文章编号:1000-582X(2011)05-135-08

结合信任和项目的抗攻击协同过滤算法

高 旻[1a],江 峰[2],吴中福[1b]
(1.重庆大学 a.软件学院; b.计算机学院,重庆 400044; 2.重庆广播电视大学,重庆 400052)

摘 要:为提高基于项目协同过滤推荐方法的抗评分攻击能力,提出结合用户信任等级和项目进行资源协同过滤算法。提出根据用户兴趣相关性、评分相似性和评分相关性构建用户关联图,然后提出用户信任等级计算模型,并将用户信任等级值作为用户的权重结合到经典协同过滤推荐算法 Slope One 的项目差异性的计算中,形成基于用户信任等级的协同过滤方法。实验数据表明新算法在不影响推荐的预测准确性的基础上,比传统的过滤推荐算法具有更好的抗攻击能力。

关键词:协同计算;算法;推荐系统;信任;个性化
中图分类号:TP311 **文献标志码**:A

An anti-"shilling attacks" collaborative filtering algorithm based on user trust ranks and items

GAO Min[1a], *JIANG Feng*[2], *WU Zhong-fu*[1b]
(1a. College of Software Engineering; 1b. College of Computer Science, Chongqing University, Chongqing, 400044, P. R. China; 2. Chongqing Radio and TV University, Chongqing, 400052, P. R. China)

Abstract: A collaborative filtering algorithm based on user trust ranks and items is proposed to improve the anti-"shilling attacks" ability. Firstly, a user relationship graph is built based on user interest similarities, rating similarities, and rating correlations. Secondly, using the relationship graph, a userrank model is proposed to calculate user trust ranks. Thirdly, the userrank values are taken as users' weights to incorporated into the typical item-based Slope One algorithm. Finally, we experimentally evaluate our approach and compare it to Slope One. The experiment results suggest that our approach provides better recommendation than Slope One.

Key words: collaborative computing; algorithms; recommendation systems; trust; personalization

随着互联网上资源的迅速增长,个性化推荐系统已经逐渐成为研究者和用户关注的重要研究内容[1-2]。协同过滤推荐方法不受推荐内容的限制并可以为用户发现潜在的兴趣,在推荐系统中得到广泛的应用。

目前,个性化推荐技术在诸如冷启动问题、预测精度问题和基于情境的推荐等方面取得了重大突破[3-5],但仍然面临着新的问题和严峻的挑战,如某些销售商为了使自己的商品畅销,采取欺骗手法提高商品被推荐的频率[4-10](托攻击)。当编造的用户

收稿日期:2010-12-05
基金项目:国家科技支撑计划(2007BAF23B0302);国家自然科学基金资助项目(61075053);重庆市自然科学基金(CSTC,2010BB224);高等教育出版社数字出版支撑环境项目(基于本体、语义和语用的智能化教育资源应用平台);重庆市教育委员会科学技术研究项目(KJ101602)
作者简介:高旻(1980-),女,重庆大学博士,主要从事个性化推荐、协同过滤、远程教育的研究,(Tel)02365127900;(E-mail)gaomin@cqu.edu.cn。

评分被注入商务网站后，很可能对商品的推荐排名造成影响，若不能有效地对托攻击进行检测，将影响推荐用户真正喜欢的商品，致使用户满意度下降。如果能对评分攻击分析出用户的信任等级，将虚假用户的信任度降低，就能有效地解决虚假评分所产生的问题。

受攻击问题现已成为推荐算法中的研究热点，例如，文献[4，5，7，8]就协同过滤推荐算法受评分攻击的鲁棒性进行了研究，分析了攻击模型和攻击效果。文献[9，10]探讨了如何识别攻击用户，但其方法并未验证其对协同过滤推荐算法的作用。国内具有代表性的文献[6]，也提出过滤推荐系统受评分攻击的研究，但算法抗攻击能力仍有待进一步提高。另外，对于基于信任的推荐也有一些初步的研究，例如，文献[18]提出了项目级和用户概要级的信任模型及基于信任的推荐以减少推荐的错误率。Massa在文献[10]中提出让用户自己提供对他人的信任数据，然后根据这些数据进行推荐，其又在文献[9]中提出利用构建信任网络来解决协同过滤的稀疏性和隐私性问题。这些算法可实现性并不强。国内张富国[6]提出项目级、主题级和用户概要级的信任度计算方法，但其3种级别的信任度计算都只是基于用户已知评分数量，还需要进一步完善和提高。这些文献都对笔者的研究提供了良好的基础，笔者利用用户信任等级对基于项目的协同过滤推荐算法的抗攻击能力进行了深入的研究，并与文献中的研究方法和结果进行了比较。

首先提出基于用户兴趣相似性、评分相似性和相关性构建用户关联图的方法；然后提出基于PageRank的用户信任计算模型，并基于用户信任等级计算项目之间差异性进行评分预测；并对新的推荐方法用标准数据集进行实验。实验表明基于用户信任等级的协同过滤推荐可以提高传统的基于项目的协同过滤推荐方法的抗评分攻击能力。

1 相关工作介绍

由于笔者在用户信任等级的计算模型中将考虑评分攻击对信任等级的影响，因此本节首先分析推荐系统中的评分攻击问题，然后对信任与推荐的关系进行分析，最后总结目前已有的基于信任的个性化推荐方法的优缺点。

1.1 协同过滤推荐中的评分攻击问题

攻击者通过注入虚假用户概貌信息，试图改变系统的推荐结果的这类攻击被称为“托攻击”，也被称为“用户概貌注入攻击”[11-12]。根据攻击目的的不同托攻击可分为两类：如果攻击是为了提高目标项目的推荐频率，则称为“推”攻击；反之则称为“核”攻击。

一个评分攻击信息 $\boldsymbol{AP}$[4，13]是 p 维的向量，其中 p 是系统的项目数。一个 $\boldsymbol{AP}$ 中的项目可以分成4个集合：填充集 I^{F}、未评分集 I^{ϕ}、选择集 I^{S} 和目标集 I^{T}，如图1所示。$|AP|=|I^{\mathrm{F}}|+|I^{\phi}|+|I^{\mathrm{S}}|+|I^{\mathrm{T}}|$，即 $p=k+l+m+n$。

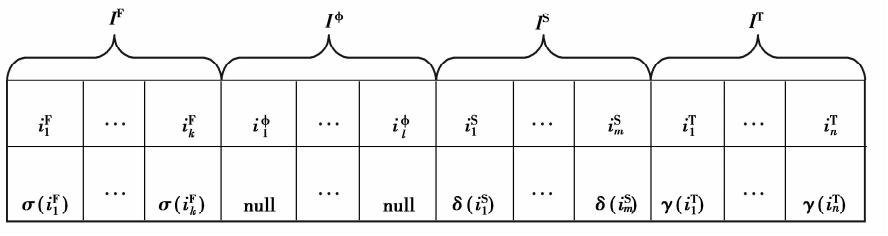

图1 评分攻击通用模型

I^{F} 是用来输入相似评分的集合，一般随机选择。

I^{s} 是空集或者很小的集合，是与目标项目有某种关系的项目集合。

I^{T} 是一个或几个目标项目的集合，其预定值在推攻击时为最高分，在核攻击时为最低分。

I^{F} 和 I^{S} 在不同的攻击策略中的填充方法不同[11,14,15]。目前对基于用户的协同过滤推荐和基于项目的协同过滤攻击效果较好的有[4,7]：

1)流行攻击(Bandwagon Attacks)。I^{F} 填充符合评分正态分布的随机值，I^{S} 是流行项目的集合，填充最高评分，对 I^{T} 中的目标项目也填充最高分。

2)部分攻击(Segment Attacks)。I^{F} 填充最低评分；I^{S} 则是流行的项目集合，填充最高评分；I^{T} 中的目标项目一般也填充最高分。

据研究者分析，对未加任何防范的经典推荐算法使用这两种攻击策略，只需要1%的虚假评分就可以将一个项目置顶[7]。这使系统的推荐质量下

降,进而使用户对系统的可信性产生怀疑。因此,在笔者提出的信任等级计算模型中,考虑了对攻击的防范,具体内容见第 2 节。

1.2 相关工作

文献[18]提出项目级和用户概要级的信任模型及基于信任的推荐,其主要目的是减少推荐的错误率,而不是提高算法的鲁棒性。

文献[10]也提出在协同过滤系统中根据信任进行推荐,但其方法不是根据已经存在的评价数据构建信任模型,而是让用户自己提供对他人的信任数据,这种方法在实际系统中难以奏效。

后来文献[9]提出构建信任网络解决协同过滤的稀疏性和隐私性问题,并能在一定程度上提高推荐系统的荐全率和荐准率。信任网络的构建可以更准确地寻找用户邻居,但研究侧重于提高推荐预测的精度,而不是提高抗攻击能力。

文献[6]提出项目级、主题级和用户概要级的信任度计算方法。其推荐算法在一定程度上解决评分攻击的问题,但其 3 种级别的信任度计算都只是基于用户已知评分数量,还有待于进一步完善和提高。与此相似的有文献[19]。

文献[20]提出全局和局部信任相结合的信任模型。其中,全局信任根据用户已知评分的多少和用户的朋友数目确定,局部信任是指用户的评分相似性。该算法中并未考虑信任的传递问题,而传递是信任等级的一个重要特性。

2 基于信任等级的个性化推荐

本研究基于信任推荐的系统架构包括 3 个部分(如图 2 所示):第一,提出构建用户关联图模型的方法(根据兴趣相似性,用户相似性和评分相关性构建);第二,提出信任等级计算模型;第三,将用户信任等级结合到项目间的差异性计算中并进行相应的评分预测。

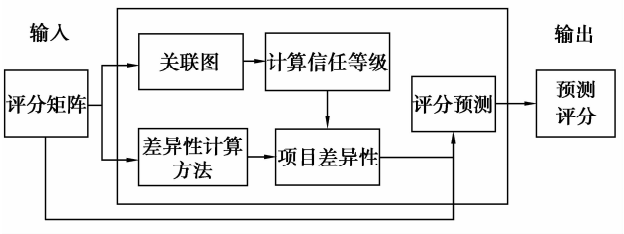

图 2 基于信任的协同推荐架构

2.1 构建关联图模型

在大部分推荐系统中,用户关系是指用户相似性,也即判断用户评分的相似程度,但这种相似性关系只反应了这两个用户关系的一个侧面。采用这种关系计算方式时,在两个用户可能同时对很多项目都评过分且评分差异很大的情况下,这两个用户就不会被认为是有紧密关联关系的;但既然这两个用户浏览过或购买过相同的资源项,说明这两个用户在某些方面是有紧密关联关系的。因此用户之间的关系应该从如下几方面分析:

1)兴趣相似性。两个用户共同评价过的项目越多,就说明用户的关注点和兴趣点是相似的。这种相似性体现了用户兴趣之间的关系,对推荐是非常重要的,因此在研究中被认为是用户之间的基础关系之一[6, 20]。

2)用户相似性。用户对共同评价过的项目的评分可能不同,说明用户对资源项本身的质量或能产生效果的评论不同,如果两个用户之间的评分越相近,说明他们具有较高的评分相似性或评论标准相似性。用户相似性是基于用户的协同推荐系统中最常用的关系[1, 21]。在选择商品的时候,人们更加信任与自己评分相似和评论标准相近的人的推荐,因此,在构造用户相关图时,这种关系也是非常重要的。

3)评分相关性。指对象属性之间线性联系的度量(又指相关系数)。有研究[7]指出,虚假用户之间评分的协方差 $Cov(X,Y)$ 以及虚假用户与正常用户之间的评分的协方差远低于正常用户评分之间的协方差。因此,这种关系也是笔者研究中考虑的用户关系之一。由于协方差是一个有量纲的量,必须依赖于对象属性的度量单位,因此在实际应用中,通常使用相关系数 $\rho_{X,Y}$ 而不用协方差判断两个向量的线性相关程度[22]。因此,在构造用户关联图的时候将考虑用户评分之间的相关系数,以此更好地抵御评分的攻击。

在笔者的研究中,用户相似性的计算采用常用的调整余弦相似性计算方法。下面介绍兴趣相关性和相关系数的计算。

2.1.1 兴趣相关性计算

对兴趣相关性的计算考虑如下两点:1)如果两个用户共同评价过的项目越多,则他们的兴趣相关性越高;2)一对用户共同评分的项目个数相同,但其中一个用户总的评分项目多,而另一个较少,则他们的兴趣相关性也不同。因此,对共同评分个数标准化来解决这个问题。标准化后的矩阵为 ***UIM*** 矩阵,计算方法如式(1)所示。$\boldsymbol{UIM}_{u_i,u_j}$ 由用户 u_i 和 u_j 之间的共同评分项目数和用户 u_j 或用户 u_i 和其他所

有用户 u_k 共同评分项目数决定。不失一般性，假定 $\sum_{u_k \in U} | I(u_i, u_k) | \neq 0$。

$$\boldsymbol{UIM}_{u_i,u_j} = \frac{| I(u_i, u_j) |}{\sum_{u_k \in U} | I(u_i, u_k) |}。 \quad (1)$$

2.1.2 用户评分相关性的计算

对具有 n 对观测值的样本，x 与 y 的协方差为 $Cov(x,y) = \frac{1}{(n-1)} \sum_{k=1}^{n} (x_k - \overline{x})(y_k - \overline{y})$。在得到协方差的基础上，可以通过 $\rho_{X,Y} = \frac{Cov(X,Y)}{\sqrt{D(X)}\sqrt{D(Y)}}$ 计算向量之间的相关系数，也即 $\rho_{X,Y} = \frac{\sum_{k=1}^{n}(x_k - \overline{x})(y_k - \overline{y})}{\sqrt{\sum_{k=1}^{n}(x_k - \overline{x})^2}\sqrt{\sum_{k=1}^{n}(y_k - \overline{y})^2}}$。从公式可知，$\rho_{X,Y}$ 与 $Cov(X,Y)$ 总是成正比。又因为 $\rho_{X,Y}$ 是无量纲的量，所以在本研究中采用相关系数表示用户 u 与 v 评分的相关性：

$$\rho_{u,v} = \frac{\sum_{i \in I(u) \cap I(v)} (r_{u,i} - \overline{r_u})(r_{v,i} - \overline{r_v})}{\sqrt{\sum_{i \in I(u) \cap I(v)} (r_{u,i} - \overline{r_u})^2}\sqrt{\sum_{i \in I(u) \cap I(v)} (r_{v,i} - \overline{r_v})^2}}, \quad (2)$$

其中：$r_{u,i}$ 为用户 u 对项目 i 的评分；$\overline{r_u}$ 为用户 u 所有评分的平均值；$i \in I(u) \cap I(v)$ 为用户 u 和 v 都评过分的项目。计算所有用户评分的相关系数后，就可以得到用户相关系数矩阵 $\boldsymbol{U\rho M}$。

这样就得到所有构成用户关联关系的要素：用户兴趣相关性矩阵 $\boldsymbol{UIM}$、评分相似性矩阵 $\boldsymbol{USM}$ 和评分相关性矩阵 $\boldsymbol{U\rho M}$。他们分别代表了用户之间的不同侧面的关系，且具有相似量纲，因此，采用均值作为用户之间的关系，$\boldsymbol{UCM} = \frac{\boldsymbol{UIM} + \boldsymbol{USM} + \boldsymbol{U\rho M}}{3}$。

$\boldsymbol{UCM}$ 可以被看作是一个关联图 G 的带权重的连接矩阵。G 代表用户集合，如果 $\boldsymbol{UCM}_{u_i,u_j} \neq 0$，则存在一条从用户 u_i 到 u_j 的连接，此连接的权重为 $\boldsymbol{UCM}_{u_i,u_j}$，此时就构建了用户关联图模型。图3是一个用户关联图模型的实例。关联图 G 正是进行用户关联关系计算的数据模型。

2.2 信任计算模型

在用户信任等级计算模型的构建过程中，考虑影响信任等级的两个方面。第一，用户的开放性。用户的开放性体现在用户评价项目的数量，并由此构成用户信任等级的初始值。第二，信任的传递性。信任在用户之间是有传递性的。传递性是指用户信任等级可以在图内结点之间流动，如何根据信任等级流在图中的流动进行信任等级值的计算是非常重要的。

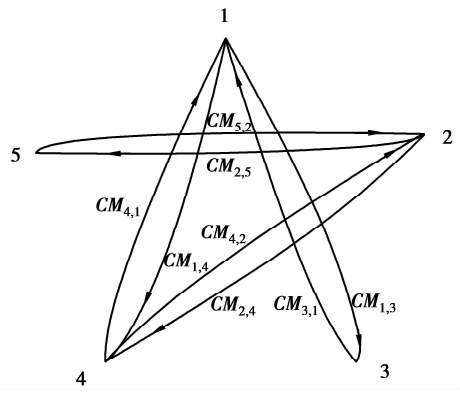

图3 用户关联图模型实例

在笔者实验研究中发现这种用户信任等级值的流动遵循3个规则：1）如果用户 u_i 被一个或多个高信任等级的用户连接，则该用户具有较高的信任等级；2）当用户连接到其他用户时，其信任等级值将随着连接传播，而这种传播将减少其信任等级值，随着连接层次的增加，其传播影响将越来越弱；3）如果一个具有高信任等级值的用户 u_i 连接到其他多个用户，这些用户将共享该用户 u_i 的部分信任等级值，共享多少由连接的权重确定。

不难得出，此3条规则与 PageRank 模型中的传播和衰减规则相似；但此关联图的连接是有权重的，这又与 PageRank 模型不同。因此基于 PageRank 模型的计算研究[23-25]，便可以高效地计算 UserRank。

在 PageRank 模型中，假定有一个图 $G=(V, E)$，V 是结点，E 是结点之间有向弧的连接。如果一个结点被重要的结点连接且出度比较小，则这个结点的重要性高，其重要性计算公式为 $PR(i) = (1-\alpha) \cdot \frac{1}{|V|} + \alpha \cdot \sum_{q:(q,i) \in E} \frac{PR(q)}{O(q)}$，此处 $O(q)$ 是结点 q 的连出结点，α 是衰减系数，其常用的值为 0.85[3]。

由此得到用户 u_n 的信任等级 UserRank 的计算方法：

$$UR(u_n) = (1-\alpha) \cdot \frac{1}{V_w(u_n)} \cdot UR(u_n) + \alpha \cdot \sum_{u_k:(u_k,u_n) \in E} \frac{UR(u_k)}{O_w(u_k)}。$$

其中：u_k 是一个连到用户 u_n 的用户；$O_w(u_k)$ 是用户 u_k 连接到的用户集合，$O_w(u_k) = \frac{\sum_{u_m:(u_k,u_m) \in E} w_{u_k,u_m}}{w_{u_k,u_n}} =$

$\frac{\sum_{u_m:(u_k,u_m)\in E} CM_{u_k,u_m}}{CM_{u_k,u_n}}$；$V_w(u_n)=\sum_{u_m:(u_m,u_n)\in E} CM_{u_m,u_n}$。因此，用户 u_n 的信任等级 UserRank 的计算公式为：

$$UR(u_n)=\frac{(1-\alpha)\cdot UR(u_n)}{\sum_{u_m:(u_m,u_n)\in E} CM_{u_m,u_n}}+\alpha\cdot \sum_{u_k:(u_k,u_n)\in E}\frac{UR(u_k)\times CM_{u_k,u_n}}{\sum_{u_m:(u_k,u_m)\in E} CM_{u_k,u_m}}。$$

2.3 基于用户信任等级的资源推荐算法

本研究中，把用户信任等级 $UR(u)$ 作为用户 u 的权重 w_u，即 $w_u=UR(u)$，再把权重结合到 Slope One 的项目之间相异性的计算中，得到新的算法计算 $d_{i,j}$：

$$d_{i,j}=\frac{\sum_{u\in U(i)\cap U(j)}(r_{u,i}-r_{u,j})\cdot w_u}{\sum_{u\in U(i)\cap U(j)} w_u},\qquad(3)$$

其中，$U(i)\cap U(j)$ 表示对项目 i 和 j 都进行过评分的用户集合。

得到项目之间的差异性后，采用公式(4)完成对未知评分项的预测。

$$p_{u,i}=\overline{r_u}+\frac{\sum_{j\in R_u} d_{i,j}}{|R_u|}。\qquad(4)$$

3 实验及结果分析

3.1 实验数据集与实验过程

为验证信任等级对资源推荐算法的影响，把两个算法(Slope One 和 UserRank-based Slope One)分别用明尼苏达大学的 MovieLens 数据集(十万条记录)进行实验。数据集中每个用户至少对 20 部电影进行了评分。数据集分 5 次从十万条记录中选取 80%作为训练集，20%作为测试集，形成 ***U*1*base***，…，***U*5*base*** 和 ***U*1*test***，…，***U*5*test***。实验过程如下：

1)对评分矩阵 ***Uibase*** 生成用户关联评分矩阵 ***CM***(用户-用户矩阵)，计算每个用户的重要性等级 UserRank。

2)将 UserRank 结合到基于项目的协同过滤经典算法 Slope One 进行评分预测。

3)比较新算法得到的评分预测结果与 ***Uitest*** 中的真实结果，求得平均绝对误差、*Predshift* 和 *HitRatioShift* 等性能值。

4)比较原有旧算法计算评分预测结果与 ***Uitest*** 中的真实结果，也得到平均绝对误差、*Predshift* 和 *HitRatioShift* 等性能值。

5)分别注入不同比例的虚假用户评分信息，且每次使用的填充规模不同，重复步骤 1)-4)。

3.2 实验评价指标

实验中将对各个算法受攻击前后平均预测值的偏移量 *PredShift*[12]、命中率偏移量 *HitRatioShift*[4] 及平均绝对误差 *MAE* 进行分析。

$$PsredShift=\frac{\sum_{i\in I}\sum_{u\in U} abs(p'_{u,i}-p_{u,i})}{|U||I|},$$

其中：$p_{u,i}$ 和 $p'_{u,i}$ 分别为攻击前后的预测评分值；U 为用户集合；I 为测试的目标项目集合；abs 为取绝对值。

HitRatioShift 为攻击前后推荐列表中用户相关项目出现个数的变化值。因为大多数用户只对推荐列表中靠前的项目感兴趣，而预测值 *PredShift* 的变化并不一定能引起推荐列表的变化。所以，又引入 *HitRatioShift* 来计算用户相关项目出现个数的变换情况。其中，H_u 和 H'_u 分别表示攻击前后用户 u 的推荐列表中相关项目出现的个数。

$$HitRatioShift=\frac{\sum_{u\in U} abs(H'_u-H_u)}{|U|},$$

MAE 通过计算预测的评分与实际评分之间的偏差度量预测的准确性，*MAE* 越小，推荐质量越高。设所有预测评分集合$\{p_1,p_2,\cdots,p_n\}$，其对应的实际评分为$\{r_1,r_2,\cdots,r_n\}$，则预测结果的误差为

$$MAE=\frac{\sum_{i=1}^{n}|p_i-r_i|}{n}。$$

3.3 实验具体数据的设定

因为评分攻击中“推”攻击的使用较为频繁，所以本研究只针对推攻击进行实验。在实验中各选取 10、15 和 20 个项目作为推攻击的对象进行 20 次实验，且每次的项目都是随机选取的。实验中所采用的最近邻居数为 20，且兴趣相关用户也取 20。*PredShift* 与 *HitRatioShift* 值以选中项目对应于测试集合中的评分进行计算。

在测试鲁棒性时，考虑了如下因素：

1)攻击模式。流行攻击和部分攻击策略各占攻击集合的 50%。

2)攻击评分信息规模。攻击评分信息的数量占攻击前训练集合中用户数量的百分比，分别取 5%、10%、15%与 20%。

3)填充规模。每个攻击评分信息所填充的项目数量占总项目数量的百分比，分别取 5%与 10%。

2 种攻击策略的设定如下：

1)流行攻击。

①I^F项目填充的评分符合均值3.6、偏差1.1的正态分布的随机值。

②I^S项目是评分数量处在前20的项目,填充5分(最高分)。

③I^T填充5分。

2)部分攻击。

①I^F项目填充1分(最低分)。

②I^S项目是攻击项目的相似项目,取前20个项目,填充5分。

③I^T填充5分。

3.4 实验结果分析

3.4.1 攻击对算法评分预测的影响

图4表示攻击对基于信任SlopeOne和传统SlopeOne算法的评分预测的影响。图中,—■—、—▲—和—●—三条线代表传统算法,—◆—、—■—和—▲—三条线代表基于信任的推荐算法;都分别表示系统在攻击10个项目、15个项目和20个项目时对评分预测的影响;Y轴是预测评分受到攻击后产生的评分偏移量;X轴表示不同的攻击规模和填充规模:攻击规模分别为5%、10%、15%和20%;填充规模分别为5%和10%。图中数据显示:与传统的推荐方法相比,基于信任的SlopeOne推荐算法受评分攻击后的评分预测不会因攻击规律和填充规律发生太大变化,最大也不超过0.1。而随攻击规模和填充规模的增加,传统SlopeOne推荐方法受攻击的影响呈上升趋势。

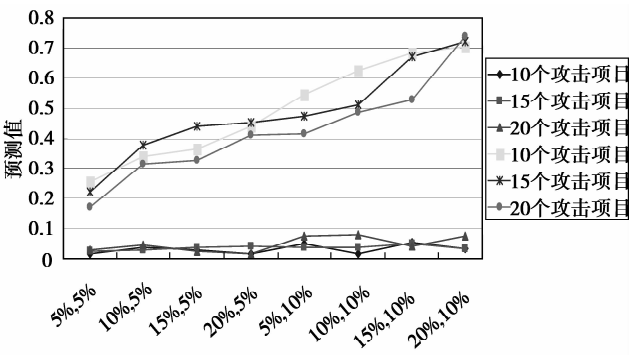

图4 攻击对算法评分预测的影响

3.4.2 攻击对推荐命中率影响的比较

攻击对基于信任的SlopeOne推荐算法和传统SlopeOne推荐算法的命中率的影响如图5所示。其中Y轴表示影响命中率的数值,X轴表示不同的攻击规模和填充规模。图中,—■—和—■—线是攻击对传统算法前10和20个推荐命中率的影响,—✳—和—●—是攻击对基于信任推荐方法前10和20个推荐命中率的影响。

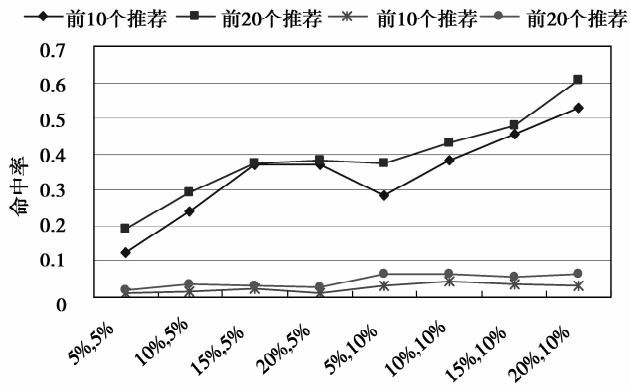

图5 攻击对Slope One算法推荐命中率的影响

图中数据显示:与传统的SlopeOne推荐算法相比,评分攻击对基于信任SlopeOne推荐算法的推荐命中率的影响小得多,基于信任的SlopeOne算法,命中率的影响都在0.1以下,差不多与Slope One算法有着一个数量级的差距;随着攻击规模和填充规模的增加,攻击对传统SlopeOne推荐算法的推荐命中率的影响越来越大,而对基于信任SlopeOne推荐算法推荐命中率的影响不明显。

3.4.3 *MAE*值的比较

如表1所示,引入信任的SlopeOne推荐算法与传统的SlopeOne推荐算法有相似的评分预测准确性。

表1 算法平均绝对误差结果的比较

SlopeOne	UserRank-based SlopeOne
0.740	0.738

3.4.4 算法整体性能比较

从实验数据和图表结果来看,在不影响推荐预测准确性的基础上,引入信任的SlopeOne推荐算法比传统的SlopeOne推荐算法有更好的抗攻击能力,主要体现在两点:1)攻击对引入信任的SlopeOne推荐算法的评分预测和推荐命中率的影响都非常小,而对传统的SlopeOne推荐算法却很大;2)随着攻击规模和填充规模的增加,攻击对传统的SlopeOne推荐算法的影响越来越大,而对基于信任SlopeOne推荐算法的影响却不明显。

4 结 语

近年来,个性化推荐中托攻击问题越来越受到

关注。本研究中引入用户信任等级进行推荐项目之间关系的运算,使系统具有更强的抗评分攻击能力。为验证算法的有效性,用 MovieLens 数据集进行了多组实验,根据攻击策略随机生成的不同攻击评分集合,着重分析比较了在多种攻击规模和填充规模下,攻击对新算法和原有算法的评分预测和命中率的影响。实验数据表明基于信任的 SlopeOne 推荐算法在不影响推荐的预测准确性的情况下比传统 SlopeOne 推荐算法具有更好的抗攻击能力。

参考文献:

[1] Gao M, LIU K C, WU Z F. Personalisation in web computing and informatics: theories, techniques, applications, and future research [J]. Information Systems Frontiers, 2010, 12(5): 607- 629.

[2] Gao M, WU Z F. Personalized context-aware collaborative filtering based on neural network and slope one[C]// Cooperative Design, Visualization, and Engineering 6th International Conference, CDVE 2009, September 20-23, 2009, Luxembourg. Berlin: Springer-Verlag, 2009: 109-116.

[3] Gori M, PUCCI A. Itemrank: a random-walk based scoring algorithm for recommender engines[C]// IJCAI 2007, Proceedings of the 20th International Joint Conference on Artificial Intelligence, January 6-12, 2007, Hyderabad, India. USA: Morgan Kaufmann Publishers Incorporated, 2007: 778-781.

[4] Mobasher B, BURKE R, WILLIAMS C, et al. Analysis and detection of segment-focused attacks against collaborative recommendation [C]// Advances in Web Mining and Web Usage Analysis, 7th International Workshop on Knowledge Discovery on the Web, WebKDD 2005, August 21, 2005, Chicago, IL, USA. USA: Springer, 2006: 96-118.

[5] Mobasher B, BURKE R, BHAUMIK R, et al. Toward trustworthy recommender systems: an analysis of attack models and algorithm robustness[J]. Journal of ACM Transactions on Internet Technology (TOIT), 2007, 7(4): 23.

[6] 张富国. 用户多兴趣下基于信任的协同过滤算法研究. 小型微型计算机系统[J]. 小型微型计算机系统, 2008, 29(8): 1415-1419.
ZHANG GUO-FU. Research on trust based collaborative filtering algorithm for user's multiple interests[J]. Journal of Chinese Computer Systems, 2008, 29(8): 1415-1419.

[7] MEHTA B, HOFMANN T, FANKHAUSER P. Lies and propaganda: detecting spam users in collaborative filtering [C]// Proceedings of the 12th international conference on Intelligent user interfaces, January28-31, 2007, Honolulu, HI, USA. New York: Association for Computing Machinery, 2007: 21-28.

[8] MEHTA B, HOFMANN T, NEJDL W. Robust collaborative filtering [C]//Proceedings of the 2007 ACM conference on Recommender systems in ACM Conference On Recommender Systems, October19-20, 2007, Minneapolis, MN, USA. New York: Association for Computing Machinery, 2007: 49-56.

[9] MASSA P, AVESANI P. Trust-aware collaborative filtering for recommender systems[C]//On the Move to Meaningful Internet Systems 2004: CoopIS, DOA, and ODBASE, October25-29, 2004, Agia Napa, Cyprus. Berlin: Springer-Verlag, 2004: 492-508.

[10] MASSA P, BHATTACHARJEE B. Using trust in recommender systems: an experimental analysis[C]// Trust Management: Second International Conference, March 29-April 1, Oxford, UK. [S. l.]: Springer, 2004: 221-235.

[11] LAM S K, RIEDL J. Shilling recommender systems for fun and profit [C]//13th international conference on World Wide Web, May 17-22, 2004, New York, NY, USA. New York: Association for Computing Machinery, 2004: 393-402.

[12] O'MAHONY M, HURLEY N, KUSHMERICK N, et al. Collaborative recommendation: a robustness analysis[J]. Journal of ACM Transactions on Internet Technology (TOIT), 2004, 4(4): 344-377.

[13] MOBASHER B, BURKE R, BHAUMIK R, et al. Effective attack models for shilling item-based collaborative filtering systems[C]// In Proceedings of the 2005 WebKDD Workshop, August21-24 2005, Chicago, Illinois, USA. [S. l.]: Citeseer, 2005: 13-23.

[14] BURKE R MOBASHER B, WILLIAMS C, et al. Classification features for attack detection in collaborative recommender systems[C]//Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining, August20-23, 2006, Philadelphia, PA, USA. New York: Association for Computing Machinery, 2006: 542-547.

[15] SARWAR B, KARYPIS G, KONSTAN J, et al. Item-based collaborative filtering recommendation algorithms[C]// Proceedings of the 10th international conference on World Wide Web, May1-5, 2001, Hongkong, China. New York: Association for Computing Machinery, 2001: 285-295.

[16] GAMBETTA D. Trust: Making and Breaking Cooperative Relations [M]. United Kingdom:

University of Oxford,2000: 213-237.

[17] 王宏宇.商务推荐系统的设计研究[D].安徽:中国科技大学,2007.

[18] O'DONOVAN J, SMYTH B. Trust in recommender systems[C]//In Proceedings of the 10th international conference on Intelligent user interfaces, January9-12, 2005, San Diego, CA, USA. New York: Association for Computing Machinery, 2005: 167-174.

[19] 高滢,齐红,刘亚波,等. 基于用户等级的协同过滤推荐算法[J]. 吉林大学学报:理学版, 2008, 46(3): 489-493.
GAO YING, QI HONG, LIU YA-BO, et al. A user grade-based collaborative filtering recommendation algorithm[J]. Journal of Jilin University: Science Edition, 2008, 46(3): 489-493.

[20] 郭艳红.推荐系统的协同过滤算法与应用研究[D].大连:大连理工大学,2008.

[21] ADOMAVICIUS G, TUZHILIN A. Toward the next generation of recommender systems: a survey of the state-of-the-art and possible extensions[J]. IEEE Transactions on Knowledge and Data Engineering, 2005, 7(6): 734-749.

[22] 谢明文.关于协方差、相关系数与相关性的关系[J].数理统计与管理,2004,23(3):33-36.
XIE MING-WEN. The relation of covariance, correlation coeffcient and correlation[J]. Application of Statistics and Management, 2004, 23(3): 33-36.

[23] LANGVILLE A N, MEYER C D. Deeper inside pagerank[J]. Internet Mathematics, 2004, 1(3): 335-380.

[24] HAVELIWALA T H. Efficient computation of Pagerank[R]. Stanford University: Stanford digital library technologies project, 1999.

[25] KAMVAR S D, HAVELIWALA T H, MANNING CD, et al. Extrapolation methods for accelerating PageRank computations[C]//The 12th International Conference on World Wide Web, May 20-24, 2003, Budapest, Hungary. New York: Association for Computing Machinery, 2003: 261-270.

[26] BRIN S, PAGE L. The anatomy of a large-scale hypertextual Web search engine[C]// the seventh international conference on World Wide Web, April14-18, 1998, Brisbane, Australia. The Netherlands: Elsevier Science Publishers, 1998: 107-117.

(编辑 王维朗)

(上接第 134 页)

[10] MANTIKTALA S. 精通开关电源设计[M]. 王志强,译.北京:人民邮电出版社,2008.

[11] 刘金琨.先进 PID 控制 MATLAB 仿真(第二版)[M].北京:电子工业出版社,2004.

[12] 刘凤君.现代逆变技术及应用[M].北京:电子工业出版社, 2006.

[13] 马建林.数字式乳腺 X 射线机电控系统设计[D].长沙:湖南大学, 2009.

[14] 张冬梅, 杨苹,刘军,等. 基于 UC3875 的双闭环控制稳流型开关电源[J]. 微计算机信息, 2009, 25(19): 127-128.
ZHANG DONG-MEI, YANG PING, LIU JUN, et al. Double closed-loop controlled stabilized current switching power supply based on UC3875[J]. Microcomputer Information, 2009, 25(19): 127-128.

[15] 王聪,徐刚. 辅助二极管谐振极逆变器的分析、设计与实现[J]. 电工技术学报, 1998, 13(3): 40-45.
WANG CONG, XU GANG. The analysis, design and implementation of ADRPI[J]. Journal of electrical technology, 1998, 13(3): 40-45.

(编辑 郑 洁)