙乔,左莎琳,等.分布式多天线跳空收发技术:II[J].西安交通大学学报,2013,47(1):1 – 6.
Yin Qin-ye, Jia Shu-qiao, Zuo Sha-lin, et al. Adistributed multi-antenna space hopping transceiver technique:II[J]. Journal of Xi'an Jiaotong University,2013,47(1):1 – 6.(in Chinese)

作者简介

崔　波　男,1985 年出生,安徽长丰人.国家数字交换系统工程技术研究中心博士,从事物理层安全、盲信号处理等方面的研究.

刘　璐　男,1988 年出生,安徽宿州人.国家数字交换系统工程技术研究中心博士生,从事物理层安全的研究.

李翔宇　男,1987 年出生,河南淮阳人.国家数字交换系统工程技术研究中心博士生,从事物理层安全的研究.

金　梁(通信作者)　男,1969 年出生,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,从事物理层安全、通信信号处理和阵列信号处理等方面的研究.
E-mail:liangjin@263.net