文算法.但是由于其算法设置在 IDFT 之后,加密过程虽然破坏了子载波的正交性,提高了加密效果,但是同样破坏了 IDFT 的循环特性,为合法接收者设置循环前缀,实现系统同步造成了困难.而本文算法设置在 IDFT 之前,不会造成这样的影响.

总之,本文算法是针对现有物理层安全算法存在的密钥空间依赖于子载波个数和不能抵抗明文密文对攻击的共性问题而提出的,算法充利用 DFT-S-OFDM 体制的调制特点,合理设置密钥,利用物理层的已有的调制环节设置加密算法,使得明文、密文和密钥之间形成非线性方程组关系,在子载波数较小的情况下,不仅保证了密钥的安全,而且也实现了数据的可靠保护.

8 结 论

本文提出了一种基于 DFT-S-OFDM 传输方式的物理层双矩阵密钥加密算法.理论分析和仿真结果说明,在较小子载波数的情况下,算法在第一种密钥工作模式下,可以有效抵抗穷举攻击和明文密文对的攻击,可以有效保护无线数据连路;在第二种密钥工作模式下,可以通过控制发射功率,利用信道噪声保证算法安全.理论分析和仿真结果表明,算法对原系统的峰均比、误码率影响很小,具有良好的适应性.从而可以有效解决终端能源、计算能力等受限的无线宽带通信系统的安全问题.

致 谢 感谢徐捷、罗永玲、王少迪等所有为本文研究给予支持和帮助的人!

参 考 文 献

[1] Wang Ying-Min, Sun Shao-Hui. TD-LTE Principle and System Design. Beijing: The People's Posts and Telecommunications Press, 2010(in Chinese)
(王映民, 孙韶晖. TD-LTE 技术原理与系统设计. 北京: 人民邮电出版社, 2010)

[2] Chen Xi, Li An, Gao Guanjun. Experimental demonstration of improved fiber nonlinearity tolerance for unique-word DFT-spread OFDM systems. Optics Express, 2011, 19(27): 26198-26207

[3] Shulkind G, Nazarathy M. An analytical study of the improved nonlinear tolerance of DFT-spread OFDM and its unitary-spread OFDM generalization. Optics Express, 2012, 20(23): 25884

[4] Huo F, Gong G. A new efficient physical layer OFDM encryption scheme//Proceedings of the IEEE INFOCOM 2014-IEEE Conference on Computer Communications. Toronto, Canada, 2014: 1024-1032

[5] Hu Xiannan, Yang Xuelin, Shen Zanwei, et al. Chaos-based partial transmit sequence technique for physical layer security in OFDM-PON. IEEE Photonics Technology Letters, 2015, 27(23): 1-1

[6] Liu Bo, Zhang Lijia, Xin Xiangjun, et al. Physical layer security in OFDM-PON based on dimension-transformed chaotic permutation. IEEE Photonics Technonlogy Letter, 2014, 26(2): 127-130

[7] Zhang Lijia, Xin Xiangjun, Liu Bo, et al. Secure OFDM-PON based on chaos scrambling. IEEE Photonics Technology Letters, 2011, 23(14): 998-1000

[8] Liu Bo, Zhang Lijia, Xin Xiangjun, et al. Physical layer security in CO-OFDM transmission system using chaotic scrambling. Optics Communications, 2011, 1: 1-8

[9] Ma Ruifeng, Dai Linglong, Wang Zhaocheng, et al. Secure communication in TDS-OFDM system using constellation rotation and noise insertion. IEEE Transactions on Consumer Electronics, 2010, 56(3): 1328-1332

[10] Reilly D, Kanter G S. Noise-enhanced encryption for physical layer security in an OFDM radio//Proceedings of the 2009 IEEE Radio and Wireless Symposium, San Diego, USA, 2009: 344-347

[11] Dong Jian-E, Gao Bao-Jian, Du Min. Low-PAPR OFDM algorithm to guarantee data security. Computer Engineering, 2011, 37(2): 286-289(in Chinese)
(董建娥, 高宝建, 杜敏. 一种保证数据安全的低峰平比 OFDM 算法. 计算机工程, 2011, 37(2): 286-289)

[12] Chorti A. Masked-OFDM: A physical layer encryption for future OFDM applications//Proceedings of the IEEE Globecom 2010 Workshop on Mobile Computing and Emerging Communication Networks. Miami, USA, 2010: 1254-1258

[13] Yucek T, Arslan H. Feature suppression for physical-layer security in OFDM systems//Proceedings of the 2007 IEEE Military Communications Conference. Orlando, USA, 2007: 1-5

[14] Gallo G. Complexity Issues in Computational Algebra [Ph. D. dissertation]. Courant Institute of Mathematical Sciences, New York University, New York, USA, 1992

[15] Hansen E. Numerical methods for unconstrained optimization and nonlinear equations (J. E. Dennis, Jr. and Robert B. Schnabel). SIAM Review, 1986, 28(3): 417-419

[16] Wu W J. On the decision problem and the mechanization of theorem-proving in elementary geometry. Science in China Ser A, 1979, 21(2): 117-138

[17] Wu F F, Sadatoshi K. Steady-state security regions of power systems. IEEE Transactions on Circuits and Systems, 1982, 29(11): 703-711

[18] Slimane S B. Reducing the peak-to-average power ratio of OFDM signals through precoding. IEEE Transactions on Vehicular Technology, 2007, 56(2): 686-695

GAO Bao-Jian, born in 1963, associate professor. His research interests include physical layer security and communication signal processing.

HUANG Shi-Ya, born in 1990, M. S. His research interest is physical layer security.

JING Li, born in 1991, M. S. Her research interest is physical layer security.

HU Yun, born in 1990, M. S. Her research interest is physical layer security.

Background

This paper explored the physical layer encryption technology. With bandwidth broadening and merging of the wireless communication system, foreign scholars have been paying attention to such security problems of the physical layers encryption and algorithm studies of the physical layer. In OFDM transmitting system, some algorithms exhibiting satisfied results are born, like constellation scrambling, constellation random phase rotation, and noise cover. However, with the superb transmission performance required, the physical layer encryption algorithms are confined to simple encrypting process, which make the algorithms themselves unsafe and cannot resist plaintext to ciphertext attacking. Generally, the size of key spaces proportional to the number of subcarriers. The algorithm safety drops dramatically when the number of subcarriers become less.

The aiming at the safety problem of existing algorithms, subcarrier fewer DFT-S-OFDM system as the research object, combined with LTE's resource partitioning and scheduling model design a double matrix key physical layer encryption algorithm based on, the algorithm can effectively guarantee the security of the wireless data link. The peaks of the original system are influenced the inherent properties of ratio and bit error rate. Under the condition that the number of sub carriers is greater than or equal to 12, the larger key space can be guaranteed, which can resist the attack of the plain text cipher text, and overcome the security problems of the existing algorithms.

Our research team has undertaken the Shaanxi Natural Science Foundation Project (2011JM8034) "Data Security New Mechanism Research Combined with the Characteristics of OFDM Modulation", which was completed in 2013. And our team is committed to the National Natural Science Foundation of China (61501372) and the Shaanxi Province Natural Science Foundation (2017JM6012). The physical layer security algorithm based on the unitary matrix pre coding is proposed, which is based on the interpolation of the physical layer security algorithm. And has made the physical layer encryption aspect of the invention patent (ZL 2013 1 0337275. X).