基于信任的托攻击用户检测算法

张 鑫 黄 刚
(南京邮电大学计算机学院 江苏 南京 210000)

摘 要 随着电子商务的迅速发展,协同过滤技术在推荐领域中,得到了广泛的运用。托攻击问题和数据稀疏性问题,导致推荐结果不理想。研究证明,用户间信任关系可以极大缓解数据稀疏问题,使得推荐更为准确。但是,包含信任关系的推荐算法,大多未能考虑到托攻击对于推荐的影响,使得系统的鲁棒性下降。通过研究包含信任信息的推荐情景中托攻击用户的统计量表现特征,提出一种在信任网络下,检测托攻击用户的 TSAD 算法。实验证明,该算法能够准确地识别托攻击用户,增强系统的鲁棒性。

关键词 信任 托攻击 推荐 统计量 协同过滤

中图分类号 TP3 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2020.11.046

TRUST-BASED SHILLING ATTACKS USER DETECTION ALGORITHM

Zhang Xin Huang Gang
(*School of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210000, Jiangsu, China*)

Abstract With the rapid development of e-commerce, collaborative filtering technology has been widely used in the field of recommendation. The problem of shilling attacks and data sparseness has led to poor recommendation results. Studies have shown that trust relationships between users can greatly alleviate data sparseness and make recommendations more accurate. However, most of the recommendation algorithms including the trust relationship fail to take into account the impact of the shilling attacks on the recommendation, which makes the robustness of the system declining. By studying the statistical performance characteristics of the shilling attacks user in the recommendation with trust information, this paper proposes a TSAD algorithm for detecting the shilling attacks under the trust network. Experiments show that the algorithm can accurately identify the shilling attacks and enhance the robustness of the system.

Keywords Trust Shilling attacks Recommendation Statistics Collaborative filtering

0 引 言

2018 年,阿里巴巴的年营收是 321.54 亿元人民币,亚马逊的年营收是 177 866.0 百万美元,电子商务发展如此迅猛,协同过滤算法功不可没。信息数量的爆炸式增长,使得用户难以在海量的信息中,找到自己感兴趣的商品。如何准确快速地定位用户偏好的商品,从而对用户进行推荐,成为推荐系统设计的首要目标。协同过滤算法[1-4]从相似的用户和相似的项目角度出发,分析项目之间和用户之间的相似程度,找到用户偏好的项目,可以在大数据的情境下,较为可靠地完成推荐任务。

研究表明[5-7],数据稀疏性问题和托攻击问题,对于推荐的准确度有较大的影响。为了缓解现实生活中用户只评论少量的项目导致的数据稀疏性问题,研究证明[8-10],在推荐过程中,综合考虑用户添加的信任关系来改进用户之间的相似度,往往可以获得更好的推荐效果。

基于信任的推荐算法,已经有许多学者进行了研究,但是算法大多没有考虑到托攻击问题的影响。托攻击问题指托攻击用户向推荐系统中注入虚假的评分信息,最终影响系统的推荐结果。如表 1 所示,托攻击用户 X 通过对项目 1 和项目 2 正常评分伪装为正常用

收稿日期:2019-06-25。国家自然科学基金项目(61171053);南京邮电大学基金资助项目(SG1107)。**张鑫**,硕士生,主研领域:推荐系统。**黄刚**,教授。

户的邻居用户,对项目 3 实施托攻击,使得项目 3 的评分上升。

表 1　托攻击用户对于项目进行恶意评分

用户	项目 1	项目 2	项目 3
正常用户 A	2	2	1
正常用户 B	2	1	1
正常用户 C	3	2	1
托攻击用户 X	2	2	5

针对以上问题,本文提出一种信任网络下的托攻击用户检测算法 TSAD,通过研究信任网络下托攻击的统计量特征检测托攻击用户,提升系统的鲁棒性。

1　相关工作

1.1　信　任

1998 年,Gambetta 首次定义了信任[11],从社会学的角度出发,叙述了信任的本质:如果我们信任某个人,就表明这个可信的人的行为有可能对我们有帮助,因此我们会考虑与其合作;相反地,如果我们不信任某个人,就表明这个人对我们没有帮助甚至有害,因此我们不会考虑与其合作。信任包含以下性质:(1) 不对称性,用户 A 对于用户 B 添加了信任关系,并不能说明用户 B 也信任用户 A;(2) 传递性,如果用户 A 对于用户 B 添加了信任关系,用户 B 又信任用户 C,可以得出用户 A 在一定程度上信任用户 C ;(3) 多样性,根据信任的不同表现形式,可以分为直接信任、间接信任等;(4) 动态性,信任的程度会随着时间等因素发生变化。

针对以上性质,潘一腾等[12]提出了一种新的基于信任关系隐含相似度的度量方法,并与协同推荐算法相结合,提升了推荐质量;Wang[13]提出了一种基于改进 D-S 证据理论的多源属性信任预测方法,通过七重交叉验证方法验证了属性证据的充分性和信任预测结果,改善了推荐效果;Shabut 等[14]提出了一种新的信任模型,该模型具有防御方案,利用聚类技术,动态地过滤不诚实的信任关系,增加了推荐的精度;林韶娟等[15]基于二值信任网络,提出了 GenTrust 算法来预测新的信任关系,提升了原始信任网络推荐的准确率。虽然上述算法都结合信任进行评分预测,但是都没有考虑到托攻击问题,导致系统的鲁棒性较差。

1.2　托攻击

协同过滤推荐系统中,系统根据每个用户的邻居的概貌信息为其生成推荐列表,因此恶意用户可人为地向系统中注入大量虚假概貌,成为多个真实用户的近邻,进而达到影响推荐结果的目的,这种向推荐系统注入虚假概貌的行为即为托攻击,2004 年 Lam 等[16]首次正式提出了这个概念。托攻击问题被提出之后,如何在推荐的过程中对于托攻击进行检测和抵御,成为了推荐领域中的又一重要课题。托攻击方式主要分为两种:提升攻击项目排名的推攻击;降低攻击项目排名的核攻击。图 1 是托攻击的一般结构[17]。

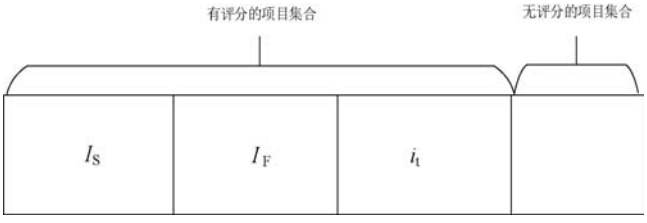

图 1　托攻击的一般结构

图 1 中,I_S 为选择项目集合,I_F 为填充项目集合,i_t 为攻击项目集合。根据攻击方式的不同,托攻击又可以分为平均攻击、随机攻击、混合攻击等。由于本文实验中采用的托攻击方式为随机攻击,下面只对该方式进行介绍:选择项目为空,评分为空,填充项目为随机选择,评分为该项目全局评分的临近值,攻击项目为要攻击的目标,评分为最大值或者最小值。

1.3　托攻击用户在信任网络中的行为特征

在含有用户信任信息的推荐系统中,托攻击方式有了以下行为特征[18-21]:

1) 对称性:托攻击用户为了使自身的评分有更高的可信性,往往会对其他托攻击用户添加信任关系。与正常的信任关系的非对称性相比,其信任关系往往是双向的,并且多个托攻击用户之间会形成区域性质的信任关系,如图 2 所示。

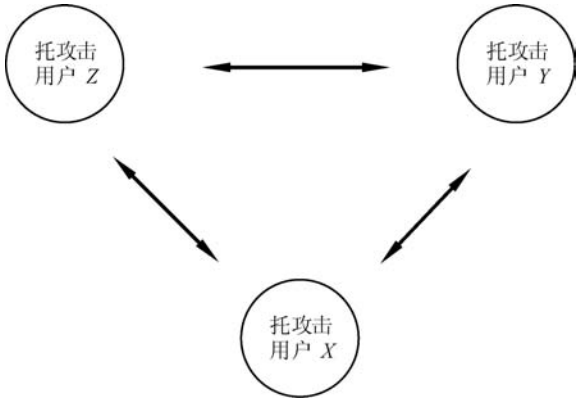

图 2　托攻击用户的对特征

2) 伪装性:托攻击用户为了隐藏自身的恶意评分,对正常用户添加信任关系。另外,由于托攻击用户的评分对于正常用户难以分辨,使得正常用户也会对其信任,如图 3 所示。

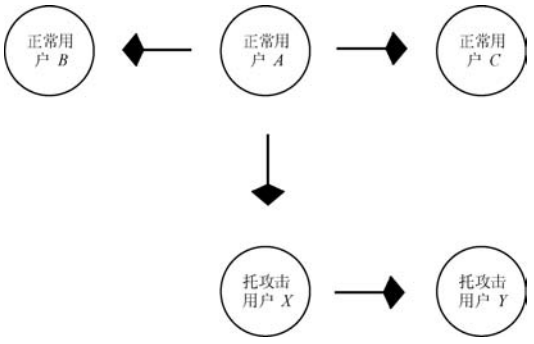

图 3 托攻击用户的伪装性

3）传染性：多个托攻击用户对于同一个正常用户添加信任，导致该正常用户被检测为托攻击用户。如果该正常用户被多数正常用户所信任，恶意的信任关系的添加会降低该用户在信任网络中的可信度，最终导致整体的评分失衡，如图 4 所示。

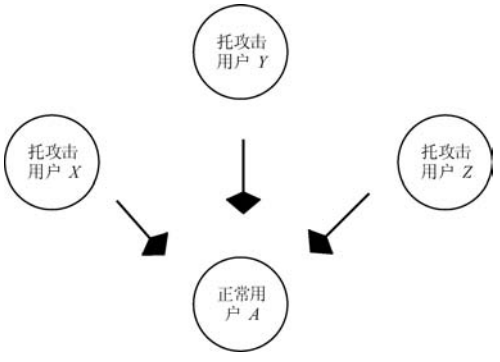

图 4 托攻击用户的传染性

2 统计量与 TSAD 算法描述

根据 1.3 节中托攻击用户在信任网络下的表现特征，与正常用户的信任关系对比，提出以下统计量：信任集群等级 TCL（Trust Cluster Level）、信任项目等级 TPL（Trust Project Level）、信任相似度等级 TSL（Trust Similarity Level）、全局一致度等级 GCL（Global Consistency Level）。结合以上统计量计算，给出信任托攻击检测 TSAD 算法（Trust Shilling Attacks Detection）的相关描述。

2.1 信任集群等级 TCL

该等级描述了信任网络中的用户彼此信任的“集群”程度。由于正常用户 A 的信任关系呈现非对称性，其信任的用户往往不会有较大的交集。而托攻击用户的对称性特征，导致彼此之间的信任关系形成一定的集群特征。对于该等级，定义如下：

$$TCL = \frac{T_A \cap T_{T_A}}{T_A} \tag{1}$$

式中：T_A 表示用户 A 信任的用户集合；T_{T_A} 表示信任 T_A 的用户集合。对于托攻击用户的传染性特征，式（1）一方面削减托攻击用户对于正常用户添加信任的影响，另一方面正常用户误信任托攻击用户的影响也在公式中进行削减。以图 3 为例，对于分子，托攻击用户 X 对正常用户 A 信任时，托攻击用户 X 不会出现在用户 A 信任的用户集合中；对于分母，用户 A 信任了托攻击用户 X，但是由于托攻击用户 X 信任的托攻击用户集合 Y，没有被用户 A 信任，不会参与计算。

2.2 信任项目等级 TPL

为了欺骗正常用户，托攻击用户会对填充项目进行评分，一方面成为正常用户 A 的邻居用户，一方面对于目标项目进行最大最小值评分而改变评分预测。评分可以由托攻击的随机攻击的特性得出。托攻击用户的评分物品数量几乎相同且评分物品数目较多。而实际推荐情景中，正是由于用户对于较少的物品评分，导致评分矩阵数据稀疏使得推荐不理想。利用托攻击用户的这一特征，定义 TPL 为：

$$TPL = \frac{\sum_{t \in T_A} \frac{I_A \cap I_t}{I_A}}{Number_{I_A}} \tag{2}$$

式中：I_t 表示用户 t 评价的项目集合；I_A 表示用户 A 评价的项目集合；$Number_{I_A}$ 表示用户 A 评价的项目集合的数目。现实生活中，正常用户 A、B、C 可能为同一个宿舍的同学，都只是评论了一个项目，并且其互相之间添加了信任关系。按照式（2）最终计算得到的三个正常用户的 TPL 较高，该等级的设计目的应该是托用户有较高的 TPL。考虑到托用户评分特点，改善式（2），定义式（3），作为 TPL 的判定。

$$TPL = \varphi \frac{\sum_{t \in T_A} \frac{I_A \cap I_t}{I_A}}{Number_{I_A}} + \omega \frac{Number_{I_A}}{Number_{\max}} \tag{3}$$

式中：$Number_{\max}$ 为评分最多项目的用户的评分项目总数，实际上对 $Number_{I_A}$ 进行归一化处理。对于正常用户，由于其数据稀疏性，虽然评价了同一个商品，但是评论数量往往较少，通过调节参数 φ 和 ω 的大小，能够适应不同信任情况的推荐情形，同时也降低正常用户的 TPL 等级。

2.3 信任相似度等级 TSL

托用户攻击方式，不论是托举攻击还是诋毁攻击，对于填充项目都能取得项目的全局平均值，与正常用户相比，尤其考虑正常用户往往没有过多的项目评分，所以两者相似度不高。在信任网络中，由于托攻击用户的相互信任行为和托攻击的相似攻击行为，导致其信任关系中的两个用户有很高的相似度。而不论正常用户是否有信任关系，两者的相似度都不会很高。利

用托攻击用户的这个特征,定义 TSL:

$$TSL = \frac{\sum_{t \in T_A} sim_{A,t}}{Number_{I_A}} \tag{4}$$

式中:$sim_{A,t}$ 为用户 A 和用户 t 的余弦相似度。

2.4　全局一致度等级 GCL

部分托攻击用户不添加信任信息,对系统进行随机攻击,为了增加系统抵御该种托攻击方式的鲁棒性,提出全局一致度等级 GCL,定义如下:

$$GCL = \frac{\sum_{i \in I_A} (r_{A,i} - \bar{r}_i)}{Number_{I_A}} \tag{5}$$

式中:$r_{A,i}$ 为用户 A 对于项目 i 的评分;$\bar{r}_i$ 为项目 i 所有评分的平均评分,最大削弱信任关系导致的计算不确定性。对于托攻击用户,由于其采用相同的攻击方式,最终计算得到的全局一致度等级稳定在某一个数值附近。根据该特征,通过计算托用户集合中的全局一致性等级,就能发现没有添加信任信息的托攻击用户。

2.5　TSAD 算法描述

算法主要分为信任网络中的托用户判断和未添加信任信息的托用户判断两个部分。

1)信任网络中的托用户判断。首先计算信任网络的统计量 TCL、TPL、TSL,将每个统计量大于各自阈值 α、β、γ 的用户加入托攻击用户集合。在添加之后,在托攻击用户集合中的用户,满足以下条件:信任关系中有较大的"集群",评论了较多的项目且信任关系的用户共同评分的项目较多,信任关系中的用户与自身有较高的相度。可以认为,此时集合中的用户是添加了信任信息的托攻击用户。

2)未添加信任信息的托用户判断。通过信任网络中的托用户集合,计算其 GCL 的平均值。此时正常用户集合中包含有信任信息的用户和未添加用户信任信息的集合,对于正常用户集合计算每一个用户的 GCL,根据阈值 δ 将位于特定区间$[\overline{GCL} - \delta, \overline{GCL} + \delta]$的用户加入托用户集合。

算法步骤如下:

1. 将用户分为托攻击用户集合 *attackUser* 和正常用户集合 *normalUser*,初始化为空。

2. 在信任关系数据集中,计算每一个有信任关系用户的 TCL、TPL、TSL。

3. 将 TCL > α,TPL > β,TSL > γ 的用户添加到 *attackUser* 集合中。

4. 计算 *attackUser* 集合所有用户的 GCL 的平均值,记为 $\overline{GCL}$。

5. 计算 *normalUser* 中的每一个用户的 GCL,并将 GCL 位于区间 $[\overline{GCL} - \delta, \overline{GCL} + \delta]$ 的用户添加到 *attackUser* 集合中。

6. 算法结束,*attackUser* 集合中的用户为检测出的托攻击用户。

3　仿真实验

3.1　实验数据集

本次实验的数据采用含有信任信息的 Eponions 数据集[22-23],数据集包含 49 290 位用户,139 738 个不同的项目,664 824 条评分记录和 487 181 条信任记录。数据集包含两个文件,用户评分数据 ratings_data.txt.bz2 和用户信任关系数据 trust_data.txt.bz2。用户评分数据格式:user_id item_id rating_value,例如:3 12 5。用户信任关系数据格式:source_user_id target_user_id trust_statement_value,例如:22633 12220 1。

3.2　实验环境

系统:Ubuntu。软件:Java,Spark,Hadoop。内存:16 GB。CPU:4 核。编程语言:Scala,Java。

3.3　评价标准

托攻击用户检测率:该项反映了不同攻击程度下,算法对于托攻击的检测效果,衡量了系统的鲁棒性。定义如下:

$$\text{托攻击用户检测率} = \frac{\text{检测出的托攻击用户}}{\text{托攻击用户总数}} \tag{6}$$

由于托攻击的目的就是将项目的评分拉高或者降低,最终达到提高推荐或者减低推荐的目的。采用该标准来检测对比的两种算法与文本算法在受攻击时的抵抗攻击程度。该值越小,说明托攻击未能对攻击项目的评分加以影响,算法的鲁棒性更好。定义如下:

$$\text{受攻击时的抵抗攻击程度} = \frac{\sum_{i \in I_{\text{Attack}}} \bar{r}_{i_{\text{Attack}}} - \bar{r}_{i_{\text{Original}}}}{Number_{I_{\text{Attack}}}} \tag{7}$$

式中:I_{Attack} 表示托攻击的攻击项目集合;$Number_{I_{\text{Attack}}}$ 表示托攻击的攻击项目集合项目总数;$\bar{r}_{i_{\text{Attack}}}$ 表示加入了托攻击的数据集中受攻击项目的 i 的平均评分;$\bar{r}_{i_{\text{Original}}}$ 表示原始数据集,即未加入托攻击的数据集中项目 i 的平均评分。

3.4　实验结果及分析

本次实验对比的对象是协同过滤算法和林韶娟等[15]提出的基于二值信任网络的推荐算法。托攻击方式选择随机攻击的托举攻击,在信任信息数据集中,人为地增加托攻击用户的信任关系,其信任关系为双

向的,人数数量为 50,编号范围为 50000 – 50050,并且对于正常用户随机的对编号 50000 – 50050 的托攻击用户添加信任关系。在用户评分数据中,人为地增加托攻击用户,人数数量为 50,编号范围为 50051 – 50100。采取随机攻击的方式,按照不同的填充大小和攻击大小,增加托用户的评分信息。

对于原始数据集,采用协同过滤和基于信任的推荐算法,得到结果数据;对于添加了托用户攻击的数据集,采用协同过滤和基于信任的推荐算法,得到结果数据;使用 TSAD 算法进行托用户检测之后,对正常用户集合采用协同过滤和基于二值信任网络的推荐算法,得到结果数据。实验结果如下:

图 5 为不同填充大小、不同攻击大小下的托攻击用户检测率。在填充大小和攻击大小都为 0.10% 的情况下,由于托攻击用户的特征不够明显,此时一小部分正常用户由于也具有较高的 TCL、TPL、TSL,而被加入托用户集合。而当填充大小和攻击大小的数量上升到 1.00% 时,正常用户已经很难获得较高的 TCL、TPL、TSL,而不会被误加入托攻击用户集合。

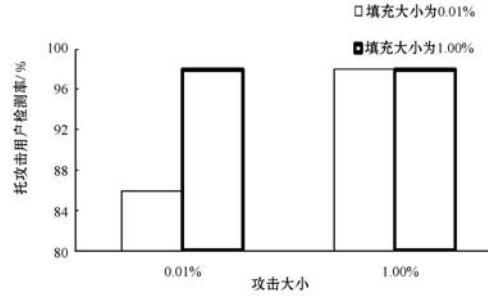

图 5 不同填充大小、不同攻击大小下的托攻击用户检测率

图 6 为未使用 TSAD 算法的协同过滤算法的受攻击项目的攻击程度,填充项目在评分数大于 3 且评分为 3 的项目集合中选择 100 个项目,攻击大小分别为 5、10、20。可以看到,由于填充项目的评分与正常用户的评分一致,使得托攻击用户与每一个用户都拥有很高的相似度,在相似用户中排名靠前。并且托攻击用户的平均评分接近正常评分,在预测评分公式中,对于攻击项目得到更高的评分,算法对于托攻击用户抵御较差。

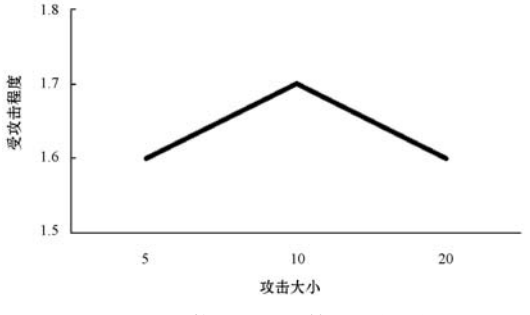

图 6 未使用 TSAD 算法的协同过滤算法的受攻击项目的攻击程度

图 7 为基于二值信任网络算法的受攻击项目的攻击程度,该算法在预测评分时采用了用户之间的信任度,而信任度是根据信任用户的个数计算的。为了方便比较,依然采用协同过滤算法时的填充大小和攻击大小。可以看到,虽然二值网络算法使用信任值增强了推荐的精确性,但由于实验数据集中,人为增加正常用户对于托攻击用户的信任关系,导致托攻击用户在用户预测评分计算时,信任值较高较大,使得最终的受攻击项目预测评分依然有较大的偏差,无法较好地消除托攻击用户的影响。

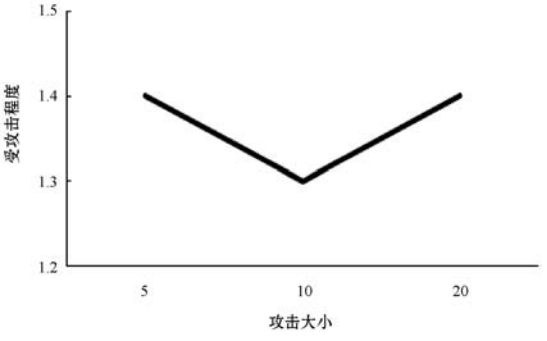

图 7 基于二值信任网络算法的受攻击项目的攻击程度

图 8 为 TSAD 算法检测之后的受攻击项目的攻击程度,由于填充大小较少,修正 TPL 计算中项目数量的权重,将 φ 增大,ω 减小,使得托攻击用户即使拥有较少的总评分项目数,依然会有较大的 TPL,会被算法检测为托攻击用户,加入到托攻击用户集合中。与之前的实验结果对比,说明在推荐的过程中,对于托攻击用户进行检测,TSAD 算法能够提升推荐系统的准确率,增强系统的鲁棒性。

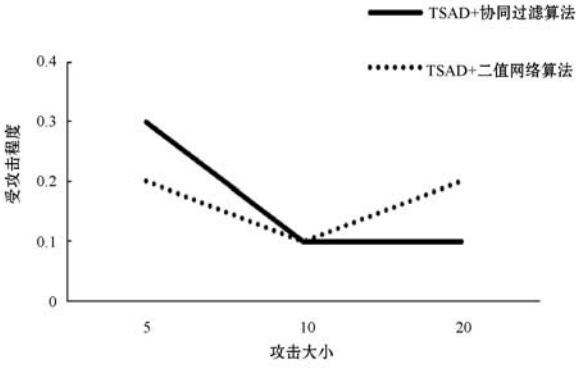

图 8 TSAD 算法检测之后的受攻击项目的攻击程度

4 结 语

在包含信任信息的推荐情景下,为了增加系统的鲁棒性,本文从抵御托攻击的角度提出信任网络下的托攻击用户检测算法 TSAD。通过分析信任网络下托攻击用户的行为特征,提出信任网络下的不同托攻击检测统计量,以检测隐藏在正常用户集合中的托攻击

用户。经过实验的验证,在使用本文的 TSAD 算法检测过滤到托攻击用户之后,对于协同过滤等易受托攻击的算法,均能较好地抵御托攻击用户的托举攻击或者诋毁攻击。但是,由于托攻击手段的复杂性,往往在实际的托攻击情况中,多种攻击方式混合使用。此情境下,本文提出的统计量可能不能准确检测出托攻击用户,需要多种统计量来作为衡量维度或者综合机器学习等知识去检测。即便如此,TSAD 算法也增加了信任网络下推荐系统对于随机攻击托攻击方式的鲁棒性。面对更加复杂的托攻击手段,希望本文能给其他学者解决问题提供一些思路。

参 考 文 献

[1] Wang H X. An improved collaborative filtering recommendation algorithm[C]//2019 IEEE 4th International Conference on Big Data Analytics (ICBDA),2019.

[2] Kharita M K,Kumar A,Singh P. Item-Based collaborative filtering in movie recommendation in real time[C]//2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC),2018.

[3] Zheng Q. An improved collaborative filtering algorithm based on expert trust and time decay[C]//2018 11th International Symposium on Computational Intelligence and Design (ISCID),2018.

[4] Wu C S M,Garg D,Bhandary U. Movie recommendation system using collaborative filtering[C]//2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS),2018.

[5] Lam S K,Riedl J. Shilling recommender systems for fun and profit[C]//13th International Conference on World Wide Web,2004.

[6] Burke R,Mobasher B,Williams C,et al. Classification features for attack detection in collaborative recommender systems[C]//12th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. ACM,2006.

[7] O'Mahony M,Hurley N,Kushmerick N,et al. Collaborative recommendation:A robustness analysis[J]. ACM Transactions on Internet Technology,2004,4(4):344 - 377.

[8] 窦文,王怀民,贾焰,等. 构造基于推荐的 Peer-to-Peer 环境下的 Trust 模型[J]. 软件学报,2004,15(4):571 - 583.

[9] 李勇军,代亚非. 对等网络信任机制研究[J]. 计算机学报,2010,33(3):390 - 405.

[10] 朱艳春,刘鲁,张巍. 在线信誉系统中的信任模型构建研究[J]. 控制与决策,2007,22(4):413 - 417,422.

[11] Griaznova O. Trust and Uncertainty:How to Communicate Successfully Book Review:Gambetta D. (2011) Kody kriminal'nogo mira. Kak obshñhayutsya mezhdu soboy prestupniki [Codes of the Underworld:How Criminals Communicate], Cheboksary:Perfektum[J]. Journal of Economic Sociology,2015,16(2):80 - 89.

[12] 潘一腾,何发智,于海平. 一种基于信任关系隐含相似度的社会化推荐算法[J]. 计算机学报,2018,41(1):65 - 81.

[13] Wang Y. A trust prediction method for recommendation system[C]//2017 9th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC),2017.

[14] Shabut A M,Dahal K P,Bista S K,et al. Recommendation based trust model with an effective defence scheme for MANETs[J]. IEEE Transactions on Mobile Computing,2015,14(10):2101 - 2115.

[15] 林韶娟,陶晓鹏. 基于二值信任网络的推荐算法改进[J]. 计算机应用与软件,2012,29(12):157 - 160.

[16] Lam S K,Riedl J. Shilling recommender systems for fun and profit[C]//13th International Conference on World Wide Web. ACM,2004.

[17] 田俊峰,蔡红云. 托攻击与推荐系统安全[J]. 河北大学学报(自然科学版),2018,38(6):640 - 647,655.

[18] Yang H S,Sun J H. A study on hybrid trust evaluation model for identifying malicious behavior in mobile P2P[J]. Peer-to-Peer Networking and Applications,2016,9(3):578 - 587.

[19] Jiang F,Tian R. The influence of shilling attacks with different attack cycles[C]//2017 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI),2017.

[20] Zhang F,Ling Z,Wang S. Unsupervised approach for detecting shilling attacks in collaborative recommender systems based on user rating behaviours[J]. IET Information Security,2019,13(3):174 - 187.

[21] Chichani A,Golwala J,Gundecha T,et al. Advancing recommender systems by mitigating shilling attacks[C]//2018 9th International Conference on Computing,Communication and Networking Technologies (ICCCNT),2018.

[22] Massa P,Souren K. Trustlet,open research on trust metrics [J]. Journal of Scalable Computing:Practice and Experience,2008,9(4):341 - 351.

[23] Massa P,Avesani P. Trust-aware recommender systems[C]//2007 ACM Conference on Recommender Systems,2007.

(上接第 245 页)

[9] 杨洁,王国胤,刘群,等. 正态云模型研究回顾与展望[J]. 计算机学报,2018,41(3):724 - 744.

[10] 马超红,翁小清. 基于 PAA 的时间序列早期分类[J]. 计算机科学,2018,45(2):291 - 296,317.

[11] 汪军,朱建军,刘小弟. 兼顾形状-距离的正态云模型综合相似度测算[J]. 统工程理论与实践,2017,37(3):742 - 751.

[12] 查翔,倪世宏,谢川,等. 云相似度的概念跃升间接计算方法[J]. 系统工程与电子技术,2015,37(7):1676 - 1682.