

论文与报告

一种探测推荐系统托攻击的无监督算法

李聪, 骆志刚, 石金龙

1. 国防科学技术大学计算机学院 长沙 410073

收稿日期 2010-7-27 修回日期 2010-10-22 网络版发布日期 接受日期

摘要

托攻击是当前推荐系统面临的重大安全性问题之一. 开发托攻击探测算法已成为保障推荐系统准确性与鲁棒性的关键. 针对现有托攻击探测算法无监督程度较低的局限, 在引入攻击概貌群体效应的定量度量及基于此的遗传优化目标函数的基础上, 将自适应参数的后验推断与攻击探测过程相融合, 提出了迭代贝叶斯推断遗传探测算法, 降低了算法探测性能对系统相关先验知识的依赖. 实验结果显示这种算法能够有效探测各种常见攻击.

关键词 [推荐系统](#) [托攻击](#) [群体效应](#) [遗传算法](#) [贝叶斯推断](#)

分类号

An Unsupervised Algorithm for Detecting Shilling Attacks on Recommender Systems

LI Cong, LUO Zhi-Gang, SHI Jin-Long

1. School of Computer, National University of Defense Technology, Changsha 410073

Abstract

Shilling attack is one of the significant security problems involved in recommender systems. Developing detection algorithms against shilling attacks has become the key to guaranteeing both the preciseness and robustness of recommender systems. Considering the low degree of unsupervised features the existing algorithms suffer from, this paper proposes an iterative Bayesian inference genetic detection algorithm (IBIGDA) through the introduction of the quantitative metric for the group effect of attack profiles and the corresponding object function for genetic optimization. This algorithm combines the posterior inference for the adaptive parameters with the process of attack detection, thus relaxes the dependence of the detection performance on the relating prior knowledge of the systems. Experimental results show that this algorithm can effectively detect shilling attacks of typical types.

Key words [Recommender system](#) [shilling attack](#) [group effect](#) [genetic algorithm](#) [Bayesian inference](#)

DOI: 10.3724/SP.J.1004.2011.00160

通讯作者 李聪 licongwhy@gmail.com

作者个人主页 李聪; 骆志刚; 石金龙

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF\(1044KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [参考文献\[PDF\]](#)

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](#)

相关信息

- ▶ [本刊中 包含“推荐系统”的 相关文章](#)
- ▶ 本文作者相关文章

- [李聪](#)
- [骆志刚](#)
- [石金龙](#)