西安电子科技大学学报 2007 34 (5): 814-817 ISSN: 1001-2400 CN: 61-1076/TN

通用可组合安全的Mesh网络认证协议

杨超, 曹春杰, 马建峰

(西安电子科技大学 计算机学院，陕西 西安 710071)

收稿日期 修回日期 网络版发布日期 2007-9-29 接受日期

摘要 无线Mesh网络的现有认证协议不支持双向802.1X的认证端口开放. 基于密钥交换协议交换, 利用“通用可组合”安全模型的组合特性与信任传递技术，在应答消息中安全结合反向认证信息，实现了满足Mesh网络双向认证需求的认证协议，不仅具有可证明的安全性，且通信开销较原协议降低60%以上.

关键词 Mesh网络 通用可组合 认证协议 可证明安全

分类号 TP309

Universally composable secure authentication protocol for wireless mesh networks

YANG Chao,CAO Chun-jie,MA Jian-feng

(School of Computer, Xidian Univ., Xi′an 710071， China)

Abstract

The authentication protocol of Wireless Mesh Networks does not support 802.1X-based mutual authentication. Based on Diffie-Hellman(DH) exchange and making use of the combination characteristic of the Universally Composable(UC) security model and trust transfer, a new authentication protocol is proposed. Piggybacking opposite direction authentication messages in response, this protocol not only provides two-way authentication for Wireless Mesh Networks but also affords provably UC-security. Furthermore,compared with the original scheme, the communication cost decresses by 60%.

Key words mesh networks UC-security authentication protocol provable security

DOI:

通讯作者