软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2014,25(11):2652−2665 [doi: 10.13328/j.cnki.jos.004550]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于仿生模式识别的未知推荐攻击检测*

周全强[1,2], 张付志[1,2], 刘文远[1,2]

[1](燕山大学 信息科学与工程学院,河北 秦皇岛 066004)

[2](河北省计算机虚拟技术与系统集成重点实验室(燕山大学),河北 秦皇岛 066004)

通讯作者: 张付志, E-mail: xjzfz@ysu.edu.cn

摘 要: 针对已有检测方法不能有效地检测未知推荐攻击的问题,提出了一种基于仿生模式识别(bionic pattern recognition)的检测方法.首先,依据项目流行度划分项目到不同的窗口,把用户对窗口内项目的评分视为随机事件发生.在此基础上,利用信息熵(information entropy)提取评分分布特征作为检测推荐攻击的通用特征.然后,在特征空间中,利用仿生模式识别技术覆盖真实概貌样本,将覆盖范围外的测试数据判为推荐攻击.在 MovieLens 数据集上进行实验,结果表明,该方法在检测未知推荐攻击时具有较高的命中率和较低的误报率.

关键词: 协同推荐;推荐攻击;攻击检测;信息熵;仿生模式识别

中图法分类号: TP309

中文引用格式: 周全强,张付志,刘文远.基于仿生模式识别的未知推荐攻击检测.软件学报,2014,25(11):2652−2665. http://www.jos.org.cn/1000-9825/4550.htm

英文引用格式: Zhou QQ, Zhang FZ, Liu WY. Detecting unknown recommendation attacks based on bionic pattern recognition. Ruan Jian Xue Bao/Journal of Software, 2014,25(11):2652−2665 (in Chinese). http://www.jos.org.cn/1000-9825/4550.htm

Detecting Unknown Recommendation Attacks Based on Bionic Pattern Recognition

ZHOU Quan-Qiang[1,2], ZHANG Fu-Zhi[1,2], LIU Wen-Yuan[1,2]

[1](School of Information Science and Engineering, Yanshan University, Qinhuangdao 066004, China)

[2](Key Laboratory for Computer Virtual Technology and System Integration of Hebei Province (Yanshan University), Qinhuangdao 066004, China)

Corresponding author: ZHANG Fu-Zhi, E-mail: xjzfz@ysu.edu.cn

Abstract: The existing detection approaches can not detect unknown recommendation attacks effectively. Aiming at this problem, an approach based on bionic pattern recognition is proposed. Firstly, items are partitioned into different windows according to their popularity. The ratings given by users for the items in the windows are regarded as the occurrences of random events. Further, information entropy is used to extract features of rating distribution as genuine features for the detection of recommendation attacks. In addition, the technique of bionic pattern recognition is used to cover the samples of genuine profiles in the feature space. Test data outside the coverage are judged as recommendation attacks. The experimental results on the MovieLens dataset show that the proposed approach has high hit ratio and low false alarm ratio when detecting unknown recommendation attacks.

Key words: collaborative recommendation; recommendation attack; attack detection; information entropy; bionic pattern recognition

协同过滤推荐系统[1]能够依据建立的用户概貌(user profiles)过滤出满足用户兴趣的信息,并主动推荐给用户.它为解决互联网上的信息过载问题提供了一条有效途径,已成为目前许多电子商务站点的重要组成部分.

然而,由于协同过滤推荐系统自身所具有的开放性,恶意用户出于商业竞争等目的,人为地向系统注入大量

* 基金项目: 国家自然科学基金(61379116, 61272466); 河北省自然科学基金(F2011203219, F2013203124); 河北省高等学校科学技术研究重点项目(ZH2012028)

收稿时间: 2013-05-15; 修改时间: 2013-08-21; 定稿时间: 2013-12-05

虚假的用户概貌,企图使系统产生对他们有利的推荐结果.这种向协同推荐系统注入虚假用户概貌的行为称为托攻击(shilling attacks)[2]、概貌注入攻击(profile injection attacks)[3]或推荐攻击(recommendation attacks)[4].为了区分推荐系统中的真实概貌(genuine profiles),通常把这种虚假的用户概貌称为攻击概貌(attack profiles).根据不同的攻击目的,推荐攻击可分为推攻击(push attacks)和核攻击(nuke attacks)[4],分别用于提高和降低目标项目的推荐频率.攻击模型(attack model)[5]是攻击者根据推荐系统的评分数据库、项目及用户等方面的知识建立攻击概貌所使用的策略.目前常见的攻击模型有随机攻击(random attack)、均值攻击(average attack)、流行攻击(bandwagon attack)和 AoP 攻击等[2,6,7].

近年来,关于推荐攻击检测的研究已成为推荐系统中一个新的研究热点.已有的检测方法主要包括无监督方法、有监督方法以及半监督方法.这些方法试图通过检测攻击概貌来消除推荐攻击对推荐系统产生的影响.

无监督方法不需要训练样本,但通常需要满足一定的先验知识.Chirita 等人[8]首先提出了几个统计指标检测高密度填充规模的攻击概貌.Su 等人[9]根据组攻击概貌表现出的群体特征提出一种相似度传播算法,对组攻击概貌进行检测.李聪等人[10]通过定量度量攻击概貌的群体效应构建出遗传优化的目标函数,并在遗传优化的过程中融入贝叶斯推断思想,提出了一种无监督检测算法 IBIGDA.Lee 等人[11]基于多维尺度分析和聚类技术提出了一种混合两阶段的推荐攻击检测方法.Mehta 等人[12,13]认为攻击概貌对推荐系统贡献的信息较少,并利用主元分析技术对攻击概貌进行过滤,提出了一种可以有效检测多种攻击类型的 PCA-VarSelect 检测方法.

有监督方法需要训练样本,通过在特征空间中训练有监督的分类学习算法得到分类模型,对测试数据进行分类.Williams 等人[14,15]提取了 RDMA 等 6 种通用特征以及针对特定攻击模型的多种专有特征,并在此基础上训练 KNN,C4.5 和 SVM 对攻击概貌进行检测.基于 Williams 等人提出的特征,He 等人[16]提出了基于粗糙集的检测方法.Zhang 等人[17]提出了基于元学习的检测方法,利用集成学习技术有效提升了检测精度.伍之昂等人[18]利用特征选择算法为特定攻击类型选取有效特征,提升了针对特定攻击类型的检测效果.

在推荐攻击检测方面,采用半监督方法的主要是 Wu 等人[19,20]的工作.他们基于 Williams 等人提出的特征训练贝叶斯分类器进行检测,其半监督的特性主要表现在能够利用无标识的用户概貌提升已有分类器的分类性能.

已有检测方法在检测已知类型的推荐攻击时具备一定的检测效果,但是在面对不断出现的未知(或新)类型推荐攻击时表现不佳:

1) 有监督和半监督方法的检测性能主要依赖训练集中已有的攻击概貌样本,不能有效地检测未知类型的推荐攻击.
2) 无监督方法具备识别未知推荐攻击的潜力,但已有无监督方法只能识别部分类型的推荐攻击.这类方法有待深入探讨.

本文通过引入仿生模式识别技术,提出一种针对未知推荐攻击的检测方法.该方法属于半监督方法,其半监督特性表现在该方法的训练集中只包含真实概貌样本.本文的贡献主要包括以下几点:

1) 提出了一种特征提取算法,依据项目流行度划分项目到不同的窗口,把窗口内评分作为随机事件,引入信息熵(information entropy)[21]理论,从评分分布的角度提取检测推荐攻击的通用特征;
2) 提出了一种未知推荐攻击检测算法,引入仿生模式识别技术,在特征空间中对真实概貌样本进行合理覆盖,利用边界检测未知推荐攻击;
3) 在 MovieLens 数据集上进行了对比实验,验证了所提出的方法的有效性.

与已有方法相比,本文方法的特点在于:

1) 已有无监督方法通常需要一定的先验知识作为输入,本文方法用到的知识全部从训练数集中获得.
2) 已有无监督方法通常假定测试集中真实概貌多于攻击概貌,在实际中,这种假设并非绝对成立,本文方法对测试集中两类数据的比例没有限定.
3) 已有的 6 个通用特征试图从评分值的角度区分真实概貌和攻击概貌.本文方法从评分分布的角度提取通用特征,与评分值的大小无关.

4) 已有有监督和半监督方法要求训练集中同时包含真实概貌和攻击概貌样本,对攻击概貌的标注通常难以实现,尤其是对未知类型的推荐攻击.本文方法只用到真实概貌样本,对于实际系统而言,较容易实现对部分真实用户的标识.

1 相关理论

本节首先列出本文用到的符号及其含义,并给出相关定义,然后介绍信息熵的基本知识,最后介绍仿生模式识别的基本原理与实现方法.

1.1 符号含义与相关定义

若无其他说明,本文出现的符号及其含义见表 1.

Table 1 Symbols and meanings

表 1 符号及含义

符号	含义
D_g	集合 $D_g=\{U_1,U_2,\ldots,U_G\}$表示只包含真实概貌的训练集,其中,$G$ 表示真实概貌的数目
U	向量 $U=(r_{u,1},r_{u,2},\ldots,r_{u,\lvert I\rvert})$表示用户 u 的概貌
I	全部项目的集合
$\lvert I\rvert$	全部项目的数目
$r_{u,i}$	用户 u 对项目 i 的评分
$r_{u,i}\neq\perp$	用户 u 对项目 i 进行了评分
$r_{u,i}=\perp$	用户 u 没有对项目 i 进行评分
$\Gamma(r_{u,i})$	如果 $r_{u,i}\neq\perp$,判别函数$\Gamma(r_{u,i})=1$;如果 $r_{u,i}=\perp$,判别函数$\Gamma(r_{u,i})=0$
w	窗口
J	窗口数目
q	窗口规模

以下是本文用到的相关定义.

定义 1(项目流行度(popularity of items,简记为 PopI)). 项目 $i\in I$ 的流行度为 D_g 中的用户对项目 i 的评分数目,计算公式为

$$PopI_i=\sum_{u\in D_g}\Gamma(r_{u,i}) \tag{1}$$

定义 2(窗口(window,简记为 w)). 一个窗口 w 表示一组项目的集合,形式化定义为

$$w=\{i_1,i_2,\ldots,i_q\} \tag{2}$$

其中,q 表示窗口内项目的数目,称为窗口规模.窗口内任意项目 $i\in I$,定义窗口具有以下性质:

1) 有限性:窗口规模的大小是有限的,即 $q_j=\lceil |I|/J\rceil, j=1,2,\ldots,J-1, q_J=|I|-q_1\times(J-1)$.
2) 递变性:窗口内项目的流行度是递变的,递变规律为窗口的编号越小,则该窗口内的项目的流行度越高,形式化描述为 $PopI_{j,i}\geqslant PopI_{j+1,i}$,其中,$PopI_{j,i}$ 表示第 j 个窗口内的任意项目 i 的流行度,$PopI_{j+1,i}$ 表示第 $j+1$ 个窗口内的任意项目 i 的流行度,$j=1,2,\ldots,J-1$.
3) 等级性:窗口之间的流行等级不同,一个窗口标识为一个流行等级,窗口的编号越小,则该窗口的流行等级越高.
4) 等同性:同一窗口内所有项目的流行等级相同.

1.2 信息熵

在信息论中,信息熵[21]常用于度量随机变量的不确定性.不确定性越大,信息熵就越大.

设 $E=\{e_1,e_2,\ldots,e_L\}$表示由一系列随机事件 e 构成的随机变量,则 E 的信息熵计算公式为

$$H(E)=-\sum_{l=1}^{L}p_l\log_2(p_l) \tag{3}$$

其中,p_l 表示随机事件 e_l 发生的概率.

1.3 仿生模式识别

仿生模式识别(bionic pattern recognition)[22]的基本原理是:在特征空间中研究某类样本的分布状况而加以合理覆盖,从而“认识”某类样本.与传统模式识别方法把不同类样本在特征空间中的最佳划分作为目标不同,仿生模式识别方法是以一类样本在特征空间分布的最佳覆盖作为目标.

人工神经网络的一个神经元可以是多种多样、复杂的封闭超曲面,因此,人工神经网络是实现仿生模式识别非常合适的手段[23].文献[23]通过组合 BP 和 RBF 网络中的神经元,提出了一种构造型的神经网络(constructive neuron networks,简称 CNN)分类方法,利用所构造的神经网络实现对特征空间中样本的覆盖,从而达到分类的目的.

设在特征空间 R^n 中,训练样本集合为 $\{S_1,S_2,\ldots,S_m\}$,其中,第 i 个样本 $S_i=(s_{i,1},s_{i,2},\ldots,s_{i,n})$ 表示一个 n 维向量,m 为样本数目.$X=(x_1,x_2,\ldots,x_n)$ 为测试样本.该神经网络由 3 层神经元来实现.

- 第 1 层是 BP 网络的神经元模型:

$$Y_{1,i}=f_{1,i}\left(\sum_{j=1}^{n}\omega_{i,j}^{1}x_j-\beta_i\right) \tag{4}$$

其中,$f_{1,i}(t)=\begin{cases}0, & t<0\text{或}t>\|S_{i+1}-S_i\|\\ t, & \text{其他}\end{cases}$,$i$ 表示正整数且 $i<m$,$\omega_{i,j}^{1}=\dfrac{(s_{i+1,j}-s_{i,j})}{\|S_{i+1}-S_i\|}$,$\beta_i=\sum_{j=1}^{n}\dfrac{(s_{i+1,j}-s_{i,j})s_{i,j}}{\|S_{i+1}-S_i\|}$.

- 第 2 层是 RBF 网络的神经元模型:

$$Y_{2,i}=f_{2,i}\left(\sum_{j=1}^{n}(x_j-\omega_{i,j}^{2})^2-Y_{1,i}^{2}-\theta\right) \tag{5}$$

其中,$f_{2,i}(t)=\begin{cases}0, & t>0\\ 1, & t\leqslant 0\end{cases}$,$\omega_{i,j}^{2}=s_{i,j}$,$i$ 表示正整数且 $i\leqslant m$;$\theta=k^2$,k 为 n 维超球的半径.当与 $Y_{2,i}$ 相连的 $Y_{1,i}$ 不存在时,以 $Y_{1,i}=0$ 计算.

- 第 3 层是输出层,其数学模型为

$$Y_3=f_3\left(\sum_{i=1}^{m}Y_{2,i}\right) \tag{6}$$

其中,$f_3(t)=\begin{cases}1, & t>0\\ 0, & t\leqslant 0\end{cases}$.

当输入实例在样本覆盖范围内时,输出为 1;否则,输出为 0.

2 未知推荐攻击检测方法

本文提出的未知推荐攻击检测框架如图 1 所示.其中,训练集只包含真实概貌样本;边界由 CNN 网络利用特征提取后的训练集生成,用于检测未知推荐攻击.本节将从特征提取和检测算法两个方面详细介绍所提出的检测方法.

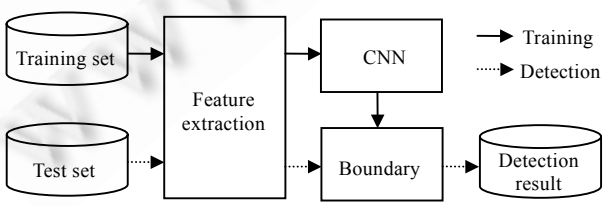

Fig.1 Detection framework for unknown recommendation attacks

图 1 未知推荐攻击检测框架

2.1 特征提取

攻击者和真实用户通常有着不同的兴趣偏好,这些兴趣偏好体现在用户概貌中用户对项目的评分,若能准确地描述这些评分的分布特征,即可将其用于区分攻击概貌和真实概貌.

为了准确地描述用户的评分分布特征,我们首先依据真实概貌度量项目的流行度;然后,按项目的流行度划分项目到不同的窗口(即划分出不同的流行等级);最后,利用信息熵提取用户的评分分布特征.

根据窗口的等级性,利用 J 个窗口可将 I 中的全部项目划分为 J 个不同的流行等级.根据窗口的有限性,通过划分流行等级 J 就可以确定窗口规模 q.等级 J 的取值范围不能太大(本文设置 J=10),因为流行等级 J 划分得越大,窗口规模 q 就越小,而评分数据通常是极端稀疏的,在这种情况下,很多用户在窗口内的评分数目为 0,使得这些窗口成为冗余窗口.

窗口能够较好地呈现出用户的评分分布特征.图 2 是一个真实概貌和一个攻击概貌在不同窗口上的评分分布,其中,两类概貌所包含的评分数目均为 40,真实概貌来自 MovieLens 数据集(http://www.grouplens.org/node/73),攻击概貌由随机攻击模型产生.

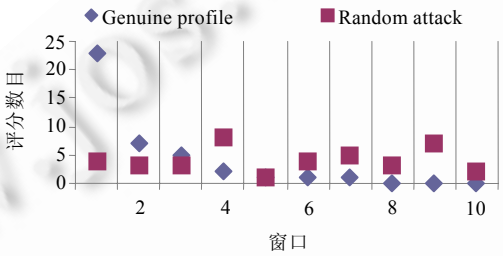

Fig.2 Distribution of user ratings on the windows

图 2 用户评分在窗口上的分布

从图 2 可以看出,真实概貌和攻击概貌有着不同的评分分布.真实概貌的评分主要分布在前 4 个窗口,攻击概貌的评分则呈现出随机分布的特征.我们在大量样本上的实验得到了与上述类似的实验结果.需要指出的是,随机攻击是一类相对简单的攻击模型,此处用该模型只是方便理解所提出的检测方法,在后面的实验部分,我们将考虑更多、更复杂的攻击模型.

为了准确地描述用户的评分分布特征,根据信息熵的基本知识,我们把用户对项目进行评分作为随机事件发生,根据窗口的等同性,把同一窗口内的评分看作是相同的随机事件,把用户在不同窗口内的评分数目作为随机变量.在此基础上计算信息熵,作为描述评分分布的特征,用于检测推荐攻击.

基于上述分析,对用户 u 而言,$r_{u,i}\neq\perp$表示发生了一次随机事件,第 j 个窗口 w_j 内随机事件发生的次数 $N_{u,j}$ 为用户 u 在第 j 个窗口内的评分数目,计算公式为

$$N_{u,j}=\sum_{i\in w_j}\Gamma(r_{u,i}) \tag{7}$$

第 j 个窗口 w_j 内随机事件发生的概率 $p_{u,j}$ 为 $N_{u,j}$ 与用户 u 的全部评分数目的比率,计算公式为

$$p_{u,j}=\frac{N_{u,j}}{\sum_{i\in I}\Gamma(r_{u,i})} \tag{8}$$

其中,j=1,2,…,J.

综上所述,本文提出的用于检测推荐攻击的通用特征如下:

1) 整体信息熵(entire information entropy,简记为 EntireIE)

用户 u 的 EntireIE 描述了用户 u 的整体评分在各个窗口分布的不确定性,计算公式为

$$EntireIE_u=-\sum_{j=1}^{J}p_{u,j}\log_2 p_{u,j} \tag{9}$$

2) 窗口信息熵(window information entropy,简记为 WindowIE)

用户 u 的 WindowIE 描述了用户 u 的评分在一个窗口与其余窗口分布的不确定性,计算公式为

$$WindowIE_{u,j}=-p_{u,j}\log_2 p_{u,j}-(1-p_{u,j})\log_2(1-p_{u,j}) \tag{10}$$

其中,$(1-p_{u,j})$表示第 j 个窗口之外随机事件发生的概率,$j=1,2,\ldots,J$.

从信息熵的角度出发,用户评分数目可视为随机事件发生的次数,直接影响到上述特征的计算,是用户概貌的重要信息.因此,本文提取如下两个基于评分数目的特征.

3) 整体填充规模(entire filler size,简记为 EntireFS)

用户 u 的 EntireFS 描述了用户 u 的评分数目与全部项目数目的比例,计算公式为

$$EntireFS_u=\frac{\sum_{i\in I}\Gamma(r_{u,i})}{|I|} \tag{11}$$

4) 窗口填充规模(window filler size,简记为 WindowFS)

用户 u 的 WindowFS 描述了用户 u 在一个窗口内的评分数目与用户 u 的全部评分数目的比率,计算公式为

$$WindowFS_{u,j}=\frac{\sum_{i\in w_j}\Gamma(r_{u,i})}{\sum_{i\in I}\Gamma(r_{u,i})} \tag{12}$$

其中,$j=1,2,\ldots,J$.注意到,WindowIE 和 WindowFS 是一系列特征,包含的特征数目均为 J.

基于上述分析,用 V_u 表示任意用户 u 的特征向量,本文所提出的特征提取算法如算法 1 所示.

算法 1. 特征提取算法.

输入:D_g,I,J,u.

输出:V_u.

1. for each item $i\in I$ do
2. $count\leftarrow 0$;
3. for each user $v\in D_g$ do
4. $count\leftarrow count+\Gamma(r_{v,i})$; /*评分计数*/
5. end for
6. $PopI_i\leftarrow count$; /*得到项目流行度*/
7. end for
8. $q\leftarrow\lceil |I|/J\rceil$; /*计算窗口规模*/
9. for $j=1$ to $J-1$ do
10. $w_j\leftarrow\{i|i\in I, i$ belongs to the q most popular items$\}$; /*依据项目流行度划分项目到窗口*/
11. $I\leftarrow I-w_j$;
12. end for
13. $w_J\leftarrow I$; /*剩余项目分配给最后一个窗口*/
14. $V_u\leftarrow(EntireIE_u,WindowIE_{u,1},\ldots,WindowIE_{u,J},EntireFS_u,WindowFS_{u,1},\ldots,WindowFS_{u,J})$; /*利用公式(9)~公式(12)计算特征*/
15. return V_u.

算法 1 首先计算项目流行度(第 1 行~第 7 行),然后划分项目到不同的窗口(第 8 行~第 13 行),完成特征计算(第 14 行)之后将结果返回(第 15 行).

算法 1 第 1 行~第 7 行计算项目流行度,该过程的时间复杂度为 $O(|I|\times G)$.第 8 行计算窗口规模,可在常数时间内完成.第 9 行~第 12 行把项目划分到窗口,该过程时间复杂度为 $O(J)$.第 13 行划分剩余项目到最后一个窗口,第 14 行计算特征值,第 15 行返回计算结果.这些操作均可在常数时间内完成.由于项目数目$|I|>J$,所以算法 1 在最坏情况下的时间复杂度为 $O(|I|\times G)$.

2.2 检测算法

仿生模式识别的目标是实现特征空间中样本的最佳覆盖.为了检测未知推荐攻击,我们将利用 CNN 网络对真实概貌样本进行覆盖.显然,在覆盖范围内的测试数据将被判为真实概貌,否则被判为攻击概貌.

在 CNN 网络中,神经元的超球半径 k 决定了神经元的覆盖区域.图 3 是一个神经元的覆盖区域二维示意图,其中,方块表示训练集中的第 i 个和第 i+1 个真实概貌样本,圆圈和圆点分别表示测试集中的攻击概貌和真实概貌.

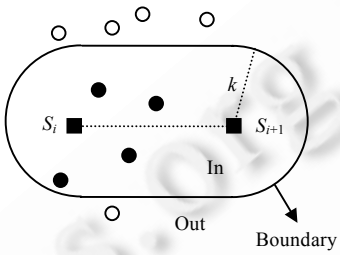

Fig.3 Illustration of one neuron coverage in 2-dimensional space

图 3 神经元覆盖区域二维示意图

从图 3 可以看出,k 是一个非常重要的参数,若设置过小会增加误报率,若设置过大则会降低对推荐攻击的命中率.为了合理地设置参数 k,我们首先把 D_g 随机分为数目相等的两个子数据集 $D_{g,1}$ 和 $D_{g,2}$,之后,让这两个数集相互覆盖,分别为 $D_{g,1}$ 和 $D_{g,2}$ 确定超球半径 k_1 和 k_2.

基于上述分析,本文提出的神经元超球半径计算算法如算法 2 所示.

算法 2. 神经元超球半径计算算法.

输入:$D_{g,1}$, $D_{g,2}$.

输出:k_1.

```
1.  k1←0.01;                                  /*初始化*/
2.  repeat
3.      flag←true;
4.      for each user u∈Dg,2 do
5.          if CNN(Dg,1,k1,Vu)=0 then         /*如果没有完全覆盖*/
6.              flag←false;
7.              k1←k1+0.01;                   /*扩大覆盖范围*/
8.          end if
9.      end for
10. until flag=true
11. return k1.
```

算法 2 首先给超球半径 k_1 初始化一个较小的值(第 1 行),然后,通过判断 $D_{g,1}$ 是否覆盖 $D_{g,2}$(第 5 行),逐步扩大覆盖范围(第 7 行),直到完全覆盖(第 10 行),最后为 $D_{g,1}$ 返回超球半径(第 11 行).在算法 2 中,函数 $CNN(D_{g,1}, k_1, V_u)$表示 CNN 网络以 $D_{g,1}$ 作为训练集,以 k_1 作为超球半径.对用户 u 的输出结果,实现过程如公式(2)~公式(4)所示.将算法 2 的输入 $D_{g,1}$ 和 $D_{g,2}$ 位置互换,利用同样的方法可以为 $D_{g,2}$ 确定超球半径 k_2.

算法 2 的第 1 行进行初始化,第 11 行返回计算结果,这些操作均可在常数时间内完成.第 5 行判断是否覆盖,需要与所有神经元的覆盖区域进行比较,因此时间复杂度为 $O(|D_{g,1}|)$,第 4 行~第 9 行遍历 $D_{g,2}$ 中的用户并判断是否覆盖,时间复杂度为 $O(|D_{g,2}|\times|D_{g,1}|)$,第 10 行的外层循环用于判断是否满足条件,可在常数时间内完成.由于 $|D_{g,2}|=|D_{g,1}|=G/2$,所以算法 2 在最坏情况下的时间复杂度为 $O(G^2)$.

循环不变式(loop invariant)[24]常用于证明算法的正确性.下面利用循环不变式证明算法 2 的正确性.

利用 CNN 网络覆盖真实概貌样本,也就是在特征空间中,把 D_g 中的真实概貌样本正好划分到如图 3 所示的边界(boundary)之内,此后边界不再扩大.在算法 2 中,当把子数据集 $D_{g,1}$ 作为训练集时,$D_{g,1}$ 中的样本显然已经在边界之内,此时只需基于 $D_{g,1}$,通过不断增大超球半径 k_1,把 $D_{g,2}$ 中的样本划分到边界之内即可.

因此,利用循环不变式证明算法 2 的正确性,只需证明在第 2 行~第 10 行的循环中,以 $D_{g,1}$ 作为训练集、以 k_1 作为超球半径的 CNN 网络只对 $D_{g,2}$ 中的真实概貌样本进行了覆盖,当循环结束时,$D_{g,2}$ 中的样本正好包含在边界之内.以下是算法 2 正确性的证明过程.

- 初始化:在循环的第 1 轮开始之前,有 k_1=0.01.由于这是一个相当小的超球半径(相对于本文来说), CNN 网络要么只覆盖了极少量 $D_{g,2}$ 中的样本,要么覆盖 $D_{g,2}$ 的样本数目为 0.循环不变式显然成立.
- 保持:假设第 j(j=1,2,…)次循环成立并且没有达到停止条件,那么,在第 j+1 次循环时,执行的操作为第 7 行 k_1 增大 0.01,即,增大如图 3 所示的边界.之后会出现两种情况:
  - 第 1 种情况,当第 4 行遍历 $D_{g,2}$ 中的样本时,第 5 行的判断结果不全为假,第 6 行 *flag*←false,表明 CNN 网络还没有完全覆盖 $D_{g,2}$ 中的样本,超球半径 k_1 需要继续增大;
  - 第 2 种情况,当第 4 行遍历 $D_{g,2}$ 中的样本时,第 5 行的判断结果全为假,表明在第 j+1 次增大 k_1 之后,$D_{g,2}$ 刚好被 CNN 网络完全覆盖.

  显然,这两种情况下,循环不变式都是成立的.
- 终止:当循环结束时,第 5 行的判断结果全为假,第 10 行的 *flag*=true,CNN 网络以 k_1 作为超球半径,刚好把 $D_{g,2}$ 中的样本包含在边界之内.这说明算法 2 是正确的,第 11 行返回结果.

由算法 2 计算出的超球半径所确定的 CNN 网络的覆盖范围,针对训练集中的数据是正确的、合理的.为了进一步提升 CNN 网络在测试集上的检测性能,在 CNN 网络利用超球半径进行检测时,本文引入一个缩放因子 α 作为超球半径的系数,对超球半径进行缩放处理,其中,α>0.基于上述分析,用 D_{test} 表示测试集,用 $Result_{test}$ 表示检测结果集,本文提出的未知推荐攻击检测算法如下所述.

算法 3. 未知推荐攻击检测算法.

输入:$D_{g,1}$, k_1, $D_{g,2}$, k_2, D_{test}, α.

输出:$Result_{test}$.

1. k_1←k_1×α;
2. k_2←k_2×α;
3. $Result_{test}$←∅;
4. for each user u∈D_{test} do
5. if $CNN(D_{g,1},k_1,V_u)$=1 and $CNN(D_{g,2},k_2,V_u)$=1 then
6. $Result_{test}$←$Result_{test}$∪{genuine profile}; /*判为真实概貌*/
7. else
8. $Result_{test}$←$Result_{test}$∪{attack profile}; /*判为攻击概貌*/
9. end if
10. end for
11. return $Result_{test}$;

算法 3 首先对超球半径进行缩放处理(第 1 行、第 2 行),然后依次检测测试集 D_{test} 中的用户(第 4 行),若在覆盖范围内,则判为真实概貌(第 5 行、第 6 行),否则判为攻击概貌(第 7 行、第 8 行),然后返回检测结果 $Result_{test}$(第 11 行).本文将采用实验手段,通过引入一个校验集为算法 3 确定合适的缩放因子α的值.

算法 3 第 1 行~第 3 行的计算和初始化操作以及第 11 行返回计算结果操作,均可在常数时间内完成.与对算法 2 第 5 行的分析相同,第 5 行的时间复杂度为 $O(G)$,第 4 行~第 10 行遍历 D_{test} 中的用户并进行类别判断,时间复杂度为 $O(G\times|D_{test}|)$.因此,算法 3 在最坏情况下的时间复杂度为 $O(G\times|D_{test}|)$.

算法 3 在标识真实概貌时采用的是比攻击概貌更为严格的限制条件,只有同时被覆盖才被判定为真实概貌,保证算法在略微增加误报率的前提下,提高对攻击概貌的命中率.这是因为在评分数据库中,真实评分通常远远多于虚假评分,而少量虚假评分则可能会产生较大的攻击效果.

3 实验与评价

本节首先介绍实验数据和实验设置,之后介绍检测方法的评价标准,最后对实验结果进行分析.

3.1 实验数据和设置

利用 MovieLens 数据集建立实验数据.该数据集包含 6 040 个用户对 3 952 个项目的 1 000 209 条评分.评分值为区间[1,5]之间的整数值,5 为最高分,表示很喜欢;1 为最低分,表示不喜欢.其中,每个用户概貌至少包含 20 条评分记录.我们将 MovieLens 数据集中的全部用户概貌作为真实概貌样本.

我们利用常见的攻击模型生成攻击概貌作为攻击概貌样本,所用攻击模型包括随机攻击、均值攻击、流行攻击和 AoP 攻击[2,6,7].其中,随机攻击最易于部署;均值攻击用到更多的知识成本,攻击效果较好;流行攻击的攻击效果与均值攻击相当,但知识成本较低;AoP 攻击在均值攻击的基础上进行模糊处理,从前 a%最流行的项目中选取项目构建攻击概貌,记为 a% AoP.通过设置填充规模(filler size)[25]生成包含不同评分数目的攻击概貌.

表 2 给出了本文所用实验数据,包含 1 组训练集、1 组校验集和 7 组测试集.

Table 2 Experimental data

表 2 实验数据

用户概貌类型	训练集	校验集	测试集						
			1st	2nd	3rd	4th	5th	6th	7th
Genuine	1 000	500	500	500	500	500	500	500	500
Random	0	0	60	0	0	0	0	0	30
Average	0	0	0	60	0	0	0	0	30
Bandwagon	0	0	0	0	60	0	0	0	30
20% AoP	0	0	0	0	0	40	0	0	20
30% AoP	0	0	0	0	0	0	40	0	20
40% AoP	0	0	0	0	0	0	0	40	20

如表 2 所示,为了建立训练集和校验集,我们从 MovieLens 数据集中依次随机选取 1 000 和 500 个用户概貌作为真实概貌样本.注意到,训练集和校验集中都不包含攻击概貌样本.这是因为本文旨在检测未知类型的推荐攻击,所以训练集和校验集中不包含关于推荐攻击的任何先验知识.

为了建立测试集,我们依次从 MovieLens 数据集中剩余用户概貌中选取 500 个用户概貌作为第 1 组~第 7 组测试集的真实概貌样本;然后,我们在第 1 组~第 6 组测试集中分别注入一类攻击概貌样本,在第 7 组测试集中注入多类攻击概貌样本作为混合攻击(mixture attack)的测试数据.

第 1 组~第 6 组测试集中攻击概貌样本的生成过程为:

- 设置随机攻击,均值攻击和流行攻击的填充规模分别为{1%,3%,5%,10%,25%,50%},每个填充规模下生成 10 个攻击概貌样本;
- 设置 20% AoP,30% AoP 和 40% AoP 的填充规模为{1%,3%,5%,10%},每个填充规模下生成 10 个攻击概貌样本.

第 7 组测试集中攻击概貌样本的生成方法与上述过程相似,不同之处在于,各类攻击模型在不同填充规模下生成的攻击概貌的数目为 5.

为了确保实验的可信性,上述过程将在随机选取目标项目的基础上重复执行 50 次,将检测结果的平均值作为最终的实验结果.由于本文方法对推攻击和核攻击的检测效果相同,本文只对推攻击进行检测.为便于后文讨论,我们将利用测试集中包含的攻击概貌类型表示第 1 组~第 7 组测试集.

3.2 评价标准

本文采用命中率(hit ratio,简称 HR)和误报率(false alarm ratio,简称 FAR)作为检测方法的性能评价指标,命中率和误报率的定义如下[26]:

$$HR=\frac{TP}{P} \tag{13}$$

$$FAR=\frac{FP}{N} \tag{14}$$

其中,TP 表示被正确检测出的攻击概貌的数目,P 表示全体攻击概貌的数目,FP 表示被误判为攻击概貌的真实概貌数目,N 表示全体真实概貌的数目.

3.3 实验结果与分析

在机器学习领域,信息增益(information gain,简称 IG)[27]常用于评价特征在分类系统中的重要程度,特征的信息增益越大,表明该特征越重要.本节中,我们将首先利用信息增益评价所提到的特征的重要程度.

然后,对比和分析本文方法(记为 CNN-Entropy)与另外 3 种检测方法的实验结果:

- 采用 PCA-VarSelect[12]作为第 1 种对比方法,作为经典的无监督方法,PCA-VarSelect 在检测性能方面表现优异,实验中,我们满足 PCA-VarSelect 对先验知识的需求,即,假定 PCA-VarSelect 方法已知测试集中攻击概貌的数目.
- 在有监督方法中,Williams 等人提出了 6 个通用特征[14].我们在相同的检测框架下,用该 6 个特征替换本文所提到的特征,作为另一种对比方法(记为 CNN-Six).
- 把半监督方法 HySAD[20]作为第 3 种对比方法.

根据算法 1~算法 3 的时间复杂度,得到本文提出的检测方法 CNN-Entropy 最坏情况下的时间复杂度为 $O(|I|\times G+G^2+G\times|D_{test}|)$.在另外 3 种方法中,CNN-Six 的时间复杂度与 CNN-Entropy 的时间复杂度相同;无监督方法 PCA-VarSelect 不需要训练样本,其时间复杂度只与测试集的输入规模有关,为 $O(|D_{test}|^3)$;HySAD 的时间复杂度为 $O(G+|D_{test}|)$.其中,$|I|$表示项目数目,G 表示训练样本数目,$|D_{test}|$表示测试样本数目.

3.3.1 信息增益

本文所提到的特征在测试集上的平均信息增益见表 3,其中,Rank 表示对特征重要程度的排序.

Table 3 Information gain of the proposed features

表 3 所提出的特征的信息增益

特征	Random		Average		Bandwagon		20% AoP		30% AoP		40% AoP		Mixture	
	IG	Rank	IG	Rank	IG	Rank	IG	Rank	IG	Rank	IG	Rank	IG	Rank
EntireIE	0.491	1	0.491	1	0.491	1	0.381	1	0.381	1	0.381	1	0.779	1
WindowIE	0.465	4	0.464	3	0.458	3	0.175	4	0.193	4	0.209	4	0.542	4
EntireFS	0.469	2	0.447	4	0.445	4	0.358	2	0.326	2	0.353	2	0.731	2
WindowFS	0.466	3	0.465	2	0.459	2	0.177	3	0.197	3	0.211	3	0.545	3

从表 3 可以看出,在检测所有攻击模型时,EntireIE 始终是最重要的,这表明基于窗口划分随机事件在区分真实概貌和攻击概貌时具有较好的识别效果.

在检测随机攻击、AoP 攻击和混合攻击时,基于评分数目的特征 EntireFS 和 WindowFS 具有较大的信息增益;在检测均值攻击和流行攻击时,WindowFS 具有较大的信息增益.该结果表明:攻击者在进行攻击时,除谨慎设置评分分布外,还要慎重考虑评分数目,以避免被检测方法识别.

3.3.2 参数设置

采用实验手段设置算法 3 中的缩放因子α.利用本文提出的 CNN-Entropy 检测方法,通过设置不同的缩放因子α值对校验集进行检测,得到缩放因子α对检测方法 CNN-Entropy 误报率的影响,如图 4 所示.注意到,由于校验集中不包含攻击概貌,因此无法统计 CNN-Entropy 检测方法对校验集的命中率.

从图 4 可以看出,随着缩放因子α的增大,误报率逐渐降低.这是因为随着α的增大,超球半径会逐渐增大,即,增大了 CNN 网络对真实概貌的覆盖范围,使得校验集中更多的真实概貌被正确识别,所以降低了误报率.与此同时,超球半径的增大会减少 CNN 网络对攻击概貌的覆盖范围,这通常又会导致命中率的下降.因此,通过合理设置缩放因子α,可以对误报率和命中率进行平衡.

在后面的实验部分,3 种检测方法 PCA-VarSelect,CNN-Six 和 HySAD 的平均误报率分别为 0.03,0.42 和 0.6.我们依据这三者中的最小值 0.03 设置 CNN-Entropy 方法的缩放因子,即,设置α=0.7.采用这种设置方法的主要依据是:在误报率相当的情况下,只需得到较高的命中率即可验证本文提出方法 CNN-Entropy 的有效性.

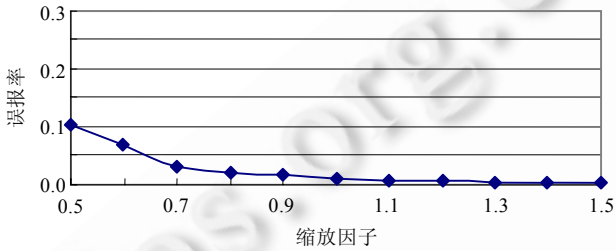

Fig.4 Influence of scaling factor on false alarm ratio

图 4 缩放因子对误报率的影响

3.3.3 命中率和误报率对比

4 种检测方法 PCA-VarSelect,CNN-Six,HySAD 和 CNN-Entropy 在测试集上的检测结果如图 5 和图 6 所示.

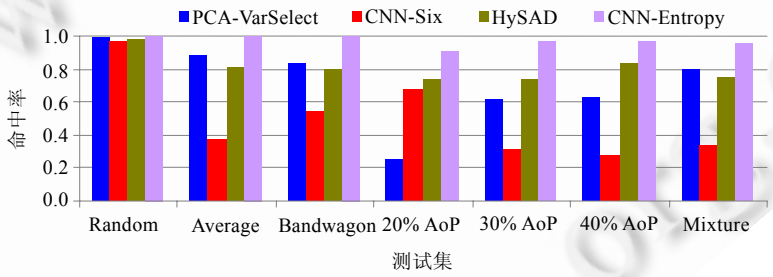

Fig.5 Hit ratio of the four approaches

图 5 4 种方法的命中率

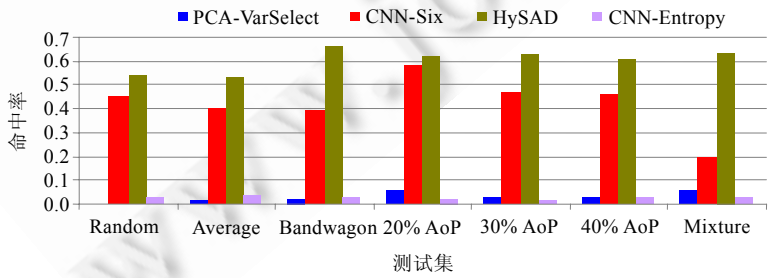

Fig.6 False alarm ratio of the four approaches

图 6 4 种方法的误报率

从图 5 可以看出:

- CNN-Six 只有在检测随机攻击时命中率才较高;
- PCA-VarSelect 在检测随机攻击、均值攻击和流行攻击时具有较高的命中率;

- HySAD 对各类攻击模型都具备一定的命中率;
- 本文提出的 CNN-Entropy 的命中率明显优于其他 3 种方法,对各种攻击模型都具有较高的命中率.

如图 5 所示,4 种检测方法对随机攻击均有较高的命中率,与其他攻击模型相比,简单的随机攻击更容易被检测.这表明攻击者在实施推荐攻击时,若要避免被轻易检测,则必要的知识成本必不可少.

评分值是随机攻击和均值攻击的主要不同之处,它们分别采用随机评分和平均评分生成攻击概貌.从图 5 可以看出:CNN-Six 在检测随机攻击时具有较高的命中率,但该方法不能有效地检测均值攻击;CNN-Entropy 对两类攻击都有较好的检测效果.这是因为 CNN-Entropy 提取的是评分分布特征,攻击者仅改变评分值并不会影响 CNN-Entropy 的检测性能.

从图 6 可以看出:

- CNN-Six 和 HySAD 具有较高的误报率,平均误报率都在 0.4 以上;
- 在检测 20% AoP,30% AoP,40% AoP 和混合攻击时,CNN-Entropy 的误报率均低于 PCA-VarSelect,这两种方法的平均误报率分别为 0.027 和 0.03.

上述实验结果充分验证了本文方法的有效性.

4 结论及进一步工作

推荐攻击的检测是提高协同推荐系统的鲁棒性和确保系统推荐可信性的关键.我们在这方面进行了有益的探索和尝试.提出了一种特征提取算法,从评分分布的角度提取了基于信息熵的通用特征,能够有效地区分真实概貌和攻击概貌.提出了一种未知推荐推荐攻击检测算法,在特征空间中通过仿生模式识别技术覆盖真实概貌样本,检测未知推荐攻击.在 MovieLens 数据集上进行了对比实验,实验结果表明,本文方法对未知推荐攻击具有较好的检测性能.进一步的工作将是利用社会网络分析技术从用户关系角度提取通用特征.

References:

[1] Meng XW, Hu X, Wang LC, Zhang YJ. Mobile recommender systems and their applications. Ruan Jian Xue Bao/Journal of Software, 2013,24(1):91−108 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4292.htm [doi: 10.3724/SP.J.1001.2013.04292]

[2] Lam SK, Riedl J. Shilling recommender systems for fun and profit. In: Feldman S, Uretsky M, Najork M, eds. Proc. of the 13th Int'l Conf. on World Wide Web. New York: ACM Press, 2004. 393−402. [doi: 10.1145/988672.988726]

[3] Aghili G, Shajari M, Khadivi S, Morid MA. Using genre interest of users to detect profile injection attacks in movie recommender systems. In: Chen XW, Tharam D, Hisao I, eds. Proc. of the 10th Int'l Conf. on Machine Learning and Applications. Washington: IEEE Computer Society, 2011. 49−52. [doi: 10.1109/ICMLA.2011.151]

[4] Zhang S, Ouyang Y, Ford J, Makedon F. Analysis of a low-dimensional linear model under recommendation attacks. In: Efthimiadis EN, Dumais S, Hawking D, eds. Proc. of the 29th Annual Int'l ACM SIGIR Conf. on Research and Development in Information Retrieval. New York: ACM Press, 2006. 517−524. [doi: 10.1145/1148170.1148259]

[5] Mobasher B, Burke R, Bhaumik R, Williams C. Towards trustworthy recommender systems: An analysis of attack models and algorithm robustness. ACM Trans. on Internet Technology, 2007,7(4):23:1−23:38. [doi: 10.1145/1278366.1278372]

[6] Burke R, Mobasher B, Williams C, Bhaumik R. Classification features for attack detection in collaborative recommender systems. In: Tina ER, Ungar L, Craven M, Gunopulos D, eds. Proc. of the 12th ACM SIGKDD Int'l Conf. on Knowledge Discovery and Data Mining. New York: ACM Press, 2006. 542−547. [doi: 10.1145/1150402.1150465]

[7] Hurley N, Cheng ZP, Zhang M. Statistical attack detection. In: Bergman L, Tuzhilin A, Burke R, Felfernig A, Lars ST, eds. Proc. of the 3rd ACM Conf. on Recommender Systems. New York: ACM Press, 2009. 149−156. [doi: 10.1145/1639714.1639740]

[8] Chirita PA, Nejdl W, Zamfir C. Preventing shilling attacks in online recommender systems. In: Bonifati A, Lee D, eds. Proc. of the 7th Annual ACM Int'l Workshop on Web Information and Data Management. New York: ACM Press, 2005. 67−74. [doi: 10.1145/1097047.1097061]

[9] Su XF, Zeng HJ, Chen Z. Finding group shilling in recommendation system. In: Ellis A, Hagino T, Douglis F, Raghavan P, eds. Special Interest Tracks and Posters of the 14th Int'l Conf. on World Wide Web. New York: ACM Press, 2005. 960−961. [doi: 10.1145/1062745.1062818]

[10] Li C, Luo ZG, Shi JL. An unsupervised algorithm for detecting shilling attacks on recommender systems. Acta Automatica Sinica, 2011,37(2):160−167 (in Chinese with English abstract). [doi: 10.3724/SP.J.1004.2011.00160]

[11] Lee JS, Zhu D. Shilling attack detection—A new approach for a trustworthy recommender system. JNFORMS Journal on Computing, 2012,24(1):117−131. [doi: 10.1287/ijoc.1100.0440]

[12] Mehta B, Hofmann T, Fankhauser P. Lies and propaganda: Detecting spam users in collaborative filtering. In: Chin D, Zhou M, Lau T, Puerta A, eds. Proc. of the 12th Int'l Conf. on Intelligent User Interfaces. New York: ACM Press, 2007. 14−21. [doi: 10.1145/1216295.1216307]

[13] Mehta B, Nejdl W. Unsupervised strategies for shilling detection and robust collaborative filtering. User Modeling and User-Adapted Interaction, 2009,19(1/2):65−79. [doi: 10.1007/s11257-008-9050-4]

[14] Williams CA, Mobasher B, Burke R. Defending recommender systems: Detection of profile injection attacks. Service Oriented Computing and Applications, 2007,1(3):157−170. [doi: 10.1007/s11761-007-0013-0]

[15] Williams CA, Mobasher B, Burke R, Bhaumik R. Detecting profile injection attacks in collaborative filtering: A classification-based approach. In: Nasraoui O, Spiliopoulou M, Srivastava J, eds. Proc. of the 8th Knowledge Discovery on the Web Int'l Conf. on Advances in Web Mining and Web Usage Analysis. LNCS 4811, Heidelberg: Springer-Verlag, 2007. 167−186. [doi: 10.1007/978-3-540-77485-3_10]

[16] He FM, Wang XR, Liu BX. Attack detection by rough set theory in recommendation system. In: Yager R, Zhang B, eds. Proc. of the 2010 IEEE Int'l Conf. on Granular Computing. Washington: IEEE Computer Society, 2010. 692−695. [doi: 10.1109/GrC.2010.130]

[17] Zhang FZ, Zhou QQ. A meta-learning-based approach for detecting profile injection attacks in collaborative recommender systems. Journal of Computers, 2012,7(1):226−234. [doi: 10.4304/jcp.7.1.226-234]

[18] Wu ZA, Zhuang Y, Wang YQ, Cao J. Shilling attack detection based on feature selection for recommendation systems. Acta Electronica Sinica, 2012,40(8):1687−1693 (in Chinese with English abstract). [doi: 10.3969/j.issn.0372-2112.2012.08.031]

[19] Wu ZA, Gao J, Mao B, Wang YQ. Semi-SAD: Applying semi-supervised learning to shilling attack detection. In: Mobasher B, Burke R, Jannach D, Adomavicius G, eds. Proc. of the 5th ACM Conf. on Recommender Systems. New York: ACM Press, 2011. 289−292. [doi: 10.1145/2043932.2043985]

[20] Wu ZA, Wu JJ, Cao J, Tao DC. HySAD: A semi-supervised hybrid shilling attack detector for trustworthy product recommendation. In: Yang Q, Agarwal D, Pei J, eds. Proc. of the 18th ACM SIGKDD Int'l Conf. on Knowledge Discovery and Data Mining. New York: ACM Press, 2012. 985−993. [doi: 10.1145/2339530.2339684]

[21] Shannon CE. A mathematical theory of communication. Bell System Technical Journal, 1948,27(4):623−656.

[22] Wang SJ. Bionic (topological) pattern recognition—A new model of pattern recognition theory and its applications. Acta Electronica Sinica, 2002,30(10):1417−1420 (in Chinese with English abstract).

[23] Wang XB, Zhou DL, Wang SJ. Constructive neuron networks classification algorithm based on biomimetic pattern recognition. Chinese Journal of Computers, 2007,30(12):2109−2114 (in Chinese with English abstract). [doi: 10.3969/j.issn.1001-3695.2009.09.032]

[24] Cormen TH, Leiserson CE, Rivest RL, Stein C. Introduction to Algorithms. 2nd ed., London: MIT Press, 2001. 17−19.

[25] Mehta B, Nejdl W. Attack resistant collaborative filtering. In: Chua TS, Leong MK, Myaeng SH, Oard DW, Sebastiani F, eds. Proc. of the 31st Annual Int'l ACM SIGIR Conf. on Research and Development in Information Retrieval. New York: ACM Press, 2008. 75−82. [doi: 10.1145/1390334.1390350]

[26] Fawcett T. An introduction to ROC analysis. Pattern Recognition Letters, 2006,27(8):861−874. [doi: 10.1016/j.patrec.2005.10.010]

[27] Ambert KH, Cohen AM. *K*-Information gain scaled nearest neighbors: A novel approach to classifying protein-protein interaction-related documents. IEEE/ACM Trans. on Computational Biology and Bioinformatics, 2012,9(1):305−310. [doi: 10.1109/TCBB.2011.32]

附中文参考文献:

[1] 孟祥武,胡勋,王立才,张玉洁.移动推荐系统及其应用.软件学报,2013,24(1):91−108. http://www.jos.org.cn/1000-9825/4292.htm [doi: 10.3724/SP.J.1001.2013.04292]

[10] 李聪,骆志刚,石金龙.一种探测推荐系统托攻击的无监督算法.自动化学报,2011,37(2):160−167. [doi: 10.3724/SP.J.1004.2011.00160]

[18] 伍之昂,庄毅,王有权,曹杰.基于特征选择的推荐系统托攻击检测算法.电子学报,2012,40(8):1687−1693. [doi: 10.3969/j.issn.0372-2112.2012.08.031]

[22] 王守觉.仿生模式识别(拓扑模式识别)——一种模式识别新模型的理论与应用.电子学报,2002,30(10):1417−1420.

[23] 王宪保,周德龙,王守觉.基于仿生模式识别的构造型神经网络分类方法.计算机学报,2007,30(12):2109−2114. [doi: 10.3969/j.issn.1001-3695.2009.09.032]

周全强(1985－),男,山东沂水人,博士,主要研究领域为信息安全,个性化推荐.
E-mail: zhouqiang128@126.com

刘文远(1968－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为无线传感器网络,信息安全,电子商务.
E-mail: wyliu@ysu.edu.cn

张付志(1964－),男,博士,教授,博士生导师,主要研究领域为智能信息处理,网络与信息安全,面向服务计算.
E-mail: xjzfz@ysu.edu.cn