

网络、通信、安全

## 一种乐观电子商务协议的公平性分析

阮峰<sup>1</sup>, 候建敏<sup>2</sup>, 张中秋<sup>3</sup>, 范志勇<sup>2</sup>

1.南京信息工程大学 信息与控制学院, 南京 210044

2.南京理工大学 计算机学院, 南京 210000

3.南京航空航天大学 计算机学院, 南京 210000

收稿日期 2009-8-5 修回日期 2009-9-25 网络版发布日期 2009-12-16 接受日期

**摘要** 乐观电子商务协议通常具有复杂结构, 由多个子协议组合而成, 与传统认证协议具有显著不同。电子商务协议最主要目的是实现买卖双方的公平交换, 同时假定交换双方都可能是不诚实的, 需要考虑来自协议合法实体的内部攻击。文章在深入分析公平交换协议各项属性的基础上, 定义了电子项的认证属性, 对SVO逻辑进行了扩展, 使用SVO逻辑语法定义了电子商务协议应满足的公平性。文章以一种真实的电子商务协议为对象, 演示了基于SVO逻辑的电子商务协议公平性分析方法, 并指出该协议存在安全缺陷, 提出改进意见。

**关键词** [电子商务](#) [乐观公平交换](#) [公平性](#) [SVO逻辑](#)

**分类号** [TP393](#)

## Fairness analysis of optimistic e-commerce protocol

RUAN Feng<sup>1</sup>, HOU Jian-min<sup>2</sup>, ZHANG Zhong-qiu<sup>3</sup>, FAN Zhi-yong<sup>2</sup>

1.College of Information and Control, Nanjing University of Information Science & Technology, Nanjing 210044, China

2.College of Computer, Nanjing University of Science & Technology, Nanjing 210000, China

3.College of Computer, Nanjing University of Aeronautics and Astronautics, Nanjing 210000, China

### Abstract

The optimistic e-commerce protocol is made up of multiple sub-protocols, and is significantly different from traditional authentication protocol. The main purpose of the e-commerce protocol is to realize fair exchange between both buyers and sellers who are assumed to be dishonest. That is, it is necessary for those buyers and sellers to prevent the internal attack. Based on the deep analysis of each attribute in fair exchange protocols, the authentication attribute of item is defined. The fairness that should be met by e-commerce protocols is defined, and an extended SVO logic syntax which takes an optimistic e-commerce protocol as an object is proposed to demonstrate the fairness analysis method. The security vulnerabilities and improvement suggestions of the e-commerce protocol are also discussed.

**Key words** [electronic commerce](#) [optimistic fair exchange](#) [fairness](#) [SVO logic](#)

DOI: 10.3778/j.issn.1002-8331.2009.35.026

通讯作者 阮峰 [rf1999@yahoo.cn](mailto:rf1999@yahoo.cn)

### 扩展功能

#### 本文信息

▶ [Supporting info](#)

▶ [PDF\(729KB\)](#)

▶ [\[HTML全文\]\(0KB\)](#)

▶ [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“电子商务”的相关文章](#)

▶ [本文作者相关文章](#)

- [阮峰](#)
- [候建敏](#)
- [张中秋](#)
- [范志勇](#)