基于模糊核聚类和支持向量机的鲁棒协同推荐算法

伊华伟[①②③] 张付志*[①②] 巢进波[①②]
[①](燕山大学信息科学与工程学院 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) 秦皇岛 066004)
[③](辽宁工业大学电子与信息工程学院 锦州 121001)

摘 要：该文针对现有推荐算法在面对托攻击时鲁棒性不高的问题，提出一种基于模糊核聚类和支持向量机的鲁棒推荐算法。首先，根据攻击概貌间高度相关的特性，利用模糊核聚类方法在高维特征空间对用户概貌进行聚类，实现攻击概貌的第 1 阶段检测。然后，利用支持向量机分类器对含有攻击概貌的聚类进行分类，实现攻击概貌的第 2 阶段检测。最后，基于攻击概貌检测结果，通过构造指示函数排除攻击概貌在推荐过程中产生的影响，并引入矩阵分解技术设计相应的鲁棒协同推荐算法。实验结果表明，与现有的基于矩阵分解模型的推荐算法相比，所提算法不但具有很好的鲁棒性，而且准确性也有提高。

关键词：鲁棒推荐算法；托攻击；矩阵分解；模糊核聚类；支持向量机
中图分类号：TP391; TP311 **文献标识码**： A **文章编号**：1009-5896(2017)08-1942-08
DOI: 10.11999/JEIT161154

Robust Collaborative Recommendation Algorithm Based on Fuzzy Kernel Clustering and Support Vector Machine

YI Huawei[①②③] ZHANG Fuzhi[①②] Chao Jinbo[①②]
[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*)
[③](*School of Electronics and Information Engineering*, *Liaoning University of Technology*, *Jinzhou* 121001, *China*)

Abstract: The existing collaborative recommendation algorithms have low robustness against shilling attacks. To solve this problem, a robust collaborative recommendation algorithm is proposed based on Fuzzy Kernel Clustering (FKC) and Support Vector Machine (SVM). Firstly, according to the high correlation characteristic between attack profiles, the FKC method is used to cluster user profiles in high-dimensional feature space, which is the first stage of the attack profile detection. Then, the SVM classifier is used to classify the cluster including attack profiles, which is the second stage of the attack profile detection. Finally, an indicator function is constructed based on the attack detection results to reduce the influence of attack profiles on the recommendation, and it is combined with the matrix factorization technology to devise the corresponding robust collaborative recommendation algorithm. Experimental results show that the proposed algorithm outperforms the existing methods in terms of both recommendation accuracy and robustness.

Key words: Robust recommendation algorithm; Shilling attacks; Matrix factorization; Fuzzy Kernel Clustering (FKC); Support Vector Machine (SVM)

1 引言

协同过滤推荐系统作为电子商务快速发展的一个重要产物，能够为人们提供精确又快速的推荐[1,2]。由于推荐系统的开放特性，一些商家为了个人利益蓄意伪造虚假用户评分，并将其注入到系统中干扰正常的决策推荐过程，企图影响正常的推荐结果，这种恶意行为被称为托攻击(shilling attacks)、推荐攻击(recommendation attacks)或概貌注入攻击(profile infection attacks)。根据攻击的目的可将托攻击分为推攻击和核攻击[3]。托攻击的存在严重影响了系统的推荐质量以及用户对系统的信任。因此，

收稿日期：2016-10-27；改回日期：2017-04-19；网络出版：2017-05-11
*通信作者：张付志 xjzfz@ysu.edu.cn
基金项目：国家自然科学基金(61379116)，河北省自然科学基金(F2015203046)，辽宁省教育厅科学研究项目(L2015240)
Foundation Items: The National Natural Science Foundation of China (61379116), The Natural Science Foundation of Hebei Province (F2015203046), The Scientific Research Foundation of Liaoning Provincial Education Department (L2015240)

如何降低托攻击的影响，确保系统推荐结果的可信性已成为亟待解决的问题。本文的主要目的就是设计一种抗攻击能力强、推荐准确性高的鲁棒推荐算法。

针对托攻击问题，目前主要有两种解决方法：一种是在推荐算法运行之前采用托攻击检测技术识别攻击概貌并将其过滤掉，使其不进入推荐过程；另一种是采用鲁棒推荐技术，提高推荐算法的鲁棒性[4]。基于这两种方法，人们提出了诸多鲁棒推荐算法。

从攻击检测角度，Mehta 等人[5]基于攻击概貌间的高相关性提出了变量选择-奇异值分解算法，首先使用主元方法检测可疑用户，然后在推荐模型构建过程中排除可疑用户的干扰。Lee 等人[6]提出了一种混合两阶段攻击检测方法，分别利用多维尺度和 k-means 技术过滤和标识攻击概貌。Bhaumik 等人[7]利用 k-means 技术把用户概貌聚成两类，将用户概貌数量少的类判定为攻击概貌所在类，并将该类中的全部用户概貌都视为攻击概貌。李聪等人[8]通过度量攻击概貌的群体效应构建遗传优化的目标函数，并在遗传优化过程中融入贝叶斯推断思想，提出了一种无监督检测算法。Williams 等人[9,10]基于用户评分数据提取若干推荐攻击特征，并训练有监督机器学习算法生成分类器，然后用分类器对测试集中用户概貌进行分类。He 等人[11]在 Williams 等人提出的一系列攻击特征基础上，提出了一种基于粗糙集理论的托攻击检测方法。伍之昂等人[12]也同样基于 Williams 等人提出的一系列攻击特征，提出了一种基于特征选择的托攻击检测方法，在一定程度上提高了针对特定攻击类型的检测效果。李文涛等人[13]从用户选择评分项目方式入手，提出了基于流行度分类特征和决策树的托攻击检测算法。Zhang 等人[14]针对有监督攻击检测方法精度低的问题，基于 BP 神经网络和集成学习提出一种集成检测模型。

为了提高推荐算法的鲁棒性，文献[15,16]对基于 k-means 聚类、概率潜在语义分析、主成分分析和关联规则的 4 种协同过滤推荐算法进行了研究。与传统的 k-近邻方法相比，在面对托攻击时 4 种算法的鲁棒性都有明显提高，但是准确性会有所降低。Mehta 等人[17]提出了基于 M-估计量的鲁棒推荐算法，但是该方法只适用于中小规模攻击。Cheng 等人[18]提出了一种基于最小截尾二乘估计量的鲁棒矩阵分解算法，在梯度下降过程中通过丢弃残差值较大的评分来抵制恶意攻击的影响。Yi 等人[19]提出了基于 k-距离与 Tukey M-估计量的鲁棒协同推荐算法，与文献[17]和文献[18]相比，在鲁棒性和准确性方面都有提高。李聪等人[20]提出了用于鲁棒协同推荐的元信息增强变分贝叶斯矩阵分解模型，将用户嫌疑性及项类属等原信息与贝叶斯概率矩阵分解模型相融合，有效提高了推荐系统的鲁棒性。张燕平等人[21]结合协同过滤推荐领域内的隐语义模型并引入用户声誉系数，提出了基于用户声誉的隐语义模型鲁棒协同算法，从人为攻击和自然噪声两个方面对系统的鲁棒性进行了改善，在准确性得到一定提升的情况下增强了系统抵御攻击的能力。李改等人[22]将 Sigmoid 和 Fidelity 两个成对损失函数分别与基于矩阵分解和基于最近邻的协同过滤推荐算法进行结合，提出了两个鲁棒的单类协同排序算法，在含有大量噪声数据点的真实数据集上进行实验验证，提出的算法在各个评价指标下均优于当前最新的单类协同排序算法。

已有的鲁棒推荐算法具有一定的抗攻击能力，但是存在一些不足，一是容易将真实概貌误判为攻击概貌，导致算法准确性受损；二是算法鲁棒性的提高是以损失准确性为代价的。

为了解决上述问题，本文提出一种基于模糊核聚类和支持向量机的鲁棒协同推荐算法(RCR-FKCSVM)。与现有鲁棒推荐算法相比，本文算法综合考虑了托攻击检测技术和鲁棒推荐技术。首先基于托攻击检测技术，对攻击概貌进行识别和标记；然后运用鲁棒推荐技术，降低攻击概貌对推荐结果的影响。本文的主要贡献包括：(1)提出了一种基于模糊核聚类的攻击概貌检测算法。依据攻击概貌之间的高度相关特性，利用模糊核聚类方法对用户概貌进行聚类，实现攻击概貌的第 1 阶段检测。(2)提出了一种基于支持向量机的攻击概貌识别算法。利用支持向量机分类器对含有攻击概貌的类进行分类，实现攻击概貌的第 2 阶段检测。(3)将攻击检测结果融入矩阵分解模型，设计一种鲁棒协同推荐算法，在 MovieLens 数据集上与现有相关算法从评分预测和 top-N 推荐两个方面进行对比实验，对算法的准确性和鲁棒性进行性能评价，以验证所提算法的有效性。

2　基于模糊核聚类和支持向量机的鲁棒协同推荐算法 RCR-FKCSVM

本文提出的鲁棒协同推荐算法 RCR-FKCSVM 框架如图 1 所示。从图 1 可以看出，算法主要由基于模糊核聚类的攻击概貌检测、基于支持向量机的攻击概貌识别和基于矩阵分解模型的鲁棒推荐 3 部分构成。

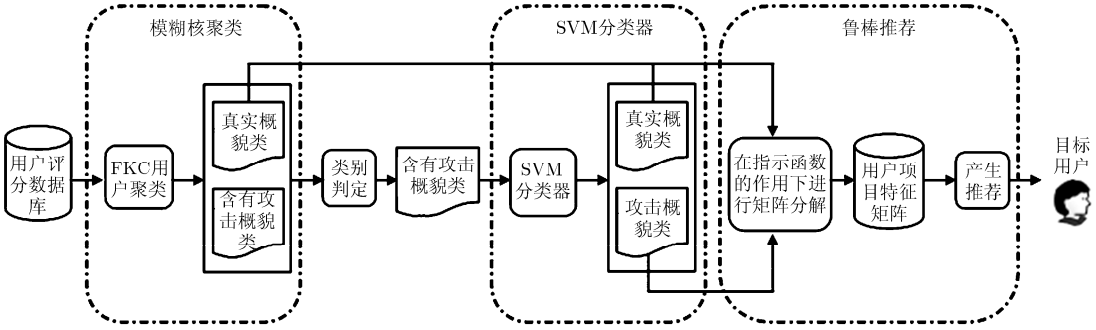

图 1 鲁棒协同推荐算法RCR-FKCSVM框架图

2.1 基于模糊核聚类的攻击概貌检测

通常情况下，受生成模型的影响，攻击概貌彼此之间具有较高的相似度。因此，根据概貌间的相似度，利用模糊核聚类对用户概貌进行聚类，将用户概貌聚为两类，一类是真实概貌的类，一类是含有攻击概貌的类。设含有 m 个用户概貌的数据集合 $X=\{x_i \mid i=1,2,\cdots,m\}$，通过核函数 K 将 X 映射到高维特征空间 F，在 F 中完成用户概貌的聚类。本文采用高斯核函数 $K\left(x_i,x_j\right)=\exp\left(\left(-\left\|x_i-x_j\right\|^2\right)\Big/2\sigma^2\right)$，其中，$\sigma$ 为高斯核函数的宽度(本文取 $\sigma=38$)。

基于模糊核聚类的攻击概貌检测算法(APD-FKC)如表 1 的算法 1 所示。

2.2 基于支持向量机的攻击概貌识别

本节提出了基于支持向量机的攻击概貌识别方法(API-SVM)，采用文献[9]和文献[10]提出的关于推荐攻击的 13 个用户概貌特征。将训练集样本表示为特征向量的形式，然后用特征向量组成的训练集来训练支持向量机生成 SVM 分类器。在识别过程中，首先对算法 1 得到的聚类结果进行类别判定，根据文献[23]，将用户概貌评分偏离度的平均值较小的类作为含有攻击概貌的聚类，然后将该类作为待识别用户概貌集，根据上面提到的 13 个概貌特征将其映射到特征空间，得到待识别用户概貌集所对应的特征向量集，最后利用已训练好的 SVM 分类器对其进一步识别攻击概貌，排除部分真实用户概貌，得到最终的攻击概貌集合。

基于上述分析，给出基于支持向量机的攻击概貌识别算法(API-SVM)如表 2 的算法 2 所示。

2.3 基于矩阵分解模型的鲁棒协同推荐算法

本节基于 SVM 分类器识别得到的攻击概貌结果，结合矩阵分解模型[18]，设计鲁棒协同推荐算法 RCR-FKCSVM。算法的预测评分公式为 $\tilde{r}_{ui}=\boldsymbol{q}_i^{\mathrm{T}}\boldsymbol{p}_u$，为了得到用户特征向量 $\boldsymbol{p}_u$ 和项目特征向量 $\boldsymbol{q}_i$，通过梯度下降分别对 $\boldsymbol{p}_u$ 和 $\boldsymbol{q}_i$ 进行迭代更新：

$$\boldsymbol{p}_u \leftarrow \boldsymbol{p}_u+\gamma(\boldsymbol{q}_i e_{ui}-\lambda\boldsymbol{p}_u) \tag{1}$$

$$\boldsymbol{q}_i \leftarrow \boldsymbol{q}_i+\gamma(\boldsymbol{p}_u e_{ui}-\lambda\boldsymbol{q}_i) \tag{2}$$

$$e_{ui}=\tilde{r}_{ui}-r_{ui} \tag{3}$$

表 1 APD-FKC 算法

算法 1 基于模糊核聚类的攻击概貌检测算法(APD-FKC)
输入：用户评分矩阵 $\boldsymbol{R}$，用户数目 m，项目数目 n
输出：用户概貌聚类结果 $\boldsymbol{C}$ Begin
1: $c\leftarrow 2$, $s\leftarrow 2$, $t\leftarrow 0$, $\varepsilon\leftarrow 0.00001$;
2: Initialize the $\boldsymbol{V}_t$, $\boldsymbol{H}_t$;
3: **repeat**
4: $\boldsymbol{V}_{t+1}\leftarrow$ Renew-clustercenter($\boldsymbol{H}_t,\boldsymbol{V}_t$);
5: $\boldsymbol{H}_{t+1}\leftarrow$ Renew-membership($\boldsymbol{V}_{t+1}$)
6: $t\leftarrow t+1$;
7: **until** $\left\|\boldsymbol{H}_{t+1}-\boldsymbol{H}_t\right\|<\varepsilon$
8: $\{\boldsymbol{C}_1,\boldsymbol{C}_2\}\leftarrow$ User-cluster($\boldsymbol{H}$);
9: **return** $\{\boldsymbol{C}_1,\boldsymbol{C}_2\}$;
End

表 2 API-SVM 算法

算法 2 基于支持向量机的攻击概貌识别算法 API-SVM
输入：待识别用户概貌集 $\text{Userprofile}_{\text{set}}$
输出：$\text{Attackprofile}_{\text{set}}$
Begin
1: $\text{Feature-Userprofile}_{\text{set}}\leftarrow\varnothing$, $\text{Attackprofile}_{\text{set}}\leftarrow\varnothing$;
2: **for** each Userprofile $\in\text{Userprofile}_{\text{set}}$ **do**
3: Feature-Userprofile $\leftarrow$ Feature-extract(Userprofile);
4: $\text{Feature-Userprofile}_{\text{set}}\leftarrow\text{Feature-Userprofile}_{\text{set}}\cup$ Feature-Userprofile;
5: **end for**
6: **for** each Feature-Userprofile $\in\text{Feature-Userprofile}_{\text{set}}$ **do**
7: predictresult $\leftarrow$ SVM-Classifier(Feature-Userprofile);
8: **if** predictresult $=1$ **then**
9: $\text{Attackprofile}_{\text{set}}\leftarrow\text{Attackprofile}_{\text{set}}\cup$Feature-Userprofile;
10: **end if**
11: **end for**
12: **return** $\text{Attackprofile}_{\text{set}}$;
End

其中， r_{ui} 表示用户 u 对项目 i 的真实评分， $\tilde{r}_{ui}$ 表示用户 u 对项目 i 的预测评分， e_{ui} 被称为残差， γ 表示梯度下降的变化步长， λ 为常数。

在迭代过程中，为了避免攻击概貌对项目特征向量 $\boldsymbol{q}_i$ 的影响，基于 SVM 分类器识别得到的攻击概貌结果，构造指示函数 $I(u)$ 并将其融入到式(2)中，得到式(4)。

$$\boldsymbol{q}_i \leftarrow \boldsymbol{q}_i + I(u)\gamma(\boldsymbol{p}_u e_{ui} - \lambda \boldsymbol{q}_i) \tag{4}$$

$$I(u) = \begin{cases} 0, & u \in \text{Attack},\ u \in U \\ 1, & u \notin \text{Attack},\ u \in U \end{cases} \tag{5}$$

其中， Attack 为攻击概貌集合， U 为全体用户概貌集合。

从式(1)和式(4)可以看出，在梯度下降过程中，如果是攻击概貌，根据指示函数的取值，只对 $\boldsymbol{p}_u$ 进行更新， $\boldsymbol{q}_i$ 保持不变，因此可以降低攻击概貌对 $\boldsymbol{q}_i$ 的影响，提高算法的鲁棒性。最后得到用户特征矩阵 $\boldsymbol{P}$ 和项目特征矩阵 $\boldsymbol{Q}$ ，实现对用户的鲁棒推荐 $\widetilde{\boldsymbol{R}} = \boldsymbol{Q}^{\mathrm{T}}\boldsymbol{P}$ 。

基于上述算法思想，给出基于模糊核聚类和支持向量机的鲁棒协同推荐算法 RCR-FKCSVM 描述如表 3 的算法 3。

表 3　RCR-FKCSVM 算法

算法 3　鲁棒推荐算法 RCR-FKCSVM

输入：用户-项目评分矩阵 $\boldsymbol{R}$ ，潜在分类特征个数 f ，用户数目 m ，项目数目

输出：用户特征矩阵 $\boldsymbol{P}$ 、项目特征矩阵 $\boldsymbol{Q}$

```
Begin
Initialize the feature matrix P, Q;
{C1, C2} ← APD-FKC(R);
Userprofile-Attack_set ← Judgment(C1, C2);
Attackprofile_set ← API-SVM(Userprofile-Attack_set);
repeat
for each u ∈ U do
  if u ∈ Attackprofile_set then
    I(u) ← 0;
  else
    I(u) ← 1;
  end if
  for each i ∈ I do
   if r_ui ≠ 0 then
     e_ui ← r_ui − q_i^T × p_u;
   end if;
   for k = 1 to f do
     p_uk ← p_uk + γ(q_ik e_ui − λ p_uk);
     q_ik ← q_ik + I(u)γ(p_uk e_ui − λ q_ik);
   end for
  end for
end for
until Convergence of P, Q
return P, Q;
End
```

3　实验与评价

3.1 实验数据集

本文实验采用美国明尼苏达大学 Grouplens 研究小组公布的 Movielens 100K 公共数据集。该数据集由 943 名用户对 1682 部电影的 10 万条评分数据组成，评分值为 1~5 之间的任一整数，评分值越大，说明用户对该部电影的偏好程度就越大。为了验证算法的性能，将整个数据集的 80%用作训练集，20%用作测试集。

3.2 性能评价指标

为了评价评分预测算法的准确性和鲁棒性，我们采用平均绝对误差(Mean Absolute Error, MAE)和预测偏差(Prediction Shift, PS)作为各自的评价指标，计算公式为[24]

$$\text{MAE} = \frac{1}{|T|}\sum_{u\in U, i\in I}\left|r_{ui} - \tilde{r}_{ui}\right| \tag{6}$$

其中， r_{ui} 和 $\tilde{r}_{ui}$ 分别表示用户 u 对项目 i 的真实评分和预测评分， T 表示测试集。

$$\text{PS} = \frac{1}{|T|}\sum_{u\in U, i\in I}\left|\tilde{r}'_{ui} - \tilde{r}_{ui}\right| \tag{7}$$

其中， $\tilde{r}_{ui}$ 和 $\tilde{r}'_{ui}$ 分别表示系统被注入攻击前后用户 u 对目标项目 i 的预测评分， T 表示测试集。

为了评价 top-N 推荐算法的准确性和鲁棒性，我们采用召回率(Recall)和命中率(Hit Ratio, HR)作为各自的评价指标，计算公式为[25]

$$\text{Recall} = \frac{\sum_{u\in U}|R(u)\cap T(u)|}{\sum_{u\in U}|T(u)|} \tag{8}$$

其中， $R(u)$ 表示在训练集上为用户 u 推荐的项目集合， $T(u)$ 表示用户 u 在测试集上喜欢的项目集合。

$$\text{HR} = \frac{1}{|U|}\sum_{u\in U} H_{ui} \tag{9}$$

其中， U 表示真实用户集合， H_{ui} 表示目标项目 i 是否出现在用户 u 的 top-N 推荐列表中，如果出现在列表中，令 $H_{ui}=1$ ，否则 $H_{ui}=0$ 。

3.3 实验结果与性能分析

为了评价本文算法 RCR-FKCSVM 的性能，我们将其与下面 3 种算法进行对比。(1) MMF: Mehta 等人[17]提出的基于 M-估计量的矩阵分解方法。(2) LTSMF: Cheng 等人[18]提出的基于最小截尾二乘估计量的矩阵分解方法。(3)RCR-FKC：首先利用模

糊核聚类对用户概貌进行聚类，然后进行类别判断，识别出含有攻击概貌的类，并将该类中全部用户概貌标识为攻击概貌，最后进行基于矩阵分解的鲁棒推荐。

3.3.1 评分预测算法的准确性及鲁棒性对比分析 为了评价攻击概貌存在情况下算法的预测准确性及鲁棒性，向训练集中分别注入均值攻击和 AOP 攻击这两种不同类型的攻击概貌，攻击规模和填充规模如表 4～表 5 中所示。各算法在不同的攻击类型、攻击规模和填充规模下的 MAE 值和 PS 值的实验对比结果如表 4～表 5 所示。实验过程中注入的攻击为推攻击。

从表 4 和表 5 可以看出，在不同类型攻击下，算法 MMF 和 LTSMF 的 MAE 值均在 0.75 以上，随着攻击规模和填充规模的增加，二者的 MAE 值波动范围不大，说明算法的稳定性较好。算法 RCR-FKC 的 MAE 值在 0.7360～0.7449 之间，同算法 MMF 和 LTSMF 相比，MAE 值偏小，原因是算法 RCR-FKC 在预测运行之前利用模糊核聚类方法将攻击概貌聚到同一类内，将含有攻击概貌的类内用户概貌全部标识为攻击概貌，从而在预测过程中排除攻击概貌的影响，有效提高算法的预测准确性。算法 RCR-FKCSVM 的 MAE 值在 0.7295～0.7358 之间，在 4 种推荐算法中 MAE 值是最小的。相比算法 RCR-FKC 来说，算法 RCR-FKCSVM 在模糊核聚类之后，针对含有攻击概貌的类利用 SVM 分类器再次对其进行攻击概貌的识别，有助于保留部分真实概貌，进一步提高算法的预测准确性，也验证了利用 SVM 分类器进一步识别攻击概貌的必要性。因此，在系统被注入攻击概貌的情况下，同算法 MMF, LTSMF 和 RCR-FKC 相比，本文算法 RCR-FKCSVM 的预测准确性最好。

从表 4 和表 5 可以看出，在均值攻击下，算法 MMF 的 PS 值变化范围在 0.9057～1.7731 之间，算法 LTSMF 的 PS 值变化范围在 0.7700～1.6167 之间；在 AOP 攻击下，算法 MMF 的 PS 值变化范围在 0.9595～1.8735 之间，算法 LTSMF 的 PS 值变化范围在 0.8599～1.7193 之间。由此可见，算法 LTSMF

表 4 均值攻击下各算法的 MAE 和 PS 对比

		攻击规模(%)											
		1		2		4		6		8		10	
填充规模(%)		3	5	3	5	3	5	3	5	3	5	3	5
MMF	MAE	0.7538	0.7547	0.7530	0.7531	0.7530	0.7528	0.7524	0.7532	0.7542	0.7543	0.7534	0.7535
	PS	0.9057	0.9425	1.3347	1.3536	1.5586	1.5794	1.6336	1.6441	1.7224	1.6739	1.7494	1.7731
LTSMF	MAE	0.7510	0.7508	0.7508	0.7507	0.7514	0.7521	0.7500	0.7503	0.7509	0.7521	0.7503	0.7518
	PS	0.7700	0.8561	1.1773	1.2031	1.3939	1.4099	1.458	1.4992	1.5505	1.5285	1.5798	1.6167
RCR-FKC	MAE	0.7425	0.7417	0.7421	0.7420	0.7419	0.7424	0.7406	0.7418	0.7410	0.7407	0.7416	0.7406
	PS	0.0713	0.0678	0.0659	0.069	0.0716	0.1354	0.0696	0.0679	0.0764	0.1345	0.0789	0.1234
RCR-FKCSVM	MAE	0.7307	0.7315	0.7320	0.7318	0.7321	0.7296	0.7358	0.7315	0.7306	0.7297	0.7305	0.7314
	PS	0.0633	0.0688	0.0643	0.0686	0.0704	0.1287	0.0677	0.066	0.0759	0.1121	0.0744	0.1107

表 5 AOP 攻击下各算法的 MAE 和 PS 对比

		攻击规模(%)											
		1		2		4		6		8		10	
填充规模(%)		3	5	3	5	3	5	3	5	3	5	3	5
MMF	MAE	0.7569	0.7547	0.7556	0.7531	0.7589	0.7558	0.7590	0.7562	0.7542	0.7563	0.7564	0.7555
	PS	0.9595	0.9981	1.4465	1.5562	1.6746	1.6782	1.8439	1.8467	1.8289	1.8352	1.936	1.8735
LTSMF	MAE	0.7530	0.7508	0.7523	0.7515	0.7528	0.7521	0.7514	0.7527	0.7515	0.7533	0.7522	0.7528
	PS	0.8599	0.9464	1.3019	1.3565	1.5077	1.5654	1.6733	1.7347	1.6605	1.7275	1.7185	1.7193
RCR-FKC	MAE	0.7449	0.7397	0.7360	0.7420	0.7409	0.7424	0.7396	0.7398	0.7410	0.7407	0.7416	0.7406
	PS	0.066	0.0743	0.0677	0.078	0.0653	0.0743	0.0766	0.0757	0.0689	0.0723	0.0677	0.076
RCR-FKCSVM	MAE	0.7309	0.7319	0.7295	0.7310	0.7312	0.7323	0.7322	0.7295	0.7307	0.7320	0.7300	0.7313
	PS	0.0645	0.0707	0.0676	0.072	0.0664	0.0723	0.0672	0.0765	0.0679	0.0708	0.0671	0.0756

的鲁棒性要好于算法 MMF，原因是算法 LTSMF 利用最小截断二乘估计量对参数进行鲁棒估计，通过排除残差较大的攻击概貌来提高算法的鲁棒性。在 AOP 攻击下，相比均值攻击，算法 MMF 和 LTSMF 的 PS 值要偏大，原因是 AOP 攻击选取一定比例的流行项目作为填充项，使攻击概貌与真实概貌间具有很高的相似性，以致一些攻击概貌被当作真实用户概貌进入到预测过程中，导致预测偏差增大。对于算法 RCR-FKC 和 RCR-FKCSVM 来说，在均值攻击和 AOP 攻击下，算法的 PS 值变化范围均在 0.1 以下，相比算法 MMF 和 LTSMF 的 PS 值来说要小很多，所以算法 RCR-FKC 和 RCR-FKCSVM 的鲁棒性要优于算法 MMF 和 LTSMF。而算法 RCR-FKCSVM 和 RCR-FKC 的 PS 值差别不是很大，说明在模糊核聚类之后，已经成功地将攻击概貌聚到同一类内，从而验证了模糊核聚类的有效性。综上，算法 RCR-FKCSVM 的鲁棒性最好，是因为首先通过模糊核聚类将用户概貌映射到高维特征空间，放大用户概貌之间的特征，使得用户概貌间具有更好的分离性，能够将攻击概貌聚到同一类内，然后又利用 SVM 分类器对含有攻击概貌类进一步识别，将攻击概貌与类内真实概貌进行分离，最大限度地保留了真实用户概貌，在提高算法鲁棒性的同时提高预测准确性。

3.3.2 top-N 推荐算法的准确性及鲁棒性对比分析

为了检验推荐列表的长度 N 对推荐准确性的影响，本文在未注入攻击情况下，根据 N 的不同取值情况，将各算法的召回率进行了对比，具体结果如图 2 所示。

从图 2 可以看出，随着推荐列表长度 N 的逐渐增大，4 种算法的召回率也逐渐增大。由此可知，为目标用户推荐的项目个数越多，其中包含用户喜欢的项目也就越多。在同一推荐列表长度下，算法 RCR-FKCSVM 的召回率最高，算法 RCR-FKC 的召回率较高，算法 LTSMF 的召回率次之，算法 MMF 的召回率最低。正如 3.3.1 节中所述，本文提出的 RCR-FKCSVM 算法首先采用模糊核聚类对用户概貌进行聚类，将攻击概貌聚到同一类内，然后又利用 SVM 分类器进一步对攻击概貌进行识别，最大限度地保留了真实用户概貌，能够有效提高算法的推荐准确性。

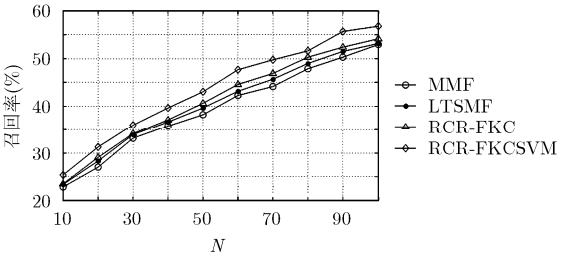

图 2 不同推荐列表长度下各算法的召回率变化情况

采用 3.3.1 节中所述的实验设置方式，对攻击概貌存在情况下各算法的推荐准确性及鲁棒性进行了对比。在实验过程中，我们选取推荐列表长度 N=70。各算法在不同的攻击类型、攻击规模和填充规模下的 Recall 值和 HR 值如表 6 和表 7 所示。

从表 6 和表 7 中的 Recall 值可以看出，在不同的攻击类型、填充规模和攻击规模下，算法 RCR-FKCSVM 的 Recall 值在 4 种算法当中是最大的，召回率越大，说明算法的推荐准确性越高，从而证明算法 RCR-FKCSVM 的推荐准确性是最好的。从表 6 和表 7 的 HR 值可以看出，对于算法 MMF 和 LTSMF 来说，在填充规模为 3%和 5%的情况下，当均值攻击和 AOP 攻击的攻击规模超过 1%时，HR 值就已经接近 1 了，说明系统被注入攻击概貌后，

表 6 均值攻击下各算法的 Recall 值和 HR 值对比

		攻击规模(%)											
		1		2		4		6		8		10	
填充规模(%)		3	5	3	5	3	5	3	5	3	5	3	5
MMF	Recall(%)	47.82	47.13	47.25	48.07	48.07	46.95	47.00	47.82	48.19	47.69	47.94	46.87
	HR	0	0	0.9842	0.9873	0.9889	0.9889	0.9889	0.9889	0.9889	0.9889	0.9889	0.9889
LTSMF	Recall(%)	48.32	48.44	48.07	48.92	48.88	48.17	48.50	48.06	48.91	48.94	48.00	47.20
	HR	0.0016	0	0.9810	0.9826	0.9889	0.9889	0.9889	0.9889	0.9889	0.9889	0.9889	0.9889
RCR-FKC	Recall(%)	49.32	49.34	48.99	49.78	49.72	49.02	49.02	48.91	49.38	49.45	49.02	48.34
	HR	0	0	0	0	0	0	0	0	0	0	0	0
RCR-FKCSVM	Recall(%)	50.86	50.12	49.93	50.49	51.16	50.18	50.99	49.98	50.05	50.37	49.92	49.98
	HR	0	0	0	0	0	0	0	0	0	0	0	0

表 7 AOP 攻击下各算法的 Recall 值和 HR 值对比

		攻击规模(%)											
		1		2		4		6		8		10	
填充规模(%)		3	5	3	5	3	5	3	5	3	5	3	5
MMF	Recall(%)	47.12	48.99	47.68	46.89	47.45	47.51	47.63	47.09	47.57	47.25	47.69	48.12
	HR	0	0.0063	0.9889	0.9889	0.9889	0.9889	0.9889	0.9889	0.9889	0.9889	0.9889	0.9889
LTSMF	Recall(%)	48.19	49.11	48.31	48.31	48.19	48.69	48.19	48.76	48.18	48.07	48.30	49.01
	HR	0	0.0206	0.9873	0.9889	0.9889	0.9889	0.9889	0.9889	0.9889	0.9889	0.9889	0.9889
RCR-FKC	Recall(%)	48.90	50.02	48.95	49.67	49.00	49.22	48.79	49.12	49.02	48.99	49.01	49.89
	HR	0	0	0	0	0	0	0	0	0	0	0	0
RCR-FKCSVM	Recall(%)	49.91	50.99	49.86	50.80	50.17	50.30	49.93	50.17	49.80	50.06	49.87	50.90
	HR	0	0	0	0	0	0	0	0	0	0	0	0

攻击项几乎出现在所有目标用户的推荐列表当中，被推荐给目标用户，因此说明这两种算法的抗攻击能力差，鲁棒性弱。对于算法 RCR-FKC 和 RCR-FKCSVM 来说，在推荐列表长度被设置为 70 的情况下，两种算法的 HR 值均为 0，说明系统被注入攻击概貌后，攻击项并未出现在各用户的推荐列表里，从而也说明了这两种算法未受攻击概貌的影响，鲁棒性强。综合上述分析，算法 RCR-FKC 和 RCR-FKCSVM 能够抵制攻击概貌影响系统的推荐结果，而算法 RCR-FKCSVM 相比 RCR-FKC 来说，能够进一步保留真实用户概貌，在保证系统推荐准确性的基础上提高鲁棒性。

3.3.3 算法运行时间对比分析 为了评价算法的时间性能，将填充规模为 5%和攻击规模为 6%的均值攻击注入到训练集中，并以该情况为例，分别运行文中提出的算法和对比算法，记录各自的模型训练时间和在线预测时间，对各算法进行时间性能对比分析。其中在线预测时间是指测试集中全部用户预测评分时间的平均值。

从表 8 可以看出，对模型训练时间来说，算法 RRA-FKCSVM 用时稍长一些，因为首先要进行模糊核聚类和 SVM 分类操作，然后再对用户特征矩阵和项目特征矩阵进行迭代运算；其次是算法 RRA-FKC，主要包括模糊核聚类操作以及对用户特征矩阵和项目特征矩阵进行迭代运算；算法 MMF 和 LTSMF 用时相差不大，主要对用户特征矩阵和项目特征矩阵进行迭代运算。对在线预测时间来说，4 种算法用时几乎没有差别，时间都很短。结合 3.3.1 节和 3.3.2 节的实验结果，本文算法 RRA-FKCSVM 在保证时间性能的前提下，算法的评分预测性能均优于其他 3 种对比算法。

表 8 各算法的时间性能对比

算法	迭代次数	模型训练时间(s)	在线预测时间(s)
MMF	60	68.791	0.231×10^{-6}
LTSMF	60	67.233	0.226×10^{-6}
RRA-FKC	50	70.386	0.212×10^{-6}
RRA-FKCSVM	50	79.102	0.229×10^{-6}

4 结束语

如何使推荐系统不受恶意攻击的影响是保障推荐质量的关键，本文在这方面进行了有益的探索和尝试。提出了一种基于模糊核聚类的攻击检测方法，根据概貌间的相似度将攻击概貌聚到同一类内。提出了一种基于 SVM 分类器的攻击概貌检测方法，进一步识别攻击概貌。通过构造指示函数将攻击概貌检测结果融入到基于矩阵分解模型的推荐算法中，提出鲁棒推荐算法 RCR-FKCSVM。同现有的鲁棒推荐算法相比，本文提出的算法在保证预测准确性和推荐准确性的前提下，提高了算法的鲁棒性。下一步工作是提高 SVM 分类器的检测性能，尝试提出更有效的推荐攻击特征来精准地识别攻击概貌，减少误判，提高算法的准确性。

参 考 文 献

[1] 孟祥武, 刘树栋, 张玉洁, 等. 社会化推荐系统研究[J]. 软件学报, 2015, 26(6): 1356–1372.
MENG Xiangwu, LIU Shudong, ZHANG Yujie, *et al*. Research on social recommendation systems[J]. *Journal of Software*, 2015, 26(6): 1356–1372.

[2] CHEN L, CHEN G L, WANG F. Recommender systems based on user reviews: The state of the art[J]. *User Modeling and User-Adapted Interaction*, 2015, 25(2): 99–154. doi: 10.1007/s11257-015-9155-5.

[3] GUNES I, KALELI C, BILGE A, *et al*. Shilling attacks against recommender systems: A comprehensive survey[J]. *Artificial Intelligence Review*, 2014, 42(4): 767–799. doi: 10.1007/s10462-012-9364-9.

[4] 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. doi: 10.1145/1031114.1031116.

[5] MEHTA B and NEJDL W. Attack resistant collaborative filtering[C]. Proceedings of the 31st Annual International ACM SIGIR Conference on Research and Development in Information Retrieval, Singapore, 2008: 75–82.

[6] LEE J and ZHU D. Shilling attack detection-a new approach for a trustworthy recommender system[J]. *Informs Journal on Computing*, 2012, 24(1): 117–131. doi: 10.1287/ijoc.1100.0440.

[7] BHAUMIK R, MOBASHER B, and BURKE R. A clustering approach to unsupervised attack detection in collaborative recommender systems[C]. Proceedings of the 7th International Conference on Data Mining, IEEE Computer Society, Washington: 2011: 181–187.

[8] 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[J]. 自动化学报, 2011, 37(2): 160–167.
LI Cong, LUO Zhigang, and SHI Jinlong. An unsupervised algorithm for detecting shilling attacks on recommender systems[J]. *Acta Automatica Sinica*, 2011, 37(2): 160–167.

[9] WILLIAMS C A, MOBASHER B, BURKE R, *et al*. Detecting profile injection attacks in collaborative filtering: A classification-based approach[C]. Proceedings of the 8th Knowledge Discovery on the Web International Conference on Advances in Web Mining and Web Usage Analysis, Berlin, 2007: 167–186.

[10] WILLIAMS C, MOBASHER B, and BURKE R. Defending recommender systems: Detection of profile injection attacks [J]. *Service Oriented Computing and Applications*, 2007, 1(3): 157–170. doi: 10.1007/s11761-007-0013-0.

[11] HE F, WANG X, and LIU B. Attack detection by rough set theory in recommendation system[C]. 2010 IEEE International Conference on Granular Computing, Washington, 2010: 692–695.

[12] 伍之昂, 庄毅, 王有权, 等. 基于特征选择的推荐系统托攻击检测算法[J]. 电子学报, 2012, 40(8): 1687–1693. doi: 10.3969/j.issn.0372-2112.2012.08.031.
WU Zhiang, ZHUANG Yi, WANG Youquan, *et al*. Shilling attack detection based on feature selection for recommendation systems[J]. *Acta Electronica Sinica*, 2012, 40(8): 1687–1693. doi: 10.3969/j.issn.0372-2112.2012.08.031.

[13] 李文涛, 高旻, 李华, 等. 一种基于流行度分类特征的托攻击检测算法. 自动化学报, 2015, 41(9): 1563–1575.
LI Wentao, GAO Min, LI Hua, *et al*. An shilling attack detection algorithm based on popularity degree features[J]. *Acta Automatica Sinica*, 2015, 41(9): 1563–1575. doi: 10.16383/j.aas.2015.c150040.

[14] ZHANG F and ZHOU Q. Ensemble detection model for profile injection attacks in collaborative recommender systems based on BP neural network[J]. *Iet Information Security*, 2015, 9(1): 24–31. doi: 10.1049/iet-ifs.2013.0145.

[15] SANDVIG J J, MOBASHER B, and BURKE R. A survey of collaborative recommendation and the robustness of model-based algorithms[J]. *Bulletin of the Technical Committee on Data Engineering*, 2008, 31(2): 3–13.

[16] SANDVIG J J, MOBASHER B, and BURKE R. Robustness of collaborative recommendation based on association rule mining[C]. Proceedings of the 2007 ACM Conference on Recommender Systems, Minneapolis, 2007: 105–112.

[17] MEHTA B, HOFMANN T, and NEJDL W. Robust collaborative filtering[C]. ACM Conference on Recommender Systems, Recsys, Minneapolis, MN, USA, 2007: 49–56.

[18] CHENG Z and HURLEY N. Robust collaborative recommendation by least trimmed squares matrix factorization[C]. Proceedings of the 22nd IEEE International Conference on Tools with Artificial Intelligence, Arras, France, 2010: 105–112.

[19] YI Huawei and ZHANG Fuzhi. A robust collaborative recommendation algorithm based on k-distance and Tukey M-estimator[J]. *China Communications*, 2014, 11(9): 119–130. doi: 10.1109/CC.2014.6969776.

[20] 李聪, 骆志刚. 用于鲁棒协同推荐的元信息增强变分贝叶斯矩阵分解模型[J]. 自动化学报, 2011, 37(9): 1067–1076.
LI Cong and LUO Zhigang. A metadata-enhanced variational Bayesian matrix factorization model for robust collaborative recommendation[J]. *Acta Automatica Sinica*, 2011, 37(9): 1067–1076.

[21] 张燕平, 张顺, 钱付兰, 等. 基于用户声誉的鲁棒协同推荐算法[J]. 自动化学报, 2015, 41(5): 1004–1012. doi: 10.16383/j.aas.2015.c140073.
ZHANG Yanping, ZHANG Shun, QIAN Fulan, *et al*. Robust collaborative recommendation algorithm based on user's reputation[J]. *Acta Automatica Sinica*, 2015, 41(5): 1004–1012. doi: 10.16383/j.aas.2015.c140073.

[22] 李改, 李磊. 鲁棒的单类协同排序算法[J]. 自动化学报, 2015, 41(2): 405–418. doi: 10.16383/j.aas.2015.c140231.
LI Gai and LI Lei. Robust ranking algorithms for one-class collaborative filtering[J]. *Acta Automatica Sinica*, 2015, 41(2): 405–418. doi: 10.16383/j.aas.2015.c140231.

[23] YI H and ZHANG F. Robust recommendation algorithm based on the identification of suspicious users and matrix factorization[J]. *Journal of Information and Computational Science*, 2014, 11(13): 4769–4777. doi: 10.12733/JICS20104307.

[24] RICCI F, SHAPIRA B, and ROKACH L. Recommender Systems Handbook[M]. New York, Springer US, 2015: 961–995. doi: 10.1007/978-1-4899-7637-6_28.

[25] DESHPANDE M and KARYPIS G. Item-based top-N recommendation algorithms[J]. *ACM Transactions on Information Systems*, 2004, 22(1): 143–177.

伊华伟： 女，1978 年生，副教授，研究方向为推荐系统、信息安全.

张付志： 男，1964 年生，教授，研究方向为智能网络信息处理、网络与信息安全、面向服务计算.

巢进波： 女，1977 年生，讲师，研究方向为网络与信息安全.