计算机应用 2006 26 (06): 1328-1330 ISSN: 1001-9081 CN: 51-1307/TP

信息安全

自组网中基于簇的混合密钥管理策略

章静, 许 力, 林志伟

福建师范大学数学与计算机科学学院计算机科学系

收稿日期 2005-12-29 修回日期 网络版发布日期 接受日期

摘要 自组网以灵活的组网特性正越来越受到人们的关注。然而，这种灵活特性又给自组网的安全性带来了巨大的挑战。密钥管理是实现该类网络安全的重要环节。首先，基于补图团的着色思想提出了分布式分簇算法，在此基础上，结合TGDH(Tree-Based Group Diffie-Hellman)算法给出了一种混合密钥管理方案。理论分析此方案具有良好的性能。

Abstract Ad Hoc networks have attracted more and more attention recently due to its character of self-organization. However，this character brings big challenges to it in the field of security. Key management is one of most importance things in security service. A new distributed coloring-based clustering method was introduced. Based on it, a hybrid key management scheme using the TGDH algorithm was proposed. The good performance of this strategy was proved by theoretical analysis.

关键词 自组网,分簇,密钥管理,连通支配集

Key words Ad Hoc networks,cluster,key management,connected dominating set

分类号

DOI:

通讯作者:
章静 jing165455@126.com

作者个人主页: 章静; 许 力; 林志伟