Indoor Positioning System Techniques and Security

SungIl Kim, SunHwa Ha, ALSHIHRI SAAD, JuHo Kim
Department of Computer Science
Sogang University
Seoul, Korea
Email: joongjum@sogang.ac.kr, shonoozoo@sogang.ac.kr, saaad77.sa@gmail.com, jhkim@sogang.ac.kr

***Abstract*— Nowadays location based techniques are used various fields such as traffic navigation, map services, etc. Because people spend a lot of time in the indoor place, it is important for users and service providers to get exact indoor positioning information. There are many technologies to get indoor location information like Wi-Fi, Bluetooth, Radio Frequency Identification (RFID), etc. In spite of importance of IPS, there is no standard for IPS techniques. In addition because of characteristic of data, security and privacy problems become issue. This paper introduces the IPS techniques and analyzes each IPS techniques in terms of cost, accuracy, etc. Then introduce related security threats.**

Keywords*— *Indoor Positioning System (IPS); Security; Location; Bluetooth4.0; Wi-Fi; Privacy

I. INTRODUCTION

In recent years, with the development of mobile network, many kinds of services are provided by various ways. Many people spend most of their time in indoor places, so service related indoor environment become increasingly important and global LBS market also grow. Fig.1 [1] show the Location Based Services (LBS) market size. In this situation, many companies like Apple, Google, provide LBS like traffic navigation, map services, location-based mobile advertising, healthcare systems, indoor object search, etc. Typically, outdoor localization use Global Positioning System (GPS). This system use GPS satellites, GPS receiver monitors multiple satellites(minimum 3) and solves equations to determine the exact position of the receivers.

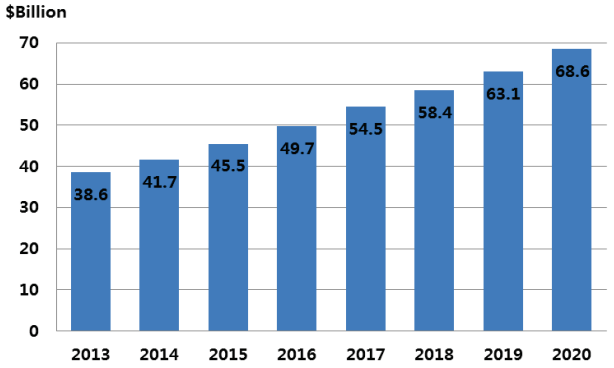

Fig. 1. Location Based Technologies – Global Market Forecast

Even if GPS show high accuracy, performance in outdoor environments, it is not suitable for indoor environments because in building or basement, strength of satellite signal is very poor. So other method is required to get exact indoor position information. Currently diverse techniques and algorithms are used to measure indoor positioning information. For example Wi-Fi, Bluetooth 4.0(Bluetooth Low Energy; BLE), Radio Frequency Identification (RFID), Zigbee, etc.

Traditionally, wireless network has various security threats such as Man In the Middle Attack (MITM), MAC spoofing, Rogue Access Points. So to prevent those attacks, existing security solutions should be applied. The other issue is Lightweight. Usually, outdoor and indoor positioning systems are accessed by smart device, but smart device's computing power and battery capacity is limited, thus existing security solutions are not appropriate. Therefore proper lightweight cryptography scheme should be used for constrained devices [2].

The aim of this paper is to introduce existing IPS technologies and possible security threats in IPS environments and solutions. The rest of this paper is organized as follows. Section II we introduce current Indoor Positioning System techniques like using Wi-Fi or BLE. In Section III we discuss security threats in IPS. Finally describe conclusion in Section V.

II. CURRENT INDOOR POSITIONING SYSTEM TECHNIQUES

Indoor Positioning System (IPS) generally needs two components: base station (BS) with known location information, and device (user) which needed to know the location. As GPS could not provide high precision, IPS uses Wi-Fi, Bluetooth, and so forth.

There are some approaches used in indoor localization, such as Time of Arrival (TOA), Angle of Arrival (AOA), Hybrid TOA/AOA, and Received Signal Strength (RSS) and fingerprint. [3]

Fig 2 shows the concept of TOA. TOA is the propagation time of a radio signal from a base station to a user. The distance between the base station and the user is calculated from the absolute time and the known velocity of the signal. One TOA gives a circle of possible location in a two dimensional space. This circle have its center point at the base station, and its radius equals to the distance.

ISBN: 978-1-4799-8451-0/15/$31.00 ©2015 IEEE

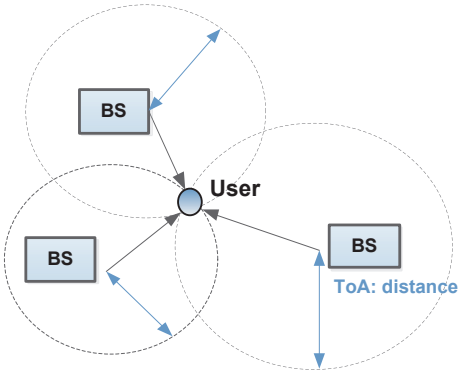

Fig 2. Concept of TOA

Three circles can give one intersection point of possible user location. [4]

AOA is defined by the direction of propagation from a transmitter on the antenna array. This method estimate the location of the user from the intersection of more than two direction lines. However, signal reflections could decrease the accuracy. [3] Fig 3 shows the concept of AOA.

Hybrid TOA/AOA reduces the number of base station needed. We describe the concept of hybrid TOA/AOA in Fig 4. It is possible to estimate the user location with a single base station. Intersection of a direction line and possible location circle gives the user location. For example, Fig 5 shows the scenario that with base station located on (a, b), user location is calculated with the distance and the angle. It is determined by the simple equations : $x = a + r \times \cos\theta$, $y = b + r \times \sin\theta$. this This approach is very sensitive to the AOA error. Generally provides better result than conventional approaches. [5]

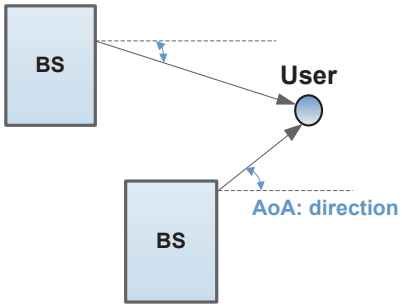

Fig 3. Concept of AOA

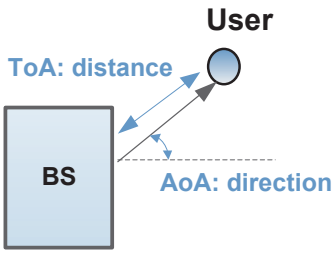

Fig 4. Concept of Hybrid TOA/AOA

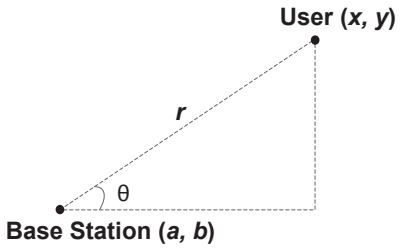

Fig 5. Hybrid TOA/AOA Localization by using BS

Received Signal Strength (RSS) and fingerprint approach need to survey the site in advance, Fig 6 shows this algorithms. At each pre-defined point, signal strength and distance to the base station are measured. As multipath effect gives unique signal to each location, user location can be deduced with the signal fingerprint data. This pre-measured database gives the statistical probability to the possible user location for certain signal strength. The accuracy for this approach relies on the distances between the points, signal differences, and the database for RSS and fingerprints. [6][7]

A. Wi-Fi based techniques

Wi-Fi based indoor positioning systems generally use the Wi-Fi Access Points (AP) to calculate the possible position of user. The rapid growth of APs makes it possible to implement Wi-Fi based IPS in many places. Wi-Fi based methods are as follows. [6]

1) Strongest Base Station

Strongest base station method is very simple. The location of the strongest base station near the user is considered as the user's location.

2) Fingerprinting

Fingerprinting is a pre-survey based method. It needs to measure the signal strength and other properties on the pre-defined location points in advance. User location is selected from the pre-measured fingerprint database: choose the most similar fingerprint. If the difference among the fingerprints is quite small, the accuracy could decrease.

This method need not to know the location of the Wi-Fi APs. It provides good accuracy as a fingerprint is consist of all the signal properties in the certain location point. However, this method may increase the cost during the database sampling. Also, it may need to do the re-measure the database.

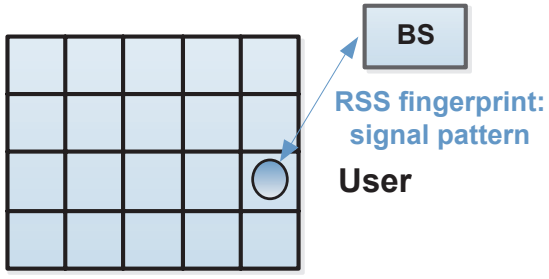

Fig 6. RSS and fingerprint approach

ISBN: 978-1-4799-8451-0/15/$31.00 ©2015 IEEE

3) Multilateration

With use of APs, TOA, AOA, and hybrid models can be implemented. Mathematical models are used to calculate the angle and/or distance between the AP and the user, but in real propagation environment, some factors such as reflection, absorption, and refraction could cause errors.

B. Bluetooth (Beacon) based techniques

In 2010, Bluetooth 4.0 was adopted into the main Bluetooth standard. As Bluetooth Low Energy (BLE) was released, many mobile payment providers have released BLE based beacon services.

It is quite simple to estimate the location using BLE. A BLE device transmits advertising packet, which includes data such as device ID, name of the place, and signal strength, to the user devices nearby. When a user device receives this packet, it calculate the location by the ID for the BLE device or the distance between the device itself and the BLE device.

It is possible to measure the location by only beacon based method, but it provides better performance when beacon based method and conventional methods used together.

III. Security Threats of IPS

This section introduces security problems related IPS. There are many IPS techniques and algorithms, so various security threats are existed. Existing attacks are possible and new problems also arise such as user privacy problems, because service provider is able to know user's current locations. If service provider abuse the information, personal privacy is infringed.

The following are attacked that can happen in a typical IPS environment.

A. Threats in Wi-Fi IPS Environment

Rogue AP attack scenario in IPS environment is that when wireless sensor detects rogue access point, the information of AP send to the IPS including overall connectivity information of the rogue AP. [8] Indoor Location system by using positioning mechanism such as location fingerprinting so the current IPS system can measure location of device to make good accuracy. [9] And rogue AP can collect user information and user location data.

Another example of indoor location of managed mobile device AP collect RSSI information of the AP devices. And the information like AP ID, user device ID and RSSI is sent to the IPS server. And using Wi-Fi indoor positioning mechanism as location fingerprinting and after collecting RSSI values, the mechanism specific data such like location fingerprinting database, and the IPS server sends the location information to the device. [10] When offline (pre-survey) phase in fingerprinting, unexpected rogue AP disturbs make fingerprinting DB. In addition in online phase rogue AP makes user device calculate wrong RSSI.

B. Threats in Using Bluetooth 4.0 (BLE) Beacon

In section II, we describe iBeacon. As mentioned above, beacons are open and static. For example, iBeacons broadcast same payload repeatedly. As result, anyone can detect and access the beacon's payload. In the beacon's payload, that involves the beacon's IDs. It make following risks such as spoofing and piggybacking. [11]

The notion of beacon spoofing is that detecting and cloning beacon IDs. If attacker know beacon IDs, attacker can make same beacon ID by using another beacon or other device. Attacker is able to use spoofed beacons to send the modified packet. As result user who is using IPS by BLE beacons in a different place than intended. It makes customer confused.

The concept of beacon piggybacking(Hijacking) is using beacon for unintended objects. Because detecting beacon IDs is possible, attacker include beacon IDs in his program. For example, beacon A is intended advertise store A. Then attacker already know beacon A's IDs, he can make program C that advertise store B by using beacon A. When customer installed program C, each time customer pass a store A, his device shows event or discount of store B. In this situation, despite the installation of beacon A, store A cannot get advertisement results.

C. Network attacks

Even if secure communication between Wi-Fi AP or bluetooth beacons and user device is done, the communication between user device and service server may have possibility of attacks.

If attacker get message form user and service server, attacker will be able to know user's location information. So service provider should protecting algorithm for the man-in-the-middle attack (MITM). Usually MITM is defended by authentication techniques such as Public Key Infrastructures (PKI) mutual authentication, stronger mutual authentication like secret keys or passwords.

In case, attacker know secret key information, despite cryptography mechanism is done, it is useless. So secret key management also very important issues.

IV. Conclusion

In this paper, we first reviewed Indoor Positioning System (IPS) techniques as Location Based Services (LBS) has grown. Basic techniques for the IPS and the implementing methods were introduced, and security issues for IPS environments were presented. Global companies such as Apple and Google are already in the process of developing IPS techniques and contents. Many mobile service providers around the world are also providing indoor positioning services using their infrastructure.

Moreover, security for IPS will become a very important issue as IPS services have access to and manage the private information of the user. So many countries have enacted laws related to collect personal location information. These laws include contents about network communication encryption and authentication standards, server DB encryption standards. Only

company to satisfy the laws can collect and service the location services. But this standard is not enough to protects privacy, so more research about LBS security will be needed.

REFERENCES

[1] http://marketinfogroup.com/location-based-technologies-market/

[2] Alippi C, Bogdanov A and Regazzoni F, "Lightweight cryptography for constrained devices," Integrated Circuits (ISIC), 2014 14th International Symposium on, Singapore, pp 144 – 147, Dec. 2014

[3] Chouchang Y, and Huai-Rong S. "WiFi-based indoor positioning."*Communications Magazine, IEEE* 53.3, pp.150-157, 2015.

[4] Ravindra S., and S. N Jagadeesha. "Time Of Arrival Based Localization in Wireless Sensor Networks: A Linear Approach." *arXiv preprint arXiv:1403.6697*, 2014.

[5] Victoria Ying. Z, Wong A.K.-S, Kam T.M and Ouyang R.W, "Hybrid TOA/AOA-based mobile localization with and without tracking in CDMA cellular networks." *Wireless Communications and Networking Conference (WCNC), 2010 IEEE*. IEEE, 2010.

[6] Jiang, Landu. *"A WLAN fingerprinting based indoor localization technique*." Diss. University of Nebraska, 2012.

[7] Feng C, Au W.S.A, Valaee S, Zhenhu T. "Received-signal-strength-based indoor positioning using compressive sensing." *Mobile Computing, IEEE Transactions on* 11.12, pp.1983-1993, 2012.

[8] Rogue Access Point: http://en.wikipedia.org/wiki/Rogue_acess_point,

[9] Fang S.H. and Lin T.N.: Principal component localization in indoor WLAN environments. LEEE Trans. Mob. Comput. 11

[10] Beyah R. and Venkataraman A, "Rogue-access-point detection-Challenges, solutions, and future directions." IEEE Comput. Reliab. Soc IEEE Oct. 2011

[11] "iBeacon Security overview" localz, Published on Mar 02, 2015