电子与信息学报
JOURNAL OF ELECTRONICS & INFORMATION TECHNOLOGY

电子与信息学报 » 2010, Vol. 32 » Issue (9) :2106-2111 DOI: 10.3724/SP.J.1146.2009.01191

论文

协议组合逻辑安全的WiMAX无线网络认证协议

冯涛[①②③] 张子彬[①] 马建峰[②]*

[①](兰州理工大学计算机与通信学院 兰州 730050)
[②](西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)
[③](福建师范大学网络安全与密码技术重点实验室 福州 350007)

Security Authentication Protocol for WiMAX Wireless Network Based on Protocol Composition Logic

Feng Tao[①②③] Zhang Zi-bin[①] Ma Jian-feng[②]*

[①](School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China)
[②](Key Laboratory of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an 710071, China)
[③](Key Lab of the Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, China)

摘要 参考文献 相关文章

Download: PDF (251KB) HTML 1KB Export: BibTeX or EndNote (RIS) Supporting Info

摘要 国际标准IEEE 802.16e-2005中PKMv2协议的安全性是WiMAX无线网络安全的重要保证。论文基于协议组合逻辑(PCL)分析了PKMv2协议中认证协议的安全性，发现PKMv2安全认证协议存在交错攻击，在此基础上基于协议演绎系统(PDS)提出了一种新的WiMAX无线网络安全认证协议，并使用协议组合逻辑(PCL)给出新协议的模块化正确性和安全性证明，新协议相对于PKMv2安全认证协议更加安全，更适应WiMAX无线网络复杂的网络应用环境。

关键词： 无线网络 认证协议 协议演绎系统 协议组合逻辑 WiMAX

Abstract: IEEE 802.16e-2005 standard's PKMv2 protocol is an important secure guarantee for WiMAX (Worldwide Interoperability for Microwave Access) wireless network. In this paper, based on Protocol Composition Logic (PCL), the PKMv2 authentication protocol's security is analyzed, the interleaving attack is found, and a new authentication protocol is proposed by using the Protocol Derivation System (PDS) in WiMAX wireless network based on the vulnerability of system security, finally a formal correctness and security proof of it is presented with Protocol Composition Logic (PCL). This new protocol is more secure than the PKMv2 security authentication protocol, and more suitable for complicated wireless network application environment used in WiMAX.

Keywords: Wireless network Authentication protocol Protocol Derivation System (PDS) Protocol Composition Logic (PCL) WiMAX

Received 2009-09-08;

本文基金:

国家高技术研究发展计划(863)(2007AA01Z429)，国家自然科学基金(60702059，60972078)，甘肃省自然科学基金(2007GS04823)，网络安全与密码技术福建省高校重点实验室开放课题(09A006)和兰州理工大学博士基金(BS14200901)资助课题

通讯作者: 张子彬 Email: zzb020511@hotmail.com

引用本文:
冯涛, 张子彬, 马建峰.协议组合逻辑安全的WiMAX无线网络认证协议[J] 电子与信息学报, 2010,V32(9): 2106-2111

Feng Tao, Zhang Zi-Bin, Ma Jian-Feng.Security Authentication Protocol for WiMAX Wireless Network Based on Protocol Composition Logic[J] , 2010,V32(9): 2106-2111

链接本文:
http://jeit.ie.ac.cn/CN/10.3724/SP.J.1146.2009.01191 或 http://jeit.ie.ac.cn/CN/Y2010/V32/I9/2106

Service
把本文推荐给朋友
加入我的书架
加入引用管理器
Email Alert
RSS
作者相关文章
冯涛
张子彬
马建峰