KBhave_Discussion4.Rmd

Kumudini Bhave

July 12, 2017

Overview : Attacks On Recommender Systems

The author talks about the attack on the IMDb, to rate a movie negatively much before it's release date, in the context of the political scenario. The article discusses, how everyday world issues influences such attacks on recommender systems.

Points To Ponder

Recommenders Systems have become a dependancy of everyday life of a common man , as we have gradually inched more and more towards ever progressing technology in a competitive world. It has influenced us to a greater extent from normal grocery shopping to high end electronics, books buying to online articles reading, From following people on twitter to marketing our own profile. We get (or we want!) recommendations to up our spending(be it in time, money) and to up the revenue (of the Recommender companies).

This influence is what drives the mischief. That is because a mass can be easily influenced to target their following, be it a product, a movie, an article, or a person profile.

It is a medium that is available, cheap and easy, and more so because it's known that it would be accepted .

There can be different types of attacks, some of them are : - random attack : where all item ratings of injected profile are filled with random values. The intuitive idea is that generated profile should contian typical ratings so they are considered neighbours to other real profile. It is relatively simple, and less effective as does not require much knowledge.

- average attack : avarage rating per item is used to determine the injected profile ratings. Such profiles have more neighbours.And such attacks are hence more effective when applied to memory based user-user , item-item based collaborative filtering systems.
- bandwagon attack :exploits more knowledge about ratings database so as to craete more neighbours of injected profiles. It targets the popular items.
- segment attack : this is derived more from the marketing insight that promotional activities are more effective when applied to individual tailored market segments.

Possible Strategies

One of the aspects of recommender systems is the privacy and security of users which can be compromised by such attacks. This could be dealt with by considering some of the following ways.

- Data perturbation: Here ,there are privacy preserving variants of CF algorithms that work on centralized but obfuscated data. The idea is to scramble the orginal data in a way that the server , even though doesnot know the exact values of the customer ratings , but knows a range of data, can still do meaningful computation .

- Distributed collaborative filtering : Here the ideas is to store the private information in a distributed manner , ie to distribute the knowldge and avoid storing in central place, making it harder for attacker to gain access.

Reference :

1. Recommender Systems: The Textbook
2. https://www.washingtonpost.com/news/morning-mix/wp/2017/04/19/wisdom-of-the-crowd-imdb-users-gang-up-on-the ?utm_term=.0cd86bd6e658
