(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108470052 B
(45)授权公告日 2021.03.19

(21)申请号 201810200894.7

(22)申请日 2018.03.12

(65)同一申请的已公布的文献号
申请公布号 CN 108470052 A

(43)申请公布日 2018.08.31

(73)专利权人 南京邮电大学
地址 210046 江苏省南京市栖霞区文苑路9号

(72)发明人 张涵峰 陈蕾 周宇轩 曹璐 张冯崇

(74)专利代理机构 南京苏高专利商标事务所(普通合伙) 32204
代理人 柏尚春

(51)Int.Cl.
G06F 16/9535(2019.01)
G06F 17/16(2006.01)

(56)对比文件
CN 106874427 A,2017.06.20
JP 2017027480 A,2017.02.02
CN 107689960 A,2018.02.13
陈蕾等.矩阵补全模型及其算法研究综述.《软件学报》.2017,第28卷(第6期),第1547-1564页.
Dietmar Jannach等.Recommender systems—beyond matrix completion.《Communications of the ACM》.2013,第59卷(第11期),第94-102页.

审查员 李萌

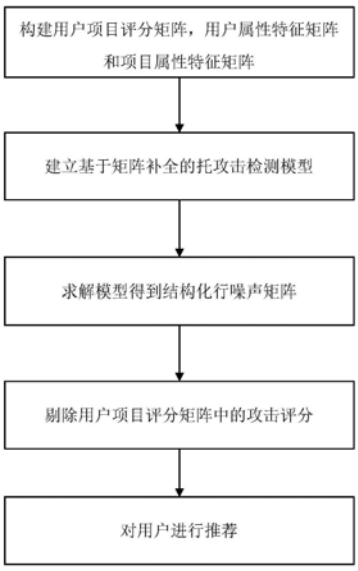
权利要求书2页 说明书8页 附图1页

(54)发明名称

一种基于矩阵补全的抗托攻击推荐算法

(57)摘要

本发明公开了一种基于矩阵补全的抗托攻击推荐算法,首先统计用户对项目的评分,提取用户的属性特征和项目的属性特征,分别构建用户-项目评分矩阵,用户属性特征矩阵和项目属性特征矩阵;然后将用户-项目评分矩阵中的托攻击评分建模为矩阵补全模型中的结构化噪声;然后采用分块坐标下降算法对各变量进行迭代更新,求得结构化行噪声矩阵;随后根据结构化行噪声矩阵剔除用户-项目评分矩阵中的托攻击评分;最后使用传统推荐算法进行评分预测,求得预测评分矩阵。本发明提供的推荐算法能够有效地检测出推荐系统中的托攻击用户,在托攻击干扰下可取得比传统推荐算法更精确的个性化评分预测效果,有效提高了推荐算法的鲁棒性。



CN 108470052 B

1.一种基于矩阵补全的抗托攻击推荐算法,其特征在于:包括如下步骤:

1)建立用户-项目评分矩阵R:

在推荐系统中,m名用户构成用户集合U=$\{U_1,U_2,\cdots,U_m\}$,n件项目构成项目集合I=$\{I_1,I_2,\cdots,I_n\}$,则用户-项目评分矩阵可表示为$R \in \mathbb{R}^{m\times n}$:

$$R=\begin{bmatrix} ? & ? & ? \\ * & r_{i,j} & * \\ * & ? & ? \end{bmatrix}$$

其中,第i个用户U_i对第j件项目I_j的评分记作R_{ij},“*”表示已知评分,“?”表示未知评分;

2)建立基于矩阵补全的推荐模型:

基于矩阵补全的推荐模型建模为:

$$\min_{X\in\mathbb{R}^{m\times n}} \|X\|_* \quad s.t.\ \ \mathrm{P}_\Omega(R)=\mathrm{P}_\Omega(X)$$

其中Ω集合表示评分矩阵中已收到评分的元素下标集合,$\Omega \subseteq \{1,2\cdots m\}\times\{1,2\cdots n\}$,X矩阵是低维未知矩阵,$\|X\|_*=\sum_{i=1}^{\min(m,n)}\sigma_i$为矩阵核范数,$\sigma_i$为矩阵X的第i大奇异值,$\mathrm{P}_\Omega(\bullet)$是投影算子,表示当元素下标(i,j)∈Ω时,得到对应位置采样元素:

$$[\mathrm{P}_\Omega(R)]_{i,j}=\begin{cases} r_{i,j} & (i,j)\in\Omega \\ 0 & (i,j)\notin\Omega \end{cases}$$

3)根据步骤2)建立基于属性优化矩阵补全的托攻击检测模型:

基于属性优化矩阵补全的托攻击检测模型为:

$$\min_{X\in\mathbb{R}^{k\times k},Z\in\mathbb{R}^{m\times n}} \|X\|_*+\lambda\|Z\|_{2,1}+\frac{\beta}{2}\|\mathrm{P}_\Omega(A^TXB+Z-R)\|_F^2$$

其中,A、B分别是用户特征矩阵和项目特征矩阵,Z表示结构化噪声矩阵,||X||$_*$和||Z||$_{2,1}$分别表示对X矩阵进行低秩性约束以及对Z矩阵进行行稀疏性约束,$\|\mathrm{P}_\Omega(A^TXB+Z-R)\|_F^2$是为了平滑评分细微波动的正则化项,λ,β为可调参数,$\Omega\subseteq\{1,2\cdots m\}\times\{1,2\cdots n\}$表示评分矩阵中已反馈的评分元素下标集合;

4)求解基于属性优化矩阵补全的托攻击检测模型,得到结构化行噪声矩阵Z;

5)根据步骤4)中计算得到的结构化噪声矩阵Z从用户-项目矩阵R中剔除托攻击评分;

6)采用传统推荐系统对修正后用户-项目评分矩阵进行评分预测,求得完整的用户-项目评分矩阵,基于完整的用户-项目评分矩阵中的预测评分对目标用户进行项目推荐。

2.根据权利要求1所述的一种基于矩阵补全的抗托攻击推荐算法,其特征在于:所述步骤4)采用分块坐标下降算法求解基于属性优化矩阵补全的托攻击检测模型,得到结构化行噪声矩阵Z,具体步骤如下:

步骤4.1):在基于属性优化矩阵补全的托攻击检测模型中引入变量C并令C=A^TXB,利用Frobenius范数将其进一步改写成相应的罚函数形式,公式转换为:

$$\min_{X\in\mathbb{R}^{k\times k},C,Z\in\mathbb{R}^{m\times n}} =\|X\|_*+\lambda\|Z\|_{2,1}+\frac{\beta}{2}\|\mathrm{P}_\Omega(C+Z-R)\|_F^2+\frac{\rho}{2}\|C-A^TXB\|_F^2$$

步骤4.2):采用分块坐标下降算法求解步骤4.1)中的罚函数,令:

$$\mathrm{L}_\rho(X,Z,C)=\|X\|_*+\lambda\|Z\|_{2,1}+\frac{\beta}{2}\|\mathrm{P}_\Omega(C+Z-R)\|_F^2+\frac{\rho}{2}\|C-A^TXB\|_F^2$$

初始化变量X、Z、C,令变量X^0=0,Z^0=0,C^0=0,则可对各个变量做如下的迭代更新:

X的迭代更新公式为：

$$\begin{cases} Y^{k+1} = X^k - \delta_X \rho(AA^T XBB^T - AC^k B^T) \\ X^{k+1} = \mathrm{D}_{\delta_X}(Y^{k+1}) \end{cases}$$

其中，Y为引入变量，δ_X为引入参数，参数δ_X需满足$0 < \delta_X < \frac{2}{\sigma_{\max}(BB^T) * \sigma_{\max}(AA^T)}$；

类似于X的更新过程Z的迭代更新公式为：

$$\begin{cases} V^{k+1} = Z^k - \delta_Z \beta \mathrm{P}_\Omega(C^k + Z^k - R) \\ (Z^{k+1})^{(i)} = \max\left\{1 - \frac{\delta_Z \lambda}{\|(V^{k+1})^{(i)}\|_2}, 0\right\} * (V^{k+1})^{(i)} \qquad i = 1,2,\cdots,m \end{cases}$$

其中，$(Z^{k+1})^{(i)}$表示第k+1次迭代中矩阵Z的第i行，$(V^{k+1})^{(i)}$表示第k+1次迭代中矩阵V的第i行，V为引入变量，λ、β为可调参数，参数δ_Z需满足$0 < \delta_Z < \frac{2}{\beta}$；

C的迭代更新公式为：

$C^{k+1} = [(\rho+\beta)A^T X^{k+1} B + \beta P_\Omega (R - Z^{k+1} - A^T X^{k+1} B)] / (\rho+\beta)$

其中β为可调参数。

3.根据权利要求2所述的一种基于矩阵补全的抗托攻击推荐算法，其特征在于：所述参数$\delta_X = \frac{1}{\sigma_{\max}(BB^T) * \sigma_{\max}(AA^T)}$。

4.根据权利要求2所述的一种基于矩阵补全的抗托攻击推荐算法，其特征在于：所述参数$\delta_Z = \frac{1}{\beta}$。

5.根据权利要求1所述的一种基于矩阵补全的抗托攻击推荐算法，其特征在于：所述步骤6)采用的推荐算法为不具备抗托攻击能力的传统推荐算法。

一种基于矩阵补全的抗托攻击推荐算法

技术领域

[0001] 本发明属于计算机技术领域中的信息安全领域，具体涉及一种基于矩阵补全的抗托攻击推荐算法。

背景技术

[0002] 面对信息过载问题，推荐系统应运而生。推荐系统是一种软件系统，它通过收集用户信息，项目信息以及用户与项目的交互信息，了解用户的偏好，从而将用户可能感兴趣的项目推荐给用户，在一定程度上解决困扰用户的信息过载问题。当前实现推荐系统的一种主流算法是协同过滤(collaborative filtering)算法。它依赖于用户的历史行为，分析过去的用户-项目交互，建立新的用户-项目联系。然而，用户-项目交互数据的产生者是所有用户，并没有设置准入门槛，这种数据来源的开放性导致协同过滤推荐系统极易受到恶意用户的干扰，这种现象称为托攻击(shilling attack)。

[0003] 托攻击是当前推荐系统遇到的严峻挑战之一。恶意商家或用户为了达成其特殊目的，往往是为了经济利益，冒充正常用户，在与项目交互的过程中，向推荐系统注入精心设计的虚假用户概貌，从而影响正常的推荐结果。这种攻击的存在会严重干扰推荐系统的正常运转，误导用户接受或购买并非真正所需的信息或项目，使用户逐渐丧失对此推荐系统的信任，造成客户群的流失，推荐系统会蒙受信誉与利润的双重损失。

[0004] 当前，针对无托攻击评分数据集已经有了很多行之有效的高精度推荐算法，但在含托攻击数据集上，这些传统推荐算法往往会面临性能下降的问题。

发明内容

[0005] 发明目的：本发明基于结构化噪声矩阵补全技术提出一种鲁棒的抗托攻击个性化推荐算法以提高推荐系统抵御托攻击能力，首先检测出推荐系统中的托攻击用户并剔除相应攻击评分再进行推荐，从而解决推荐系统中存在的托攻击问题，将合适的项目推荐给相应用户。实验表明，该推荐算法在托攻击下可取得比传统推荐算法更精确的个性化评分预测效果，有效提高推荐算法的鲁棒性。

[0006] 技术方案：为实现上述目的，本发明采用如下技术方案：一种基于矩阵补全的抗托攻击推荐算法，包括如下步骤：

[0007] 1)建立用户-项目评分矩阵：

[0008] 设m名用户构成用户集合U＝{u_1,u_2,…u_m}，n件项目构成项目集合I＝{i_1,i_2,…i_n}，用户-项目评分矩阵可表示为$R \in \mathbb{R}^{m\times n}$：

[0009] $$R=\begin{bmatrix} ? & ? & ? \\ * & r_{i,j} & * \\ * & ? & ? \end{bmatrix} \quad (1)$$

[0010] 其中，用户u对项目i的评分记作$r_{i,j}$，“*”表示已知评分，“?”表示未知评分。由于每个用户只可能对有限的项目进行评分，而每件项目也仅可能收到有限用户的评分，故这个

评分矩阵通常包含大量的空缺评分，是一个稀疏矩阵。

[0011] 2)根据步骤一的用户-项目评分矩阵建立基于矩阵补全的推荐系统模型：

[0012] 在推荐系统中，大量的用户之间和大量的项目之间必然存在着偏好相近的用户和属性相近的项目，这种相近性使得用户-项目评分矩阵往往具有近似低秩性，故推荐系统问题可利用低秩矩阵补全技术进行评分预测。用R表示当前观察到的评分矩阵，则推荐系统问题可建模为：

[0013] $$\min_{X\in\mathbb{R}^{m\times n}} \operatorname{rank}(X) \quad s.t.\ \ \mathrm{P}_{\Omega}(R)=\mathrm{P}_{\Omega}(X) \tag{2}$$

[0014] 其中Ω集合表示评分矩阵中已收到评分的元素下标集合，$\Omega\subseteq\{1,2\cdots m\}\times\{1,2\cdots n\}$，X矩阵是低维未知矩阵，$X\in\mathbb{R}^{k\times k}$ $\mathrm{P}_{\Omega}(\cdot)$是投影算子，表示当元素下标(i，j)∈Ω时，得到对应位置采样元素：

[0015] $$[\mathrm{P}_{\Omega}(R)]_{i,j}=\begin{cases} r_{i,j} & (i,j)\in\Omega \\ 0 & (i,j)\notin\Omega \end{cases} \tag{3}$$

[0016] 但是，秩函数rank(X)是非凸的，直接使用秩函数建模得到的是一个NP-Hard问题，其计算代价会随着问题规模的扩大而急剧增大。因此，往往将秩函数松弛化为核范数来解决此问题：

[0017] $$\min_{X\in\mathbb{R}^{m\times n}}\|X\|_{*} \quad s.t.\ \ \mathrm{P}_{\Omega}(R)=\mathrm{P}_{\Omega}(X) \tag{4}$$

[0018] 其中，$\|X\|_{*}=\sum_{i=1}^{\min(m,n)}\sigma_i$为矩阵核范数，$\sigma_i$为矩阵X的第i大奇异值。

[0019] 3)建立基于属性优化矩阵补全的托攻击检测模型：

[0020] 在实际应用中，推荐系统往往会遭受恶意用户的托攻击。面对托攻击干扰，标准矩阵补全模型的推荐精度将严重降低。因此，为了保证推荐的质量，有必要抵御这些攻击数据的影响。通过对托攻击特点进行分析可知，托攻击的目的是更改原来自然情况下的评分情况，假如在自然情况下的评分情况已经符合攻击者的意图，则没有进行攻击的必要，故托攻击用户的评分与自然状态下正常用户的评分存在不一致性。另外，托攻击用户的评分通常是机械填充的，这也会与基于兴趣偏好而形成的正常用户评分具有相异之处。基于以上分析，本发明将用户-项目评分矩阵中的托攻击评分建模为结构化行噪声，这些结构化行噪声与正常用户评分的潜在规律相违背，打破了评分矩阵的近似低秩性。对于评分矩阵中存在的结构化行噪声，可利用矩阵$L_{2,1}$范数对其进行解析。在剔除攻击评分之后，再进行评分预测，将有效提高推荐精度，此时，基于属性优化矩阵补全的托攻击检测模型为：

[0021] $$\min_{X,Z\in\mathbb{R}^{m\times n}}\|X\|_{*}+\lambda\|Z\|_{2,1}\ \text{s.t.}\quad \mathrm{P}_{\Omega}(R)=\mathrm{P}_{\Omega}(X+Z) \tag{5}$$

[0022] 其中，$\|Z\|_{2,1}=\sum_{i=1}^{m}\sqrt{\sum_{j=1}^{n}z_{i,j}^{2}}$为矩阵$L_{2,1}$范数。

[0023] 此外，用户往往会出于情绪波动而打出不太精确的评分，为了平滑评分的这种细微波动，可引入矩阵的Frobenius范数，将式(5)改写成罚函数形式：

[0024] $$\min_{X,Z\in\mathbb{R}^{m\times n}}\|X\|_{*}+\lambda\|Z\|_{2,1}+\frac{\beta}{2}\|\mathrm{P}_{\Omega}(X+Z-R)\|_{F}^{2} \tag{6}$$

[0025] 其中，$\|X\|_{F}=\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}|x_{i,j}|^{2}}$为矩阵的Frobenius范数。

[0026] 正如之前所叙述的，评分矩阵通常是稀疏矩阵，能够收到的评分数远小于评分矩阵元素个数。在MovieLens的ml-20m数据集中，138493名用户对于27278部电影仅有20000263个评分；在EachMovie数据集中，72916个用户对1628部电影仅进行了2811983次评分。基于稀疏数据求取高维未知矩阵很难确保求解的准确性。为解决数据稀疏性问题[16]，我们考虑引入属性特征信息，将简单的评分矩阵R细化为三个矩阵的乘积R＝A^PXB，其中，A和B分别是用户特征矩阵和项目特征矩阵，$A \in \mathbb{R}^{k\times m}$，$B \in \mathbb{R}^{k\times n}$，矩阵列向量分别是用户特征向量和项目特征向量，即量化了的属性信息；X矩阵是低维未知矩阵，$X \in \mathbb{R}^{k\times k}$。此时，托攻击检测模型可改为：

[0027] $$\min_{X\in\mathbb{R}^{k\times k},Z\in\mathbb{R}^{m\times n}} \|A^TXB\|_* + \lambda\|Z\|_{2,1} + \frac{\beta}{2}\|\mathrm{P}_\Omega(A^TXB+Z-R)\|_F^2 \quad (7)$$

[0028] 然而，由于rank(A^TXB)≤min{rank(A)，rank(B)}，即只要特征矩阵A与B其中之一的秩足够小，比如A或B的维度过小，包含信息过少等，则无论X矩阵取何值，乘积A^TXB的秩都必然会更小，将直接满足低秩条件。为避免这种解的任意性，我们仅对待求变量X进行低秩约束。综上所述，基于属性优化矩阵补全的托攻击检测模型为：

[0029] $$\min_{X\in\mathbb{R}^{k\times k},Z\in\mathbb{R}^{m\times n}} \|X\|_* + \lambda\|Z\|_{2,1} + \frac{\beta}{2}\|\mathrm{P}_\Omega(A^TXB+Z-R)\|_F^2 \quad (8)$$

[0030] 其中，$\|X\|_*$和$\|Z\|_{2,1}$分别表示对X矩阵进行低秩性约束以及对Z矩阵进行行稀疏性约束，$\|\mathrm{P}_\Omega(A^TXB+Z-R)\|_F^2$是为了平滑评分细微波动的正则化项，λ，β为可调参数，$\Omega \subseteq \{1,2\cdots m\}\times\{1,2\cdots n\}$表示评分矩阵中已反馈的评分元素下标集合。

[0031] 4)采用分块坐标下降算法迭代求解公式(8)中的基于属性优化矩阵补全的托攻击检测模型，得到结构化行噪声矩阵Z。具体步骤如下：

[0032] 步骤4.1)：在公式(8)中引入变量C并令C＝A^TXB，将公式转换为：

[0033] $$\begin{cases}\min\limits_{X\in\mathbb{R}^{k\times k},C,Z\in\mathbb{R}^{m\times n}} \|X\|_* + \lambda\|Z\|_{2,1} + \frac{\beta}{2}\|\mathrm{P}_\Omega(C+Z-R)\|_F^2 \\ s.t.\ C - A^TXB = 0\end{cases} \quad (9)$$

[0034] 利用Frobenius范数将其进一步改写成相应的罚函数形式：

[0035] $$\min_{X\in\mathbb{R}^{k\times k},C,Z\in\mathbb{R}^{m\times n}} = \|X\|_* + \lambda\|Z\|_{2,1} + \frac{\beta}{2}\|\mathrm{P}_\Omega(C+Z-R)\|_F^2 + \frac{\rho}{2}\|C-A^TXB\|_F^2 \quad (10)$$

[0036] 步骤4.2)：采用分块坐标下降算法求解罚函数问题(10)，不妨令：

[0037] $$\mathrm{L}_\rho(X,Z,C) = \|X\|_* + \lambda\|Z\|_{2,1} + \frac{\beta}{2}\|\mathrm{P}_\Omega(C+Z-R)\|_F^2 + \frac{\rho}{2}\|C-A^TXB\|_F^2 \quad (11)$$

[0038] 则可对各个变量做如下的迭代更新：

[0039] $$\begin{cases}X^{k+1} = \arg\min\limits_{X\in\mathbb{R}^{k\times k}} \mathrm{L}_\rho(X,Z^k,C^k) \\ Z^{k+1} = \arg\min\limits_{Z\in\mathbb{R}^{m\times n}} \mathrm{L}_\rho(X^{k+1},Z,C^k) \\ C^{k+1} = \arg\min\limits_{C\in\mathbb{R}^{m\times n}} \mathrm{L}_\rho(X^{k+1},Z^{k+1},C)\end{cases} \quad (12)$$

[0040] 步骤4.3)：采用近邻前向后向分裂技术对其式(12)中的子问题进行优化求解，各变量迭代更新公式如下：

[0041] 步骤4.3.1)X的迭代更新公式求解如下：

[0042] 采用近邻前向后向分裂(proximal forward backward splitting,PFBS)技术对其进行优化求解,令:

[0043] $$\begin{cases} F_1(X) = \|X\|_* \\ F_2(X) = \frac{\rho}{2}\|C - A^T XB\|_F^2 \end{cases} \quad (13)$$

[0044] 其中函数$F_2(X)$的导数为:

[0045] $$\nabla F_2(X) = \rho(AA^T XBB^T - ACB^T) \quad (14)$$

[0046] 为简化公式,方便求解,引入一个新变量Y,令:

[0047] $$Y^{k+1} = X^k - \delta_X \nabla F_2(X^k) = X^k - \delta_X \rho(AA^T XBB^T - AC^k B^T) \quad (15)$$

[0048] 其中,根据PFBS规则,引入参数δ_X用于对X进行迭代更新。则:

[0049] $$X^{k+1} = arg \ \ min_{X\in\mathbb{R}^{k\times k}} \frac{1}{2}\|X - Y^{k+1}\|_F^2 + \delta_X\|X\|_* \quad (16)$$

[0050] 对于矩阵$Y \in \mathbb{R}^{k\times k}$和常数$\tau>0$,有:

[0051] $$D_\tau(Y) = arg \ \ min_{X\in\mathbb{R}^{k\times k}} \left\{\frac{1}{2}\|X - Y\|_F^2 + \tau\|X\|_*\right\} \quad (17)$$

[0052] 其中$D_\tau(Y)$是奇异值阈值算子,若矩阵Y的奇异值分解为:$Y = U\Sigma V^T$,则τ所对应的奇异值阈值算子为$D_\tau(Y) = U * [\mathrm{sign}(Y) \circ \max(|Y| - \tau, 0)] * V^T$,其中符号“$\circ$”是Hadamard积,表示两矩阵对应元素相乘。

[0053] 因此,X的更新可按如下步骤迭代进行:

[0054] $$\begin{cases} Y^{k+1} = X^k - \delta_X \rho(AA^T XBB^T - AC^k B^T) \\ X^{k+1} = D_{\delta_X}(Y^{k+1}) \end{cases} \quad (18)$$

[0055] 在PFBS中,参数δ需满足$\mathbf{0 < \delta < \frac{2}{L_f}}$。通过计算,$L_{f\_X} = \sigma_{max}(BB^T) * \sigma_{max}(AA^T)$,故参数$\delta_X$需满足$\mathbf{0 < \delta_X < \frac{2}{\sigma_{max}(BB^T) * \sigma_{max}(AA^T)}}$,在实验中,我们取$\mathbf{\delta_X = \frac{1}{\sigma_{max}(BB^T) * \sigma_{max}(AA^T)}}$。

[0056] 步骤4.3.2)Z的迭代更新公式求解如下,令:

[0057] $$\mathbf{F_2(Z) = \frac{\beta}{2}\|P_\Omega(C + Z - R)\|_F^2} \quad (19)$$

[0058] 其导数为:

[0059] $$\mathbf{\nabla F_2(Z) = \beta P_\Omega(C + Z - R)} \quad (20)$$

[0060] 为简化公式,方便求解,引入一个新变量V,令:

[0061] $$\mathbf{V^{k+1} = Z^k - \delta_Z \nabla F_2(Z^k) = Z^k - \delta_Z \beta P_\Omega(C^k + Z^k - R)} \quad (21)$$

[0062] 则:

[0063] $$\mathbf{Z^{k+1} = arg \ \ min_{Z\in\mathbb{R}^{m\times n}} \frac{1}{2}\|Z - V^{k+1}\|_F^2 + \delta_Z \lambda \|Z\|_{2,1}} \quad (22)$$

[0064] 对于Z矩阵内每一行:

[0065] $$\mathbf{(Z^{k+1})^{(i)} = max\left\{1 - \frac{\delta_Z \lambda}{\|(V^{k+1})^{(i)}\|_2}, 0\right\} * (V^{k+1})^{(i)} \qquad i = 1, 2, \cdots, m} \quad (23)$$

[0066] 因此，Z的更新可按照如下步骤迭代进行：

[0067] $$\begin{cases}\mathbf{V^{k+1}=Z^{k}-\delta_{Z}\beta P_{\Omega}(C^{k}+Z^{k}-R)}\\ \mathbf{(Z^{k+1})^{(i)}=max\left\{1-\frac{\delta_{Z}\lambda}{\|(V^{k+1})^{(i)}\|_{2}},0\right\}*(V^{k+1})^{(i)}i=1,2,\cdots,m}\end{cases}\quad(24)$$

[0068] 类似的，通过计算，$L_f\_Z=\beta$，故参数δ_Z需满足$\mathbf{0<\delta_Z<\frac{2}{\beta}}$。，在实验中，我们取$\delta_Z=\frac{1}{\beta}$。

[0069] 步骤4.3.3)对于变量C的迭代更新公式求解，令：

[0070] $$F(C)=\frac{\beta}{2}\|P_{\Omega}(C+Z-R)\|_F^2+\frac{\rho}{2}\|C-A^TXB\|_F^2\quad(25)$$

[0071] 即：$C^{k+1}=\arg\min_{C\in\mathbb{R}^{m\times n}}F(C)$（26）

[0072] 此时有：

[0073] $$\nabla F(C)=\beta P_{\Omega}(C+Z-R)+\rho(C-A^TXB)\quad(27)$$

[0074] 令$\nabla F(C)=0$，可求得C的迭代更新公式：

[0075] $C^{l+1}=4(\rho+\beta)A^TX^{l+1}B+\beta P_{\Omega}(R-Z^{k+1}-A^TX^{l+1}B)]/(\rho+\beta)$ (28)

[0076] 至此，我们可得到基于属性优化矩阵补全的托攻击检测模型的求解步骤，并求得噪声矩阵Z：

[0077] 5)根据结构化行噪声矩阵Z从用户-项目评分矩阵中剔除托攻击评分；

[0078] 6)采用传统推荐算法对修正后的用户-项目评分矩阵中的缺失值进行评分预测，求得完整的用户-项目评分矩阵，基于完整的用户-项目评分矩阵中的预测评分对目标用户进行项目推荐。

[0079] 有益效果：本发明针对个性化推荐系统面临的托攻击问题，从矩阵补全角度出发，将托攻击用户评分建模为干扰了自然状态下评分矩阵近似低秩性的结构化行噪声，并利用范数正则化对这些托攻击评分进行解析，本发明在攻击检测过程中融入用户与物品的属性特征信息，提出了基于属性优化矩阵补全的托攻击检测模型，提高了攻击检测精度。最后，本发明基于所提出的基于属性优化矩阵补全的托攻击检测模型，改进了传统的不具备抗托攻击能力的推荐算法，提出了一种基于属性优化矩阵补全的抗托攻击个性化推荐算法。实验结果证明，在托攻击干扰下，本发明所提供的推荐算法依旧可以产生鲁棒的评分预测结果，在推荐系统的实际应用中具有现实意义。

附图说明

[0080] 图1是本发明提供的基于矩阵补全的抗托攻击推荐算法的流程示意图。

具体实施方式

[0081] 一种基于矩阵补全的抗托攻击推荐算法，包括如下步骤：

[0082] 1)建立用户-项目评分矩阵：

[0083] m名用户构成用户集合$U=\{u_1,u_2,\cdots u_m\}$，n件项目构成项目集合$I=\{i_1,i_2,\cdots i_n\}$，用户-项目评分矩阵可表示为$R\in\mathbb{R}^{m\times n}$：

[0084] $$R=\begin{bmatrix} ? & ? & ? \\ * & r_{i,j} & * \\ * & ? & ? \end{bmatrix} \quad (29)$$

[0085] 其中，用户u对项目i的评分记作$r_{i,j}$，“*”表示已知评分，“?”表示未知评分。

[0086] 2)建立推荐系统模型：

[0087] 推荐系统问题可利用低秩矩阵补全技术进行评分预测。用R表示当前观察到的评分矩阵，则推荐系统问题可建模为：

[0088] $$\min_{X\in\mathbb{R}^{m\times n}}\|X\|_* \quad s.t.\ \ \mathrm{P}_{\Omega}(R)=\mathrm{P}_{\Omega}(X) \quad (30)$$

[0089] 其中Ω集合表示评分矩阵中已收到评分的元素下标集合，$\Omega\subseteq\{1,2\cdots m\}\times\{1,2\cdots n\}$，X矩阵是低维未知矩阵，$\|X\|_*=\sum_{i=1}^{\min(m,n)}\sigma_i$为矩阵核范数，$\sigma_i$为矩阵X的第i大奇异值，$X\in\mathbb{R}^{k\times k}$ $\mathrm{P}_{\Omega}(\cdot)$是投影算子，表示当元素下标(i,j)∈Ω时，得到对应位置采样元素：

[0090] $$[\mathrm{P}_{\Omega}(R)]_{i,j}=\begin{cases} r_{i,j} & (i,j)\in\Omega \\ 0 & (i,j)\notin\Omega \end{cases} \quad (31)$$

[0091] 3)根据步骤2)建立基于属性优化矩阵补全的托攻击检测模型：

[0092] 对于用户-项目评分评分矩阵中存在的结构化行噪声，即托攻击评分，利用矩阵$L_{2,1}$范数对其进行解析。在剔除攻击评分之后，再进行评分预测，将有效提高推荐精度，此时，基于属性优化矩阵补全的托攻击检测模型为：

[0093] $$\min_{X\in\mathbb{R}^{k\times k},Z\in\mathbb{R}^{m\times n}}\|X\|_*+\lambda\|Z\|_{2,1}+\frac{\beta}{2}\|\mathrm{P}_{\Omega}(A^TXB+Z-R)\|_F^2 \quad (32)$$

[0094] 其中，$\|X\|_*$和$\|Z\|_{2,1}$分别表示对X矩阵进行低秩性约束以及对Z矩阵进行行稀疏性约束，$\|\mathrm{P}_{\Omega}(A^TXB+Z-R)\|_F^2$是为了平滑评分细微波动的正则化项，λ，β为可调参数，$\Omega\subseteq\{1,2\cdots m\}\times\{1,2\cdots n\}$表示评分矩阵中已反馈的评分元素下标集合。

[0095] 4)采用分块坐标下降算法迭代求解公式(32)中的基于属性优化矩阵补全的托攻击检测模型，得到结构化行噪声矩阵Z。具体步骤如下：

[0096] 步骤4.1)：在公式(32)中引入变量C并令$C=A^TXB$，利用Frobenius范数将其进一步改写成相应的罚函数形式，公式转换为：

[0097] $$\min_{X\in\mathbb{R}^{k\times k},C,Z\in\mathbb{R}^{m\times n}}=\|X\|_*+\lambda\|Z\|_{2,1}+\frac{\beta}{2}\|\mathrm{P}_{\Omega}(C+Z-R)\|_F^2+\frac{\rho}{2}\|C-A^TXB\|_F^2 \quad (33)$$

[0098] 步骤4.2)：采用分块坐标下降算法求解罚函数问题(33)，不妨令：

[0099] $$\mathrm{L}_{\rho}(X,Z,C)=\|X\|_*+\lambda\|Z\|_{2,1}+\frac{\beta}{2}\|\mathrm{P}_{\Omega}(C+Z-R)\|_F^2+\frac{\rho}{2}\|C-A^TXB\|_F^2 \quad (34)$$

[0100] 初始化变量X、Z、C，令变量$X^0=0$，$Z^0=0$，$C^0=0$，则可对各个变量做如下的迭代更新：

[0101] $$\begin{cases} X^{k+1}=\arg\min_{X\in\mathbb{R}^{k\times k}}\mathrm{L}_{\rho}(X,Z^k,C^k) \\ Z^{k+1}=\arg\min_{Z\in\mathbb{R}^{m\times n}}\mathrm{L}_{\rho}(X^{k+1},Z,C^k) \\ C^{k+1}=\arg\min_{C\in\mathbb{R}^{m\times n}}\mathrm{L}_{\rho}(X^{k+1},Z^{k+1},C) \end{cases} \quad (35)$$

[0102] 步骤4.3)：采用近邻前向后向分裂技术对其式(35)进行优化求解，各变量迭代更

新公式如下：

[0103] X的更新按照如下公式(36)迭代进行：

[0104] $$\begin{cases} Y^{k+1} = X^k - \delta_X \rho(AA^T XBB^T - AC^k B^T) \\ X^{k+1} = \mathrm{D}_{\delta_X}(Y^{k+1}) \end{cases} \quad (36)$$

[0105] 其中，参数δ_X需满足$0 < \delta_X < \frac{2}{\sigma_{\max}(BB^T)*\sigma_{\max}(AA^T)}$，在实验中，我们取$\delta_X = \frac{1}{\sigma_{\max}(BB^T)*\sigma_{\max}(AA^T)}$。

[0106] 类似于X的更新过程Z的更新按照如下公式(37)迭代进行：

[0107] $$\begin{cases} V^{k+1} = Z^k - \delta_Z \beta \mathrm{P}_\Omega(C^k + Z^k - R) \\ (Z^{k+1})^{(i)} = \max\left\{1 - \frac{\delta_Z \lambda}{\left\|(V^{k+1})^{(i)}\right\|_2}, 0\right\} * (V^{k+1})^{(i)} \qquad i = 1,2,\cdots,m \end{cases} \quad (37)$$

[0108] 其中，参数δ_Z需满足$0 < \delta_Z < \frac{2}{\beta}$，在实验中，我们取$\delta_Z = \frac{1}{\beta}$。

[0109] C的更新按照如下公式(38)迭代进行：

[0110] $C^{k+1} = [(\rho+\beta)A^T X^{k+1} B + \beta P_\Omega(R - Z^{k+1} - A^T X^{k+1} B)] / (\rho+\beta)$ (38)

[0111] 5)根据步骤4)中计算得到的结构化行噪声矩阵Z从用户-项目矩阵中剔除托攻击评分；

[0112] 6)采用传统推荐算法对修正后用户-项目评分矩阵进行缺失评分预测，求得完整的用户-项目评分矩阵，基于完整的用户-项目评分矩阵中的预测评分对目标用户进行项目推荐。

[0113] 至此，我们可整理得到基于矩阵补全的抗托攻击个性化推荐的算法步骤：

[0114]

算法 1：基于矩阵补全的抗托攻击推荐算法

输入：用户与物品属性特征矩阵 A，B，采样评分矩阵 R，采样下标集合Ω，参数β,ρ,λ以及迭代次数 Maxiter。

输出：预测评分矩阵 M。

```
INITIALIZE X^0 = 0, Z^0 = 0, C^0 = 0;
FOR k=0 to Maxiter
    根据式(8)更新 X;
    根据式(9)更新 Z;
    根据式(10)更新 C;
END FOR
RETURN Z;
根据结构化行噪声矩阵 Z 从用户-项目评分矩阵中剔除托攻击评分；
采用传统推荐算法对修正后的用户-项目评分矩阵进行评分预测，求得预测评分矩阵，
基于预测评分对目标用户进行项目推荐
```

[0115] 以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员所具备的知识范围内，在不脱离本发明宗旨的前提下，可以进行若干改进和润饰，这些改

进和润饰也应视为本发明的保护范围内。

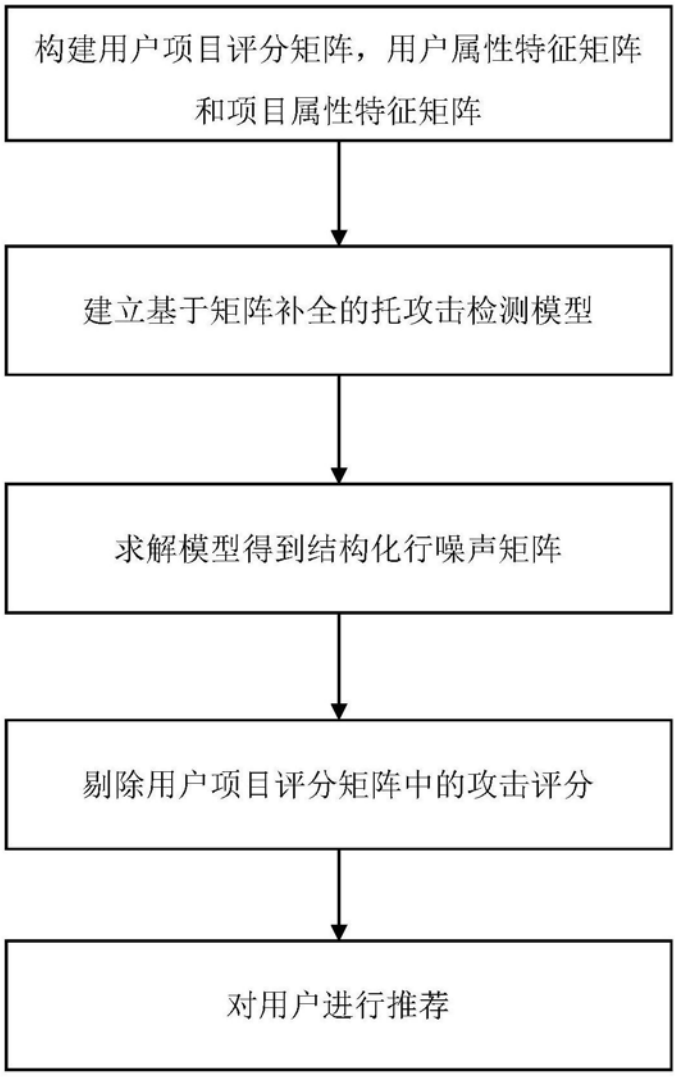

构建用户项目评分矩阵，用户属性特征矩阵和项目属性特征矩阵
建立基于矩阵补全的托攻击检测模型
求解模型得到结构化行噪声矩阵
剔除用户项目评分矩阵中的攻击评分
对用户进行推荐

图1