

DOI:10.11830/ISSN.1000-5013.201510059



采用矩阵分解模型的托攻击防御算法

方楷强, 王靖

(华侨大学 计算机科学与技术学院, 福建 厦门 361021)

摘要: 提出一种基于矩阵分解模型的托攻击防御算法框架. 首先, 利用托攻击检测技术, 度量用户是托用户的概率, 并以此构造信任度权值矩阵; 然后, 将此权值矩阵引入到矩阵分解模型, 以降低托用户攻击行为的影响; 最后, 通过求解新模型实现对用户评分的预测. 实验结果表明: 这类算法与其他协同过滤算法相比较, 能够更有效地抵御托攻击.

关键词: 推荐系统; 托攻击; 矩阵分解; 信任度权值矩阵

中图分类号: TP 311 **文献标志码:** A **文章编号:** 1000-5013(2018)01-0109-06

Shilling Attack Defense Algorithm Using Matrix Factorization Model

FANG Kaiqiang, WANG Jing

(College of Computer Science and Technology, Huaqiao University, Xiamen 361021, China)

Abstract: A shilling attack defense algorithm framework based on matrix factorization model is proposed. Firstly, using the technology of shilling attack detection, measuring the probability of the shilling and constructing a trust weight matrix. Then, the weight matrix is introduced into the matrix factorization model to reduce the influence of the shilling attack. Finally, by solving the new model to realize the user values prediction. Experimental results show that this algorithms are more effective in resisting the shilling attacks compared to other collaborative filtering algorithms.

Keywords: recommender systems; shilling attack; matrix factorization; trust weight matrix

推荐系统能够满足用户的个性化需求, 因此被广泛地应用于电子商务. 协同过滤技术是推荐系统中应用最广泛和成功的技术之一. 目前, 协同过滤技术的方法有基于内存的算法、基于模型的算法和混合推荐算法^[1]. 由于推荐系统本身具有一定的开放性, 攻击者出于商业竞争等目的, 人为地向系统注入大量虚假用户概貌^[2], 企图使系统产生对他们有利的推荐结果. 这种托攻击(shilling attacks)^[3]主要有两种攻击方式: 推攻击提高目标项目的推荐频率和核攻击减少目标项目的推荐频率. 基本的攻击模型有随机攻击和均值攻击, 填充规模和攻击规模是两个与攻击概貌相关的基本量^[4]. 针对托攻击问题的研究主要包括托攻击的检测和托攻击的防御. Mobasher 等^[5]把概率潜在语义分析(PLSA)模型应用到推荐系统的鲁棒性方面. Mehta 等^[6]提出一种鲁棒的矩阵分解算法(Robust MF). 李聪等^[7]提出一种迭代贝叶斯推断遗传探测算法. 伍之昂等^[8]概述现有的一些关于推荐系统托攻击模型与检测技术的方法. 在现有的协同过滤算法中, 基于矩阵分解模型的协同过滤算法受到学者们的广泛关注, 如基于非负矩阵分

收稿日期: 2015-10-29
通信作者: 王靖(1981-), 男, 教授, 博士, 主要从事模式识别、推荐系统的研究. E-mail: wroaring@hqu.edu.cn.
基金项目: 国家自然科学基金资助项目(61370006); 福建省自然科学基金资助项目(2014J01237); 福建省教育厅科技项目(JA12006); 福建省高等学校新世纪优秀人才支持计划(2012FJ-NCET-ZR01); 华侨大学中青年教师科技创新资助计划(ZQN-PY116)

解(NMF)的协同过滤算法^[9]. 这些算法能够很好地处理大规模矩阵、高稀疏性等问题. 但是, 很少有托攻击防御工作涉及这些算法. 基于此, 本文提出一种基于矩阵分解模型的托攻击防御算法.

1 基于矩阵分解的协同过滤技术

1.1 矩阵分解的基本模型

矩阵分解(matrix factorization, MF)技术是一种有效的寻找内部潜在特征的方法, 它希望找到一个低秩的矩阵逼近原始矩阵 \mathbf{R} . 在推荐系统中, 用户对项目的评分往往是有限的, 因此, 评分矩阵中很多数据是未知的. 为了表明矩阵中哪些评分是已知, 引入一个标志矩阵 \mathbf{T} , 表示为

$$\left. \begin{aligned} \min \sum_{i,j \in \Omega} (R_{i,j} - (\mathbf{U}\mathbf{V}^T)_{i,j})^2 = & \|\mathbf{T} \cdot (\mathbf{R} - \mathbf{U}\mathbf{V}^T)\|_{\text{F}}^2, \\ \text{s. t. } & \mathbf{U} \in \mathbf{R}^{m \times d}, \mathbf{V} \in \mathbf{R}^{n \times d}. \end{aligned} \right\} \tag{1}$$

式(1)中: Ω 是 \mathbf{R} 中已知评分的位置的集合; \mathbf{T} 相当于原来矩阵有评分项设置为 1, 未评分项设置为 0; \cdot 表示点乘($\mathbf{A} = \mathbf{T} \cdot \mathbf{R}$ 等价于 $A_{i,j} = T_{i,j}R_{i,j}$).

求解矩阵分解的基本模型存在过拟合问题, 且评分预测的范围不合理. 因此, 学者们在不同应用背景下, 对基本模型提出不同的约束条件.

1.2 正则化矩阵分解模型

Srebro 等^[10]在模型(1)的基础上, 加入关于 \mathbf{U}, \mathbf{V} 的正则项防止过拟合现象, 从而生成正则化矩阵分解(RMF)模型, 即 $\min \|\mathbf{T} \cdot (\mathbf{R} - \mathbf{U}\mathbf{V}^T)\|_{\text{F}}^2 + \lambda_u \|\mathbf{U}\|_{\text{F}}^2 + \lambda_v \|\mathbf{V}\|_{\text{F}}^2$. 其中, λ_u, λ_v 分别是 \mathbf{U} 和 \mathbf{V} 的正则化参数.

1.3 非负矩阵分解模型

Finesso 等^[9]在模型(1)的基础上, 添加了关于 \mathbf{U}, \mathbf{V} 的非负性约束条件, 得到非负矩阵分解(NMF)模型, 即 $\min_{\text{s. t. } \mathbf{U}, \mathbf{V} \geq 0} \|\mathbf{T} \cdot (\mathbf{R} - \mathbf{U}\mathbf{V}^T)\|_{\text{F}}^2$. 其中, $\mathbf{U}, \mathbf{V} \geq 0$ 表示矩阵 \mathbf{U}, \mathbf{V} 中所有元素均大于等于 0.

1.4 核范数正则化矩阵分解模型

Mazumder 等^[11]在模型(1)的基础上, 引入核范数约束条件, 这种约束条件不需要把矩阵的维度作为输入参数, 得到核范数的矩阵分解模型, 即 $\min_{\mathbf{Z}} \frac{1}{2} \|\mathbf{T} \cdot (\mathbf{R} - \mathbf{Z})\|_{\text{F}}^2 + \lambda \|\mathbf{Z}\|_*$. 其中, \mathbf{Z} 是 $\mathbf{U}\mathbf{V}^T$ 的乘积; $\lambda > 0$, 是控制核范数的正则化参数; $\|\mathbf{Z}\|_*$ 是核范数(即 \mathbf{Z} 的奇异值之和).

1.5 基于矩阵分解模型的托攻击防御算法

为了降低托攻击对推荐结果的影响, 使用现有的托攻击检测方法, 检测哪些用户可能是虚假用户, 通过降低虚假用户评分在模型中的影响, 提高矩阵分解模型对托攻击的防御能力. 原有的工作都是把检测出来的托用户直接从数据集中剔除而不参与运算, 是一个二元分类问题(即检测结果是托用户和正常用户). 但实际中, 可能存在误检的情况(即正常用户被检测成托用户). 例如, 一个用户的喜好就是对不同的项目打平均分, 对比较热门、流行的项目给最高分, 这个用户的概貌和托的概貌就非常类似, 很可能被误检为托用户. 因此, 文中不采用 0, 1 的分类思想剔除检测的托用户, 而是通过降低检测是托用户的信任度, 从而减少托攻击用户的影响.

利用 Chirita 等^[12]提出的偏离平均度(RDMA)的托攻击检测算法构造权值矩阵. 其算法思想是, 根据攻击用户和其他用户在目标评分项出现的次数不同, 计算目标项与其他用户平均评分的偏离程度判断是托用户的概率. 记 r_i 为托攻击检测算法计算的用户 i 的偏离平均度(RDMA). r_i 的范围为 $[0, 1]$, 且 r_i 越大, 表示用户 i 是托的可能性越大. 利用 r_i , 构造用户信任度权值矩阵 $\mathbf{W} = \text{diag}(w_1, w_2, \dots, w_m)$, 其中, $w_i = \exp(-r_i^2)$.

将权值矩阵 \mathbf{W} 引入到矩阵分解模型, 提出基于矩阵分解模型的托攻击防御算法框架. 鲁棒的正则化矩阵分解(Robust RMF)算法模型为

$$\min_{\mathbf{U}, \mathbf{V}} \|\mathbf{W} \times \mathbf{T} \cdot (\mathbf{R} - \mathbf{U}\mathbf{V}^T)\|_{\text{F}}^2 + \lambda_u \|\mathbf{U}\|_{\text{F}}^2 + \lambda_v \|\mathbf{V}\|_{\text{F}}^2. \tag{2}$$

鲁棒的非负矩阵分解(Robust NMF)算法模型为

$$\min_{\mathbf{s}, \mathbf{t}, \mathbf{U}, \mathbf{V} \geq 0} \|\mathbf{W} \times \mathbf{T} \cdot (\mathbf{R} - \mathbf{UV}^T)\|_{\text{F}}^2. \quad (3)$$

鲁棒的软填充(Robust soft-impute)算法模型为

$$\min_{\mathbf{Z}} \frac{1}{2} \|\mathbf{W} \times \mathbf{T} \cdot (\mathbf{R} - \mathbf{UV}^T)\|_{\text{F}}^2 + \lambda \|\mathbf{Z}\|_{*}. \quad (4)$$

1.6 鲁棒的正则化矩阵分解算法模型

模型(2)的求解参考 Wang 等^[13]提出的求解特征子空间变换的方法,根据其模型求解的思路,可以得到该模型的求解方法,即

$$\mathbf{P} = \begin{bmatrix} V_{1,1} & \cdots & V_{1,d} & & & \\ \vdots & & \vdots & \cdots & & \mathbf{0} \\ V_{n,1} & \cdots & V_{n,d} & & & \\ & \vdots & & & & \\ & & & V_{1,1} & \cdots & V_{1,d} \\ & \mathbf{0} & & \vdots & & \vdots \\ & & & V_{n,1} & \cdots & V_{n,d} \end{bmatrix}_{m,n \times n,d}, \quad \mathbf{u} = \begin{bmatrix} U_{1,1} \\ \vdots \\ U_{1,d} \\ \vdots \\ U_{m,1} \\ \vdots \\ U_{n,d} \end{bmatrix}_{m,d},$$

$$\mathbf{Q} = \begin{bmatrix} U_{1,1} & \cdots & U_{1,d} & & & \\ \vdots & & \vdots & \cdots & & \mathbf{0} \\ U_{n,1} & \cdots & U_{n,d} & & & \\ & \vdots & & & & \\ & & & U_{1,1} & \cdots & U_{1,d} \\ & \mathbf{0} & & \vdots & & \vdots \\ & & & U_{n,1} & \cdots & U_{n,d} \end{bmatrix}_{m,n \times n,d}, \quad \mathbf{v} = \begin{bmatrix} V_{1,1} \\ \vdots \\ V_{1,d} \\ \vdots \\ V_{m,1} \\ \vdots \\ V_{n,d} \end{bmatrix}_{m,d}.$$

模型(2)的函数可以改写为

$$\|\mathbf{W} \times \mathbf{T} \cdot (\mathbf{R} - \mathbf{UV}^T)\|_{\text{F}} = \|\mathbf{SPu} - \mathbf{r}\|_{\text{F}} = \|\mathbf{SQv} - \mathbf{r}\|_{\text{F}}.$$

式中: \mathbf{S} 是由权值矩阵 \mathbf{W} 和训练矩阵 \mathbf{T} 构成的选择矩阵.

接下来,可以求解 $\Psi(\mathbf{u}, \mathbf{v}) \rightarrow \min$,其中, $\Psi(\mathbf{u}, \mathbf{v}) = \|\mathbf{PSu} - \mathbf{RS}\|_{\text{F}}^2 + \lambda_u \|\mathbf{u}\|_{\text{F}}^2 + \lambda_v \|\mathbf{v}\|_{\text{F}}^2 = \|\mathbf{QSv} - \mathbf{RS}\|_{\text{F}}^2 + \lambda_u \|\mathbf{u}\|_{\text{F}}^2 + \lambda_v \|\mathbf{v}\|_{\text{F}}^2$.然后,对 $\Psi(\mathbf{u}, \mathbf{v})$ 函数分别对 \mathbf{u} 和 \mathbf{v} 求偏导,令偏导数等于0.则

$$\partial \Psi(\mathbf{u}, \mathbf{v}) \partial \mathbf{u} - 2\mathbf{Hu} - 2\mathbf{P}_s^T \mathbf{r}_s = 0.$$

因此,可以得到 \mathbf{u} 的更新公式为

$$\mathbf{u} \leftarrow \mathbf{H}^{-1} \mathbf{P}_s^T \mathbf{r}_s, \quad \mathbf{H} = \mathbf{P}_s^T \mathbf{P}_s + \lambda_u \mathbf{I}. \quad (5)$$

同样,可以计算 \mathbf{v} 的更新公式为

$$\mathbf{v} \leftarrow \mathbf{G}^{-1} \mathbf{Q}_s^T \mathbf{r}_s, \quad \mathbf{G} = \mathbf{Q}_s^T \mathbf{Q}_s + \lambda_v \mathbf{I}. \quad (6)$$

1.7 鲁棒的非负矩阵分解算法模型

模型(3)的求解参考 Cai 等^[14]关于非负矩阵分解求解的算法,能得到模型的求解方法,记

$$f(\mathbf{U}, \mathbf{V}) = \|\mathbf{W} \times \mathbf{T} \cdot (\mathbf{R} - \mathbf{UV}^T)\|_{\text{F}}^2, \quad \mathbf{W}_x = \mathbf{W} \times \mathbf{T}.$$

因此,将函数改写为

$$f(\mathbf{U}, \mathbf{V}) = \|\mathbf{W}_x \cdot \mathbf{R} - \mathbf{W}_x \cdot \mathbf{UV}\|_{\text{F}}^2.$$

然后,利用求导法则对函数 f 求出 \mathbf{U} 的偏导 $\frac{\partial f(\mathbf{U}, \mathbf{V})}{\partial \mathbf{U}} = 2(-\mathbf{W}_x \cdot \mathbf{RV} + \mathbf{W}_x \cdot \mathbf{UV}^T \mathbf{V})$.接着,利用梯度下降法的更新规则 $X_{i,j} \leftarrow X_{i,j} + \eta_{i,j} \nabla f(X_{i,j})$,得到 $u_{i,k}$ 的更新公式为

$$u_{i,k}^{n+1} = \frac{u_{i,k}^n ((\mathbf{W}_x \cdot \mathbf{R})\mathbf{V})_{i,k}}{((\mathbf{W}_x \cdot \mathbf{UV}^T)\mathbf{V})_{i,k}}. \quad (7)$$

式(7)中: $u_{i,k}$ 为 \mathbf{U} 的每一个元素.

使用同样的方法可以得到 $v_{i,k}$ 的更新公式,即

$$v_{i,k}^{n+1} = \frac{v_{i,k}^n ((\mathbf{W}_x \cdot \mathbf{R})\mathbf{V})_{i,k}}{((\mathbf{W}_x \cdot \mathbf{UV}^T)\mathbf{V})_{i,k}}. \quad (8)$$

1.8 鲁棒的软填充算法模型

模型(4)参考软填充算法^[11],得到鲁棒的软填充(Robust soft-impute)算法模型的求解方法,记 $f = \frac{1}{2} \|W \times T \cdot (R - Z)\|_F^2 + \lambda \|Z\|_*$.

首先,把函数 f 对 z 求偏导 $\frac{\partial f}{\partial z} = W \times T \cdot (ZR) + \lambda \delta \|Z\|_*$;然后,令偏导数为 0,即 $0 \in W \times T \cdot (Z - R_\Delta) + \lambda \delta \|Z\|_*$,记 $W \times T \cdot (Z - R_\Delta) = Y_\Delta - Z_\Delta$. 则由 $\frac{\partial f}{\partial z} = 0$ 可知, $Z_\Delta - Y_\Delta + \lambda \delta \|Z\|_* = 0$,其最优解等价于下面函数的最优解 $\min \frac{1}{2} \|W \times T \cdot (R - Y_\Delta)\|_F^2 + \lambda \|Z\|_*$,其解为 $Z_\Delta S_\lambda(Y_\Delta)$. $Z_\Delta S_\lambda(Y_\Delta)$ 的计算方法为 $[U, S, V] = \text{svd}(Y_\Delta)$, $S = \max(S - \lambda, 0)$, $Z^{k+1} = U \times S \times V$. 其中, $Y_\Delta = Z_\Delta - W \times T \cdot (Z_\Delta - R)$,简化后为 $Y_\Delta = R + V \times Z^{\text{old}}$,

进一步化简,得到 Z 的更新公式为

$$Z^{\text{new}} = S_\lambda(Y_\Delta).$$
 (9)

2 实验分析

为了验证基于矩阵分解模型的托攻击防御算法(包括 Robust RMF, Robust NMF, Robust soft-impute)的有效性,分别采用基于用户相似度的协同过滤(K-NN)算法和 Mehta 等^[6]提出的鲁棒的矩阵分解(Robust MF)算法做对比实验. 同时,采用基于矩阵分解的协同过滤(包括 RMF, NMF, soft-impute)算法进行对比实验.

2.1 数据和评价标准

Movielens 数据集是由明尼苏达大学的 GroupLens 小组发布的电影评分数据集. 实验采用了 1 M 的数据集,该数据集包含了 6 040 个用户对 3 952 项电影进行的 1 000 209 个评分,每个用户至少评价了 20 部电影,且每部电影至少属于 19 种影片类型之一,评分范围为 1~5.

EachMovie 数据集是由 Digital Equipment Corporation 系统研究中心收集的电影评分数据集. 数据集包含了 72 916 个用户对 1 628 个电影项目的 2 800 万条评分,其评分范围为 1~6.

采用均方根误差(E_{RMS})和平均绝对误差(E_{MA})评估算法的准确性,计算式分别为

$$E_{\text{RMS}} = \sqrt{\frac{\sum_{i,j \in T} (Z_{i,j} - R_{i,j})^2}{|T|}}, \quad E_{\text{MA}} = \sqrt{\frac{\sum_{i,j \in T} |Z_{i,j} - R_{i,j}|}{|T|}}.$$

上式中: $Z_{i,j}$ 是预测的评分; $R_{i,j}$ 是真实的评分; T 是测试的数据集, $|T|$ 是测试数据的总个数. 这 2 个指标的值越小,说明算法越准确.

2.2 参数设定

采用基于用户相似度的协同过滤算法时,选取的最近邻个数为 10;对于 RMF, Robust RMF, NMF 和 Robust NMF 算法,都涉及到特征维度参数 d ,其选取范围为 $\{5, 10, 15, 20\}$;对于 RMF 和 Robust RMF 算法,还涉及正则化参数 λ ,其选取范围为 $\{0.1, 1, 5, 10\}$;对于 soft-impute 和 Robust soft-impute 算法,核正则参数选取范围为 $\{10, 15, 20, 25\}$. 所有的实验中,只列出最优的结果.

2.3 方案和结果

首先,测试在同一填充规模下,不同攻击规模的托攻击对不同算法的影响. 采用均值攻击模型构造攻击概貌,攻击类型是推攻击. 对 Movielens 数据集采用 3% 的填充规模和不同的攻击规模的攻击,分别测试在不同攻击规模下,算法受到的影响. 这些攻击的目标项针对的都是同一组目标项. 选择的填充项目有 2 个标准^[6]:这些项目有不多于 5% 的用户对其评分;这些项目的评分的平均分小于等于 3. 根据这个原则,随机选出 80% 的数据进行训练,剩下的用于测试.

在 Movielens 数据集上,选取填充规模为 3%,攻击规模为 1%, 3%, 5%, 10% 时,分别采用 Robust RMF, Robust NMF, Robust soft-impute 算法和 Robust MF 算法及 RMF, NMF, soft-impute 算法进行对比实验,结果如图 1 所示. 图 1 中: η 为攻击规模.

由图 1 可知:随着攻击规模的增加,采用不同算法计算出的预测误差都有所增加,其中,Robust MF

算法受到的影响最大. 整体上, 基于矩阵分解模型的托攻击防御算法(Robust RMF, Robust NMF, Robust soft-impute)都有更好的鲁棒性, 其中, 鲁棒的正则化(Robust RMF)算法对托攻击有更明细的防御效果. 攻击规模从 5% 增加到 10% 的过程中, Robust MF 算法的 E_{RMS} 值变化 0.11; 而 Robust RMF 算法只变化了 0.02, 说明 Robust RMF 算法在大规模攻击下, 受到的影响不大.

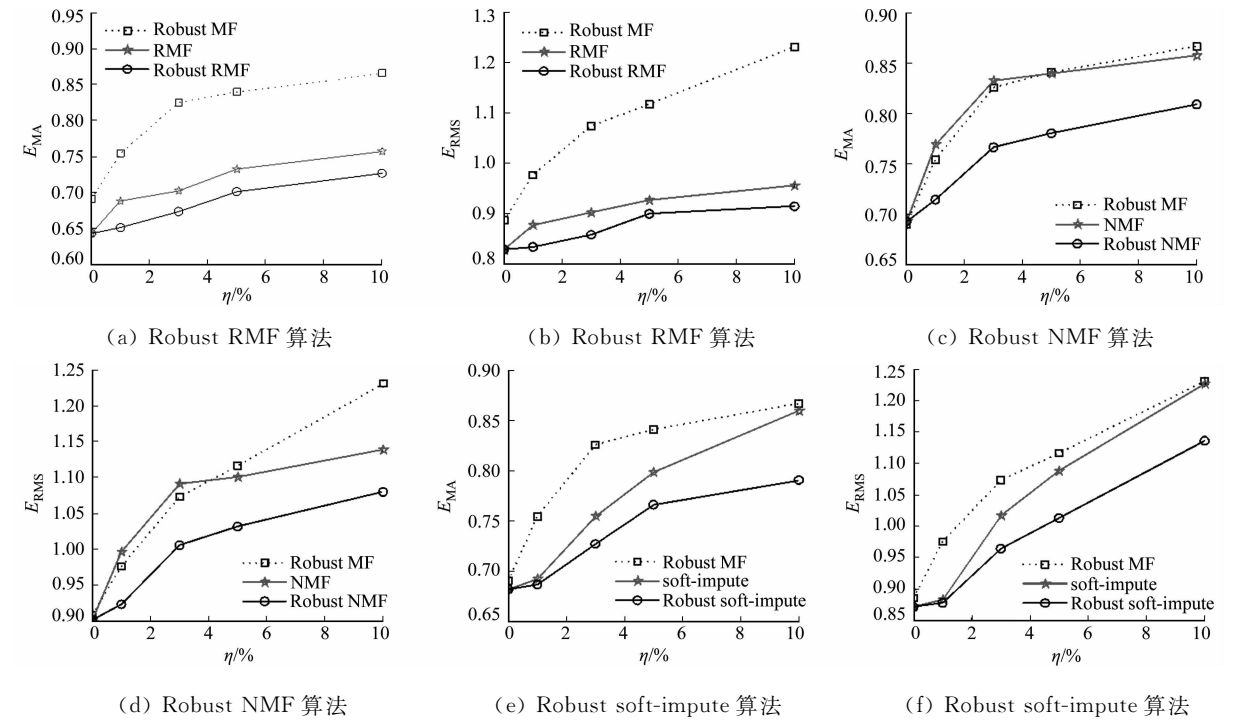


图 1 3%填充规模、不同攻击规模时的预测精度

Fig. 1 Prediction accuracy of 3% filler size with different attack size

其次, 测试同一攻击规模时, 不同填充规模的托攻击对不同算法的影响. 采用均值攻击模型构造攻击概貌, 攻击类型是推攻击. 对 EachMovie 数据集采用 3% 的攻击规模和不同的填充规模, 分别测试不同填充规模时, 算法受到的影响. 在 EachMovie 数据集上, 选取攻击规模为 3%, 填充规模为 3%, 5%, 10%, 25% 时, 分别使用 Robust RMF, Robust NMF, Robust soft-impute 算法和 K-NN, Robust MF 算法及 RMF, NMF, soft-impute 算法进行对比实验, 结果如表 1 所示. 表 1 中: R-MF 为 Robust MF 算法; R-NMF 为 Robust NMF 算法; S-IM 为 soft-impute 算法; R S-IM 为 Robust soft-impute 算法; R-RMF 为 Robust RMF 算法.

表 1 3%攻击规模、不同填充规模时的预测精度

Tab. 1 Prediction accuracy of 3% attack size with different filler size

填充规模	指标	K-NN	R-MF	NMF	R-NMF	S-IM	R S-IM	RMF	R-RMF
0%	E_{MA}	1.274 4	0.913 1	0.889 6	0.889 6	0.810 7	0.810 7	0.764 7	0.764 7
	E_{RMS}	1.417 2	1.192 8	1.179 0	1.179 0	1.041 7	1.041 7	1.011 3	1.011 3
3%	E_{MA}	1.355 9	0.981 1	0.961 1	0.907 4	0.894 0	0.839 0	0.797 5	0.769 6
	E_{RMS}	1.534 0	1.284 3	1.258 1	1.193 4	1.114 3	1.061 8	1.018 4	1.012 6
5%	E_{MA}	1.521 0	1.121 2	1.079 2	0.931 2	0.981 7	0.876 1	0.849 6	0.807 9
	E_{RMS}	1.695 8	1.438 6	1.405 8	1.239 4	1.275 8	1.102 6	1.137 9	1.064 1
10%	E_{MA}	1.806 1	1.152 5	1.161 5	0.981 7	1.096 1	0.920 8	0.941 1	0.831 6
	E_{RMS}	2.036 5	1.556 1	1.560 5	1.305 8	1.365 4	1.184 1	1.241 8	1.125 6
25%	E_{MA}	2.149 1	1.293 5	1.307 5	1.032 4	1.231 3	1.016 2	1.079 8	0.893 7
	E_{RMS}	2.448 6	1.618 7	1.620 5	1.385 7	1.505 8	1.264 4	1.384 1	1.206 2

由表 1 可知: 随着填充规模的增加, 采用不同算法计算出的预测误差都有所增加, 其中, K-NN 算法受到的影响最大, 其次是 Robust MF 算法. 整体上, 基于矩阵分解模型的托攻击防御算法(Robust RMF, Robust NMF, Robust soft-impute)对预测精度都有明显的改进. 即使在填充规模不大(填充规模

3%)时,K-NN 和 R-MF 算法的预测精度都有明显的变化,而基于矩阵分解模型的托攻击防御算法的预测精度变化很小.在实际应用中,由于小规模填充的托攻击更易于操作,许多推荐系统往往面临着这种类型的攻击.采用基于矩阵分解模型的托攻击防御算法能够有效地抵御此类托攻击的影响.

3 结束语

把一些矩阵分解的模型应用到推荐系统的鲁棒性研究上,并提出基于矩阵分解的托攻击防御算法.基于矩阵分解的托攻击防御算法在原有模型的基础上,加入了对真实可能发生的情况的考虑,引入了信任度权值矩阵,使模型的构造趋于合理.这种模型在一定程度上提高了基于模型的协同过滤算法的鲁棒性,能更好地抵御托用户的攻击.

参考文献:

- [1] SU Xiaoyun,KHOSHGOFTAAR T M. A survey of collaborative filtering techniques[J]. Advances in Artificial Intelligence,2009(4):1-19. DOI:10.1155/2009/421425.
- [2] LI Qing,KIM B M. Constructing user profiles for collaborative recommender system[C]//6th Asia-Pacific Web Conference. Hangzhou:Springer Berlin Heidelberg,2004:100-110. DOI:10.1007/978-3-540-24655-8_11.
- [3] LAM S K,RIEDL J. Shilling recommender systems for fun and profit[C]//Proceedings of the 13th International Conference on World Wide Web. New York:ACM,2004:393-402. DOI:10.1145/988672.988726.
- [4] MOBASHER B,BURKE R,BHAUMIK R,*et al.* Effective attack models for shilling item-based collaborative filtering systems[C]//Proceedings of the 2005 Webkdd Workshop. New York:ACM,2005:13-23.
- [5] MOBASHER B,BURKE R,SANDVIG J J. Model-based collaborative filtering as a defense against profile injection attacks[C]//The Twenty-First National Conference on Artificial Intelligence and the Eighteenth Innovative Applications of Artificial Intelligence Conference. Boston:DBLP,2006:1388-1393.
- [6] MEHTA B,HOFMANN T,NEJDL W. Robust collaborative filtering[C]//Proceedings of the 2007 ACM Conference on Recommender Systems. New York:ACM,2007:49-56. DOI:10.1145/1297231.1297240.
- [7] 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.
- [8] 伍之昂,王有权,曹杰. 推荐系统托攻击模型与检测技术[J]. 科学通报,2014(7):551-560. DOI:10.1360/972012-1712.
- [9] FINESSO L,SPREIJ P. Nonnegative matrix factorization and I-divergence alternating minimization[J]. Linear Algebra and Its Applications,2006,416(2):270-287. DOI:10.1016/j.laa.2005.11.012.
- [10] SREBRO N,RENNIE J,JAANKOLA T S. Maximum-margin matrix factorization[C]//Advances in Neural Information Processing Systems. Vancouver:DBLP,2004:1329-1336.
- [11] MAZUMDER R,HASTIE T,TIBSHIRANI R. Spectral regularization algorithms for learning large incomplete matrices[J]. The Journal of Machine Learning Research,2010,11(12):2287-2322.
- [12] CHIRITA P A,NEJDL W,ZAMFIR C. Preventing shilling attacks in online recommender systems[C]//Proceedings of the 7th annual ACM International Workshop on Web Information and Data Management. Bremen:ACM,2005:67-74. DOI:10.1145/1097047.1097061.
- [13] WANG Jing,KE Liangwen. Feature subspace transfer for collaborative filtering[J]. Neurocomputing,2014,136(1):1-6. DOI:10.1016/j.neucom.2014.01.035.
- [14] CAI Deng,HE Xiaofei,HAN Jiawei,*et al.* Graph regularized nonnegative matrix factorization for data representation[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence,2011,33(8):1548-1560.

(责任编辑:黄晓楠 英文审校:吴逢铁)