系统工程与电子技术 2010, 32(1) 195-199 DOI: ISSN: 1001-506X CN: 11-2422/TN

软件、算法与仿真

认知系统AES-LDPC纠错加密器的设计与性能分析

鲁凌云1, 肖扬1, 姜月秋2, 宋丽丽1

(1. 北京交通大学信息科学研究所, 北京 100044; 2. 沈阳理工大学信息通信工程学院, 辽宁 沈阳 110168)

摘要:

在多跳的认知系统中，由于不存在可信实体作为服务器控制密钥分发，安全性将面临更大挑战，需要建立完善的加密体系结构来解决这一问题。将高级加密标准AES和在通信纠错领域性能优异的低密度奇偶校验码（low-density parity-check, LDPC）结合，设计出了分组长度为128 bit的六轮宽轨迹加密策略、密钥由128 bit AES密钥和LDPC生成矩阵组成的LDPC纠错加密器。由于LDPC生成矩阵具有更好的扩散性能，使得这种新设计的LDPC纠错加密器能在更少的轮数下具有较好的安全性。最后，通过实验结果验证了AES-LDPC纠错加密器的性能。

关键词： 认知无线电 高级加密标准 LDPC编码 交织干扰器

Design and performance analysis of AES-LDPC error correcting cipher for cognitive radio systems

LU Ling-yun1, XIAO Yang1, JIANG Yue-qiu2, SONG Li-li1

(1. Inst. of Information Science, Beijing Jiaotong Univ., Beijing 100044, China; 2. Coll. of Computer and Communication, Shenyang Inst. of Technology, Shenyang 110168, China)

Abstract:

In the hopping cognitive radio (CR) system, the security is facing a challenge because there does not exist that a server as the credible entity to display the keyboard. So it is necessary to enhance the encrypting system to solve the problem. The paper presents an LDPC error correcting cipher by combining the advanced encryption standard (AES) and LDPC code. The LDPC error correcting cipher, which is based on wide trail strategy, is a six round block cipher that encrypts 128 bit plaintexts, and the key is composed of 128 bit AES secret keys and an LDPC generator matrix. By using the LDPC generator matrix with high performance in the property of diffusion, the LDPC error correcting cipher has a fairly good property in security in fewer rounds. Simulation results show that the processes of encrypting/decrypting have the better performance.

Keywords: cognitive radio advanced encryption standard LDPC channel coding interleaving jammer

收稿日期 修回日期 网络版发布日期

DOI:

基金项目:

通讯作者:

作者简介:

作者Email:

参考文献:

本刊中的类似文章

1. 薛 楠, 周贤伟, 林 琳, 周 健.性能优化的认知无线电网络安全路由选择算法[J]. 系统工程与电子技术, 2009,31(11): 2756-2760
2. 李一兵, 杨蕊, 高振国.基于着色理论的认知无线电频谱分配算法[J]. 系统工程与电子技术, 2010,32(6): 1109-1112
3. 张继良, 汪洋, 刘法, 张乃通.控制信道受限的认知无线电联合频谱感知[J]. 系统工程与电子技术, 2010,32(6): 1113-1116
4. 焦传海, 王可人.一种基于免疫遗传算法的认知决策引擎[J]. 系统工程与电子技术, 2010,32(05): 1083-1087

5．蒋清平，杨士中， 张天骐， 任智.时变衰落信道下OFDM信号参数融合估计[J]. 系统工程与电子技术, 2011,33(7期): 1627-1632
6．邹卫霞, 丁奇, 周正, 张春青.基于特征值极限分布的双门限频谱感知算法[J]. 系统工程与电子技术, 2012,34(3): 588-591
7．汤海冰, 胡志刚.认知无线电系统帧长参数优化[J]. 系统工程与电子技术, 2012,34(9): 1918-1922
8．陈昊, 杨俊安, 吴彦华.认知无线电中的一种频谱盲感知算法[J]. 系统工程与电子技术, 2009,31(6): 1311-1313
