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

李 聪 [1] 骆志刚 [1]

摘 要 托攻击是协同过滤推荐系统面临的重大安全威胁. 研究可抵御托攻击的鲁棒协同推荐技术已成为目前的重要课题. 本文在引入用户嫌疑性评估策略的基础上, 通过将用户嫌疑性及项类属等元信息与贝叶斯概率矩阵分解模型相融合, 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 (Metadata-enhanced variational Bayesian matrix factorization, MVBMF), 并设计了相应的模型增量学习策略. 实验表明, 与现有推荐模型相比, 这种模型具备更强的攻击耐受力, 能够有效提高推荐系统的鲁棒性.

关键词 协同过滤, 托攻击, 矩阵分解, 变分推断, 鲁棒线性回归

DOI 10.3724/SP.J.1004.2011.01067

A Metadata-enhanced Variational Bayesian Matrix Factorization Model for Robust Collaborative Recommendation

LI Cong[1] LUO Zhi-Gang[1]

Abstract Shilling attacks pose a significant threat to the security of collaborative filtering recommender systems. It has come to be an important task to develop the attack-resistant techniques for robust collaborative recommendation. Through evaluating the user suspiciousness, and further integrating Bayesian probabilistic matrix factorization model with the metadata including user suspiciousness as well as item types, this paper proposes the metadata-enhanced variational Bayesian matrix factorization (MVBMF) model for robust collaborative recommendation, and designs the corresponding incremental learning strategy. Experimental results show that comparing with the existed recommendation models, this model has stronger resistibility and can effectively improve the robustness of recommender systems.

Key words Collaborative filtering, shilling attacks, matrix factorization, variational inference, robust linear regression

协同过滤 (Collaborative filtering) 推荐技术在信息检索领域具有广阔的应用前景[1], 它能为终端用户提供个性化的信息服务, 有效缓解了信息过载 (Information overload) 问题. 目前, Amazon[1], eBay[2], NetFlix[3] 等大型商业站点都应用了此项技术.

协同过滤推荐系统 (以下简称推荐系统) 中的实体集包括用户集 U ($U = \{user_i | i = 1, \cdots, I\}$) 与项集 I ($I = \{item_j | j = 1, \cdots, J\}$), 项通指电影、音乐、书籍等检索对象. 推荐系统通过分析用户历史行为, 可向特定用户推荐其所需信息. 用户的历史行为记录为评分矩阵 (Rating matrix) $R_{I\times J}$, 其第 i 行第 j 列元素 R_{ij} 是 $user_i$ 对 $item_j$ 的评分 $\mathrm{R}(user_i, item_j)$, 代表偏好程度. 由于用户一般只关注系统中少数的项, 导致了 $R_{I\times J}$ 中大量评分的缺失. 协同推荐的任务正是预测缺失评分, 据此推荐用户的潜在偏好项.

准确性与稳定性是推荐系统鲁棒性的两个重要方面[2]. 准确性衡量评分预测值与真实值之间的吻合程度. 稳定性衡量面临外部扰动时推荐结果的变动程度. 本文中推荐系统的外部干扰主要指自然与人为的评分噪声[3]. 自然噪声源于用户在心理或环境等因素影响下无意识引入的评分偏差, 人为噪声则来自一种有意识的恶意行为 — 托攻击 (Shilling attacks)[4]. 攻击者向推荐系统注入虚假评分, 从而操纵推荐结果, 牟取不当利益. 托攻击会严重损害推荐系统的鲁棒性.

推荐系统的鲁棒性由底层推荐算法决定. 推荐算法一般分为基于存储的 (Memory-based), 基于模型的 (Model-based) 与混合 (Hybrid) 算法. 文献 [5] 系统地介绍了每类中的经典算法. 现有推荐算法普遍致力于提高推荐准确性, 却忽视了算法本身对托攻击的易感性, 因此, 推荐系统鲁棒性无法得到有效保障. 鲁棒协同推荐技术已成为目前学界研究的热点与难点.

现有的鲁棒协同推荐技术主要运用两种托攻击防御策略: 1) 在推荐算法运行之前探测并删除攻击者; 2) 依靠推荐算法内在的健壮性平滑托攻击的不

收稿日期 2010-11-29 录用日期 2011-03-31
Manuscript received November 29, 2010; accepted March 31, 2011

1. 国防科学技术大学计算机学院 长沙 410073
1. School of Computer, National University of Defense Technology, Changsha 410073

[1] http://www.amazon.com/
[2] http://www.ebay.com/
[3] http://www.netflix.com/

良影响. 然而, 这些策略存在难以回避的局限: 策略 1) 依赖于探测技术的准确性, 可能会误删非攻击者; 策略 2) 只适用于低强度攻击, 因为中高强度攻击会扭转推荐系统的 “主流意见”.

鉴于此, 本文提出了元信息增强变分贝叶斯矩阵分解 (Metadata-enhanced variational Bayesian matrix factorization, MVBMF) 模型, 综合了两种策略的优势. 主要思路包括: 1) 利用概率潜在语义分析 (Probabilistic latent semantic analysis, PLSA) 方法分析用户评分行为, 在此基础上提出用户嫌疑性的评估策略; 2) 将用户嫌疑性以及项类属信息分别以模型参数和 Logistic 回归方式导入贝叶斯概率矩阵分解 (Bayesian probabilistic matrix factorization, BPMF) 模型, 实现对评分噪声的抑制, 并利用变分期望最大化 (Variational expectation maximization, Variational EM) 算法学习模型变量; 3) 基于鲁棒线性回归技术, 设计模型增量学习策略, 降低对模型重构的需求.

实验表明 MVBMF 模型有效克服了现有鲁棒协同推荐技术的局限, 具备较强的攻击耐受力, 在强弱泛化情形下均确保了推荐系统的鲁棒性.

1 推荐系统的托攻击及相关研究

由于推荐系统的开放性及交互式特点, 攻击者能以极低代价向系统中注入虚假评分, 轻易改变推荐结果. 依攻击目的, 托攻击可划为两类[6]: 提高目标项的评价, 称为推攻击 (Push attack); 降低目标项的评价, 称为核攻击 (Nuke attack). 实际情况中推攻击更为普遍.

1.1 推荐系统的托攻击

攻击者的所有评分构成攻击概貌 (Attack profile), 它是一个 n 维向量, n 是系统中项的个数. 图 1 为攻击概貌的形式结构.

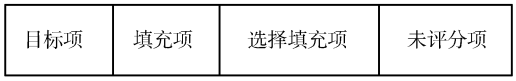


图 1 攻击概貌的形式结构

Fig. 1 General framework of attack profiles

目标项 (Target item) 在推攻击时设为最高评分 $r_{\max}$, 在核攻击时设为最低评分 $r_{\min}$. 未评分项 (Unrated items) 的评分设为 $\varnothing$, 即不予评分. 攻击概貌构建自不同的攻击模型, 随机攻击 (Random attack)、均值攻击 (Average attack) 和流行攻击 (Bandwagon attack)[7] 是三种典型的攻击模型, 三者的差异主要体现在填充项 (Filler items) 与选择填充项 (Selected items) 的选取与评分策略上. 定义填充率 (Filler size)$p^{fill} = |\{\textit{填充项}\}|/n$, 攻击强度 (Attack size)$p^{att} = |\{\textit{攻击者}\}|/|\{\textit{真实用户}\}|$.

1.2 鲁棒协同推荐技术的相关研究

文献 [8] 利用概貌效用 (Profile utility) 改进了基于 Pearson 相关性的 K–最近邻选取策略, 阻止攻击者进入目标用户的最近邻. 类似地, 文献 [9] 将显著性加权 (Significance weighting) 应用于最近邻选取. 然而这两种推荐算法的鲁棒性并不理想. 文献 [10] 表明挖掘关联规则可以增强鲁棒性, 但会降低推荐覆盖率. 文献 [11] 的鲁棒矩阵分解 (Robust matrix factorization, RMF) 算法利用 M–估计子 (M-estimator)[12] 对离群点的容忍性, 一定程度抑制了评分噪声的影响. 文献 [13] 提出的变量选择–奇异值分解 (Singular value decomposition using variable-selection, VarSelect SVD) 算法基于主成分分析 (Principal component analysis, PCA) 方法探测并标识可疑用户, 限制其对推荐模型构建过程的干扰, 鲁棒性显著优于 RMF 算法.

2 元信息增强变分贝叶斯矩阵分解模型

推荐算法普遍将评分矩阵作为唯一信息源, 然而托攻击会损害评分矩阵的可信度, 这是推荐系统对托攻击易感的根本原因. 如果推荐算法能吸纳攻击者难以篡改的系统实体元信息, 比如用户与项的描述性信息, 势必会增强推荐系统的鲁棒性[7]. 此即 MVBMF 模型的设计思想.

推荐系统中, 项的元信息 (名称、类型、产地等) 由系统负责维护, 真实性较高, 可直接加以利用. 而用户的元信息 (年龄, 性别, 职业等) 由用户在注册时填写, 利用价值有限, 因为无论是否攻击者, 都有提供虚假个人隐私信息的理由与动机. 不过, 用户的评分行为暗含了一种客观存在的用户元信息 — 嫌疑性, 即成为攻击者的可能性. 用户嫌疑性信息将是确保 MVBMF 模型鲁棒性的重要因素. 为揭示这种特殊元信息, 本文提出了基于 PLSA 的用户嫌疑性评估策略.

2.1 用户嫌疑性的评估

PLSA 是一种能揭示共现数据 (Co-occurring data) 间潜在语义关系的贝叶斯网络模型[14]. 推荐系统中, 共现数据 $(user, item)$ 可视为二元随机变量 $(User, Item)$ 的抽样值. PLSA 假设任一抽样值 $(user, item)$ 都与一隐含类属变量 s 相关联, $s \in S = \{s_h | h = 1, \cdots, H\}$. 且给定 s 时, $user$ 与 $item$ 条件独立, 即 $p(user, item|s) = p(user|s)p(item|s)$, 此时有:

$$p(user, item) = \sum_{h=1}^{H} p(s_h)p(user|s_h)p(item|s_h)$$

所有共现数据的对数似然为

$$L(U, I) = \sum_{\substack{user\in U\\ item\in I}} \mathrm{R}(user, item) \ln p(user, item)$$

$p(s_h), p(user|s_h), p(item|s_h)$ 作为 PLSA 的参数, 其最大似然估计可用 EM 算法求解[14], 主要包括以下两步:

期望步 (E-step):

$$p(s_h|user, item) \propto p(s_h)p(user|s_h)p(item|s_h)$$

最大化步 (M-step):

$$p(s_h) \propto \sum_{\substack{user\in U\\ item\in I}} \mathrm{R}(user, item)p(s_h|user, item)$$

$$p(user|s_h) \propto \sum_{item\in I} \mathrm{R}(user, item)p(s_h|user, item)$$

$$p(item|s_h) \propto \sum_{user\in U} \mathrm{R}(user, item)p(s_h|user, item)$$

参数初始化后迭代上述两步至收敛, 即可得参数的局部最优解.

若存在托攻击, 则攻击类必然会被某个类 s^{att} 所解释. 同时, 攻击者独特的评分行为, 即评分项 (填充项) 的随机选取, 导致了攻击者兴趣点的极端分散[15]. 因此, 本文认为攻击类在选取评分项时的不确定性 — 熵 (Entropy) 必然超越所有真实用户类. 形式化地, 设随机变量 $Q^s \sim p(item|s)$, 则可定位攻击类:

$$s^{att} = \arg\max_s \mathrm{H}[Q^s]$$

其中, 熵函数 $\mathrm{H}[x] = -\sum_x p(x) \ln p(x)$. 令 $user_i$ 的嫌疑性 θ_i 等于 $user_i$ 隶属攻击类的概率:

$$\theta_i = p(s^{att}|user_i) \propto p(user_i|s^{att})p(s^{att})$$

实验表明 θ 能够良好地指示用户的嫌疑性. 例如, 将 $p^{att} = 10\,\%$, $p^{fill} = 9\,\%$ 的均值攻击注入 MovieLens100K 数据集[4] (实验部分介绍), 此时, θ 的分布如图 2. 易见攻击用户的 θ 值显著大于真实用户, 而后者基本集中于 0 附近, 区分度明显.

为避免 EM 算法收敛至较差的局部极值, 本文采取一种启发式策略: 重复多次 EM 学习过程, 利用攻击类熵值最大的那次迭代结果计算 θ.

[4]http://www.grouplens.org/node/73

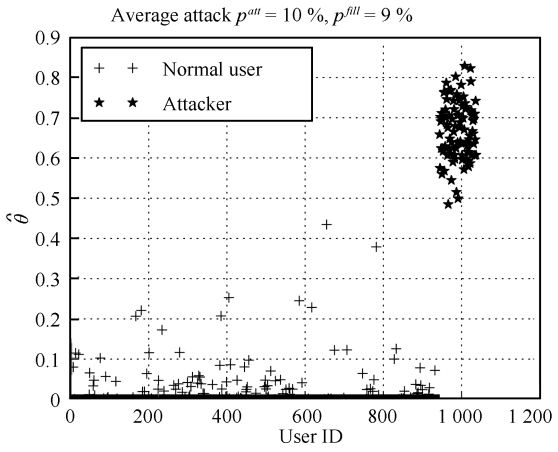


图 2　用户嫌疑性

Fig. 2　User suspiciousness

2.2　MVBMF 的形式化描述

本质上, MVBMF 是一种矩阵分解模型. 矩阵分解是协同推荐问题常见且有效的解决方案, 典型地如基于 EM 的 SVD[16] (本文暂称其为 EMSVD) 与 BPMF[17]. MVBMF 继承了 BPMF 的基础架构, 并根据整合元信息的需要进行相应扩展.

BPMF 属于概率产生模型 (Probabilistic generative model), 它以贝叶斯推断的观点来看待矩阵分解问题, 对模型变量作出概率分布假设. 图 3 是 BPMF 的概率图模型 (又称贝叶斯网络). 随机变量 R_{ij}, $\boldsymbol{U}_i$, $\boldsymbol{V}_j$, $\boldsymbol{\mu}_u$, Λ_u, $\boldsymbol{\mu}_v$, Λ_v 分别符合以下分布:

$$p(R_{ij}|\boldsymbol{U}_i, \boldsymbol{V}_j) = \mathrm{N}(R_{ij}|\boldsymbol{U}_i^{\mathrm{T}}\boldsymbol{V}_j, \sigma^2)^{I_{ij}}$$

$$p(\boldsymbol{U}_i|\boldsymbol{\mu}_u, \Lambda_u) = \mathrm{N}(\boldsymbol{U}_i|\boldsymbol{\mu}_u, \Lambda_u^{-1})$$

$$p(\boldsymbol{V}_j|\boldsymbol{\mu}_v, \Lambda_v) = \mathrm{N}(\boldsymbol{V}_j|\boldsymbol{\mu}_v, \Lambda_v^{-1})$$

$$p(Y_t|\kappa) = \mathrm{N}(\boldsymbol{\mu}_t|\boldsymbol{\mu}_0, (\beta\Lambda_t)^{-1})\mathcal{W}(\Lambda_t|\nu_0, \Lambda_0)$$

其中, $\kappa = \{\boldsymbol{\mu}_0, \nu_0, \beta, \Lambda_0\}, Y_t = \{\boldsymbol{\mu}_t, \Lambda_t\}$, $t \in \{u, v\}$. I_{ij} 表示 R_{ij} 是否缺失, 缺失为 0, 否则为 1. 模型参数 Y_t 的先验为 Gaussian–Wishart 分布, 先验分布的引入有利于抑制过度拟合. $\boldsymbol{U}_i$ 和 $\boldsymbol{V}_j$ 称作特征向量 (Feature vector), 分别代表 $user_i$ 的偏好特征和 $item_j$ 的类属特征. 然而, BPMF 无法确保后验分布 $P(\boldsymbol{U}, \boldsymbol{V}|\boldsymbol{R})$ 反映实体真实特征, 因为先验信息 $\boldsymbol{R}$ 可能存在噪声. MVBMF 则通过纳入用户与项的元信息, 削弱了评分噪声对模型变量后验的不利影响.

图 4 是 MVBMF 的概率图模型, 各随机变量符合下列分布:

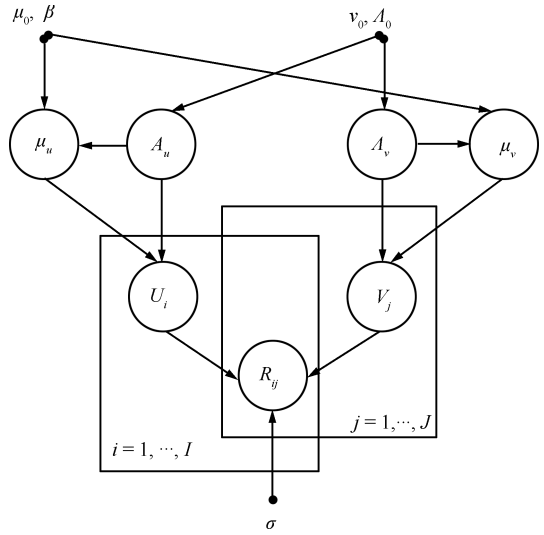


图 3 贝叶斯概率矩阵分解的图模型

Fig. 3 Graphical model for Bayesian probabilistic matrix factorization (BPMF)

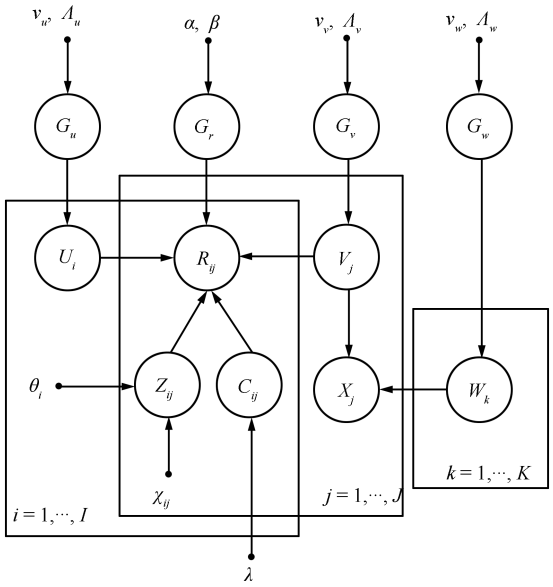


图 4 元信息增强变分贝叶斯矩阵分解的图模型

Fig. 4 Graphical model for metadata-enhanced variational Bayesian matrix factorization (MVBMF)

$$p(G_t|\nu_t, \Lambda_t) = \mathcal{W}(G_t|\nu_t, \Lambda_t) \tag{1}$$

$$p(G_r|\alpha, \beta) = \mathrm{Gam}(G_r|\alpha, \beta) \tag{2}$$

$$p(\boldsymbol{C}|\lambda) = \prod_{i,j} \mathrm{Gam}\left(C_{ij}|\frac{\lambda}{2}, \frac{\lambda}{2}\right) \tag{3}$$

$$p(\boldsymbol{Z}|\Theta, \Upsilon) = \prod_{i,j} \mathrm{Bern}(Z_{ij}|\theta_i \cdot \chi_{ij}) \tag{4}$$

$$p(\boldsymbol{U}|G_u) = \prod_i \mathrm{N}(\boldsymbol{U}_i|\boldsymbol{0}, G_u^{-1}) \tag{5}$$

$$p(\boldsymbol{V}|G_v) = \prod_j \mathrm{N}(\boldsymbol{V}_j|\boldsymbol{0}, G_v^{-1}) \tag{6}$$

$$p(\boldsymbol{W}|G_w) = \prod_k \mathrm{N}(\boldsymbol{W}_k|\boldsymbol{0}, G_w^{-1}) \tag{7}$$

$$p(\boldsymbol{X}|\boldsymbol{V}, \boldsymbol{W}) = \prod_{j,k} \mathrm{Bern}(X_{jk}|\sigma(\boldsymbol{W}_k^{\mathrm{T}}\boldsymbol{V}_j')) \tag{8}$$

$$p(\boldsymbol{R}|\boldsymbol{U}, \boldsymbol{V}, \boldsymbol{Z}, \boldsymbol{C}, Gr) = \prod_{i,j} \mathrm{N}(R_{ij}|\boldsymbol{U}_i^{\mathrm{T}}\boldsymbol{V}_j, (G_r \cdot C_{ij})^{-1})^{I_{ij}\cdot(1-Z_{ij})} \tag{9}$$

其中, $t \in \{u, v, w\}$, $\mathrm{Gam}(\cdot)$ 和 $\mathrm{Bern}(\cdot)$ 分别为 Gamma 分布和 Bernoulli 分布. 参数 χ_{ij} 表示 R_{ij} 是否极端值 ($r_{\max}$ 或 $r_{\min}$), 是则取 1, 否则为 0. 式 (8) 中, Logistic sigmoid 函数 $\sigma(x) = 1/(1 + \exp(-x))$, 且 $\boldsymbol{V}_j' = [\boldsymbol{V}_j^{\mathrm{T}}\ 1]^{\mathrm{T}}$, $\boldsymbol{W}_k = [\boldsymbol{W'}_k^{\mathrm{T}}\ W_k^0]^{\mathrm{T}}$, W_k^0 与 $\boldsymbol{V}_j'$ 的常数分量相对应. 矩阵 Λ_t 的阶数满足关系 $\mathrm{size}(\Lambda_u) = \mathrm{size}(\Lambda_v) = \mathrm{size}(\Lambda_w) - 1 = D\,(\geq 1)$, 因而, D 也是 $\boldsymbol{U}_i$ 和 $\boldsymbol{V}_j$ 的维数.

用户和项的元信息以各自不同的方式与模型相融合. 参数 θ_i 为 $user_i$ 的嫌疑性信息, 它以模型参数形式通过式 (4) 导入 MVBMF. 变量 $\boldsymbol{X}_j$ ($\boldsymbol{X}_j = [X_{j1}, X_{j2}, \cdots, X_{jk}]^{\mathrm{T}}$) 为 $item_j$ 在 K 个类别上的 0−1 类属信息, 它通过式 (8) 的 Logistic 回归导入 MVBMF, $\boldsymbol{W}_k$ 充当回归系数, 其中包含截距项 W_k^0. 实际上, 也可采用无截距项的线性回归作为信息导入方式, 这能显著降低模型推断的难度[18], 但考虑到 $\boldsymbol{X}$ 的取值特点以及回归的准确性等因素, 选用含截距项的 Logistic 回归更为合理, 代价则是牺牲了 $\boldsymbol{X}$ 与 $\boldsymbol{V}$, $\boldsymbol{W}$ 间的共轭性, 需要在模型推断时采取针对性措施.

2.3 MVBMF 的鲁棒性保障机制

MVBMF 提供了三重鲁棒性保障机制:

首先, 若评分 R_{ij} 为极端值且其评分者 $user_i$ 的嫌疑性强, 则式 (4) 将使 $Z_{ij} = 1$ 以较高概率出现, 而在 $Z_{ij} = 1$ 时, R_{ij} 会被式 (9) 屏蔽. 这样, 依概率屏蔽攻击性最强的极端评分, 既消除了其对模型构建的负面影响, 又降低了误伤真实用户的可能. 显然, 用户嫌疑性信息在这种评分屏蔽机制中发挥了关键作用.

其次, 考虑到用户偏好的易变性与项类属的稳定性, MVBMF 认为项的类属特性存在隐式确定的真实值, 故应优先确保变量 $\boldsymbol{V}$ 后验的可信度. 式 (8) 的 Logistic 回归将类属信息 $\boldsymbol{X}$ 导入 MVBMF, 先验信息 $\boldsymbol{X}$ 的可靠性使 $p(\boldsymbol{V}|\boldsymbol{R}, \boldsymbol{X})$ 比 $p(\boldsymbol{V}|\boldsymbol{R})$ 更真实地还原了项的类属特征. 同时, 这也为下文中 MVBMF 增量学习策略的设计奠定了基础.

最后, MVBMF 还具备滤除自然噪声的能力. 因为对于式 (9), 若 $\exists i,j$, 使 $I_{ij}=1$ 且 $Z_{ij}=0$, 则积去 C_{ij} 可得:

$$\begin{aligned}&p(R_{ij}|\boldsymbol{U}_i,\boldsymbol{V}_j,Gr)=\\&\int_0^\infty p(R_{ij}|\boldsymbol{U}_i,\boldsymbol{V}_j,C_{ij},Gr)p(C_{ij})\,\mathrm{d}C_{ij}=\\&\int_0^\infty \mathrm{N}(R_{ij}|\boldsymbol{U}_i^{\mathrm{T}}\boldsymbol{V}_j,(G_r\cdot C_{ij})^{-1})\times\\&\quad\mathrm{Gam}\left(C_{ij}|\frac{\lambda}{2},\frac{\lambda}{2}\right)\mathrm{d}C_{ij}=\\&\mathrm{St}(R_{ij}|\boldsymbol{U}_i^{\mathrm{T}}\boldsymbol{V}_j,G_r,\lambda)\end{aligned}\tag{10}$$

其中, $\mathrm{St}(\cdot)$ 为 t 分布. t 分布在概率模型中常被用于平滑噪声点的干扰, 这归因于其 "重尾" (Heavy tail) 特性[19].

2.4 MVBMF 的变分推断

令 Ω^h 与 Ω^o 分别表示 MVBMF 的隐含随机变量 $\{\boldsymbol{U},\boldsymbol{V},\boldsymbol{Z},\boldsymbol{C},\boldsymbol{W},G_u,G_r,G_v,G_w\}$ 与可见随机变量 $\{\boldsymbol{R},\boldsymbol{X}\}$. 由变量间的条件独立性, 可知联合分布 $p(\Omega^o\cup\Omega^h)$ 等于式 $(1)\sim(9)$ 的乘积. 在进行模型推断时, 会发现难以求出后验分布 $p(\Omega^h|\Omega^o)$ 的规则形式. 对此, 本文采取变分贝叶斯方法[20], 寻求 $p(\Omega^h|\Omega^o)$ 的近似替代 $q(\Omega^h)$. 首先, 简要介绍变分贝叶斯方法.

随机变量 Ω^o 的对数边缘似然满足关系:

$$\ln p(\Omega^o)=\mathcal{L}(q)+\mathrm{KL}(q||p)$$

其中

$$\begin{aligned}\mathcal{L}(q)&=\int q(\Omega^h)\ln\frac{p(\Omega^o\cup\Omega^h)}{q(\Omega^h)}\,\mathrm{d}\Omega^h\\\mathrm{KL}(q||p)&=-\int q(\Omega^h)\ln\frac{p(\Omega^h|\Omega^o)}{q(\Omega^h)}\,\mathrm{d}\Omega^h\end{aligned}\tag{11}$$

$\mathrm{KL}(q||p)$ 代表变分后验 $q(\Omega^h)$ 与真实后验 $p(\Omega^h|\Omega^o)$ 间的 Kullback-Leibler (KL) 离散度, 其值非负, 所以 $\mathcal{L}(q)$ 是定值 $\ln p(\Omega^o)$ 的下界. 为使 $q(\Omega^h)\to p(\Omega^h|\Omega^o)$, 只需 $\mathrm{KL}(q||p)\to 0$, 这等价于最大化 $\mathcal{L}(q)$. 为简化优化过程, 通常对 $q(\Omega^h)$ 的形式作以下假设:

$$q(\Omega^h)=\prod_{\varphi\in\Omega^h}q(\varphi)$$

此时, 任取随机变量 $\varphi\in\Omega^h$, 固定其余分布 $\{q(\varphi')|\varphi'\in\Omega^h\wedge\varphi'\neq\varphi\}$. $q(\varphi)$ 满足如下关系时 $\mathcal{L}(q)$ 达到最大[20]:

$$q(\varphi)\propto\exp\mathrm{E}_{-\varphi}[\ln p(\Omega^o\cup\Omega^h)]\tag{12}$$

其中, $\mathrm{E}_{-\varphi}[\cdot]$ 是关于分布 $\prod_{\varphi'\neq\varphi}q(\varphi')$ 的期望算子. 可利用式 (12) 迭代更新 Ω^h 中每个变量的变分后验, 每步迭代均使下界 $\mathcal{L}(q)$ 得到提升. 迭代收敛时, $q(\Omega^h)$ 则为 $p(\Omega^h|\Omega^o)$ 的良好近似. 以上是变分贝叶斯法的概要过程.

图 4 中, 由于节点 $\boldsymbol{X}$ 与其父节点 $\boldsymbol{V},\boldsymbol{W}$ 间不存在共轭特性, 所以从式 (12) 难以推出 $\boldsymbol{V}_j$ 和 $\boldsymbol{W}_k$ 变分后验的规则形式. 对此, 本文进一步采取局部变分法推导 $\mathcal{L}(q)$ 的下界, 现有不等式[21]:

$$\sigma(a)\geq\sigma(\xi)\exp\left(\frac{a-\xi}{2}-\tau(\xi)(a^2-\xi^2)\right)=\sigma'(a,\xi)$$

其中, $\tau(\xi)=(1/4\xi)\tanh(\xi/2)$. 上式代入式 (8) 有:

$$\begin{aligned}&p(\boldsymbol{X}|\boldsymbol{V},\boldsymbol{W})=\prod_{j,k}p(X_{jk}|\sigma(\boldsymbol{W}_k^{\mathrm{T}}\boldsymbol{V}_j'))=\\&\prod_{j,k}\sigma(\boldsymbol{W}_k^{\mathrm{T}}\boldsymbol{V}_j')^{X_{jk}}(1-\sigma(\boldsymbol{W}_k^{\mathrm{T}}\boldsymbol{V}_j'))^{1-X_{jk}}=\\&\prod_{j,k}\exp(\boldsymbol{W}_k^{\mathrm{T}}\boldsymbol{V}_j'X_{jk})\sigma(-\boldsymbol{W}_k^{\mathrm{T}}\boldsymbol{V}_j')\geq\\&\prod_{j,k}\exp(\boldsymbol{W}_k^{\mathrm{T}}\boldsymbol{V}_j'X_{jk})\sigma'(-\boldsymbol{W}_k^{\mathrm{T}}\boldsymbol{V}_j',\xi_{jk})\end{aligned}$$

上式替换 $p(\Omega^o\cup\Omega^h)$ 中乘积因子 $p(\boldsymbol{X}|\boldsymbol{V},\boldsymbol{W})$ 可得:

$$p(\Omega^o\cup\Omega^h)\geq p^v(\Omega^o\cup\Omega^h|\Phi)\tag{13}$$

其中, 变分参数 $\Phi=\{\xi_{jk}|j=1\sim J\wedge k=1\sim K\}$. 式 (13) 代入式 (11) 得出 $\mathcal{L}(q)$ 的下界:

$$\mathcal{L}(q)\geq\int q(\Omega^h)\ln\frac{p^v(\Omega^o\cup\Omega^h|\Phi)}{q(\Omega^h)}\,\mathrm{d}\Omega^h=\mathcal{L}^v(q,\Phi)$$

至此, 可用变分 EM 算法[21] 最优化 $\mathcal{L}^v(q,\Phi)$: 首先, 初始化分布 $q^{(0)}$ 和参数 $\Phi^{(0)}$, 之后交替固定一个因子, 以另一因子为变元最大化 $\mathcal{L}^v(q,\Phi)$, 直至迭代收敛. 形式化地:

$$\begin{aligned}&(E\text{-step}):\ q^{(k+1)}=\arg\max_q\mathcal{L}^v(q,\Phi^{(k)})\\&(M\text{-step}):\ \Phi^{(k+1)}=\arg\max_\Phi\mathcal{L}^v(q^{(k)},\Phi)\end{aligned}$$

在 M-step, 对 $\forall j,\ k$ 有:

$$\begin{aligned}&\frac{\partial\mathcal{L}^v(q,\Phi)}{\partial\xi_{jk}}=\frac{\partial\mathrm{E}[\ln p^v(\Omega^o\cup\Omega^h|\Phi)]}{\partial\xi_{jk}}=0\Rightarrow\\&\xi_{jk}^2=\mathrm{tr}(\mathrm{E}[\boldsymbol{W}_k\boldsymbol{W}_k^{\mathrm{T}}]\mathrm{E}[\boldsymbol{V}_j'\boldsymbol{V}_j'^{\mathrm{T}}])\end{aligned}$$

在 E-step, 仍用式 (12) 推导变分后验 q, 只需将 $p(\Omega^o\cup\Omega^h)$ 替换为 $p^v(\Omega^o\cup\Omega^h|\Phi)$. 推导过程较为庞杂, 在此略去, 以下为最终结果:

$$\begin{aligned}q(G_t)&=\mathcal{W}(G_t|\nu_t',\Lambda_t')\\q(G_r)&=\mathrm{Gam}(G_r|\alpha',\beta')\end{aligned}$$

$$q(\boldsymbol{C}) = \prod_{i,j}\mathrm{Gam}(C_{ij}|\lambda_{ij}^a, \lambda_{ij}^b)$$
$$q(\boldsymbol{Z}) = \prod_{i,j}\mathrm{Bern}(Z_{ij}|\delta_{ij})$$
$$q(\boldsymbol{U}) = \prod_{i}\mathrm{N}(\boldsymbol{U}_i|\boldsymbol{\mu}_i^u, \Lambda_i^u)$$
$$q(\boldsymbol{V}) = \prod_{j}\mathrm{N}(\boldsymbol{V}_j|\boldsymbol{\mu}_j^v, \Lambda_j^v)$$
$$q(\boldsymbol{W}) = \prod_{k}\mathrm{N}(\boldsymbol{W}_k|\boldsymbol{\mu}_k^w, \Lambda_k^w)$$

其中, $t \in \{u, v, w\}$, 各分布参数为

$$\nu_u' = \nu_u + I, \quad {\Lambda_u'}^{-1} = \Lambda_u^{-1} + \sum_i \mathrm{E}[\boldsymbol{U}_i\boldsymbol{U}_i^{\mathrm{T}}]$$
$$\nu_v' = \nu_v + J, \quad {\Lambda_v'}^{-1} = \Lambda_v^{-1} + \sum_j \mathrm{E}[\boldsymbol{V}_j\boldsymbol{V}_j^{\mathrm{T}}]$$
$$\nu_w' = \nu_w + K, \quad {\Lambda_w'}^{-1} = \Lambda_w^{-1} + \sum_k \mathrm{E}[\boldsymbol{W}_k\boldsymbol{W}_k^{\mathrm{T}}]$$
$$\alpha' = \alpha + \frac{1}{2}\sum_{i,j} I_{ij}(1 - \mathrm{E}[Z_{ij}])$$
$$\beta' = \beta + \frac{1}{2}\sum_{i,j} I_{ij}\mathrm{E}[C_{ij}]\mathrm{E}[(R_{ij} - \boldsymbol{U}_i^{\mathrm{T}}\boldsymbol{V}_j)^2] \times (1 - \mathrm{E}[Z_{ij}])$$
$$\lambda_{ij}^a = \frac{\lambda + I_{ij}(1 - \mathrm{E}[Z_{ij}])}{2}$$
$$\lambda_{ij}^b = \frac{\lambda + I_{ij}(1 - \mathrm{E}[Z_{ij}])\mathrm{E}[G_r]\mathrm{E}[(R_{ij} - \boldsymbol{U}_i^{\mathrm{T}}\boldsymbol{V}_j)^2]}{2}$$
$$\delta_{ij} = (1 + \exp(S_2 - S_1))^{-1}$$
$$S_1 = \ln(\theta_i\chi_{ij})$$
$$S_2 = \ln(1 - \theta_i\chi_{ij}) + \frac{I_{ij}}{2}(\mathrm{E}[\ln G_r] + \mathrm{E}[\ln C_{ij}] - \ln 2\pi - \mathrm{E}[G_r]\mathrm{E}[C_{ij}]\mathrm{E}[(R_{ij} - \boldsymbol{U}_i^{\mathrm{T}}\boldsymbol{V}_j)^2])$$
$$\Lambda_i^{u\,-1} = \mathrm{E}[G_u] + \sum_j I_{ij}(1 - \mathrm{E}[Z_{ij}])\mathrm{E}[G_r] \times \mathrm{E}[C_{ij}]\mathrm{E}[\boldsymbol{V}_j\boldsymbol{V}_j^{\mathrm{T}}]$$
$$\boldsymbol{\mu}_i^u = \Lambda_i^u\sum_j I_{ij}(1 - \mathrm{E}[Z_{ij}])\mathrm{E}[G_r]\mathrm{E}[C_{ij}]\mathrm{E}[\boldsymbol{V}_j]R_{ij}$$
$$\Lambda_j^{v\,-1} = \mathrm{E}[G_v] + \sum_i I_{ij}(1 - \mathrm{E}[Z_{ij}])\mathrm{E}[G_r]\mathrm{E}[C_{ij}] \times \mathrm{E}[\boldsymbol{U}_i\boldsymbol{U}_i^{\mathrm{T}}] + 2\sum_k \tau(\xi_{jk})\mathrm{E}[\boldsymbol{W}_k'\boldsymbol{W}_k'^{\mathrm{T}}]$$
$$\boldsymbol{\mu}_j^v = \Lambda_j^v(\sum_i I_{ij}(1 - \mathrm{E}[Z_{ij}])\mathrm{E}[G_r]\mathrm{E}[C_{ij}]\mathrm{E}[\boldsymbol{U}_i]R_{ij} + \sum_k(\mathrm{E}[\boldsymbol{W}_k'](X_{jk} - \frac{1}{2}) - 2\mathrm{E}[\boldsymbol{W}_k'W_k^0]\tau(\xi_{jk})))$$
$$\Lambda_k^{w\,-1} = \mathrm{E}[G_w] + 2\sum_j \tau(\xi_{jk})\mathrm{E}[\boldsymbol{V}_j'\boldsymbol{V}_j'^{\mathrm{T}}]$$
$$\boldsymbol{\mu}_k^w = \Lambda_k^w\sum_j (X_{jk} - \frac{1}{2})\mathrm{E}[\boldsymbol{V}_j']$$

简洁起见, 以上未将期望算式展开. 变分 EM 算法收敛时, 将 $\mathrm{E}[\boldsymbol{U}_i]$ 和 $\mathrm{E}[\boldsymbol{V}_j]$ 分别视作 $user_i$ 和 $item_j$ 的特征向量, 缺失评分 R_{ij} 可预测为

$$\mathrm{R}(user_i, item_j) = \mathrm{E}[\boldsymbol{U}_i]^{\mathrm{T}}\mathrm{E}[\boldsymbol{V}_j] \tag{14}$$

2.5 MVBMF 的增量学习

推荐算法应同时具备弱泛化 (Weak generalization) 与强泛化 (Strong generalization) 能力[22]. 前者要求算法能预测训练集内用户的评分, 后者进一步要求算法能预测与训练集独立的测试集中用户的评分.

MVBMF 目前仅有弱泛化能力, 无法为新用户提供推荐服务. 一种朴素的解决思路是每次新用户加入时触发模型重构, 但这会引起计算成本的剧增. 针对这种问题, 本文提出了基于鲁棒线性回归[23] 的 MVBMF 模型增量学习策略.

由于项类属的稳定性, 对 $\forall item_j$, 可认为除了模型的重构操作, 任何新用户的加入都不会改变特征向量 $\mathrm{E}[\boldsymbol{V}_j]$, 而且项的元信息又增强了 $\mathrm{E}[\boldsymbol{V}_j]$ 的可信度. 因此, 类比式 (14), 只要获知新用户 $user'$ 的特征向量 $\widehat{\boldsymbol{U}'}$, 则可预测评分:

$$\mathrm{R}(user', item_j) = \widehat{\boldsymbol{U}'}^{\mathrm{T}}\mathrm{E}[\boldsymbol{V}_j] \tag{15}$$

注意到, 对于训练集中任意用户 $user_i$, 式 (9) 实际是对其所有评分做预测子为 $\{\boldsymbol{V}_j|j = 1, \cdots, J\}$ 的线性回归, 回归系数 $\boldsymbol{U}_i$ 即为 $user_i$ 的特征向量, 且随机误差符合 t 分布 (式 (10)). 同样, 对新用户 $user'$, 为求其特征向量 $\widehat{\boldsymbol{U}'}$ 并同时滤除自然噪声, 可对 $user'$ 的现有评分做预测子为 $\{\mathrm{E}[\boldsymbol{V}_j]|j = 1, \cdots, J\}$ 的鲁棒线性回归.

设 $R(U')$ 代表用户 $user'$ 已评价项的索引集, 定义:

$$\begin{aligned} r(j, \boldsymbol{\eta}) &= \mathrm{R}(user', item_j) - \mathrm{E}[\boldsymbol{V}_j]^{\mathrm{T}}\boldsymbol{\eta} \\ \boldsymbol{\eta}^0 &= \arg\min_{\boldsymbol{\eta}} \sum_{j \in R(U')} |r(j, \boldsymbol{\eta})| \\ res &= \{|r(j, \boldsymbol{\eta}^0)| \ | j \in R(U') \wedge r(j, \boldsymbol{\eta}^0) \neq 0\} \\ \widehat{\sigma} &= \frac{\mathrm{Median}(res)}{0.675} \\ \Psi(\boldsymbol{\eta}) &= \sum_{j \in R(U')} \rho\left(\frac{r(j, \boldsymbol{\eta})}{\widehat{\sigma}}\right) \end{aligned}$$

则 $user'$ 的特征向量等于回归系数的 M–估计量 $\widehat{\boldsymbol{\eta}}$:

$$\widehat{\boldsymbol{U}'} = \widehat{\boldsymbol{\eta}} = \arg\min_{\boldsymbol{\eta}} \Psi(\boldsymbol{\eta}) \tag{16}$$

其中, $\boldsymbol{\eta}^0$ 是回归系数的最小绝对偏差 (Least absolute deviation, LAD) 估计, 算法见文献 [24]. 扩展度估计量 $\widehat{\sigma}$ 赋予 $\widehat{\boldsymbol{\eta}}$ 缩放不变性[23]. 函数 $\rho(\cdot)$ 是回归鲁棒性的决定因素, 这里选用 Tukey 双权函数:

$$\rho(x) = \begin{cases} 1 - \left(1 - \left(\dfrac{x}{k}\right)^2\right)^3, & |x| \le k \\ 1, & |x| > k \end{cases}$$

式 (16) 解 $\widehat{\boldsymbol{\eta}}$ 存在的必要条件为

$$\nabla\Psi(\widehat{\boldsymbol{\eta}}) = \boldsymbol{0} \;\Rightarrow\; \sum_{j \in R(U')} \omega\left(\frac{r(j,\widehat{\boldsymbol{\eta}})}{\widehat{\sigma}}\right) \mathrm{E}[\boldsymbol{V}_j] r(j,\widehat{\boldsymbol{\eta}}) = \boldsymbol{0}$$

此处利用迭代变权最小二乘 (Iteratively reweighted least squares, IRWLS) 算法[25] 求解 $\widehat{\boldsymbol{\eta}}$. 权值 $\omega(x) = (1-(x/k)^2)^2 I(|x| \le k)$. 可见若 $\exists r(j,\widehat{\boldsymbol{\eta}}) \notin [-k\widehat{\sigma}, k\widehat{\sigma}]$, 则 $\omega(r(j,\widehat{\boldsymbol{\eta}})/\widehat{\sigma}) = 0$, 表明噪声评分 $\mathrm{R}(user', item_j)$ 对 $\widehat{\boldsymbol{\eta}}$ 的影响被消除.

由于集合 $R(U')$ 基数较小, 故鲁棒线性回归过程耗时极少, 计算代价远小于模型重构.

2.6　基于 MVBMF 的协同推荐

基于 MVBMF 的协同推荐由线下 (Off-line) 与线上 (On-line) 操作组成. 线下操作包括模型构建与增量学习, 增量学习适用于少量新用户, 若新用户总量超出容忍阈值, 为保证模型的有效性, 则需要重构模型, 即重新启动用户嫌疑性的评估与模型的变分 EM 推断. 线上操作负责预测与推荐, 根据用户是否属于训练集, 从式 (14) 和式 (15) 中选择合适的评分策略, 而后推荐若干高评价项. 线下与线上操作在计算负荷方面形成了高低搭配与负载分离, 高耗时的线下操作保证了线上操作的实时性.

3　实验与分析

实验数据集为 MovieLens100K, 包含了 943 个用户对 1 682 部电影的 10 万个评分, 评分范围为 1～5, 代表喜好程度从低到高, 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. 实验中向数据集注入的托攻击均为推攻击. 式 (1)～(3) 中模型参数取值为: $\nu_t = 1, \Lambda_t = I$ (单位矩阵), $\alpha = 8$, $\beta = 4$, $\lambda = 8$. 所有实验均在一台 Intel Pentium Dual CPU 1.60 GHz 的 PC 机上进行, 程序采用 Python+MySQL 实现.

3.1　鲁棒性度量标准

鲁棒性的定量度量利用了两种指标: 绝对平均误差 (Mean absolute error, MAE) 与预测偏差 (Prediction shift, PS)[6].

准确性指标 MAE 用于衡量真实评分与预测评分间的平均偏差. 设 T 为测试集, 元素为 $(user, item)$ 二元组, 对 $\forall t \in T$, $\mathrm{R}(t)$ 与 $\mathrm{R}^p(t)$ 分别代表真实评分与预测评分, 则 MAE 定义为

$$\mathrm{MAE} = \frac{1}{|T|}\sum_{t \in T} |\mathrm{R}(t) - \mathrm{R}^p(t)|$$

MAE 越小, 算法的准确性越好.

稳定性指标 PS 用于衡量托攻击前后目标项评分的预测偏差. 设 T 为测试集, 元素为 $(user, item^a)$ 二元组, $item^a$ 是托攻击目标项, 对 $\forall t \in T$, $\mathrm{R}^n(t)$ 与 $\mathrm{R}^a(t)$ 分别代表攻击前后的预测评分, 则 PS 定义为

$$\mathrm{PS} = \frac{1}{|T|}\sum_{t \in T} |\mathrm{R}^n(t) - \mathrm{R}^a(t)|$$

同样, PS 越小, 算法的稳定性越强.

3.2　维数选取

贝叶斯模型的复杂度不宜过高或过低, 否则会引起过度拟合或降低观察值的似然[26]. MVBMF 模型中, 正整数 D 作为用户与项特征向量的维数, 直接控制着模型复杂度. 为选取合适的 D 值, 本文对比了 $D = 2, 5, 10, 15, 20$ 时, MVBMF 模型的 MAE 值, 测试方法为留一法, 即随机保留每个用户的一个评分用于预测. 一般而言, D 较小时难以充分揭示用户与项的类型多样性, 而 D 较大时则有过度拟合的风险, 两类情况都会降低模型泛化能力. 图 5 中实验结果与上述分析一致, 模型仅在适中的维数 $D = 5$ 时获得最佳准确性. 据此, 下列各实验中, $D = 5$ 默认为 MVBMF 及其他参照模型的维数设置.

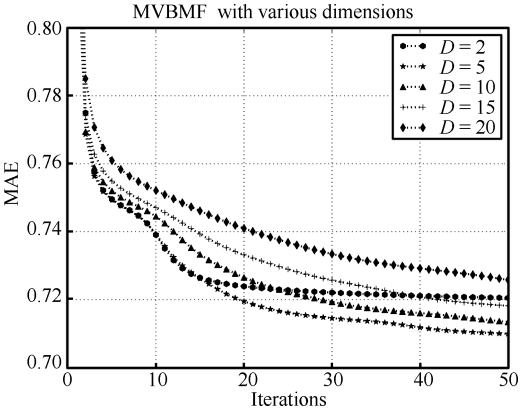


图 5　MVBMF 的维数选取

Fig. 5　Dimension selection for MVBMF

3.3 弱泛化情形

为评估 MVBMF 的弱泛化能力, 实验采取 $3 \times 3 \times 2$ 的设计模式, 攻击模型 (随机攻击、均值攻击、流行攻击), 攻击强度 p^{att} (3 %, 5 %, 10 %) 和填充率 p^{fill}(3 %, 6 %) 的不同组合对应一组实验配置. 测试方法为留一法, 最终数据取自十次独立实验的均值.

表 1 ∼ 3 为实验结果. 其中的 sMVBMF 是对 MVBMF 的简化, 删去了用户与项的元信息, 保留其余特性, 用于验证元信息对鲁棒性的影响. 总体上, 贝叶斯模型 (BPMF, sMVBMF, MVBMF) 的准确性优于非贝叶斯模型 (EMSVD, RMF, VarSelect SVD). 这归因于前者引入了参数先验, 抑制了过度拟合. 其中, sMVBMF 与 BPMF 的准确性最佳, 且由于 sMVBMF 能滤除自然噪声, 其 MAE 大体上略优于 BPMF. 作为 sMVBMF 的增强版本, MVBMF 需进一步拟合评分矩阵之外的元信息, 导致 MAE 稍逊于 sMVBMF, 然而这换取了稳定性的显著提升, 较之其余模型, MVBMF 对托攻击的抵御能力占据绝对优势, 且攻击强度的增加不会引起其稳定性的显著退化. 特别地, VarSelect SVD 虽凭借高效的托攻击探测与删除手段而获得了较好的稳定性, 但 PS 值仍平均高出 MVBMF 两倍以上. 注意到, sMVBMF 的 PS 指标并不理想, 侧面印证了元信息对改善算法鲁棒性的积极作用. MVBMF 的用户嫌疑性评估与变分 EM 推断都是迭代寻优过程, 故 MVBMF 在执行时间上并无优势, 如图 6. 不

表 1 随机攻击对不同推荐模型的影响

Table 1 Effect of random attack on various models for recommendation

		EMSVD		RMF		VarSelect SVD		BPMF		sMVBMF		MVBMF	
p^{att}	p^{fill}	MAE	PS	MAE	PS	MAE	PS	MAE	PS	MAE	PS	MAE	PS
3 %	3 %	0.717	0.823	0.740	1.228	0.758	**0.129**	0.708	0.643	**0.701**	0.542	**0.713**	**0.045**
	6 %	0.718	0.765	0.739	1.239	0.757	**0.155**	0.708	0.617	**0.703**	0.582	**0.710**	**0.076**
5 %	3 %	0.717	1.027	0.739	1.555	0.756	**0.198**	0.706	0.840	**0.706**	0.607	**0.709**	**0.064**
	6 %	0.717	0.873	0.744	1.500	0.758	**0.166**	0.706	0.720	**0.700**	0.614	**0.706**	**0.073**
10 %	3 %	0.720	1.174	0.747	1.775	0.755	**0.200**	0.710	1.125	**0.710**	0.876	**0.711**	**0.050**
	6 %	0.717	1.019	0.747	1.871	0.755	**0.245**	0.705	0.918	**0.701**	0.741	**0.709**	**0.117**

表 2 均值攻击对不同推荐模型的影响

Table 2 Effect of average attack on various models for recommendation

		EMSVD		RMF		VarSelect SVD		BPMF		sMVBMF		MVBMF	
p^{att}	p^{fill}	MAE	PS	MAE	PS	MAE	PS	MAE	PS	MAE	PS	MAE	PS
3 %	3 %	0.717	0.905	0.745	1.325	0.756	**0.172**	0.705	1.098	**0.707**	1.187	**0.712**	**0.061**
	6 %	0.718	0.871	0.741	1.316	0.755	**0.128**	0.708	1.087	**0.710**	1.205	**0.711**	**0.084**
5 %	3 %	0.721	1.158	0.741	1.670	0.758	**0.183**	0.710	1.423	**0.707**	1.568	**0.714**	**0.044**
	6 %	0.720	1.181	0.737	1.684	0.758	**0.193**	0.707	1.422	**0.706**	1.565	**0.710**	**0.056**
10 %	3 %	0.718	1.546	0.741	2.005	0.753	**0.210**	0.704	1.731	**0.704**	1.813	**0.708**	**0.106**
	6 %	0.720	1.497	0.737	1.997	0.748	**0.299**	0.708	1.775	**0.704**	1.867	**0.708**	**0.053**

表 3 流行攻击对不同推荐模型的影响

Table 3 Effect of bandwagon attack on various models for recommendation

		EMSVD		RMF		VarSelect SVD		BPMF		sMVBMF		MVBMF	
p^{att}	p^{fill}	MAE	PS	MAE	PS	MAE	PS	MAE	PS	MAE	PS	MAE	PS
3 %	3 %	0.716	0.922	0.740	1.239	0.757	**0.124**	0.705	0.726	**0.705**	0.561	**0.708**	**0.054**
	6 %	0.716	0.744	0.741	1.229	0.755	**0.133**	0.706	0.58	**0.707**	0.487	**0.708**	**0.088**
5 %	3 %	0.719	1.211	0.747	1.474	0.758	**0.122**	0.707	1.395	**0.701**	1.534	**0.713**	**0.072**
	6 %	0.719	0.883	0.740	1.442	0.757	**0.198**	0.706	0.734	**0.706**	0.635	**0.709**	**0.055**
10 %	3 %	0.716	1.221	0.740	1.775	0.759	**0.286**	0.704	1.150	**0.699**	0.853	**0.711**	**0.050**
	6 %	0.715	1.034	0.742	1.859	0.755	**0.227**	0.707	0.912	**0.705**	0.739	**0.709**	**0.153**

过考虑到模型构建对于线上操作的透明性, 以及鲁棒性获得的显著改善, 付出这种时间代价是有意义的.

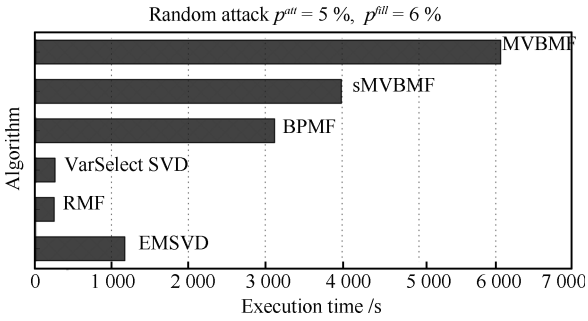


图 6　执行时间对比

Fig. 6　Comparison of execution time

3.4　强泛化情形

为评估 MVBMF 的强泛化能力, 现将数据集划分为独立的训练集与测试集, 测试集用以模拟新用户. 实验采取 3×4 的设计模式, 训练集比例 $(20\,\%, 50\,\%, 80\,\%)$ 与攻击情境 (无攻击、随机攻击、均值攻击、流行攻击) 的不同组合对应一组实验配置. 攻击参数设为 $p^{att} = 10\,\%$, $p^{fill} = 6\,\%$, 代表中高强度攻击. 实验随机保留每个新用户的 10 个评分, 以评测模型增量学习策略对大量缺失评分的预测能力. 最终数据取自十次独立实验的均值.

理论上, 由于新用户信息未参与模型构建, MVBMF 的强泛化能力必然不及弱泛化时水平. 从表 4 可知, 仅在 20 % 训练集下, MVBMF 的鲁棒性欠佳, 需重构模型. 其余情况下, MVBMF 的 MAE 与 PS 值已接近弱泛化情形, 且随训练集的增大显现出递减趋势. 特别地, 以不显著损耗鲁棒性为前提, MVBMF 能容许加入至少与训练集等量的新用户, 极大降低了对模型重构的需求.

表 4　增量学习的性能

Table 4　Performance of incremental learning strategy

训练集比例	20 %		50 %		80 %	
	MAE	PS	MAE	PS	MAE	PS
无攻击	0.900	—	0.816	—	0.794	—
随机攻击	0.883	1.538	0.800	0.254	0.792	0.233
均值攻击	0.911	1.475	0.808	0.275	0.784	0.241
流行攻击	0.874	1.585	0.811	0.267	0.782	0.235

4　结论

本文提出的 MVBMF 模型综合利用了 PLSA, Logistic 回归与变分 EM 等方法, 在对用户嫌疑性进行评估的基础上, 将用户嫌疑性与项类属信息纳入矩阵分解过程, 弱化了评分噪声对模型变量变分后验的负面影响. 同时基于鲁棒线性回归的增量学习策略也降低了对模型重构的需求. MVBMF 对托攻击具有显著的耐受力, 其强弱泛化能力达到了较高水平, 同时确保了准确性与稳定性, 可向用户提供鲁棒的协同推荐服务.

References

1 Adomavicius G, Tuzhilin A. Toward the next generation of recommender systems: a survey of the state-of-the-art and possible extension. *IEEE Transactions on Knowledge and Data Engineering*, 2005, **17**(6): 734−749

2 O′Mahony M P, Hurley N J, Kushmerick N, Silvestre G C M. Collaborative recommendation: a robustness analysis. *ACM Transactions on Internet Technology*, 2004, **4**(4): 344−377

3 O′Mahony M P, Hurley N J, Silvestre G C M. Detecting noise in recommender system databases. In: Proceedings of the 11th International Conference on Intelligent User Interfaces. Sydney, Australia: ACM, 2006. 109−115

4 Lam S, Riedl J. Shilling recommender systems for fun and profit. In: Proceedings of the 13th Conference on World Wide Web. New York, USA: ACM, 2004. 393−402

5 Su X, Khoshgoftaar T M. A survey of collaborative filtering techniques. *Advances in Artificial Intelligence*, 2009, **2009**: 1−20

6 Mobasher B, Burke R, Bhaumik R, Williams C. Toward trustworthy recommender systems: an analysis of attack models and algorithm robustness. *ACM Transactions on Internet Technology*, 2007, **7**(4): 1−40

7 Mobasher B, Burke R, Bhaumik R, Sandvig J J. Attacks and remedies in collaborative recommendation. *IEEE Intelligent Systems*, 2007, **22**(3): 56−63

8 O′Mahony M P, Hurley N J, Silvestre G C M. Efficient and secure collaborative filtering through intelligent neighbor selection. In: Proceedings of the 16th European Conference on Artificial Intelligence. Valencia, Spain: IOS Press, 2004. 383−387

9 Sandvig J J, Mobasher B, Burke R. Impact of relevance measures on the robustness and accuracy of collaborative filtering. In: Proceedings of the 8th International Conference on E-commerce and Web Technologies. Berlin, Germany: Springer, 2007. 99−108

10 Sandvig J J, Mobasher B, Burke R. Robustness of collaborative recommendation based on association rule mining. In: Proceedings of the ACM Conference on Recommender Systems. New York, USA: ACM, 2007. 105−112

11 Mehta B, Hofmann T, Nejdl W. Robust collaborative filtering. In: Proceedings of the ACM Conference on Recommender Systems. New York, USA: ACM, 2007. 49−56

12 Huber P J. Robust estimation of a location parameter. *The Annals of Mathematical Statistics*, 1964, **35**(1): 73−101

13 Mehta B, Nejdl W. Attack resistant collaborative filtering. In: Proceedings of the 31st Annual International ACM SIGIR Conference on Research and Development in Information Retrieval. New York, USA: ACM, 2008. 75−82

14 Hofmann T. Probabilistic latent semantic indexing. In: Proceedings of the 22nd Annual International ACM SIGIR Conference on Research and Development in Information Retrieval. New York, USA: ACM, 1999. 50−57

15 Hurley N, Cheng Z, Zhang M. Statistical attack detection. In: Proceedings of the 3rd ACM Conference on Recommender Systems. New York, USA: ACM, 2009. 149−156

16 Zhang S, Wang W, Ford J, Makedon F, Pearlman J. Using singular value decomposition approximation for collaborative filtering. In: Proceedings of the 7th IEEE International Conference on E-commerce Technology. Washington D. C., USA: IEEE, 2005. 257−264

17 Salakhutdinov R, Mnih A. Bayesian probabilistic matrix factorization using Markov chain Monte Carlo. In: Proceedings of the 25th International Conference on Machine Learning. New York, USA: ACM, 2008. 880−887

18 Williamson S, Ghahramani Z. Probabilistic models for data combination in recommender systems. In: Proceedings of the NIPS Workshop: Learning from Multiple Sources. Vancouver, Canada: The MIT Press, 2008. 1−4

19 Tipping M E, Lawrence N D. Variational inference for student-t models: robust Bayesian interpolation and generalised component analysis. *Neurocomputing*, 2005, **69**(1−3): 123−141

20 Attias H. Inferring parameters and structure of latent variable models by variational Bayes. In: Proceedings of the 15th Annual Conference on Uncertainty in Artificial Intelligence. San Francisco, USA: Morgan Kaufmann, 1999. 21−30

21 Jaakkola T S, Jordan M I. Bayesian parameter estimation via variational methods. *Statistics and Computing*, 2000, **10**(1): 25−37

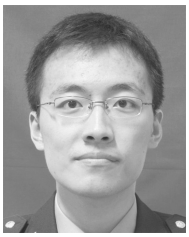
22 Marlin B. Collaborative Filtering: a Machine Learning Perspective [Master dissertation], University of Toronto, Canada, 2004

23 Huber P J, Ronchetti E M. *Robust Statistics (Second Edition)*. New Jersey: John Wiley and Sons, 2009. 149−199

24 Barrodale I, Roberts F D K. An improved algorithm for discrete L_1 linear approximation. *SIAM Journal on Numerical Analysis*, 1973, **10**(5): 839−848

25 Street J O, Carroll R J, Ruppert D. A note on computing robust regression estimates via iteratively reweighted least squares. *The American Statistician*, 1988, **42**(2): 152−154

26 MacKay D J C. Bayesian interpolation. *Neural Computation*, 1992, **4**(3): 415−447



李 聪 国防科学技术大学计算机学院博士研究生. 主要研究方向为机器学习, 人工智能与信息检索. 本文通信作者.
E-mail: licongwhy@gmail.com
(**LI Cong** Ph. D. candidate at the School of Computer, National University of Defense Technology. His research interest covers machine learning, artificial intelligence, and information retrieval. Corresponding author of this paper.)

骆志刚 国防科学技术大学计算机学院教授. 主要研究方向为高性能计算, 数据挖掘与生物信息学.
E-mail: zgluo@nudt.edu.cn
(**LUO Zhi-Gang** Professor at the School of Computer, National University of Defense Technology. His research interest covers high performance computing, data mining, and bioinformatics.)