

安全技术

可证明安全的移动代理路由协议

田 旭1, 刘仁金2, 陈明华2

(1. 皖西学院现代教育技术中心, 六安 237012; 2. 皖西学院计算机科学与技术系, 六安 237012)

收稿日期 修回日期 网络版发布日期 2008-4-1 接受日期

摘要 针对移动代理路由安全问题, 利用Hash函数单向性和迭代方法提出一种移动代理路由协议。用户主机通过Hash函数的单向性保证路由信息安全到达路由主机, 路由主机之间根据Hash函数值的迭代进行交互认证。该协议的计算复杂度显著降低, 特别是在大数据传输的情况下。采用常规方法和串空间模型方法分析并证明了该协议的安全性。

关键词 [移动代理](#) [迭代](#) [单向散列](#) [串空间](#) [计算复杂度](#)

分类号 [TP393](#)

DOI:

通讯作者:

作者个人主页: 田 旭1; 刘仁金2; 陈明华2

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF\(142KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [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“移动代理”的 相关文章](#)
- ▶ 本文作者相关文章
- [田 旭1, 刘仁金2, 陈明华2](#)