计算机工程 2012, 38(3) 246-248 DOI: 10.3969/j.issn.1000-3428.2012.03.081 ISSN: 1000-3428 CN: 31-1289/TP

工程应用技术与实现

铁路信号安全通信协议中的MAC改进算法

张元玲，徐中伟，万勇兵，夏志翔

(同济大学电子与信息工程学院，上海 201804)

摘要： 改进铁路信号安全通信协议II(RSSP-II)中的ER层消息验证码(MAC)算法，将高级加密标准作为MAC的核心算法，使用密文分组链接方式对报文加解密，并将其运用到CTCS-3列控系统临时限速服务器测试平台的RSSP-II仿真测试中。结果表明，改进算法能够克服原算法存在的弱密钥、半弱密钥等安全隐患，具有更强的安全性与实时性。

关键词： 铁路信号安全通信协议II 数据加密标准 高级加密标准 密文分组链接 消息验证码

Improved MAC Algorithm in Railway Signal Safety Communication Protocol

ZHANG Yuan-ling, XU Zhong-wei, WAN Yong-bing, XIA Zhi-xiang

(School of Electronics and Information Engineering, Tongji University, Shanghai 201804, China)

Abstract: To improve Message Authentication Code(MAC) algorithm of ER in Railway Signal Safety Communication Protocol II(RSSP-II), an improved MAC algorithm using Advanced Encryption Standard (AES) as core algorithm and Cipher Block Chaining(CBC) as encryption and decryption method is put forward. The proposed method will be applied to RSSP-II simulation test in TSRS test platform of CTCS-3, whose results show that the improved algorithm conquers such safety problems as weak key and semi weak key, thus having more advantage in safety and real-time compared.

Keywords: Railway Signal Safety Communication Protocol II(RSSP-II) Data Encryption Standard(DES) Advanced Encryption Standard(AES) Cipher Block Chaining(CBC) Message Authentication Code(MAC)

收稿日期 2011-08-08 **修回日期** **网络版发布日期** 2012-02-05

DOI: 10.3969/j.issn.1000-3428.2012.03.081

基金项目:

通讯作者:

作者简介: 张元玲(1987－)，女，硕士研究生，主研方向：软件形式化建模与仿真；徐中伟，教授、博士生导师；万勇兵，博士研究生；夏志翔，硕士研究生

通讯作者E-mail: cloudylynn@163.com

参考文献：

[1] 于宏博. 中国列车控制系统(CTCS)安全通信机制的研究[D]. 北京: 北京交通大学.[J]..2004,:-

[3] 杨小红. 基于MAC认证的新型确定性包标记[J].计算机工程.2010, 36(16):148-150 浏览

[6] Stinson D R. Cryptography Theory and Practice[M]. 2nd ed. [S. l.]: CRC Press.[J]..2002,:-

本刊中的类似文章

1. 邱伟星, 肖克芝, 倪昉, 黄华.一种DES密钥延长方法[J]. 计算机工程, 2011,37(5): 167-168,171
2. 胡伟.基于嵌入式Linux的RFID安全性研究[J]. 计算机工程, 2011,37(23): 155-158
3. 王红胜, 宋凯, 张阳, 陈开颜.针对高级加密标准算法的光故障注入攻击 [J]. 计算机工程, 2011,37(21): 97-99
4. 张新贺, 张月华, 白茹雪, 刘鸿雁.AES算法优化及其在ARM上的应用[J]. 计算机工程, 2011,37(18): 142-144
5. 常小龙, 丁国良, 武翠霞, 王创伟.抗电磁侧信道攻击的AES S盒设计[J]. 计算机工程, 2011,37(17): 93-95
6. 曾永红;叶旭鸣.抗差分功耗分析攻击的AES S盒电路设计[J]. 计算机工程, 2010,36(9): 20-22
7. 冷 文;曹进才;王安国.基于小型FPGA的快速AES算法研究[J]. 计算机工程, 2010,36(7): 159-161
8. 刘上力;赵劲强;聂勤务.AES差分故障攻击的建模与分析[J]. 计算机工程, 2010,36(1): 189-190,
9. 张新贺;张月华;刘鸿雁.

基于FPGA的16位数据路径的AES IP核

[J]. 计算机工程, 2009,35(24): 162-164
10. 王简瑜;张鲁国.基于FPGA的AES加/解密算法的可重构设计[J]. 计算机工程, 2008,34(7): 163-164,

文章评论

反馈人		邮箱地址	
反馈标题		验证码	4379
	5		