SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

August 2017, Vol. 60 082102:1–082102:16
doi: 10.1007/s11432-015-9029-y

FCT: a fully-distributed context-aware trust model for location based service recommendation

Zhiquan LIU[1], Jianfeng MA[1,2*], Zhongyuan JIANG[2] & Yinbin MIAO[2]

[1]*School of Computer Science and Technology, Xidian University, Xi'an* 710071*, China;*
[2]*School of Cyber Engineering, Xidian University, Xi'an* 710071*, China*

Received September 8, 2016; accepted January 21, 2017; published online July 4, 2017

Abstract With the popularity of location based service (LBS), a vast number of trust models for LBS recommendation (LBSR) have been proposed. These trust models are centralized in essence, and the trusted third party may collude with malicious service providers or cause the single-point failure problem. This work improves the classic certified reputation (CR) model and proposes a novel fully-distributed context-aware trust (FCT) model for LBSR. Recommendation operations are conducted by service providers directly and the trusted third party is no longer required in our FCT model. Besides, our FCT model also supports the movements of service providers due to its self-certified characteristic. Moreover, for easing the collusion attack and value imbalance attack, we comprehensively consider four kinds of factor weights, namely number, time decay, preference and context weights. Finally, a fully-distributed service recommendation scenario is deployed, and comprehensive experiments and analysis are conducted. The results indicate that our FCT model significantly outperforms the CR model in terms of the robustness against the collusion attack and value imbalance attack, as well as the service recommendation performance in improving the successful trading rates of honest service providers and reducing the risks of trading with malicious service providers.

Keywords trust model, fully-distributed, context-aware, location based service, service recommendation

Citation Liu Z Q, Ma J F, Jiang Z Y, et al. FCT: a fully-distributed context-aware trust model for location based service recommendation. Sci China Inf Sci, 2017, 60(8): 082102, doi: 10.1007/s11432-015-9029-y

1 Introduction

Nowadays, mobile services are ubiquitous owing to the rapid development of mobile devices and wireless technologies [1, 2]. As mobile services are characterized by mobility, ubiquity, convenience, etc., service consumers can access them through mobile devices (e.g., smart phone, tablet computer, etc.) via wireless networks at anytime anywhere [3].

As we know, lots of mobile services (e.g., hotel, restaurant, store, etc.) are closely related to locations, and they form an independent research area known as LBS, which is a kind of the most important mobile service and generally focuses on providing mobile services to service consumers based on their current locations [4]. In addition, LBSR system aims at providing valuable service suggestions to service consumers for meeting their functional and personalized requirements [5–7].

[*] Corresponding author (email: jfma@mail.xidian.edu.cn)

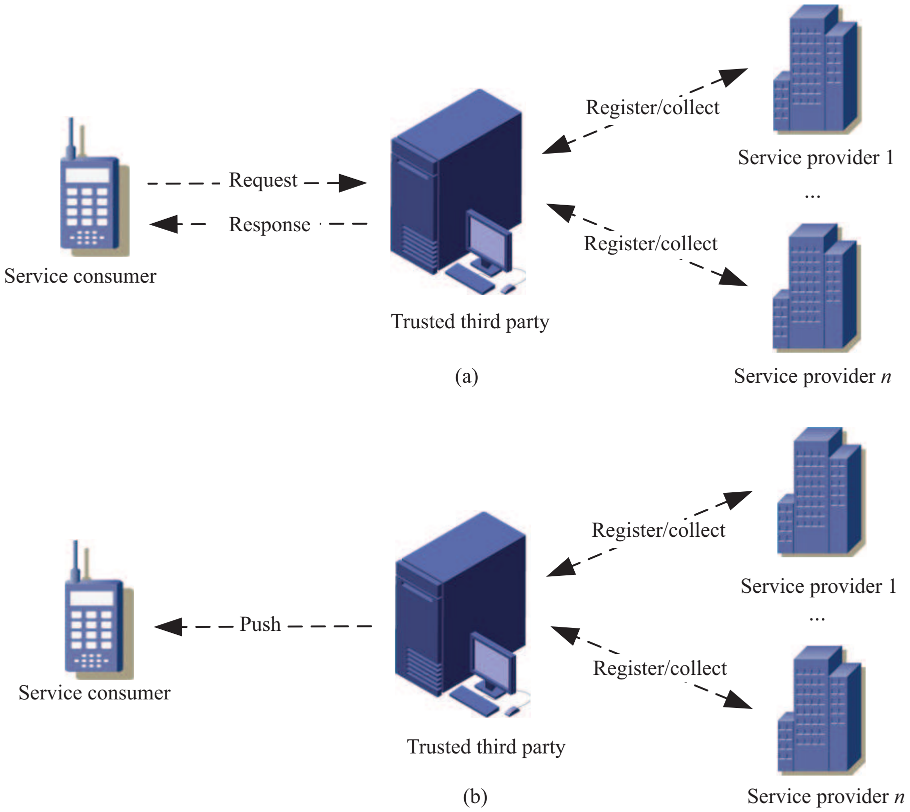

Figure 1 (Color online) The classic trust models for LBSR. (a) Request-response trust models; (b) push trust models.

The trust management in LBSR is of necessity for both service consumers and service providers. On one hand, service consumers need to select trustworthy service providers for mobile services which meet their functional and personalized requirements and avoid trading with malicious service providers [8]. On the other hand, service providers need to prove their trust to potential service consumers for the purpose of enjoying the trust of more service consumers and improving their transaction volumes [9].

Recently, a large number of trust models for LBSR have been proposed [10–19]. In the classic request-response trust models as shown in Figure 1(a), a trusted third party (e.g., a web platform) is assumed. In the pre-processing stage, service providers (e.g., hotels) register their mobile services (e.g., rooms) with the trusted third party, or the trusted third party collects the information of service providers. When a service consumer (e.g., a tourist) needs a mobile service (e.g., booking a room), he/she first sends a request to the trusted third party. Then the trusted third party obtains the top-k recommendation list by utilizing some strategies (e.g., matrix factorization [15], data mining [16], fuzzy mathematics [18,19], collaborative filtering [19], etc.) based on the current location and other information (e.g., time, preference, moving-speed, etc.) of the service consumer. Afterwards, the trusted third party sends a response (i.e., the top-k recommendation list) to the service consumer. With the aid of recommendation list, the service consumer can make a better decision about mobile service selection. The classic push trust models illustrated in Figure 1(b) are similar to the request-response ones, and the only difference is that the trusted third party proactively pushes recommendation information to service consumers in a timely manner.

Apparently, the classic trust models for LBSR have the following limitations.

• **The classic trust models are centralized.** In the classic trust models, a trusted third party is needed to specialize in collecting mobile service information and providing mobile service recommendations. These models are centralized in nature, and the trusted third party is assumed to be completely reliable and upright (i.e., never colludes with malicious service providers). However, in reality the trusted third party is usually a commercial institution (e.g., Baidu[1]), Meituan[2]), Dianping[3]), etc.), and it is very likely to collude with some malicious service providers for its commercial interests. A typical example is the notorious paid listing [20] (i.e., the top-k recommendation services are not the best services but the ones for which their providers have paid much money to the trusted third party). Once the trusted third party colludes with malicious service providers, it will provide misleading service recommendations and all the service consumers may suffer vast losses as they totally trust the trusted third party (e.g., Zexi Wei's death is mainly due to the deceitful service recommendation from Baidu[4])). Meanwhile, there exists the single-point failure problem in these models and the trusted third party may become the bottleneck of the whole recommendation system. Thus it is of necessity and significance to explore decentralized trust models for LBSR. Besides, in LBS service providers are usually in close proximity to service consumers and they can communicate directly with each other, which makes it possible to build a fully-distributed LBSR model.

- **The locations of service providers are fixed.** In the classic trust models, only the movements of service consumers are considered, and the locations of service providers are regarded as fixed. Nevertheless, it is not always correct, such as in the situation where some traveling salesmen walk around a city for selling their commodities to nearby residents. The residents need to select trustworthy traveling salesmen to obtain good commodities and avoid trading with malicious traveling salesmen. Another example is the taxi. In several previous studies [21–23], the researchers have analyzed the significance of trust/reputation in taxi selection. In most cases, the taxi drivers are strangers to the passengers. If a passenger takes a malicious taxi, he/she may be taken a roundabout route (meaning higher fee-charging), be robbed, or even be murdered, and these conditions frequently occur in our daily life[5]). Thus, when a passenger needs a taxi, not only the distance (i.e., waiting time) but also the trust (i.e., reliability and security) of taxi should be considered. In the above two cases, the locations of service providers are no longer fixed, thus a more general trust model, in which the movements of both service consumers and service providers are considered, for LBSR should be built.

- **Service providers are passive.** In the classic trust models, service providers will do nothing but wait to be recommended by the trusted third party and then be selected by service consumers. It is far from sufficient for service providers to improve their transaction volumes due to the competitions with others. Therefore, we should consider building a novel trust model, in which service providers are able to proactively participate in the recommendation process, for LBSR.

To the best of our knowledge, there are no existing trust models yet that can deal with the aforementioned limitations, and this is just the motivation for this work. In this paper, we improve the outstanding CR model [24] and propose a novel FCT model for LBSR. The main characteristics and contributions of our FCT model are summarized as follows:

- **Our FCT model is fully-distributed.** In our FCT model, the recommendation operations are conducted by service providers directly instead of the trusted third party, so the latter is no longer needed. Besides, in our model the service consumers do not completely trust other entities. Instead, they will comprehensively consider several kinds of factor weights, such as number, time decay, preference and context weights, to discount the service feedbacks of previous service consumers and derive the trust of candidate service providers. As a result, even there exists some proportion of collusion (between malicious service providers and a portion of service consumers), the potential service consumers can still effectively distinguish between honest and malicious service providers, which has been validated by the experiments and analysis in Subsection 4.3. Besides, the single-point failure problem of the classic centralized trust models no longer exists in our FCT model due to the decentralized architecture.

- **The locations of service providers are movable.** In our FCT model, the locations of both

[1]) http://www.baidu.com.

[2]) http://www.meituan.com.

[3]) http://www.dianping.com.

[4]) http://qz.com/674030/baidu-chinas-version-of-google-is-evil-a-growing-number-of-users-say.

[5]) http://www.eastbuzz.com/2016/05/04/response-to-female-passengers-robbed-kills-to-the-last-drop-drivers-registered; https://www.boston.com/news/crime/2016/08/11/uber-driver-arrested-on-rape-charge-by-everett-police; http://www.the-week.co.uk/76037/uber-driver-accused-of-taking-sleeping-woman-on-85-detour.

service consumers and service providers are movable, so our FCT model is more general than the classic ones. Moreover, the trust information is portable when service providers move due to the self-certified characteristic of our FCT model.

- **Service providers are proactive.** In our FCT model, service providers proactively release their mobile service recommendation information to nearby potential service consumers through their mobile devices, which assists service providers to enjoy the trust of more service consumers and improve their transaction volumes.
- **Our FCT model is context-aware.** In our FCT model, the similarities of service type context and service price context between the potential and previous transactions are calculated so as to ease the notorious value imbalance attack [25].
- **Our FCT model contains user preferences.** To better characterize the trust, the service rating consists of various trust aspects with different preference weights, which can be determined by service consumers. Besides, service consumers can also set multi-attributes according to their requirements, and the recommendation information which is mismatched with their multi-attributes will be ignored.
- **Our FCT model is of robustness.** In our FCT model, we consider four kinds of factor weights, namely number, time decay, preference and context weights, so as to ease the collusion attack and value imbalance attack.
- **Our FCT model is of high performance.** The comprehensive experiments and analysis demonstrate that our FCT model significantly surpasses the CR model in terms of the service recommendation performance in improving the successful trading rates of honest service providers and reducing the risks of trading with malicious service providers, as well as the robustness against collusion attack and value imbalance attack.

The rest of this paper is structured as follows. Section 2 introduces some related work and its limitations. Section 3 presents our FCT model and trust evaluation method in detail. Afterwards, comprehensive experiments and analysis are shown in Section 4, followed by the conclusion in Section 5.

2 Related work

In recent years, LBSR has been widely studied in the literature, and lots of trust models have been put forward. We review some classic trust models according to the theory foundations and research emphases in them.

Context and user preference are considered in many studies. To provide personalized recommendations for mobile tour planning, a novel LBSR model containing various factors (i.e., location, preference, time, constraint, etc.) was put forward by Yu et al. [10]. Afterwards, Waga et al. [11] proposed a context-aware LBSR system based on four factors, namely content, location, time and social network. This system can provide useful recommendations and relevant items in most cases. Subsequently, Barranco et al. [12] paid attention to on-the-move users and brought forward a LBSR system for traveling users. This system incorporates both the speeds and trajectories of users into context, and it can provide personalized service recommendations according to the current locations and driving speeds of users. Besides, Biancalana et al. [13] took both context and user preference into consideration and presented a LBSR system which can identify the functional and personalized needs of users and provide personalized recommendations about the interest points around the current locations of users.

There also exist a lot of researches based on other theories and technologies. Yang et al. [14] brought forward a hybrid LBSR model by integrating the preferences derived from both check-ins and tips with the sentiment analysis technology, and they also proposed a social matrix factorization algorithm which incorporates both social influence and location similarity into location recommendations. In addition, a novel LBSR model based on random walks in a user-space graph was raised by Noulas et al. [15]. This model combines both social network and location visit frequency, and it outperforms the previous trust models. Furthermore, Tan et al. [16] came up with a novel preference-oriented approach for location-based store search based on data mining technology. This approach can efficiently search for the top-k nearby

Table 1 Intuitive comparisons between our FCT model and other LBSR models

Trust model	Architecture	Locations of service provider	Proactive party
Request-response models [10–17]	Centralized	Fixed	Service consumers
Push models [18, 19]	Centralized	Fixed	Trusted third party
Our FCT model	Fully-distributed	Moveable	Service providers

stores which are the most suitable for users. In addition, a synthetic LBSR system which combines online recommendation and offline modeling was put forward by Bao et al. [17]. The online recommendation part relies on the opinions of selected local experts, and the offline modeling part depends on weighted category hierarchy and iterative learning model to derive the preferences and experiences of users, respectively.

Obviously, the above approaches follow a request-response pattern. That is to say, the recommendation system will not return any recommendation information until a service consumer sends an explicit request to it. In order to facilitate service consumers to receive interested recommendation information in a timely manner, several researches took the proactive service recommendation into consideration. Ciaramella et al. [18] came up with a context-aware LBSR system which utilizes the fuzzy logic to derive the situations of users and can deliver recommendations in a proactive way. Besides, a situation-aware LBSR system which can proactively push relevant service recommendations to potential service consumers was put forward by Bedi et al. [19]. The recommendation process is divided into situation assessment and item assessment. The former can be handled by fuzzy inference while the latter can be dealt with by collaborative filtering technology.

Although the above LBSR models provide some brilliant ideas, there exist three common limitations as analyzed in Section 1. Recently, the trusted third party (TTP) free architecture has been widely adopted for location privacy preserving in LBS [26]. These TTP-free schemes usually utilize user collaboration, obfuscation or private information retrieval (PIR) to protect users' location privacy (i.e., hide users' actual locations when they access to certain service provider) [27] and can overcome the limitations of classic centralized TTP-based schemes. However, there is no consideration of trust evaluation or service recommendation in these schemes, thus they cannot be adopted for LBSR. In this paper, we propose a novel FCT model and the intuitive comparisons with other LBSR models are shown in Table 1.

3 Our FCT model and trust evaluation method

In this section, we first introduce our FCT model in detail. Next, we present a matching method based on multi-attributes. Moreover, we introduce the representation of service feedback and comprehensively consider four kinds of factor weights, namely number, time decay, preference and context weights, for service feedback. Finally, we present the detail of trust evaluation procedure.

3.1 Our FCT model

In our FCT model as demonstrated in Figure 2, the recommendation operations are conducted by service providers directly and the trusted third party is no longer needed. Thus our FCT model is significantly distinct from the classic ones as shown in Figure 1.

The concrete scenario of service recommendation in our FCT model is shown in Figure 3. There exist two different perspectives of service provider (SP) and service consumer (SC):

- **In the perspective of SP.** As shown in Figure 3(a), SP(j) broadcasts a service recommendation to nearby SCs (i.e., SC(1)–SC(m)) through its mobile device via wireless technologies, such as Bluetooth, Wireless Fidelity Direct (Wi-Fi Direct), Device-to-Device (D2D) and so on.
- **In the perspective of SC.** As shown in Figure 3(b), SC(i) is surrounded by lots of SPs (i.e., SP(1)–SP(n)), which all satisfy the functional requirements of SC(i). SC(i) first requests SPs to provide their service feedbacks, which are generated with digital signatures and sent to SPs by their previous trading partners, and then stored and updated by SPs in local storage for proving their trust. After receiving these service feedbacks, SC(i) can verify their authenticity with digital signature technology

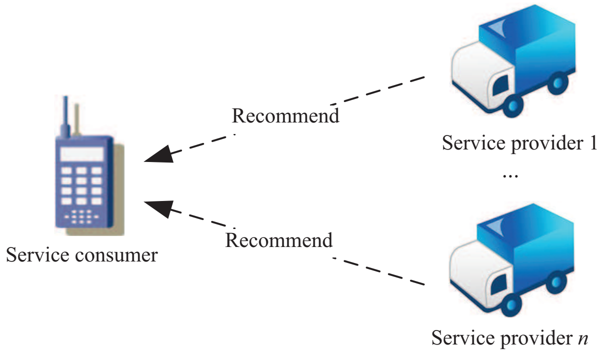

Figure 2 (Color online) Our FCT model for LBSR.

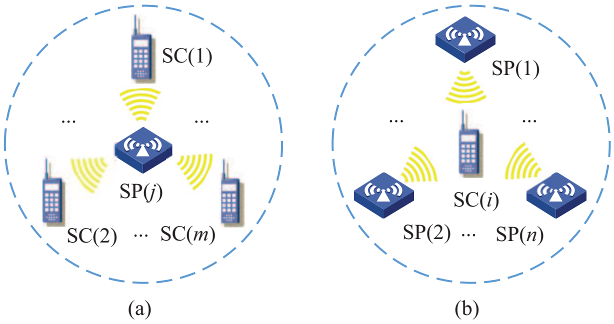

Figure 3 (Color online) The scenario of service recommendation in our FCT model. (a) In the perspective of SP; (b) in the perspective of SC.

when necessary and then calculate out the trust value of every SP. Afterwards, SC(i) can derive the top-k recommendation list and decide which SP it will trade with (e.g., SP(j) is selected). After the trading, SC(i) provides a new service feedback to SP(j) according to its satisfaction degree.

As the service feedbacks are stored and provided by SPs selves (i.e., self-certified [24]), they are portable when SPs move. Therefore, our FCT model supports the movements of SPs.

Benefiting from the rapid development of wireless technologies, most of the existing mobile devices are equipped with Bluetooth and Wi-Fi Direct modules. Based on them, the mobile devices can send messages to each other directly within a certain distance, with the aid of a special application (APP). As we know, the ranges of Bluetooth and Wi-Fi Direct are about tens meters, and the promising D2D technology has a larger communication range [28]. For instance, through the long term evolution direct (LTE Direct) technology, mobile devices can utilize their LTE radios to directly send/broadcast messages to other mobile devices up to 500 m away [29]. In addition, our FCT model can support multi-hops, thus its maximum working range can reach thousands of meters by leveraging the multi-hop LTE Direct technology. Meanwhile, our FCT scheme is lightweight and the calculated amount is very small, thus the trust evaluation can be easily conducted on mobile devices.

As a result, both service providers and service consumers merely need to install an APP (which takes charge of sending/broadcasting and receiving messages by invoking underlying Bluetooth, Wi-Fi Direct and LTE Direct modules, as well as making the trust evaluation and interacting with humans) on their mobile devices. This is very convenient for service providers and service consumers.

In our daily life, we rarely go to a far away place to eat or to shop, thus the main function of LBSR is to assist the potential service consumers to select out the most suitable (i.e., trustworthy) services (e.g., restaurants or stores) from nearby service providers. Therefore, our decentralized scheme can meet with the general LBSR requirements, whereas the long-distance LBSR cannot be provided by our FCT scheme due to its unique characteristics. This is an inherent limitation of the distributed LBSR scheme.

In essence, our FCT scheme adopts the local optimization strategy, just like the well-known ant colony algorithm (ACA) [30]. In ACA, the ants merely care for the nearby situation (instead of the global one)

Table 2 A simple example of our matching method based on multi-attributes

Entity	Multiple attributes with various operations	Match or not
SP(j)	Input device AND (mouse OR keyboard)	–
SC(1)	Input device AND mouse	√
SC(2)	Input device AND scanner	×
SC(3)	Toy AND mouse	×

and make decisions based on their local knowledge. Furthermore, they can update their decisions when they encounter new situations. Similarly, our FCT scheme mainly assists potential service consumers to choose the most suitable (i.e., trustworthy) services from nearby service providers. Furthermore, the top-k recommendation list can be dynamically updated as the situation changes (e.g., some service providers move into or out of the communication range of certain potential service consumer).

3.2 Matching method based on multi-attributes

As the recommendation operations are conducted by SPs directly in our FCT model, SCs are more likely to receive a large number of irrelevant service recommendations. To address this problem, we propose a matching method based on multi-attributes. Both SPs and SCs can set multiple attributes (e.g., function, type, price, etc.) according to their requirements, and various operations (e.g., AND, OR, NOT, XOR, etc.) for multiple attributes are supported. A simple example is shown in Table 2.

When SP(j) broadcasts a service recommendation, SC(1) will receive this service recommendation as its multi-attributes are matched with those of SP(j), whereas SC(2) and SC(3) will ignore this service recommendation as their multi-attributes are mismatched with those of SP(j). Therefore, SCs can only receive interested service recommendations without the trouble caused by a mass of irrelevant ones.

3.3 The representation of service feedback

In our scheme, the service feedback generated by SC(i) for SP(j) is denoted as

$$\mathbf{Sf}(i,j) = (\mathrm{Id}(i), \mathrm{Id}(j), \mathbf{Rt}(i,j), \mathbf{Wg}(i), \mathrm{St}(i,j), \mathrm{Sp}(i,j), \mathrm{Ts}(i,j), \mathrm{Ds}(i,j)),$$

where Id(i) and Id(j) represent the IDs of SC(i) and SP(j), respectively. $\mathbf{Rt}(i,j)$ is denoted as

$$\mathbf{Rt}(i,j) = (\mathrm{Rt}(i,j,1), \mathrm{Rt}(i,j,2), \ldots, \mathrm{Rt}(i,j,\gamma)),$$

where $\mathrm{Rt}(i,j,p)$ $(1 \leqslant p \leqslant \gamma)$ indicates the rating value of p-th trust aspect and its value is an element of the set

$$\mathbb{R} = \{0,1,2,3,4\},$$

where 0, 1, 2, 3 and 4 represent very dissatisfied, dissatisfied, general, satisfied and very satisfied, respectively. $\mathbf{Wg}(i)$ is denoted as

$$\mathbf{Wg}(i) = (\mathrm{Wg}(i,1), \mathrm{Wg}(i,2), \ldots, \mathrm{Wg}(i,\gamma)),$$

where $\mathrm{Wg}(i,p)$ $(1 \leqslant p \leqslant \gamma)$ indicates the preference weight of corresponding trust aspect and its value is an element of the set

$$\mathbb{W} = \{0,1,2\},$$

where 0, 1 and 2 represent uninterested, general and very interested, respectively. $\mathrm{St}(i,j)$ and $\mathrm{Sp}(i,j)$ denote the type and price of mobile service, respectively. $\mathrm{Ts}(i,j)$ represents the timestamp when $\mathbf{Sf}(i,j)$ is generated and $\mathrm{Ds}(i,j)$ denotes the digital signature. Furthermore, the synthetic rating value $\mathrm{Rs}(i,j)$ of $\mathbf{Sf}(i,j)$ can be gained from

$$\mathrm{Rs}(i,j) = \frac{\sum_{p=1}^{\gamma} \mathrm{Rt}(i,j,p) \cdot \mathrm{Wg}(i,p)}{\sum_{p=1}^{\gamma} \mathrm{Wg}(i,p)} \quad \left(\text{where } \sum_{p=1}^{\gamma} \mathrm{Wg}(i,p) \neq 0\right). \tag{1}$$

3.4 Four kinds of factor weights for service feedback

Because of the self-certified characteristic in our FCT model, SPs may merely provide profitable service feedbacks to potential SCs, or even collude with part of SCs to improve their trust values (i.e., collusion attack). Meanwhile, they may also first accumulate high trust values by providing cheap and excellent services, and then cheat SCs by providing expensive and poor services (i.e., value imbalance attack). To ease these attacks, we comprehensively consider four kinds of factor weights, namely number, time decay, preference and context weights.

3.4.1 *The number weight*

To balance the robustness against the collusion attack and the consumptions of storage and bandwidth, $\mathrm{SP}(j)$ merely stores and updates $N(j)$ ($N(j) \leqslant \eta$) service feedbacks, which come from $N(j)$ different previous SCs and are the most favorable for $\mathrm{SP}(j)$. Where η is a system threshold and is set empirically such that the maximum number of SCs colluding with $\mathrm{SP}(j)$ within ω (which is a time window) is less than a half of it. The number weight $\mathrm{Wn}(j)$ corresponding to $N(j)$ is represented as a 0-1 function:

$$\mathrm{Wn}(j) = \begin{cases} 0, & \text{if } N(j) < \eta, \\ 1, & \text{otherwise.} \end{cases}$$

If $N(j)$ is less than η, the service feedbacks are viewed as incredible, so $\mathrm{Wn}(j)$ is set as 0. Otherwise, the service feedbacks are regarded as authentic, so $\mathrm{Wn}(j)$ is set as 1.

3.4.2 *The time decay weight*

Next, we consider the time decay weight $\mathrm{Wt}(i,j)$ for $\mathbf{Sf}(i,j)$, due to the fact that the relatively recent service feedback is more convincing than the less recent one and the outdated service feedback may be completely incredible. Thus $\mathrm{Wt}(i,j)$ is denoted as a piecewise function of $\mathrm{Ts}(i,j)$:

$$\mathrm{Wt}(i,j) = \begin{cases} 0, & \text{if } \mathrm{Tn} - \mathrm{Ts}(i,j) > \omega, \\ \mathrm{e}^{-(\mathrm{Tn}-\mathrm{Ts}(i,j))/\alpha}, & \text{otherwise,} \end{cases} \tag{2}$$

where Tn is the current timestamp and α is a constant. If the time difference between Tn and $\mathrm{Ts}(i,j)$ exceeds ω, $\mathbf{Sf}(i,j)$ is regarded as unreliable, so $\mathrm{Wt}(i,j)$ is set as 0. Otherwise, $\mathrm{Wt}(i,j)$ is denoted as an exponential decay function of $\mathrm{Ts}(i,j)$ [31].

3.4.3 *The preference weight*

Expect for $\mathrm{Wn}(j)$ and $\mathrm{Wt}(i,j)$, we also consider the preference weight $\mathrm{Ws}(i,x)$ between the potential $\mathrm{SC}(x)$ and the previous $\mathrm{SC}(i)$, as the service feedback from a SC which has similar preferences is more trustworthy than that from an entirely different SC. In the sight of $\mathrm{SC}(x)$, there is noting available but $\mathbf{Wg}(i)$ regarding to the preferences of $\mathrm{SC}(i)$, as $\mathrm{SC}(x)$ and $\mathrm{SC}(i)$ may come from different places and be strangers to each other. In addition, $\mathrm{SC}(x)$ can also determine its preference weight $\mathbf{Wg}(x)$. Therefore, $\mathrm{Ws}(i,x)$ can be derived according to the weighted Euclidean distance between $\mathbf{Wg}(x)$ and $\mathbf{Wg}(i)$ [32]:

$$\mathrm{Ws}(i,x) = 1 - \frac{1}{2} \cdot \sqrt{\frac{\sum_{p=1}^{\gamma} (\mathrm{Wg}(x,p) - \mathrm{Wg}(i,p))^2 \cdot \mathrm{Wg}(x,p)}{\sum_{p=1}^{\gamma} \mathrm{Wg}(x,p)}} \quad \left(\text{where } \sum_{p=1}^{\gamma} \mathrm{Wg}(x,p) \neq 0\right).$$

3.4.4 *The context weight*

The last but not least, we also take the context weight into consideration. In concrete terms, we mainly consider two types of most important contextual properties, namely service type and service price.

- **For service type context.** We adopt the eCL@ss[6]), which is a famous industry standard for service and product categorization. For illustration purposes, we give a part of eCL@ss as shown in Figure 4. It

[6]) http://www.eclasscontent.com.

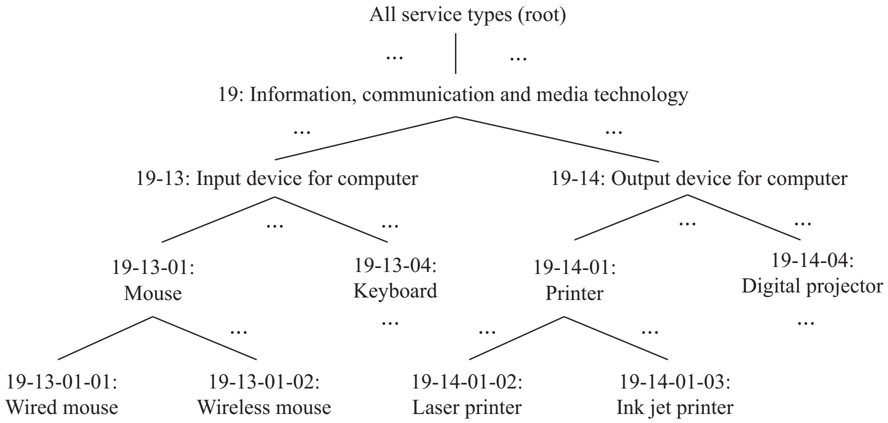
All service types (root)
...
...
19: Information, communication and media technology
...
...
19-13: Input device for computer
19-14: Output device for computer
...
...
...
...
19-13-01: Mouse
19-13-04: Keyboard
...
19-14-01: Printer
19-14-04: Digital projector
...
...
...
...
19-13-01-01: Wired mouse
19-13-01-02: Wireless mouse
19-14-01-02: Laser printer
19-14-01-03: Ink jet printer

Figure 4 A part of eCL@ss (version 9.0).

is a hierarchy tree, in which the nodes represent service types. The similarity of two nodes (e.g., s and t) is measured by the depth $\mathrm{Dp}(s,t)$ of their deepest common ancestor node. For example, the deepest common ancestor node of wired mouse and wireless mouse is mouse, and its depth is 3. A small depth of common ancestor node means weak similarity and a great depth is consistent with strong similarity. Thus the service type context weight $\mathrm{Wy}(i,j,x)$ is represented as a hyperbolic tangent function (where β is a constant) [33]:

$$\mathrm{Wy}(i,j,x)=\frac{\mathrm{e}^{\beta\cdot\mathrm{Dp}(\mathrm{St}(x,j),\mathrm{St}(i,j))}-\mathrm{e}^{-\beta\cdot\mathrm{Dp}(\mathrm{St}(x,j),\mathrm{St}(i,j))}}{\mathrm{e}^{\beta\cdot\mathrm{Dp}(\mathrm{St}(x,j),\mathrm{St}(i,j))}+\mathrm{e}^{-\beta\cdot\mathrm{Dp}(\mathrm{St}(x,j),\mathrm{St}(i,j))}}. \tag{3}$$

- **For service price context.** We consider two cases: (a) The service price of the potential trading is no higher than that of the previous one; (b) The service price of the potential trading is higher than that of the previous one. The former is relatively credible while the latter contains the risks caused by the value imbalance attack, and the risks increase with the price gap. Thus the service price context weight $\mathrm{Wp}(i,j,x)$ is denoted as a piecewise function (where θ is a constant):

$$\mathrm{Wp}(i,j,x)=\begin{cases}1, & \text{if } \mathrm{Sp}(x,j)\leqslant \mathrm{Sp}(i,j),\\ \mathrm{e}^{-(\mathrm{Sp}(x,j)-\mathrm{Sp}(i,j))/\theta}, & \text{otherwise.}\end{cases} \tag{4}$$

3.5 The procedure of trust evaluation

In this subsection, we mainly introduce the procedure of trust evaluation as shown in Figure 5. In concrete terms, the procedure for each trading consists of five steps as follows.

Step 1: Broadcast a service recommendation. At the beginning of a potential trading, $\mathrm{SP}(j)$ broadcasts a service recommendation to nearby potential SCs through its mobile device. The service recommendation contains multiple attributes with various operations to describe the mobile service which $\mathrm{SP}(j)$ provides.

Step 2: Request for service feedbacks. When $\mathrm{SC}(x)$ receives the interested service recommendation from $\mathrm{SP}(j)$, it sends a request to $\mathrm{SP}(j)$ for service feedbacks through its mobile device.

Step 3: Provide service feedbacks. When $\mathrm{SP}(j)$ receives the request from $\mathrm{SC}(x)$, it sends its $N(j)$ service feedbacks to $\mathrm{SC}(x)$. Then $\mathrm{SC}(x)$ can derive their weights and obtain the trust value of $\mathrm{SP}(j)$. In the perspective of $\mathrm{SC}(x)$, $\mathrm{Wn}(j)$, $\mathrm{Wt}(i,j)$, $\mathrm{Ws}(i,x)$, $\mathrm{Wy}(i,j,x)$ and $\mathrm{Wp}(i,j,x)$ are all available, where in essence $\mathrm{Ws}(i,x)$, $\mathrm{Wy}(i,j,x)$ and $\mathrm{Wp}(i,j,x)$ all describe the similarity between the pervious transaction and potential transaction while $\mathrm{Wn}(j)$ and $\mathrm{Wt}(i,j)$ indicate the credibility of service feedbacks from the number and freshness perspectives, respectively. As a result, we combine two methods (i.e., average and product [24,34]) to derive the total weight $\mathrm{Wf}(i,j,x)$ for $\mathbf{Sf}(i,j)$ as

$$\mathrm{Wf}(i,j,x)=\mathrm{Wn}(j)\cdot\mathrm{Wt}(i,j)\cdot(\mathrm{Ws}(i,x)+\mathrm{Wy}(i,j,x)+\mathrm{Wp}(i,j,x))/3, \tag{5}$$

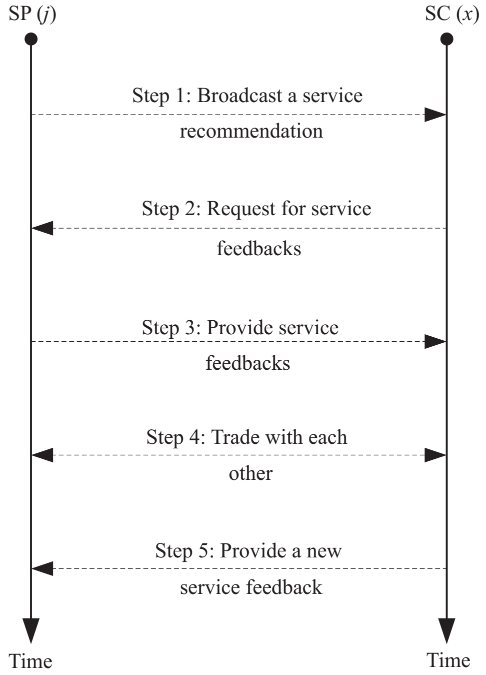
SP (j)
SC (x)
Step 1: Broadcast a service recommendation
Step 2: Request for service feedbacks
Step 3: Provide service feedbacks
Step 4: Trade with each other
Step 5: Provide a new service feedback
Time
Time

Figure 5 The procedure of trust evaluation.

and then the weighted rating value $\mathrm{Rw}(i,j,x)$ of $\mathbf{Sf}(i,j)$ can be computed as

$$\mathrm{Rw}(i,j,x)=\mathrm{Rs}(i,j)\cdot\mathrm{Wf}(i,j,x). \tag{6}$$

Finally, the trust value $\mathrm{Tf}(j,x)$ of $\mathrm{SP}(j)$ can be calculated from

$$\mathrm{Tf}(j,x)=\begin{cases}\dfrac{\sum_{i=1}^{N(j)}\mathrm{Rw}(i,j,x)}{4\cdot N(j)}, & \text{if } N(j)\neq 0,\\ 0, & \text{otherwise.}\end{cases} \tag{7}$$

From (5), we can find that the range of $\mathrm{Wf}(i,j,x)$ is [0, 1] as $\mathrm{Wn}(j)$, $\mathrm{Wt}(i,j)$, $\mathrm{Ws}(i,x)$, $\mathrm{Wy}(i,j,x)$ and $\mathrm{Wp}(i,j,x)$ all fall in the range of [0, 1], and Eq. (1) reveals that $\mathrm{Rs}(i,j)$ is within the range of [0, 4]. Thus we can discover from (6) that the range of $\mathrm{Rw}(i,j,x)$ is also [0, 4], and that of $\mathrm{Tf}(j,x)$ is [0, 1] due to the normalization processing in (7).

Step 4: Trade with each other. If $\mathrm{Tf}(j,x)$ reaches the trust threshold $\mathrm{Th}(x)$ of $\mathrm{SC}(x)$, $\mathrm{SP}(j)$ is regarded as a trustworthy candidate. Similarly, $\mathrm{SC}(x)$ can derive the trust values of other interested SPs and decide whether they are credible candidates or not. Afterwards, $\mathrm{SC}(x)$ can obtain the trustworthy candidate set $\mathrm{Cs}(x)$ as well as the top-k recommendation list according to the trust values of trustworthy candidates, where k is set as the size of $\mathrm{Cs}(x)$ such that all the trustworthy candidates have a chance to be selected. Finally, $\mathrm{SC}(x)$ can select certain SP (e.g., $\mathrm{SP}(j)$) from $\mathrm{Cs}(x)$ to trade with each other with a probability of $\mathrm{Pr}(j,x)$, which can be calculated from

$$\mathrm{Pr}(j,x)=\frac{\mathrm{Tf}(j,x)}{\sum_{\mathrm{SP}(q)\in\mathrm{Cs}(x)}\mathrm{Tf}(q,x)}. \tag{8}$$

Step 5: Provide a new service feedback. After the trading, $\mathrm{SC}(x)$ generates a new service feedback $\mathbf{Sf}(x,j)$ and sends it to $\mathrm{SP}(j)$. Afterwards, $\mathrm{SP}(j)$ updates its local storage by reselecting $N(j)$ most favorable service feedbacks according to the weighted rating value $\mathrm{Rp}(x,j)$. As $\mathrm{SP}(j)$ has no information about future potential service consumers (e.g., $\mathrm{SC}(x')$), $\mathrm{Ws}(x,x')$, $\mathrm{Wy}(x,j,x')$ and $\mathrm{Wp}(x,j,x')$ are all unavailable to $\mathrm{SP}(j)$. Besides, $\mathrm{Wn}(j)$ is the same to all the alternative service feedbacks for $\mathrm{SP}(j)$, thus it is meaningless for reselecting $N(j)$ most favorable service feedbacks. As a result, $\mathrm{SP}(j)$ takes $\mathrm{Wt}(x,j)$

Table 3 The values of parameters in experiments

Parameter	Description	Value
γ	The number of trust aspects	3
η	The number threshold of service feedbacks	20
ω	The time window	200
α	The constant in (2)	100
β	The constant in (3)	0.4
θ	The constant in (4)	10000
τ	The initial trust value	0.1

as the total weight to derive $\mathrm{Rp}(x, j)$, i.e.,

$$\mathrm{Rp}(x, j) = \mathrm{Rs}(x, j) \cdot \mathrm{Wt}(x, j).$$

It should be noted that there exists no available service feedback for newcome SPs, so their trust values derived from the above trust evaluation procedure are 0. In order for them to have certain opportunities to trade with SCs and accumulate the trust, their initial trust values are set as τ, which is a default low value. Meanwhile, in our FCT model, $\mathbf{Sf}(i, j)$ contains the digital signature (i.e., $\mathrm{Ds}(i, j)$) and any change to it can be easily detected, thus SPs cannot modify $\mathbf{Sf}(i, j)$ for self-praise [24]. Moreover, SCs can first select out all the interested SPs from a quality-of-service (QoS) perspective (as revealed in Subsection 3.2), and then choose a credible SP from a trust perspective (as illustrated in Subsection 3.5).

4 Experiments and analysis

To illustrate the performance of our FCT model, we present comprehensive experiments and analysis in this section. In concrete terms, we first introduce the scenario of fully-distributed service recommendation deployed in this work. Next, we present the variations of both average trust values and average successful trading rates of honest SP (HSP) and malicious SP (MSP), respectively. Moreover, we verify the robustness of our FCT model against two kinds of attacks, namely collusion attack and value imbalance attack. Besides, we also deploy and necessarily modify the classic CR model in our scenario for comparison.

4.1 Experiment setting

In our experiments, we employ the standard evaluation indexes (i.e., average trust value variation, average successful trading rate, robustness against the collusion attack and value imbalance attack) and prevalent experiment methods, which are widely adopted in the classic trust schemes [24, 31, 33, 35, 36]. As there is no existing application or open source dataset yet for fully-distributed LBSR, we deploy the following scenario to facilitate the experiments and analysis. There are a total of 1000 SCs and 2 SPs (i.e., a HSP and a MSP). SPs broadcast their service recommendations about various types of mobile services with different prices. SCs can receive these recommendations and evaluate the trust values of SPs. Specifically, every SC takes a trading test as shown in Subsection 3.5 and the timestamp adds 1 after each trading test. If HSP/MSP is selected, the successful trading number of HSP/MSP adds 1. The trust thresholds and preference weights of SCs, as well as the types and prices of mobile services, are randomly generated. The parameters in experiments are set as shown in Table 3.

4.2 Experiment 1

In this experiment, we mainly illustrate the variations of both average trust values and average successful trading rates of HSP and MSP in an honest environment through comparing to the classic CR model. To demonstrate the variations of average successful trading rates, we divide the 1000 times trading tests into 5 equal intervals (i.e., I1–I5) and compute the successful trading rates of HSP and MSP in every interval, respectively. The experiment is repeated 5000 times and the average outputs are shown in Figures 6 and 7.

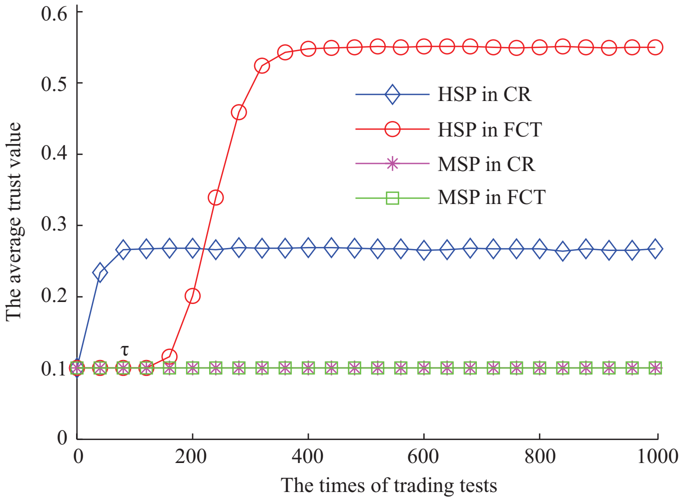

Figure 6 (Color online) The average trust value variations of HSP and MSP in two kinds of trust models.

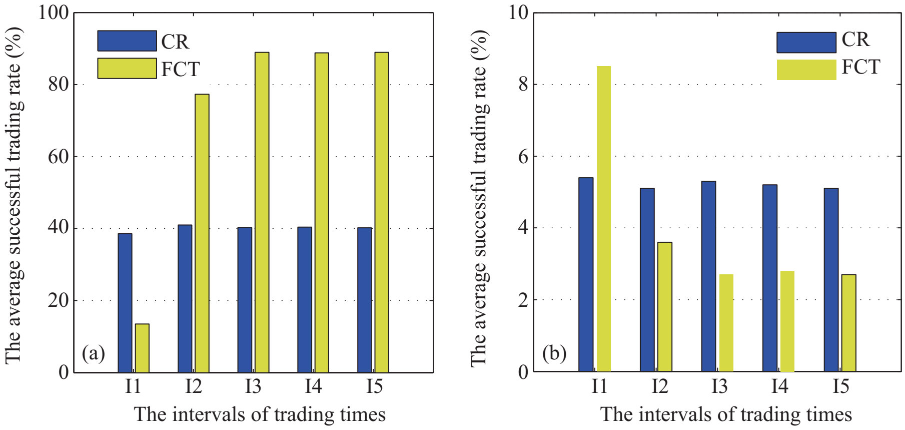

Figure 7 (Color online) The average successful trading rate variations of HSP and MSP in two kinds of trust models. (a) HSP; (b) MSP.

We first analyze the average trust value variations of HSP and MSP in two kinds of trust models as shown in Figure 6. In the initial stage, all the average trust values are equal to τ (0.1) because there is no available service feedback to prove their trust. With the increase of test times (0–80 times), the average trust value of HSP in the CR model rises rapidly (from 0.1 to 0.27), as HSP can provide favorable service feedbacks and the number of service feedbacks is not viewed as a weight in the CR model. In the later trading tests (80–1000 times), HSP in the CR model dynamically maintains a relatively high average trust value (0.27) due to its stable performance, whereas the average trust value of HSP in our FCT model remains unchanged as τ at the start of trading tests (0–120 times) because the number of service feedbacks is less than η, and then quickly improves (from 0.1 to 0.55) in the subsequent trading tests (120–400 times). Moreover, in the later trading tests (400–1000 times), HSP in our FCT model dynamically keeps a greatly higher average trust value (0.55) than that in the CR model (0.27) due to the limitations of the CR model and the improvements in our FCT model. The average trust value of MSP remains unchanged as τ all along since it cannot provide favorable service feedbacks in two kinds of trust models.

Next, we analyze the average successful trading rate variations of HSP and MSP in two kinds of trust models as shown in Figure 7, respectively. For HSP, the variation of average successful trading rate shown in Figure 7(a) is basically consistent with that of average trust value in two kinds of trust models. In I1, the average successful trading rate of HSP in our FCT model (13.5%) is lower than that in the CR model (38.6%). However, with the increase of test times, the average successful trading rate of HSP in our FCT

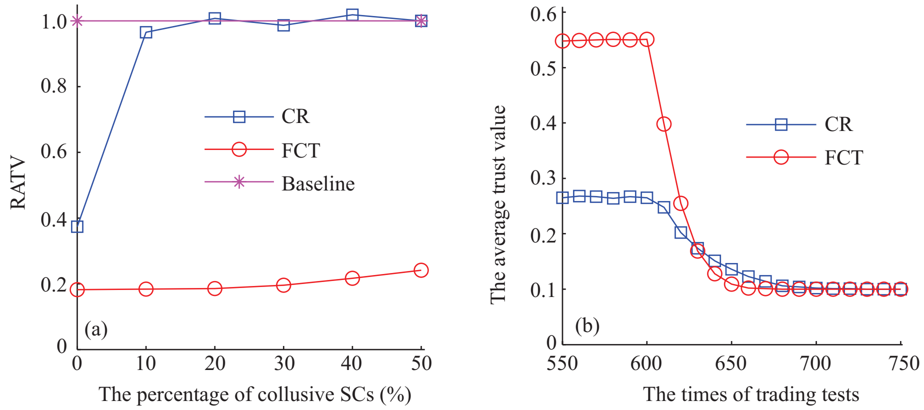

Figure 8 (Color online) The robustness of two kinds of trust models against collusion attack and value imbalance attack. (a) Collusion attack; (b) value imbalance attack.

model rises rapidly (from 13.5% to 88.9%) while that in the CR model basically keeps constant (40.2%). In the stable intervals (i.e., I3–I5), our FCT model significantly improves the average successful trading rate of HSP (by 121.1%) when compared with the CR model. For MSP, though its average trust value keeps unchanged as τ, its average successful trading rate shown in Figure 7(b) changes with the average trust value variation of HSP according to (8). In concrete terms, the average successful trading rate of MSP decreases with the increasing average trust value of HSP. In I1, the average successful trading rate of MSP in our FCT model (8.5%) is higher than that in the CR model (5.4%). However, with the increase of test times, the average successful trading rate of MSP in our FCT model decreases rapidly (from 8.5% to 2.7%) while that in the CR model basically remains unchanged (5.2%). In the stable intervals, our FCT model greatly reduces the average successful trading rate of MSP (by 48.1%) when compared with the CR model.

As we well know, trading with HSP brings benefits and trading with MSP means risks, thus the above analysis indicates that our FCT model significantly outperforms the CR model in terms of two aspects, namely improving the average successful trading rate of HSP and reducing the risks of trading with MSP.

4.3 Experiment 2

In this experiment, we mainly validate the robustness of our FCT model against collusion attack and value imbalance attack with compared with the CR model, respectively.

4.3.1 *Collusion attack*

Owing to the self-certified characteristic, SPs will not provide adverse service feedbacks, thus we merely need to consider the case that MSP colludes with some SCs to improve its trust value. For illustration purposes, we introduce a new concept called RATV, namely the ratio between the average trust value of collusive MSP and that of HSP. A small distance between the RATV and 1 means that it is of difficulty to distinguish collusive MSP and HSP. In this part, we calculate the RATV in two kinds of trust models when there are 0%–50% of η SCs colluding with MSP, respectively. This calculation procedure is repeated 5000 times and the average outputs are illustrated in Figure 8(a). In addition, we also draw a baseline for comparison.

In the CR model, the number of service feedbacks is not explicitly viewed as a weight, and the filtering method based on the experiences of SCs is no longer available to our scenario, in which each SC trades with certain SP for only once. As a result, the RATV rises rapidly (from 0.37 to 0.97) to the proximity of baseline once there are SCs colluding with MSP. That is to say, collusive MSP and HSP cannot be effectively distinguished when there exists the collusion attack in the CR model, while in our FCT model, the number of service feedbacks is treated as an important weight and η is set such that the maximum number of collusive SCs is less than its 50%. Consequently, the RATV grows slowly (from 0.18 to 0.24) with the percentage of collusive SCs, and the gap with baseline is so large that collusive MSP and HSP can be easily distinguished in our FCT model. Thus our FCT model is superior to the CR model in the robustness against the collusion attack.

4.3.2 *Value imbalance attack*

As we mentioned above, the value imbalance attack means that certain SP (VSP) first disguises itself as a HSP and provides cheap and excellent services, and then turns to be a MSP and provides expensive and poor services. In this part, we mainly validate the average trust value variation of VSP when it converts from a HSP to a MSP in two kinds of trust models. In concrete terms, VSP provides cheap and excellent services at the beginning of trading tests (0–600 times), and turns to provide expensive and poor services in the later trading tests (600–1000 times). This validation procedure is repeated 5000 times and the average results are shown in Figure 8(b).

In the CR model, the service price context is not taken into consideration, and the service type context merely consists of two kinds of simple cases, namely the same or different service types, whereas in our FCT model, the service type context is viewed as a hierarchy tree and the service price context is also considered. As a result, the average trust value of VSP in our FCT model decreases more quickly (from 0.55 to 0.1 within 170 times trading tests) than that in the CR model (from 0.27 to 0.1 within 190 times trading tests). Thus our FCT model greatly outperforms the CR model in terms of the robustness against the value imbalance attack.

5 Conclusion

In this work, we have proposed a novel FCT model, in which the recommendation operations are conducted by service providers directly and the trusted third party is no longer needed, for LBSR. It is built in a fully-distributed way and the limitations of the classic centralized trust models can be made up. In addition, the locations of both service consumers and service providers are movable in our FCT model. Moreover, for the purpose of easing the collusion attack and value imbalance attack, we have taken four kinds of factor weights, namely number, time decay, preference and context weights, into consideration. Finally, we have deployed a fully-distributed service recommendation scenario and conducted comprehensive experiments and analysis. The results show that our FCT model has better robustness against the collusion attack and value imbalance attack than the classic CR model, and also indicate that our FCT model is greatly superior to the CR model in terms of the service recommendation performance in improving the successful trading rates of honest service providers and reducing the risks of trading with malicious service providers.

Due to the decentralized architecture and lightweight feature, our model does not support long-distance (e.g., between different cities) LBSR, and also cannot incorporate some classic recommendation techniques (e.g., collaborative filtering, matrix factorization, etc.), whereas several traditional recommendation concerns (e.g., multi-attributes matching, user preference, context-awareness, etc.) have been absorbed into our FCT model. Furthermore, due to the significant merits as shown in Section 1, our model is a primary but meaningful exploration of decentralized LBSR models and there is a huge potential to further improve our model. In future work, we will attempt to introduce more recommendation techniques into our FCT model and further improve its recommendation performance and robustness.

Acknowledgements This work was supported by National High Technology Research and Development Program (863 Program) (Grant No. 2015AA016007), National Natural Science Foundation of China (Grant No. 61502375, 61370078), Key Program of NSFC (Grant No. U1405255), and Natural Science Basis Research Plan in Shaanxi Province of China (Grant No. 2016JQ6046).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Wang N, Shen X L, Sun Y. Transition of electronic word-of-mouth services from web to mobile context: a trust transfer perspective. Decis Support Syst, 2013, 54: 1394–1403

2 Dhar S, Varshney U. Challenges and business models for mobile location-based services and advertising. Commun ACM, 2011, 54: 121–128

3 Bao J, Zheng Y, Wilkie D, et al. Recommendations in location-based social networks: a survey. GeoInformatica, 2015, 19: 525–565

4 Kuo M H, Chen L C, Liang C W. Building and evaluating a location-based service recommendation system with a preference adjustment mechanism. Expert Syst Appl, 2009, 36: 3543–3554

5 Liu Q, Ma H, Chen E, et al. A survey of context-aware mobile recommendations. Int J Inf Tech Decis, 2013, 12: 139–172

6 Li W, Yao M, Zhou X, et al. Recommendation of location-based services based on composite measures of trust degree. J Supercomput, 2014, 69: 1154–1165

7 Gavalas D, Konstantopoulos C, Mastakas K, et al. Mobile recommender systems in tourism. J Netw Comput Appl, 2014, 39: 319–333

8 Zhang T, Ma J F, Li Q, et al. Trust-based service composition in multi-domain environments under time constraint. Sci China Inf Sci, 2014, 57: 092109

9 Liu Z, Ma J, Jiang Z, et al. LCT: a lightweight cross-domain trust model for the mobile distributed environment. KSII Trans Internet Inf, 2016, 10: 914–934

10 Yu C C, Chang H. Personalized location-based recommendation services for tour planning in mobile tourism applications. In: Proceedings of the 10th International Conference on E-Commerce and Web Technologies. Berlin: Springer, 2009. 38–49

11 Waga K, Tabarcea A, Fränti P. Context aware recommendation of location-based data. In: Proceedings of the 15th International Conference on System Theory, Control and Computing. Piscataway: IEEE, 2011. 1–6

12 Barranco M J, Noguera J M, Castro J, et al. A context-aware mobile recommender system based on location and trajectory. In: Management Intelligent Systems. Berlin: Springer, 2012. 153–162

13 Biancalana C, Gasparetti F, Micarelli A, et al. An approach to social recommendation for context-aware mobile services. ACM Trans Intel Syst Tec, 2013, 4: 10

14 Yang D, Zhang D, Yu Z, et al. A sentiment-enhanced personalized location recommendation system. In: Proceedings of the 24th ACM Conference on Hypertext and Social Media. New York: ACM, 2013. 119–128

15 Noulas A, Scellato S, Lathia N, et al. A random walk around the city: new venue recommendation in location-based social networks. In: Proceedings of the 11th International Conference on Privacy, Security, Risk and Trust. Piscataway: IEEE, 2012. 144–153

16 Tan J S F, Lu E H C, Tseng V S. Preference-oriented mining techniques for location-based store search. Knowl Inf Syst, 2013, 34: 147–169

17 Bao J, Zheng Y, Mokbel M F. Location-based and preference-aware recommendation using sparse geo-social networking data. In: Proceedings of the 20th International Conference on Advances in Geographic Information Systems. New York: ACM, 2012. 199–208

18 Ciaramella A, Cimino M G C A, Lazzerini B, et al. Situation-aware mobile service recommendation with fuzzy logic and semantic web. In: Proceedings of the 9th International Conference on Intelligent Systems Design and Applications. Piscataway: IEEE, 2009. 1037–1042

19 Bedi P, Agarwal S K. A situation-aware proactive recommender system. In: Proceedings of the 12th International Conference on Hybrid Intelligent Systems. Piscataway: IEEE, 2012. 85–89

20 Li K, Lin M, Lin Z, et al. Running and chasing–the competition between paid search marketing and search engine optimization. In: Proceedings of the 47th Hawaii International Conference on System Sciences. Piscataway: IEEE, 2014. 3110–3119

21 Guemez E. Safety system for taxi users combining reputation mechanisms and community notifications. US Patent, 13/230,632, 2011-9-12

22 Gambetta D, Hamill H. Streetwise: How Taxi Drivers Establish Customer's Trustworthiness. New York: Russell Sage Foundation, 2005. 1–28

23 Balafoutas L, Beck A, Kerschbamer R, et al. What drives taxi drivers? a field experiment on fraud in a market for credence goods. Rev Economic Studies, 2013, 80: 876–891

24 Huynh T D, Jennings N R, Shadbolt N R. Certified reputation: how an agent can trust a stranger. In: Proceedings of the 5th International Joint Conference on Autonomous Agents and Multiagent Systems. New York: ACM, 2006. 1217–1224

25 Kerr R, Cohen R. Modeling trust using transactional, numerical units. In: Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services. New York: ACM, 2006. 21

26 Solanas A, Martínez-Ballesté A. A TTP-free protocol for location privacy in location-based services. Comput Commun, 2008, 31: 1181–1191

27 Rao U P, Girme H. A novel framework for privacy preserving in location based services. In: Proceedings of the 15th International Conference on Advanced Computing and Communication Technologies. Piscataway: IEEE, 2015. 272–277

28 Doppler K, Rinne M P, Janis P, et al. Device-to-device communications; functional prospects for LTE-advanced

networks. In: Proceedings of the 2009 IEEE International Conference on Communications Workshops. Piscataway: IEEE, 2009: 1–6

29 Condoluci M, Militano L, Orsino A, et al. LTE-direct vs. WiFi-direct for machine-type communications over LTE-A systems. In: Proceedings of the 26th Annual International Symposium on Personal, Indoor and Mobile Radio Communications. Piscataway: IEEE, 2015: 2298–2302

30 Dorigo M, Gambardella L M. Ant colony system: a cooperative learning approach to the traveling salesman problem. IEEE Trans Evolut Comput, 1997, 1: 53–66

31 Liu Z, Ma J, Jiang Z, et al. LSOT: a lightweight self-organized trust model in VANETs. Mob Inf Syst, 2016, 2016: 7628231

32 Nguyen H T, Zhao W, Yang J. A trust and reputation model based on bayesian network for web services. In: Proceedings of the 2010 IEEE International Conference on Web Services. Piscataway: IEEE, 2010. 251–258

33 Zhang H, Wang Y, Zhang X. Transaction similarity-based contextual trust evaluation in e-commerce and e-service environments. In: Proceedings of the 2011 IEEE International Conference on Web Services. Piscataway: IEEE, 2011. 500–507

34 Liu G, Liu A, Wang Y, et al. An efficient multiple trust paths finding algorithm for trustworthy service provider selection in real-time online social network environments. In: Proceedings of the 2014 IEEE International Conference on Web Services. Piscataway: IEEE, 2014. 121–128

35 Liu Z, Ma J, Jiang Z, et al. IRLT: integrating reputation and local trust for trustworthy service recommendation in service-oriented social networks. Plos One, 2016, 11: e0151438

36 Sun Y L, Han Z, Yu W, et al. A trust evaluation framework in distributed networks: vulnerability analysis and defense against attacks. In: Proceedings of the 2006 IEEE International Conference on Computer Communications. Piscataway: IEEE, 2006. 1–13