计算机工程与应用 2009 45 (20): 92-95 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

基于SVD的协同过滤算法的欺诈攻击行为分析

徐 翔，王煦法

中国科学技术大学 计算机科学与技术系，合肥 230027

收稿日期 2008-10-6 修回日期 2009-1-4 网络版发布日期 2009-7-9 接受日期

摘要 协同过滤是一种个性化推荐系统最常用的技术，但它对用户概貌信息较为敏感，欺诈攻击者很容易通过注入有偏差的用户概貌使系统的推荐结果有利于他们。研究表明欺诈攻击的攻击模型、攻击成本对攻击性能有不同程度的影响。针对这个问题，实验分析基于奇异值分解（SVD）的协同过滤算法在不同攻击模型下的性能表现，并以三种评估参数分析不同填充规模和攻击规模对攻击效率的影响。

关键词 协同过滤 推荐系统 欺诈攻击 奇异值分解

分类号

Analysis of shilling attacks on SVD-based collaborative filtering algorithm

XU Xiang，WANG Xu-fa

Department of Computer Science and Technology，University of Science and Technology of China，Hefei 230027，China

Abstract

Collaborative filtering is a vital central technology in personalized recommendation，but it is so sensitive to user profiles，that shilling attackers can easily inject biased profiles in an attempt to force a system to adapt in a manner advantageous to them.Recent research shows that the model and the cost of shilling attacks have different impacts on attack performance.This paper analyzes the attack effectiveness of different attack models on a SVD-based collaborative filtering algorithm，and the performances of attack models with different fill sizes and attack sizes using three evaluation parameters.

Key words collaborative filtering recommender systems shilling attacks Singular Value Decomposition（SVD）

DOI: 10.3778/j.issn.1002-8331.2009.20.028

通讯作者 徐 翔 xuustc@gmail.com