西安电子科技大学学报 2008 35 (6): 1063-1068 ISSN: 1001-2400 CN: 61-1076/TN

可证明安全的MANET按需距离矢量路由协议分析

毛立强1, 马建峰1, 2

(1. 西安电子科技大学 计算机学院，陕西 西安 710071；
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 2008-6-16 修回日期 网络版发布日期 2008-11-19 接受日期

摘要 基于模拟证明方法，Acs等提出了一个MANET安全按需距离矢量路由协议的形式化分析模型，并利用该模型证明了ARAN协议的安全性．对该模型进行了深入分析，指出其中合并相邻敌手节点操作和正确系统状态定义的不合理性，以及ARAN协议安全性证明过程中的错误，并给出了一种针对ARAN协议的攻击方法，表明该协议即使在其分析模型下仍然存在安全漏洞．

关键词 路由协议 可证明安全 形式化分析 模拟
分类号 TP393.04

扩展功能
本文信息
Supporting info
PDF(703KB)
[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“路由协议”的相关文章
本文作者相关文章
· 毛立强
· 马建峰
·

Analysis of provably secure on-demand distance vector routing in MANET

MAO Li-qiang1,MA Jian-feng1,2

(1. School of Computer Science and Technology, Xidian Univ., Xi’an 710071， China;
2. Ministry of Education Key Lab. of Computer Network and Information Security, Xidian Univ., Xi’an 710071， China)

Abstract

Based on the simulation paradigm, Acs et al proposed a formal model tailored to the security analysis of on-demand distance vector routing protocols in MANET, and a routing protocol, called ARAN, was proven secure in the model. We indicate the improper manipulations such as mergence of the adjacent adversarial nodes, the improper definition of the correct system state in the model, and the flaw in the proof for ARAN. A new attack to ARAN is presented, which shows that ARAN is not provably secure even in their model.

Key words routing protocol provable security formal analysis simulation paradigm

DOI:

通讯作者 毛立强 lqmao@xidian.edu.cn