ROBUSTNESS ANALYSIS OF LOCATION AWARE COLLABORATIVE FILTERING FOR WEB SERVICE RECOMMENDATION

Xiang Li[1,2], Min Gao[1,2,*], Wenge Rong[3], Junhao Wen[1,2], Qingyu Xiong[1,2]
[1]Key Laboratory of Dependable Service Computing in Cyber Physical Society (Chongqing University), Ministry of Education, Chongqing, 400044, China
[2]School of Software, Chongqing University, Chongqing 400044, China
[3]School of Computer Science and Engineering, Beihang University, Beijing 100191, China
smzy.lx@cqu.edu.cn, gaomin@cqu.edu.cn, w.rong@buaa.edu.cn, jhwen@cqu.edu.cn, xiong03@cqu.edu.cn

Abstract

The collaborative filtering (CF) is one of the most successful technique to predict the Quality of Service (QoS) in Internet of Things (IoT) service recommendation systems. In which, location aware CF (LACF) has widely been paid attention as it takes geographical position into consideration. However, the openness of CF web service recommendation makes them vulnerable to the injection of attack profiles consisted by malicious QoS values (also identified as shilling attacks). If attackers construct the profiles with the information of location, the LACF may be affected more severely than CF. Therefore, to demonstrate the vulnerability of LACF to location aware shilling attack, this paper first constructs three kinds of attack models including LAA, LAB, and LAR (location aware -average, bandwagon, and random) attack models according to the different behaviors of attackers. Furthermore, the paper compares the impact of the classical shilling attacks and location aware shilling attacks on LACF. The experimental results on WSDREAM dataset show the LACF indeed suffers from shilling attacks and location aware shilling attacks. Besides, the results show an interesting phenomena: in comparison with classical shilling attacks, the location aware shilling attacks do not always make more influence on the LACF.

Keywords: Collaborative filtering, Location aware shilling attacks, QoS, Web service

1. INTRODUCTION

The tremendous growth of Internet of Things (IoT) services makes it difficult for users to obtain suitable services. Quality-of-Service (QoS) is usually employed for describing nonfunctional characteristics of services (Zheng, 2011) including response time, price, throughput, availability, and popularity (Chen, 2015). It also plays a key role in the service recommendation and a lot of QoS-aware paradigms have been applied to the domain of service selection (Thio, 2005; Zheng, 2010). Collaborative filtering (CF) is one of the most successful and widely used recommendation technique, which is based on the core assumption that users who have expressed similar interests in the past will share common interests in the future (Shi, 2014; Shao, 2007; Chen, 2010; Yu, 2014). The traditional web service recommendation algorithm, CF is usually used to estimate QoS values of a target service for an active user, either based on QoS experiences of the other users similar to the active user or based on QoS records of the other services similar to the target service. However, some QoS properties (e.g., response time and invocation failure-rate) are highly related to the locations of the service users (Zheng, 2009). For example, customers in the same geographic location will have similar response time values when invoking a same service. Moreover, many researchers have taken the information of user location into consideration (Wanaka, 2016), not matter in recommendation systems or the other fields. Thus, researchers (Lo, 2012; Chen, 2014) proposed CF web service recommendation systems combine the QoS and the locations of users and services. Although these algorithms improve the accuracy of the recommendation results in a degree, they also face to a serious challenge.

Open service-oriented environment provides pportunities for malicious users to make biased feedback ratings to impair the measurement results for commercial benefit. Malicious users are usually called shilling attackers (Zhang, 2010). They insert attack profiles which include biased QoS values for the target services and other selected services into recommendation systems to affect the accuracy of these systems. Qiu (2013) also revealed some user-contributed QoS values can be untrustworthy. For example, the service providers may give high QoS values of their own services and bad mouthing their competitors' services. To solve the problem, Wang (2015) proposed a reputation measurement approach to detect and prevent the malicious feedback. Li et.al (2016) analyzed how the classical shilling attacks and Parote attacks affect the CF web service recommendation algorithms. But if the shilling attackers construct the attack profiles combine the information of users' location, how impact will be caused on location aware web service recommendation systems? This question is short of discussion in recent years.

Therefore, in this paper, we explore the impact of location aware shilling attacks behavior on location aware CF (LACF) service recommendation. 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

*Corresponding author

DOI: 10.29268/iciot.2016.0003

on three classical shilling attack models (CSA) (Gunes, 2014): average attack (CAA), bandwagon attack (CAB), random attack (CAR), which have been used on the stability of recommendation algorithms in recently years. Moreover, we compare how the LACF is affected by CSA and LASA on the WSDREAM dataset.

The rest of the paper is organized as follows. Section 2 introduces background of the related work including CF, web service recommendation, and the LACF web service recommendation. Section 3 illustrates the construction of LASA models and provides a location aware shilling attack scenario to give a better understanding of LASA. Experimental study and discussion are elaborated in Section 4, and Section 5 concludes this paper and points out some possible future directions.

2. BACKGROUND

2.1 CF Recommendation Algorithms

At present, CF is one of the most popular methods in predicting QoS of web services. CF recommends personalized products or services for the users based on QoS values of service invocation or other factors. It predicts the QoS values of invoking service by collecting information from historical services invocation data. In the process of user-based CF, it first determines similar user set, for example, calculates similarity by Pearson correlation coefficient (PCC). For instance, for a given user-service response time matrix (R), the similarity of user a and user b can be calculated with (1) (Mobasher, 2005):

$$sim(a,b)=\frac{\sum_{s\in S}(r_{a,s}-\bar{r}_a)(r_{b,s}-\bar{r}_b)}{\sqrt{\sum_{s\in S}(r_{a,s}-\bar{r}_a)^2}\sqrt{\sum_{s\in S}(r_{b,s}-\bar{r}_b)^2}} \quad (1)$$

where S denotes the service set that are invoked by both user a and user b, $r_{a,s}$ and $r_{b,s}$ denote the response time which were produced when a and b invoked service s respectively, and $\bar{r}_a$, $\bar{r}_b$ represents the average response time of a and b respectively.

Then it utilizes the response times of selected K nearest neighbors (KNN) to predict response time of service s according to the user similarities. The prediction value is calculated as follows (Cai, 2014),

$$P_{a,s}=\bar{r}_a+\frac{\sum_{b\in K} sim(a,b) * (r_{b,s}-\bar{r}_b)}{\sum_{b\in K} sim(a,b)} \quad (2)$$

where b denotes one of a's neighbors, K is the set of selected most similar neighbor, sim (a, b) denotes the similarity between a and b, $\bar{r}_a$ and $\bar{r}_b$ represent the average response time of a and b respectively, and $r_{b,s}$ denotes the response time of service s invoked by user b. It recommends top-N web services to the user according to the predictions of response time.

Except the user-based CF algorithm, item-based CF, hybrid CF, matrix factorization based CF algorithms are also usually used in web service recommender systems. But, we only select the user-based CF algorithm at the preliminary discussion of the effect of shilling attacks in service recommendation systems.

2.2 Service Recommendation

In recent years much research has been devoted to web service recommendation. During the recommendation process, different features have been employed for different purposes, e.g., invocation rate (Rong, 2015). As a type of non-functional properties, QoS is also widely used in web service recommendation. For example, the users might expect service candidates with lower cost and faster response time. At present, one of the popular methods in predicting QoS aware web services recommendation is using CF techniques and a lot of sophisticated approaches have been proposed in the literature. Shao et al. (2007) proposed a user-based CF algorithm to predict QoS values, while several other researchers (Chen, 2010; Yu, 2014; Chen, 2013) combined user-based and item-based CF algorithm to recommend services (Zheng, 2011; Wu, 2013). For example, Jiang et al. (2011) proposed a hybrid CF method by considering the personalization of both services items and users according to the fact that QoS values of popular services are stable to every user and the contribution of popular services to calculate the user similarities is small. Similarly, Zhang et al. (2011) proposed a CF-based service ranking mechanism based on historical invocation data. Although prior work has shown that CF algorithms are effective in predicting QoS values, QoS values from invocations are easily affected by network environment factors. QoS in different regions will have a big difference and then make the recommendation results a great deviation (Chen, 2014; Lo, 2012). In next subsection, we will introduce a location-aware CF web service recommendation approaches.

2.3 Location aware service recommendation

To improve the recommend accuracy, Chen et al. (2014) took the locations of users into consideration when predicting QoS. They employed the location information and QoS values to cluster users and services, and then generated the recommendation list by combing the user-based and item-base CF algorithms for users based on the clustering results. Lo et al. (2012) also utilized the location information for the QoS prediction through an improved matrix factorization model with two novel location-based regularization terms. Other researchers (Tang, 2012; Liu, 2016) mined more information about users and services from IP address. They identified the Autonomous System (AS) and the country user belongs to according to his IP address and preferred find the similar neighbors in same AS and country.

Tang proposed an approach (2012) compute the users and services similarity combine the location information of users and services. They represented a user location as a triple (IP_u,

ASN_u, $CountryID_u$), where IP_u denotes IP address of the user hosts, ASN_u denotes number of the Autonomous System (AS) that IP_u belongs to, and $CountryID_u$ denotes the ID of the country that IP_u belongs to. Generally speaking, intra-AS traffic is much better than inter-AS traffic regarding transmission performance, such as response time (Zhang, 2012). Therefore, the Internet AS-level topology has been widely used to measure the distance between Internet users. Note that users located in the same AS are not always geographically close, and vice versa. When they predicted the missing QoS, they chose neighbors for the active user u in same AS to compute user similarity first. If u has no neighbors in the AS that u belongs to, the neighbors will be chosen in the same country with u. If there is no neighbors in AS and country that u belongs to, neighbors will be chosen from all of users in the system. They could get a user similarity vector which is composed by the degree of similarity between the active user and all other users. Then they adapted the traditional Top-K algorithm to identify the Top-K similar neighbors for u. Finally, they predicted the missing QoS by equation (2) and get a recommendation list for u. Our paper mainly studies the location aware shilling attack based on this recommendation algorithm.

3. SHILLING ATTACKS IN LACF SERVICE RECOMMENDATION

In this section, we will present a scenario to illustrate how shilling attackers (malicious users) alter the recommendation results by injecting LASA profiles into a certain LACF and introduce how to construct the LASA profiles.

3.1 Shilling Attack Example in the LACF Service Recommendation

In general, the purpose of shilling attack in service recommendation is to increase or decrease the recommended frequency of target services. Shilling attacks can be divided into push attacks and nuke attacks (Zhang, 2014). Push attacks increase target services' ranking and make them much easier to be recommended. On the contrary, nuke attacks reduce the recommendation frequency of the target services. When a target service is chosen, multiple attack profiles can be produced to make the target service to be easier or more difficult to be recommended. Assuming that a recommendation system has five normal users Alice and {U_2, U_3, U_4, U_5}, three malicious users {A_1, A_2, A_3}, and five services {S_1, S_2, S_3, S_4, S_5} (see Table I). Alice lives in New York (CountryID is 31) and the number AS is 17 that she belongs to. The three malicious users counterfeit their IP address to make their AS number and CountryID same as Alice. Each item in the table denotes the invocation response time for a web service S_i. In the example, Alice wants to invoke a weather forecasting service, and S_3 and S_5 are such services. The shilling attackers want to inject the attack profiles to increase the invocation frequency of S_5.

Table I. LASA in LACF Service Recommendation

	ASN_u	CountryID	S_1	S_2	S_3	S_4	S_5	Correlation with Alice
Alice	AS17	31	4	1.01	?	8	?	-
U_2	AS9	11	0.5	0.6		3.3	5	0.7362
U_3	AS8	13	2	6	0.2	5	6.02	-0.1525
U_4	AS200	22	8		0.6	5.03	5	0.0193
U_5	AS73	20	6	0.6	0.3	6.01	3	0.8167
A_1	AS17	31	3.87		2	8	0.1	0.9965
A_2	AS17	31		1	3	8.1	0.1	0.9745
A_3	AS17	31	4	1	2	7.9	0.1	0.9847

We can get the similarities of users by PCC as shown in Table I. Under normal circumstances, there is no user in the AS and country Alice belongs to. So we get the similarities of Alice with other normal users. And U_5 is the most similar user with Alice. Thus, the recommender system can predict the response time of S_3 and S_5 for Alice by the QoS values of services U_5 invoked. The results are 1.45 and 4.15 by CF technique. The recommender system will recommend S_3 to Alice because it has a shorter response time. After injecting attack profiles into this system, the AS and country of attackers are same to Alice. So attackers will be chosen for compute the user similarity. A_1 is the most similar to Alice. Then the system predicts the response time for Alice by A_1 instead of U_5. The results are 2.867 and 0.727 by CF technique. Finally S_5 will be recommended to Alice and the shilling attacker achieves its goal. The above example shows that injection of fake profiles can affect the LACF service recommendation algorithm indeed. Therefore, it is important to study how shilling attacks will influence the LACF service recommender systems.

3.2 LASA models

Generally, attack models are approach to constructing attack profiles based on knowledge of recommender systems, e.g., its rating database or the response time in the systems. An attack against the kind of systems consists of a set of attack profiles. An attack profile, as shown in Figure1 (Mobasher, 2005, 2007), consists of an m-dimensional vector of ratings, where m is the total number of items in the system. . Where S_S denotes the selected services, S_F denotes randomly filled services, S_ϕ denotes services that are not invoked and do not have QoS values, and S_t is the attack target set. Malicious users use these fictitious profiles to pretend the closed neighbors of normal users.

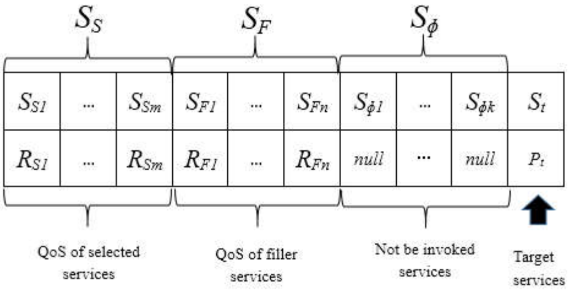


Figure 1. The General Form of Attack Profiles in CF-Based Web Service Recommendation

Similarly, shilling attacks in LACF can be constructed by injecting biased QoS profiles with the users' location information. LASA models can be constructed based on the three CSA models: average attack, random attack, bandwagon attack. The form of LASA profile can be shown in Figure 2, where ASNu and CountryID denote the AS and country of users who invoked the target services S_t, the rest of the profile are same as the Figure1. We will introduce the three new attack models LAR, LAA, LAB in the following subsections.

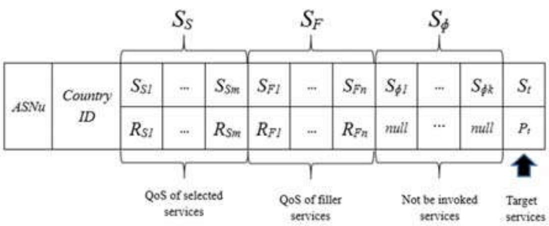


Figure 2. The General Form of Attack Profiles in Location-Aware CF-Based Web Service Recommendation

With the different selection and filler method for the sets of above mentioned S_S, S_F, S_t different shilling attack models can be built. The values of S_F are open to any probability distribution, but the normal distribution is usually used (Mobasher, 2007). Thus we choose the normal distribution for S_F in classical models.

1) LAR: Filler services are selected randomly from the set of all services. The QoS of S_F in random attack are randomly generated with normal distribution, where μ and σ denote the average value and the standard deviation of QoS values of all the services, respectively. It is a low-knowledge attack as minimal knowledge is required to obtain the mean of all services.

2) LAA: The set of select services is empty. Filler services are obtained with normal distribution, where μ uses the individual mean for each service in S_F rather than the global mean and σ is the standard deviation of each service in S_F. In a web service recommendation system, we set S_t as the minimum response time in push attack.

3) LAB: This attack model takes advantage of the Zipf's law. The attacker using this model will build attack profiles containing the popular services. Such profiles will have a good probability of being similar to a large number of users, since the popular services have been invoked by many users. The selected services are the frequently invoked services. QoS of S_S and S_t will be designated as the minimum in web services recommendation. QoS of S_F is obtained based on a normal distribution, where μ is the average value of S_F and σ is the standard deviation of S_F. The LAB is also a low-knowledge attack as the popular services can usually be easily obtained.

Though attackers can construct some more sophisticated models, for instance, by mixing the mentioned models to be a hybrid attack or mixing the attacks with noise profiles to get more complicated attack models, for the preliminary discussion of the basic shilling attack models in LACF and their influence, only the low cost attack models mentioned above are taken into consideration in this paper.

3.3 Attack Effect Evaluation Metrics

To evaluate the attack effect, prediction shift is usually used (O'Mahony et al, 2004). To evaluate how the LACF will be affected by CSA and LASA, we use average prediction shift (preshift). The calculation of preshift is shown as (3):

$$preshift = \frac{\sum_{u \in U} (P'_{u,s} - P_{u,s})}{|U|} \quad (3)$$

where $P_{u,s}$ and $P'_{u,s}$ denotes the predicted response time of user u to service s before and after attacks, and U denotes the users in the test set who have invoked the service s.

4. EXPERIMENTAL STUDY

The dataset used in the experiments is WSDREAM dataset, which is collected by Zheng et al. (2010). This dataset include QoS values that contain response time and throughput of 1,974,675 invocations executed by 339 users on 5,825 services. To simulate the real situation, we randomly removed a certain number of response time records to reduce data density to 20%. Then we randomly took 80% of the data as a training set and the rest as a test set. To illustrate the effect of attacks, without loss of generality, we applied push attacks and analyzed how the CSA and LASA attacks affect the predictions of the response times in LACF service recommendation.

4.1 Overall Attack Effects on LACF

To evaluate the overall attack effects on LACF service recommendation when they facing CSAs and LASAs, we random chose the 10 services as the attack targets. For each attack models, attack sizes are 3%, 6%, 9%, 12%, and 15%, the filler size is 10%, and the number of neighbor is 30.

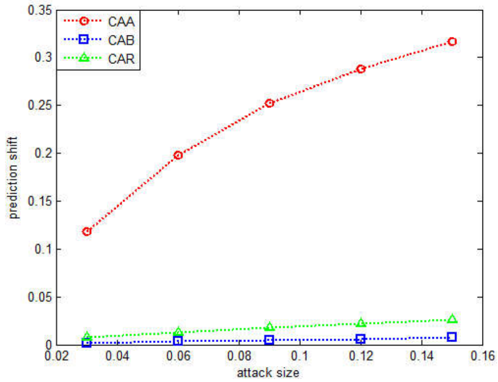


Figure 3. The Effect Caused by CSA Models

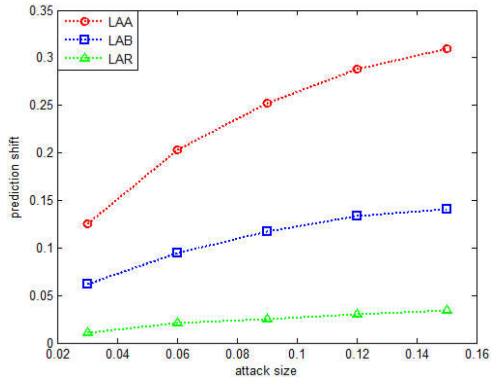


Figure 4. The Effect Caused by LASA Models

The experimental results (See Figure 3 and Figure 4) show that:

(1) All of the three CSA models and three LASA models can affect LACF service recommendation. The performance of the various attack models gets increased as the attack size increases.

(2) Two average attack models: CAA and LAA are more powerful than other attack models. They cause 0.12 to 0.32 prediction shifts.

(3) For the random attack models, the LAR causes slightly higher prediction shifts than the CAR.

(4) But for the bandwagon attack models, the prediction shifts caused by LAB attacks, with the range (0.6, 1.3), are significantly higher than those caused by CAB attacks with the range (0, 0.1).

In the dataset, more than 90 percent of response times are in [0, 1] second, as can be seen in the Figure 5. Therefore, the prediction shift caused by these attacks are considerable.

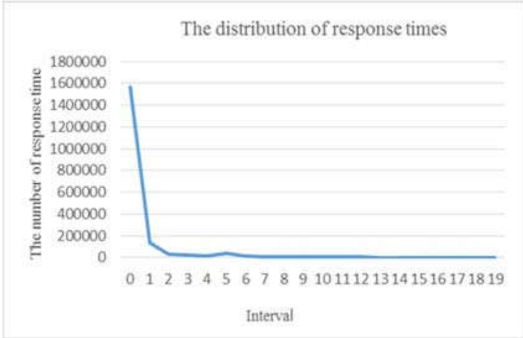


Figure 5. The Distribution of Response Times

4.2 Attack Effects on LACF for Selected Services

In a web service recommender system, the services that have better QoS values are more easily recommended to users, e.g., services with shorter response times. Therefore, the services which response times are shorter are valuable for the research on the attack effects. In Figure 5, we found the most of response times are less than 1s. Therefore, we conducted experiments for these services. The attack sizes and attack models and the number of neighbors are set same as in the 4.1 subsection. The response times of services less than 1s were selected as target services.

Table 2. The Prediction shift of Selected Services under LASAs and CSAs

Attack size	LAA	LAB	LAR	CAA	CAB	CAR
0.03	13.72%	0.85%	1.81%	15.40%	1.21%	2.70%
0.06	21.07%	1.35%	2.84%	23.60%	1.33%	3.90%
0.09	25.50%	2.19%	3.94%	29.08%	1.43%	4.89%
0.12	28.52%	2.58%	4.67%	32.94%	1.56%	5.66%
0.15	30.20%	2.88%	5.10%	35.94%	1.71%	6.20%

The experimental results are shown in Table 2. The number in the table is the ratio of prediction shift (preshift * 100%). The results show that:

(1) For the selected services, LACF service predictions are influenced by all of the attack models. Similar to the results for all services, the performance of the attack models increases as the attack size increases.

(2) The average attacks (CAA and LAA) achieve the best (same to the results of overall attack effects) with prediction shifts of 13~36 percent.

(3) Different with the overall results, the random attacks (CAR and LAR) achieve the second with prediction shifts of 1 ~ 6 percent.

(4) The bandwagon attacks (CAB and LAB) achieve the worst with prediction shifts of about 1 ~ 3 percent. Only in bandwagon attacks, LASA outperform the CSA model.

4.3 Analysis

As shown as the experimental results, LACF suffered from all attack models of CSA and LASA, whether for all services or for selected services. In which, average attack models achieve the best.

LASA models construct the attack profiles combining the information of location by forging the IP address of the users. It was expected to improve the number of the nearest neighbors and increase the effect of attack profiles. However, the experiment results show an interesting phenomenon: in comparison with CSA, LASA models only make slight influence on the LACF in some cases; they achieve worse results than CSA models in most cases. Although the location of user has been taken into consideration in the attack profile, it is difficult to ensure every attacker become the closest neighbors with the active user. The phenomenon should be owed to this reason.

5. CONCLUSIONS

LACF service recommender systems have widely been paid attention, but the characteristics of systems relying on the information of user location and QoS provided by users would make them vulnerable to QoS injection attacks. In this paper, we constructed three LASA models based on three CSA models. Through injecting attack profiles generated from these different attack models, we compared the effects of CSA and LASA on LACF. At the same time, we focus on the impact of attacks on predicting response time in different attack sizes. Experiments indicate that all the attack models achieve influence on the QoS prediction, the LAB model has considerable influence on response time prediction, and the location information can improve the attack effect only in some cases.

6. ACKNOWLEDGEMENT

This research was partially supported by the National Natural Science Foundation of China (61472021), the National Key Basic Research Program of China (2013CB328903), the Chongqing Research Program of Basic Research and Frontier Technology (cstc2015jcyjA40049), and the Fundamental Research Funds for the Central Universities (106112014CDJZR095502).

7. REFERENCES

Cai, Y., Leung, H. F., Li, Q., Min, H., Tang, J., Li, J. (2014). Typicality-based collaborative filtering recommendation. IEEE Transactions on Knowledge and Data Engineering, 26(3), pp.766-779.

Chen, X., Liu, X., Huang, Z., Sun, H. (2010). Regionknn: A scalable hybrid collaborative filtering algorithm for personalized web service recommendation, Proceedings of the IEEE International Conference on Web Services, USA, 2010, pp. 9–16.

Chen, X., Zheng, Z., Liu, X., Huang, Z., Sun, H. (2013). Personalized qos-aware web service recommendation and visualization, IEEE Transactions on Services Computing, 6(1), pp.35-47.

Chen, X., Zheng, Z., Yu, Q., Lyu, M. R. (2014). Web service recommendation via exploiting location and QoS information, IEEE transactions on parallel and distributed systems, 25(7), pp. 1913-1924.

Chen, W., Paik, I., Hung, P. C. (2015). Constructing a global social service network for better quality of web service discovery, IEEE Transactions on Services Computing, 8(2), pp. 284-298.

Gunes, I., Kaleli, C., Bilge, A., Polat, H. (2014). Shilling attacks against recommender systems: a comprehensive survey, Artificial Intelligence Review, 42(4), pp.767-799.

Jiang, Y., Liu, J., Tang, M., Liu, X. (2011). An effective web service recommendation method based on personalized collaborative filtering, Proceedings of the IEEE International Conference on Web Services, USA, 2011, pp.211-218.

Li, X., Gao, M., Rong, W., Xiong, Q., Wen, J. (2016). Shilling Attacks Analysis in Collaborative Filtering Based Web Service Recommendation Systems, Proceedings of the IEEE International Conference on Web Services, USA, 2016, pp.538-545.

Lo, W., Yin, J., Deng, S., Li, Y., Wu, Z. (2012). Collaborative web service qos prediction with location-based regularization, Proceedings of the IEEE International Conference on Web Services, USA, 2012, pp. 464-471.

Liu, J., Tang, M., Zheng, Z., Liu, X., Lyu, S. (2015). Location-Aware and Personalized Collaborative Filtering for Web Service Recommendation, in IEEE Transactions on Services Computing, 9(5), pp. 686-699.

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

Mobasher, B., Burke, R., Bhaumik, R., Williams, C. (2005). Effective attack models for shilling item-based collaborative filtering systems, Proceedings of the 2005 WebKDD Workshop, USA, 2005.

O'Mahony, M., Hurley, N., Kushmerick, N., Silvestre, G. (2004). Collaborative recommendation: A robustness analysis, ACM Transactions on Internet Technology (TOIT), 4(4), pp. 344-377.

Qiu, W., Zheng, Z., Wang, X., Yang, X., Lyu, M. R. (2013). Reputation-aware qos value prediction of web services, Proceedings of Services Computing (SCC), USA, 2013, pp. 41-48.

Rong, W., Peng, B., Ouyang, Y., Liu, K., Xiong, Z. (2015). Collaborative personal profiling for web service ranking and recommendation, Information Systems Frontiers, 17(6), pp.1265-1282.

Shao, L., Zhang, J., Wei, Y., Zhao, J., Xie, B., Mei, H. (2007). Personalized qos prediction for web services via collaborative filtering, Proceedings of the IEEE International Conference on Web Services, USA, 2007, pp. 439-446.

Shi, Y., Larson, M., Hanjalic, A. (2014). Collaborative filtering beyond the user-item matrix: A survey of the state of the art and future challenges, ACM Computing Surveys, 47(1), pp.1-45.

Tang, M., Jiang, Y., Liu, J., Liu, X. (2012). Location-aware collaborative filtering for QoS-based service recommendation, Proceedings of the IEEE International Conference on Web Services, USA, 2012, pp. 202-209.

Thio, N., Karunasekera, S. (2005). Automatic measurement of a qos metric for web service recommendation, Proceedings of Australian Software Engineering, Australia, 2005, pp. 202-211.

Wang, S., Zheng, Z., Wu, Z., Lyu, M. R., Yang, F. (2015). Reputation measurement and malicious feedback rating prevention in web service recommendation systems, IEEE Transactions on Services Computing, 8(5), pp.755-767.

Wu, J., Chen, L., Feng, Y., Zheng, Z., Zhou, M. C., Wu, Z. (2013). Predicting quality of service for selection by neighborhood-based collaborative filtering, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 43(2), pp. 428-439.

Wanaka S, Tsubouchi K. (2016). Location History Knows What You Like: Estimation of User Preference from Daily Location Movement, *Proceedings of the Second International Conference on IoT in Urban Space*, JAPAN, 2016, pp. 8-13.

Yu, Q. (2104). Qos-aware service selection via collaborative Qos evaluation, *World Wide Web*, 17(1), pp. 33–57

Zheng, Z., Ma, H., Lyu, M. R., King, I. (2009). Wsrec: A collaborative filtering based web service recommender system, *Proceedings of the IEEE International Conference on Web Services*, USA, 2009, pp. 437-444.

Zhang, F. (2010). Analysis of love-hate shilling attack against e-commerce recommender system, *Proceedings of Information Science and Management Engineering (ISME)*, China, 2010, pp. 318– 321.

Zhang, Q., Ding, C., Chi, C. H.(2011), Collaborative filtering based service ranking using invocation histories, *Proceedings of the IEEE International Conference on Web Services*, USA, 2011, pp. 195–202.

Zhang, F. (2014), Analysis of profile injection attacks against recommendation algorithms on bipartite networks, *Proceedings of 2014 International Conference on Management of e-Commerce and e-Government*, China, 2014, pp. 1–5

Zhang, G., Tang, M., Cheng, S., Zhang, G., Song, H., Cao, J., Yang, J. (2012). P2P traffic optimization, *Science China Information Science*, 55(7), pp.1475-1492.

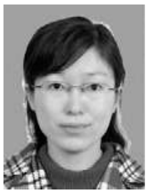
Zheng, Z., Zhang, Y., Lyu, M. R. (2010). Distributed qos evaluation for real-world web services, *Proceedings of Web Services (ICWS), 2010 IEEE International Conference on*, USA, 2010, pp. 83-90.

Zheng, Y., Ni, H., Deng, H., Liu, L.(2010), A dynamic web services selection based on decomposition of global QoS constraints, *Proceedings of 2010 IEEE Youth Conference on Information Computing and Telecommunications*, China, 2010, pp. 77–80.

Zheng, Z., Ma, H., Lyu, M. R., King, I. (2011). Qos-aware web service recommendation by collaborative filtering, *IEEE Transactions on Services Computing*, 4(2), pp. 140-152.

Authors

Xiang Li. He is currently an MSc student in School of Software Engineering, Chongqing University, China. His research interests include machine learning, data mining, and recommendation systems.



Min Gao received the MS and PhD degrees in computer science from Chongqing University in 2005 and 2010 respectively. She is an associate professor at the School of Software Engineering, Chongqing University. She was a visiting researcher at the School of Business, University of Reading. Her research interests include recommendation system, service computing, and data mining. She has published over 30 refereed journal and conference papers in these areas. She has grants from the National Natural Science Foundation of China, the China Postdoctoral Science Foundation, and the China Fundamental Research Funds for the Central Universities. She is member of the IEEE and CCF.

Wenge Rong is an associate professor at Beihang University, China. He received his PhD from University of Reading, UK, in 2010; MSc from Queen Mary College, University of London, UK, in 2003; and BSc from Nanjing University of Science and Technology, China, in 1996. He has many years of working experience as a senior software engineer in numerous research projects and commercial software products. His area of research covers machine learning, data mining, service computing, and information management.

Junhao Wen is the vice dean and professor of the School of Software Engineering, Chongqing University. He received the PhD degree from Chongqing University in 2008. His research interests include service computing, cloud computing, and software dependable engineering. He has published more than 80 refereed journal and conference papers in these areas. He has more than 30 research and industrial projects and developed many commercial systems and software tools.

Qingyu Xiong is the dean of the School of Software, Chongqing University. He received the BS and MS degrees from the School of Automation, Chongqing University in 1986 and 1991, respectively, and the PhD degree from Kyushu University of Japan in 2002. His research interests include neural networks and their applications. He has published more than 100 journal and conference papers in these areas. Moreover, he has more than 20 research and applied grants.