西安电子科技大学学报　2007 34 (6): 974-979　ISSN: 1001-2400　CN: 61-1076/TN

一种无证书Ad hoc密钥管理与认证模型

刘淳1, 刘建伟1, 张其善1, 李晖2

(1. 北京航空航天大学 电子信息工程学院，北京 100083；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，陕西 西安 710071)

收稿日期　修回日期　网络版发布日期 2007-11-19 接受日期

摘要　设计了一种用于Ad hoc网络的新密钥管理与认证模型．该模型应用椭圆曲线组合公钥技术，仅在密钥初始化阶段需要可信认证中心的支持．在网络运行阶段，应用门限密码技术实现了自组织的节点公私密钥对更新和撤销，以及共享私钥种子矩阵更新．设计了一种认证与密钥协商协议，协议中用计算的方法产生公钥，减少了两次证书传递过程和验证运算．相比基于证书和基于身份的模型，新模型的安全性、灵活性和效率更高，适合Ad hoc网络自组织和资源受限的特点．

关键词　组合公钥 门限密码 Ad hoc网络 密钥管理 认证 椭圆曲线

分类号 TP393.02

A non-certificated Ad hoc key management and authentication model

LIU Chun1,LIU Jian-wei1,ZHANG Qi-shan1,LI Hui2

(School of Electronics and Information Engineering, BeiHang Univ., Beijing 100083， China;2. Ministry of Education Key Lab. of Computer Network and Information Security, Xidian Univ., Xi′an 710071，China)

Abstract

A new key management and authentication model for Ad hoc networks is proposed. In this model, the elliptic curve combined public key is applied, and the trusted authentication center support is needed only in the key initialization phase. In the operation phase, the self-organized public / private key update, revocation, and shared-private-key-matrix update are implemented with threshold cryptograph. An authentication and key agreement protocol is designed. The interlocutor's public key is produced by computing, and two-time certificate transmission and verification are therefore reduced in the protocol. Compared with the certificate-based and the identity-based models, the new model is more secure, flexible and efficient. And it is more suitable for the self-organized and resource-constrained features of Ad hoc networks. <BR>

Key words combined public key threshold cryptograph Ad hoc network key management authentication elliptic curve

DOI:

通讯作者

扩展功能

本文信息

Supporting info

PDF(637KB)

[HTML全文](0KB)

参考文献

服务与反馈

把本文推荐给朋友

加入我的书架

加入引用管理器

复制索引

Email Alert

文章反馈

浏览反馈信息

相关信息

本刊中 包含“组合公钥”的相关文章

本文作者相关文章

- 刘淳
- 刘建伟
- 张其善
- 李晖