 CMC, vol.59, no.3, pp.983-993, 2019

Location Privacy in Device-Dependent Location-Based Services: Challenges and Solution

Yuhang Wang[1], Yanbin Sun[1, *], Shen Su[1], Zhihong Tian[1], Mohan Li[1], Jing Qiu[1] and Xianzhi Wang[2]

Abstract: With the evolution of location-based services (LBS), a new type of LBS has already gain a lot of attention and implementation, we name this kind of LBS as the Device-Dependent LBS (DLBS). In DLBS, the service provider (SP) will not only send the information according to the user's location, more significant, he also provides a service device which will be carried by the user. DLBS has been successfully practised in some of the large cities around the world, for example, the shared bicycle in Beijing and London. In this paper, we, for the first time, blow the whistle of the new location privacy challenges caused by DLBS, since the service device is enabled to perform the localization without the permission of the user. To conquer these threats, we design a service architecture along with a credit system between DLBS provider and the user. The credit system tie together the DLBS device usability with the curious behaviour upon user's location privacy, DLBS provider has to sacrifice their revenue in order to gain extra location information of their device. We make the simulation of our proposed scheme and the result convince its effectiveness.

Keywords: Location privacy, device-dependent location-based service, location-based service, credit system, location privacy preserving mechanism, shared bicycle.

1 Introduction

Location-based services (LBSs) have changed the way of getting information in daily life. Different kind of LBSs, such as positioning, navigation, POI searching and social network check-in, are already the fundamental applications in almost everyone's smartphone. Though may be different in details, all of these LBSs belong to the information service, which means that the user will send her location (along with other query or personal information) information to the certain LBS provider, and the provider send back the information the user needs. One most basic fact is that the location is firstly generated on the user side (for example, a smartphone) and then be sent to the LBS provider, LBS

[1] Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou, 510006, China,
[2] School of Software, University of Technology Sydney, Sydney NSW 2007, Australia.
[*] Corresponding Author: Yanbin Sun. Email: yanbin_hit@foxmail.com.

provider cannot know the user's location till the user wills it.

Meanwhile, location privacy preservation has gain increasing attention along with the popularity of LBSs, tremendous of works have been focused on the location privacy preserving mechanism (LPPM), and a lot of outstanding works have been proposed to preserve the location privacy of the user while she enjoying LBS. The LPPM will ensure the location privacy has been preserved before the location was sent to the LBS provider. Although various of schemes such as anonymity, obfuscation and noise addition have been performed by these LPPMs, the threat that the LBS provider may steal the user's location unknowingly is out of the LPPM's concern.

The recently noteworthy evolution of LBS may change the whole picture of LBS and the LPPM upon it. In this paper, we define this novel LBS as the Device-dependent Location-based Service (DLBS). Quite different from LBS, which is considered as a pure information service, DLBS provides not just the location-based information, but also the entity device-dependent service. The types of device are usually the common used utilities, such as bicycle, laptop, and the mobile power supply equipments. Moreover, these devices are smart chip embedded and self-localizable, and these ability enable the device to be aware of its situation and so as to maintain the DLBS system.

Although DLBS has greatly expanded the concept of LBS, however, from the view of location privacy, it also completely overturned the architecture and the threat model of the existing LPPMs. This huge change mainly comes down to the alter of the way of location obtaining by the service provider. Just as the location privacy has been regarded as the part of the basic human rights, the very right of the DLBS provider to know the location of their own device is also a solid fact. This two basic rights belonging to the user and the DLBS provider has formed a subtle conflict, which needs to be solved and the traditional LPPMs failed to.

In order to solve this conflict, which means that to preserve the location privacy of DLBS user and at the same time enable the DLBS provider to be aware of the location of their device, in this paper, we design a DLBS service framework, including the system architecture and the judge-and-weight credit system. Our scheme encourage the DLBS provider to obtain the device location that just enough to maintain their service. As to the force query of the device location, DLBS provider has to sacrifice the usability of the whole DLBS system.

In general, we mainly make contributions as follows:

1. To the best of our knowledge, we for the first time defined a new type of device-dependent LBS, and we pointed out the location privacy challenges caused by DLBS.

2. To conquer the location privacy threats in DLBS, we designed a DLBS framework, in which we bind together the location privacy and the usability of the DLBS system, DLBS provider has to be cautious when he is curious on the location of user.

3. We proposed the credit system rules to balance the location privacy and DLBS usability,

and we analysed these rules with game theory, the result shows that the location privacy can be preserved on the best utmost.

4. We simulate our system on a virtual shared bicycle system, and the simulation result verifies the effectiveness of our scheme.

The remainder of the paper is organized as follows. Section 2 Introduce the DLBS in details, and list the changes and the challenges it brings to location privacy. We describe the design details of our scheme in Section 3. Sections 4provide the analyse and the experimental simulation. Section 5briefly reviews the related work, and finally, Section 6 concludes the paper.

2 Location privacy challenges in DLBS

2.1 Device-dependent location-based service

DLBS greatly expands the range of LBS, as its a newly practiced form of LBS, in this section, we fist list the features of DLBS which this paper refers to.

1. A localizable service device is involved in the procedure of DLBS, the device will serve the user, while at the same time perform the localization and communicate with the DLBS provider all by itself and without the awareness of user.

2. DLBS devices are separated in the urban area and ready to serve. In order to enjoy DLBS, user needs to move close to a DLBS device and activate it. For instance, scanning the QR code of the device with her smart phone.

3. During the service, the device will offer the user the special capacity, also it will be taken by the user. During DLBS, the locations of the device and the user are regarded as the same.

4. For the purpose of maintaining the DLBS system, and also by his proprietary rights on the DLBS devices, DLBS provider need to learn the locations of the devices. This requirement (also it is his right) go against the location privacy preservation need of the user. In the most basic condition, DLBS provider at least needs to know the locations of those devices which are not in service, so that the DLBS provider can ensure the maintenance of the DLBS system.

2.2 Location privacy challenges

Due to the features mentioned above, in DLBS scenario, traditional LPPMs and their threat model are facing the challenges.

1. LPPMs in traditional LBS scenario do not have to consider the situation that the service provider are able to obtain the location without the permission of user. But in DLBS, this assumption no longer exist due to the localizable device. This is a disastrous challenge to those LPPMs that only considering how to perform the preservation on the location information which are about to send to the service provider.

2. In general, from the legal perspective, the DLBS provider do have the right to know

the location of their DLBS device. This is at least an equally right than the proposition of location privacy in the user side. This contradiction also beyond the scope of capacity of traditional LPPMs. New type of LPPM is needed to balance the location privacy demands and the "right to know" fact.

3. Specifically, in DLBS scenario, the activation location, where the user takes the device and activates the DLBS, is almost impossible to hide, since the DLBS provider has to know the location of his own device.

Combining the above mentioned DLBS features and the location privacy challenges, in this paper, we design a brand new DLBS framework to cope with these issues. Generally, in our framework, both the location privacy demands and the requirement of location-awareness from the user and DLBS provider side will be respected, protected and fulfilled. The basic principle of our framework is that we only encourage the DLBS provider to ask for the location information which is just enough for the maintenance at the minimum level of satisfaction. Finally, our framework have the compatibility to the traditional LPPMs, user is still available to use their LPPM to preserve their location privacy on our framework. In the next section, we will introduce it in detail.

3 Our proposed schemes

In our framework, we firstly unbundle the direct communication between the user and the DLBS provider, also between the DLBS provider and their devices. A trusted third party proxy is introduced here to perform the credit system. Fig. 1 shows our system architecture.

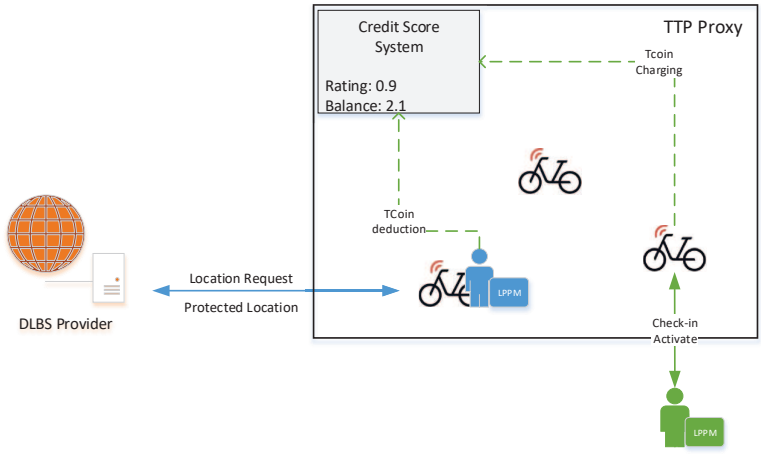

Figure 1: System architecture of our framework. TTP proxy maintain the location updating of the user and DLBS device, and the credit score system

In general, DLBS provider broadcasts the locations of the devices to the TTP proxy, and the user query the available device from TTP proxy. When the location information is needed, the TTP proxy receives the location request from the DLBS provider, decides whether

to fulfill him depending on his credit value. On the user side, if the location request is approved, she can use the LPPM to perform a certain degree of preservation, and send back the preservation result to the DLBS provider. Next, we details the design of our scheme.

3.1 Basic idea

As DLBS provider has the right to know the location of their devices when necessary, and this is also a natural right, so we cannot assume the real motivation of DLBS provider to obtain the location. Therefore, different from the traditional LPPMs, here in DLBS, we put the user's location privacy and the usability of the DLBS system on the two sides of the scale. In other word, we allow the DLBS provider to know the device's location (protected by LPPM), but he must bear the corresponding cost. From the perspective of interests, the DLBS provider must maintain the balance of the scale so that to make his own DLBS system functional. This means that it cannot excessively grab the user's location privacy, but can only obtain the appropriate location information just enough to maintain the operation of DLBS.

Our system assumption are as follow:

1. The user is honest, she enjoys the DLBS without any wicked idea. She always takes the DLBS device along with him, and reports her location, although preserved by LPPM, honestly.

2. The activation location of the user is beyond the protection of our scheme, as introduced about the features of DLBS, we consider the activation location as the necessary cost to pay by the user who wants to enjoy DLBS. What we want to preserve in our framework, is the trajectory information during the DLBS.

3. The DLBS provider is untrusted, curious by honest, he knows the location information of all the deactivated devices, and he has the right to query the location of the activated device, if the TTP proxy approve his request, the user has to report a location to him. On the other hand, since the location query will hurt the usability of DLBS system, the DLBS provider will always seeking for the benefit maximization between the location privacy and the system usability.

3.2 The credit score system of DLBS provider

To minimize the location information requirement of maintaining the DLBS system, the DLBS provider only needs to know the deactivation location of device, where the user terminates the DLBS and leave the device at. DLBS provider will obtain this location and updates the state of the device in order to get ready for the next round of service.

In our framework, we set up the credit score system to encourage the DLBS provider to only request from the TTP proxy the deactivation location of his device. We introduce the concept of "Trust Coin" which are used by the DLBS provider to get the location information in exchange on the TTP proxy. We details how this system works as follows:

1. For each time a user activate a DLBS, the system will create a certain amount of TCoin,

and give them to DLBS provider. In basic condition, for each time of DLBS service, 1 TCoin will be created and will be given to the DLBS.

2. For the in service devices, DLBS provider has to "purchase" the locations of them. He proposes the bargain to TTP proxy, and TPP proxy will inform the user of this request. Due to the "right to know" principle, the user has to response this request , however, it is up to the user who can determine the level of precision of the location DLBS provider could obtain.

3. We define the precise location worths 1 TCoin, and the value of location output from the LPPMs depends on the granularity of the privacy level. The lower precision the location is, the cheaper it will be.

4. Due to the one-to-many relationship between DLBS provider and the users, the DLBS provider may have the "balance" of TCoin during the runtime of DLBS system. Apparently, the lesser TCoin remains, the more trustworthy DLBS provider will be. Therefore, in our system, we define the credit rating of DLBS provider as a number between 0 to 1, 1 indicates that the DLBS provider have no balance of TCoin, and 0 means the balance of TCoin is equal or greater than the number of the current active users. At last, we further define the amount of TCoins when created at the beginning of service as $1 \times C$ TCoins.

Given the credit score system above and our system assumption, we can ensure the DLBS provider will behave to maintain the usability of his DLBS system, for the rational situation, this is prior to obtaining the location privacy of users. In our system, the ideal case is that the DLBS provider always spend his TCoin on requesting the precise location after the end of DLBS. Since no redundant TCoins left, he will always get 1 TCoin when a DLBS start, and always spend 1 TCoin after the DLBS end.

In the next section, we will analyse the credit score system, and the behaviors of the DLBS provider and the user under such rules. Next, based on this credit score system, we introduce some other detail features and designs of our framework.

3.2.1 LPPM preservation metric

We use the location privacy metric defined in [Shokri, Theodorakopoulos, Le Boudec et al. (2011)] and quantify the user's location privacy as the adversary's expected error. This metric also indicates how fuzzy the location is after the LPPM's preservation. Then, we can use this value to price the cost by DLBS provider to obtain the locations.

3.2.2 Device hiding

For the abuse of TCoins and unable to afford the location obtaining after the DLBS, for the purpose of practical application, we use the device hiding instead of just letting the device disappear for ever as the punishment. If the DLBS provider does not require the device's location after DLBS, TTP proxy will hide the existence of this device long enough, for example, 24 hours. This will causes DLBS provider certain financial loss.

3.2.3 Deactivation delaying

To avoid the deactivation location of DLBS reveals the current location of user, in our scheme, when a DLBS is end up by the user, we set up a time interval between the end time of DLBS and the searchable time of DLBS provider. DLBS provder could spend 1 TCoin for the device location after this delaying period, if he wish to obtain the device location inside this period, he still has to spend extra TCoins for it.

4 Privacy analysis and system simulation

In this Section, we first analyse our scheme from the view of the DLBS provider and the user separately. Then we simulate our framework and show its performance against various of behaviors. In practical, we choose the shared bicycle as the prototype of our simulation, and the parameters involved in our frameworks are assumed to be rational.

4.1 Analysis

Although the request of the device location from DLBS provider has to be fulfilled, our system provides a strong repellence against the malicious behaviour upon the location privacy of users.

First, if the DLBS provider spend his TCoins on requesting the location during DLBS, he would be incapable to obtain the location of his device after the DLBS, and that means the property lost as well as the reduction of usability of DLBS system, this is not acceptable for the DLBS provider.

Second, when the DLBS provider seeks out some balance of TCoins and ready to use them to obtain more location privacy, he can only remains a time window to do so, because due to the TCoin generating mechanism, more balance means lesser TCoins gain in each time of DLBS, and in order to maintain the DLBS system, the provider always needs to spend 1 TCoin each time to obtain the device's location. this deficit will soon wipes out the DLBS provider's TCoins.

At last, even in the situation that the DLBS provider, regardless about all usability and the benefits, trying very hard to obtain the user's location, he will get the location information not better than what he can get in the traditional LBS scenario, because the LPPM of the user side controls the granularity of the location information send back.

4.2 Simulation

We implement the simulation of our framework on our PC with Intel 8 Core 2.4 Hz CPU and 16 GB ROM. 1000 devices were launched into a 100 km^2 square area. We randomly trigger the DLBS services and the corresponding random trajectories with different frequency, the observed outputs are shown and explained in this section. We design the architecture and the credit score system, different types of behaviors are also involved in the simulation.

4.2.1 Functionality of the framework

We investigate our framework to see if it can support the DLBS system running smoothly. Fig. 2 shows the simulation result of the credit rating, the TCoin balance of the DLBS provider, and the percentage of the current missing device.

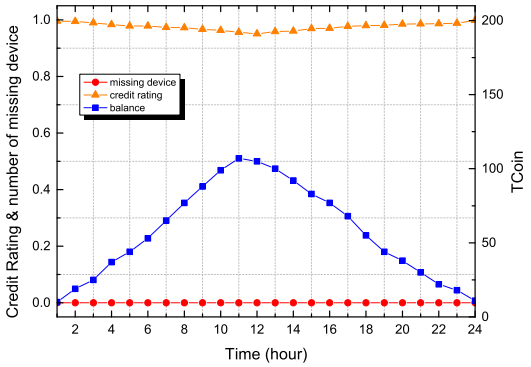

Figure 2: T *vs.* TCoins balance, the credit rating and the number of missing device, within a 24 hours simulation. Random number in normal distribution of users visit the DLBS system and use the device in a random time interval

We assume a honest DLBS provider here to measure the functionality of our framework. The number of missing devices, which are loss of communication due to the DLBS cannot afford the request, remain 0 in the whole simulation, since the DLBS keeps holding a reasonable balance of TCoins. During the mid-term of the simulation when the number DLBS rises, the balance rises together, and that leads the credit rating of the DLBS provider declines. Then, as shown in the latter period, the balance keeps consuming, and the credit rating return to the normal level.

4.2.2 Regulatory mechanism

The regulatory mechanism of the credit score system is tested by performing a shoot up of the TCoin balance. Fig. 3 shows the change of balance and the score rating when we assign the balance with 200 upon the same condition in the previous simulation. The shoot up of balance may happens in real-world situation if the DLBS provider carries out the collusion attack with the collaborators by sacrificing the usability of DLBS system.

As shown in Fig. 3, the shoot up of balance directly crushed down the credit rating to 0.03 at the beginning, as the result, barely income is generated in the previous few hours, and the net outflow of TCoin in order to obtain the deivces' location nearly exhausts the balance in 8 hours. In other word, even in such a extreme case, the time window for the DLBS provider to perform the malicious obtaining is less than 8 hour in our simulation.

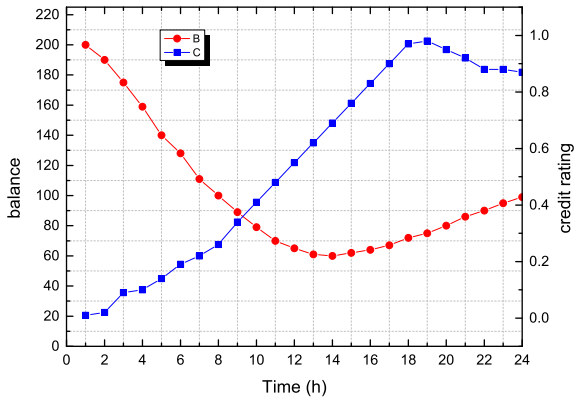

Figure 3: T *vs.* TCoin balance and the credit rating. When we assign the balance of the beginning as 200

4.2.3 Regulatory mechanism

We further consider the situation that the DLBS provider is willing to sacrifice the DLBS usability and is very curious about the user's location privacy. In the former case of simulation, we consider that the DLBS will use the TCoins to request extra location information, and the user will use the basic obfuscating LPPM to preserve her location privacy. Fig. 4 shows the result of this behavior.

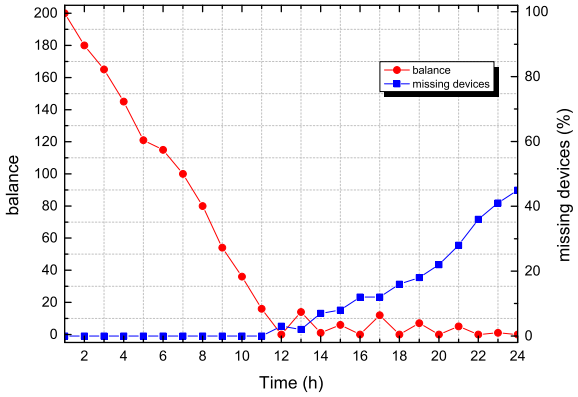

Figure 4: T *vs.* TCoin balance and the missing devices in percentage. When DLBS provider spend the balance to request more locations

When DLBS provider spend extra TCoin on requesting the devices' location, the balance soon falls close to zero, while remains numbers of in service devices' location need to be obtained at later time. As the result, the percentage of missing devices begin to increase, in our simulation, 45% of all the DLBS devices are missing in the last period, and this is a disastrous result for the malicious behavior.

5 Related works

Recent researches tried to built up the entire mechanism of location privacy preservation. These LPPMs have been well surveyed in Liu et al. [Liu, Darabi, Banerjee et al. (2007); Ahmadi and Bouallegue (2017); Chow and Mokbel (2011); Krumm (2009)]. Upon these works, it is necessary to measure how many privacy these LPPMs really offered to the location, and the location privacy metric were studies in Wernke et al. [Wernke, Skvortsov, Dürr et al. (2014); Wang, Zhang and Yu (2015); Damiani and Cuijpers (2013); Tippenhauer, Rasmussen, Pöpper et al. (2009)]. For the LBS scenario, these researches focused on how to use the location safely.

On the other hand, researches devoted to preserve location privacy in the location getting scenario, which can be described as how to get the location safely. Literatures such as Li et al. [Li, Sun, Zhu et al. (2014); Wang, Zhang, Su et al. (2018); Wang, Tian, Zhang et al. (2018)] provides efficient methods to cope with this threat.

In general, methods including anonymity, obfuscation, noise addition, differential privacy and the encryption-based method are well deployed and deeply studied in the pas decades of research. No matter what specific method they wish to perform, they almost shared the same system model as well as the boundary assumptions. When in the LBS scenario, they did not concern about the LBS provider could get the location information without the awareness of the user, or where the location came from. On the other hand, in location getting scenario, researches also do not care how the location could be generated. In the new service scenarios such as proposed in Tian et al. [Tian, Cui, An et al. (2018); Li, Sun, Jiang et al. (2018); Hou, Wei, Wang et al. (2018)], it is inevitable that the location might be obtained beyond the awareness of the user.

To the best of our knowledge, few of the researches paid enough attention on the development of LBS and the following location privacy challenge. We for the first time define the DLBS and the new privacy challenges along with it. Our proposed scheme is the forefront research which can solve the location privacy challenges in DLBS scenario.

6 Conclusion

In this paper, we defined a new type of location-based service which named the device-dependent location-based service. For DLBS, traditional LPPMs will be invalid since the overturning system model. Then, based on the credit score system and the proxy architecture, we designed a brand new DLBS framework, which can preserve the location privacy efficiently. We balance the location privacy with the usability of DLBS system, this can leads to the fact that the malicious behavior on location privacy will be bound to the harm on the usability to the DLBS system. The simulation result indicates that our framework can preserve the location privacy effectively in the real circumstance.

Acknowledgement: This work was supported by National Natural Science Foundation of China (Grant Nos. 61871140, 61702223, 61702220, 61572153, 61723022, 61601146), and the National Key research and Development Plan (Grant No. 2018YFB0803504,

2017YFB0803300).

References

Ahmadi, H.; Bouallegue, R. (2017): Exploiting machine learning strategies and rssi for localization in wireless sensor networks: a survey. *Wireless Communications and Mobile Computing Conference*, pp. 1150-1154.

Chow, C. Y.; Mokbel, M. F. (2011): Trajectory privacy in location-based services and data publication. *ACM Sigkdd Explorations Newsletter*, vol. 13, no. 1, pp. 19-29.

Damiani, M. L.; Cuijpers, C. (2013): Privacy challenges in third-party location services. *IEEE 14th International Conference on Mobile Data Management*, pp. 63-66.

Hou, M.; Wei, R.; Wang, T.; Cheng, Y.; Qian, B. (2018): Reliable medical recommendation based on privacy-preserving collaborative filtering. *Computers, Materials & Continua*, vol. 56, no. 1, pp. 137-149.

Krumm, J. (2009): A survey of computational location privacy. *Personal and Ubiquitous Computing*, vol. 13, no. 6, pp. 391-399.

Li, H.; Sun, L.; Zhu, H.; Lu, X.; Cheng, X. (2014): Achieving privacy preservation in wifi fingerprint-based localization. *IEEE Conference on Computer Communications*, pp. 2337-2345.

Li, M.; Sun, Y.; Jiang, Y.; Tian, Z. (2018): Answering the min-cost quality-aware query on multi-sources in sensor-cloud systems. *Sensors*, vol. 18, no. 12, pp. 4486.

Liu, H.; Darabi, H.; Banerjee, P.; Liu, J. (2007): Survey of wireless indoor positioning techniques and systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 37, no. 6, pp. 1067-1080.

Shokri, R.; Theodorakopoulos, G.; Le Boudec, J. Y.; Hubaux, J. P. (2011): Quantifying location privacy. *IEEE Symposium on Security and Privacy*, pp. 247-262.

Tian, Z.; Cui, Y.; An, L.; Su, S.; Yin, X. et al. (2018): A real-time correlation of host-level events in cyber range service for smart campus. *IEEE Access*, vol. 6, pp. 35355-35364.

Tippenhauer, N. O.; Rasmussen, K. B.; Pöpper, C.; Čapkun, S. (2009): Attacks on public wlan-based positioning systems. *Proceedings of the 7th International Conference on Mobile Systems, Applications, and Services*, pp. 29-40.

Wang, Y.; Tian, Z.; Zhang, H.; Su, S.; Shi, W. (2018): A privacy preserving scheme for nearest neighbor query. *Sensors*, vol. 18, no. 8, pp. 2440.

Wang, Y.; Zhang, H.; Su, S.; Tian, Z. (2018): A location privacy-aware method for knn query in location based services. *IEEE Third International Conference on Data Science in Cyberspace*, pp. 537-541.

Wang, Y.; Zhang, H.; Yu, X. (2015): Research on location privacy in mobile internet. *Journal on Communications*, vol. 36, no. 9, pp. 2015167.

Wernke, M.; Skvortsov, P.; Dürr, F.; Rothermel, K. (2014): A classification of location privacy attacks and approaches. *Personal and Ubiquitous Computing*, vol. 18, no. 1, pp. 163-175.