文章编号：2095-4980(2016)02-0263-07

方向调制技术分布式加权窃密方法

郭　彬，杨育红，王　彬，辛　刚

(信息工程大学 信息系统工程学院，河南 郑州 450001)

摘　要：针对方向调制物理层安全技术提出了一种分布式加权窃密方法。分析了分布式窃密的可能性，指出窃听者可以实现窃密的本质原因是能够利用多个窃听信道对合法信道进行拟合，消除信号星座点畸变和干扰。然后针对具有恒模特性的相移键控(PSK)信号，设计了分布式接收模型和基于修正恒模的加权窃密方法。最后仿真了分布式窃密方法的性能，从理论上指出方向调制信号在一定条件下仍然是不安全的。

关键词：物理层安全；方向调制；窃密；分布式接收

中图分类号：TN918.8　　**文献标识码**：A　　**doi**：10.11805/TKYDA201602.0263

A distributed eavesdropping method for directional modulation

GUO Bin, YANG Yuhong, WANG Bin, XIN Gang

(Institute of Information System Engineering, Information Engineering University, Zhengzhou Henan 450001, China)

Abstract: A distributed eavesdropping method for directional modulation is proposed. Firstly, the possibility of distributed eavesdropping is analyzed, and it is pointed out that the eavesdroppers can use sufficient illegal channels to imitate the legitimate channel and eliminate the interference. Then, the constant modulus property of Phase-Shift-Keying(PSK) modulation is applied to design a distributed receive approach and a theft weighted algorithm. Simulation results show the eavesdropping method could get confidential message, pointing out that directional modulation technology still remains unsafe in theory.

Key words: physical layer security; directional modulation; eavesdropping; distributed receive

物理层安全技术在信息安全尤为重要的今天受到了越来越多研究者的关注，相对于传统加密技术，其优点是不依赖于加密算法的复杂度，而是充分利用信道的特性来保证通信安全。方向调制(Directional Modulation，DM)技术是一种应用于视距通信的物理层安全技术，能形成与方位角相关的通信信号：星座图在期望方向上正常，而在其他方向发生畸变，进而保证合法用户正常通信的同时提高窃听者误码率，能有效避免旁瓣泄密[1−7]。

自 Babakhani A 最早提出具有方向性特征的通信信号[1]以来，方向调制技术已经有了很大的发展。Michael P Daly 利用相控阵天线，使用波束成型技术实现了方向调制[2]，随后洪涛等在此基础上进行了优化并将方向调制和测向技术进行了结合[3−4]。Yuan Ding 等人首次将向量作为工具对阵列天线 DM 信号进行了设计和分析，把阵列激励分为信息激励和干扰激励，利用处于合法信道零空间的向量形成干扰激励，根据是否动态更新干扰激励分为静态 DM 和动态 DM[5]。方向调制理论目前已经有较为深入的研究，一些学者已经在实验室中实现了实际测试系统[6−7]，但是目前人们对方向调制技术安全性的认识仅仅停留在通过扭曲或者扰乱星座点来保证安全的直观理解，缺乏足够的安全评估。窃听者能否设计一些具有针对性的窃密技术去对抗 DM，这方面的工作内容还未见刊出。

基于此，本文研究了一种针对方向调制信号的分布式加权窃密方法。首先假设窃听者在空间多个方位角位置布置多个接收机，证明了当非法接收机数目大于或等于发射机阵列天线根数的时候，存在一组权值使得窃听者可以用加权相加的方法对扭曲的星座进行校正。针对窃听者信道状态信息未知的情况下，给出了分布式接收模型并结合修正恒模均衡算法设计了窃密方案，最后仿真分析了该窃密方法的性能。

收稿日期：2015-07-20；**修回日期**：2015-09-15

基金项目：国家自然科学基金资助项目(61379006,61171108)

1 系统模型及方向调制原理

图 1 给出了阵列天线方向调制发射机模型，通信时信息序列直接控制激励向量变化。假设发射机采用 N_A 元均匀直线阵，阵元间距为载波波长一半即 $\lambda/2$，发射 M 进制相位调制信号 MPSK。

不考虑自由空间的衰减，阵列天线对应的视距信道向量可写作：

$$\boldsymbol{H}(\theta)=\left[\mathrm{e}^{\mathrm{j}\pi[1-(\frac{N_A+1}{2})\cos\theta]}\ \mathrm{e}^{\mathrm{j}\pi[2-(\frac{N_A+1}{2})\cos\theta]}\cdots\mathrm{e}^{\mathrm{j}0}\cdots\mathrm{e}^{\mathrm{j}\pi[N_A-1-(\frac{N_A+1}{2})\cos\theta]}\ \mathrm{e}^{\mathrm{j}\pi[N_A-(\frac{N_A+1}{2})\cos\theta]}\right]^{\mathrm{T}} \tag{1}$$

发送符号 u 对应的阵列天线激励向量为：

$$\boldsymbol{S}=A\boldsymbol{P}u+\boldsymbol{V} \tag{2}$$

即激励向量为信息激励 $A\boldsymbol{P}u$ 和干扰激励 $\boldsymbol{V}$ 之和，假设合法接收机所在的方位角为 θ_0，则其中的波束成型向量 $\boldsymbol{P}=\dfrac{\boldsymbol{H}(\theta_0)}{\|\boldsymbol{H}(\theta_0)\|}$，$u$ 代表发送符号，A 表示幅度值，$\boldsymbol{V}$ 处于 $\boldsymbol{H}(\theta_0)^{\mathrm{H}}$ 的零空间，$\boldsymbol{S}$，$\boldsymbol{P}$ 和 $\boldsymbol{V}$ 均为 $N_A\times1$ 维复数列向量。

合法接收机收到的信号为：

$$y_{\mathrm{B}}=\boldsymbol{H}(\theta_0)^{\mathrm{H}}\boldsymbol{S}+n_{\mathrm{B}}=A\boldsymbol{H}(\theta_0)^{\mathrm{H}}\boldsymbol{P}u+\boldsymbol{H}(\theta_0)^{\mathrm{H}}\boldsymbol{V}+n_{\mathrm{B}}=A\|\boldsymbol{H}(\theta_0)\|u+n_{\mathrm{B}} \tag{3}$$

式中：$\boldsymbol{H}(\theta_0)^{\mathrm{H}}$ 表示 $\boldsymbol{H}(\theta_0)$ 的共轭转置向量；n_{B} 为加性复高斯噪声。

假设窃听者接收机所在方位角为 θ_n，一般而言 $\theta_0\neq\theta_n$，那么窃听者接收到的信号为：

$$y_{\mathrm{E}}=\boldsymbol{G}(\theta_n)^{\mathrm{H}}\boldsymbol{S}+n_{\mathrm{E}}=\boldsymbol{G}(\theta_n)^{\mathrm{H}}A\boldsymbol{P}u+\boldsymbol{G}(\theta_n)^{\mathrm{H}}\boldsymbol{V}+n_{\mathrm{E}}=A\frac{\boldsymbol{G}(\theta_n)^{\mathrm{H}}\boldsymbol{H}(\theta_0)}{\|\boldsymbol{H}(\theta_0)\|}u+\boldsymbol{G}(\theta_n)^{\mathrm{H}}\boldsymbol{V}+n_{\mathrm{E}} \tag{4}$$

式中：$\boldsymbol{G}(\theta_n)$ 是窃听信道的信道向量，形式与式(1)相同；n_{E} 为加性复高斯噪声。干扰激励 $\boldsymbol{V}$ 与 $\boldsymbol{G}(\theta_n)$ 并不正交，所以 $\boldsymbol{G}(\theta_n)^{\mathrm{H}}\boldsymbol{V}\neq0$，从而对信息 u 带来了扰乱。设 $\boldsymbol{H}(\theta_0)$ 零空间标准正交基向量为 $\boldsymbol{V}_p(p=1,2,\cdots,N_A-1)$，那么干扰激励可以设置为：

$$\boldsymbol{V}=\frac{1}{N_A-1}\sum_{p=1}^{N_A-1}\boldsymbol{V}_p\cdot v_p \tag{5}$$

式中 v_p 为一随机变量。

根据是否动态更新 $\boldsymbol{V}$，可将方向调制分为动态方向调制和静态方向调制[5]，动态方向调制每发送一个符号，$\boldsymbol{V}$ 随机发生变化；静态方向调制每种符号唯一对应一个干扰激励向量，方位角固定后星座图样式固定不变。

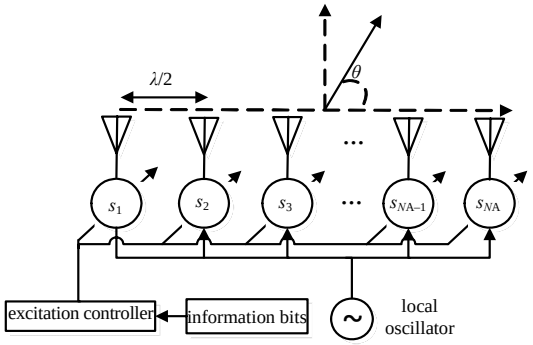

Fig.1 Phased array directional modulation transmitter
图 1 阵列天线 DM 发射机模型

为了衡量干扰激励占用功率的大小，定义方向调制效率 PE_{DM}：

$$PE_{\mathrm{DM}}=\frac{E(\|A\boldsymbol{P}u\|)}{E(\|A\boldsymbol{P}u+\boldsymbol{V}\|)}=\frac{A^2}{A^2+E[\sum_{p=1}^{N_A-1}(\frac{1}{N_A-1}\cdot v_p)^2]} \tag{6}$$

其含义是信息激励平均功率与方向调制激励平均功率之比。

2 分布式加权窃密方法

2.1 分布式窃密可能性分析

假设窃听者会在空间内 N_E 个方位角布置 N_E 个单天线接收机，对应的方位角为 $\theta_n,n=1,2,3,\cdots,N_E$，各非法接收机的信道信息为 $\boldsymbol{G}(\theta_n)$，多个接收机可以通过相互协作实现符号的同步对齐。可以将多个窃听者接收机信道视为一个广义的窃听信道：

$$\boldsymbol{G}=[\boldsymbol{G}(\theta_1)\,\boldsymbol{G}(\theta_2)\,\boldsymbol{G}(\theta_3)\cdots\boldsymbol{G}(\theta_{N_E})] \tag{7}$$

窃听者多个接收机在时刻 k 接收无噪信号为：

$$\boldsymbol{Y}_E(k)=\boldsymbol{G}^{\mathrm{H}}\boldsymbol{S}=\left[y_1(k),y_2(k),y_3(k),\cdots,y_{N_E}(k)\right]^{\mathrm{T}} \tag{8}$$

下面分析窃听者可以通过对 $\boldsymbol{Y}_E(k)$ 内元素通过加权相加方法实现信息恢复。

假设对信号元素使用的加权集合为 $\boldsymbol{W}=\left[w_1,w_2,w_3,\ldots,w_{N_E}\right]^{\mathrm{T}}$，则 $\boldsymbol{Y}_E(k)$ 加权相加后输出符号为:

$$\begin{aligned}z(k)=\boldsymbol{W}^{\mathrm{T}}\boldsymbol{Y}_E(k)=w_1y_1(k)+w_2y_2(k)+w_3y_3(k)\cdots w_{N_E}y_{N_E}(k)=\\ A\left[w_1\boldsymbol{G}(\theta_1)^{\mathrm{H}}+w_2\boldsymbol{G}(\theta_2)^{\mathrm{H}}+\cdots+w_{N_E}\boldsymbol{G}(\theta_{N_E})^{\mathrm{H}}\right]\cdot\frac{\boldsymbol{H}(\theta_0)}{\left\|\boldsymbol{H}(\theta_0)\right\|}u+\\ \left[\left[w_1\boldsymbol{G}(\theta_1)^{\mathrm{H}}+w_2\boldsymbol{G}(\theta_2)^{\mathrm{H}}+\cdots+w_{N_E}\boldsymbol{G}(\theta_{N_E})^{\mathrm{H}}\right]\right]\cdot\boldsymbol{V}\end{aligned} \tag{9}$$

为了消除干扰项，需满足:

$$\left[w_1\boldsymbol{G}(\theta_1)^{\mathrm{H}}+w_2\boldsymbol{G}(\theta_2)^{\mathrm{H}}+\cdots+w_{N_E}\boldsymbol{G}(\theta_{N_E})^{\mathrm{H}}\right]\cdot\boldsymbol{V}=0 \tag{10}$$

即综合后的各窃听者的信道向量应与 $\boldsymbol{V}$ 正交，不妨令:

$$w_1\boldsymbol{G}(\theta_1)+w_2\boldsymbol{G}(\theta_2)+\cdots+w_{N_E}\boldsymbol{G}(\theta_{N_E})=\boldsymbol{H}(\theta_0) \tag{11}$$

因为 $\boldsymbol{V}$ 处在 $\boldsymbol{H}(\theta_0)^{\mathrm{H}}$ 的零空间，所以此时满足式(10)，式(11)展开即为:

$$\begin{bmatrix}G_1(\theta_1) & G_1(\theta_2) & G_1(\theta_3) & \cdots & G_1(\theta_{N_E})\\ G_2(\theta_1) & G_2(\theta_2) & G_2(\theta_3) & \cdots & G_2(\theta_{N_E})\\ G_3(\theta_1) & G_3(\theta_2) & G_3(\theta_3) & \cdots & G_3(\theta_{N_E})\\ \vdots & \vdots & \vdots & & \vdots\\ G_{N_A}(\theta_1) & G_{N_A}(\theta_2) & G_{N_A}(\theta_3) & \cdots & G_{N_A}(\theta_{N_E})\end{bmatrix}\begin{bmatrix}w_1\\ w_2\\ w_3\\ \vdots\\ w_{N_E}\end{bmatrix}=\begin{bmatrix}H_1(\theta_0)\\ H_2(\theta_0)\\ H_3(\theta_0)\\ \vdots\\ H_{N_A}(\theta_0)\end{bmatrix} \tag{12}$$

可见对 $\boldsymbol{W}$ 的求解等价于对上式方程的求解，该式给出了多个窃听者能够联合窃密的本质原因，即利用多个窃听信道的信道状态信息拟合出合法信道的信道状态信息，此时，无论是静态 DM 还是动态 DM，都能够通过多个方向信号加权相加的方法消除干扰激励的影响。

根据线性代数知识，可知式(12) $\boldsymbol{G}\cdot\boldsymbol{W}=\boldsymbol{H}(\theta_0)$ 有解的充分必要条件是 $\boldsymbol{G}$ 的秩等于增广矩阵 $\boldsymbol{B}=(\boldsymbol{G},\boldsymbol{H}(\theta_0))$ 的秩，即:

$$rank(\boldsymbol{G})=rank(\boldsymbol{B}) \tag{13}$$

下面就窃听者接收机数目与发射机使用天线根数的大小关系以及权值 $\boldsymbol{W}$ 解的存在性给出结论和证明:

a) 当 $N_E=N_A$，接收机数目等于合法发射机天线根数，那么权值 $\boldsymbol{W}$ 存在唯一解;

b) 当 $N_E>N_A$ 时，即非法接收机数目大于合法发射机天线根数，$\boldsymbol{W}$ 存在无穷多解;

c) 当 $N_E<N_A$ 时，即非法接收机数目小于合法发射机天线根数，$\boldsymbol{W}$ 解不存在，窃听者不能完全消除干扰激励的影响。

证明:

式(1)的 $\boldsymbol{H}(\theta)$ 在以第 1 根天线作为参考天线时，实际上也可以写作:

$$\boldsymbol{H}(\theta)=\left[1\ \ \mathrm{e}^{\mathrm{j}\pi\cos\theta}\ \cdots\ \mathrm{e}^{\mathrm{j}\pi(N_A-2)\cos\theta}\ \ \mathrm{e}^{\mathrm{j}\pi(N_A-1)\cos\theta}\right]^{\mathrm{T}} \tag{14}$$

同理 $\boldsymbol{G}(\theta)$ 也可以写作该形式。

当 $N_E=N_A$，容易验证 $\boldsymbol{G}$ 是 N_E 阶 Vandermonde 矩阵，当 $\theta_i,i=1,2,3,\cdots,N_E$ 互不相同时，$\boldsymbol{G}$ 非奇异，此时 $\boldsymbol{G}$ 是满秩矩阵，此时存在唯一解[8]。

当 $N_E>N_A$，$\boldsymbol{G}$ 是 $N_A\times N_E$ 阶 Vandermonde 矩阵，$\boldsymbol{B}$ 是 $N_A\times(N_E+1)$ 阶 Vandermonde 矩阵，由 Vandermonde 矩阵性质可知 $rank(\boldsymbol{G})=rank(\boldsymbol{B})=N_A<N_E$，所以此时 $\boldsymbol{W}$ 存在无穷多解;

当 $N_E<N_A$，由 Vandermonde 矩阵的有关结论可知，$rank(\boldsymbol{G})=N_E$ 即 $\boldsymbol{G}$ 是列满秩的，同理 $rank(\boldsymbol{B})=N_E+1$，此时，$rank(\boldsymbol{G})<rank(\boldsymbol{B})$，因此 $\boldsymbol{W}$ 的解不存在。

实际中，窃听者很难获取窃听信道和合法信道的状态信息，因此下面仅研究在未知信道状态信息情况下的窃密方法。

2.2 分布式接收模型

采用的分布式接收模型如图 2 所示，窃听者将 N_E 个接收机布置在 N_E 个方向上，多个接收机将截获到的符

号传输至汇聚中心，由于发射机到达多个接收机的信道不同，多个接收机可能会接收不同时刻的信息符号，汇聚中心需要对多个接收机的符号进行同步对齐，这个过程可以使用多天线增强接收的同步对齐算法如 ETDE、SIMPLE 算法[9]实现，在此仅研究符号完全对齐假设下的权值获取问题，符号同步对齐技术不做探讨。

2.3 加权分布式窃密方法

汇聚中心经过同步对齐后输出了 K 个符号周期的信号 $\boldsymbol{Y}_E=[\boldsymbol{Y}_E(1),\boldsymbol{Y}_E(2),\boldsymbol{Y}_E(3),\cdots,\boldsymbol{Y}_E(K)]$，其中 $\boldsymbol{Y}_E(k)=\left[y_1(k),y_2(k),y_3(k),\cdots,y_{N_E}(k)\right]^{\mathrm{T}}$，$k=1,2,3,\cdots,K$。针对方向调制信号为恒模特性的 PSK 信号，文献[10]提出的一种 MCMA 算法启发，下面阐述一种改进常数模算法(Modified Constant Modulus Algorithm，MCMA)的加权窃密方法。

MCMA 对信号的实部和虚部分开进行均衡，使得最终分别收敛于近似的 2 个值，这样就消除了相位偏移，比较适用于方向调制中的星座畸变恢复。

设第 n 次迭代的权值为 $\boldsymbol{W}(n)$，长度为 $2N+1$，输入符号为 $\boldsymbol{X}(n)=[x(n+N),x(n+N-1),\cdots,x(n-N)]^{\mathrm{T}}$，输出符号为 $z(k)=\boldsymbol{W}^{\mathrm{T}}\bullet\boldsymbol{X}$。

该算法每次迭代的误差函数分为实部和虚部 2 部分：

$$\boldsymbol{e}(n)=\boldsymbol{e}_{\mathrm{R}}(n)+\mathrm{j}\boldsymbol{e}_{\mathrm{I}}(n) \tag{15}$$

$$\boldsymbol{e}_{\mathrm{R}}(n)=z_{\mathrm{R}}(n)[z_{\mathrm{R}}(n)^2-\boldsymbol{R}_{\mathrm{R}}] \tag{16}$$

$$\boldsymbol{e}_{\mathrm{I}}(n)=z_{\mathrm{I}}(n)[z_{\mathrm{I}}(n)^2-\boldsymbol{R}_{\mathrm{I}}] \tag{17}$$

式中

$$\boldsymbol{R}_{\mathrm{R}}=\frac{E\left|u_{\mathrm{R}}\right|^4}{E\left|u_{\mathrm{R}}\right|^2} \tag{18}$$

$$\boldsymbol{R}_{\mathrm{I}}=\frac{E\left|u_{\mathrm{I}}\right|^4}{E\left|u_{\mathrm{I}}\right|^2} \tag{19}$$

u_{R} 和 u_{I} 为输入信号 u 的实部和虚部，权值更新规则为：

$$\boldsymbol{W}(n+1)=\boldsymbol{W}(n)-\mu\boldsymbol{e}(n)\boldsymbol{X}^*(k) \tag{20}$$

以上是 MCMA 算法的主要内容，但是应用在方向调制中会存在以下问题：

a) MCMA 输入 $\boldsymbol{X}(k)$ 为不同时刻的信息序列，而方向调制利用的是同一时刻不同方位的序列 $\boldsymbol{Y}_E(k)$；

b) 不同方位的接收信号经过不同的信道，幅值、信噪比、畸变程度均不相同，初始权值应当有所差异；

c) 对于窃听者而言符号 u 无法获取，因此 $\boldsymbol{R}_{\mathrm{R}}$ 和 $\boldsymbol{R}_{\mathrm{I}}$ 无法得到，不同方位的信号幅度星座点扭曲程度不同，无法对数据进行归一化预处理。

对此采用以下改进的加权窃密算法。

对于第 1 个问题，采用如图 2 的窃密模型，加权符号不再是一段时间的符号序列，而是某个时刻多个方位角的符号序列，在时刻 k 输出符号为 $z(k)=\boldsymbol{W}^{\mathrm{T}}\bullet\boldsymbol{Y}_E(k)$。

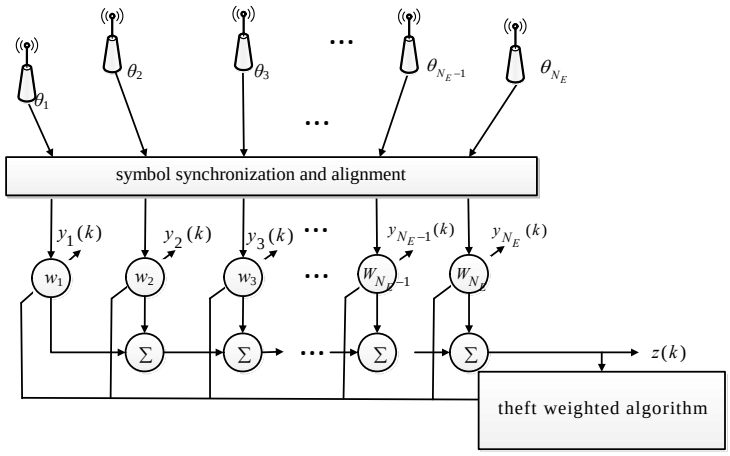

Fig.2 Distributed eavesdropping model

图 2 分布式接收模型

对于第 2 个问题可以通过适当的权值初始化完成，初始化权值的取值原理表述如下：

直观上理解应当对畸变程度低的方位信号赋予较大的权值，而对于畸变程度大的方位信号应当赋予较小的权值，因此需要衡量不同方位的信号接收质量。

误差向量幅度(Error Vector Magnitude，EVM)，是理想无误差基准信号与实际信号的向量差，能够衡量方向

调制信号的幅度误差和相位误差[11]，数学定义为：

$$EVM=\left[\frac{\frac{1}{T}\sum_{i=1}^{T}\left|S_{\text{meas}\_i}-S_{\text{ref}\_i}\right|^2}{\frac{1}{T}\sum_{i=1}^{T}\left|S_{\text{ref}\_i}\right|^2}\right]^{1/2} \tag{21}$$

式中：S_{meas_i}和S_{ref_i}分别表示第i个符号的测量值和参考标准值；T为一段时间内符号的长度。实际中，很难知道不同方位角的S_{ref_i}，因此将同等功率下的标准符号作为参考标准值，即：

$$\sum_{i=1}^{T}\left|S_{\text{ref}\_i}\right|^2=\sum_{i=1}^{T}\left|S_{\text{meas}\_i}\right|^2 \tag{22}$$

可以算出$\left|S_{\text{ref}_i}\right|$，下一步将修正误差向量幅度 MEVM(Modified Error Vector Magnitude)作为衡量标准：

$$MEVM=\left[\frac{\frac{1}{T}[\sum_{i=1}^{T}\left\|S_{\text{meas}\_i}^{\text{R}}\right|-\left|S_{\text{ref}\_i}^{\text{R}}\right\|^2+\left\|S_{\text{meas}\_i}^{\text{I}}\right|-\left|S_{\text{ref}\_i}^{\text{I}}\right\|^2]}{\frac{1}{T}\sum_{i=1}^{T}\left|S_{\text{ref}\_i}\right|^2}\right]^{1/2} \tag{23}$$

式中：$S_{\text{meas}_i}^{\text{R}}, S_{\text{meas}_i}^{\text{I}}$分别表示$S_{\text{meas}_i}$的实部和虚部；$S_{\text{ref}_i}^{\text{R}}, S_{\text{ref}_i}^{\text{I}}$分别表示$S_{\text{ref}_i}$的实部和虚部，对于 QPSK 信号而言$\left|S_{\text{ref}_i}^{\text{R}}\right|=\left|S_{\text{ref}_i}^{\text{I}}\right|=\frac{\sqrt{2}}{2}\left|S_{\text{ref}_i}\right|$。

MEVM 值越大，表示信号发生的畸变越严重，应当赋予的初始值越小，因此可令：

$$\boldsymbol{W}_{\theta}(0)=\frac{1}{MEVM(\theta)} \tag{24}$$

对于第 3 个问题，将输出符号$z(k)$替代为信息符号u，即：

$$\boldsymbol{R}_{\text{R}}=\frac{E\left|z_{\text{R}}\right|^4}{E\left|z_{\text{R}}\right|^2} \tag{25}$$

$$\boldsymbol{R}_{\text{I}}=\frac{E\left|z_{\text{I}}\right|^4}{E\left|z_{\text{I}}\right|^2} \tag{26}$$

3　仿真与性能分析

对本文提出的分布式窃密方法进行仿真验证，假设方向调制阵列天线根数$N_A=5$，动态 DM 和静态 DM 设置期望通信方向的方位角均为 45°。6 个窃听接收机布置在方位角为 25°,30°,35°, 55°,60°,65°的 6 个方位，空间内所有位置存在相同功率谱密度的加性高斯白噪声，使用 2 000 个训练序列，迭代 2 000 次。

3.1 算法的收敛性及初始化权值性能仿真

比较本文提出的权值初始化方法和一般权值性能，设$\boldsymbol{W}_A$为本文提出的利用 MEVM 权值，$\boldsymbol{W}_B=[1,1,1,1,1,1]^{\text{T}}$为对比权值初始值。设置 2 种方向调制的$PE_{\text{DM}}$为 0.5，即干扰激励功率与信息激励功率相同。图 3 表示了静态 DM 和动态 DM 2 种情况下的输出符号均方误差 MSE(Mean Square Error)与迭代次数的关系，可见算法能够进行收敛，并且与一般权值相比，采用 MEVM 权值加快了算法的收敛速度。

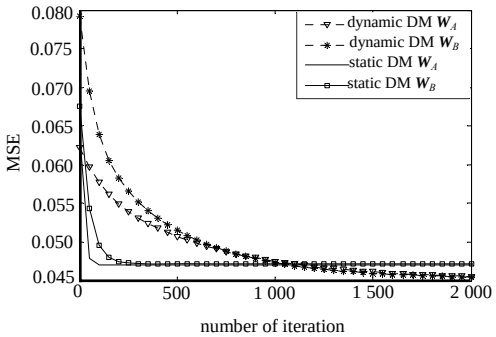

Fig.3 MSE versus the iteration number
图 3 输出符号 MSE 与迭代次数关系

3.2 窃密性能仿真

设合法接收机 45°方位角R_{SN}=10 dB，其他方向具有相同功率大小的高斯加性噪声，2 种方向调制的PE_{DM}为 0.5。图 4a 为动态方向调制 6 个窃听者方位角星座图，图 4b 为加权窃密方法输出信号星座图，可见，该窃密方法能够有效消除动态干扰激励的影响。

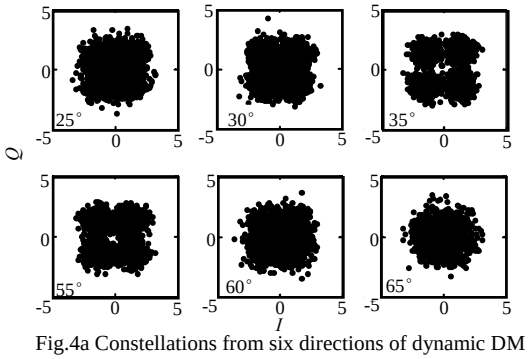

Fig.4a Constellations from six directions of dynamic DM
图 4a 动态 DM 6 个方位角星座图

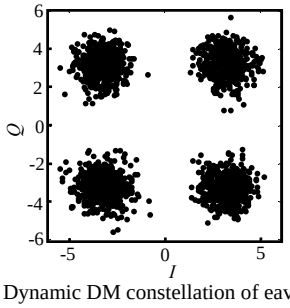

Fig.4b Dynamic DM constellation of eavesdropper
图 4b 动态 DM 加权窃密后的星座图

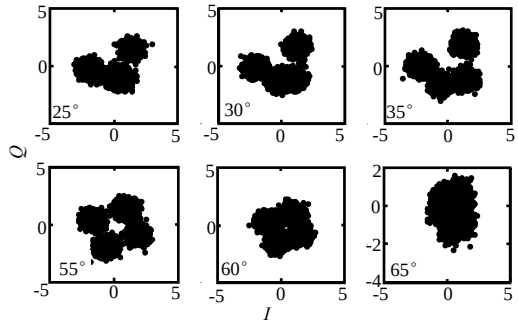

Fig.5a Constellations from six directions of static DM
图 5a 静态 DM 6 个方位角星座图

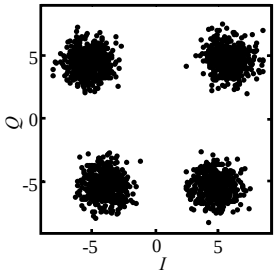

Fig.5b Static DM constellation of eavesdropper
图 5b 静态 DM 窃密输出星座图

图 5a 表示了静态 DM 6 个窃听者方位角接收星座图；图 5b 为静态 DM 加权窃密方法输出星座图，与动态 DM 窃密结果相比虽然仍存在一定程度的畸变，但是星座点的收敛性相对较好。(图中 Q,I 表示星座点的 Q 路和 I 路分量)。

图 6 表示了干扰激励功率取不同值时(即 PE_{DM} 取不同值时)，动态 DM 和静态 DM 以及合法接收机的误码率随着期望方向 45° 信噪比的变化曲线。

可以看到随着信噪比的提高，2 种方向调制窃听者均能得到很低的误码率，这表明分布式加权窃密方法能够有效对抗 2 种方向调制技术。静态方向调制的误码率始终低于动态方向调制的误码率，这说明动态 DM 的安全性要优于静态 DM。2 种方向调制的误码率随着干扰激励功率的增大(PE_{DM} 变小)，窃密性能有所下降，说明强干扰激励有助于提高方向调制的安全性能，但是牺牲了额外的功率。另一方面期望方向上合法者接收机的误码率始终高于 2 种窃密方法得到的误码率，这是由于分布式窃密方法利用多天线联合接收合成的思想在矫正方向调制畸变的同时提高了通信信号的信噪比。

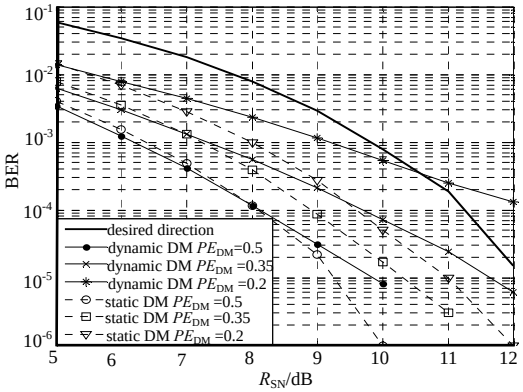

Fig.6 BER versus SNR of eavesdropper
图 6 窃密输出误码率与信噪比关系曲线

4 结论

针对方向调制物理层安全技术的窃密问题，本文提出了一种加权窃密方法，指出结合分布式接收和恒模均衡 2 种手段能够对抗方向调制技术，因此可以认为利用正交向量原理形成的方向调制信号在一定程度上是不安全的，并且相对于动态方向调制技术，静态方向调制的安全性能更差。需要指出的是本文采用的加权窃密算法是在分布式接收符号完全对齐的假设下进行的，实际中符号对齐存在误差的情况下窃密算法的性能还有待进一步研究。

参考文献：

[1] BABAKHANI A,RUTLEDGE D B,HAJIMIRI A. Transmitter architectures based on near-field direct antenna modulation[J]. Solid-State Circuits,IEEE Journal of, 2008,43(12):2674–2692.

[2] DALY M P,BERNHARD J T. Directional modulation technique for phased arrays[J]. Antennas and Propagation,IEEE Transactions on, 2009,57(9):2633–2640.

[3] 洪涛,宋茂忠,刘渝. 多目标遗传算法方向调制物理层安全通信信号设计[J]. 应用科学学报, 2014,32(1):51–56.(HONG Tao,SONG Maozhong,LIU Yu. Design of directional modulation signal based on multi-objective genetic algorithm for physical layer secure communication[J]. Journal of Applied Sciences, 2014,32(1):51–56.)

[4] 洪涛. 方向调制在物理层安全通信和通信测向综合系统中的应用研究[D]. 南京:南京航空航天大学, 2012. (HONG Tao. Research on directional modulation for the physical layer security communication and the integration system with communication and direction-finding[D]. Nanjing,China:Nanjing University of Aeronautics and Astronautics, 2012.)

[5] DING Y,FUSCO V F. A vector approach for the analysis and synthesis of directional modulation transmitters[J]. Antennas and Propagation,IEEE Transactions on, 2014,62(1):361–370.

[6] ZHU Quanjiang,YANG Shiwen,YAO Ruilin,et al. Directional modulation based on 4-D antenna arrays[J]. Antennas and Propagation, IEEE Transactions on, 2014,62(2):621–628.

[7] DING Y,ZHANG Y,FUSCO V. Fourier Rotman lens enabled directional modulation transmitter[J]. International Journal of Antennas and Propagation, 2015:1–13.

[8] 张贤达. 矩阵分析与应用[M]. 北京:清华大学出版社, 2013:120–122. (ZHANG Xianda. Matrix Analysis and Applications[M]. Beijing:Tsinghua University Press, 2013:120–122.)

[9] 沈彩耀. 多天线联合接收的合成技术研究[D]. 郑州:信息工程大学, 2011. (SHEN Caiyao. Research on the combining techniques on joint reception for multi-antenna signals[D]. Zhengzhou,China:University of Information Engineering, 2011.)

[10] KIL Nam Oh,YONG Ohk Chi. Modified constant modulus algorithm:blind equalization and carrier phase recovery algorithm[C]// Communications,ICC 95 Seattle,Gateway to Globalization. Seattle,WA:IEEE, 1995:498–502.

[11] FORESTIER S,BOUYSSE P,QUERE R,et al. Joint optimization of the power-added efficiency and the error-vector measurement of 20-GHz pHEMT amplifier through a new dynamic bias-control method[J]. Microwave Theory and Techniques,IEEE Transactions on, 2004,52(4):1132–1141.

作者简介：

郭　彬(1990–)，男，河北省保定市人，在读硕士研究生，主要研究方向为无线通信物理层安全.email:dcr_2013@163.com.

杨育红(1964–)，女，南昌市人，副教授，主要研究方向为卫星通信.

王　彬(1970–)，女，郑州市人，副教授，主要研究方向为通信信号处理.

辛　刚(1979–)，男，郑州市人，讲师，主要研究方向为通信信号处理.

* *