基于时域参考的物理层安全传输方案*

李明亮[1]，黄开枝[1]，朱　晖[2]
（1. 国家数字交换系统工程技术研究中心，郑州 450000；2. 大唐数据通信科学技术研究所，北京 100000）

摘　要：在 SIMO-OFDM 通信系统中，基于发送端多天线冗余的物理层安全算法不再适用。针对这一问题，提出一种基于时域参考的物理层安全传输方案。合法接收者在各个子载波上构造多天线随机加权向量，使构造的加权向量在合法信道上的投影等于随 OFDM 符号快变的时域参考变量，发送端利用前一时刻接收端构造的参考变量对当前时刻的发送调制符号进行相位旋转。时域参考变量的随机变化，扰乱了窃听者的接收信号星座图，导致其无法正确解调。而合法用户能够利用之前构造的多天线加权向量正确解调接收信号。安全性分析和仿真结果表明，当天线数为 8、信噪比为 10 dB 时，合法用户误比特率达到 10^{-4}，而窃听者始终无法正确解调。

关键词：物理层安全；SIMO-OFDM；多天线随机加权
中图分类号：TN918.82　　**文献标志码**：A　　**文章编号**：1001-3695(2013)12-3738-04
doi:10.3969/j.issn.1001-3695.2013.12.057

Time-domain reference based physical layer security method

LI Ming-liang[1], HUANG Kai-zhi[1], ZHU Hui[2]
(1. *National Digital Switching System Engineering & Technological Research Center*, *Zhengzhou* 450000, *China*; 2. *Datang Data Communication Science & Technology Research Institute*, *Beijing* 100000, *China*)

Abstract: The physical-layer security method based on the transmitter's multi-antenna redundant isn't applicable to the SIMO-OFDM system. To solve the problem, this paper proposed a physical layer security method based on time-domain reference. The legitimate receiver constructs the random multi-antenna vector in each subcarrier, of which the projection in the main channel was equal to the varying time-domain reference variable. The transmitter secured the transmitted signal of this moment with the previous time-domain reference variable. The random variation of the reference variable disturbed the eavesdropper's received signal constellation, so that the eavesdropper couldn't intercept the secret information. Security analysis and simulation results show that the legitimate receiver's BER is 10^{-4}, the eavesdropper couldn't correctly demodulate the received signals when the received SNR and antenna number is respectively 10 dB and 8.

Key words: physical layer security; SIMO-OFDM; random multi-antenna weighting

在现代移动通信系统中，OFDM（orthogonal frequency division multiplexing，正交频分复用）作为一种并行调制技术[1]，具有频谱利用率高、抗多径衰落能力强等优点，通常与多天线技术结合使用。目前保障多天线 OFDM 系统安全的手段依然是高层的密钥加密体制[2,3]，但是由于无线通信的广播特性，密钥的分发和管理存在很大的安全隐患。与此同时，无线通信信道具有多样性、时变性和短时互易性等对安全通信有利的特点，因此出现了一种利用物理层特性保障信息安全传输的新思路。

目前，多天线多载波物理层安全算法主要分为低截获概率算法和提高保密容量的算法。在低截获概率算法中，文献[4]利用收发双方已知的码本，旋转各个子载波发射符号的相位，并且加入噪声扰动，窃听者不知道码本信息，因此无法还原原始发送信息；文献[5]针对 MISO（multiple input single output）模型，首次提出利用天线阵列冗余进行随机加权的方式，扰乱窃听方的接收信号，使其无法对接收信号进行盲信道估计，从而使得系统具有低截获概率；文献[6,7]通过对随机多天线加权方法进行改造，以随机选择发射天线的方式进行加密；文献[8]将随机多天线加权方法应用到保密 MISO-OFDMA 系统中，推导了使得合法用户信道容量最大的用户选择和资源分配方案。在提高保密容量的算法中，文献[9]首次提出通过人工噪声的方式干扰窃听用户的接收信号，从而提高了系统的保密容量。在此基础上，文献[10～12]研究了不同条件下人工噪声方法的保密容量和优化策略；文献[13,14]将人工噪声应用到 MISO-OFDMA 系统中，推导了不同约束条件下使得系统保密容量最大的资源分配方案。上述安全算法均基于发送端的多天线优势构造空域加扰来实现保密通信，但是当通信系统为 SIMO（single input multiple output）模型时，发送端只有一根天线，无法利用现有的多天线物理层安全算法对发送信号进行加密。

针对这一问题，本文提出了一种基于时域参考的物理层安全传输方案。

1　安全模型

针对 SIMO-OFDM 系统，本文构造的安全模型如图 1 所示，移动终端 Alice 通过时分双工的方式与基站 Bob 通信，同时空间中存在一个被动窃听者 Eve；Alice 具有一根天线，Bob 具有 M_B 根天线，Eve 具有 M_E 根天线，各个天线相互独立；假设

收稿日期：2013-03-06；**修回日期**：2013-04-16　**基金项目**：国家自然科学基金资助项目(61171108)；国家“863”高技术研究重大专项基金资助项目(2011AA010604)

作者简介：李明亮(1988-)，男，硕士研究生，主要研究方向为无线通信物理层安全(mingliang186@gmail.com)；黄开枝(1973-)，女，副教授，主要研究方向为移动通信；朱晖，男，高级工程师，主要研究方向为移动通信.

系统采用 OFDM 调制,每个 OFDM 符号具有 N 个子载波,OFDM 符号的持续时间为 T_s,各个子载波信道相互独立,且为慢时变块衰落信道,信道的相干周期为 T_c。由于通信双方在上下行信道发送训练序列,并且 OFDM 符号的循环前缀也会不可避免地暴露定时和信道状态信息,因此,本文假设窃听者能够通过信道估计获得精确的窃听信道的信道状态。

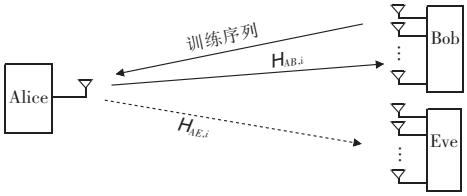

图 1　SIMO-OFDM 系统物理层安全模型

假设信道的最大多径时延小于 OFDM 符号循环前缀的长度。当 Alice 向 Bob 发送信息时,Bob 和 Eve 在第 k 个 OFDM 符号上第 i 个子载波的接收信号可分别表示为

$$y_{B,k,i} = V_{k,i} H_{AB,i} X_{k,i} + z_{AB,i} \tag{1}$$

$$Y_{E,k,i} = H_{AE,i} X_{k,i} + Z_{E,i} \tag{2}$$

其中:$H_{AB,i}$表示 Alice 和 Bob 在第 i 个子载波上的 $M_B \times 1$ 维信道状态矢量;$H_{AE,i}$表示 Alice 和 Eve 在第 i 个子载波上的 $M_E \times 1$ 维信道状态矢量;$X_{k,i}$,$i \in [1,N]$表示第 k 个 OFDM 符号上第 i 个子载波的发送符号;$V_{k,i}$表示第 k 个 OFDM 符号第 i 个子载波上 $1 \times M_B$ 维的接收端波束成型向量;$z_{AB,i}$表示 Bob 在第 i 个子载波上均值为 0、方差为 σ_B^2 的加性高斯白噪声(AWGN)变量;$Z_{E,i}$表示 Eve 在第 i 个子载波上均值为 0、方差为 σ_{AE}^2 的 $M_E \times 1$ 维 AWGN 矢量。

2　基于时域参考的物理层安全传输方案

当信道慢变时,如果 $X_{k,i}$发射符号稳定,Eve 能够根据稳定的接收信号星座图正确解调接收信号。本文利用信道的互易性,通过接收端的多天线构造随机加权向量 $V_{k,i}$,使 $V_{k,i}$在合法信道上的投影等于随 OFDM 符号快变的时域参考变量,并利用此参考变量对发送调制符号进行旋转加密,从而使得 $X_{k,i}$随机变化,导致 Eve 无法正确解调。方案分为两个阶段:在信道检测阶段,合法接收者构造多天线加权向量,并向发送端发送经过加权的训练序列,发送端通过对反向训练序列的检测获得各个子载波信道的时域参考变量;在加密传输阶段,发送端通过资源分配确定各个子载波的调制方式,并利用各个子载波的时域参考变量实现对发送调制符号的旋转加密。

2.1　信道检测

由于 Alice 只有一根天线,当 Bob 利用多天线对接收信号进行接收端波束成型时,信道模型等效为 SISO 模型。假设第 i 个子载波上的调制方式为 M_iPSK,$M_i \in [0,2,4,8,16]$。为了保证安全通信,在 Alice 发送第 k 个 OFDM 符号前,Bob 随机生成第 i 个子载波上的多天线加权向量 $V_{k,i}$,使其满足如下约束:

$$V_{k,i} H_{AB,i} = \partial_{k,i} \| H_{AB,i} \| e^{i\theta_{k,i}},\ \| V_{k,i} \| = 1 \quad i \in [1,N] \tag{3}$$

其中,$\partial_{k,i}$在$[\frac{1}{2},1]$上随机取值,表示第 k 个 OFDM 符号第 i 个子载波上 Alice 和 Bob 间的等效 SISO 信道增益;$\theta_{k,i}$在$[0,2\pi]$上随机取值;$e^{i\theta_{k,i}}$表示第 k 个 OFDM 符号第 i 个子载波上的时域参考变量。

2.2　加密传输

在移动通信系统中,基站和移动终端通常通过互相发送训练序列的方式完成信道估计和系统同步,因此为了使 Alice 完成对等效 SISO 信道的估计,Bob 在各个子载波上发送经过多天线加权的训练序列。Alice 的接收信号可表示为

$$y_{A,k,i} = \partial_{k,i} \| H_{AB,i} \| e^{i\theta_{k,i}} + z_{AB,i} \tag{4}$$

Alice 通过对接收信号进行归一化,获得时域参考变量的估计值为

$$e^{j\theta_{k,i}} = \frac{y_{A,k,i}}{|y_{A,k,i}|} \quad i \in [1,N] \tag{5}$$

为了加密发射信号,Alice 利用 $e^{j\theta_{k,i}}$对调制符号的相位进行旋转加密,第 k 个 OFDM 符号第 i 个子载波上的发送信号可表示为

$$X_{k,i} = s_{k,i} e^{-i\theta_{k,i}} \quad i \in [1,N] \tag{6}$$

其中:$s_{k,i}$为 Alice 在第 k 个 OFDM 符号第 i 个子载波上的调制符号。

Bob 利用各个子载波上事先生成的波束 $V_{k,i}$对各个天线的接收信号进行接收端波束成型,此时由式(1)得第 k 个 OFDM 符号上第 i 个子载波的接收信号为

$$y_{B,k,i} = V_{k,i} H_{AB,i} s_{k,i} e^{-j\theta_{k,i}} + z_{AB,i} \tag{7}$$

将式(3)代入式(7)得

$$y_{B,k,i} = \partial_{k,i} \| H_{AB,i} \| e^{j(\theta_{k,i} - \theta_{k,i})} s_{k,i} + z_{AB,i} \tag{8}$$

Bob 利用最大似然准则解出第 k 个 OFDM 符号第 i 个子载波上的发送数据为

$$\tilde{s}_{k,i} = \arg\min_{s_{k,i}} \| y_{B,k,i} - \partial_{k,i} \| H_{AB,i} \| s_{k,i} \|^2 \tag{9}$$

为了最大化安全通信速率,同时保证有用信号的传输质量,Alice 按照各个子载波的接收信号信噪比进行资源分配,以此来确定在各个子载波上调制方式的阶数 M_i 和发射功率 P_i。在满足通信速率和解调误码率限制的情况下,上述资源分配问题可表示为

$$\max \sum_{i=1}^{N} \mu_i \tag{10}$$

$$\text{subject}: \sum_{i=1}^{N} \frac{1}{r_i^2} f(\mu_i) = P_{\text{total}} \tag{11}$$

其中:$M_i = 2^{\mu_i}$,μ_i 表示分配给第 i 个子载波的比特数;$\frac{\| H_{AB,i} \|}{2} \leqslant r_i \leqslant \| H_{AB,i} \|$代表第 i 个子载波等效 SISO 信道的增益,为了保证系统的误比特率性能,令 $r_i = \frac{\| H_{AB,i} \|}{2}$,即以各个子载波信道的最小信道增益为标准进行资源分配;P_{total}表示系统的总功率,$f(\mu_i)$表示 Bob 以误符号率 η_e 解调接收信号所需的发送信号功率。当通信双方采用的是 PSK 调制时,由文献[15]可知

$$f(\mu_i) = \frac{\sigma_B^2}{2\mu_i \sin^2(\pi/M_i)} [Q^{-1}(\eta_e/2)]^2 \tag{12}$$

其中:$Q(x) = \frac{1}{2}\text{erfc}(\frac{x}{\sqrt{2}})$。由于在各个子载波上传输一定比特所需的功率相互独立,因此通过贪婪算法能得到最优的功率和比特分配方案[16],资源分配算法可表示成如下步骤:

a) 令 $\mu_i = 0$,$i \in [1,N]$,计算 $\Delta p_i = \frac{f(\mu_i + 1) - f(\mu_i)}{r_i^2}$,$i \in [1,N]$;

b) 选择 $j = \underset{i \in [1,N]}{\text{argmin}} \Delta p_i$;

c) $\mu_j = \mu_j + 1$;

d) 判断 $\sum_{i=1}^{N}\frac{1}{r_i^2}f(\mu_i) > P_{\text{total}}$ 是否成立，如果成立，则跳转到 f)；

e) 计算 $\Delta p_i = \frac{f(\mu_i+1)-f(\mu_i)}{r_i^2}$，$i\in[1,N]$，跳转到 b)；

f) $\mu_j = \mu_j - 1$，比特和功率分配过程完成。

其中：Δp_i 表示在第 i 个子载波上增加 1 bit 传输信息所需要的额外功率。分配算法可表述为：在一次迭代过程中，所有子载波上只分配 1 bit，并且把这 1 bit 分配给增加 1 bit 传输信息所需功率最小的子载波。当各个子载波分配的功率之和达到总功率限制时，迭代过程结束。

2.3 方案流程

基于上述分析，此物理层安全算法的发送和接收过程如图 2 所示。

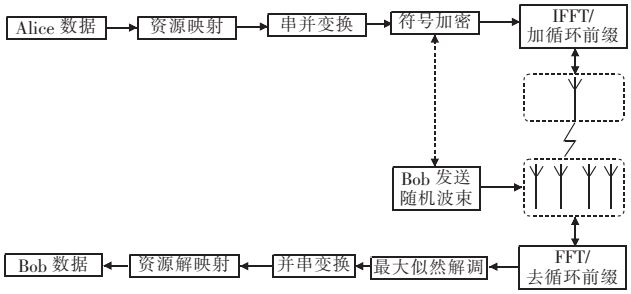

图 2 加密算法发送和接收流程

具体可分为如下步骤：

a) 初始化 $k=1$，Alice、Bob 通过互相发送训练序列建立系统同步。

b) Alice 通过信道估计获得信道状态向量 $H_{AB,i}$，$i\in[1,N]$，按照资源分配算法选择各个子载波上的调制方式，并将此信息通过广播信道发送给 Bob。

c) Bob 按照式(3)随机生成各个子载波的多天线加权向量 $V_{k,i}$，$i\in[1,N]$，然后分别组成 OFDM 符号，通过各个天线发射出去。

d) Alice 对合法信道进行检测，获取时域参考变量，并按照式(5)分别对调制符号进行加密，然后组成 OFDM 符号发射出去。

e) Bob 利用在步骤 c) 中构造的加权向量 $V_{k,i}$，对各个子载波上的接收信号进行接收端波束成型，然后按照式(9)解调各个子载波上的接收信号。

f) $k=k+1$。

g) 当 $kT_s \leqslant T_c/2$ 时，返回 c)。

h) 当 $kT_s > T_c/2$ 时，返回 a)。

3 安全性分析

当 Alice 发送加密信息时，在第 i 个子载波上，由式(2)(6)得 Eve 的接收信号为

$$Y_{AE,k,i} = H_{AE,i}s_{k,i}e^{-i\theta_{k,i}} + Z_{E,i} \tag{13}$$

时域参考变量的估计值 $e^{-i\theta_{k,i}}$ 在 $[0,2\pi]$ 上随机变化，扰乱了 Eve 的接收信号。为了解调加密信号，Eve 必须设法获得 $e^{-i\theta_{k,i}}$。当 Bob 向 Alice 发送反向训练序列时，在第 k 个 OFDM 符号的第 i 个子载波上，Eve 的接收信号可表示为

$$Y_{BE,k,i} = H_{BE,i}V_{k,i}^{\mathrm{T}} + Z_{E,i} \tag{14}$$

其中：$H_{BE,i}$ 表示 Eve 和 Bob 在第 i 个子载波上 $M_E\times M_B$ 维的信道状态矩阵。当 $M_E \geqslant M_B$ 时，通过对信道求逆，Eve 的接收信号可重新表示为

$$\tilde{Y}_{BE,i} = (H_{BE,i}^{\mathrm{H}}H_{BE,i})^{-1}H_{BE,i}^{\mathrm{H}}\begin{bmatrix} Y_{BE,1,i}^{\mathrm{T}} \\ Y_{BE,2,i}^{\mathrm{T}} \\ \vdots \\ Y_{BE,K,i}^{\mathrm{T}}\end{bmatrix}^{\mathrm{T}} = \begin{bmatrix} V_{1,i} \\ V_{2,i} \\ \vdots \\ V_{K,i}\end{bmatrix}^{\mathrm{T}} + \begin{bmatrix} \tilde{Z}_{E,i}^{\mathrm{T}} \\ \tilde{Z}_{E,i}^{\mathrm{T}} \\ \vdots \\ \tilde{Z}_{E,i}^{\mathrm{T}}\end{bmatrix}^{\mathrm{T}} \tag{15}$$

其中：$\tilde{Z}_{E,i}^{\mathrm{T}}$ 表示对信道求逆后的信道噪声；$\tilde{Y}_{BE,i}$ 表示 Eve 接收 K 个 OFDM 符号后，在第 i 个子载波上 $M_B\times K$ 维的时域累积信号矩阵。同样，式(3)可重新表示为

$$\underbrace{\begin{bmatrix} V_{1,i} \\ V_{2,i} \\ \vdots \\ V_{K,i}\end{bmatrix}}_{\Delta V_i} H_{AB,i} = \|H_{AB,i}\| \underbrace{\begin{bmatrix} \partial_{1,i} & 0 & \cdots & 0 \\ 0 & \partial_{2,i} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \partial_{K,i}\end{bmatrix}}_{\Delta\alpha_i} \underbrace{\begin{bmatrix} e^{i\theta_{1,i}} \\ e^{i\theta_{2,i}} \\ \vdots \\ e^{i\theta_{K,i}}\end{bmatrix}}_{\Delta\theta_i} \quad i\in[1,N] \tag{16}$$

其中：$\Delta\theta_i$ 表示 K 个 OFDM 符号上第 i 个子载波的时域参考矢量，ΔV_i 表示 K 个 OFDM 符号上第 i 个子载波的多天线加权矩阵，$\Delta\alpha_i$ 表示 K 个 OFDM 符号上第 i 个子载波的等效 SISO 信道增益矩阵。由式(4)(6)可知，为了正确解调 Alice 发送的有用符号，Eve 必须首先获得 $\Delta\theta_i$。假设 Eve 通过式(15)获得了 ΔV_i 的精确估计，当 $K>M_B$ 时，对 ΔV_i 进行奇异值分解：

$$\Delta V_i = [U_s, U_n]\Sigma_i\begin{bmatrix} G_s^{\mathrm{H}} \\ G_n^{\mathrm{H}}\end{bmatrix} \tag{17}$$

其中：$[U_s, U_n]$ 表示左奇异值矩阵；$\begin{bmatrix} G_s^{\mathrm{H}} \\ G_n^{\mathrm{H}}\end{bmatrix}$ 表示右奇异值矩阵。由于 ΔV_i 的秩为 M_B，因此 U_n 张成了 $K-M_B$ 维的零空间，此时式(16)可重新表示为

$$U_n^{\mathrm{H}}\Delta V_i H_{AB,i} = \|H_{AB,i}\| U_n^{\mathrm{H}}\Delta\alpha_i\Delta\theta_i = 0 \tag{18}$$

假设时域参考变量 $e^{j\theta_{k,i}}$ 具有 M_θ 种相位，则 $\Delta\theta_i$ 具有 M_θ^K 种可能的排列组合。Eve 能够以式(18)为准则，对所有可能的排列组合进行遍历搜索[15]，遍历准则可表示为

$$\arg\min_R(R^{\mathrm{H}}U_nU_n^{\mathrm{H}}R) \tag{19}$$

其中：R 为 $K\times 1$ 维的矢量，表示 K 个时域参考变量的一种排列组合，Eve 能够通过对式(19)进行 NM_θ^K 次遍历来获得正确的 $\Delta\theta_i$，$i\in[1,N]$。又由于 $K\geqslant M_B+1$，因此在理想条件下，Eve 破解 OFDM 加密系统的最小复杂度为对式(19)进行 $NM_\theta^{(M_B+1)}$ 次遍历搜索。但是由于 $\theta_{k,i}$ 在 $[0,2\pi]$ 上随机取值，M_θ 趋向于无穷，因此 $NM_\theta^{(M_B+1)}$ 趋向于无穷，Eve 无法通过穷举搜索的方式获得 $\Delta\theta_i$，$i\in[1,N]$，从而无法正确解调相位旋转后的加密符号。

此外，当 $\partial_{k,i}$ 在各个 OFDM 符号上取值恒定为 1 时，由式(3)得 $V_{k,i} = \frac{H_{AB,i}^{\mathrm{H}}}{\|H_{AB,i}\|}e^{j\theta_{k,i}}$，$i\in[1,N]$，将其代入式(14)得

$$e^{j\theta_{k,i}} = \frac{Y_{BE,k,i}(1)-Z_{E,i}(1)}{Y_{BE,1,i}(1)-Z_{E,i}(1)}e^{j\theta_{1,i}} \tag{20}$$

其中：$Z_{E,i}(1)$、$Y_{BE,k,i}(1)$ 分别表示 $Z_{E,i}$、$Y_{BE,k,i}$ 的第一个元素，当窃听信道噪声 $Z_{E,i}$ 很小时，各个 OFDM 符号的时域参考变量将不再相互独立，Eve 能够通过式(20)获得时域参考变量的信息，从而解调接收信号。当 $M_B=1$ 时，式(20)同样成立，并且当 $\partial_{k,i}$ 趋向于 0 时，由式(7)得 Bob 的接收信噪比将急剧降低。

因此，为保证时域参考变量相互独立和提高 Bob 接收信号的质量，本文限定 $M_B\geqslant 2$；$\partial_{k,i}$ 在各个 OFDM 符号上，在 $[1/2,1]$ 内随机取值。当这些条件被满足时，即使在理想条件下，Eve 依然无法截获私密信息。而合法用户能够根据提出的算法，正确解调接收信号。

4 仿真结果

使用 MATLAB 软件对所提方案性能进行蒙特卡洛仿真，仿真参数如表 1 所示，假设每对发射和接收天线间的信道均相

互独立,且为瑞利块衰落信道,即在一帧内信道状态不改变,每帧之间信道状态独立变化,发送 100 帧数据。

表 1　算法仿真参数设置

参数名	M_B	M_E	N	P_{total}	每帧数据长度	调制方式
取值	2、4、8	8	64	1 w	40 符号	PSK

当采用贪婪算法对各个子载波的发射功率和调制方式进行分配时,假设目标误符号率 $\eta_e = 10^{-3}$,OFDM 系统的频谱效率与 SNR 的关系如图 3 所示,随着 SNR 的提高,系统的频谱效率逐渐增大,并且在相同信噪比下,频谱效率随 Bob 天线数的增多而增大,这是由于信道增益 $\| H_{AB,i} \|, i \in [1, N]$ 随着 Bob 天线数的增大而增大,在相同发送功率情况下,频谱效率随信道增益提高而增大。

假设在第 i 个子载波上,Alice 选择 QPSK 作为发送符号的调制方式,当 Eve 采用 8 根天线对接收信号进行 MRC(最大比合并)解调时,Bob 和 Eve 的误比特率曲线如图 4 所示,随着信噪比的提高,Bob 的解调误比特率快速下降。并且在相同信噪比下 Bob 的解调误比特率随着天线数的增大而下降。当 Bob 采用 8 根天线、SNR 为 10 dB 时,Bob 的解调误比特率达到 10^{-4}。与之相反,Eve 始终无法正确解调接收信号。

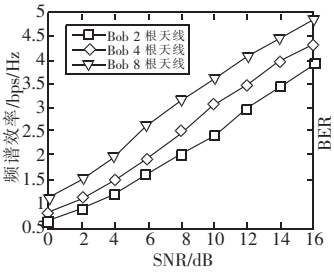

图 3　频谱效率性能图

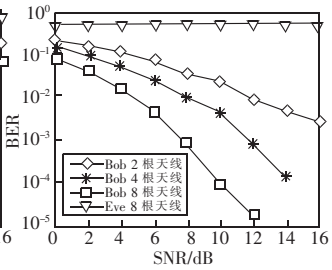

图 4　Bob 和 Eve 的误比特率性能对比

当 Alice 在第 i 个子载波上采用 QPSK 调制、Bob 采用 8 根天线、Eve 同样采用 8 根天线进行接收、Bob 和 Eve 的信噪比为 10 dB 时,Bob 和 Eve 在第 i 个子载波上的接收星座图如图 5、6 所示。在图 5 中,Eve 利用各个天线对接收信号进行 MRC,Bob 利用构造的加权向量 $V_{k,i}$ 对各个天线接收信号进行接收端波束成型,此时 Bob 形成了稳定的星座图,而 Eve 的接收信号相位在[0,2π]上随机分布,无法正确解调接收信号。

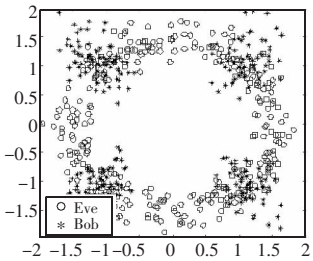

图 5　Eve 采用 MRC 解调时的星座图

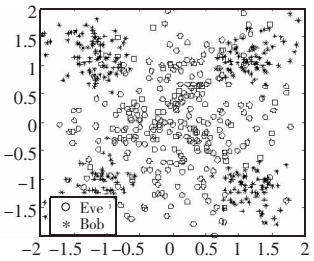

图 6　Eve 采用发送加权解调时的星座图

在图 6 中,Eve 利用式(13)中恢复的加权向量 $V_{k,i}$ 对接收信号进行接收端波束成型,可发现此时 Eve 的接收星座点呈现随机分布,无法正确解调接收信号,而 Bob 形成了稳定的接收信号星座图。比较图 5 和 6 可发现,当 Eve 采用不同的解调方式时,其接收星座图的分布不相同,但是 Eve 始终无法正确解调,这进一步验证了所提算法的安全性能。

5　结束语

本文针对 SIMO-OFDM 系统的安全通信问题,提出了一种低截获概率的物理层安全传输方案。合法接收者在各个子载波上构造多天线随机加权向量,使构造的加权向量在合法信道上的投影等于随 OFDM 符号快变的时域参考变量,发送端通过对反向训练序列的检测,获得各个子载波信道的时域参考变量,并对发送的调制符号进行随机旋转。上述加密过程对窃听者是透明的,但是由于信道的差异性,窃听者无法通过信道检测还原合法接收者构造的时域参考变量,从而无法对接收信号进行正确解调。理论分析和仿真结果表明,当天线数为 8、信噪比为 10 dB 时,合法用户误比特率达到 10^{-4},窃听者始终无法正确解调。本文方法的不足之处是在每次发送加密 OFDM 符号之前,发送端需要对多天线加权信道进行检测。

参考文献:

[1] HWANG T, YANG C. OFDM and its wireless applications: a survey [J]. IEEE Trans on Vehicular Technology, 2009, 58(4): 1673-1689.

[2] SHANNON C E. Communication theory of secrecy systems [J]. Bell System Technical Journal, 1949, 28(4): 656-715.

[3] POOR H V. Information and inference in the wireless physical layer [J]. IEEE Wireless Communications, 2012, 19(1): 40-47.

[4] MA Rui-feng, DAI Ling-long, WANG Jun. Secure communication in TDS-OFDM system using constellation rotation and noise insertion [J]. IEEE Trans on Consumer Electronics, 2010, 56(3): 1328-1332.

[5] LI Xiao-hua, HWU J, RATAZZZI E P. Array redundancy and diversity for wireless transmissions with low probability of interception [C]// Proc of IEEE International Conference on Acoustics, Speech and Signal Processing. 2006: 4.

[6] 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.

[7] ALVES H, SOUZA R D, DEBBAH M. Performance of transmit antenna selection physical layer security schemes [J]. IEEE Signal Processing Letters, 2012, 6(19): 372-375.

[8] LUO W Y, LIANG Jin, LIU S P. Wireless physical layer security model and resource allocation algorithm in MISO-OFDMA [J]. Electronics Letters, 2011, 47(6): 414-416.

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

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

[11] ZURITA N R, GHOGHO M, McLERNON D. Outage probability based power distribution between data and artificial noise for physical layer security [J]. IEEE Signal Processing Letters, 2012, 19(2): 71-74.

[12] LIAO W C, CHANG T H, MA W K, *et al*. QoS-based transmit beamforming in the presence of eavesdroppers: an optimized artificial noise-aided approach [J]. IEEE Trans on Signal Processing, 2011, 59(3): 1202-1216.

[13] LUO W Y, JIN L, HUANG K Z. User selection and resource allocation for secure multiuser MISO-OFDMA systems [J]. Electronics Letters, 2011, 47(15): 884-886.

[14] NG D W K, LO S, SCHOBER R. Energy-efficient resource allocation for secure OFDMA systems [J]. IEEE Trans on Vehicular Technology, 2012, 61(6): 2572-2585.

[15] PROAKIS J G. 数字通信[M]. 张力军,张宗橙,译. 4 版. 北京:电子工业出版社, 1995: 196-198.

[16] WONG C. Multiuser OFDM with adaptive subcarrier, bit and power allocation [J]. IEEE Journal on Selected Areas in Communications, 1999, 17(10): 1747-1758.

[17] 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.