计算机应用 2009, 29(09) 2432-2434 DOI: ISSN: 1001-9081 CN: 51-1307/TP

网络与通信

知性Cord逻辑：验证Ad Hoc网络匿名路由协议

李沁[1],曾庆凯[2]

1. 南京大学
2. 南京大学计算机软件新技术国家重点实验室,江苏 南京 210093； 南京大学 计算机科学与技术系,江苏 南京 210093

摘要： 为形式化验证移动自主网的匿名路由协议，提出了基于知性Cord逻辑的模块化验证方法。首先将协议分解为针对不同子安全功能的组件，然后分别利用知性Cord逻辑证明是否满足安全属性的规范。在这个框架下路径匿名的安全属性得到了规范。

关键词： 匿名 移动自主网 知性Cord逻辑 模块化 形式化方法 anonymity Ad Hoc network Epistemic Cord Logic (ECL) modularity formal method

Epistemic Cord logic: verifying anonymous routing protocols in Ad Hoc network

Abstract: For verifying Ad Hoc anonymous routing protocols, a modular method was proposed, which was based on epistemic Cord logic. This method decomposed a protocol into several components according to different security sub-function, and then proved whether these components satisfied their specifications of security properties. The security property of path anonymity was defined and was specified by this logic.

Keywords:

收稿日期 2009-03-23 修回日期 2009-05-18 网络版发布日期 2009-09-01

DOI:

基金项目:

国家级基金

通讯作者: 李沁

作者简介:

作者Email:

参考文献：

本刊中的类似文章

1. 刘喻 吕大鹏 冯建华 周立柱 .数据发布中的匿名化技术研究综述[J]. 计算机应用, 2007,27(10): 2361-2364

2． 蔡伟鸿 邓宇乔 .一个具有公平匿名性的数字版权管理系统[J]. 计算机应用, 2006,26(12): 2924-2927
3．汤念 王雷 姚焯善 张大方 徐红云.一种基于分组填充Mix策略的匿名通信机制[J]. 计算机应用, 2007,27(7): 1606-1608
4．吴拥民 黄宇航 安健鹏.MMORPG服务器逻辑模块的消费/供应模式[J]. 计算机应用, 2007,27(7): 1799-1801
5．向文 陶良升 王同洋.一种高效的WTLS握手协议[J]. 计算机应用, 2008,28(11): 2798-2800
6．陈泗盛 许力 陈志德.自组网匿名通信中的一个基于伪身份的签名方案[J]. 计算机应用, 2007,27(11): 2707-2709
7．谢鲲 邓琳 李仁发 文吉刚.P2P匿名通信系统的匿名度量[J]. 计算机应用, 2008,28(12): 3190-3193
8．李洁 吴振强 于璐 孙鹏 程瑶.一种改进的直接匿名认证方案[J]. 计算机应用, 2009,29(2): 364-366
9．陶颋 孙乐昌.N-path重路由匿名通信系统负载分析[J]. 计算机应用, 2008,28(3): 626-628
10．谢诚 徐红云 刘京.一种无线可控匿名认证协议[J]. 计算机应用, 2008,28(6): 1392-1394
11．张依惠 许力 陈泗盛.一个高效的双向无线Ad Hoc网络匿名路由协议[J]. 计算机应用, 2008,28(9): 2220-2224
12．张向军 陈克非.基于PBOC智能卡的匿名可分电子货币协议[J]. 计算机应用, 2009,29(07): 1785-1789
13．马海英 石振国 顾翔.标准模型下的高效短群签名 [J]. 计算机应用, 2009,29(08): 2220-2222
14．章志明 邓建刚 邹成武 余敏.安全有效的无线传感器网络匿名通信方案 [J]. 计算机应用, 2009,29(09): 2351-2354

文章评论

反馈人		邮箱地址	
反馈标题		验证码	3857