电子与信息学报
JOURNAL OF ELECTRONICS & INFORMATION TECHNOLOGY

电子与信息学报 » 2010, Vol. 32 » Issue (9) :2241-2244 DOI: 10.3724/SP.J.1146.2009.01265

研究简报

Ad hoc网络中ARAN路由协议的安全性分析

闫丽丽[①②] 彭代渊[①]*

[①](西南交通大学信息安全与国家计算网格实验室 成都 610031)
[②](成都信息工程学院网络工程学院 成都 610225)

Security Analysis of ARAN Routing Protocol for Ad hoc Networks

Yan Li-li[①②] Peng Dai-yuan[①]*

[①](Information Security and National Computing Grid Laboratory, Southwest Jiaotong University, Chengdu 610031, China)
[②](The Department of Network Engineering, Chengdu University of Information Technology, Chengdu 610225, China)

摘要 | 参考文献 | 相关文章

Download: PDF (198KB) HTML 1KB Export: BibTeX or EndNote (RIS) Supporting Info

摘要 由于Ad hoc网络的特性，传统的串空间理论无法分析其路由协议的安全性，该文首先对串空间理论进行了扩展，添加了证明中间节点可信的条件。随后，使用扩展后的串空间理论分析了ARAN路由协议的安全性，提出了使用该理论分析Ad hoc网络中安全路由协议的新方法。分析和证明结果表明，ARAN路由协议中存在重放和合谋两种攻击，说明采用文中提出的分析方法对Ad hoc网络中的按需距离矢量路由协议的安全性进行分析是有效的。

关键词： Ad hoc网络 路由协议 串空间 形式化分析 一致性

Abstract： Because of the characteristics of Ad hoc networks, the theory of strand spaces can not analyzes the security of routing protocol. In this paper, the theory of strand spaces is first extended and the credibility of intermediate node is added. Subsequently, this extended theory is applied to analyzing the security of ARAN routing protocol and a new formal analysis method is proposed for Ad hoc networks routing protocol. The results show that it has replay attacks and conspiracy attacks in ARAN routing protocol. The method is proved to be valid.

Keywords： Ad hoc network Routing protocol Strand spaces Formal analysis Agreement property

Received 2009-09-25;

本文基金:

国家自然科学基金(60872015)资助课题

通讯作者: 闫丽丽 Email: yanlili@vip.163.com

引用本文:

闫丽丽, 彭代渊.Ad hoc网络中ARAN路由协议的安全性分析[J] 电子与信息学报, 2010,V32(9): 2241-2244

Yan Li-Li, Peng Dai-Yuan.Security Analysis of ARAN Routing Protocol for Ad hoc Networks[J] , 2010,V32(9): 2241-2244

链接本文:

http://jeit.ie.ac.cn/CN/10.3724/SP.J.1146.2009.01265 或 http://jeit.ie.ac.cn/CN/Y2010/V32/I9/2241