通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

李兴华1,2,邓凌娟1,张渊1,马建峰1.基于博弈论的身份认证协议的分析——NGUYEN L H方案的改进[J].通信学报,2013,(8):18~26

# 基于博弈论的身份认证协议的分析——**NGUYEN L H**方案的改进

# Rational analysis of authentication protocolsbased on NGUYEN L H scheme

投稿时间： 2012-06-29

**DOI**：10.3969/j.issn.1000-436x.2013.08.003

中文关键词：身份认证协议 博弈论 协议安全

英文关键词：identity authentication protocol game theory protocol security

基金项目：国家科技部重大专项基金资助项目(2011ZX03005-002)；国家自然科学基金资助项目(U1135002, 61072066)；中央高校基本科研业务费基金资助项目(JY10000903001, JY10000901034)

| 作者 | 单位 |
|---|---|
| 李兴华1,2，邓凌娟1，张渊1，马建峰1 | 1. 西安电子科技大学 计算机学院，陕西 西安 710071； 2. 南京大学 计算机软件新技术国家重点实验室，江苏 南京210032 |

摘要点击次数: **344**

全文下载次数: **670**

中文摘要:

NGUYEN L H在博弈论思想的指导下来对身份认证协议进行了修改，协议参与方在进行协议交互之前以一定的概率 来发送无用数据，使得攻击者攻击协议所获得的收益比不攻击协议所获得的收益还要小，以此保证了协议的安全性。但该方案存在2个缺陷：考虑的攻击者过于强大，且仅仅考虑了其收益，忽略了其发起攻击所要消耗的代价；没有考虑诚实节点在什么条件下才会选择发送无用数据。针对这2个缺陷对NGUYEN L H方案进行改进，给出了更具有一般意义的 值。同时引入了攻击概率 ，给出了诚实节点发送无用数据的前提条件以及在不同的 值下 的取值范围。相对于原方案，改进方案的结论更具有一般性，且更全面。同时，通过P2P下面的一个具体案例分析证明了所提结论的正确性。

英文摘要:

Using the ideas of game theory, NGUYEN L H transformed two families of authentication protocols where the honest party transmitted some useless data with probability before the normal protocol run, so that even if an attacker attacks a protocol, the attacker’ s payoff will still be lower than that when it does not. In such a way, the security of the protocol was guaranteed. However, this scheme suffers from two shortcomings: the considered is too attacker powerful, and only its payoff was considered and the cost of the attacks was ignored; the situation in which the honest node would choose to send useless data was not considered. To improve this scheme, the value of , with the consideration of the attack cost, of which the value is more general was given. What’ s more, the attack probability was introduced. Based on this, the precondition that the honest node transmits the useless data was presented, as well as the value of under the different values. Compared with the original scheme, this results are more generic and comprehensive. Meanwhile, through a case analysis in the P2P network, the correctness of the conclusion is proved.

查看全文 查看/发表评论 下载PDF阅读器

关闭

地址：北京市丰台区成寿寺路11号邮电出版大厦8层 电话：010-81055478，81055479
81055480，81055482 电子邮件：xuebao@ptpress.com.cn
技术支持：北京勤云科技发展有限公司