计算机工程与应用 2010 46 (6): 103-106 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

IEEE802.16e标准安全机制的改进

朱英敏[1]，黄生叶[1]，冯穗力[2]，叶 梧[2]
1.湖南大学 计算机与通信学院，长沙 410082
2.华南理工大学 电子与信息学院，广州 510640

收稿日期 2008-8-27 修回日期 2008-10-31 网络版发布日期 2010-2-23 接受日期

摘要 指出了IEEE802.16e安全机制中所存在的严重漏洞。针对无线移动设备存在存储容量有限、处理速度慢、带宽低等问题，利用无线公钥设施中的证书标识符URL和椭圆曲线加密算法对IEEE802.16e中的密钥管理协议（PKM）进行了改进。仿真结果表明改进后的安全机制更适合于无线网络环境。

关键词 IEEE802.16e 安全机制 密钥管理协议 无线公钥设施
分类号 TP309

Improved security mechanism for IEEE802.16e standard

ZHU Ying-min[1]，HUANG Sheng-ye[1]，FENG Hui-li[2]，YE Wu[2]

1.College of Computer and Communication，Hunan University，Changsha 410082，China
2.College of Electronics and Information，South China University of Technology，Guangzhou 510640，China

Abstract
This paper points out some serious leaks in the security mechanism of IEEE802.16e.In the face of limited resources of wireless mobile devices such as low processing，bandwidth and storage capabilities，this paper utilizes the certificate URL in the WPKI and ECC encryption algorithm to improve the Key Management Protocol（PKM） of IEEE802.16e.The simulator result shows that the improved security mechanism is more suitable for the wireless network.

Key words IEEE802.16e security mechanism Key Management Protocol（PKM） Wireless Public Key Infrastructure（WPKI）

DOI: 10.3778/j.issn.1002-8331.2010.06.030

通讯作者 朱英敏 zhuyingmin_2002@163.com