电子商务推荐攻击研究*)

余 力 董斯维 郭 斌
(中国人民大学信息学院 北京 100872)

摘 要 个性化推荐是实现客户关系管理的重要手段和技术。协同过滤作为最核心、最典型的个性化推荐技术,被广泛应用于电子商务,但其推荐结果对用户偏好信息敏感,使得推荐系统易受到人为攻击,电子商务推荐安全成为个性化推荐能否成功应用的关键。作者先简要介绍了电子商务个性化推荐的基本概念,然后系统阐述了推荐攻击的概念、特征、攻击成本及攻击效率,并详细比较了各种攻击模型,以及各种攻击模型对不同推荐模型的稳定性和健壮性的影响,分析比较了各种攻击检测模型。最后总结评述了电子商务推荐安全的研究现状,并提出了未来研究的挑战。

关键词 协同过滤,推荐系统,个性化推荐,攻击模型,电子商务安全

Research on Attack on Personalized Recommendations in E-commerce

YU Li DONG Si-Wei GUO Bin
(Information School, Renmin University of China, Beijing 100872)

Abstract Personalized recommendation is important method and technology to carry out CRM. Collaborative filtering which is used widely is vital central technology of personalized recommendation, but the recommended result is so sensitive to user perfect information that the recommendcd system has significant vulnerabilitics. E-business recommended secure is the key of whether the personalized recommendation can success or not, Concept of E-business recommended system is bricfly intruduced. Concepts, character, attack cost and attack effectiveness of recommended attack are elaborated, then alanyzing and comparing all kinds of attack model, as following the attack defective model. Finally, the authors make conclusion and present research challenge in the future.

Keywords Collaborative filtering, Rccommended system, Personalized rccommendation, Attack model, Secure in E-commercc

1 引言

电子商务的发展模式对企业服务提出了许多新要求,其中如何提供一对一的客户关怀成为企业成功与否的决定性因素之一。推荐系统(Recommender Systems)根据用户的偏好,推荐符合其偏好的商品,也称个性化推荐系统(Personalized Recommender Systems)[1~3]。

但在竞争环境下,有的竞争者为获取更大市场占有率,人为给竞争对手的推荐系统制造大量假数据,使其推荐结果符合自己的商业利益,影响推荐系统的准确性。所以,如何提高推荐系统的抵御假能力,检测并发现假数据就显得尤为重要。电子商务推荐安全研究成为电子商务推荐系统成功应用的关键[2]。

本文第2节简要介绍了电子商务个性化推荐;第3节系统阐述了推荐攻击的概念、特征、攻击成本及攻击效率;第4节分析比较了各种攻击模型及其对不同推荐模型的稳定性和健壮性的影响;第5节比较了各种攻击检测模型。最后,总结评述了电子商务推荐安全的研究现状,并提出了未来研究的挑战。

2 电子商务个性化推荐

2.1 电子商务推荐系统

电子商务推荐系统利用电子商务网站向客户提供商品信息和建议,帮助用户决定应该购买什么产品,模拟销售人员帮助客户完成购买过程[1]。其最大的优点在于能根据用户偏好主动为用户推荐符合其个性化需要的商品[3]。电子商务推荐系统包括输入、个性化推荐、输出3个组成模块,其中个性化推荐是系统的核心部分,决定系统性能的优劣[4]。

2.2 个性化推荐技术

个性化推荐技术是电子商务推荐系统最关键、最核心的组成部件。目前主要的推荐技术有协同过滤推荐(Collaborative Filtering Recommendation)、基于内容的推荐(Content-based Recommendation)[5,6]、基于知识的推荐(Knowledge-based Recommendation)[7,8]、基于效用的推荐(Utility-based Recommendation)、关联推荐(Association Rule-based Recommendation)和基于用户统计信息的推荐(Demographic-based Recommendation)[5]等。协同过滤是目前研究和应用最为广泛的个性推荐技术,也是真正意义上的个性化推荐技术[2],但其推荐结果对用户偏好信息资料非常灵敏。在市场经济环境下,出于商务竞争目的,某企业会人为向推荐系统注入大量假用户,以使推荐结果朝自己有利的方向发展。本文重点研究基于协同过滤的推荐安全问题。

协同过滤推荐一般主要分为三类:基于用户的协同过滤推荐[9,10]、基于项目的协同过滤推荐[11]和基于模型的协同过滤推荐[12,13]。

*)信息管理与信息经济学教育部重点实验室开放基金资助(F0607-31)。余 力 讲师,博士,研究方向:个性化推荐、电子商务、商务智能;董斯维 本科生,研究方向:电子商务、管理信息系统;郭 斌 本科生,研究方向:信息管理与信息系统。

2.2.1 基于用户的协同过滤(User-based Collaborative Filtering,UB_CF)

基于用户的协同过滤是最典型的协同过滤推荐算法,如图1所示。它根据用户的兴趣资料寻找具有相似兴趣偏好的邻居用户,综合邻居用户兴趣资料来预测当前用户的偏好,以此为基础为用户作出个性化推荐[9]。

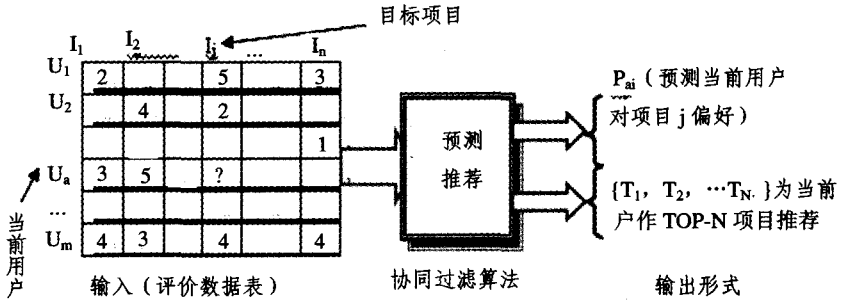

图1 基于用户的协同过滤推荐

用户间的相似性可采用Pearson相关系数、向量余弦夹角等计算方法来预测当前用户 u 对目标产品 i 的偏爱程度,可采用如下计算公式:

$$p_{u,i}=\bar{r}_u+\frac{\sum_{v\in V} Sim_{u,v}*(r_{u,v}-\bar{r}_v)}{\sum_{v\in V}|Sim_{u,v}|} \quad (1)$$

2.2.2 基于项目的协同过滤(Item-based Collaborative Filtering,IB_CF)

基于项目的协同过滤是通过寻找相似的商品,并基于其他用户对相似商品的评价信息来预测当前用户对某商品的偏好程度[9]。由于项目间相似度可以离线(Off-line)计算,因此基于项目的协同过滤的运算性能更好,但运算精确度更依赖于数据规模[12]。

2.2.3 基于模型的协同过滤推荐(Model-based Collaborative Filtering,MB_CF)

基于模型的协同过滤推荐,先用历史数据得到一个模型,再用此模型进行预测[11]。常用的有k-Means Clustering算法和PLSA(Probabilistic Latent Semantic Analysis)[13],前者通过聚类算法到具有相似偏好的用户群,后者是通过变换用户评价矩阵空间,抽取具有潜在意义的偏好向量。

3 推荐攻击

3.1 攻击的概念

攻击(Attack)指攻击者通过向推荐系统注入虚假用户,以使系统的推荐结果产生偏差[14]。每个攻击由多个假用户资料组成。一个攻击用户资料(User Profile,简写为UP)通常用一个 m 维向量表示,即

$$UP=\{r_1,r_2,r_3,\cdots,r_m\} \quad (2)$$

其中 m 为系统中商品的总数量。

记 I 为推荐系统中商品集,根据不同攻击模型的特点,I 由 i_t,I_S,I_F 和 I_Φ4部分组成,即

$$I=i_t\cup I_S\cup I_F\cup I_\Phi \quad (3)$$

其中 i_t 是攻击目标商品,I_S 是被用于确定目标用户提高攻击效率的商品集,I_F 是需指定评价值的商品集,I_Φ 是未赋予评价值的商品集。不同攻击模型的区别就体现在 I_S,I_F 和 I_Φ 及其评价值的设定。攻击资料的通用形式被描述为如图2。

i_1^s	…	i_k^s	i_1^f	…	i_l^f	i_1^φ	…	0	i_t
$\delta(i_1^s)$	…	$\delta(i_k^s)$	$\sigma(i_1^f)$	…	$\sigma(i_l^f)$	null	null	null	$r(i_t)$

图2 通用攻击模型[15]

一个攻击由多个攻击用户资料组成,即

$$Attack=\{UP_1,UP_2,\cdots,UP_{n-1},UP_n\} \quad (4)$$

其中 n 为注入的攻击用户数量。

3.2 攻击成本

攻击成本反映攻击者实施攻击的难易程度及投入量,包括知识成本(Knowledge Cost)和执行成本(Execution Cost)[14,15]。前者指收集被攻击系统的信息及用户信息时所付出的努力,后者指为了进行攻击需向系统中注入的攻击用户资料数量与系统数据库中现有用户资料数量的比值——攻击规模(Attack Size)、每个攻击用户资料中 $I-I_\Phi$ 所占的比重——填充规模(Filler Size)。

3.3 攻击效率

攻击效率一般采用平均预测增量和命中率两个指标来度量[11,13,15]。

3.3.1 平均预测增量(Average Prediction Shift)

预测增量描述系统在受攻击前后对同一商品给出的预测的变化值。平均预测增量[14,16]是对预测增量在用户集和商品集上进行加权平均。平均预测增量越大,表明系统易受攻击,或者表明攻击越有效;反之,表明系统越稳定,攻击效果越差。但高的预测增量并不表明某商品 i 一定会被系统推荐,还要看其它商品预测增量的大小。因此,国外学者又引入了一个新的衡量标准:命中率[15]。

3.3.2 命中率(Hit Ratio)

命中率[14,16]表示的是目标商品进入系统前 N 个推荐的概率。记 R_u 表示系统向用户 u 推荐的前 N 个商品的集合,$H_{ui}=1$ 表示 $i\in R_u$,否则 $H_{ui}=0$,对于所有用户商品 i 的平均hit表示为

$$\text{Hit Ratio}_i=\sum_{u\in U}H_{ui}/|U| \quad (5)$$

相似地,对于所有商品的命中率表示为

$$\text{Hit Ratio}_i=\sum_{i\in I}\text{HitRatio}_i/|I| \quad (6)$$

相比较而言,命中率比平均预测增量更能从直观上反映攻击效果。

4 攻击模型

如前所述，不同攻击模型的区别主要反映攻击用户资料。根据注入假用户资料组成的不同，攻击模型主要有样本攻击(Sampling Attack)、随机攻击(Random Attack)、平均攻击(Average Attack)、倾向攻击(Bandwagon attack)、最喜爱商品攻击(favorite item attack)、分块攻击(segmented attack)和群攻击(group attack)五类。

4.1 主要攻击模型

4.1.1 样本攻击

样本攻击[18~20]又称作完备知识攻击(Perfect Knowledge Attack)，即全部的攻击资料都取自于真实数据库中的用户资料。样本攻击注入的假用户与目标用户的相似度最大，攻击准确性高，但攻击成本也是最大的。在现实中，由于攻击者难以准确知道目标用户的偏好资料，因此样本攻击几乎是不可能实现的。

4.1.2 随机攻击

随机攻击[19]就是攻击者确定攻击目标后，选取一定填充规模的用户资料，使 I_F 中所有商品的评价值在以所有用户对所有商品的平均评价值为中心的某个很小的范围内随机选取。攻击用户资料如图3所示。由于很多系统中所有用户对所有商品的平均评价值是公开的，攻击者能够取得这些信息，因此随机攻击的知识成本是最小的，现实中是可行的，但攻击效率不够高[16,18]。

$i_1^{I_F}$	...	$i_l^{I_F}$	$i_1^{\varnothing}$	...	$i_v^{\varnothing}$	i_t
$\sigma(i_1^{I_F})$	...	$\sigma(i_l^{I_F})$	null	null	null	$r_{\max}$

图3 随机攻击模型

4.1.3 平均攻击

平均攻击[20,21]与随机攻击基本相同，主要区别在于攻击者是如何对 I_F 商品集中商品 i 指定评价值的。平均攻击中，评价值是在以所有用户对商品 i 的平均评价值为中心的某个很小的范围内随机选取的，因此较随机攻击而言，具有较高的效率。但知识成本较高，现实中实现难度较大。

4.1.4 倾向攻击

倾向攻击[21]是基于随机攻击的一种攻击，二者的区别在于其含有 I_S，为在市场中受关注度较高的商品。攻击资料如图4所示。攻击者指定这些高关注度商品的评价值，是因为推荐系统中的用户一般也会对这些商品给出与市场中相似的评价值(例如销售最好的书籍)，所以这种攻击资料更有可能与大量用户有较高的相似度。由于这些商品是容易获知的，其知识成本是比较低的。

$i_1^{I_S}$	...	$i_k^{I_S}$	$i_1^{I_F}$	...	$i_l^{I_F}$	$i_1^{\varnothing}$	...	$i_v^{\varnothing}$	i_t
$r_{\max}$	...	$r_{\max}$	$\sigma(i_1^{I_F})$	...	$\sigma(i_l^{I_F})$	null	null	null	$r_{\max}$

图4 倾向攻击模型

4.1.5 最喜爱商品攻击

最喜爱商品攻击[21]关注的是某个用户 u 的偏爱，而不是商品。这种攻击不能影响到整个系统，而是针对某一特定用户进行的。攻击者需挑选出用户 u 偏爱的商品集，并将其评价值指定为 $r_{\max}$，其他则用随机攻击或平均攻击。显然，攻击者需对用户 u 的知识有准确且具体的了解，因此这种攻击对知识成本有很高的要求。

4.1.6 分块攻击

分块攻击[19,20]是基于最喜爱商品攻击的一种攻击。由于知道某个用户的具体偏好几乎是不可能的，而发现某类有共同偏爱的用户是切实可行的。例如一位科幻小说的作者，他更容易向 Harry Potter 的书迷推荐他的新书。攻击者只需知道目标用户群所偏爱的某类商品，并将这类商品的评价值设为最大，就可进行攻击。分块攻击资料如图5所示。

$i_1^{I_S}$	...	$i_k^{I_S}$	$i_1^{I_F}$	...	$i_l^{I_F}$	$i_1^{\varnothing}$	...	$i_v^{\varnothing}$	i_t
$r_{\max}$	...	$r_{\max}$	$r_{\min}$	...	$r_{\min}$	null	null	null	$r_{\max}$

图5 分块攻击模型

4.1.7 群攻击

群攻击[21]的攻击者不同于传统的攻击者，因为他们设计一些与攻击无关的评价值来隐藏他们的攻击目的。在每个群攻击资料中，攻击目标会与无关的商品掺杂在一起，产生不明确的攻击目标。但当攻击达到一定数量，形成群攻击后，攻击目标就会凸现出来。

4.2 攻击模型比较

不同攻击模型的攻击成本和攻击效率不同，各有优劣，如表1。攻击成本主要反映攻击者实施攻击的难易程度及投入量，攻击评价主要体现了攻击者在实施攻击后的回报量。由于同一攻击模型对不同协同过滤的效果不一样，这里作者对3种协同过滤(UB_CF，IB_CF，MB_CF)分别进行比较。

通过对攻击模型的比较，可以得到以下结论：

1)UB_CF 的稳定性与健壮性最差，各种攻击都会对系统产生较大的影响。

表1 攻击模型比较

攻击模型	特征	攻击成本		攻击评价			
		知识成本	执行成本	攻击范围	UB_CF	IB_CF	MB_CF
样本攻击	攻击资料从数据库中直接获得	高	低	一个用户	很高	低	低
随机攻击	填充评价值取所有商品平均评价值	低	较高	全体用户	一般	较低	低
平均攻击	填充评价值取该商品平均评价值	一般	较低	全体用户	较高	较低	低
倾向攻击	挑选出大众比较关注的商品集	较低	一般	全体用户	较高	较低	低
最喜爱商品攻击	针对一个用户进行攻击	较高	较低	一个用户	很高	较低	低
分块攻击	按不同的偏好对用户进行分类	较低	较低	部分用户	高	高	较高
群攻击	多个攻击资料配合攻击才能达到攻击目的	较低	高	全体用户	高	高	暂无研究

2)IB_CF 和 MB_CF 都对基本攻击具有一定的防御能力，前者对部分攻击的防御能力较差，后者有一定的防御能力。

3)执行成本与攻击效率不是完全的正比关系。

5 攻击检测模型

5.1 攻击检测模型概念

攻击检测模型[20]是通过对用户评价数据库进行挖掘的算法模型，用来分辨攻击用户资料与真实用户资料，并对前者作出反应。使用检测模型的前提是攻击资料与真实资料有不同。两者的不同可以表现在很多方面，例如前者的评价分可能与系统的平均值有很大的偏差；前者中的评价数量不同于后者；前者间的相似度应比后者间的大得多。

5.2 主要攻击检测模型

目前主要攻击检测模型有基础监测模型(Basic Detection)、Chirita 模型和部分检测模型(Segment Model Detection)3 类。

5.2.1 基础检测模型

基础检测模型[21]是通过比较每个用户的预测变化值、用户评价值背离程度、与其他用户相适度、邻居用户相似程度和背离平均度等指标来实现的。

1)预测变化值(Number of Prediction-Differences，NPD)：表示一个用户不参与系统的推荐算法后系统预测值产生的变化。

2)用户评价值背离程度(Standard Deviation in User's Ratings)：表示一个用户对一个商品的评价值与其对其他商品平均评价值的背离程度。

3)与其他用户相适度(Degree of Agreement with Other Users)：一个用户对商品的评价值与该商品平均评价值的背离程度的加权平均。

4)邻居用户相似程度(Degree of Similarity with Top Neighbors，DegSim)[13]：通过计算目标用户 u 对于 K 个邻居 v 的平均相似度来判别用户的可信度。

5)背离平均度(Rating Deviation from Mean Agreement，RDMA)：是一个比较重要的评价标准，在后面的检测模型中都用到了它。它表示用户 u 对商品的评价与其它用户之间的背离程度，其计算公式如下：

$$RDMA_u=\frac{\sum_{i=0}^{u}\frac{|r_{u,i}-Avg_i|}{NR_i}}{N_u} \tag{6}$$

N_u 表示对用户 u 的资料中做出评价的数量。$r_{u,i}$ 表示用户 u 的资料中用户对商品 i 做出的评价分，NR_i 表示商品 i 得到的所有评价数量。

根据上述 5 个指标值，如果某个用户的预测变化值、与其他用户相适度、邻居用户相似程度、背离平均度值过高，且用户评价值背离程度过低，则认定是攻击者。

5.2.2 Chirita 模型

为克服基础检测模型计算量过大的缺点，2004 年 Chirita 等人在其基础上提出了一种新的检测模型及应用方案—Chirita 模型[22]。该模型只需计算两个值：RDMA 和 PA(Probability of Attack)。攻击可能度(PA)是在 RDMA 基础上得出的，它定量地表示了一个注入资料是攻击资料的可能性。当用户 u 的 RDMA 小于平均值时取 0，大于平均值时取以 $RDMA_u$ 为自变量的一个函数值。通过使用 PA 对 KNN 算法中对相似值(Sim)的算法进行修正，在基于用户的过滤算法中，其方法如下：

$$Sim_{u,v}=Sim_{u,v}*(1-PA_u) \tag{7}$$

但是，这种模型在稍后的研究中被证明攻击在填充规模较小时的检测效果不好，且对分块攻击的监测效果不好[22]。

5.2.3 分块检测模型

因为 Chirita 模型本身存在缺陷，Burke 等人在其基础上提出了分块检测模型[16]，它是通过对两个参数——注入平均目标差异 FMTD(Filler Mean Target Difference)和相符权重度 WDA(Weighted Degree of Agreement)——的比较实现的，其具体计算如下：

$$FMTD_u=\left|\left(\frac{\sum_{i\in P_{target}} r_{u,i}}{P_{target}}\right)-\left(\frac{\sum_{k\in P_{filler}} r_{u,k}}{P_{filler}}\right)\right| \tag{8}$$

P_{target} 包含了用户 u 做出最高评价的所有商品，P_{filler} 即 I_F 的数量。WDA 即 RDMA 的分子。如果两个参数都分别大于各自的临界值，则用户 u 即是攻击用户。

5.3 攻击检测模型比较

综上所述，各种攻击检测模型比较如表 2 所示。

表 2 攻击检测模型比较

攻击检测模型	优点	缺点
基础检测模型	综合多个指标检测；形象直观	检测较复杂
Chirita 模型	攻击用户定量化	对低填充规模的攻击检测效果不好
分块检测模型	复杂度最低；对系统准确性影响最小	对高攻击规模的攻击检测效果不好

通过对攻击检测模型的比较，有以下主要结论：

1)三种攻击检测模型对各种攻击模型都有一定的监测效率，起到了作用。

2)部分检测模型对部分攻击的检测效果很好，且不受填充规模的限制。

3)检测模型都会将一些真实用户误认为是攻击者，影响了系统的准确度。

4)算法复杂度过高，需要遍历数据库中每一个用户进行计算，在现实中不太可行。

总结与展望 电子商务个性化推荐是一种重要的客户关系管理手段与方法，成为众多学者研究的重点。过去十多年(上世纪 90 年代中期至本世纪初)，大多数学者研究的重点是如何得到一种高性能、准确的推荐算法。近年来(本世纪初)，更多学者注意到电子商务推荐系统应用的实际背景是一种市场经济下的商业竞争环境，电子商务推荐安全问题成为各学者关注的焦点，成为电子商务推荐一个新兴的领域，在攻击模型、攻击检测模型方法等方面取得了一定的研究成果。但目前的研究成果离实际电子商务推荐安全问题的解决还相差甚远，必须加大对电子商务推荐安全理论问题的研究，才能真正使电子商务推荐系统得到广泛应用，提高电子商务服务质量。未来应对以下几方面问题进行重点研究：

(1)减少攻击成本，提高攻击模型的可行性。

目前已有各种攻击模型，但不同攻击的应用条件、攻击成本不一样，大多数攻击模型的前提假设太强，在现实中根本不可行，只是一种理论模型。有些攻击模型虽然条件较弱，但攻击效率差，难以发挥作用。今后应对攻击模型做进一步基础研究，设计一种既实际可行(攻击成本较低)又具有一定效率的攻击模型。尤其是注意攻击模型前提假设的可行性。

(2)提高攻击检测模型研究的可行性和普遍性。

目前关于攻击检测模型的研究更多致力于发现在一定前提条件下，推荐系统中是否有假用户注入。研究存在两方面

问题:一是条件较强,很多偏好信息无法获取;其次,大多数攻击检测模型只能检测对某一种攻击模型所产生的攻击,但实际中企业不知道其竞争对手将采用何种攻击模型,所以今后必须提高攻击检测模型的普遍适应性,使之能检测出各种类型的攻击。

(3)综合 Web 挖掘等其它方法,提高攻击检测的准确性与成功率。

目前所有推荐安全研究所涉及的用户资料都是基于用户评价信息。在实际中,可采用 Web 挖掘方法,通过结合对访问路径分析,获取用户的偏好模式,同时通过对所有用户 Web 日志分析,发现假用户,提高攻击检测的准确性与成功率。

(4)切实以推荐模型的稳定性和健壮性为研究目标,提高推荐系统的准确性。

攻击模型和攻击检测模型是电子商务推荐安全研究的基础,电子商务推荐安全研究要求不但要能检测假用户,还要根据检测到的假用户以及假用户所用的攻击模型,提出推荐模型的改进办法,真正在存在攻击的情况下仍能做出较为准确的推荐,提高推荐模型的稳定性和健壮性。

参 考 文 献

1 Resnick, Varian. Recommender systems [J]. Communications of the ACM, 1997, 40 (3): 56～58

2 Schafer J B, Konstan J, Riedl J. Recommender Systems in E-Commerce [C]. In: EC '99 Proceedings of the First ACM Conference on Electronic Commerce, Denver, CO, 1999. 158～166

3 余力,刘鲁. 电子商务个性化推荐研究综述. 计算机集成制造系统,2004,10(10):1306～1313

4 Herlocker J, Konstan J, Tervin L G, et al. Evaluating collaborative filtering recommender systems. ACM Transactions on Information Systems, 2004, 22(1): 5～53

5 赵亮,胡乃静,张守志. 个性化推荐算法设计[J]. 计算机研究与发展,2002,39(8):986～991

6 Ben J, Konstan J A, John R. E - commerce recommendation applications [R]. University of Minnesota, 2001

7 Billsus D, Pazzani M. Learning Collaborative Information Filters [C]. In: Proceedings of the International Conference on Machine Learning (Madison WI, July 1998), Morgan Kaufmann Publishers

8 余力,刘鲁,罗掌华. 我国电子商务推荐策略的比较分析. 系统工程理论与实践,2004-08

9 Robin B. Hybrid Recommender Systems: Survey and Experiments [R]. Department of Information Systems and Decision Sciences, California State University, Fullerton

10 Ben J, Konstan J A, John R. E-Commerce Recommendation Applications [R]. University of Minnesota, 2001

11 Burke R, Mobasher B, Zabicki R, et al. Identifying attack models for secure recommendation. In: Beyond Personalization: A Workshop on the Next Generation of Recommender Systems, San Diego, California, 2005

12 Yu Li, Liu Lu, Li Xuefeng. A Hybrid Collaborative Filtering Method for Multiple-interests and Multiple-content Recommendation in E-Commerce. International Journal of Expert System with Application, Jan. 2005, 28: 67～77

13 Burke R, Mobasher B, Zabicki R, et al. Analysis and Detection of Segment-Focused Attacks Against Collaborative Recommendation

14 Burke R, Mobasher B, Bhaumik R. Limited knowledge shilling attacks in collaborative filtering systems. In: Proceedings of the 3rd IJCAI Workshop in Intelligent Techniques for Personalization, Edinburgh, Scotland, 2005

15 Mobasher B, Burke R, Bhaumik R, et al. Effective attack models for shilling item-based collaborative filtering systems. In: Proceedings of the 2005 WebKDDWorkshop, held in conjuction with ACM SIGKDD 2005, Chicago, Illinois, 2005

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

17 Lam S, Reidl J. Shilling recommender systems for fun and profit. In: Proceedings of the 13th International WWW Conference, New York, 2004

18 Burke R, Mobasher B, Zabicki R, et al. Segment-based Injection Attacks Against Collaborative Filtering Recommender Systems-icdm05

19 Resnick P, Iacovou N, Suchak M, et al. Grouplens: an open architecture for collaborative filtering of netnews. In: CSCW '94: Proceedings of the 1994 ACM conference on Computer supported cooperative work, ACM Press, 1994. 175～186

20 Burke R, Mobasher B, Zabicki R, et al. Detecting Profile Injection Attacks in Collaborative Recommender Systems-cec06

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

22 Chirita P A, Nejdl W Zamfir C. Preventing shilling attacks in online recommender systems. In: WIDM '05: Proceedings of the 7th annual ACM international workshop on Web information and data management, New York, NY, USA, ACM Press, 2005. 67～74

(上接第 82 页)

由于本地安全策略、信任度计算策略、反馈评估策略等均可由本地用户根据实际情况具体制定,因此该模型具有灵活、通用、自动学习的特点。

结束语 本文设计了一个含有信任度的反馈式信任管理模型,该模型在对实体进行信任评估时,综合考虑了感性信任和理性信任两方面的因素,同时该模型还具有自主学习反馈的功能,能够根据访问者在访问过程中的不同表现做出不同的反应,将每次访问的经验反馈至系统,使系统在学习中不断得到修正和完善。但本文所提出的模型只是一个初步的框架,有许多工作尚需进一步深入研究,例如如何合理有效地制定本地安全策略,如何对本次访问结果进行综合评估,如何根据不同类型的访问来确定评估发生的时间等都需要细化和完善。

参 考 文 献

1 Blaze M, Feigenbaum J, Lacy J. Decentralized Trust Management. In: Proc. of the 17th Symposium on Security and Privacy, pages164-173. IEEE Computer Society Press, Los Alamitos, 1996. 164～173

2 Blaze M, Feigenbaum J, Strauss M. Compliance-checking in the PolicyMaker trust management system. In: Proceedings of Second International Conference on Financial Cryptography (FC'98), volume 1465 of Lecture Notes in Computer Science, Springer, 1998. 254～274

3 Blaze M, Feigenbaum J, Ioannidis J, Keromytis A. The KeyNote Trust-Management System. Version 2. Internet RFC 2704, September 1999

4 Chu Y, Feigenbaum J, LaMacchia B, Resnick P, Strauss M. REFEREE: Trust management for web applications. World Wide Web Journal, 1997(2): 706～734

5 徐锋,曹春,等. 一个软件服务协同中的信任管理框架设计. 计算机科学,2003,30(6)