International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 9 (2017) pp. 1982-1986
© Research India Publications. http://www.ripublication.com

Privacy Protection Mechanism for Indoor Positioning Systems

[1]Sungil Kim, [2,3,*]Sang Guun Yoo and [1,]Juho Kim**

[1]Department of Computer Science and Engineering, Sogang University,
35 Baekbeom-ro, Mapo-gu, Seoul, Republic of Korea.

[2]Departamento de Ciencias de la Computación, Universidad de las Fuerzas Armadas ESPE,
Av. General Rumiñahui s/n, Sangolquí, Ecuador.

[3]Facultad de Ingeniería de Sistemas, Escuela Politécnica Nacional,
Ladrón de Guevara, E11-253, Quito, Ecuador.

ORCID ID: 0000-0003-1376-3843, Scopus Author ID: 36187649600 Researcher ID: R-5327-2016
*****(Corresponding Author)***

Abstract
Usage of location based services in indoor environments has grown as the popularity of smart devices has been extended. Location Based Services can be generally classified in Indoor LBS and Outdoor LBS. The most common and well-known Outdoor LBS mechanism is the Global Positioning System (GPS) because of its high coverage and accuracy in outdoor environments. However, GPS is not used for Indoor environments because its accuracy is downgraded dramatically due to the loss of signal strength when crossing the walls. Fingerprinting technique is considered one of the most popular indoor positioning system technology because of its high accuracy. In this technique, the location information of fixed devices (e.g. access points) is stored in the server to use it as the basis for calculating the position of mobile devices of users. In this paper, a privacy protection mechanism for the server-based fingerprinting technique is presented. The proposed method protects users, not only from service provider, but also from external attackers. The proposed method only generates low overhead which rises its possibility to be implemented in real-time applications.

Keywords: Location based service, indoor positioning system, security, privacy

INTRODUCTION

The evolution and growth of smart devices market have allowed the development of different technologies in the field of Internet of Things (IoT) including the Location Based Services (LBS). Location Based Services can be generally classified in Indoor LBS and Outdoor LBS. The most common and well-known Outdoor LBS mechanism is the Global Positioning System (GPS) because of its high coverage and accuracy in outdoor environments. However, GPS is not used for Indoor environments because its accuracy is downgraded dramatically due to the loss of signal strength when crossing the walls. Due to this reason, several mechanisms for Indoor LBS based on wireless communication technologies has been created (Zhongliang et al., 2013; Mainetti et al., 2014). Among those mechanisms, one of the most commonly used indoor positioning system (IPS) is based on Wi-Fi because of its low cost and high availability. Lately, Bluetooth version 4 (with the inclusion of Bluetooth Low Energy *BLE*) also has been used as an alternative for developing Indoor positioning systems. Fingerprinting, Time of Arrival (TOA) (Kbar, 2005), Angle of Arrival (AOA), Strongest Base Station and other algorithms are used to estimate user location in indoor environment. Among those algorithms, one the most important is the fingerprinting technique because of its accuracy. In this method, a database of access points with their signal strength and physical location information is created; then, such database is used to calculate the position of users by comparing with the signal strength of the access points near to users' devices. However, even though the mechanism is very effective, it has limitations in terms of security because the historical location data of users could be misused, creating a serious threat in terms of privacy.

Several works have provided methods to protect users' privacy, such as efficient authentication to prevent attacks, key exchange protocol based on identification (Gruteser & Grunwald, 2003), and privacy-preserving data management with k-anonymity algorithm (Konsantinidis et al., 2015). However, those solutions require many additional components increasing the implementation cost or make possible guessing of approximate location of users which do not solve the privacy threat issue. Because of these limitations, this paper intends to provide a solution with high privacy but with lower overhead.

BACKGROUND: LOCATION BASED SERVICES

Vehicle navigation is one of the most well-known location based services. But, vehicle navigations is not the only one. Recently, with the increase of smart devices, several location based services have become popular, such as location based advertisements (Jengchung et al., 2014).

Location Based Services can be generally classified in Indoor LBS and Outdoor LBS. The most common and well-known Outdoor LBS mechanism is the Global Positioning System (GPS). On the other hand, WiFi, Bluetooth, RFID, and ZigBee technologies are used in indoor positioning systems. This work only provides an introduction of techniques used in Indoor Positioning Systems as it provides a privacy solution for such systems.

Indoor Positioning System

Wireless communication technologies such as Wi-Fi, Bluetooth, RFID, and ZigBee are used in Indoor Positioning Systems (IPS). Among those technologies, Wi-Fi is the most popular because of high rate of installations of access points and well-built databases containing the location of such devices. Furthermore, most of smart devices are able to connect to this kind of networks making easy the implementation of the system (Hui et al., 2007). After Wi-Fi, Bluetooth based methods are also considered popular. Bluetooth Low Energy (BLE) of Bluetooth version 4.0 makes suitable for mobile device as it consumes low power and gives high efficiency. Recently, Apple has indicated to have plans to provide a positioning system based on BLE called iBeacon. Both Wi-Fi and Bluetooth communication technologies requires of a location recognition algorithm. One of the most popular of those algorithms is the Fingerprinting technique.

Fingerprinting technique

Fingerprinting technique (Xiekomg et al., 2010; Chan & Sohn, 2012) is divided into two phases: offline and online phases. In offline phase, the Received Signal Strength Indicator (RSSI) messages sent by access points are measured and stored in the database. The offline phase can be considered as the process of recollection of access points' locations. Once executed the Offline phase, a database similar to Figure 1 is created. Once created the database, the online phase is executed. In this second phase, signal strength of access points is measured by the user device, and such measurement is compared with the database (created in the previous phase) to calculate the location of the user. Figure 2 illustrates the fingerprinting technique.

X	*Y*	$RSSI_{\#1}$	$RSSI_{\#2}$	…	$RSSI_{\#n}$
X_1	Y_1	…	…	…	…
X_2	Y_2	…	…	…	…
X_3	Y_3	…	…	…	…
…	…	…	…	…	…
X_n	Y_n	…	…	…	…

Figure 1. Database constructed after Fingerprinting Offline phase

When the indoor environment changes, the RSSI values of access points change. In such situations, the database needs to be updated. This is the reason why the database requires considerable quantity of memory and computation power. For these reasons, the database is managed commonly by service providers.

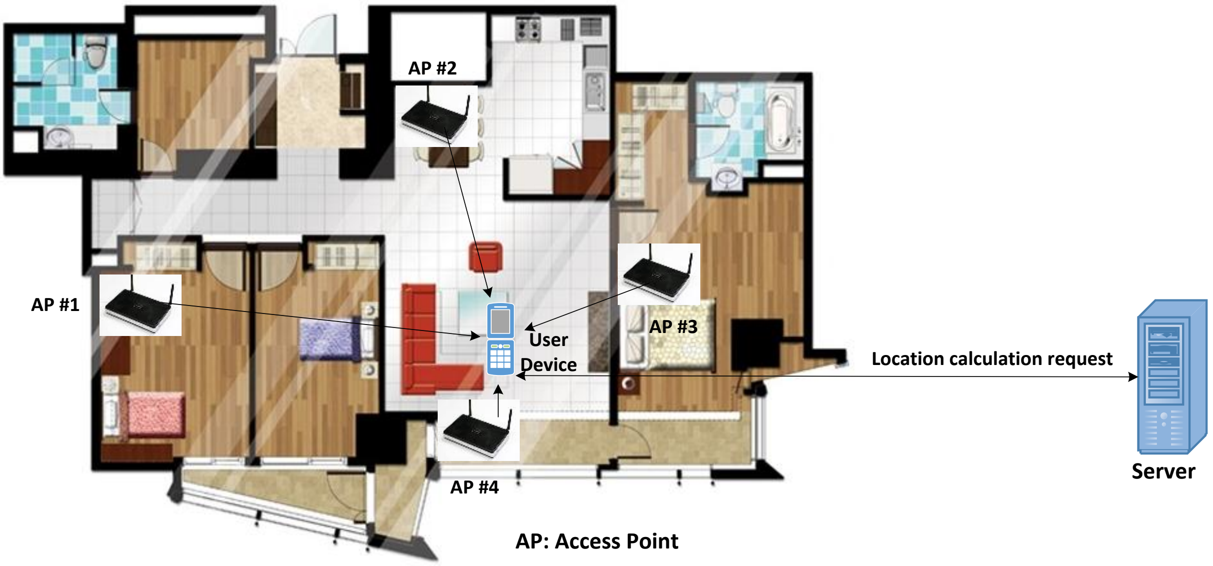

Figure 2. Measuring location by Fingerprinting method

PRIVACY AWARE FINGERPRINTING MODEL

In this section, security vulnerabilities and threats related to the fingerprinting model are presented. Later, an improved model is proposed.

Security threats

The mobile device of the user usually uses an application provided from the service provider to access to the indoor positioning services. In such case, as user's mobile device sends its unique identifier (e.g. MAC address) to the server, the service provider can know the historical position of the user which become a serious threat against the privacy of the user. The situation could become more serious if the information gathered by the service provider were leaked because of external attacks. Works such as Yoo et al. (2012) confirm the importance of considering the security issue in mobile devices.

To solve the privacy issue, some works propose usage of encryption of data (Sadikin & Kyas, 2014; Ghinita et al., 2008) which could be a possible solution for data leakage.

However, it cannot be a complete solution because it does not provide any solution for the threat against user's privacy due to service provider can access the plaintext version of data. Additionally, service provider's server could be victim of external attacks leading into leaking of encryption keys and private data which is not unusual nowadays (Zetter, 2015).

User identification in IPS service

User identification in IPS service is as follows. If the user requires registration, the service provider identifies their users with their ID and password. On the other hand, if the user does not requires registration, the service provider identifies to the users by using unique values of the smart device. Unique values able to be used for identification in smart phones are IMSI (International Mobile Station Identity) and IMEI (International Mobile Equipment Identity). IMSI is a 15-digit number of USIM serial number composed of PLMN ID (Public Land Mobile Network Identification) and MSIN (Mobile Subscription Identification Number). PLMN tells the nationality and mobile carrier while MSIN is a subscriber identification number assigned from the mobile carrier. On the other hand, IMEI is a 15-digit unique number assigned when the hardware device is produced. This number is unique to the device and it includes details such as device manufacturer and model number. Since, IMSI and IMEI are not available for every smart devices, MAC addresses are used as alternatives in some services (Keiji, 2012).

Proposed Privacy Protection Mechanism for Indoor Positioning Systems

The proposed mechanism uses the MAC address to identify different users because it is more widely used in this kind of applications (see Figure 3). Usage of MAC addresses allows service providers to identify a specific user, but prevents to know who really such user is, because the MAC address is related to the smart device and not to the user. However, this mechanism still as a limitation because the service provider can accumulate data to determine the behavior pattern of users by tracing MAC addresses (e.g. user with a specific MAC address has visited 5 times to a specific store in this week). Recently, there have been researches that identify and track a device using its MAC address such as Keiji (2012).

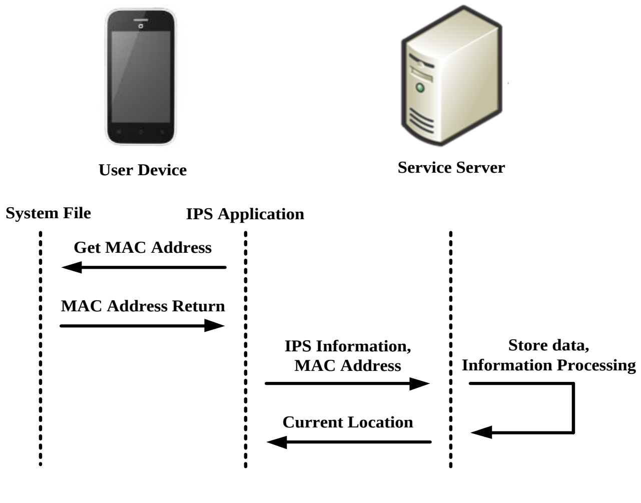

Figure 3. MAC Address collecting IPS service model

To solve this limitation and upgrade the protection in terms of privacy, this work proposes the installation of an application before accessing the IPS service. This application will change periodically the MAC address used by the device with random values. This simple solution will allow users to have a total privacy.

Table 1: Notations in algorithm

Notation	Definition
U_i	User *i*
UD_i	User Device of U_i
SM	Security Module (Application) installed in UD_i
SF	System File containing the MAC address
MA	MAC Address
MA_{new}	New random MAC Address
SS	Service Server which provides the IPS service

In details, the proposed solution will work as follows (see Table 1 for notations).

Step 1. $U_i \rightarrow SM$: Request access to IPS service

U_i request the IPS service access by launching the application created for this purpose.

Step 2. $SM \rightarrow UD_i$: Request Wi-Fi activation

SM requests to UD_i the activation of Wi-Fi connection if it were deactivated.

Step 3 $UD_i \rightarrow SM$: Responds Wi-Fi activation request

UD_i activates the Wi-Fi connection and notifies to *SM* that the Wi-Fi was connected correctly.

Step 4. *SM* : Generate MA_{new}

SM generates a new random MAC Address MA_{new} to be used for the IPS service.

Step 5. $SM \rightarrow SF$: MA_{new}

SM modifies the *MA* with MA_{new} stored in *SF*

Step 6. $SM \rightarrow UD_i$: Request access to IPS Service

SM indicate the successful modification of MAC Address and allows UD_i to access to the IPS Service

Step 7. UD_i : Access to IPS service

The UD_i access to the IPS service in the normal way.

This simple but effective process will allow U_i to use the IPS service with high level of privacy.

SECURITY VERIFICATION AND OVERHEAD ANALYSIS

In this section, security and implementation overheads for the proposed model is presented.

Security verification for the proposed model

In this section, security for the proposed mechanism is verified. The security verification will be based in terms of the threats presented in previous section.

- Misuse of data by service provider / Behavior pattern recognition: The service provider cannot determinate the pattern of a user because the MAC Addresses used by user's device are random values. Therefore, the privacy of the user is not affected in any way. The service provider cannot determinate the behavior pattern of a particular user, but it can determinate the pattern of whole group of users which will allow them to plan infrastructure upgrades and new services.
- Leakage of information from server: Leakage of information is not a problem because the attacker cannot determine the position of a particular user. The encryption of data stored in the server could be added to create a more secure mechanism.
- Sniffing attack: As explained before, data obtained by sniffing the network will not produce any effect in terms of privacy of users because the MAC addresses are random. A secure communication between the user's device and server could be implemented for major security if required.

Implementation Result and Overhead Analysis

To measure the overhead of the proposed method, an Android application was created. The implemented application executes the following steps.

(1) Generation of a random MAC address: the 48 bits random MAC address was generated by taking the first 48-bits of the 64-bits random number returned by the random function of Java.

(2) Replacement of the previous MAC address stored in the system file with the new MAC address generated in the previous step.

The developed Android application was executed in a mobile device with the features detailed in Table 2. The application was executed 10000 times and the average measurement was considered for overhead calculation. Results of the experiment is detailed in Table 3. Generation of a random MAC address required 0.031ms while writing of the generated MAC address consumed 2.799ms.

The overhead required for implementation of the proposed solution is minor, therefore, it has no impediments to be implemented in real life environments in terms of overhead.

Table 2: Experiment environment of Android virtual machine

Feature	Value
Device	Nexus 7
Target version	Android 6.0 – API Level 23
CPU/ABI	ARM (armeabi-v7a)
RAM	1024MB
Internal storage	200 MiB

Table 3: Time consumption overhead

Process	**Time (ms)**
Random MAC Address Generation	0.031
Writing of the MAC address in the System File	2.799
Total consumption time	2.830

CONCLUSION

Exposure of user information can lead to different damage for both users and service providers. Therefore, it is important to manage private data securely; not only applying the existing methods of encryption in communications and databases, but also providing a solution for hiding users' information from different kind of risks. The mechanism proposed in this paper provides a simple, but effective solution for maintain the privacy of users when using the location based services. The proposed solution can also be applied to hide important information such as IMEI, IMSI, and other unique information of the mobile device. It is true that modification of unique values such as MAC address, IMEI and IMSI are not (legally) allowed at the moment. However, it is possible to think about a new initiative allowing device manufacturers or service providers the management of a pool of device IDs (e.g. MAC addresses, IMEI, or IMSI) having as objective provision of privacy while protecting against spoofing of device IDs.

ACKNOWLEDGMENT

This research was supported by the MISP (Ministry of Science, ICT & Future Planning), Korea, under the National Program for Excellence in SW (2015-0-00910) supervised by the IITP (Institute for Information & communications Technology Promotion)

REFERENCES

[1] Zhongliang, D. et al. (2013). Situation and development tendency of indoor positioning. China Communications, 10, 3, 42-55. DOI: 10.1109/CC.2013.6488829.

[2] Mainetti, L. et al. (2014). A survey on indoor positioning systems. 22nd International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 111-120.

[3] Gruteser, M. and Grunwald, D. (2003). Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. Proceedings of the 1st international conference on Mobile systems, applications and services (Mobisys'03), 31-42.

[4] Konstantinidis, A. et al. (2015). Privacy-Preserving Indoor Localization on Smartphones. IEEE Transactions on Knowkedge and Data Engineering, 27, 3042-3055. DOI: 10.1109/TKDE.2015.2441724.

[5] Hui, L. et al. (2007). Survey of wireless indoor positioning techniques and systems. IEEE Transactions on Man and Cybernetics, Part C (Applications and Reviews), 37, 6, 1067-1080. DOI: 10.1109/TSMCC.2007.905750

[6] Kbar, G. (2005). Mobile station location based on hybrid of signal strength and time of arrival. Proceedings of the International Conference on Mobile Business ICMB 2005, 585 - 591.

[7] Yoo, S. et al. (2012). Confidential information protection system for mobile devices. Security Communications and Networks, 5, 1452-1461. DOI: 10.1002/sec.516

[8] Xuejing, J. et al. (2010). An Enhanced Location Estimation Approach Based on Fingerprinting Technique. 2010 International Conference on Communications and Mobile Computing (CMC), 424-427.

[9] Chan, S. and Sohn, G. (2012). Indoor localization using Wi-Fi based fingerprinting and trilateration techiques for LBS applications. International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, XXXVIII-4/C26.

[10] Jengchung, V. et al. (2014). Location-based advertising in an emerging market: a study of Mongolian mobile phone users. International Journal of Mobile Communications, 12, 3, 291–310. DOI: 10.1504/IJMC.2014.061462.

[11] Keiji, T. (2012). User Identification and Tracking with online device fingerprints fusion. 2012 IEEE International Carnahan Conference on Security Technology (ICCST), 163-167.

[12] Sadikin, M.F. and Kyas, M. (2014). IMAKA-Tate: Secure and efficient privacy preserving for Indoor Positioning applications. 2014 International Conference on Smart Communications in Network Technologies (SaCoNeT), 1-6.

[13] Ghinita, G., et al. (2008). Private Queries in Location Based Services: Anonymizers Are Not Necessary. Proceedings of the 2008 ACM SIGMOD international conference on Management of data (SIGMOD'08), 121-132.

[14] Zetter K. (2015, October). The most controversial hacking cases of the past decade. Wired, https://www.wired.com/2015/10/cfaa-computer-fraud-abuse-act-most-controversial-computer-hacking-cases/