The Performance of Location Aware Shilling Attacks in Web Service Recommendation

Min Gao, Key Laboratory of Dependable Service Computing in Cyber Physical Society, Ministry of Education, Chongqing University, Chongqing, China & School of Software Engineering, Chongqing University, Chongqing, China
Xiang Li, Key Laboratory of Dependable Service Computing in Cyber Physical Society, Ministry of Education, Chongqing University, Chongqing, China & School of Software Engineering, Chongqing University, Chongqing, China
Wenge Rong, School of Computer Science and Engineering, Beihang University, Beijing, China
Junhao Wen, Key Laboratory of Dependable Service Computing in Cyber Physical Society, Ministry of Education, Chongqing University, Chongqing, China & School of Software Engineering, Chongqing University, Chongqing, China
Qingyu Xiong, Key Laboratory of Dependable Service Computing in Cyber Physical Society, Ministry of Education, Chongqing University, Chongqing, China & School of Software Engineering, Chongqing University, Chongqing, China

ABSTRACT

The location aware collaborative filtering (LACF) is one of the most successful technique of predicting the Quality of Service (QoS) in Internet of Things (IoT) service recommendation systems. However, the openness of CF web service recommendation renders them vulnerable to the injection of attack profiles consisting of apocryphal QoS values (also identified as shilling attacks). Combined with location factors, such profiles might exert greater impact on the LACF compared with traditional CF method. Unfortunately, to the best of the authors’ knowledge, there is few research on such kind of attack model in the literature. Therefore, in this paper, the authors first construct three kinds of attack models including LAA, LAB, and LAR (location aware - average, bandwagon, and random) models and compare the impact of the classical shilling attacks (CSA) and location aware shilling attacks (LASA) on LACF. Furthermore, the authors use two attack detectors to compare the robustness of CSA and LASA. The experimental results on WS-DREAM dataset indicate that the LACF indeed suffers from CSA and LASA. Besides, in comparison with CSA, the LASA models do not always exert more influence on the LACF and the profiles injected by LASA are easier to be detected.

KEYWORDS
Collaborative Filtering, Location Aware Shilling Attacks, QoS, Web Service

1. INTRODUCTION

It is universally acknowledged that the tremendous growth of Internet of Things (IoT) services is making it difficult for users to obtain suitable services. To tackle with this problem, Web services discovery (Kumara, Paik, Koswatte, & Chen, 2014) and services recommendation have become major research directions in recent years. Collaborative filtering (CF), based on the core assumption that users who have expressed similar interests in the past will share common interests in the future (Shi, Larson,
2014; Yu, 2014), is one of the most successful and widely used recommendation technique. The traditional CF service recommendation algorithm estimates Quality-of-Service (QoS) values of a target service for an active user, utilizing QoS values either contributed by other users resembling the active user or taken from analogous services. As a description of non-functional characteristics of services (Zheng, Ma, Lyu, & King, 2011), including response time, price, throughput, availability, and popularity (Chen, Paik, & Hung, 2015), QoS plays a key role in service recommendation since numerous QoS-aware paradigms have been applied to the domain of service selection (Zheng, Ni, Deng, & Liu, 2010). In actual fact, some QoS properties are highly related to the locations of the service users (Zheng, Ma, Lyu, & King, 2009), for example, users in the same geographic location are likely to have similar response time values when invoking the same service. Thus, one growing area of research in the area of recommendation systems is taking user location information into consideration (Li, Luo, & Yin, 2013; Lo, Yin, Deng, Li, & Wu, 2012; Chen, Zheng, Yu, & Lyu, 2014).

Although the preceding works improve the accuracy of the recommendation to a certain extent, there does exist a serious challenge. Open service-oriented environment provides opportunities for malicious users to make biased feedback ratings, impairing the evaluation of certain services for commercial benefit. Malicious users, usually known as shilling attackers (Zhang, 2010), insert attack profiles with counterfeit QoS values into recommendation systems to affect their recommendation results. Some researchers (Qiu, Zheng, Wang, Yang, & Lyu, 2013) addressed the issue that some user-contributed QoS values can be untrustworthy. For example, service providers may give high QoS values to their own services while bad mouthing services of their competitors. To solve this problem, Wang, Zheng, Wu, Lyu, and Yang (2015) proposed a reputation measurement approach to detect and prevent the malicious feedback. Li, Gao, Rong, Xiong, and Wen (2016) analyzed how the classical shilling attacks and Parote attacks affect the CF web service recommendation algorithms. However, existing literatures rarely consider user locations when applying attacks. If the shilling attackers construct the attack profiles combining the data of user location, how severe the impact will be on location aware web service recommendation systems? Whether these attack profiles are difficult to be detected? These questions are crucial to location aware CF (LACF).

Therefore, to guide individuals and groups for this, we explore the impact of location aware shilling attacks on LACF recommender system in this paper. To this end, we construct three new location aware shilling attack (LASA) models: location aware random attack (LAR), location aware average attack (LAA), and location aware bandwagon attack (LAB), based on three classical shilling attack models (CSA) (Gunes, Kaleli, Bilge, & Polat, 2014): random attack (CAR), average attack (CAA), and bandwagon attack (CAB). Moreover, we compare how LACF is affected by CSA and LASA on the WS-DREAM dataset. At last, two shilling attack detection methods are utilized to evaluate the robustness of CAS and LASA models.

The rest of the paper is organized as follows. Section 2 introduces background of the related work including CF, service recommendation, the LACF recommendation, and the shilling attack detection methods. Section 3 illustrates the construction of LASA models and describes a location aware shilling attack scenario for LASA. Experimental study and discussion are elaborated in Section 4. Finally, our conclusion and future research directions are discussed in Section 5.

2. BACKGROUND

2.1. Service Recommendation

During web service recommendation process, different features have been employed for different purposes (Rong, Peng, Ouyang, Liu, & Xiong, 2015) e.g. QoS (Zheng, et al. 2011). As a type of non-functional properties, QoS is widely used in web service recommendation. The users might expect service candidates with lower cost and faster response time. At present, one of the most popular methods in predicting QoS aware web services recommendation is CF techniques and a
Minimum Database Determination and Preprocessing for Machine Learning
www.igi-global.com/chapter/minimum-database-determination-and-preprocessing-for-machine-learning/214833?camid=4v1a

High Performance Approach for Server Side SOAP Processing
www.igi-global.com/chapter/high-performance-approach-server-side/59924?camid=4v1a