计算机工程与应用 2009 45 (21): 74-76 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

一种无证书的移动Ad hoc网络密钥管理方案

吴旭光[1]，张敏情[1]，杨晓元[1,2]，韩益亮[1]

1.武警工程学院 电子技术系 网络与信息安全武警部队重点实验室，西安 710086
2.西安电子科技大学 网络信息安全教育部重点实验室，西安 710071

收稿日期 2009-1-14 修回日期 2009-3-16 网络版发布日期 接受日期

摘要 结合无证书签密协议，提出一种分级移动Ad hoc网络密钥管理方案。该方案不需要公钥证书，用户自己生成公钥，有效地降低了用户终端计算、存储能力的需求和系统密钥管理的通信开销；同时密钥生成中心为用户生成部分私钥，解决了基于身份密码体制中的密钥托管问题；分级的结构将网上节点分成一些相对独立的自治域，既提高了安全服务的可用性和可扩充性，也便于对某些紧急情况快速做出反应。

关键词 移动Ad hoc网络 密钥管理 无证书签密

分类号

Certificateless key management in mobile Ad hoc networks

WU Xu-guang[1]，ZHANG Min-qing[1]，YANG Xiao-yuan[1,2]，HAN Yi-liang[1]

1.Key Laboratory of Network & Information Security of APF，Engineering College of APF，Xi’an 710086，China
2.Key Laboratory of Network & Information Security of the Ministry of Education，Xidian University，Xi’an 710071，China

Abstract

Combining certificateless signcryption protocol and hierarchical structure，a new key management agreement is proposed.In this scheme，public key certificates are not needed and every participant makes a public key himself.It greatly decreases the need of the ability for computation and storage of terminals，as well as communication cost for system key management.At the same time，the key generator center creates partial private keys for nodes，and then solves the key escrow problem in the identity-based cryptography.Nodes are divided into several autonomous communities based on cluster structure，which not only increases availability and scalability of networks，but also results in quick response to some emergency.

Key words mobile Ad hoc networks key management certificateless signcryption

DOI: 10.3778/j.issn.1002-8331.2009.21.020

通讯作者 吴旭光 wxguang0210@163.com