一种多天线信道特征投影物理层安全编码算法

王亚东 黄开枝* 吉 江
(国家数字交换系统工程技术研究中心 郑州 450002)

摘 要：针对现有安全编码设计方法对信道条件依赖性强、收发无法共享随机性等问题，该文提出了一种多天线信道特征投影物理层安全编码算法。在满足信道互易性的时分双工系统中，多天线发射机根据单天线接收机发送的训练符号估计信道得到授权信道特征，利用信道特征投影生成投影矢量对，发射每个符号时随机选择投影矢量作为发射权重矢量，窃听接收机由于还原码字的汉明距离发生随机置乱而无法正确译码，从而实现安全传输。仿真结果表明：该算法使窃听者的误比特率接近 0.5，授权接收机的误比特率较已有多天线物理层安全传输方法低一个数量级。

关键词：物理层安全编码；信道特征投影；汉明距离；发射权重矢量
中图分类号：TN929.53; TN911.22 **文献标识码**： A **文章编号**：1009-5896(2012)07-1653-06
DOI: 10.3724/SP.J.1146.2011.01318

A Physical Layer Secrecy Coding Algorithm Using Multi-antenna Channel Characteristics Projection

Wang Ya-dong Huang Kai-zhi Ji Jiang
(*National Digital Switching System Engineering & Technological Research Center*, *Zhengzhou* 450002, *China*)

Abstract: This paper proposed a physical layer secrecy coding algorithm using multi-antenna channel characteristics projection in consideration of the existing secrecy coding's problems, such as channel condition dependence and random sharing. In channel reciprocal Time-Division-Duplex (TDD) system, multi-antenna transmitter estimates the authorized channel characteristics according to the training symbols transmitted by the single-antenna receiver, and then generates the pair of projected vectors through multi-antenna channel characteristics projection.While transmitting weighted vector is randomly selected from the pair of projected vectors symbol-by-symbol, the Hamming distances of wiretapper's demodulated codewords are radomly confused so that it is hard to decode normally and secure transmission is qualified. Simulation results show that the scheme makes the wiretapper's BER near approximately 0.5 and the authorized receiver's BER a level lower than the existing methods of multi-antenna physical layer secure transmission.

Key words: Physical layer secrecy coding; Channel characteristics projection; Hamming distance; Transmitting weighted vector

1 引言

传统的无线通信系统利用各种加密协议来实现安全保密，其前提假设是密码分析者的计算资源有限，无法在有限时间内算出密钥。随着无线通信网络异构化、泛在化，以及终端处理能力的提升，高层加密协议的实现难度不断加大。因而，利用无线信道的随机性、专有性进行安全传输的物理层安全研究[1,2]近年来方兴未艾，基于多天线结构进行物理层安全研究更是其中的热点之一。

1949年文献[3]首次讨论了安全通信的完美保密条件，即实现编码的一次一密，但加密序列的随机性与信道特征无关，同时收发双方的密钥共享问题也一直困扰着人们。文献[4]提出了窃密信道模型，指出通信中存在保密容量，可以实现无密钥安全传输，并且通过信道编码可以实现保密容量(称可以实现保密容量的信道编码为安全编码)。在后续物理层安全的讨论中，安全编码的寻找一直是研究的热点，但实用的安全编码并没有出现，这是因为：(1)苛刻的信道条件假设，即授权信道的信道质量必须好于窃听者信道，Wyner等人[5]认为这是保密容量存在的前提，这也是安全编码实现面临的最大障碍；(2)编码随机性共享问题：安全编码为了保密传输必须引入编码随机性，而如何在收发双方间共享随机性决定了编码的安全性，这个问题到目前为止还没有很好的解决方案。在多天线物理层安全研究方面，文献[6,7]分别讨论了多天线系统在不同天线配置下私

2011-12-12收到，2012-03-21改回
国家自然科学基金(61171108)资助课题
*通信作者：黄开枝 huangkaizhi@tsinghua.edu.cn

密信道容量。文献[8–11]则讨论了几种实现多天线系统物理层安全传输的方法，这些方法只是从调制域来实现物理层安全，通过信号设计[8,9]、发射权重设计[10]或发射天线选择[11]使得窃听者的信道特征发生随机置乱而无法正确解调。可见，现有的安全编码方法并没有考虑无线信道特征的随机性和专有性，而已有多天线物理层安全传输方法也大都从调制域去实现。

针对以上问题，本文拟从编码和调制结合的角度去实现多天线系统的物理层安全传输，利用多天线系统的信道特征产生满足安全编码要求的加密随机序列，提出了一种多天线信道特征投影物理层安全编码算法。该算法首先证明了当授权信道特征与窃听信道特征保持一定差异时，存在投影矢量对；通过随机选取投影矢量，可以使得授权信道特征与投影矢量对的内积均为正，而窃听信道特征与投影矢量对的内积一正一负。利用这一特性，在满足信道互易性的时分双工MISO(Multiple-Input-Single-Output，多入单出)系统中，多天线发射机根据单天线接收机发送的训练符号估计信道得到授权信道特征，再利用多天线信道特征投影生成投影矢量对；每次发射符号时，随机选取投影矢量作为发射权重矢量；投影矢量选择的随机性确定了安全编码的随机性，可以在保证授权接收方正常接收的同时，随机置乱窃听者解调还原码字的汉明距离，使其无法正确译码，实现物理层安全传输。仿真结果表明：该算法可以使窃听者的误比特率接近0.5，授权接收机的误比特率较已有多天线物理层安全传输方法低了一个数量级。

2 多天线信道特征投影物理层安全编码模型

图 1 给出了多天线物理层安全传输模型，包含授权用户 Alice、Bob 和只听不发的窃听者 Eve; Alice 与 Bob 间的信道称授权信道，Eve 和 Alice 间的信道称窃听信道。本文以 MISO 系统作为模型分析场景，即 Alice 有 J 根天线，$J \geq 2$，Bob 和 Eve 均为 1 根天线。

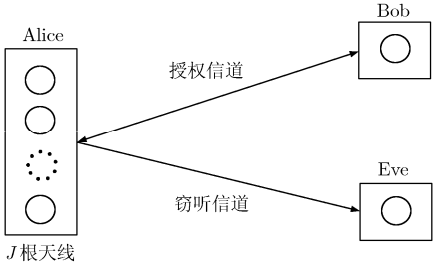

图 1 多天线物理层安全传输模型

如图 1 所示，已有的多天线物理层安全传输方法的通信机制如下：假设系统采用时分双工模式，Bob 先向 Alice 发送未加密的训练符号序列(可以包含通信请求)，Alice 根据接收训练符号序列进行信道估计得到授权信道特征。Alice 每发送一个符号都根据授权信道特征进行信号设计(即添加与授权信道特征正交的人工噪声[8,9])、发射权重设计(随机选择满足授权信道特征约束的发射权重[10])或发射天线的随机选择[11]，从而使 Bob 可以在不做任何特殊处理的情况下正常解调接收，而 Eve 则因为信道特征发生随机置乱而无法正常解调，从而保证了信息的低截获概率。

系统采用阵列波束成形传输，如图 2 所示。发射符号序列 $\{b(n)\}$ 由一组独立同分布的零均值单位方差的均匀分布随机变量组成，天线 i 的发射信号 $s_i(n)=w_i^*(n)b(n)$，$i=1,2,\cdots,J$，其中 $w_i^*(n)$ 表示第 i 根发射天线在发射符号间隔 n 内的发射权重，则发射信号矢量 $\boldsymbol{S}(n)\triangleq[s_1(n),\cdots,s_J(n)]^{\mathrm{T}}=[w_1(n),\cdots,w_J(n)]^{\mathrm{H}}b(n)$，其中 $\boldsymbol{W}(n)=[w_1(n),\cdots,w_J(n)]^{\mathrm{T}}$ 表示发射权重矢量。授权信道的信道特征矢量为 $\boldsymbol{H}_{AB}=[h_{AB,1},h_{AB,2},\cdots,h_{AB,J}]^{\mathrm{T}}$，窃听信道的信道特征矢量为 $\boldsymbol{H}_{AE}=[h_{AE,1},h_{AE,2},\cdots,h_{AE,J}]^{\mathrm{T}}$，其中 $h_{AB,i}$，$h_{AE,i}$ 均为独立同分布的零均值、单位方差的复高斯随机变量。Bob 和 Eve 的接收信号分别为 $y_B(n)$，$y_E(n)$。

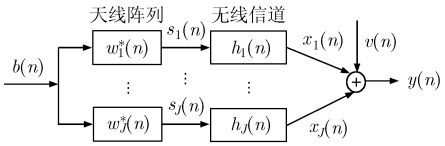

图 2 阵列波束成形传输

$$y_B(n)=\boldsymbol{S}(n)\boldsymbol{H}_{AB}+v_B(n)=\boldsymbol{W}^{\mathrm{H}}(n)\boldsymbol{H}_{AB}b(n)+v_B(n)$$
$$=\sum_{i=1}^{J}w_i^*(n)h_{AB,i}b(n)+v_B(n) \tag{1}$$

$$y_E(n)=\boldsymbol{S}(n)\boldsymbol{H}_{AE}+v_E(n)=\boldsymbol{W}^{\mathrm{H}}(n)\boldsymbol{H}_{AE}b(n)+v_E(n)$$
$$=\sum_{i=1}^{J}w_i^*(n)h_{AE,i}b(n)+v_E(n) \tag{2}$$

其中 v_B，v_E 分别为均值为零、方差为 σ_B^2，σ_E^2 的高斯白噪声。

因为需要进行信道估计，因此本文假设所涉及的信道均为分组衰落信道[6,7]，即信道特征在传输符号分组内保持不变或者慢变，而在传输符号分组间随机变化。因此，各个天线的发射功率就由发射权重决定，接收信噪比由发射权重和噪声方差共同决定。

本文从编码和调制结合的角度来考虑如何实现多天线系统的物理层安全传输。如图 3 所示，Bob 通过授权信道先向 Alice 发送训练序列，Alice 由 TDD 系统的信道互易性得到 $\boldsymbol{H}_{AB}$，再由信道特征投影生成投影矢量对；最后，在每次发射时，随机选择投影矢量，以确保安全编码的随机性。本算法是基于安全编码提出的，为了不失一般性，本文信道编码采用经典的分组码。

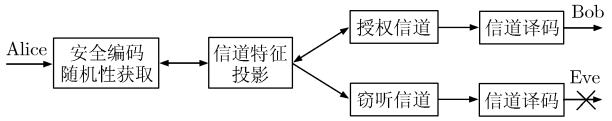

图 3 多天线信道特征投影物理层安全编码模型

信道编码的主要性能指标为纠检错能力，分组码的纠检错能力主要由编码的最小汉明距离决定，当任意两个码字的最小汉明距离为 d 时，分组可以检测到的错误为 $e_{\text{det}}=d-1$，可以纠正的错误为 $e_{\text{cor}}=\lfloor d-1/2\rfloor$，$\lfloor\bullet\rfloor$ 表示向下取整数。信道特征投影可以扰乱窃听者解调还原码字的汉明距离，使其无法正确译码，从而实现安全传输。

3　多天线信道特征投影物理层安全编码算法

可以证明(见附录)：当 $\boldsymbol{H}_{AB}$ 与 $\boldsymbol{H}_{AE}$ 保持一定差异时(即 $\angle(\boldsymbol{H}_{AB},\boldsymbol{H}_{AE})\ge\alpha$ 时，其中 $\angle(\boldsymbol{H}_{AB},\boldsymbol{H}_{AE})$ 表示 $\boldsymbol{H}_{AB}$ 和 $\boldsymbol{H}_{AE}$ 间的差异，α 为参考角)，存在投影矢量对 $(\boldsymbol{W}_1(n),\ \boldsymbol{W}_2(n))$，使得 $\boldsymbol{H}_{AB}$ 与 $(\boldsymbol{W}_1(n),\boldsymbol{W}_2(n))$ 的内积均为正，而 $\boldsymbol{H}_{AE}$ 与 $(\boldsymbol{W}_1(n),\boldsymbol{W}_2(n))$ 的内积一正一负。其中，两个矢量 $\boldsymbol{X}$ 和 $\boldsymbol{Y}$ 的复内积定义为 $\langle\boldsymbol{X},\boldsymbol{Y}\rangle=\boldsymbol{X}^{\mathrm{H}}\boldsymbol{Y}=\sum_{i=1}^{n}x_i^*y_i$。由于 Eve 的位置未知，因此一般无法知道 $\boldsymbol{H}_{AE}$，但由信道的空时频差异可以保证 $\boldsymbol{H}_{AB}$ 和 $\boldsymbol{H}_{AE}$ 存在一定差异[12]，当设定的参考角 α 较小时，可以认为满足 $\angle(\boldsymbol{H}_{AB},\boldsymbol{H}_{AE})\ge\alpha$ 的条件。

多天线信道特征投影物理层安全编码算法的具体实现步骤如下：

(1)Bob 向 Alice 发送训练符号序列，Alice 通过信道估计得到 $\boldsymbol{H}_{AB}$；

(2)设定参考角 α，定义两个归一化参考矢量 $\boldsymbol{H}_1$，$\boldsymbol{H}_2$：

$$\left\|\boldsymbol{H}_1\right\|^2=\sum_{i=1}^{J}h_{1,i}^2=\left\|\boldsymbol{H}_2\right\|^2=\sum_{i=1}^{J}h_{2,i}^2=1 \tag{3}$$

其中 $\|\bullet\|$ 表示求模 2 范数。使 $\boldsymbol{H}_1$，$\boldsymbol{H}_2$ 与 $\boldsymbol{H}_{AB}$ 的夹角都为 α，且参考矢量间夹角为 2α，即

$$\left.\begin{aligned}&\angle(\boldsymbol{H}_1,\boldsymbol{H}_{AB})=\angle(\boldsymbol{H}_2,\boldsymbol{H}_{AB})=\alpha\\&\angle(\boldsymbol{H}_1,\boldsymbol{H}_2)=2\alpha\end{aligned}\right\}$$

$$\rightarrow\left.\begin{aligned}&\boldsymbol{H}_1^{\mathrm{H}}\boldsymbol{H}_{AB}\big/\left\|\boldsymbol{H}_{AB}\right\|=\boldsymbol{H}_2^{\mathrm{H}}\boldsymbol{H}_{AB}\big/\left\|\boldsymbol{H}_{AB}\right\|=\cos\alpha\\&\boldsymbol{H}_1^{\mathrm{H}}\boldsymbol{H}_2=\sum_{i=1}^{J}h_{1,i}^*\cdot h_{2,i}=\cos2\alpha\end{aligned}\right\} \tag{4}$$

联立式(3)和式(4)组成方程组。当发射天线数超过 3 时，该方程组是非线性欠定的，无法求 $\boldsymbol{H}_1$ 和 $\boldsymbol{H}_2$ 的显式解，只能求其数值解；

(3)进一步通过求 $\boldsymbol{H}_{AB}$，$\boldsymbol{H}_1$ 和 $\boldsymbol{H}_2$ 的零空间可以得到投影空间边界 $\boldsymbol{P}_{\text{bound}}^{AB}$，$\boldsymbol{P}_{\text{bound}}^{1}$ 和 $\boldsymbol{P}_{\text{bound}}^{2}$：

$$\left.\begin{aligned}&\text{Null}(\boldsymbol{H}_{AB})=\left\{\boldsymbol{X}\in C^J:\boldsymbol{H}_{AB}\boldsymbol{X}=0\right\}=\boldsymbol{P}_{\text{bound}}^{AB}\\&\text{Null}(\boldsymbol{H}_i)=\left\{\boldsymbol{X}\in C^J:\boldsymbol{H}_i\boldsymbol{X}=0\right\}=\boldsymbol{P}_{\text{bound}}^{i},\ i=1,2\end{aligned}\right\} \tag{5}$$

其中 C^J 表示 J 维复空间；

(4)由 $\boldsymbol{H}_{AB}$，$\boldsymbol{H}_1$ 和 $\boldsymbol{H}_2$ 在投影空间边界 $\boldsymbol{P}_{\text{bound}}^{AB}$，$\boldsymbol{P}_{\text{bound}}^{1}$ 和 $\boldsymbol{P}_{\text{bound}}^{2}$ 上的投影来确定边界投影矢量[13]：

$$\left.\begin{aligned}\boldsymbol{P}_{\boldsymbol{P}_{\text{bound}}^{AB}}^{\boldsymbol{H}_i}&=\sum_{k=1}^{J-1}\left\langle\boldsymbol{H}_i,\boldsymbol{P}_{\text{bound}}^{AB}(:,k)\right\rangle\boldsymbol{P}_{\text{bound}}^{AB}(:,k),\quad i=1,2\\\boldsymbol{P}_{\boldsymbol{P}_{\text{bound}}^{i}}^{\boldsymbol{H}_{AB}}&=\sum_{k=1}^{J-1}\left\langle\boldsymbol{H}_{AB},\boldsymbol{P}_{\text{bound}}^{i}(:,k)\right\rangle\boldsymbol{P}_{\text{bound}}^{i}(:,k),i=1,2\end{aligned}\right\} \tag{6}$$

(5)由边界投影矢量的和矢量确定投影矢量对 $(\boldsymbol{W}_1(n),\boldsymbol{W}_2(n))$：

$$\boldsymbol{W}_1(n)=\boldsymbol{P}_{\boldsymbol{P}_{\text{bound}}^{AB}}^{\boldsymbol{H}_1}+\boldsymbol{P}_{\boldsymbol{P}_{\text{bound}}^{2}}^{\boldsymbol{H}_{AB}},\boldsymbol{W}_2(n)=\boldsymbol{P}_{\boldsymbol{P}_{\text{bound}}^{AB}}^{\boldsymbol{H}_2}+\boldsymbol{P}_{\boldsymbol{P}_{\text{bound}}^{1}}^{\boldsymbol{H}_{AB}} \tag{7}$$

(6)调整参考角 $\alpha'=\alpha/2^k,k\in\{0,1,2,3\}$，重复步骤(2)到步骤(5)；

(7)每次发射符号时按 1/2 的概率选取投影矢量的归一化矢量作为发射权重矢量，即

$$\boldsymbol{W}(n)=\boldsymbol{W}_i(n)\big/\left\|\boldsymbol{W}_i(n)\right\|,p(\boldsymbol{W}_i(n))=1/2,\ i=1,2 \tag{8}$$

由附录定理 1 可知，则 $\boldsymbol{H}_{AB}$ 和 $\boldsymbol{W}_i(n)$ 的内积均为正，而 $\boldsymbol{H}_{AE}$ 和 $\boldsymbol{W}_i(n)$ 的内积则为一正一负。因此，窃听者解调到的码字信息的汉明距离特性因为遭到破坏而无法正确译码。

文献[3]首次讨论了安全通信的完美保密条件，对窃听者来说即实现 $I(z(n);b(n))=0$。采用本算法进行阵列分集传输时，对 Eve 来说，其接收信号为

$$\begin{aligned}y_E(n)&=\boldsymbol{W}^{\mathrm{H}}(n)\boldsymbol{H}_{AE}b(n)+v_E(n)\\&=b(n)\sum_{i=1}^{J}w_i^*(n)h_{AE,i}+v_E(n)\end{aligned} \tag{9}$$

令 $q=\boldsymbol{W}^{\mathrm{H}}(n)\boldsymbol{H}_{AE}=\sum_{i=1}^{J}w_i^*(n)h_{AE,i}$，显然 q 是一个正负随机交替的随机变量，采用相位调制方法时，只要满足 $\angle(\boldsymbol{H}_{AB},\boldsymbol{H}_{AE})\ge\alpha$，本文提出的方法相当于对发送符号序列进行一次一密，即 $I(y_E(n);b(n))=0$，证明与文献[3]同。

4 数值仿真分析

下面对本文所设计的算法进行仿真分析，仿真中分别采用(7,4)汉明码，(15,7,3)循环码，调制方式为 BPSK，仿真条件如下：

(1)使用 10,000 组测试数据，每组包含 100 个比特数据；

(2)信道特征在每组测试数据期内保持不变，不同测试分组间保持独立；

(3)所涉随机信道相互独立，每个信道的实部和虚部也相互独立且都服从均值为 0、方差为 0.5 的正态分布，因此所涉信道增益均为 1；

(4)所涉信道噪声的实部与虚部相互独立且都服从均值为 0、方差为 0.5 的正态分布，因此噪声的功率为 1。

首先将本文算法与已有的 3 种多天线物理层安全传输方法进行比较分析：(1)方法 1：人工噪声[8,9]；(2)方法 2：随机天线发射权重[10]；(3)方法 3：随机选择天线[11]。

方法 1 采用归一化发射权重，承载信号和噪声的功率各占一半，承载信号按式(10)进行平均补偿，噪声 $\boldsymbol{W}(n)$ 由式(11)产生：

$$w_i(n)=\left\|\boldsymbol{H}_{AB}\right\|\Big/Jh_{AB,i},\quad i=1,\cdots,J \tag{10}$$

$$\boldsymbol{W}(n)=\mathrm{Null}(\boldsymbol{H}_{AB}^{\mathrm{H}})=\{\boldsymbol{X}\in C^{J}:\boldsymbol{H}_{AB}^{\mathrm{H}}\boldsymbol{X}=0\} \tag{11}$$

方法 2 中，$J-1$ 根天线发射权重的实部和虚部均服从均值为 0、方差为 0.25 的正态分布，信道增益最大的天线发射权重由式(12)产生：

$$\boldsymbol{W}^{\mathrm{H}}(n)\boldsymbol{H}_{AB}=\left\|\boldsymbol{H}_{AB}\right\|=\left\langle\boldsymbol{H}_{AB},\boldsymbol{H}_{AB}\right\rangle^{1/2} \tag{12}$$

方法 3 每次随机选择天线数为 4 或 6，发射权重矢量由式(13)和式(14)确定：

$$\boldsymbol{W}(n)=\boldsymbol{H}_{AB}\Big/\left\|\boldsymbol{H}_{AB}\right\| \tag{13}$$

$$\boldsymbol{W}(n)=\boldsymbol{I}_j(n)\boldsymbol{H}_{AB}\Big/\left\|\boldsymbol{I}_j(n)\boldsymbol{H}_{AB}\right\| \tag{14}$$

其中 $\boldsymbol{I}_j(n)$，$1\le j\le J$ 是一个 $J\times J$ 维的随机选择矩阵，其对角线上随机分布 j 个 1，其余元素全为 0，每发射一个符号 $\boldsymbol{I}_j(n)$ 随机变化一次。本文算法的参考角 α 分别取 $\pi/3$，$\pi/4$，$\pi/6$，参考角调整指数 k 为 1。

图 4 给出了参考角 α 为 $\pi/6$ 时方法 3 随机选择天线数为 4 的误比特率(Bit-Error-Rate, BER)-发射功率性能曲线。由图 4 可知：随着发射功率增加，所有方法的 Bob 的 BER 都处于下降趋势，其 BER 值顺序为：$\mathrm{BER}_{\text{方法1}}>\mathrm{BER}_{\text{方法3}}>\mathrm{BER}_{\text{方法2}}>\mathrm{BER}_{\text{本文算法}}$。方法 1 需要很大的发射功率才能使 Bob 实现低 BER，方法 3 牺牲了天线的分集增益，其 BER 比方法 2 高。因为发射天线在投影矢量方向上的“点聚焦”特性[12]和多天线的分集增益，本文算法的 BER 较方法 2 低一个数量级；前 3 种方法都是在调制域实现对 Eve 信道特征的随机置乱使其无法正常解调，所以 BER 差不多。本文算法从编码和调制结合的角度去实现多天线系统的物理层安全传输，目的是即使 Eve 可以正常解调，其译码码字的汉明距离也发生了随机置乱，其 BER 接近 0.5。图 5 是本文算法的参考角 α 分别取 $\pi/6$，$\pi/4$，$\pi/3$ 时，与方法 3 随机天线数为 6 时的 BER-发射功率性能曲线。由图 5 知，随机天线数增加，天线的分集增益增大，方法 3 的 Bob 的 BER 明显降低；本文算法参考角越大，Bob 的 BER 越大。这是因为参考角越大，投影矢量的取值空间就越小，$\boldsymbol{H}_{AB}$ 在其上的投影分量就越小，即内积越小，接收信噪比下降，其 BER 变大。

其次考虑 Bob 与 Eve 在发射天线数、参考角和信道编码变化时 BER 的性能变化情况。图 6 给出的是 BER 与发射天线数的关系。总发射功率设为 1，参考角固定为 $\pi/3$，调整指数 $k=1$，发射天线数由 2 根变为 12 根，变化间隔为 2 根。随着发射天线数

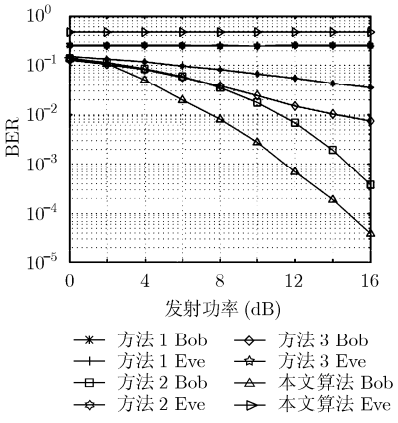

图 4 误比特率随发射功率变化情况

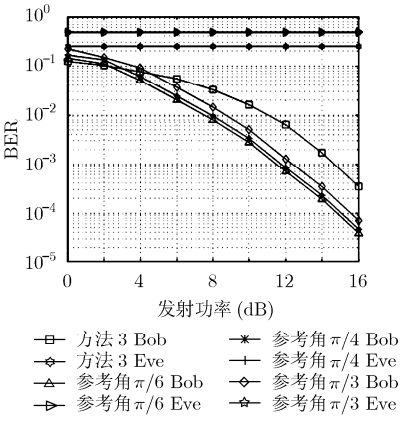

图 5 误比特率随发射功率变化情况

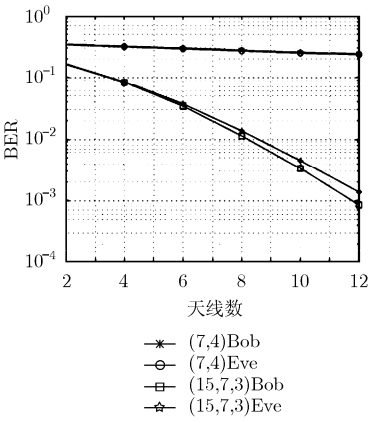

图 6 误比特率随发射天线数的变化情况

的增加，天线的分集增益增大，Bob 的 BER 处于下降趋势，但 Eve 的误比特率变化不大，在 0.5 附近变化，这表明了本文算法的安全性不受发射天线数的影响。图 7 给出的是 BER 与参考角的关系。总发射功率设为 1，发射天线数固定为 8，调整指数 $k=0$，参考角在 0.7 rad 到 1.5 rad 间变化，变化间隔为 0.1 rad。随着参考角的增大，Bob 的 BER 呈上升趋势，这是因为参考角越大，投影矢量的取值空间就越小，$\boldsymbol{H}_{AB}$ 在其上的投影分量就越小，即内积越小，接收信噪比下降，其 BER 变大。Eve 的 BER 变化不大，在 0.5 附近变化，这进一步验证了本文算法的安全性。

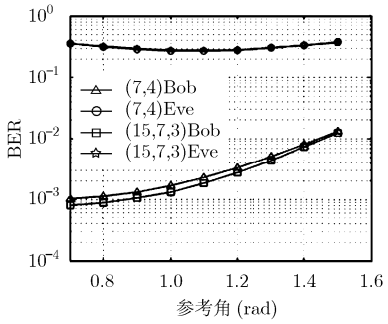

图 7 误比特率随参考角的变化情况

由上面的仿真分析知，Bob 采用码长更长和纠检错能力更强的编码，BER 降低，这表明编码增益可以提高 Bob 的接收性能，而已有多天线物理层安全传输方法则没有这一特性。

5 结论

本文结合编码和调制提出了一种多天线信道特征投影物理层安全编码算法。在满足信道互易性的时分双工 MISO 系统中，多天线发射机根据单天线接收机发送的训练符号估计信道得到授权信道特征，再利用授权信道特征投影生成投影矢量对；每次发射符号时随机选择投影矢量作为发射权重矢量，在保证 Bob 正常接收的同时使 Eve 还原码字的汉明距离特性遭到破坏而无法正确译码。仿真结果表明：在参考角选择足够小时，窃听者的误比特率接近 0.5, Bob 的误比特率较已有多天线物理层安全传输方法低了一个数量级。

附录

引理 1　在信道特征空间 Ω 内，若信道特征矢量 $\boldsymbol{H}$ 与投影矢量 $\boldsymbol{W}$ 的夹角满足 $0<\angle(\boldsymbol{H},\boldsymbol{W})<\pi/2$，则信道特征矢量在投影矢量上的投影为正；反之，若 $\pi/2<\angle(\boldsymbol{H},\boldsymbol{W})<\pi$，则信道特征矢量在投影矢量上的投影为负[16]。

引理 2　在信道特征空间 Ω 内，若信道特征矢量对 $(\boldsymbol{H}_A,\boldsymbol{H}_B)$ 之间的夹角为 α，即 $\angle(\boldsymbol{H}_A,\boldsymbol{H}_B)=\alpha$，对应投影矢量对 $(\boldsymbol{W}_1,\boldsymbol{W}_2)$ 满足 $\angle\boldsymbol{W}_1\in(\angle\boldsymbol{H}_A-\pi/2,\angle\boldsymbol{H}_A+\alpha-\pi/2)$ 和 $\angle\boldsymbol{W}_2\in(\angle\boldsymbol{H}_A-\alpha+\pi/2,\angle\boldsymbol{H}_A+\pi/2)$，则 $\boldsymbol{H}_A$ 在投影矢量对上的投影均为正，即满足 $0<\angle(\boldsymbol{H}_A,\boldsymbol{W}_1)<\pi/2$ 和 $0<\angle(\boldsymbol{H}_A,\boldsymbol{W}_2)<\pi/2$。

证明　因为 $\angle(\boldsymbol{H}_A,\boldsymbol{H}_B)=\alpha$，则与 $\boldsymbol{H}_A$ 正交的投影矢量对应的角度为 $\angle\boldsymbol{H}_A-\pi/2$ 和 $\angle\boldsymbol{H}_A+\pi/2$，与 $\boldsymbol{H}_B$ 正交的投影矢量对应的角度为 $\angle\boldsymbol{H}_A+\alpha-\pi/2$ 和 $\angle\boldsymbol{H}_A-\alpha+\pi/2$。若投影矢量对 $(\boldsymbol{W}_1,\boldsymbol{W}_2)$ 对应的两个投影矢量的角度取值分别为 $\angle\boldsymbol{W}_1\in(\angle\boldsymbol{H}_A-\pi/2,\angle\boldsymbol{H}_A+\alpha-\pi/2)$ 和 $\angle\boldsymbol{W}_2\in(\angle\boldsymbol{H}_A-\alpha+\pi/2,\angle\boldsymbol{H}_A+\pi/2)$，则 $0<\angle(\boldsymbol{H}_A,\boldsymbol{W}_1)<\pi/2$ 和 $0<\angle(\boldsymbol{H}_A,\boldsymbol{W}_2)<\pi/2$，由引理 1 可知 $\boldsymbol{H}_A$ 在投影矢量对上的投影均为正。综上，引理 2 得证。

定理 1　在 J 维信道特征空间 Ω 内，若存在信道特征矢量对 $(\boldsymbol{H}_A,\boldsymbol{H}_B)$ 满足 $\angle(\boldsymbol{H}_A,\boldsymbol{H}_B)\geq\alpha$，且存在投影矢量对 $(\boldsymbol{W}_1,\boldsymbol{W}_2)$ 满足 $\angle(\boldsymbol{W}_1,\boldsymbol{H}_A)\in(\pi/2-\alpha,\pi/2)$，$\angle(\boldsymbol{W}_1,\boldsymbol{H}_B)\in(\pi/2-\alpha,\pi/2)$，即 $\boldsymbol{H}_A$ 在投影矢量对上的投影均为正。则有

$$\mathrm{Sign}(\boldsymbol{H}_B\perp\boldsymbol{W}_1)\cdot\mathrm{Sign}(\boldsymbol{H}_B\perp\boldsymbol{W}_2)=-1 \qquad \text{(A1)}$$

其中 $\perp$ 表示信道特征矢量的正交投影；Sign 表示投影的正负取值。

证明　如图 8 所示，在信道特征空间 Ω 内，投影矢量对 $(\boldsymbol{W}_1,\boldsymbol{W}_2)$ 的取值范围位于信道特征矢量 $\boldsymbol{H}_A$ 和 $\boldsymbol{H}_B$ 在空间 Ω 的正交投影空间(零空间)的交叉区域中。可用反证法证明式(A1)成立。假设式(A1)不成立，由引理 2，则有 $0<\angle(\boldsymbol{H}_B,\boldsymbol{W}_1)<\pi/2$，$0<\angle(\boldsymbol{H}_B,\boldsymbol{W}_2)<\pi/2$。而 $\angle(\boldsymbol{W}_1,\boldsymbol{H}_A)\in(\pi/2-\alpha,\pi/2)$，$\angle(\boldsymbol{W}_2,\boldsymbol{H}_A)\in(\pi/2-\alpha,\pi/2)$，则有 $\angle(\boldsymbol{H}_A,\boldsymbol{H}_B)<\alpha$，这显然与已知条件 $\angle(\boldsymbol{H}_A,\boldsymbol{H}_B)\geq\alpha$ 矛盾，因此有式(A1)成立。

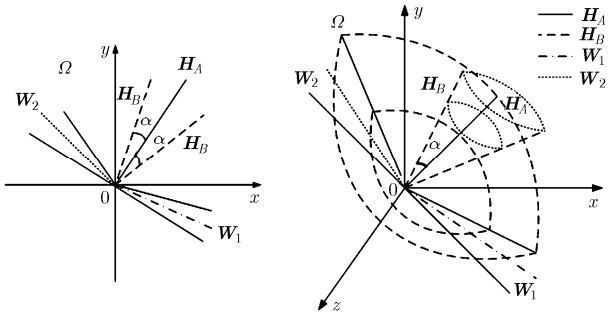

图 8 信道特征空间投影分析

参 考 文 献

[1] Shiu Y S, Chang S Y, *et al*.. Physical layer security in wireless networks: a tutorial [J]. *IEEE Wireless Communications*, 2011, 24(4): 1276–1284.

[2] Debbah M, Gamal H E, Poor H V, *et al*.. Wireless Physical Layer Security [J]. *EURASIP Journal on Wireless Communications and Networking*, 2009, 2009: 1–2.

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

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

[5] Klinc D, Ha J, McLaughlin S M, *et al*.. LDPC codes for the Gaussian wiretap channel [C]. Proceedings of Information Theory Workshop (ITW), Taormina, Sicily, Italy, 2009: 95–99.

[6] 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.

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

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

[9] Zhou X and 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.

[10] 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.

[11] 穆鹏程, 殷勤业, 王文杰. 无线通信中使用随机天线阵列的物理层安全传输方法[J]. 西安交通大学学报, 2010, 44(6): 62–66.
Mu P C, Yin Q Y, and Wang W J. A security method of physical layer transmission using random antenna arrays in wireless communication [J]. *Journal of Xi'an Jiaotong University*, 2010, 44(6): 62–66.

[12] Kim H S. Measurement and model based characterization of indoor wireless channels [D]. Korea: Kyungpook National University, 2003: 22–35.

[13] 张贤达. 矩阵分析与应用 [M]. 北京: 清华大学出版社, 2004: 657–662.
Zhang X D. Matrix Analysis and Applications [M]. Beijing: Tsinghua University Press, 2004: 657–662.

王亚东： 男，1984年生，硕士生，研究方向为物理层安全、信息论与编码.

黄开枝： 女，1973年生，副教授，硕士生导师，从事无线移动安全研究.

吉 江： 男，1983 年生，博士生，研究方向为物理层安全与信息论.