# 推荐系统中基于目标项目分析的托攻击检测研究

RESEARCH ON SHILLING ATTACK DETECTION BASED ON TARGET ITEM ANALYSIS IN RECOMMENDER SYSTEMS

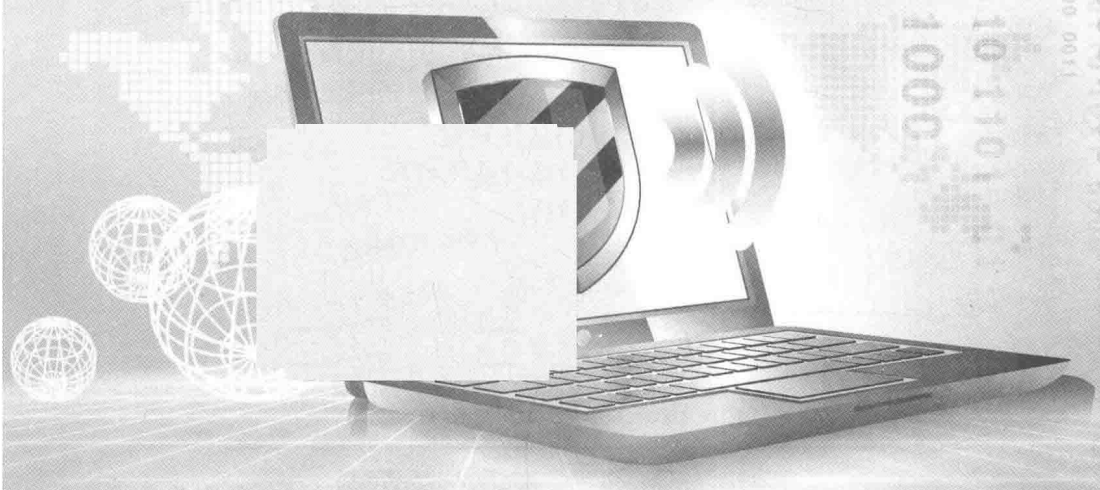
周 魏 文俊浩◎著

重庆大学出版社

# 推荐系统中基于目标项目分析的托攻击检测研究

TUIJIAN XITONG ZHONG JIYU MUBIAO XIANGMU FENXI DE TUOGONGJI JIANCE YANJIU

周 魏 文俊浩◎著



重庆大学出版社

## 内容提要

由于推荐系统开放性的特点，恶意用户可以通过注入伪造的用户概貌以改变目标项目在推荐系统中的排名，托攻击行为干扰了推荐系统的正常运行，阻碍推荐系统的应用和推广。本书提出了几种托攻击监测的方法：提出一种基于目标项目分析的托攻击检测框架；在基于目标项目分析的托攻击检测框架基础上提出了两种托攻击检测算法；提出了一种结合目标项目分析和支持向量机的检测方法；提出了一种基于目标项目分析和时间序列的托攻击检测算法。

**图书在版编目(CIP)数据**

推荐系统中基于目标项目分析的托攻击检测研究/
周魏，文俊浩著. —重庆：重庆大学出版社，2017.3
ISBN 978-7-5689-0314-1

Ⅰ.①推… Ⅱ.①周…②文… Ⅲ.①计算机网络—研究
Ⅳ.①TP393

中国版本图书馆 CIP 数据核字(2016)第 314727 号

**推荐系统中基于目标项目分析的托攻击检测研究**

周 魏 文俊浩 著
策划编辑：周 立
责任编辑：陈 力 版式设计：周 立
责任校对：关德强 责任印制：赵 晟

*

重庆大学出版社出版发行
出版人：易树平
社址：重庆市沙坪坝区大学城西路 21 号
邮编：401331
电话：(023) 88617190 88617185(中小学)
传真：(023) 88617186 88617166
网址：http://www.cqup.com.cn
邮箱：fxk@cqup.com.cn (营销中心)
全国新华书店经销
万州日报印刷厂印刷

*

开本：787mm×1092mm 1/16 印张：9 字数：121 千
2017 年 3 月第 1 版 2017 年 3 月第 1 次印刷
ISBN 978-7-5689-0314-1 定价：39.00 元

# 序

《2016年(上)中国网络零售市场数据监测报告》显示,2016年上半年中国网络零售市场交易规模达23 141.94亿元,相比2015年上半年的16 140亿元,同比增长43.4%。其中,跨境电商、农村电商、移动电商成为拉动网络零售增长的三驾马车,继续高速发展。电子商务已经直接关系到国民经济的发展和人们的生活。

推荐系统促进了电子商务的发展,同时电子商务的进一步发展依赖于推荐系统自身功能的完善。推荐系统需要用户大量的历史记录作为预测的依据,一般来说,用户提供的历史数据越多,推荐系统向用户推荐的结果就越准确。推荐系统管理者希望用户能够提供对项目真实的评价从而使推荐系统能够产生高质量的推荐服务,然而在现实中,恶意用户利用推荐系统评分驱动的工作机制与开放性的

特点来谋求不正当利益。恶意用户向推荐系统中注入虚假评价信息以达到干扰推荐系统正常推荐的目的，其结果是损害正常用户的利益和推荐系统的信誉。例如，在电子商务平台中，部分厂商为了销售更多的商品，向推荐系统注入虚假的评分信息或评论信息来提高商品在推荐系统中的排名；或者使用类似的方法打压竞争对手销售的产品，以此来提高自己商品的销量。现实生活中也不乏这样的例子：索尼影业公司就曾经伪造电影评论信息来宣传正在发行的电影；亚马逊网站曾遭到外来的攻击，当用户浏览宗教相关书籍的时候，系统会向用户推荐有关性方面的书籍。除了恶意程序对推荐系统的攻击之外，现实中还有一群专门提供托攻击服务的人群，称为“网络水军”。例如，手机软件公司为了推广自己开发的软件，通过雇用网络水军来下载使用自己的软件，使得自己的软件在软件排行榜上的名次上升，吸引更多的用户下载使用。网络水军的出现使部分公司通过人为操纵下载量的方式长期占据软件排行榜前列从而导致了不公平竞争。

推荐系统作为一种信息过滤工具，其出现与普及可有效缓解信息过载问题。然而，托攻击通过操纵商品在推荐系统中的排名，使推荐

系统向用户推荐被操纵的商品或信息，严重干扰了推荐系统的正常运行，阻碍了推荐系统的应用和推广。托攻击会对推荐系统造成严重的影响，主要表现为以下几个方面：第一，托攻击会影响推荐结果，从而导致用户选择被攻击的项目，这将导致竞争项目之间的不公平。第二，对推荐系统来说，恶意用户概貌被注入后，推荐系统将不能推荐用户感兴趣的项目，这将影响推荐系统的声誉。第三，托攻击干扰了系统对用户的正常推荐，严重阻碍了推荐系统在信息服务、电子商务等领域的应用和发展。为了减少虚假信息对于推荐系统的影响，推荐系统管理者探讨使用各种技术防御恶意程序的攻击。

如何提高推荐系统的抗托攻击能力以及减少托攻击带来的不良影响，本书针对已有推荐系统托攻击检测方法存在的缺陷和不足，在现有用户概貌属性提取技术的基础上，研究推荐系统托攻击特征提取技术及推荐系统托攻击检测方法。

本书研究新的托攻击特征和概貌提取技术，从而提出相应的托攻击检测方法，为推荐系统托攻击检测方法提供新思路。本书针对推荐系统托攻击行为的群体性特点，研究了相应的托攻击检测方法，从而减少托攻击给推荐系统

带来的不良影响，对促进推荐系统的正常运行，维护推荐系统的真实性、公平性及对电子商务的良性发展能够起一定的积极作用。

著　者

2017 年 2 月

# 前言

个性化推荐技术作为一种解决信息超载问题最有效的工具，但是由于推荐系统开放性的特点，恶意用户可以通过注入伪造的用户概貌以改变目标项目在推荐系统中的排名，此类现象称为托攻击。托攻击行为使推荐系统向用户推荐被操纵的商品或信息，干扰了推荐系统的正常运行，阻碍推荐系统的应用和推广。本书的主要内容如下：

分析了推荐系统国内外研究现状和面临的主要挑战；分析推荐系统中相似度计算方法、托攻击检测评价指标和现有的用于托攻击检测的概貌属性，并对推荐系统中概貌属性提取技术进行分析。

针对托攻击群体性特征以及用户评分矩阵稀疏性的特点，提出一种基于目标项目分析（TIA）的托攻击检测框架。首先，找出有攻击嫌疑的疑似托攻击用户集合；其次，构建由这

些疑似托攻击用户概貌组成的评分矩阵;最后,通过目标项目分析方法得到攻击意图和目标项目,检索出托攻击用户。

通过分析真实用户概貌和托攻击用户概貌属性值的分布,在基于目标项目分析的托攻击检测框架基础上提出了两种托攻击检测算法,基于 RDMA 和 DegSim 概貌属性的方法(RD-TIA)和基于一种新的概貌属性 DegSim'的检测方法(DeR-TIA)。

针对现有的 SVM 托攻击检测算法存在的缺陷以及推荐系统托攻击检测中存在的类不均衡问题,本书提出了使用自适应人工合成样本方法 Borderline-SMOTE 来缓解类不均衡问题。提出了一种结合目标项目分析和支持向量机(SVM)的检测方法(SVM-TIA)。

根据虚假用户恶意注入的评分信息在时间节点上具有集中性的特点,以及真实评分与托攻击评分在统计学上呈现的不同分布特征,提出了一种基于目标项目分析和时间序列的托攻击检测算法(TS-TIA)。

本书受国家自然科学基金面上项目"基于异构服务网络分析的 Web 服务推荐研究"(No. 61379158),国家自然科学基金青年基金项目"基于用户生成信息分析和异常群组发现的推

荐系统托攻击检测研究”(No. 61602070)等项目的资助。

本书的编写和出版受到了重庆大学软件学院的大力支持,在此表示衷心的感谢。

限于本书作者的学识水平,书中疏漏之处在所难免,恳请读者批评指正。

著　者

2016 年 9 月

# 目录

# 第1章 绪 论

## 1.1 研究背景与意义

### 1.1.1 研究背景

随着计算机和网络技术的迅速发展，人们的难题已经从如何获得信息，到如何从海量的信息中找到需要的知识。由于用户难以对海量的信息进行直接利用，这导致信息资源的使用效率较低，即所谓的“信息过载”(Information Overload)问题[1]。当今网络上各类信息纷繁复杂，因此在海量的信息中高效、及时地获取信息显得尤为重要，在海量信息中进行信息检索对用户来说是一个巨大的挑战。日常生活中不乏海量信息的例子，如 Netflix 的电影信息，当当网和亚马逊上的书籍信息，以及 YouTube 上数以万计的视频信息等。如果用户不依靠相应的工具对信息进行过滤，试图找到有用的商品或信息无异于大海捞针，因而信息资源的爆炸式增长反而降低了用户对信息资源的利用率。目前主要有两种工具应对信

息过载问题,即搜索引擎和推荐系统。

①搜索引擎是指运用一定的策略,使用特定的程序对互联网上的信息资源搜集整理,对信息组织和处理后,供用户输入关键词查询的系统[2]。它搜集并整理互联网上的信息并根据用户的查询关键词返回相应结果[3]。搜索引擎不仅能够满足人们绝大多数的搜索需求,还可以按照用户的方式对搜索结果进行个性化排序。根据有关调查报告显示,截至2014年6月,中国搜索引擎用户数达到50 749万人,较去年同期增长3 711万人,增长率为7.9%①。这表明搜索引擎已经逐渐融入人们的日常生活之中。

搜索引擎虽然在用户能提供明确需求时功能强大,但是它只能被动地向用户展示信息,无法主动地向用户提供服务,具有一定的局限性。同时对用户而言,将需求表达成一个或者几个合适的关键词是一个较大的挑战。例如,用户面对成千上万的音乐专辑时,往往难以找出符合自己兴趣音乐的关键词。此时搜索引擎难以提供有效的帮助,这就需要一个更为自动化的信息过滤工具帮助用户从庞大的音乐库中找到其感兴趣的音乐。另外,搜索结果的排序受到用户越来越多的关注,如何对搜索结果进行排序显得尤为重要,而竞价排名的出现,也成为搜索引擎被人诟病的原因之一。

②推荐系统是一种通过分析用户的历史行为信息、使用习惯等向用户主动推送信息的工具[4]。电子商务是推荐系统的主要应用领域,在电子商务不断发展壮大的今天,各种商品信息在电子商务网站上不断涌现,用户往往需要花费大量的时间在各类商品信息中寻找自己想要的商品。推荐系统通过对用户的历史消费习惯、点击情况等信息进行分析,向用户呈现感兴趣的甚至是潜在感兴趣的商品,从而减少用户浏览无用信息的时间以帮助用户获得更好的购物体验,并且能够为电子商务站点带来更多的营业额。

① http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/

推荐系统促进了电子商务的发展,同时电子商务的进一步发展依赖于推荐系统自身功能的完善。推荐系统需要用户大量的历史记录作为预测的依据,一般来说,用户提供的历史数据越多,推荐系统向用户推荐的结果就越准确。推荐系统管理者希望用户能够提供对项目真实的评价从而使推荐系统能够产生高质量的推荐服务,然而在现实中,恶意用户利用推荐系统评分驱动的工作机制与开放性的特点来谋求不正当利益。恶意用户向推荐系统中注入虚假评价信息以达到干扰推荐系统正常推荐的目的,其结果是损害正常用户的利益和推荐系统的信誉[5]。例如在电子商务平台中,部分厂商为了销售更多的商品,向推荐系统注入虚假的评分信息或评论信息来提高商品在推荐系统中的排名;或者使用类似的方法打压竞争对手销售的产品,以此来提高自己商品的销量。现实生活中也不乏这样的例子:索尼影业公司就曾经伪造电影评论信息来宣传正在发行的电影;亚马逊网站曾遭到外来的攻击,当用户浏览与宗教相关的书籍时,系统会向用户推荐有关性方面的书籍[6]。

为了减少虚假信息对于推荐系统的影响,推荐系统管理者探讨使用各种技术防御恶意程序的攻击[7]。例如,实行实名制,审核系统用户信息,增加恶意用户向推荐系统中注入托攻击概貌的难度;使用验证码,增加恶意程序的攻击成本。然而,这些方法能阻止部分恶意程序,但同时也增加了正常用户使用推荐系统的难度,不利于推荐系统的扩展。

除了恶意程序对推荐系统的攻击之外,现实中还有专门提供托攻击服务的人群,被称为“网络水军”。例如手机软件公司为了推广自己开发的软件,通过雇佣网络水军来下载使用自己的软件,使得软件在软件排行榜上的名次上升,吸引更多的用户下载使用。网络水军的出现造成部分公司通过人为操纵下载量的方式长期占据软件排行榜前列导致了不公平竞争。

研究者对推荐系统遭受的托攻击方式进行了分类,如 Burke 等人[8] 2011 年的研究报告就分析了 4 大种类、8 种不同的攻击策略。推荐系统在受到托攻击之后不能准确地向用户推荐需要的信息,甚至可能向用户

提供错误的推荐信息。托攻击的存在降低了推荐系统用户的使用体验，使得用户对推荐系统的信任降低。目前推荐系统托攻击检测研究尚处于初级阶段，且实际应用中攻击者的攻击方法层出不穷，因而需要进一步研究和探索具有普适性和高性能的推荐系统托攻击检测方法。

### 1.1.2 研究意义

推荐系统作为一种信息过滤工具，其出现与普及可有效缓解信息过载问题。然而，托攻击通过操纵商品在推荐系统中的排名，使推荐系统向用户推荐被操纵的商品或信息，严重干扰了推荐系统的正常运行，阻碍了推荐系统的应用和推广。托攻击会对推荐系统造成严重影响，主要表现为以下两个方面：第一，托攻击会影响推荐结果，从而导致用户选择被攻击的项目，这将导致竞争项目之间的不公平；第二，对推荐系统来说，恶意用户概貌被注入后，推荐系统将不能推荐用户感兴趣的项目，这将影响推荐系统的声誉。托攻击干扰了系统对用户的正常推荐，严重阻碍了推荐系统在信息服务、电子商务等领域的应用和发展。

针对如何提高推荐系统的抗托攻击能力以及减少托攻击带来的不良影响，很多研究者对各类托攻击行为进行了研究，并提出了各种增加推荐系统鲁棒性的推荐方法和具有较高普适性的托攻击检测方法[7,9,10]。本书针对已有推荐系统托攻击检测方法存在的缺陷和不足，在现有用户概貌属性提取技术的基础上，研究推荐系统托攻击特征提取技术及推荐系统托攻击检测方法，研究具有重要的理论和现实意义。

**(1)理论意义**

已有的推荐系统托攻击检测算法通过提取用户概貌属性值，在概貌属性值的基础上实施托攻击检测。然而当前概貌属性提取方法没有充分利用托攻击行为的群体性属性，不能有效描述已知类型的托攻击及无法对未知类型托攻击进行有效检测，算法检测效率随着用户概貌数据量的增加而降低。为了解决上述问题，本书研究新的托攻击特征和概貌提取技术，从而提出相应的托攻击检测方法，为推荐系统托攻击检测方法提供