D-011

ゲームにおけるレコメンダの研究開発

Research and development of the recommender System in the game

-重み付け攻撃対策-

-Measures for Weighting attacks-

張　亜偉‡
Chou　AI
指導教員:和田 雄次 教授

1 はじめに

近年，ゲーム市場の拡大により数多くのゲームが開発・発売されている。ユーザのニーズが多様化し、それに見合ったゲームが開発されることで,自分に合ったゲームを見つけることが難しくなった。そこで、オンラインショッピング、ＳＮＳサイトなどの様々な領域で普及しているレコメンドシステムを検証してみる。推薦システムの主な推薦手法は協調フィルタリングである。しかし、協調フィルタリングのアルゴリズムは公然と透明なので、偽評価の攻撃が受け易いである。特に、ゲーム推薦システムへの攻撃が多いである。現在、多くのゲーム推薦サイトは既存の協調フィルタリング手法を採用しているので、攻撃データに対して、推薦システムは脆弱性をもつ。本研究の目的は、協調フィルタリング推薦システムへの攻撃の影響が小さくなることである。

2　協調フィルタリングシステムへの攻撃

2.1 攻撃とは

ある集団や個人など、悪意を持って、特定な目的を抱えて、推薦システムの推薦動作を干渉する為に、不審なデータを推薦システムに挿入することである。悪意のないユーザが純粋に否定的な意見を示している時は、否定する理由が何であっても、攻撃とは見なさない。悪意のあるユーザが意図的に、推薦システムの動作に干渉しようとする場合を攻撃とみなす。

2.2 攻撃の分類

販売促進攻撃

特定な商品を推薦させられること。つまり、自撮自演のこと。

販売排除攻撃

特定な商品を推薦させられないこと。簡単に言うと、競争相手の商品を悪意攻撃すること。

2.3　攻撃事例

2010から2014まで、中国の大規模代表的なIT会社360とTencentがお互い、様々の領域で信用や評価を攻撃した。

2013年09月アメリカのニューヨーク州、19社の会社は偽評価という違法業務を停止し、 罰金も受け取った。

3.攻撃対策提案

3.1 評価値データを重み付け

根拠：ユーザは与えるアイテムの評価値が信頼できるかどうかを判断する為に、各評価値に信頼度を追加するより、評価値データを重み付けると、推薦システムの信頼度も向上されるかもしれない

方法：アイテムの評価値データの中で賛否の属性を追加して、評価値の重みを付ける。

評価の方式：評価値、理由（コメント）、賛と否のボタンの三つの部分で構成している。賛成と否定のデータを利用して、各ユーザがアイテムに対する評価値に重みを付ける。

イメージ：

パズル＆ドラゴンズについてどう思いますか？

□1　□ 2　□ 3　□ 4　□ 5

以上の評価点数について簡単な理由を記入してください


評価値データの重みつけの利点

1、全てのデータが静的から動的になると、動的なデータへの攻撃が非常に困難となる。(動的とは、すべての評価値のデータが各賛否の数によって変わる)

2、攻撃者の評価値データが容易に壊れる。つまり、賛否データを使って攻撃者の評価値の完全性を壊せる。

4　相加平均重み付け

4.1 計算仕組み

計算式：賛否数の平均データを利用する、相加平均重み付けアルゴリズムという計算方法である。

評価値: p　賛成数: a　否定数: b

$$p' = p + p \times \left(\frac{a - \frac{a+b}{2}}{a+b}\right)$$

例えば　$p = 80; a = 60; b = 40$

$$p' = 80 + 80 \times \left(\frac{60 - \frac{60+40}{2}}{60+40}\right) = 88$$

図１　相加平均重み付計算式

サンプル例

具体的な例について説明すると、下の図２ように、既存の協調フィルタリング推薦システムの推薦類似度リストで、攻撃者の類似度が一番高いので、この攻撃データを使用すると、間違った推薦を行うことになる。

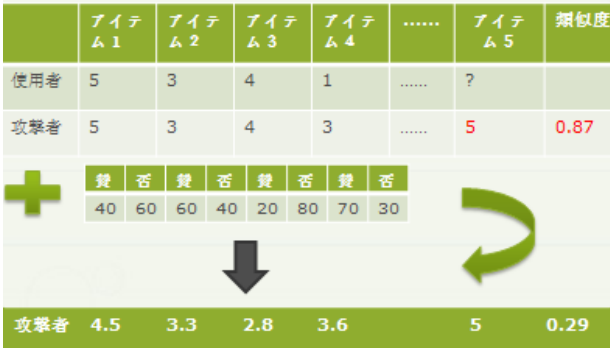

図２　　相加平均計算の例

一方、賛否データを追加し、相加平均重み付けアルゴリズムを利用すると、攻撃者の類似度が0.87 から0.29になる。つまり、類似度リストの一位から排除することで推薦システムは正確な推薦が得られる。

4.2 実験

4.2.1実験データセット

以上の提案アルゴリズムの精度を検証する為，実験を行った。まず，実験のデータセットは，賛否属性が独自の提案のため，公開されたデータセットには入って無い。データを収集する為，二段階のアンケートを実施した。第一段階のアンケート収集データは幾つかのアイテムに対してユーザが評価したデータである。第二段階のアンケートの中で，あるユーザを狙う販売促進攻撃データを追加し，別の人たちにアンケートを実施した。

4.2.2実験概要

被験者数は15人。データの完全性を考慮の上、10人のデータが採用した。

4.2.3実験結果

1).既存の協調フィルタリング

	アイテム1	アイテム2	アイテム4	アイテム5	アイテム6	平均値	ユーザAとの類似度	アイテム3	アイテム3の予測値
被推薦者	5	4	4	5	4	4.4		1	5
ユーザB	5	3	4	4	4	4.0	0.65	4	
ユーザC	5	3	3	4	3	3.3	0.87	2	
ユーザD	4	3	3	4	3	3.7	0.88	5	
ユーザE	3	2	2	3	2	2.7	0.88	4	

表１　相加平均重み付けの結果

表１、攻撃者DとEのデータがある場合、被推薦者のアイテム３の予測値が未知という仮前提の上、推薦を行う。推薦の結果はアイテム３の予測値が５であるので、被推薦者にアイテム３を推薦するべきだ。しかし、被推薦者のアイテム３の実評価値が１である。つまり、攻撃データが入ってる為、既存の推薦システムが誤推薦を行った。

2). 相加平均重み付け

	アイテム1	アイテム2	アイテム4	アイテム5	アイテム6	平均値	アイテム3	類似度	アイテム3の予測値
被推薦者	5	4	4	5	4	4.4	1		
賛成数	5	4	2	4	3				
否定数	0	1	3	1	2				
相加平均付け	7.5	5.2	3.6	6.5	4.4	5.44			2.75
ユーザB	5	3	4	4	4	4	4	0.645	
賛成数	5	2	1	3	3		2		
否定数	0	3	4	2	2		3		
相加平均付け	7.5	2.7	2.8	4.4	4.4	4.36	3.6	0.798	
ユーザC	5	3	3	4	3	3.6	2	0.871	
賛成数	5	3	3	4	4		3		
否定数	0	2	2	1	1		2		
相加平均付け	7.5	3.3	3.3	5.2	3.9	4.64	2.2	0.898	
ユーザD	4	3	3	4	3	3.4	5	0.878	
賛成数	5	3	4	4	5		2		
否定数	0	2	1	1	0		3		
相加平均付け	6	3.3	3.9	5.2	4.5	4.58	4.5	0.782	
ユーザE	3	2	2	3	2	2.4	4	0.878	
賛成数	2	1	3	3	1		3		
否定数	3	4	2	2	4		1		
相加平均付け	2.7	1.4	2.2	3.3	1.4	2.2	5	0.618	

表2　相加平均重み付けの結果

表2の青い部分のデータは相加平均重み付けしたのデータである。入力データとして、使用すると、アイテム３の予測値は2.75である。

相加平均重みを使用すると、評価値が0.5から7.5であるので、 推薦システムには、2.75の予測値ならば、ユーザAにアイテム３が推薦するべきではない。

4.2.4 実験考察

1. 攻撃者DとEは類似度ランキングの一、二位から消えることが分かった
2. 攻撃者DとEがアイテム３の評価値を少しだけ変化した（0.5）
3. 推薦結果により、相加平均重み付けを追加すると、攻撃者の影響が小さくなり、正しい推薦を行った

4.2.5 欠点

1)賛否数データだけ利用すると、誤差が大きくなる可能性がある。

2) 相加平均重み付けの計算式が簡単なので、攻撃者に再攻撃する可能性がある。つまり、攻撃者がユーザたちの評価値と賛否データが両方とも見れるから、まだ、攻撃者に利用する可能性が高い。

5. 加重平均重み付け

相加平均重み付けの欠点を考慮し、加重平均重み付けという計算式で試行した。この計算式の入力データは賛否データだけでなく、賛否ユーザの評価値も使用する。

5.1 加重平均とは

観測される値それぞれに重みがある時には、単に相加平均をとるのでなく重みを考慮した平均をとると信頼性が向上する。各データ xi に、重み wi がついているときの加重平均（重み付き平均）は

$$\frac{w_1x_1 + \cdots + w_nx_n}{w_1 + \cdots + w_n}$$

と定義される。

5.2 計算仕組み

計算方法

1. 賛成数が多いの場合
   評価値UP率＝賛成比率X（賛成加重平均値-総加重平均値）
2. 否定数多いの場合
   評価値UP率＝否定比率X（否定加重平均値-総加重平均値）

サンプル例

加重平均計算式を使用し、下の図３のデータを計算する。賛成と否定の加重平均値：x=(4x2+5+2x2)/5=3.4。賛成の加重平均値：y=(4x2+5)/3=4.3。使用者の商品の評価値：p=4+4x(60%x(4.3-3.4))=6.16

	商品の評価値	賛成数	否定数
使用者	4	3	2
	賛成ユーザ１	賛成ユーザ２	賛成ユーザ３
商品の評価値	4	4	5
	否定ユーザ１	否定ユーザ２	
商品の評価値	2	2	

図３　加重平均計算の例

5.3 実験結果

	アイテム1	アイテム2	アイテム4	アイテム5	アイテム6	アイテム3	平均値	類似度	アイテム3の予測値
被推薦者	5	4	4	5	4	1			
加重平均付け	5	4.8	2.72	5.8	4.96		4.7		3.85
ユーザB	5	3	4	4	4	4	4	0.65	
加重平均付け	5	3.6	2.56	5.28	4.96	2.72	4.1	0.88	
ユーザC	5	3	3	4	3	2	3.6	0.87	
加重平均付け	5	2.4	2.04	4.64	2.16	1.36	2.9	0.7	
ユーザD	4	3	3	4	3	5	3.4	0.88	
加重平均付け	4	2.4	1.92	3.04	3	1	2.6	0.81	
ユーザE	3	2	2	3	2	4	2.4	0.88	
加重平均付け	3.48	0.4	1.36	2.16	2.24	1.6	1.9	0.81	

表3　加重平均重み付けの結果

同じ実験データを使用し、表3の加重平均重み付けデータを使用すると、アイテム３の予測値は3.85である。

評価値は加重平均重み付けすると、変化範囲が0から9くらいなのでアイテム3は被推薦者に推薦するべきではない。

5.4 考察

1. 攻撃者DとEは類似度ランキングの変化が小さい
2. アイテム３の評価値は大きく変化した
3. 推薦の結果により、加重平均重み付けを追加すると、攻撃者の影響が小さくなり、正しい推薦を行った

5.5 欠点

加重平均重み付けしたの評価値データの変化が大きいので、類似度の計算結果が不安定かもしれない。

6 既存の協調フィルタリング＋加重平均重み付け

6.1 定義

1)類似度の計算

既存の協調ファイルタリングを用いて、類似度を計算する

2)予測値の計算

加重平均重み付したのデータを利用して、予測値を計算する

6.2 実験結果

	アイテム1	アイテム2	アイテム4	アイテム5	アイテム6	平均値	ユーザAとの類似度	アイテム3	加重平均重み付けたアイテム3	アイテム3の予測値
被推薦者	5	4	4	5	4	4.4		1		2.5
ユーザB	5	3	4	4	4	4	0.65	4	2.72	
ユーザC	5	3	3	4	3	3.3	0.87	2	1.36	
ユーザD	4	3	3	4	3	3.7	0.88	5	1	
ユーザE	3	2	2	3	2	2.7	0.88	4	1.6	

表4　既存の協調フィルタリング＋加重平均重み付けの結果

同じ実験データを使用し、類似度計算の入力データは元データを利用して、アイテム3の評価値を予測する時に、加重平均重み付けデータを使用すると、アイテム３の予測値は2.5であるので、アイテム3は被推薦者に推薦するべきではない。

6.3 考察

1. 攻撃者DとEは類似度ランキングの変化がない
2. アイテム３の評価値は大きく変化した
3. 推薦の結果により、既存の協調フィルタリング＋加重平均重み付けを追加すると、攻撃者の影響が小さくなり、正しい推薦を行った

7 課題

1)収集した実験データの中に販売促進攻撃データだけ入ってるので、これから、販売排除攻撃データを含めって、多種類実験データを収集する必要がある。

2)何%のユーザが賛成、反対を入力すればシステムは成り立つという検証が必要である。

8 おわりに

今後、多種類実験データを収集して、攻撃対策の提案手法を再検証すると進めていきたいと考えている。

参考文献

[1] 田中克己、角谷和俊（監訳）：情報推薦システム入門　理論と実践
Recommender Systems An　Introduction
(2012)
[2] 栗原　隆平：Web教材データベースからの教材推薦サービスに関する研究(Recommendation service from Web material database) 平成24年度東京電機大学情報
環境研究科梗概
[3] ゲーム推薦：http://dimguilgames.jp/other/reco.php（２０１３）
[4] ダウンロード型ゲーム推薦フォーム：http://dimguilgames.jp/cgi/reco/free/postmail.html（２０１２）