OFDM 系统中基于三维星座旋转的物理层安全加密算法

李小倩,李 为,雷 菁,程龙旺
(国防科学技术大学电子科学与工程学院,湖南长沙 410073)

摘 要: 传统无线通信的安全主要依赖于上层加密机制,无法保护物理层调制方式和调制信息的安全. 本文针对正交频分复用(OFDM,Orthogonal Frequency Division Multiplexing)系统提出了一种物理层加密调制算法. 该算法首先利用相位随机化的信号进行信道探测并提取出等效信道相位信息,然后对三维星座进行物理层调制加密,最后接收端进行解密解调. 该方案充分利用了无线信道相位响应的随机性、互易性和位置敏感性,并将该特性用于增强物理层信号的安全性. 理论分析和计算机仿真结果表明该算法具有较强的安全性,且相对于传统的 QPSK(Quadrature Phase Shift Keying)调制,该算法的误码率性能提升约 2.5dB. 本文关注于物理层安全,旨在物理信号层提供新的安全保障,在未来 5G 通信和军事安全通信中有较广泛的应用前景.

关键词: 三维映射; 星座旋转; OFDM; 信道探测; 密钥提取; 物理层安全
中图分类号: TN911 **文献标识码:** A **文章编号:** 0372-2112 (2017)12-2873-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.12.007

A Novel Physical Layer Encryption Algorithm Based on Three Dimensional Constellation Rotation in OFDM System

LI Xiao-qian, LI Wei, LEI Jing, CHENG Long-wang
(*School of Electronic Science and Engineering, National University of Defense Technology, Changsha, Hunan* 410073, *China*)

Abstract: The security of traditional wireless communication is mainly dependent on the upper layer encryption mechanism, which cannot protect the physical layer modulation mode and the modulation information security. This paper proposes a physical layer encryption modulation method for the orthogonal frequency division multiplexing (OFDM) system. In this method, the phase random signal is used to detect and extract the equivalent channel phase information, then the 3D (Three-Dimensional) constellation is modulated in the physical layer, followed by the receiver's decryption and demodulation. The scheme makes full use of the wireless channel phase response of randomness, reciprocity and location sensibility, and this characteristic is used to enhance the safety of physical layer signal. Theoretical analysis and computer simulation results show that the algorithm is secure, and compared with the traditional QPSK (Quadrature Phase Shift Keying) modulation, the BER (Bit Error Rate) of the proposed algorithm improves about 2.5dB. This paper focuses on the physical layer security, which aims at providing a new security for the physical signal layer, and has a wide application prospect in the future 5G communications and military security communications.

Key words: three-dimensional mapping; constellation rotation; OFDM; channel detection; secret key extraction; physical layer encryption

1 引言

随着无线通信技术的迅猛发展,人们对通信安全提出更高的要求. 计算机技术的发展,使得基于计算复杂度的上层传统加密算法面临挑战. 物理层安全技术利用无线信道的空时唯一性、短时互易性和时变性等特征,在底层建立安全保障,提高系统的安全性. 物理层安全作为上层加密方案的一种补充或替代,使得窃听

收稿日期:2016-08-26;修回日期:2017-04-17;责任编辑:覃怀银
基金项目:国家自然科学基金(No.61502518, No.61372098)

者获得发送信号的信息量趋向于零,成为目前的研究热点.

当前物理层安全的研究主要分为两个方向:基于窃听信道模型的无密钥物理层安全技术[1~6]以及基于密钥的物理层安全技术[7,8],后者主要是利用无线信道特征提取密钥[9],直接利用于信号层加密.

国内外针对通信系统中传统二维空间调制信号的加密已有广泛研究,主要是通过星座旋转[10]、幅相变换[11]和星座点间跳转[12]等方法,实现了对调制方式和调制信息的保护. 2008 年 Seog Geun Kang 提出了 OFDM 系统中的三维空间调制方法,利用二维离散傅里叶反变换(IDFT)对三维映射后信号进行处理[13];2010 年 Zhenxing Chen 等人给出了 OFDM 系统中三维空间调制信号符号错误概率的理论证明过程[14]. 现有研究表明三维空间调制能够获得比二维空间调制更高的频谱效率和能量效率,且多维空间使得加密变换更灵活,可以被用来提升物理层安全性能,这正是本文研究的出发点.

本文针对 OFDM 系统,提出了一种三维星座加密调制的物理层安全算法,实现对数据信息和调制信息的保护. 该算法利用信道相位响应的短时互易性提取出等效信道相位信息,并将此相位信息作为密钥,对三维星座进行加密,使得窃听者无法解调出正确的比特信息,达到安全通信的效果. 该算法具有以下两点优势:一是充分利用了无线信道特性,确保了密钥的安全性;二是在三维调制中引入旋转加密,在保证系统有效性的同时,增加了安全性.

2 系统模型

2.1 信道模型

本文考虑三个节点的 OFDM 网络模型,如图 1 所示. Alice 和 Bob 是合法通信节点,尝试从信道中提取相位信息,并且进行安全通信;Eve 为窃听者,试图在 Alice 和 Bob 的通信过程中窃取出信道相位信息. $\boldsymbol{h}_{AB}$和 $\boldsymbol{h}_{BA}$是 Alice 与 Bob 之间的互易信道,$\boldsymbol{h}_{AE}$和 $\boldsymbol{h}_{BE}$是 Alice 和 Bob 与 Eve 之间的信道. 假定 Eve 为被动窃听者,各节点采用半双工模式且都配备一根天线. 同时,为了确保相干时间内上下行信道 $\boldsymbol{h}_{BA}$和 $\boldsymbol{h}_{AB}$之间的互易性,Alice 和 Bob 采用时分复用(TDD)通信模式. 本文考虑两种情况:情况一,Eve 到 Alice 和 Bob 的距离均大于 $\lambda/2$(λ 是载波波长),在这种情况下,合法信道和窃听信道相互独立[15];情况二,Eve 离 Alice 或 Bob 中的一个距离很近(距离小于 $\lambda/2$),即若 Eve 距离 Bob 距离小于 $\lambda/2$,在这种情况下,可认为合法信道 $\boldsymbol{h}_{AB}$与窃听信道 $\boldsymbol{h}_{AE}$具有一定的相关性,即 Eve 可以从窃听信道 $\boldsymbol{h}_{AE}$中获得合法信道 $\boldsymbol{h}_{AB}$的相关信息.

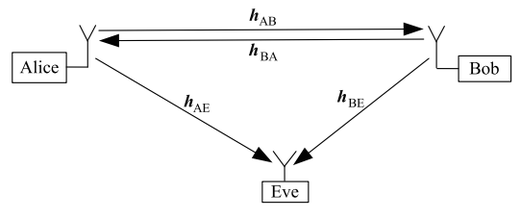


图1 系统模型

2.2 三维空间调制模型

本系统采用三维空间调制,$N_s = 2^b$ 个星座点均匀分布在球的表面,其中 b 是比特数. 考虑 $N_s = 2^2 = 4$ 的三维映射,如图 2 所示,每个两比特二进制序列映射到一个三维信号点. 不失一般性,球的半径设为 1,四个点 $S(0)$、$S(1)$、$S(2)$、$S(3)$构成一个正四面体,坐标分别是:$S(0) = (0,0,1)$,$S(1) = (-\sqrt{2}/3, -2/\sqrt{6}, -1/3)$,$S(2) = (-\sqrt{2}/3, 2/\sqrt{6}, -1/3)$,$S(3) = (2\sqrt{2}/3, 0, -1/3)$,每个点与两比特二进制序列的对应关系为:$S(0) \Longleftrightarrow (0\ \ 0)$,$S(1) \Longleftrightarrow (0\ \ 1)$,$S(2) \Longleftrightarrow (1\ \ 0)$,$S(3) \Longleftrightarrow (1\ \ 1)$.

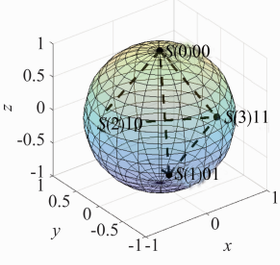


图2 $N_s = 4$ 的三维信号映射

假设 OFDM 系统中一共有 N 个子信道,信号被映射到第 k 个子信道,表示为 $\boldsymbol{s}_k = x_k\hat{x} + y_k\hat{y} + z_k\hat{z}$,$(1 \leqslant k \leqslant N)$,其中 $\hat{x}$,$\hat{y}$ 和 $\hat{z}$ 分别是 x 轴,y 轴和 z 轴的基向量或者 $\boldsymbol{s}_k = (x_k, y_k, z_k)$,$\boldsymbol{s}_k$ 表示两比特二进制序列映射到一个三维星座点的向量或者坐标. 因此,可以得到一个 OFDM 符号在频域的表达式

$$\boldsymbol{S} = (\boldsymbol{s}_1^{\mathrm{T}}\boldsymbol{s}_2^{\mathrm{T}}\cdots\boldsymbol{s}_N^{\mathrm{T}})^{\mathrm{T}} = \begin{pmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ \vdots & \vdots & \vdots \\ x_N & y_N & z_N \end{pmatrix} \tag{1}$$

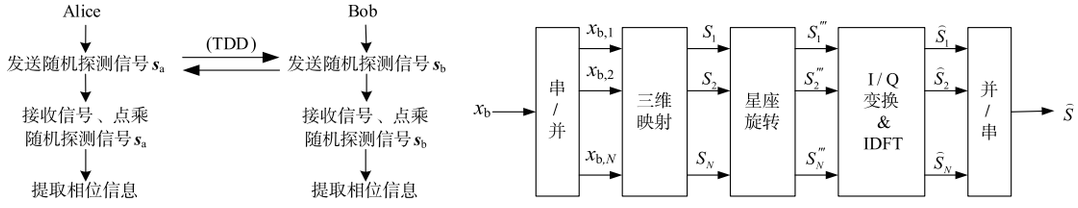
其中上标 T 代表转置.

3 基于三维星座旋转的安全算法

本节针对传统比特级加密无法保护调制方式和调制信息的安全,以及传统二维调制加密变换不灵活等缺点,提出利用信道特征提取等效相位信息对三维星座进行旋转变换,以达到置乱星座点的目的.

算法主要分为两个步骤:首先通过信道探测提取

等效相位信息作为密钥,其次利用提取的密钥对调制信号进行加解密运算. 算法流程图如图 3 所示.



(*a*) 等效信道相位提取流程图　　(*b*) 三维OFDM物理层信号加密流程图

图3　算法流程图

3.1　等效信道相位提取

与传统的信道相位提取不同,本文在提取信道相位之前将接收到的随机探测信号信息与自身发送出去的随机探测信号点乘,再提取出点乘后信息的相位,故称为等效信道相位提取.

由于 OFDM 系统的多个子信道可以提供多个随机源,本文利用 OFDM 系统中不同子信道的频域相位响应来提取相位信息,作为旋转密钥. 为保证不同子载波之间提取的密钥信息不同,假设 OFDM 子载波间间隔足够大,确保不同子载波经历相互独立的信道衰落(若子载波之间间隔较小,信道具有相关性,则可以采用间隔子载波提取的方法). 为保证信道的互易性,假定每一轮信道探测时间均小于信道相干时间,即 $\boldsymbol{h}_{AB}=\boldsymbol{h}_{BA}=\boldsymbol{h}$. 若无特别说明,论文中所有的信号都是频域信号,它们的操作都是在频域进行. 等效信道相位信息提取步骤如下:

(1)信道探测. 信道探测是合法通信方 Alice 和 Bob 之间互相发送自身产生的随机探测信号的过程. Alice 向 Bob 发送随机探测信号 $\boldsymbol{s}_a=[s_{a,1},s_{a,2},\cdots,s_{a,N}]$,随后 Bob 向 Alice 发送随机探测信号 $\boldsymbol{s}_b=[s_{b,1},s_{b,2},\cdots,s_{b,N}]$,其中 $s_{a,i}=\exp(\mathrm{j}\ \theta_{a,i})$,$s_{b,i}=\exp(\mathrm{j}\ \theta_{b,i})$,$\theta_{a,i}$、$\theta_{b,i}$分别为 $s_{a,i}$和 $s_{b,i}$的随机相位,其独立均匀分布在$[0,2\pi)$,$i=1,2,\cdots,N$,N 表示 OFDM 系统中子载波数目. 因随机探测信号是完全随机的,并且只有发送端知道探测信号的值,即探测信号 $\boldsymbol{s}_a$对于 Bob 和 Eve 是未知的,$\boldsymbol{s}_b$对于 Alice 和 Eve 是未知的.

信道探测的次数与 OFDM 的子载波个数、符号数以及传输信息的大小有关,保证提取出足够的相位用于三维星座旋转时使用.

(2)等效信道相位提取. 一轮信道探测之后,合法通信方分别将接收到的信息与自身产生的随机探测信号点乘,提取出点乘后信息相位的过程即为等效信道相位提取. 信道探测过程中 Bob 和 Alice 接收到的频域信号分别为 $\boldsymbol{r}_{b,N}$和 $\boldsymbol{r}_{a,N}$

$$\boldsymbol{r}_{b,N}=\begin{bmatrix}h_1s_{a,1}+w_{b,1}\\h_2s_{a,2}+w_{b,2}\\\vdots\\h_Ns_{a,N}+w_{b,N}\end{bmatrix},\boldsymbol{r}_{a,N}=\begin{bmatrix}h_1s_{b,1}+w_{a,1}\\h_2s_{b,2}+w_{a,2}\\\vdots\\h_Ns_{b,N}+w_{a,N}\end{bmatrix}\tag{2}$$

其中,$r_{b,i}$表示 Bob 接收到的第 i 个子载波频域信号,则 $r_{b,i}=h_is_{a,i}+w_{b,i}=|h_i|\exp(\mathrm{j}\ \theta_{h,i})s_{a,i}+w_{b,i}=|h_i|\exp(\mathrm{j}\ \theta_{h,i}+\mathrm{j}\theta_{a,i})+w_{b,i}$,$r_{a,i}$表示 Alice 接收到的第 i 个子载波频域信号,$r_{a,i}=h_is_{b,i}+w_{a,i}=|h_i|\exp(\mathrm{j}\ \theta_{h,i})s_{b,i}+w_{a,i}=|h_i|\exp(\mathrm{j}\ \theta_{h,i}+\mathrm{j}\ \theta_{b,i})+w_{a,i}$,$1\leqslant i\leqslant N$,$h_i$ 表示 h 的第 i 个子信道的频域信道响应,$\theta_{h,i}$表示第 i 个子信道的相位,$\boldsymbol{h}$ 表示信道状态向量 $\boldsymbol{h}=[h_1,h_2,\cdots,h_N]$,$N$ 表示数据传输子信道个数,即向量 $\boldsymbol{h}$ 的长度. 假设每个子信道独立同分布,即 $h_i\sim\mathrm{CN}(0,\sigma_h^2)$,$\angle h_i=\theta_{h,i}$,$w_{b,i}\sim\mathrm{CN}(0,\sigma_n^2)$和 $w_{a,i}\sim\mathrm{CN}(0,\sigma_n^2)$分别表示独立同分布的复高斯噪声. Bob 将接收到的信号点乘只有自己知道的随机探测信号 s_b,得到

$$\begin{aligned}\hat{\boldsymbol{r}}_{b,N}&=\begin{bmatrix}h_1s_{a,1}+w_{b,1}\\h_2s_{a,2}+w_{b,2}\\\vdots\\h_Ns_{a,N}+w_{b,N}\end{bmatrix}\cdot[s_{b,1},s_{b,2},\cdots,s_{b,N}]\\&=\begin{bmatrix}h_1s_{a,1}s_{b,1}+w_{b,1}s_{b,1}\\h_2s_{a,2}s_{b,2}+w_{b,2}s_{b,2}\\\vdots\\h_Ns_{a,N}s_{b,N}+w_{b,N}s_{b,N}\end{bmatrix}\end{aligned}\tag{3}$$

同样,与 Bob 相似,Alice 将接收到的信号点乘只有自己知道的随机探测信号 s_a,得到

$$\begin{aligned}\hat{\boldsymbol{r}}_{a,N}&=\begin{bmatrix}h_1s_{b,1}+w_{a,1}\\h_2s_{b,2}+w_{a,2}\\\vdots\\h_Ns_{b,N}+w_{a,N}\end{bmatrix}\cdot[s_{a,1},s_{a,2},\cdots,s_{a,N}]\\&=\begin{bmatrix}h_1s_{a,1}s_{b,1}+w_{a,1}s_{a,1}\\h_2s_{a,2}s_{b,2}+w_{a,2}s_{a,2}\\\cdots\\h_Ns_{a,N}s_{b,N}+w_{a,N}s_{a,N}\end{bmatrix}\end{aligned}\tag{4}$$

Bob 和 Alice 分别根据 $\hat{r}_{b,i}$和 $\hat{r}_{a,i}$估计出相应的子信道相位响应为:

$$\begin{aligned}\hat{\theta}_{b,i}&=\tan^{-1}(\mathrm{imag}(\hat{r}_{b,i})/\mathrm{real}(\hat{r}_{b,i}))\\&=\theta_{h,i}+\theta_{a,i}+\theta_{b,i}+\varepsilon_{b,i}\\\hat{\theta}_{a,i}&=\tan^{-1}(\mathrm{imag}(\hat{r}_{a,i})/\mathrm{real}(\hat{r}_{a,i}))\end{aligned}\tag{5}$$

$$= \theta_{\mathrm{h},i} + \theta_{\mathrm{b},i} + \theta_{\mathrm{a},i} + \varepsilon_{\mathrm{a},i} \tag{6}$$

其中 $\varepsilon_{\mathrm{b},i}$ 和 $\varepsilon_{\mathrm{a},i}$ 表示相位估计误差. 可以看出,Bob 和 Alice 估计的相位中都包含了随机探测信号的相位 $\theta_{\mathrm{a},i}$ 和 $\theta_{\mathrm{b},i}$,因此将 $\hat{\theta}_{\mathrm{b},i}$ 和 $\hat{\theta}_{\mathrm{a},i}$ 看作是等效子信道相位响应的估计值.

提取出的相位信息 $\hat{\theta}_{\mathrm{b},i}$ 和 $\hat{\theta}_{\mathrm{a},i}$ 分别用于收发两端加解密旋转,因为 Eve 无法得到此相位信息,所以不能正确解密.

3.2 基于信道相位信息的加解密算法

按照以上流程提取出等效信道相位信息后,再利用此相位信息对三维星座调制进行加解密处理.

3.2.1 三维星座调制加密算法

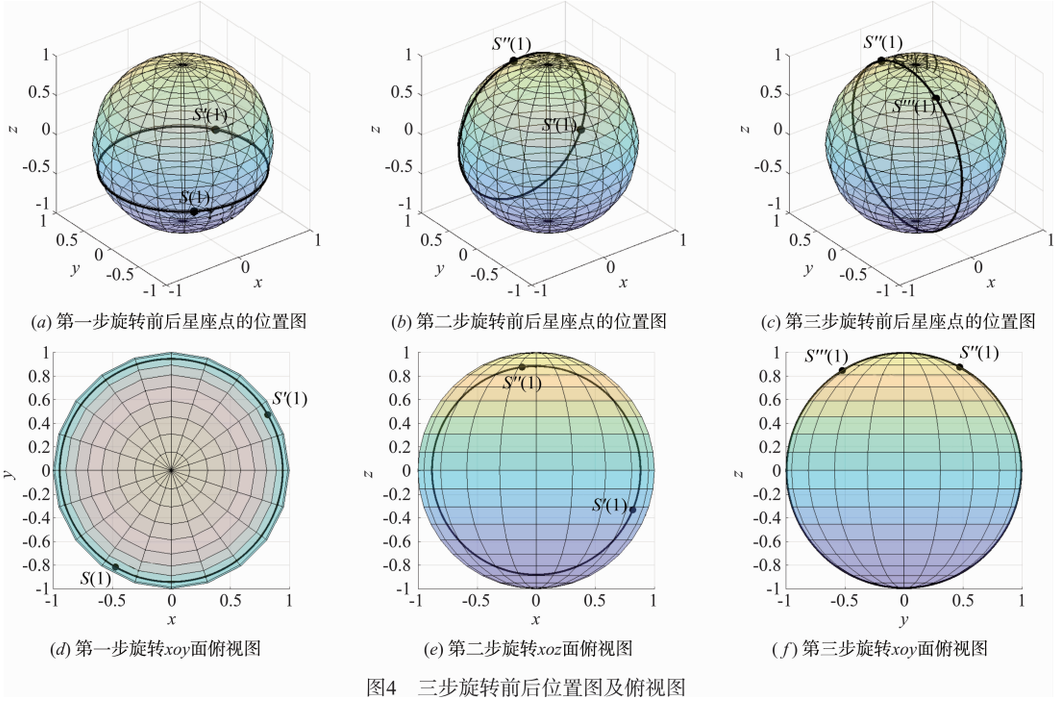
根据三维映射关系,每两比特二进制信息映射到三维空间变为一个星座点位置信息,假设每个 OFDM 符号需要传输 M 比特信息,经过三维映射后变为(M/2)个三维星座点,即

$$\boldsymbol{S} = \begin{bmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ \vdots & \vdots & \vdots \\ x_{M/2} & y_{M/2} & z_{M/2} \end{bmatrix} \tag{7}$$

实际传输中,注意数据大小与 OFDM 的子载波个数以及符号数之间的关系.

从发送端节点的等效信道相位中选出 N 组等效信道相位角度,作为星座点的旋转角度,每个星座点对应三个旋转角度,第 i 组旋转角度记为 $\hat{\boldsymbol{\theta}}_i^{\mathrm{a}} = (\hat{\theta}_{i,1}^{\mathrm{a}} \quad \hat{\theta}_{i,2}^{\mathrm{a}} \quad \hat{\theta}_{i,3}^{\mathrm{a}})$,$i = 1,2,\cdots,N$;对于 $\boldsymbol{S}$ 中每一个星座点进行三步旋转,得到加密数据信息 $\boldsymbol{S}''' = (\boldsymbol{s}_1''', \boldsymbol{s}_2''', \cdots, \boldsymbol{s}_N''')^{\mathrm{T}}$.

下面以点 $S(1) = (-\sqrt{2}/3, -2/\sqrt{6}, -1/3)$ 为例进行说明,如图 4 所示,设 $\hat{\boldsymbol{\theta}}_i^{\mathrm{a}}$ 的三个角度值分别为(150° 120° 60°).



(a) 第一步旋转前后星座点的位置图 (b) 第二步旋转前后星座点的位置图 (c) 第三步旋转前后星座点的位置图

(d) 第一步旋转xoy面俯视图 (e) 第二步旋转xoz面俯视图 (f) 第三步旋转xoy面俯视图

图4 三步旋转前后位置图及俯视图

第一步,过点 $S(1)$ 且平行于 xoy 面的平面截球体,点 $S(1)$ 绕所截曲线圆逆时针旋转角度 $\hat{\theta}_{i,1}^{\mathrm{a}}$,得到点 $S'(1)$,旋转变换公式如下:

$$\boldsymbol{s}_i' = \begin{pmatrix} x_i' \\ y_i' \\ z_i' \end{pmatrix} = \begin{pmatrix} \cos\hat{\theta}_{i,1}^{\mathrm{a}} & -\sin\hat{\theta}_{i,1}^{\mathrm{a}} & 0 \\ \sin\hat{\theta}_{i,1}^{\mathrm{a}} & \cos\hat{\theta}_{i,1}^{\mathrm{a}} & 0 \\ 0 & 0 & 1 \end{pmatrix} (x_i \quad y_i \quad z_i)^{\mathrm{T}} \tag{8}$$

其中 $(x_i \quad y_i \quad z_i)^{\mathrm{T}}$ 表示点 $\boldsymbol{s}_i$ 坐标.

第二步,过点 $S'(1)$ 且平行于 xoz 面的平面截球体,点 $S'(1)$ 绕所截曲线圆逆时针旋转角度 $\hat{\theta}_{i,2}^{\mathrm{a}}$,得到点 $S''(1)$,旋转变换公式如下:

$$\boldsymbol{s}_i'' = \begin{pmatrix} x_i'' \\ y_i'' \\ z_i'' \end{pmatrix} = \begin{pmatrix} \cos\hat{\theta}_{i,2}^{\mathrm{a}} & 0 & -\sin\hat{\theta}_{i,2}^{\mathrm{a}} \\ 0 & 1 & 0 \\ \sin\hat{\theta}_{i,2}^{\mathrm{a}} & 0 & \cos\hat{\theta}_{i,2}^{\mathrm{a}} \end{pmatrix} \begin{pmatrix} x_i' \\ y_i' \\ z_i' \end{pmatrix} \tag{9}$$

第三步,过点 $S''(1)$ 且平行于 yoz 面的平面截球体,点 $S''(1)$ 绕所截曲线圆逆时针旋转角度 $\hat{\theta}_{i,3}^{\mathrm{a}}$,得到点 $S'''(1)$,旋转变换公式如下:

$$\boldsymbol{s}_i''' = \begin{pmatrix} x_i''' \\ y_i''' \\ z_i''' \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\hat{\theta}_{i,3}^{\mathrm{a}} & -\sin\hat{\theta}_{i,3}^{\mathrm{a}} \\ 0 & \sin\hat{\theta}_{i,3}^{\mathrm{a}} & \cos\hat{\theta}_{i,3}^{\mathrm{a}} \end{pmatrix} \begin{pmatrix} x_i'' \\ y_i'' \\ z_i'' \end{pmatrix} \tag{10}$$

点 $S(1)$ 经过三步旋转最终变为点 $S'''(1)$,如图 5 所示.

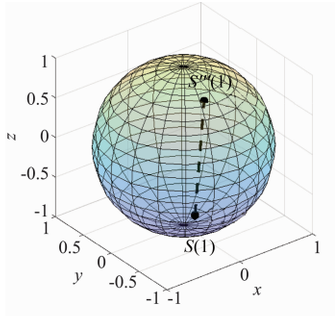


图5　三步旋转前后点$S(1)$位置对比图

所有的坐标点 $\boldsymbol{S}=(\boldsymbol{s}_1,\boldsymbol{s}_2,\cdots,\boldsymbol{s}_N)^{\mathrm{T}}=\begin{pmatrix}x_1 & y_1 & z_1\\ x_2 & y_2 & z_2\\ \vdots & \vdots & \vdots\\ x_N & y_N & z_N\end{pmatrix}$都类似于点 $S(1)$做三步旋转,最终得到

$$\boldsymbol{S}'''=\begin{pmatrix}x_1''' & y_1''' & z_1'''\\ x_2''' & y_2''' & z_2'''\\ \vdots & \vdots & \vdots\\ x_N''' & y_N''' & z_N'''\end{pmatrix}\tag{11}$$

将最后得到的数据信息变换成 I/Q 两路进行传输,变换规则如下:

$$\hat{\boldsymbol{S}}=\begin{pmatrix}x_1'''+\mathrm{j}\,y_1'''\\ z_1'''+\mathrm{j}\,x_2'''\\ y_2'''+\mathrm{j}\,z_2'''\\ \vdots\\ z_{N-1}'''+\mathrm{j}\,x_N'''\\ y_N'''+\mathrm{j}\,z_N'''\end{pmatrix}\tag{12}$$

再经过一系列处理(如插导频、调整子载波顺序、插入长短符号、快速傅里叶反变换以及加入循环前缀等一系列操作),将数据通过信道传送出去.

3.2.2　三维星座调制解密算法

接收端通过信道接收到消息之后首先通过一系列预处理(如去循环前缀、快速傅里叶变换、基于长符号的信道估计、调整子载波顺以及去导频等操作),获得待解密的数据信息 $\boldsymbol{S}$,

$$\boldsymbol{S}=\begin{pmatrix}\hat{x}_1'''+\mathrm{j}\,\hat{y}_1'''\\ \hat{z}_1'''+\mathrm{j}\,\hat{x}_2'''\\ \hat{y}_2'''+\mathrm{j}\,\hat{z}_2'''\\ \vdots\\ \hat{z}_{N-1}'''+\mathrm{j}\,\hat{x}_N'''\\ \hat{y}_N'''+\mathrm{j}\,\hat{z}_N'''\end{pmatrix}\tag{13}$$

再经过变换得到 N 行 3 列的数据矩阵

$$\hat{\boldsymbol{S}}'''=\begin{pmatrix}\hat{x}_1''' & \hat{y}_1''' & \hat{z}_1'''\\ \hat{x}_2''' & \hat{y}_2''' & \hat{z}_2'''\\ \vdots & \vdots & \vdots\\ \hat{x}_N''' & \hat{y}_N''' & \hat{z}_N'''\end{pmatrix}\tag{14}$$

与发送端相同,每一行坐标点 $\hat{\boldsymbol{s}}_i'''=(\hat{x}_i''' \quad \hat{y}_i''' \quad \hat{z}_i''')$ 对应一行旋转角度 $\hat{\boldsymbol{\theta}}_i^{\mathrm{b}}=(\hat{\theta}_{i,1}^{\mathrm{b}} \quad \hat{\theta}_{i,2}^{\mathrm{b}} \quad \hat{\theta}_{i,3}^{\mathrm{b}})$,但不同的是三次旋转的角度顺序.

第一步,过点 $\hat{\boldsymbol{s}}_i'''$ 且平行于 yoz 面的平面截球体,点 $\hat{\boldsymbol{s}}_i'''$ 绕所截曲线圆顺时针旋转角度 $\hat{\theta}_{i,3}^{\mathrm{b}}$,得到点 $\hat{\boldsymbol{s}}_i''$,旋转变换公式如下:

$$\hat{\boldsymbol{s}}_i''=\begin{pmatrix}\hat{x}_i''\\ \hat{y}_i''\\ \hat{z}_i''\end{pmatrix}=\begin{pmatrix}1 & 0 & 0\\ 0 & \cos\hat{\theta}_{i,3}^{\mathrm{b}} & -\sin\hat{\theta}_{i,3}^{\mathrm{b}}\\ 0 & \sin\hat{\theta}_{i,3}^{\mathrm{b}} & \cos\hat{\theta}_{i,3}^{\mathrm{b}}\end{pmatrix}^{-1}(\hat{x}_i''' \quad \hat{y}_i''' \quad \hat{z}_i''')^{\mathrm{T}}\tag{15}$$

第二步,过点 $\hat{\boldsymbol{s}}_i''$ 且平行于 xoz 面的平面截球体,点 $\hat{\boldsymbol{s}}_i''$ 绕所截曲线圆顺时针旋转角度 $\hat{\theta}_{i,2}^{\mathrm{b}}$,得到点 $\hat{\boldsymbol{s}}_i'$,旋转变换公式如下:

$$\hat{\boldsymbol{s}}_i'=\begin{pmatrix}\hat{x}_i'\\ \hat{y}_i'\\ \hat{z}_i'\end{pmatrix}=\begin{pmatrix}\cos\hat{\theta}_{i,2}^{\mathrm{b}} & 0 & -\sin\hat{\theta}_{i,2}^{\mathrm{b}}\\ 0 & 1 & 0\\ \sin\hat{\theta}_{i,2}^{\mathrm{b}} & 0 & \cos\hat{\theta}_{i,2}^{\mathrm{b}}\end{pmatrix}^{-1}\begin{pmatrix}\hat{x}_i''\\ \hat{y}_i''\\ \hat{z}_i''\end{pmatrix}\tag{16}$$

第三步,过点 $\hat{\boldsymbol{s}}_i'$ 且平行于 xoy 面的平面截球体,点 $\hat{\boldsymbol{s}}_i'$ 绕所截曲线圆顺时针旋转角度 $\hat{\theta}_{i,1}^{\mathrm{b}}$,得到点 $\hat{\boldsymbol{s}}_i$,旋转变换公式如下:

$$\hat{\boldsymbol{s}}_i=\begin{pmatrix}\hat{x}_i\\ \hat{y}_i\\ \hat{z}_i\end{pmatrix}=\begin{pmatrix}\cos\hat{\theta}_{i,1}^{\mathrm{b}} & -\sin\hat{\theta}_{i,1}^{\mathrm{b}} & 0\\ \sin\hat{\theta}_{i,1}^{\mathrm{b}} & \cos\hat{\theta}_{i,1}^{\mathrm{b}} & 0\\ 0 & 0 & 1\end{pmatrix}^{-1}\begin{pmatrix}\hat{x}_i'\\ \hat{y}_i'\\ \hat{z}_i'\end{pmatrix}\tag{17}$$

第四步,利用最小距离判决法进行解映射. 分别计算点 $\hat{\boldsymbol{s}}_i^{\mathrm{T}}=(\hat{x}_i \quad \hat{y}_i \quad \hat{z}_i)$ 与点 $S(0)=(0,0,1)$,点 $S(1)=(-\sqrt{2}/3,-2/\sqrt{6},-1/3)$,点 $S(2)=(-\sqrt{2}/3,2/\sqrt{6},-1/3)$,点 $S(3)=(2\sqrt{2}/3,0,-1/3)$ 之间的距离,并进行对比,选择出与点 $\hat{\boldsymbol{s}}_i^{\mathrm{T}}=(\hat{x}_i \quad \hat{y}_i \quad \hat{z}_i)$ 之间距离最小的点;根据发送端对应的映射关系进行解调,即 $S(0)\Longleftrightarrow(0\quad 0)$,$S(1)\Longleftrightarrow(0\quad 1)$,$S(2)\Longleftrightarrow(1\quad 0)$,$S(3)\Longleftrightarrow(1\quad 1)$,恢复出发端发送的数据信号.

4　性能评估与仿真验证

基于以上分析和描述,本文对所提算法进行了 MATLAB 仿真和数学分析.

仿真参数参考 802.16d 标准,具体参数设置如表 1 所示. 信道为高斯白噪声(AWGN)信道.

下面从有效性、安全性和算法复杂度三个方面对所提算法进行评估.

表 1 OFDM 系统仿真参数

特性	参数	特性	参数
调制方式	三维星座映射	FFT 点数 N	256 点
数据子载波	192 点	内插导频	8 点
CP 长度	64 点	帧长度	10 个符号
OFDM 帧短符号数	1 个	OFDM 帧长符号数	1 个

4.1 有效性分析

4.1.1 上下行信道差异对系统性能的影响

上下行信道差异主要来自两个方面:一是相位探测时,上下行链路间的时间差会影响其互易性;二是相位估计时,由式(5)和(6)可知,存在相位估计误差 $\varepsilon_{a,i}$ 和 $\varepsilon_{b,i}$. 系统性能必将受这些差异的影响,本节仿真分析了信噪比为 12dB 时信道差异 ε 与误比特率之间的关系,如图 6 所示,其中 $\varepsilon \sim \mathrm{CN}(0,\sigma_n^2)$. 由仿真图可知,随着信道差异 ε 的减小误比特率也逐渐减小,当 ε 减小到 10^{-3}时误比特率趋于稳定.

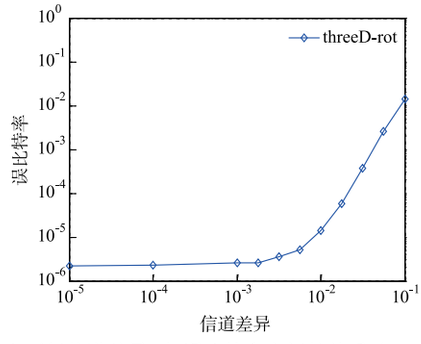


图6 上下行信道差异 ε 与误比特率之间的关系(SNR=12dB)

4.1.2 与传统 QPSK 调制映射性能对比

在 AWGN 环境中,通过信号映射的最小欧式距离(MED)和误比特率评估 OFDM 系统的性能. 将 $N_s=4$ 三维星座映射与传统的 QPSK 进行对比. 信号映射的最小欧式距离(MED)对比如表 2,最小欧式距离根据星座图上各个信号点之间的距离计算得到. 误比特率对比如图 7 所示.

表 2 信号映射的最小欧式距离

映射方式	最小欧式距离(MED)
QPSK	1.4142
$N_s=4$ 三维星座映射	1.6330

从以上分析和仿真结果可以看出,与 QPSK 映射相比,三维星座映射的最小欧式距离至少增加了 15.5%;当误比特率在 10^{-4}的时候,三维映射比 QPSK 的信噪比(SNR)小大约 2.5dB.

4.2 安全性分析

为充分评估安全性,假设窃听者 Eve 具有以下

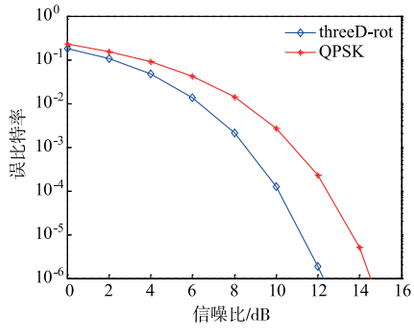


图7 $N_s=4$ 三维星座映射与传统的QPSK误比特率对比图

能力[16]:

(1) 拥有和合法通信方相同的接收能力,如符号同步和信道估计能力;

(2) 可窃听并推测出 Alice 与 Bob 之间通信的调制方式;

(3) 强大的计算能力,可以进行计算量攻击.

根据 Kerckhoffs 原理[17],假定密码分析者可获得该系统的设计和工作的相关信息. 本文中假定 Eve 除了不知道 Alice 和 Bob 各自产生的随机探测信号 $s_{a,i}$和 $s_{b,i}$之外其他的都知道,包括 Alice 和 Bob 提取等效信道相位信息的过程以及 Alice 与 Bob 之间通信的调制方式. 也就是说,加密算法和方案完全公开,系统的安全性并不依赖于算法方案的保密.

4.2.1 算法安全性证明

假设在相位提取过程中,Eve 一直处于被动窃听状态. 忽略噪声的影响,由式(5)、(6)可知 Eve 要想窃取到等效信道相位的信息,必须知道主信道系数 h_i 以及 Alice 和 Bob 各自发送的随机探测信号 $s_{a,i}$和 $s_{b,i}$的相位.

当 Eve 到 Alice 和 Bob 的距离均大于 $\lambda/2$(λ 是载波波长)时,合法信道和窃听信道相互独立,即 $\boldsymbol{h}_{AB}$与 $\boldsymbol{h}_{AE}$相互独立,$\boldsymbol{h}_{BA}$与 $\boldsymbol{h}_{BE}$相互独立. 在 Alice 向 Bob 发送随机探测信号 $\boldsymbol{s}_a$时,Eve 接收到由 Alice 发送的频域信号为:

$$\boldsymbol{r}_{ea,N}=\begin{bmatrix} h_{AE,1}s_{a,1}+w_{AE,1} \\ h_{AE,2}s_{a,2}+w_{AE,2} \\ \vdots \\ h_{AE,N}s_{a,N}+w_{AE,N} \end{bmatrix} \tag{18}$$

其中 $r_{ea,i}$表示 Eve 接收到的关于 Alice 的第 i 个子载波频域信号,则 $r_{ea,i}=h_{AE,i}s_{a,i}+w_{AE,i}=|h_{AE,i}|\exp(\mathrm{j}\,\theta_{hAE,i}+\mathrm{j}\,\theta_{a,i})+w_{AE,i}$,$h_{AE,i}=|h_{AE,i}|\exp(\mathrm{j}\,\theta_{hAE,i})$表示 Alice 到 Eve 的第 i 个子信道,$w_{AE,i}$表示 Eve 的观测噪声;在 Bob 向 Alice 发送随机探测信号 s_b 时,Eve 接收到 Bob 发送的频域信号为:

$$\boldsymbol{r}_{\mathrm{eb},N}=\begin{bmatrix} h_{\mathrm{BE},1}s_{\mathrm{b},1}+w_{\mathrm{BE},1} \\ h_{\mathrm{BE},2}s_{\mathrm{b},2}+w_{\mathrm{BE},2} \\ \vdots \\ h_{\mathrm{BE},N}s_{\mathrm{b},N}+w_{\mathrm{BE},N} \end{bmatrix} \tag{19}$$

其中 $r_{\mathrm{eb},i}$表示 Eve 接收到的关于 Bob 的第 i 个子载波频域信号,则 $r_{\mathrm{eb},i}=h_{\mathrm{BE},i}s_{\mathrm{b},i}+w_{\mathrm{BE},i}=|h_{\mathrm{BE},i}|\exp(\mathrm{j}\theta_{\mathrm{hBE},i}+\mathrm{j}\theta_{\mathrm{b},i})+w_{\mathrm{BE},i}$,$h_{\mathrm{BE},i}=|h_{\mathrm{BE},i}|\exp(\mathrm{j}\theta_{\mathrm{hBE},i})$表示 Bob 到 Eve 的第 i 个子信道,$w_{\mathrm{BE},i}$表示观测噪声.

由于 Eve 到 Alice 和 Bob 的距离均大于 $\lambda/2$(λ 是载波波长),即合法信道和窃听信道相互独立,故 Eve 不能得到主信道的任何信息;又由于 Alice 和 Bob 每次发送的探测信号 $s_{\mathrm{a},i}$和 $s_{\mathrm{b},i}$的相位随机分布在$[0,2\pi)$,Eve 不能从式(18)和(19)中通过相位估计分离出 $\theta_{\mathrm{a},i}$和 $\theta_{\mathrm{b},i}$,故 Eve 不能分析得到等效信道的相位信息破译消息.

当 Eve 离 Alice 或者 Bob 中的一个距离很近(距离小于 $\lambda/2$),即假设 Eve 距离 Bob 距离很近(小于 $\lambda/2$),近似认为 $h_{\mathrm{AE},i}=h_{\mathrm{AB},i}$,式(18)变为

$$\boldsymbol{r}_{\mathrm{ea},N}=\begin{bmatrix} h_1s_{\mathrm{a},1}+w_{\mathrm{AE},1} \\ h_2s_{\mathrm{a},2}+w_{\mathrm{AE},2} \\ \vdots \\ h_Ns_{\mathrm{a},N}+w_{\mathrm{AE},N} \end{bmatrix} \tag{20}$$

此时 $r_{\mathrm{ea},i}=h_{\mathrm{AE},i}s_{\mathrm{a},i}+w_{\mathrm{AE},i}=|h_{\mathrm{AE},i}|\exp(\mathrm{j}\theta_{\mathrm{b},i}+\mathrm{j}\theta_{\mathrm{a},i})+w_{\mathrm{AE},i}$,$h_{\mathrm{AE},i}=h_{\mathrm{AB},i}=|h_{\mathrm{AB},i}|\exp(\mathrm{j}\theta_{\mathrm{hAB},i})$与 Alice 到 Bob 的第 i 个子信道对应相等,$w_{\mathrm{AE},i}$表示 Eve 的观测噪声;式(19)不变. Eve 可以根据 $r_{\mathrm{ea},i}$估计出相应的子信道相位响应:$\hat{\theta}_{\mathrm{ea},i}=\tan^{-1}(\mathrm{imag}(r_{\mathrm{ea},i})/\mathrm{real}(r_{\mathrm{ea},i}))=\theta_{\mathrm{h},i}+\theta_{\mathrm{a},i}+\varepsilon_{\mathrm{ea},i}$,其中 $\varepsilon_{\mathrm{ea},i}$表示相位估计误差,但却不能从式(19)中分离出相位角度 $\theta_{\mathrm{b},i}$,依然无法破译消息.

针对 Eve 的被动窃听,通过分析可以看出即使窃听者知道合法通信双方使用的加密算法和方案,也无法破解消息. 此外,此加密方案与通信链路性能的优良没有太大关系,就算 Eve 与 Alice 的链路性能优于 Bob 与 Alice 之间的链路性能,只要保证 Alice 和 Bob 提取出相同的加密密钥(此密钥 Eve 未知),就能够通过此相位加密算法保证系统的安全.

4.2.2　破解计算量分析

由于每次旋转的角度完全随机,没有任何相关性,Eve 不能从中得到任何统计规律,只能通过穷举法暴力破解.

对于每一个二进制的两比特消息,Eve 通过最小距离判决解调都有 1/4 正确的概率(忽略边界点的影响). 假设一共传输 300 比特数据,窃听者破译三分之一的信息即认为窃听成功,则 Eve 最终破解成功的概率为 $(1/4)^{300/(2\times3)}=(1/4)^{50}$,即 Eve 需要做 4^{50}次尝试才可能成功一次. 以每秒运行 1000 亿次的计算机为例,破译需 4.02×10^{11}年,远远超出可计算时间. 实际中,传输的数据远大于 300 比特,想要通过穷举法破解该算法的信息是非常困难的.

4.3　复杂度分析

相较于 QPSK,本质上来说三维星座映射的复杂度并没有明显提高,因为 QPSK 是将每两比特数据映射成二维空间中四个固定坐标点中的一个,而三维映射是将每两比特数据映射成三维空间中四个固定坐标点中的一个. 本文所提算法将加密和调制合在一起,接收端收到消息后需解密和解调,复杂度主要来自于解调时,需要利用最小距离判决法解映射.

5　结论

面对高速发展的计算机,基于计算量安全的传统通信系统面临威胁,而且网络层的加密对于调制方式和调制信息的保护也不足. 针对以上问题,本文提出 OFDM 系统中基于三维星座旋转的物理层安全加密算法,置乱三维映射中星座点位置,达到加密的效果. 所提算法对于同步系统中导频以及训练序列不做改变,不影响大数据量信号实时安全传输中信号同步等问题,故对于大数据量传输(例如视频信号传输)也有意义,在未来 5G 通信和军事安全通信中有较广泛的应用前景.

参考文献

[1] Klinc D, Ha J, Mclaughlin S W, et al. LDPC codes for physical layer security[A]. GLOBECOM 2009-2009 IEEE Global Telecommunications Conference[C]. Honolulu: IEEE, 2009. 5765 – 5770.

[2] Cheng L, Li W, Ma D, et al. Moving window scheme for extracting secret keys in stationary environments[J]. Iet Communications, 2016, 10(16): 2206 – 2214.

[3] Fakoorian S A A, Swindlehurst A L. Full rank solutions for the MIMO Gaussian wiretap channel with an average power constraint[J]. IEEE Transactions on Signal Processing, 2013, 61(10): 2620 – 2631.

[4] Li W, Ghogho M, Chen B, et al. Secure communication via sending artificial noise by the receiver: outage secrecy capacity/region analysis[J]. Communications Letters IEEE, 2012, 16(10): 1628 – 1631.

[5] 李为,陈彬,魏急波,等. 基于接收机人工噪声的物理层安全技术及保密区域分析[J]. 信号处理,2012,28(9):1314 – 1320.
LI Wei, CHEN Bin, WEI Ji-bo, et al. Secure communication via sending artificial noise by the receiver: ergodic secure region[J]. Signal Processing, 2012, 28(9): 1314 –

1320. (in Chinese)
[6] Li W, Tang Y, Ghogho M, et al. Secure communications via sending artificial noise by both transmitter and receiver: optimum power allocation to minimise the insecure region[J]. Iet Communications, 2014, 8(16): 2858 – 2862.
[7] Mceliece R J. A Public-Key Cryptosystem Based on Algebraic Coding Theory [R]. Pasadena: NASA, 1978. 114 – 116.
[8] Adamo O, Fu S, Varanasi M R. Physical layer error correction based cipher[A]. 2010 IEEE Global Telecommunications Conference GLOBECOM 2010 [C]. Miami: IEEE, 2010. 1 – 5.
[9] Wang Q, Su H, Ren K, et al. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks[A]. 2011 Proceedings IEEE INFOCOM [C]. Shanghai: IEEE, 2011. 1422 – 1430.
[10] Huo F, Gong G. A new efficient physical layer OFDM encryption scheme[A]. IEEE INFOCOM 2014—IEEE Conference on Computer Communications [C]. Toronto: IEEE, 2014. 1024 – 1032.
[11] 蕾蓓蓓. 基于物理层加密的调制方式隐蔽算法研究[D]. 西安: 西北大学, 2012.
[12] 岳敖, 李为, 马东堂, 等. 拉丁阵和幅相变换相结合的物理层加密传输算法[J]. 信号处理, 2016, 32(6): 660 – 668.
YUE Ao, LI Wei, MA Dong-tang, et al. A novel physical layer encryption algorithm combined Latin rectangle and phase-amplitude mask [J]. Signal Processing, 2016, 32(6): 660 – 668. (in Chinese)
[13] Kang S G. An OFDM with 3-D signal mapper and 2-D IDFT modulator [J]. IEEE Communications Letters, 2008, 12(12): 871 – 873.
[14] Chen Z, Choi E C, Kang S G. Closed-form expressions for the symbol error probability of 3-D OFDM. [J]. IEEE Communications Letters, 2010, 14(2): 112 – 114.
[15] Jakes W. Microwave Mobile Communications[M]. New York: IEEE, 1993. 11 – 78.
[16] Chorti A. Masked-OFDM: A physical layer encryption for future OFDM applications[A]. 2011 IEEE GLOBECOM Workshops (GC Wkshps 2011) [C]. Houston: IEEE, 2011. 1254 – 1258.
[17] Stinson D R. Cryptography: Theory and Practice [M]. London: CRC, 1995. 177 – 186.

作者简介

李小倩 女, 1992 年 11 月出生于湖北省老河口市. 现为国防科学技术大学电子科学与工程学院硕士研究生. 主要研究方向为物理层安全.
E-mail: lixiaoqian15@ nudt. edu. cn

李 为 男, 1984 年 9 月出生于湖北省当阳市. 博士. 现为国防科学技术大学讲师. 主要研究方向为无线通信资源分配、物理层安全技术.
E-mail: liwei@ nudt. edu. cn

雷 菁(通信作者) 女, 1968 年 2 月出生于陕西省西安市. 教授. 博士. 博士生导师. 主要研究方向为信息论与编码技术.
E-mail: leijing@ nudt. edu. cn

程龙旺 男, 1988 年 4 月出生于安徽省蚌埠市. 研究生. 现为国防科学技术大学电子科学与工程学院博士研究生. 主要研究方向为物理层安全、基于无线信道的密钥提取以及物理层认证.
E-mail: clw860385@ 163. com