基于无线 OFDM 系统的调制方式保护算法

高宝建 王少迪 任宇辉 王玉洁
(西北大学信息科学与技术学院 西安 710127)

摘 要 随着无线通信系统的宽带化,传统的数据加密算法具有很高的计算复杂度,并且没有考虑到物理层调制方式的安全性。针对这一问题,从物理层加密的角度,提出了一种基于无线 OFDM 系统的调制方式保护算法。在单载波和多载波情况下,分别对所提算法的调制方式保护效果进行了分析,并通过采用典型的认知无线电调制识别方法对加密前后的识别率进行了仿真和比较。理论分析和仿真结果表明,所提算法在不改变原系统固有性能的情况下,具有不错的调制方式保护性能。

关键词 调制方式保护,物理层加密,OFDM,认知无线电

中图法分类号 TN918 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.10.013

Modulation Protection Algorithm Based on Wireless OFDM Systems

GAO Bao-jian WANG Shao-di REN Yu-hui WANG Yu-jie
(College of Information Science and Technology, Northwest University, Xi'an 710127, China)

Abstract With the broadband trend in wireless communication system, traditional data encryption methods have high computational complexity, and haven't taken the security of modulation modes of the physical layer into consideration. Aiming at this problem, a modulation protection algorithm based on wireless OFDM systems was proposed from the perspective of physical layer encryption. Modulation protection effect of the proposed algorithm was analyzed respectively in the cases of single-carrier and multi-carrier, and typical modulation identification methods in the cognitive radio were adopted in the simulation to analyze and compare the recognition rate before and after encryption. Theoretical analysis and simulation results show that this algorithm doesn't change the performance of original system, and has high capacity of modulation protection.

Keywords Modulation protection, Physical layer encryption, OFDM, Cognitive radio

1 引言

随着新一代宽带无线移动通信系统的迅速发展,通信系统趋于一体化,对信息的传输速率和移动通信终端的要求也越来越高[1]。与此同时,无线通信网络面临被随意窃听和由此引发的各种已知攻击和未知攻击,使得通信安全受到严重威胁。因此,如何保证无线通信网络和业务信息的安全性成为当前通信领域的研究热点[2]。

相较于传统的加密方法,物理层安全算法利用无线信道的物理特性可以显著提高加密效率和实时性[3-4]。由于认知无线电和调制识别技术的快速发展,无线信号的频率、带宽以及调制方式等相关信息容易被检测识别,窃听者可以获取大量无线数据,有针对性地对通信系统发起攻击,致使通信系统瘫痪[5-6]。然而,现有的大多数物理层安全算法没有考虑到调制信息的安全,没有对算法抵抗各种调制识别方法的能力进行分析,使得算法本身存在被窃听和被攻击的安全隐患[7-8]。例如,文献[9]提出了一种基于噪声覆盖的隐藏 OFDM 典型物理层安全算法,该算法产生一组与原 OFDM 信号子载波非正交的人工噪声信号,并在中频部分与正常信号叠加,之后由单天线发送,其具有良好的数据保护功能。但是算法本身的加密过程实质上仅仅是通过简单的加法运算完成,并且用来加密的噪声信号设置得过于简单且规律性很强。文献[10]的算法通过扰乱 OFDM 调制中的星座映射过程,使得非法用户无法辨别调制方式,达到保护调制方式的目的。然而,由于扰乱的加密矩阵放置在 IFFT 之前,窃听者可以通过截取一个子载波上的信号来恢复星座映射图案以实现调制方式的识别,因此该算法仍然存有漏洞。文献[11]提出了一种应用于 OFDM 无源光网络的双重星座加密安全算法,通过对子载波的星座映射图案进行双重加密来抵抗窃听者的星座图重构识别,但没有对算法抵抗其他调制识别的安全性能展开研究。

到稿日期:2017-12-08 返修日期:2018-03-25 本文受自然科学基金青年项目(61501372),陕西省自然科学基金项目(2017JM6012)资助。
高宝建(1963-),男,硕士,副教授,主要研究方向为物理层安全、信号处理;**王少迪**(1993-),男,硕士生,主要研究方向为物理层安全,E-mail:wittysandy@163.com(通信作者);**任宇辉**(1980-),男,博士,主要研究方向为电磁场与微波技术;**王玉洁**(1989-),女,硕士生,主要研究方向为无线通信安全。

针对上述问题和不足,本文提出了一种全新的调制方式保护算法,通过对角密钥矩阵与 IFFT 后的符号相乘对数据信息进行扰乱和加密,同时保护了物理层调制方式信息。理论分析和仿真结果验证了所提算法能够可靠并且有效地实现调制方式的保护与数据加密。

2　调制方式保护算法

调制方式保护算法的原理框图如图 1 所示。

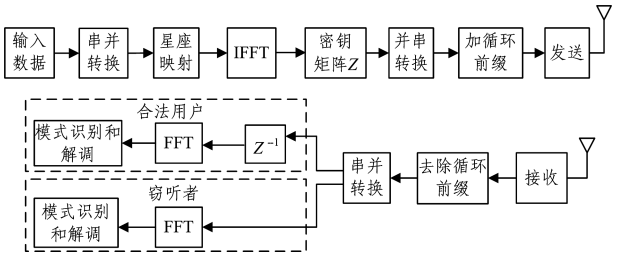


图 1　调制方式保护算法的原理框图

Fig. 1　Schematic diagram of modulation protection algorithm

算法的具体加密和解密步骤为:首先对输入数据进行串并转换,再由 MPSK/MQAM 星座映射得到符号向量 $S=[s_0,s_1,\cdots,s_{N-1}]^{\mathrm{T}}$,其中 N 为子载波个数,随后通过 IFFT 变换得到符号向量 $X=[X_0,X_1,\cdots,X_{N-1}]^{\mathrm{T}}$。在种子密钥的控制下,生成复杂的随机密钥矩阵 Z,将符号向量 X 与密钥矩阵 Z 相乘以实现加密保护,其等效于扰乱了 OFDM 符号向量 X 的相位信息。接着进行并串转换和添加循环前缀,最后发送加密符号。解密步骤为加密步骤的逆过程。

下面对密钥矩阵 Z 的生成方法进行介绍。首先采用计数器模式下的 AES 算法产生一串加密的二进制序列,选定长度为 128 比特的序列作为密钥 a_0。然后在计数器模式下生成 NL 比特的二进制数作为子密钥 a_n,其中 L 为可以改变密钥矩阵空间大小的调节参数。例如,当需要产生 NL 比特的子密钥 a_n 时,计数器只需计数$\lceil NL/128 \rceil$次。接着将子密钥 a_n 中的 0 和 1 依次以 L 位为一组,转换为由 $0,1,\cdots,2^L-1$ 构成的序列 $d(n)$,$n=0,1,\cdots,N-1$。通过 $d(n)$产生相位序列,表示为:

$$\theta_i=(d(n)/2^L)\times 2\pi,i=0,1,2,\cdots,N-1 \tag{1}$$

通过相位序列产生对角密钥矩阵 Z:

$$Z=\mathrm{diag}[\mathrm{e}^{\mathrm{j}\theta_0},\mathrm{e}^{\mathrm{j}\theta_1},\cdots,\mathrm{e}^{\mathrm{j}\theta_{N-1}}] \tag{2}$$

将密钥矩阵 Z 与向量 X 相乘后得到加密信息,表示为:

$$Y=ZX \tag{3}$$

加密信息在传输过程中会受到噪声干扰,因此接收端进行循环前缀移除和串并转换后,合法用户接收到的信号 Y_r 可表示为:

$$Y_r=Y+n \tag{4}$$

合法用户接收信号后,只需乘以密钥矩阵的逆矩阵 Z^{-1} 就可以获得解密信息 X_r,可表示为:

$$X_r=Z^{-1}Y_r \tag{5}$$

由于窃听者不能获取矩阵 Z^{-1},因此难以随机地构建出正确的解密矩阵。假设窃听者直接通过 Y_r 进行解调和调制方式识别,本文对这种情况下正确识别调制方式的可能性进行了分析研究。

3　调制方式保护算法

3.1　合法接收者

在 LTE 协议中,通过资源块的合理分配来实现多用户通信。假设第 i 位用户的资源块对应的 IFFT 矩阵为 W_i^{-1},$i=1,2,\cdots,v$,其中 $v=1,2,\cdots,q$ 表示每个子载波包含的符号个数,正交性使得 $W_iW_j^{-1}=0$,$i\neq j$。对于第 i 位合法用户,相应的解调过程可以表示为:

$$\begin{aligned}\hat{S}_i&=W_i\cdot Z^{-1}\Big(\sum_{j=1}^{v}Z\cdot W_j^{-1}\cdot S_j+n\Big)=\sum_{j=1}^{v}W_i\cdot Z^{-1}\cdot Z\cdot W_j^{-1}\cdot S_j+W_i\cdot Z^{-1}\cdot n\\&=W_i\cdot W_i^{-1}\cdot S_i+W_i\cdot Z^{-1}\cdot n\\&=S_i+W_i\cdot Z^{-1}\cdot n\end{aligned} \tag{6}$$

式(6)为合法用户解调的简约表达,发射端在 IFFT 后进行了密钥矩阵加密,接收端对含有噪声的加密信号乘以解密矩阵后再进行正常解调。可以看出,所提算法只是在解调过程中增加了密钥矩阵 Z 的逆矩阵 Z^{-1} 与噪声向量 n 相乘的部分,后续仿真结果表明增加的部分对正确解调的影响很小。

3.2　窃听者

窃听者在不知道密钥矩阵 Z 的情况下直接进行解调会使得子载波间原有的正交性遭到破坏,难以获得正确的传输信息。假定星座映射后连续传输的符号向量为 S^v,则窃听者获取的符号向量 S_e^v 可由式(7)获得:

$$\begin{aligned}S_e^v&=W\cdot Z\cdot W^{-1}\cdot S^v=\frac{1}{N}\begin{bmatrix}\sum_{i=0}^{N-1}\mathrm{e}^{\mathrm{j}\theta_i} & \sum_{i=0}^{N-1}\mathrm{e}^{\mathrm{j}(\theta_i+\frac{2\pi}{N}i)} & \cdots & \sum_{i=0}^{N-1}\mathrm{e}^{\mathrm{j}[\theta_i+\frac{2\pi}{N}i(N-1)]}\\ \sum_{i=0}^{N-1}\mathrm{e}^{\mathrm{j}(\theta_i-\frac{2\pi}{N}i)} & \sum_{i=0}^{N-1}\mathrm{e}^{\mathrm{j}\theta_i} & \cdots & \sum_{i=0}^{N-1}\mathrm{e}^{\mathrm{j}[\theta_i+\frac{2\pi}{N}i(N-2)]}\\ \vdots & \vdots & \ddots & \vdots\\ \sum_{i=0}^{N-1}\mathrm{e}^{\mathrm{j}[\theta_i-\frac{2\pi}{N}i(N-1)]} & \sum_{i=0}^{N-1}\mathrm{e}^{\mathrm{j}[\theta_i-\frac{2\pi}{N}i(N-2)]} & \cdots & \sum_{i=0}^{N-1}\mathrm{e}^{\mathrm{j}\theta_i}\end{bmatrix}\begin{bmatrix}s_0^v\\ s_1^v\\ \vdots\\ s_{N-1}^v\end{bmatrix}\\&=\frac{1}{N}\Big[\sum_{k=0}^{N-1}s_k^v\Big(\sum_{i=0}^{N-1}\mathrm{e}^{\mathrm{j}(\theta_i+\frac{2\pi}{N}ik)}\Big),\cdots,\sum_{k=0}^{N-1}s_k^v\Big(\sum_{i=0}^{N-1}\mathrm{e}^{\mathrm{j}(\theta_i+\frac{2\pi}{N}i(k-N+1))}\Big)\Big]^{\mathrm{T}}\\&=[f_0(\theta_0,\theta_1,\cdots,\theta_{N-1},s_0^v,s_1^v,\cdots,s_{N-1}^v),\cdots,f_{N-1}(\theta_0,\theta_1,\cdots,\theta_{N-1},s_0^v,s_1^v,\cdots,s_{N-1}^v)]\end{aligned} \tag{7}$$

式(7)是窃听者解调的简约表达,发射端在 IFFT 后进行密钥矩阵加密,窃听者对接收到的信号直接进行解调。可以看出,窃听者所获获得的星座符号包含相位向量 θ_i 和原始数据 s_k^v 的复杂非线性函数,并且 θ_i 由密钥控制生成。因此窃听

者难以获取原始正确的符号向量 S^v。

此外，窃听者可以截取某一固定子载波上的符号向量进行解调，当对第 n 个子载波上的符号进行向量解调时，窃听者恢复的符号向量可由式(8)运算获得，记为 S'_{en}：

$$S'_{en}=\frac{1}{N}\left[\sum_{k=0}^{N-1}s_k^1\left(\sum_{i=0}^{N-1}e^{j[\theta_i+\frac{2\pi}{N}i(k-n+1))}\right),\cdots,\sum_{k=0}^{N-1}s_k^q\left(\sum_{i=0}^{N-1}e^{j(\theta_i+\frac{2\pi}{N}i(k-n+1))}\right)\right]$$
$$=\left[g_1(\theta_0,\cdots,\theta_{N-1},s_0^1,\cdots,s_{N-1}^1),\cdots,g_q(\theta_0,\cdots,\theta_{N-1},s_0^q,\cdots,s_{N-1}^q)\right] \tag{8}$$

由式(8)可以看出，窃听者仍然难以从一组关于相位向量 θ_i 和原始数据 s_k^v 的非线性函数中获取原始传输信息。上述分析表明，所提算法可以保证密钥信息和传输数据的安全。接下来需要对所提算法的抵抗调制识别攻击性能进行分析。

3.3 抵抗调制识别攻击性能分析

瞬时参数调制识别方法首先从信号中获取瞬时相位 ϕ_{NL} 与瞬时幅度 $A(i)$ 信息，然后由式(9)获得主要的识别参数 σ_{ap}[12-13]：

$$\sigma_{ap}=\sqrt{\frac{1}{C}\left(\sum_{A_n(i)>a_\tau}\phi_{NL}^2(i)\right)-\left(\frac{1}{C}\sum_{A_n(i)>a_\tau}|\phi_{NL}(i)|\right)^2} \tag{9}$$

由于瞬时相位 ϕ_{NL} 受到所提算法的密钥信息控制，可以看出窃听者提取的瞬时参数 σ_{ap} 也会受到密钥的影响，难以有效地进行调制方式识别。

高阶累积量调制识别方式通常采用四阶累积量 C_{40} 作为识别参数[14-15]，结合所提算法可得加密信号的 C'_{40} 表达式为：

$$C'_{40}=\frac{1}{N}\sum_{i=1}^{N}(S_e^v(i))^4-\frac{3}{N^2}\left(\sum_{i=1}^{N}(S_e^v(i))^2\right)^2 \tag{10}$$

可以看出窃听者提取的四阶累积量 C'_{40} 包含受到密钥影响的符号向量 S_e^v，因此其同样难以有效地进行调制识别。

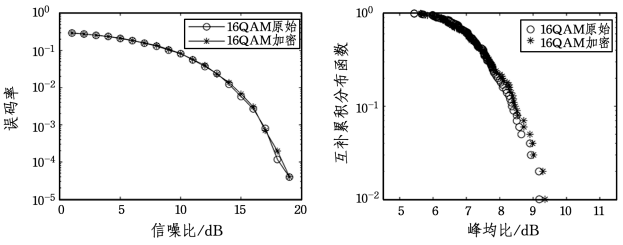
对于重构星座图调制识别方式，所提安全算法的密钥矩阵操作使得加密信号的星座分布被打乱，这就导致星座图重构时难以正确匹配星座映射图案，无法有效地进行调制方式的识别。因此以上 3 种调制识别方法都无法获取信号的正确调制方式。

4 仿真结果和分析

在数值仿真中，取 OFDM 系统的子载波数 N 为 128，混沌序列的初值为 0.5，密钥空间调节参数 L 为 3。实验中采用 1000 个 OFDM 符号的平均值作为每个信噪比下的误码率。信道为理想的高斯加性白噪声信道。本节对 QPSK，8PSK 和 16QAM 3 种调制方式下的加解密过程及算法安全性能进行仿真分析。

4.1 算法对系统固有性能的影响

图 2(a)展示了 16QAM 调制方式下，加密前后的误码率曲线，可以看出，应用加密算法后并不会使误码率曲线产生明显改变，表明所提算法不会影响系统固有的误码性能。图 2(b)为 16QAM 调制方式下加密前后系统的峰均比曲线，可以看出，所提算法同样不会影响系统固有的峰均比。同样地，当采用 QPSK 和 8PSK 调制方式时，所提算法也不会对系统的固有性能产生额外影响。



(a)16QAM 调制方式下加密前后的误码率　(b)16QAM 调制方式下加密前后的峰均比

图 2　算法对系统固有性能的影响

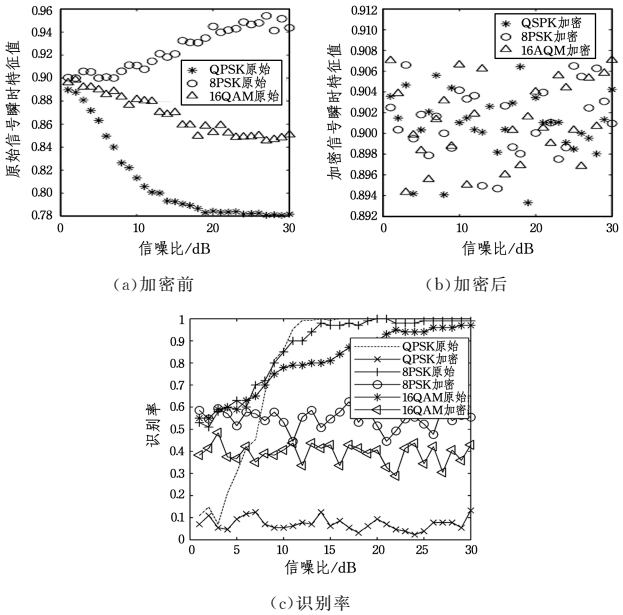
Fig. 2　Influence of proposed algorithm on inherent performance of system

4.2 调制方式保护性能分析

非法接收者可以采取两种信号窃取方式：直接截取 OFDM 符号进行数据信息解调(见式(7))；截取某一固定子载波上的符号向量进行解调(见式(8))。因此，在进行调制方式保护的性能分析时，需要对这两种情况分别进行分析和研究，以进一步保证调制信息的安全性。

4.2.1 基于瞬时特征的调制方式识别

通过前文所提的瞬时参数 σ_{ap}，利用判决理论和合理的阈值对 QPSK，8PSK 和 16QAM 3 种调制方式进行区分和识别[10]。图 3(a)和图 3(b)展示了第 128 位子载波信号加密前后所提取瞬时参数 σ_{ap} 值的变化情况。未经加密保护时，3 种调制方式的瞬时参数呈现出明显的分离趋势，并且随着信噪比的增加，分离趋势越来越明显。而当采用加密算法后，3 种调制信号的瞬时参数呈现出相互混叠的状态。通过图 3(c)所示的调制识别率曲线可以看出，应用加密算法后，该调制识别方式下的识别率均有所下降，特别是 QPSK 调制下的识别率下降速度明显。



(a)加密前　(b)加密后

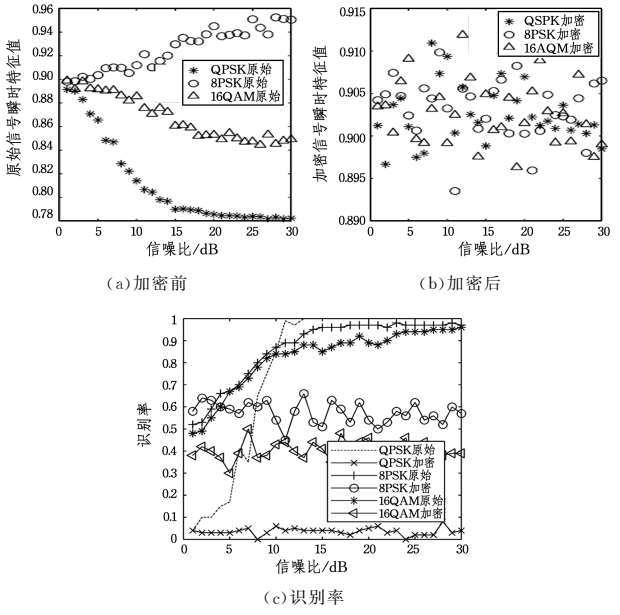
(c)识别率

图 3　基于子载波识别的瞬时特征值和识别率

Fig. 3　Instantaneous parameter and recognition rate based on sub-carriers

图 4(a)和图 4(b)展示了在直接截取 OFDM 符号进行数

据信息解调的方法下，加密前后所提取的瞬时参数 σ_{ap} 值的变化情况。与未经加密保护的瞬时参数相比，加密信号的瞬时参数同样呈现出相互混叠的状态。图 4(c)所示的调制识别率曲线也呈现出下降的趋势。综上所述，所提算法可以在一定程度上抵抗基于瞬时参数的调制方式识别。



(a)加密前　(b)加密后

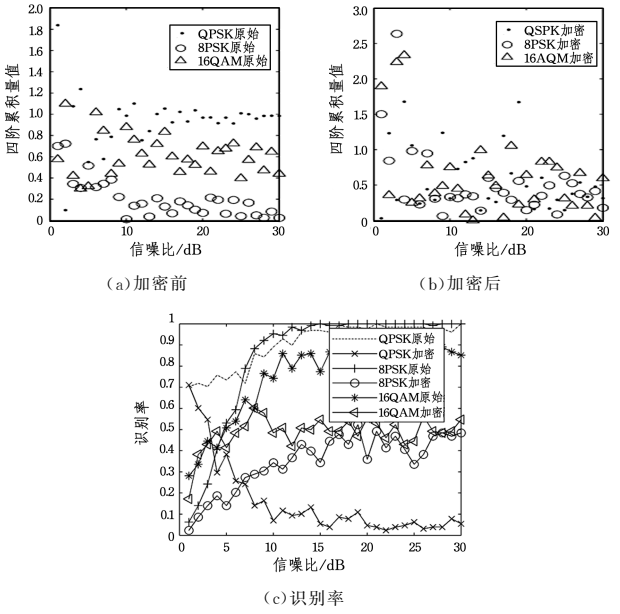
(c)识别率

图 4　基于 OFDM 符号识别的瞬时特征值和识别率

Fig. 4　Instantaneous parameter and recognition rate based on OFDM symbols

4.2.2　基于高阶统计量的调制方式识别

利用前文所提的四阶累积量 $|C_{40}|$，可以对 QPSK，8PSK 和 16QAM 3 种调制方式进行区分和识别[10]。图 5(a)和图 5(b)描述的是第 56 位子载波信号加密前后，高阶累积量 $|C_{40}|$ 值的变化情况。



(a)加密前　(b)加密后

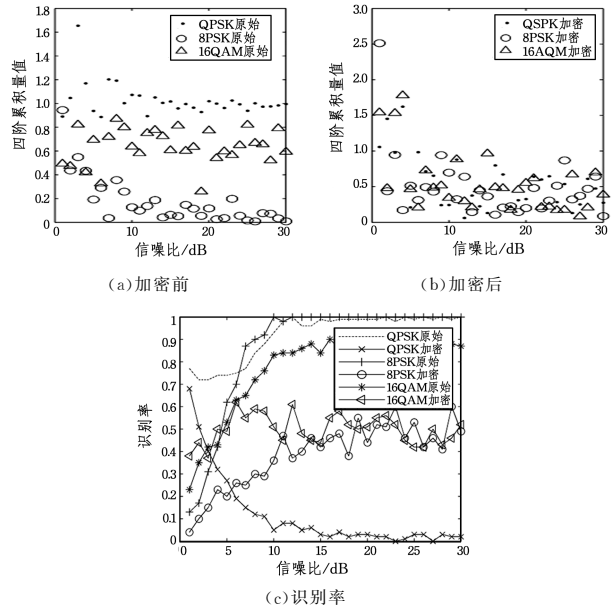
(c)识别率

图 5　基于子载波识别的四阶累积量和识别率

Fig. 5　Fourth-order cumulant and recognition rate based on sub-carriers

从图 5 可以看出，当采用加密算法后，3 种调制信号的四阶累积量值不再呈现出分离的趋势，而是相互混叠难以区分，特别是 8PSK 调制下，信号的四阶累积量值分布范围明显扩大。通过图 5(c)所示的调制识别率曲线可以看出，QPSK 调制下的加密信号识别率随着信噪比的增大下降明显，8PSK 和 16QAM 调制下的识别率也都产生了较大幅度的下降。

另一种信号截取方法的仿真分析如图 6 所示。当采用所提加密算法后，非法窃听者对 3 种调制方式下的加密信号四阶累积量值均不能进行有效区分。识别率曲线也体现出加密算法具有抵抗该调制识别方法的安全性能。以上仿真结果验证了所提加密算法同样可以有效地抵抗提取高阶累积量的调制识别攻击。



(a)加密前　(b)加密后

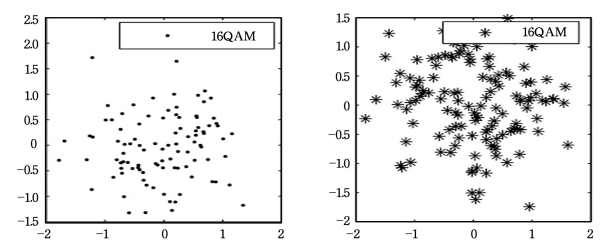
(c)识别率

图 6　基于 OFDM 符号识别的四阶累积量和识别率

Fig. 6　Fourth-order cumulant and recognition rate based on OFDM symbols

4.2.3　基于星座图重构的调制识别

通过重构星座图的调制识别方式也可以对 QPSK，8PSK 和 16QAM 3 种调制方式进行区分和识别。从图 7 可以看出，对于非法接收者采用的基于子载波和 OFDM 符号识别的两种窃听方式，16QAM 调制方式下加密信号的重构星座点都呈现无规律的随机分布，难以正确匹配星座映射图案，无法进行调制方式识别。同样地，当采用 QPSK 和 8PSK 调制方式时，也不能通过重构星座图的方法对调制方式进行有效识别。



(a)基于子载波识别的重构星座图　(b)基于 OFDM 符号识别的重构星座图

图 7　基于星座图重构的调制识别

Fig. 7　Modulation recognition based on reconstructing constellation

通过对系统固有性能的影响和抵抗 3 种调制识别算法的仿真分析，表明所提算法能够在不影响系统固有性能的前提下实现对物理层调制方式信息的保护。

结束语 本文从物理层安全的角度，提出了一种基于无线 OFDM 系统的调制方式保护算法。通过将对角密钥矩阵与 IFFT 后的符号相乘，进一步对数据信息完成了扰乱和加密，使得物理层调制信息得到保护，同时也保证了数据信息的安全。仿真结果表明，应用所提算法前后系统的误码率和峰均比并无较大变化。采用基于瞬时特征、高阶统计量以及星座图重构的调制识别方法得到了系统加密前后的识别结果，算法加密后，3 种调制识别方法的识别率均明显下降，这表明所提算法具有不错的抵抗调制识别性能。未来可以对更多的调制识别方法进行研究，构建出抵抗调制识别性能更加优异和全面的安全算法。

参 考 文 献

[1] BARENGHI A, BREVEGLIERI L, KOREN I, et al. Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures[J]. Proceeding of The IEEE, 2012, 100(11): 3056-3076.

[2] MU P C, YIN Q Y, 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. (in Chinese)
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.

[3] LIN T, HUANG K Z, LUO W Y. A Multicarrier-based Physical Layer Security Scheme for the Multicast Systems[J]. Journal of Electronics and Information Technology, 2013, 35(6): 1388-1343. (in Chinese)
林通，黄开枝，罗文宇. 一种基于多载波的多播系统物理层安全方案[J]. 电子与信息学报，2013，35(6)：1338-1343.

[4] LI M L, HUANG K Z, ZHONG Z. Physical-layer Security Algorithm Based on Joint Scrambling with Spatial and Frequency Resource[J]. Journal of Electronics and Information Technology, 2013, 35(12): 2966-2971. (in Chinese)
李明亮，黄开枝，钟州. 基于空频联合加扰的物理层安全算法[J]. 电子与信息学报，2013，35(12)：2966-2971.

[5] LIU Y, WANG G P, XIAO M, et al. Spectrum Sensing and Throughput Analysis for Cognitive Two-Way Relay Networks with Multiple Transmit Powers[J]. IEEE Journal on Selected Areas in Communications, 2016, 34(11): 3038-3047.

[6] JIANG H Q, TANG P Z, GUAN W S. Research on Signal Modulation Recognition Technology Based on PDW[J]. Transactions of Beijing Institute of Technology, 2013, 33(11): 1183-1188. (in Chinese)
江海清，唐浦钊，关文硕. 基于脉冲描述字的信号调制识别技术研究[J]. 北京理工大学学报，2013，33(11)：1183-1188.

[7] ALI A, FAN Y, SHU L. Automatic Modulation Classification of Digital Modulation Signals with Stacked Autoencoders[J]. Digital Signal Processing, 2017, 71: 108-116.

[8] MAREY M, DOBRE O A, INKOL R. Blind STBC Identification for Multiple-Antenna OFDM Systems[J]. IEEE Transactions on Communications, 2014, 62(5): 1554-1567.

[9] CHORTI A. Masked OFDM: A Physical Layer Encryption for Future OFDM Applications[C]// IEEE Globecom Workshop on Mobile Computing and Emerging Communication Networks. 2010: 1254-1258.

[10] GAO B J, WANG Y J, LUO Y L, et al. A Hiding Algorithm for OFDM Constellation Mapping Based on Physical Layer Encryption[J]. Journal of Applied Sciences, 2013, 13(18): 3790-3797.

[11] LIU B, ZHANG L, XIN X, et al. Constellation-masked Secure Communication Technique for OFDM-PON[J]. Optics Express, 2012, 20(22): 25161.

[12] BASAR B. On Multiple-Input Multiple-Output OFDM with Index Modulation for Next Generation Wireless Networks[J]. IEEE Transactions on Signal Processing, 2016, 64(15): 3868-3878.

[13] ZHENG B, CHEN F, WEN M, et al. Low-Complexity ML Detector and Performance Analysis for OFDM With In-Phase/Quadrature Index Modulation[J]. IEEE Communications Letters, 2015, 19(11): 1893-1896.

[14] YOU L, GAO X, SWINDLEHURST A L, et al. Low-Complexity ML Detector and Performance Analysis for OFDM With In-Phase/Quadrature Index Modulation[J]. IEEE Transactions on Signal Processing, 2016, 64(6): 1461-1476.

[15] GORCIN A, ARSLAN H. An OFDM Signal Identification Method for Wireless Communications Systems[J]. IEEE Transactions on Vehicular Technology, 2015, 64(12): 5688-5700.

(上接第 50 页)

[14] YAO Y Y. Three-way decisions and cognitive computing[J]. Cognitive Computation, 2016, 8(4): 543-554.

[15] YAO Y Y. Three-Way Decision: An Interpretation of Rules in Rough Set Theory[C]// RSKT. 2009: 642-649.

[16] YAO Y Y. Three-way decisions with probabilistic rough sets [J]. Information Sciences, 2010, 180(3): 341-353.

[17] QI J J, WEI L, YAO Y Y. Three-way formal concept analysis [C]// Rough sets and Knowledge Technology. Springer, Heidelberg, 2014: 732-741.

[18] REN R, WEI L. The attribute reductions of three-way concept lattices[J]. Knowledge-Based Systems, 2016, 99(C): 92-102.

[19] LIU L, QIAN T, WEI L. Rules extraction in formal decision contexts based on attributes-Induced three-way concept lattices [J]. Journal of Northwest University(Natural Science Edition), 2016, 46(4): 481-487. (in Chinese)
刘琳，钱婷，魏玲. 基于属性导出三支概念格的决策背景规则提取[J]. 西北大学学报(自然科学版)，2016，46(4)：481-487.

[20] WEI L, QI J J, ZHANG W X. Attribute reduction theory of concept lattice based on decision formal contexts[J]. Science in China E: Information Sciences, 2008, 38(2): 195-208. (in Chinese)
魏玲，祁建军，张文修. 决策形式背景的概念格属性约简[J]. 中国科学 E 辑：信息科学，2008，38(2)：195-208.