

安全技术

基于WAP的双向认证密钥协商方案

郑旋, 卢建朱, 付杰

(暨南大学信息科学技术学院, 广州 510632)

收稿日期 修回日期 网络版发布日期 接受日期

摘要

PKI用证书管理公钥。无线网络设备的能量、计算能力和存储容量有限,限制了带证书的数字签名的应用。针对上述问题,利用布鲁姆过滤器技术,结合公钥密码体制,提出一种不带数字证书的、适用于无线移动场景的双向认证密钥协商方案,并对其进行性能分析和安全性分析。结果证明,该方案结合计数型布鲁姆过滤器技术,更容易实现用户与接入点的动态管理。

关键词 [布鲁姆过滤器](#); [公钥](#); [双向认证](#)

分类号 [TP309](#)

DOI:

通讯作者:

作者个人主页: [郑旋](#); [卢建朱](#); [付杰](#)

扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF](#) (126KB)

▶ [\[HTML全文\]](#) (0KB)

▶ [参考文献\[PDF\]](#)

▶ [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](#)

▶ [引用本文](#)

▶ [Email Alert](#)

▶ [文章反馈](#)

▶ [浏览反馈信息](#)

相关信息

▶ [本刊中包含“布鲁姆过滤器; 公钥; 双向认证”的相关文章](#)

▶ [本文作者相关文章](#)