Expert Systems With Applications 44 (2016) 217–229

Contents lists available at ScienceDirect

Expert Systems With Applications

journal homepage: www.elsevier.com/locate/eswa

Robustness analysis of arbitrarily distributed data-based recommendation methods

Burcu Yurekli Yilmazel, Cihan Kaleli*

Computer Engineering Department, Anadolu University, Eskisehir 26555, Turkey

ARTICLE INFO

Keywords:
Robustness
Detection
Shilling
Distributed data
Arbitrarily
Privacy
Collaborative filtering

ABSTRACT

Due to different shopping routines of people, rating preferences of many customers might be partitioned between two parties. Since two different e-companies might sell products from the same range to the identical set of customers, the type of data partition is called arbitrarily. In the case of arbitrarily distributed data, it is a challenge to produce accurate recommendations for those customers, because their ratings are split. Therefore, researchers propose methods for enabling data holders' collaboration. In this scenario, privacy becomes a deterrent barrier for collaboration, accordingly, the introduced solutions include private protocols for protecting parties' confidentiality. Although, private protocols encourage data owners to collaborate, they introduce a new drawback for partnership. Since, whole data is distributed and parties do not have full control of data, any malicious user, who knows that two parties collaborate, can easily insert shilling profiles to system by partitioning them between data holders. Parties can have trouble to find such profile injection attacks by employing existing detection methods because of they are arbitrarily distributed. Since profile injection attacks can easily performed on arbitrarily distributed data-based recommender systems, quality, and reliability of such systems decreases, and it causes angry customers. Therefore, in this paper, we try to describe aforementioned problems with arbitrarily distributed data-based recommender systems. As a first step, we analyze robustness of proposed arbitrarily distributed data-based recommendation methods against six well-known shilling attack types. Secondly, we explain why existing detection methods cannot detect malicious user profiles in distributed data. We perform experiments on a well-known movie data set, and according to our results, arbitrarily distributed data-based recommendation methods are vulnerable to shilling attacks.

1. Introduction

The utilized technologies in Web 2.0 allow the Internet users to do more than retrieving only information. Accordingly, people become an active member of the Internet environment, and they can do most of their daily activities, e.g., socializing, shopping, and learning through the Internet (Kaleli, 2014). However, people face with more information to be handled due to huge amount of data provided by the Internet. Therefore individuals need a computer-based expert system pretending a human expert for decision-making purposes. In order to simplify extraction of useful information process, researchers introduce recommender system concept which are designed to produce personalized recommendations for individuals (Bobadilla, Ortega, Hernando, & Gutiérrez, 2013). Collaborative filtering (CF) is one of the most popular recommender systems, and it operates on a user-item matrix which containing customer preferences on various items.

Success of a CF system strongly depends on having adequate number of user data. Otherwise, accuracy of the produced predictions might not satisfy customers' expectations, herewith, reputation of such systems is decreased. Conversely, it is not always possible to collect sufficient amount of customer preferences. Especially newly established e-companies might have trouble to offer recommendation service to their customers due to lack of qualified data (Kaleli & Polat, 2012b). Besides, customer preferences might distributed among young companies. In order to overcome this challenge for such companies, intuitively, collaboration of data holders comes into mind. However, due to commercial concerns and obligations arising from the regulations published by OECD (2005)[1], they might hesitate to collaborate. Hence, researchers propose methods enabling data holders' collaboration without jeopardizing their privacy (Kaleli & Polat, 2012a; Yakut & Polat, 2012a). In the proposed studies, researchers consider two or more parties collaboration on three

* Corresponding author. Tel.: +90 222 321 35 50; fax: +90 222 323 95 01.
E-mail addresses: byurekli@anadolu.edu.tr (B. Yurekli Yilmazel), cihankaleli@gmail.com, ckaleli@anadolu.edu.tr (C. Kaleli).

[1] The organisation for Economic Co-operation and Development.

http://dx.doi.org/10.1016/j.eswa.2015.09.012
0957-4174/

different data distribution scenarios, i.e., horizontal, vertical, and arbitrarily. In horizontally distributed data, the parties have exactly different users having ratings for a common item set. Conversely, data holders have a common user set and different items in vertically distributed data. Unlike other distribution scenarios, in arbitrarily distributed data (ADD), both users and items are common for data holders.

As previously mentioned, recommender systems can be considered as a type of expert systems since they help individuals for decision making. When a recommendation process is performed on ADD, besides individuals, data owners also need an intelligent system in order to protect their privacy against collaborated parties during distributed computations.

The main motivation behind CF methods depends on user correlations. When an active user (a) requests a prediction for a target item (q), traditional CF algorithms firstly form a's neighborhood and then produce a prediction for q by employing users having rating for q in the neighborhood. Therefore, users' preference vectors are very essential components for recommender systems. However, collecting customer profiles also causes the main weakness of CF algorithms. Consider that a malicious vendor which wants to increase its products' popularity might produce fake user profiles, and might send them to the central server. Also, with the same method, a vendor might try to decrease popularity of a competitive merchant's products. Consequently, CF systems might be defenseless against such shilling attacks (Burke, Mobasher, & Bhaumik, 2005). In order to show how shilling profiles can be generated, researchers introduce several attack strategies (Gunes, Kaleli, Bilge, & Polat, 2012). As a second step, researchers also study on detection ways of the fake user profiles from a given user-item matrix. Main methods for shilling profile detection are classification, clustering, and statistical analysis methods.

In previous two paragraphs, two basic problems, insufficient data and shilling attacks, of CF systems are briefly stated. According to studies in literature, data holders can overcome insufficient data problem by employing private protocols, and it is possible to detect shilling attacks with existing detection methods. On the other hand, due to privacy concerns, the parties in collaboration with other data holders do not have full control of distributed user data. Therefore, it is inevitable that such companies becomes vulnerable to shilling attacks. If attackers who know more than one party are in collaboration during producing recommendation process and they employ private protocols, they are sure that the parties cannot access each others' data. Therefore, they can produce distributed attack profiles and can easily insert them to distributed CF system. Since existing detection methods can only discover shilling profiles if they are employed to centralized data, it is a problem to detect malicious user attacks in privacy-preserving distributed CF (PPDCF) systems. In nutshell, in this study, we aim to point out a new research problem which is robustness of PPDCF methods against shilling attacks. It is obvious that, if e-companies do not sure about being robust against malicious user attacks, they might hesitate to collaborate with other parties even if they need it. In this study, we focus on the proposed PPDCF methods for ADD between two parties, and we analyze robustness of such methods against six well known shilling attacks. Also, we show how an attacker can perform attacks to privacy-preserving CF on arbitrarily distribute data (PPCFADD) methods. Finally, we discuss why existing detection methods cannot be directly employed on PPCFADD methods.

Major contributions of this article are listed below:

1. Designing shilling attacks against PPCFADD methods for both numeric and binary data are studied.
2. Existing PPCFADD methods robustness against six attack shilling models are analyzed.
3. Why existing detection methods cannot be directly employed in PPCFADD is discussed.
4. A new research direction is figured out.

The remainder of the paper is organized as follows. In Section 2, related work in PPDCF schemes, and shilling attacks are reviewed, and the need for this study is explained. In Section 3, preliminary works are briefly described. We describe how to design shilling attacks on distributed numeric and binary data in Section 4. Real databased experiments and their results are given in Section 5. Finally, in Section 6, conclusions and future work are presented.

2. Related work

Due to need for adequate user data during CF processes, collaboration of online vendors on distributed data while preserving their privacy has become an important research field. To overcome challenges caused by insufficient data, various PPDCF schemes have been proposed. As previously mentioned, data distribution scenarios might be horizontal, vertical and arbitrarily in CF systems, and data can be distributed between two or more parties. Since our study focuses on only ADD between two parties, in this section, we cover the studies including two parties.

Initial study on collaboration of two parties in a CF process is proposed by Polat and Du (2008). The authors present schemes for binary rating based top-N recommendations on horizontally or vertically partitioned data between two parties. This study shows that it is possible to offer recommendations based on partitioned data without violating confidentiality. Besides top-N recommendation, researchers also introduce private schemes for prediction models. Kaleli and Polat (2007) provide a solution using naïve Bayesian classifier (NBC) on horizontally or vertically partitioned data between two parties with privacy, where ratings were binary. In order to make possible private party collaboration on numeric data-based CF systems, Yakut and Polat (2010) investigate how to provide singular value decomposition-based recommendations on horizontally or vertically partitioned data. Besides horizontal or vertical partitioning, researchers also propose solutions for ADD, which is more common than others in real life scenarios. Yakut and Polat (2012a) propose a numeric data-based scheme to provide predictions on PPCFADD. In (Yakut & Polat, 2012c), the authors introduce the concept of cross distributed data (CDD), which is a special and simpler case of ADD. They propose hybrid CF-based schemes that produce predictions for single items having numerical rating values, based on CDD. The authors also suggest a private scheme enabling collaboration of two vendors for producing binary predictions on ADD (Yakut & Polat, 2012b).

As a result of these studies, online vendors with insufficient data increased the accuracy of their predictions without giving up privacy through collaboration. Although accuracy problem caused by distributed data have been solved and privacy expectations that obstacles collaboration have been ensured in these studies, PPDCF algorithms can also suffer from shilling attacks.

The possibility of manipulating the outcomes of CF algorithms by injecting malicious profiles into the system database is introduced by O'Mahony, Hurley, and Silvestre (2002a). After shilling attack concept is introduced by O'Mahony et al. (2002a), a lot of research in different aspects are studied on "shilling" or "profile injection attacks". One group of researchers focuses on shilling attack strategies and generating profile injection attacks against CF algorithms. Initially, O'Mahony discusses shilling attack strategies in his doctoral dissertation (O'Mahony, 2004). In following, Lam and Riedl (2004, 2005) explore several open questions related to effectiveness of shilling attacks. Mobasher, Burke, Bhaumik, and Williams (2005) discuss basic shilling attack models such as random, average, bandwagon, and love/hate attacks, and compare their effectiveness across user-based and item-based CF. Burke et al. (2005) examine success of bandwagon and popular item attacks against CF systems. Similarly, Mobasher, Burke, Williams, and Bhaumik (2006) investigate segment attack