doi:10.3969/j.issn.1000-436x.2014.04.009

基于空域加扰信号超平面特征的窃密算法

刘璐，金梁，黄开枝，钟州
(国家数字交换系统工程技术研究中心，河南 郑州 450002)

摘 要：针对现有空域加扰信号的截获算法抗噪性能差、计算复杂度高、无法实时处理的问题，从信号空间特征的角度，证明了窃听信号的星座点服从超平面分布。据此设计了一种基于超平面聚类的窃密算法，能够盲估计出超平面参数，且该参数与发送信息一一对应，从而破解信息。分析与仿真表明，该算法比现有的类子空间法（MUSIC-like）的抗噪声性能提升 8~10 dB，计算复杂度低 6~10 个数量级。

关键词：物理层安全；人工噪声；信号盲估计；空域加扰
中图分类号：TN918 **文献标识码**：A **文章编号**：1000-436X(2014)04-0074-07

Eavesdropping against wireless spatial scrambling secure communication: hyperplane clustering

LIU Lu, JIN Liang, HUANG Kai-zhi, ZHONG Zhou
(National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, China)

Abstract: The existing eavesdropping method has poor anti-noise performance and high complexity, which makes it not practical. It is shown that the received scrambled signals are distributed within parallel hyperplanes if adequate antennas are equipped by eavesdropper. According to this distribution, a hyperplane clustering (HC) algorithm was presented to blindly estimate the hyperplane parameters which reveal the sending information. Simulation results show that the HC algorithm, compared with the existing MUSIC-like algorithms, holds the advantages of better anti-noise performance and lower computing complexity.

Key words: physical-layer security; artificial noise; signal blind estimation; spatial scrambling

1 引言

无线通信技术在给人们带来便利的同时，其信息安全问题也日益突出。传统的无线保密通信主要是照搬有线通信中的密钥体制，忽略了无线通信与有线通信的差异性。在无线通信系统中，不同用户的接收信号是有差异的，这种差异使得在物理层实现保密通信成为了可能。

Wyner[1]首先提出在窃密信道(wiretap channel)中，仅依靠物理层的编码即可实现保密通信，并且给出了保密容量的概念。Csiszár 等人在文献[2]中指出，对一般的高斯广播信道，如果主信道容量大于窃听信道容量时，系统保密容量大于零。然而实际中，窃听者的方位信息一般未知，无法确定其信道状态的优劣，若窃听者的信噪比高于接收用户，则无法保证通信的保密性。为了解决这一问题，Goel、Negi、Li 等人从不同的角度分别提出了多天线保密通信的新方法[3~6]。这些方法的相同点可以概括为：发送端在主信道方向上发送信息波束，同时在其零空间发送人工噪声。随机加入的噪声仅仅恶化窃听方信号的接收质量，而合法用户的正常通信不受影响，因而存在正的保密速率。这种利用空间方位的不同进行加密的方法，可统称为空域加扰法[7]。

当窃听者采用多天线接收时，Goel 和 Negi 指出，人工噪声会失效[4]，但没有提出相应的窃密思

收稿日期：2012-11-20；**修回日期**：2013-03-25
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)

路；Li 在数学上证明了窃听方无法通过盲解卷积的方法对空域加扰信号进行窃密[6]，但尚不清楚能否通过其他方式窃密。近几年，关于空域加扰法的研究主要集中于优化信号与噪声的功率分配[8,9]，以进一步提升保密速率。而相应的窃密算法研究较少。直到近期，吴飞龙等人提出了 MUSIC-like 窃密算法[7,10]，该算法利用信号子空间与噪声子空间正交的特性，对有限字符集内所有可能出现的信号序列进行遍历搜索，实现信息的获取。该算法存在计算开销过大的缺点。同时，受限于计算复杂度，其遍历块的长度往往较短，算法性能易受噪声影响，因而很难在实际中应用。

针对这一问题，本文从空域加扰信号的信号空间角度出发，首先证明了发送天线数小于或等于窃听天线数时，加扰信号呈现出平行的超平面分布特征，并指出这是多天线能够窃密的根本原因。然后利用该特征，提出了一种超平面聚类算法，通过选取一组相互平行的超平面去逼近接收信号，利用样本获取超平面参数，进而破解信息。分析与仿真表明，该算法比 MUSIC-like 法在抗噪声性能上提升了 8~10 dB，计算复杂度低 6~10 个数量级，能够用于实时解调。

2　系统模型

保密无线通信模型如图 1 所示，发送端 Alice 向合法用户 Bob 发送信息，遭到非法用户 Eve 的窃听。其中，Alice 天线数用 N_a 表示，Bob 单天线，Eve 天线数用 N_e 表示。

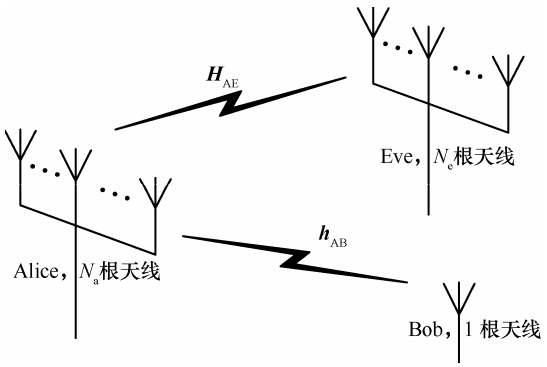


图 1　系统模型

窄带通信系统中，Alice 和 Bob 之间的主信道可以用向量 $\boldsymbol{h}_{AB}=[h_1,h_2,\cdots,h_{N_a}]^T$ 表示，其中，h_i 为 Alice 的第 i 根发送天线到 Bob 接收天线之间的信道增益，上标 T 表示矩阵转置。Alice 到 Eve 的窃听信道可以表示为一个 $N_a\times N_e$ 的矩阵

$$\boldsymbol{H}_{AE}=\begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1N_e} \\ h_{21} & h_{22} & \cdots & h_{2N_e} \\ \vdots & \vdots & \ddots & \vdots \\ h_{N_a1} & h_{N_a2} & \cdots & h_{N_aN_e} \end{bmatrix} \tag{1}$$

其中，h_{ij} 为 Alice 的第 i 根发送天线到 Eve 的第 j 根接收天线之间的信道增益。假定所有信道都是慢衰落信道，信道增益在一个数据帧内保持不变，并且在不同帧之间独立同分布。Alice 在时刻 n 发送信号矢量 $\boldsymbol{x}(n)$，Bob 和 Eve 接收到的信号分别为

$$\boldsymbol{y}_B(n)=\langle \boldsymbol{x}(n),\boldsymbol{h}_{AB}\rangle+\boldsymbol{n}_B(n) \tag{2}$$

$$\boldsymbol{y}(n)=\boldsymbol{H}_{AE}^H\boldsymbol{x}(n)+\boldsymbol{n}_E(n) \tag{3}$$

其中，$\boldsymbol{n}_B(n)$和 $\boldsymbol{n}_E(n)$分别是 n 时刻 Bob 和 Eve 天线上接收到的加性高斯白噪声；$\langle \boldsymbol{x},\boldsymbol{y}\rangle=\boldsymbol{y}^H\boldsymbol{x}$ 表示酉空间的内积，上标 H 代表矩阵共轭转置。

3　加扰信号的超平面特征

空域加扰的思想是 Alice 根据 $\boldsymbol{h}_{AB}$ 对发送信息进行随机映射，即利用多天线技术在主信道的零空间内对传统的星座点进行高维展开。Bob 首先发送训练序列给 Alice，Alice 通过信道估计得到 $\boldsymbol{h}_{AB}$。假定 Alice 的发送符号集为 $U=\{u_1,u_2,\cdots,u_m\}$，其中 m 为发送符号集的大小。Alice 在时刻 n 发送符号 $u(n)\in U$，并用主信道单位方向对信息进行波束成型调制

$$\boldsymbol{s}_1(n)=u(n)\boldsymbol{h}_{AB}/\|\boldsymbol{h}_{AB}\| \tag{4}$$

其中，$\|\cdot\|$ 表示取向量的 2 范数。$\boldsymbol{s}_1(n)$只是 N_a 维酉空间中的一个向量，因此可利用剩余的 N_a-1 维空间发送人工噪声

$$\boldsymbol{s}_2(n)=\boldsymbol{Z}\cdot\boldsymbol{v}(n)=\sum_{i=1}^{N_a-1}v_i(n)\boldsymbol{\beta}_i \tag{5}$$

其中，$\boldsymbol{v}(n)=[v_1(n),v_2(n),\cdots,v_{N_a-1}(n)]^T$ 为人工噪声系数，是服从某种分布的随机变量(一般假定其各元素独立同分布，且服从复高斯分布)，并且与发送信息 $u(n)$相互独立；$\boldsymbol{Z}=[\boldsymbol{\beta}_1,\boldsymbol{\beta}_2,\cdots,\boldsymbol{\beta}_{N_a-1}]$为 $\boldsymbol{h}_{AB}$ 零空间的一组正交基，满足$<\boldsymbol{\beta}_i,\boldsymbol{h}_{AB}>=0$，$i=1,2,\cdots,N_a-1$。

Alice 将调制信息同人工噪声叠加后发送，即 $\boldsymbol{x}(n)$为

$$\begin{aligned}\boldsymbol{x}(n)&=\boldsymbol{s}_1(n)+\boldsymbol{s}_2(n)\\&=u(n)\boldsymbol{h}_{AB}/\|\boldsymbol{h}_{AB}\|+\sum_{i=1}^{N_a-1}v_i(n)\boldsymbol{\beta}_i\end{aligned} \tag{6}$$

可见，$\boldsymbol{x}(n)$是 $u(n)$, $v_1(n)$, $v_2(n)$,$\cdots$, $v_{N_a-1}(n)$分别对主

信道以及 N_a-1 个零空间基向量进行调制叠加的结果。只有主信道方向携带信息，其他分量均为人工噪声。

定理 1　加扰信号 $\mathbf{x}(n)$的星座图呈 m 张平行的超平面分布，每个超平面对应一个原始发送符号 $u(n)$，主信道方向为超平面的法线方向，$u(n)$为超平面的偏移量。

证明　将 $\boldsymbol{x}(n)$向主信道投影，得到

$$\begin{aligned}\left\langle \boldsymbol{x}(n), \boldsymbol{h}_{\mathrm{AB}} / \left\|\boldsymbol{h}_{\mathrm{AB}}\right\| \right\rangle &= u(n)\left\langle \boldsymbol{h}_{\mathrm{AB}}, \boldsymbol{h}_{\mathrm{AB}} \right\rangle / \left\|\boldsymbol{h}_{\mathrm{AB}}\right\|^2 + \\ &\quad \sum_{i=1}^{N_a-1} v_i(n)\left\langle \boldsymbol{\beta}_i, \boldsymbol{h}_{\mathrm{AB}} \right\rangle / \left\|\boldsymbol{h}_{\mathrm{AB}}\right\| \\ &= u(n) \end{aligned} \tag{7}$$

在几何学中，集合 $H=\{\boldsymbol{x}\in C^n \mid <\boldsymbol{x}, \boldsymbol{w}>\}$为 n 维酉空间中的一个超平面(hyperplane)[11]。其中，$b\in C$，被称作 H 的偏移量；$\boldsymbol{w}\in C^n$ 且$\|\boldsymbol{w}\|=1$，被称作 H 的法向量。可见，H 被法向量和偏移量唯一决定，因此可以用$(\boldsymbol{w}, b)$来简化表示 H，其几何意义如图 2 所示，代表在 $\boldsymbol{w}$ 方向上投影为 b 的点组成的集合。当且仅当 $H_1 \cap H_2 = \varnothing$ 时，称超平面 H_1 与 H_2 相互平行，记作 $H_1 // H_2$。

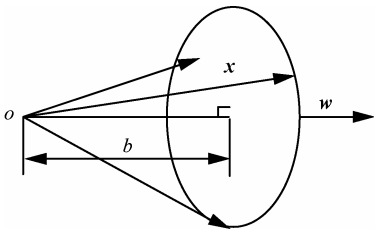


图 2　超平面示意

由式(7)可知，$\boldsymbol{x}(n)\in(\boldsymbol{h}_{\mathrm{AB}}/\left\|\boldsymbol{h}_{\mathrm{AB}}\right\|, u(n))$。令 $H_i=(\boldsymbol{h}_{\mathrm{AB}}/\left\|\boldsymbol{h}_{\mathrm{AB}}\right\|, u_i)$，由于 $u_i \neq u_j$，显然 $H_i \cap H_j = \varnothing$，即超平面 $H_i // H_j$，其中 $i, j = 1,2,\cdots,m$，$i \neq j$。可见经过时间累计，$\boldsymbol{x}(n)$ 在 N_a 维酉空间中呈 m 张平行的超平面分布，如图 3 所示，其法向量为 $\boldsymbol{h}_{\mathrm{AB}}/\left\|\boldsymbol{h}_{\mathrm{AB}}\right\|$，偏移量为相应的发送符号 u_i。

定理 2　当 $N_e \geqslant N_a$，且满足 $\mathrm{rank}(\boldsymbol{H}_{\mathrm{AE}}) = N_a$ 时，若忽略 $\boldsymbol{n}_{\mathrm{E}}(n)$的影响，则 $\boldsymbol{y}(n)$仍分布于 m 张超平面中，且不同符号对应的超平面相互平行。

证明　用 $\boldsymbol{H}_{\mathrm{AE}}^{+} = \boldsymbol{H}_{\mathrm{AE}}^{\mathrm{H}}(\boldsymbol{H}_{\mathrm{AE}}\boldsymbol{H}_{\mathrm{AE}}^{\mathrm{H}})^{-1}$ 表示 $\boldsymbol{H}_{\mathrm{AE}}$ 的广义逆矩阵，假设 $\boldsymbol{x}(n)\in H_i = (\boldsymbol{h}_{\mathrm{AB}}/\left\|\boldsymbol{h}_{\mathrm{AB}}\right\|, u_i)$，取 $\boldsymbol{w} = \boldsymbol{H}_{\mathrm{AE}}^{+}\boldsymbol{h}_{\mathrm{AB}} \in \boldsymbol{C}^{N_e}$，则

$$\begin{aligned}\left\langle \boldsymbol{y}(n), \boldsymbol{w} \right\rangle &\approx \boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{AE}}^{\mathrm{H}}\boldsymbol{x}(n) \\ &= \boldsymbol{h}_{\mathrm{AB}}^{\mathrm{H}}(\boldsymbol{H}_{\mathrm{AE}}\boldsymbol{H}_{\mathrm{AE}}^{\mathrm{H}})^{-1}\boldsymbol{H}_{\mathrm{AE}}\boldsymbol{H}_{\mathrm{AE}}^{\mathrm{H}}\boldsymbol{x}(n) \\ &= \left\langle \boldsymbol{x}(n), \boldsymbol{h}_{\mathrm{AB}} \right\rangle \\ &= u_i \end{aligned} \tag{8}$$

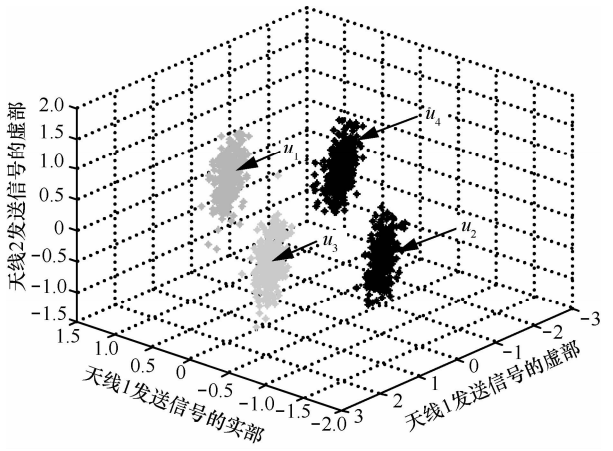


图 3　加扰信号星座图的超平面分布(2 根发送天线，QPSK 调制)

对 $\boldsymbol{w}$ 归一化，令 $\boldsymbol{w}' = \boldsymbol{w}/\left\|\boldsymbol{w}\right\|$，$u_i' = u_i/\left\|\boldsymbol{w}\right\|$，得到 $\left\langle \boldsymbol{y}(n), \boldsymbol{w}' \right\rangle = u_i'$，即 $\boldsymbol{y}(n)\in H_i' = (\boldsymbol{w}', u_i')$。可见，当 $u(n) = u_i$ 时，$\boldsymbol{y}(n)$ 位于超平面 H_i' 内，且不同发送符号对应的超平面平行，即 $H_i' // H_j'$，$i, j = 1,2,\cdots,m$，$i \neq j$，且接收信号的超平面法向量以及偏移量分别为

$$\boldsymbol{w}' = \boldsymbol{H}_{\mathrm{AE}}^{\mathrm{H}}(\boldsymbol{H}_{\mathrm{AE}}\boldsymbol{H}_{\mathrm{AE}}^{\mathrm{H}})^{-1}\boldsymbol{h}_{\mathrm{AB}} / \left\|\boldsymbol{H}_{\mathrm{AE}}^{\mathrm{H}}(\boldsymbol{H}_{\mathrm{AE}}\boldsymbol{H}_{\mathrm{AE}}^{\mathrm{H}})^{-1}\boldsymbol{h}_{\mathrm{AB}}\right\| \tag{9}$$

$$u_i' = u_i / \left\|\boldsymbol{H}_{\mathrm{AE}}^{\mathrm{H}}(\boldsymbol{H}_{\mathrm{AE}}\boldsymbol{H}_{\mathrm{AE}}^{\mathrm{H}})^{-1}\boldsymbol{h}_{\mathrm{AB}}\right\| \tag{10}$$

定理 1 从几何的角度揭示了空域加扰的本质，虽然它随机置乱了发送星座图，但为了让 Bob 能够常规解调，置乱的信号依然需要服从一定的规则，即星座点只能在相应的超平面内随机置乱。定理 2 解释了空域加扰法在 $N_e \geqslant N_a$ 时失去保密性的根本原因：当窃听天线数目充分多时，Eve 相当于在另一组基下观测加扰信号，而空间超平面的几何关系具有旋转和平移的不变性，并不会随基的变化而改变。所以超平面特征是 Eve 截获信息的突破口。

4　超平面聚类窃密算法

基于加扰信号的上述几何特征，设计超平面聚类法(HC, hyperplane clustering)进行窃密。该算法利用 m 张平行的超平面对一帧内前 K 个接收信号 $\boldsymbol{y}_1, \boldsymbol{y}_2, \cdots, \boldsymbol{y}_K$ 进行聚类，得到最佳超平面参数 $\tilde{\boldsymbol{w}}$ 和 $\tilde{b}_j$，$j = 1,2,\cdots,m$。如图 4 所示，Eve 利用所得到的参数，对该帧信号进行解调。

设 d_{ij} 为 $\boldsymbol{y}_i$ 到 H_j 的距离的平方，即

$$d_{ij} = \left\|\left\langle \boldsymbol{y}_i, \boldsymbol{w} \right\rangle + b_j\right\|^2 \tag{11}$$

建立目标函数为

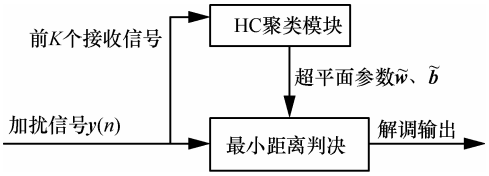


图 4　窃密解调器

$$\min_{\boldsymbol{w},\boldsymbol{b}} J(\boldsymbol{w},\boldsymbol{b},\boldsymbol{\delta}) = \sum_{i=1}^{K}\sum_{j=1}^{m}\delta_{ij}d_{ij} \tag{12}$$

其中，$\boldsymbol{b}=(b_1,b_2,\cdots,b_m)^{\mathrm{T}}$ 代表 m 张超平面的偏移量；$\boldsymbol{w}$ 是共同的法向量；布尔矩阵 $\boldsymbol{\delta}=(\delta_{ij})^{K\times m}$ 满足

$$\delta_{ij}=\begin{cases}1, & d_{ij}=\min(d_{i1},\cdots,d_{im})\\ 0, & \text{其他}\end{cases} \tag{13}$$

即用 m 张平行的超平面去逼近 K 个接收信号样本点，且“逼近效果”用各点离超平面最小距离的平方误差之和来衡量。采用如下的方法对式(12)迭代求解。

1) $n=0$，并随机初始化 $\boldsymbol{w}(0)$ 和 $\boldsymbol{b}(0)$。

2) 将 $\boldsymbol{w}(n)=\boldsymbol{w}(n)/\|\boldsymbol{w}(n)\|$ 和 $\boldsymbol{b}(n)$ 代入式(11)，得到 d_{ij} 并根据式(13)，确定 $\boldsymbol{\delta}$。

3) 最优化 $\boldsymbol{w}$ 和 $\boldsymbol{b}$，并重新划分超平面。即在式(12)中，对 $\boldsymbol{w}$ 和 $\boldsymbol{b}$ 分别求偏导，并令导数为零（详细计算过程见附录），可得

$$\boldsymbol{w}(n+1)=\boldsymbol{A}^{-1}\boldsymbol{q} \tag{14}$$

$$b_j(n+1)=-\sum_{i=1}^{K}\delta_{ij}\langle\boldsymbol{y}_i,\boldsymbol{w}(n)\rangle/\sum_{i=1}^{K}\delta_{ij} \tag{15}$$

其中，$\boldsymbol{A}$ 为对称矩阵，且

$$\boldsymbol{A}=\sum_{i=1}^{K}\sum_{j=1}^{m}\delta_{ij}\boldsymbol{y}_i\boldsymbol{y}_i^{\mathrm{H}} \tag{16}$$

$$\boldsymbol{q}=-\sum_{i=1}^{K}\sum_{j=1}^{m}\delta_{ij}b_j^{*}(n)\boldsymbol{y}_i \tag{17}$$

4) $n=n+1$，重复步骤 2)和步骤 3)，直至 $\boldsymbol{w}$ 和 $\boldsymbol{b}$ 收敛到 $\tilde{\boldsymbol{w}}$ 和 $\tilde{\boldsymbol{b}}$。

得到超平面 $H_j=\left(\tilde{\boldsymbol{w}},\tilde{b}_j\right)$ 后，$j=1,2,\cdots,m$，Eve 可以采用最小距离准则，对 $\boldsymbol{y}(n)$ 进行符号判决，即 $u(n)=u_i$，其中，$i=\arg\min_{i=1,\cdots,m}(\|\tilde{b}_i-\langle\boldsymbol{y}(n),\tilde{\boldsymbol{w}}\rangle\|)$。

5　性能仿真和复杂度分析

本节仿真验证所提算法，讨论参数：N_e、K、Eve 接收信噪比 SNR 以及信干扰比 SIR(Alice 信息发送功率与干扰发送功率的比值，SIR 越小，干扰功率越大)对窃听 BER(误比特率)的影响。并且在相同条件下，将超平面聚类法(HC)的 BER 以及计算复杂度同现有的 MUSIC-like 法进行比较。

5.1　性能仿真

性能仿真参数如表 1 所示。

表 1　仿真参数

系统参数	参数值
帧长 L	1 024 符号
接收帧数	100 000 帧
信道 h_{AB}, $\boldsymbol{H}_{\mathrm{AE}}$	在一帧时间内，矩阵各元素保持不变，帧间相互独立且服从零均值、单位方差的复高斯分布
调制方式	BPSK
天线数 N_{a}, N_{e}	Alice 天线数 Na=4 Eve 天线数 Ne=4,6
Eve 接收噪声 $n_{\mathrm{E}}(n)$	每根天线接收噪声相互独立，且服从零均值单位方差复高斯分布

1) 聚类样本点个数 K 的影响

由于窃听方无法获取训练样本，只能通过盲辨识途径截获信息，因此需要利用较多的接收样本点（该样本点所携带的具体信息未知）校正超平面参数。从几何角度看，只有接收信号足够多时，其超平面分布的特征才会更加明显。如图 5 所示，开始时，*BER* 大幅下降，但 K 增大到一定程度后，*BER* 不再显著变化。因此，综合考虑窃密性能和计算复杂度，样本数无需过大，下面仿真中均取 K=200。

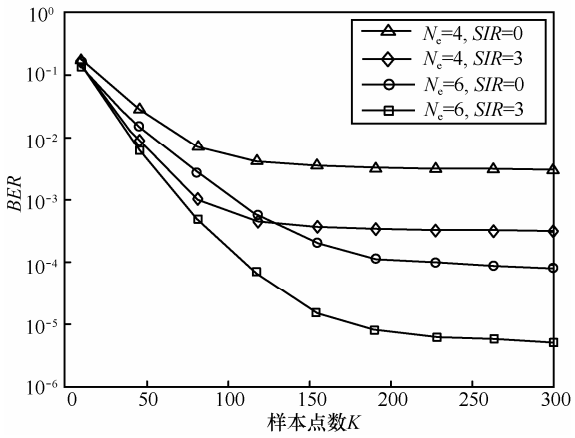
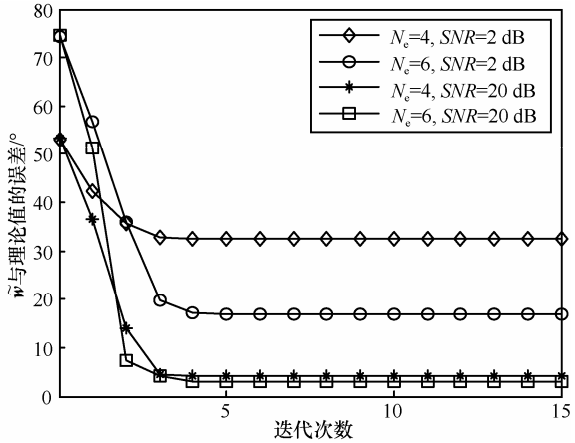


图 5　聚类样本个数 K 对算法性能的影响(*SNR*=10 dB)

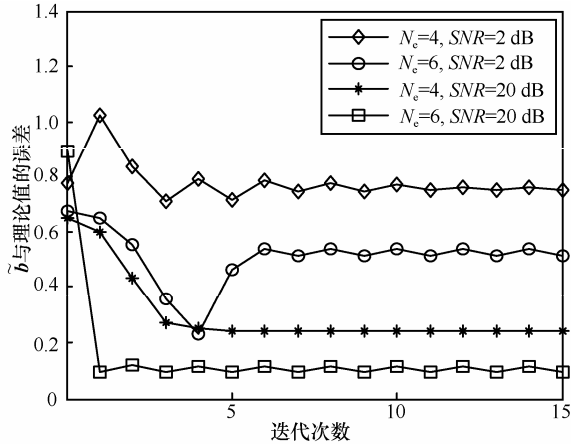
2) 算法收敛性

将式(9)和式(10)所示的理论值与 HC 所获得的估计值进行对比，分别在大小信噪比下验证算法的收敛性。结果如图 6 所示，其中，用向量夹

角衡量 $\tilde{\boldsymbol{w}}$ 和 $\boldsymbol{w}$ 的误差，用 $\left\|\boldsymbol{b}-\tilde{\boldsymbol{b}}\right\|$ 衡量偏移量误差。可见，算法收敛速度较快，且在大信噪比下能够逼近实际值，同时，算法收敛性随天线数增大而改善。



(a) 法向量的收敛性



(b) 偏移量的收敛性

图 6　算法的收敛性(SIR=0 dB)

3) 抗噪声性能

在 Alice 采用相同功率发送干扰和信息的条件下，Eve 的信息截获性能如图 7 所示。同 MUSIC-like 算法相比(设其遍历块长度 $\hat{K}=9$)，HC 法的 BER 曲线向左平移了约 8~10 dB。原因分为两方面：从 MUSIC-like 方法来说，其计算复杂度随 $\hat{K}$ 呈指数增长，所以 $\hat{K}$ 的取值不能太大(通常取 6~9，远小于 K)，无法充分利用样本信息，易受信道噪声影响；从 HC 算法来说，向法向量 $\boldsymbol{w}$ 做投影的过程，不仅保留了信息成分、抵消了人工噪声，同时也消除了信号空间中其他方向上的噪声。所以，HC 的抗噪性优于 MUSIC-like 算法。

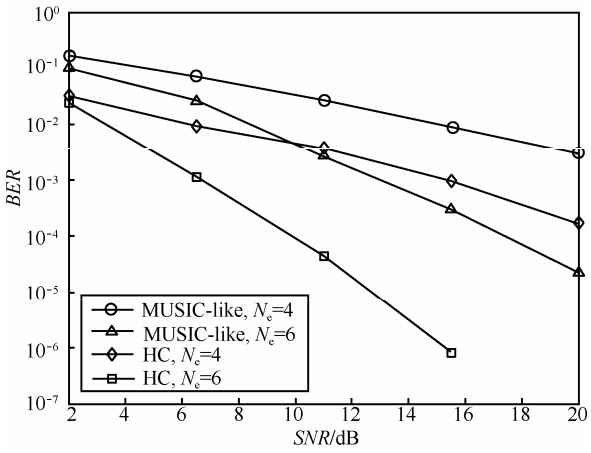


图 7　窃密算法的 BER 性能(SIR=0 dB)

4) 信干扰比的影响

信干扰比对算法解调性能的影响如图 8 所示。随着 SIR 的提升，HC 法的误码率急剧下降。这是因为 SIR 越大，超平面间距越大，相应聚类效果就会越好。然而，MUSIC-like 法没有利用该特征，性能提升较小。

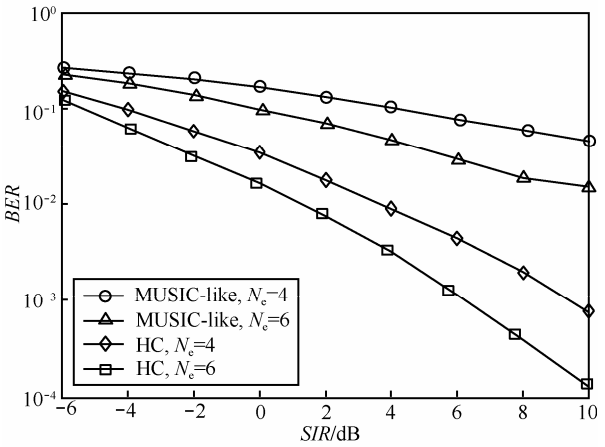


图 8　SIR 对算法性能的影响(SNR=2 dB)

5.2　计算复杂度分析

HC 法利用了超平面特征对信号建模分类，其计算复杂度主要集中于算法的第 2 步，需要乘累加个数约为 $O(mKN_e)$。得到 $\tilde{\boldsymbol{w}}$ 和 $\tilde{\boldsymbol{b}}$ 后，解调一帧符号所消耗的乘累加数约为 $O(LN_e)$。因此，共需消耗乘累加数约为 $O(TmKN_e+LN_e)$，其中，T 为迭代次数；而同样条件下，由于需要遍历符号集，MUSIC-like 法计算复杂度较高，消耗乘累加数约为 $O(L\hat{K}^2m^{\bar{K}})$。

为了直观地对比 2 种算法的计算量，假设 Alice 采用表 2 所示的物理层参数(为 3GPP2 推荐

的标准物理层格式[12]）发送加扰信号，Eve 实时解调所需处理速度如图 9 所示。可见 MUSIC-like 法所需的处理速度大大超出常规 DSP 器件的处理速度（约 1 000 亿次乘加运算/秒，MMAC）。而 HC 法比 MUSIC-like 法的计算复杂度下降了 6~10 个数量级，目前 DSP 器件的运算速度能够满足其实时处理的需求。

表 2　　物理层帧格式

物理层传输格式	数据帧长 L/symbol	一帧时间/ms	调制方式	符号集大小 m
(1 024,16,1 024)	512	26.66	QPSK	4
(3 072,2,64)	1 024	3.33	8PSK	8

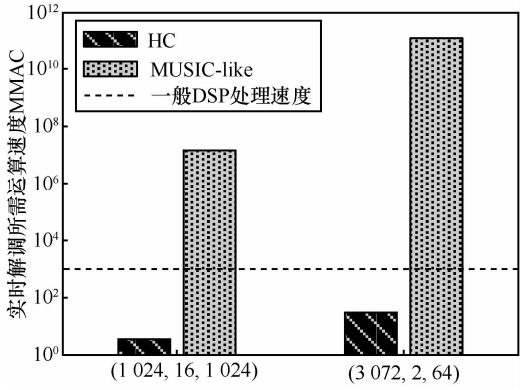


图 9　实时解调所需运算速度

6　结束语

在文献[7]的研究基础之上，本文对空域加扰法做了更为深入的分析，从几何角度入手，指出了窃密的可行性在于加扰信号存在超平面分布特征，并据此设计了超平面聚类算法，完成信息截获。HC 法比现有的 MUSIC-like 算法抗噪性能好，计算复杂度低，便于实际应用。若要利用空域加扰法实现保密通信，一方面要缩短帧长来隐藏超平面特征；另一方面也可以优化加扰图案，零空间内的高斯白噪声能被多天线分离，并不具有隐蔽性，反而容易暴露超平面特征。如何设计具有信息隐蔽性的加扰图案，值得进一步研究。

附录　式(14)和式(15)的证明

设复向量 $\boldsymbol{a},\boldsymbol{x}\in C^n$，$b\in C$，令 $y=\boldsymbol{x}^{\mathrm{H}}\boldsymbol{a}+b$，为了方便对 $\boldsymbol{x}$ 的实部和虚部分别求偏导，可将 n 维复向量看作 $2n$ 维实向量进行处理：

$$\begin{aligned}\hat{\boldsymbol{y}}&=\begin{bmatrix}y_{\mathrm{r}}\\ y_{\mathrm{i}}\end{bmatrix}=\begin{bmatrix}\boldsymbol{a}_{\mathrm{r}}^{\mathrm{T}} & \boldsymbol{a}_{\mathrm{i}}^{\mathrm{T}}\\ \boldsymbol{a}_{\mathrm{i}}^{\mathrm{T}} & -\boldsymbol{a}_{\mathrm{r}}^{\mathrm{T}}\end{bmatrix}\begin{bmatrix}\boldsymbol{x}_{\mathrm{r}}\\ \boldsymbol{x}_{\mathrm{i}}\end{bmatrix}+\begin{bmatrix}b_{\mathrm{r}}\\ b_{\mathrm{i}}\end{bmatrix}\\&=\boldsymbol{A}\hat{\boldsymbol{x}}+\hat{\boldsymbol{b}}\end{aligned}\tag{18}$$

其中，下标 r 和 i 分别代表相应变量的实部和虚部，即 $\boldsymbol{x}=\boldsymbol{x}_{\mathrm{r}}+j\boldsymbol{x}_{\mathrm{i}}$，$\boldsymbol{a}=\boldsymbol{a}_{\mathrm{r}}+j\boldsymbol{a}_{\mathrm{i}}$，$y=y_{\mathrm{r}}+jy_{\mathrm{i}}$，$b=b_{\mathrm{r}}+jb_{\mathrm{i}}$，并且

$$\boldsymbol{A}=\begin{bmatrix}\boldsymbol{a}_{\mathrm{r}}^{\mathrm{T}} & \boldsymbol{a}_{\mathrm{i}}^{\mathrm{T}}\\ \boldsymbol{a}_{\mathrm{i}}^{\mathrm{T}} & -\boldsymbol{a}_{\mathrm{r}}^{\mathrm{T}}\end{bmatrix},\quad \hat{\boldsymbol{x}}=\begin{bmatrix}\boldsymbol{x}_{\mathrm{r}}\\ \boldsymbol{x}_{\mathrm{i}}\end{bmatrix},\quad \hat{\boldsymbol{b}}=\begin{bmatrix}b_{\mathrm{r}}\\ b_{\mathrm{i}}\end{bmatrix}$$

式(18)中的元素均为实数，而

$$\begin{aligned}\|y\|^2&=y_{\mathrm{r}}^2+y_{\mathrm{i}}^2=\hat{\boldsymbol{y}}^{\mathrm{T}}\hat{\boldsymbol{y}}=(\boldsymbol{A}\hat{\boldsymbol{x}}+\hat{\boldsymbol{b}})^{\mathrm{T}}(\boldsymbol{A}\hat{\boldsymbol{x}}+\hat{\boldsymbol{b}})\\&=\hat{\boldsymbol{x}}^{\mathrm{T}}A^{\mathrm{T}}A\hat{\boldsymbol{x}}+2\boldsymbol{b}^{\mathrm{T}}A\hat{\boldsymbol{x}}+\hat{\boldsymbol{b}}^{\mathrm{T}}\hat{\boldsymbol{b}}\end{aligned}\tag{19}$$

所以利用实数求导公式可以得到

$$\frac{\partial\|y\|^2}{\partial\hat{\boldsymbol{x}}}=2A^{\mathrm{T}}A\hat{\boldsymbol{x}}+2A^{\mathrm{T}}\hat{\boldsymbol{b}}\tag{20}$$

$$\frac{\partial\|y\|^2}{\partial\hat{\boldsymbol{b}}}=2A\hat{\boldsymbol{x}}+2\hat{\boldsymbol{b}}\tag{21}$$

令偏导为零，可得

$$\hat{\boldsymbol{x}}=-(A^{\mathrm{T}}A)^{-1}A^{\mathrm{T}}\hat{\boldsymbol{b}}\tag{22}$$

$$\hat{\boldsymbol{b}}=-A\hat{\boldsymbol{x}}\tag{23}$$

将式(22)和式(23)转换成相应的复数形式，即

$$\boldsymbol{x}=(\boldsymbol{a}\boldsymbol{a}^{\mathrm{H}})^{-1}\boldsymbol{a}\cdot b^{*}\tag{24}$$

$$b=-\boldsymbol{x}^{\mathrm{H}}\boldsymbol{a}\tag{25}$$

将式(24)、式(25)代入对式(12)的求导过程中，即可得到式(14)、式(15)。

参考文献：

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

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

[3] NEGI R, GOEL S. Secret communications using artificial noise[A]. IEEE Vehicular Technology Conference[C]. Dallas, USA, 2005.1906-1910.

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

[5] LI X, HWU J, RATAZZI E P. Array redundancy and diversity for wireless transmissions with low probability of interception[A]. IEEE International Conference on Acoustics, Speech and Signal Processing[C]. Toulouse, France, 2006.211-221.

[6] LI X, HWU J, RATAZZI E P. Using antenna array redundancy and channel diversity for secure wireless transmissions[J]. Journal of Communications, 2007, 2(3): 224-232.

[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, 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]. Science China, 2012, 42(4): 483-492.

[8] ZHOU X, MCKAY M R. Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation[J]. IEEE Transactions on Vehicular Technology, 2010, 59(8): 3831-3842.

[9] YANG Y C, WANG W, HUI Z. Transmitter beamforming and artificial noise with delayed feedback: secrecy rate and power allocation[J]. IEEE Journal on Communications and Networks, 2012, 14(4): 374-384.

[10] LI H, WANG W J, YIN Q Y. A MUSIC-like blind co-channel signals separation algorithm and its performance analysis, circuits and systems[A]. IEEE International Symposium on Circuits and Systems[C]. Taipei, China, 2009. 844-847.

[11] LUENBERGER D. Optimization by Vector Space Methods[M]. New York: Wiley, 1969.

[12] 3GPP2 C. S0024-A, cdma2000 High Rate Packet Data Air Interface Specification-part 13: SUBTYPE 2 Physical Layer-Modulation Characteristics[S]. 2006.

作者简介：

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，主要研究方向为通信信号处理与无线物理层安全。

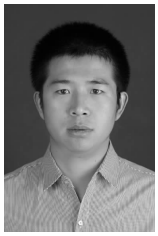
金梁（1969-），男，北京人，国家数字交换系统工程技术研究中心教授、博士生导师，主要研究方向为超宽带无线通信、智能天线以及通信信号处理。

黄开枝（1973-），女，安徽来安人，国家数字交换系统工程技术研究中心教授、硕士生导师，主要研究方向为移动通信与无线网络安全。

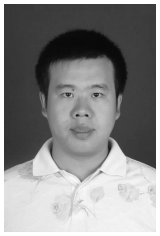
钟州（1982-），男，吉林省吉林市人，国家数字交换系统工程技术研究中心讲师，主要研究方向为移动通信、信道编码与无线物理层安全。

（上接第 73 页）

作者简介：



王亮（1986-），男，陕西乾县人，西安电子科技大学博士生，主要研究方向为认知网络 MAC 协议、认知网络能效。



张琰（1983-），男，河南开封人，博士，西安电子科技大学副教授，主要研究方向为无线分布式网络、协作通信、认知网络。

盛敏（1975-），女，湖南长沙人，西安电子科技大学教授、博士生导师，主要研究方向为移动 ad hoc 网络、QoS 保障技术、认知网络。

马骁（1984-），男，陕西咸阳人，西安电子科技大学博士生，主要研究方向为无线通信、异构网络融合。