电子与信息学报 2007 29 (4): 901-905 ISSN: 1009-5896 CN: 11-4494/TN

论文

基于ATL的公平电子商务协议形式化分析

文静华[①②③], 李 祥[①], 张焕国[②], 梁 敏[③], 张 梅[③]

[①]贵州大学计算机软件与理论研究所 贵阳 550025;[②]武汉大学计算机学院 武汉 430072;[③]贵州财经学院信息学院 贵阳 550004

收稿日期 2005-8-30 修回日期 2006-1-11 网络版发布日期 2008-2-25 接受日期

摘要
针对传统时序逻辑LTL，CTL及CTL*等把协议看成封闭系统进行分析的缺点，Kremer博士(2003)提出用一种基于博弈的ATL(Alternating-time Temporal Logic)方法分析公平电子商务协议并对几个典型的协议进行了公平性等方面的形式化分析。本文讨论了ATL逻辑及其在电子商务协议形式化分析中的应用，进一步扩展了Kremer博士的方法，使之在考虑公平性等特性的同时能够分析协议的安全性。最后本文用新方法对Zhou等人(1999)提出的 ZDB协议进行了严格的形式化分析，结果发现该协议在非保密通道下存在两个可能的攻击：保密信息泄露和重放攻击。

关键词 电子商务协议 公平性 安全性 形式化分析 ATL

分类号 TP309

Formal Analysis of Fair E-Commerce Protocols Based on ATL

Wen Jing-Hua[①②③], Li Xiang[①], Zhang Huan-guo[②], Liang Min[③], Zhang Mei[③]

[①]Institute of Software and Theory, Guizhou University, Guiyang 550025, China;
[②]School of Computer, Wuhan University, Wuhan 430072, China;[③]Information Institute, Guizhou Financial Institute, Guiyang 550004, China

Abstract
Aiming at the shortcoming that traditional temporal logic such as LTL,CTL and CTL* regards protocols as close system to analyze, Dr Kremer(2003) proposes an ATL (Alternating-time Temporal Logic) logical method based on game to analyze fair E-commerce protocols, and analyses formally several typical protocols on their fairness and other properties. In this paper, ATL logical and its applications in formal analysis of E-commerce protocols are discussed, and Dr Kremer' approach is ulteriorly extended to analyze security of protocols besides fairness. Finally, the strict formal analysis is made for ZDB protocol(1999) proposed by Zhou et al. With this new method, as a result there exists 2 possible attacks in the ZDB protocol under non-secrecy channels: leakiness of secret information and reply attacks.

Key words E-commerce protocols Fairness Security Formal analysis ATL

DOI:

通讯作者

作者个人主页 文静华[①②③]; 李 祥[①]; 张焕国[②]; 梁 敏[③]; 张 梅[③]