Spontaneous Privacy-friendly Indoor Positioning Using Enhanced WLAN Beacons

Florian Gschwandtner* and Corina Kim Schindhelm**
*Mobile and Distributed Systems Group, Ludwig-Maximilians-University Munich, Germany. Email: florian.gschwandtner@ifi.lmu.de
**Mobile and Distributed Systems Group, Ludwig-Maximilians-University Munich, Germany. Email: corina-kim.schindhelm@ifi.lmu.de

***Abstract*—Location based services pervade our lives more and more. Not only are outdoor movement of people and vehicles sensed via GPS, but with the use of wireless networks it is possible even indoors to locate people. On the one hand, this offers helpful and entertaining features, where GPS is not available; on the other hand, individual privacy is at risk with the unprotected release of highly sensitive location data. Many state of the art positioning methods require data exchange between the device and the network to enable positioning. Thus the users must implicitly reveal their current position to the network provider. In this paper, we address this problem and offer a new approach that allows users to ascertain their positions without exposing themselves to the network provider. Our approach embeds position data as information elements into IEEE 802.11 beacon frames, which are broadcasted periodically within each 802.11 basic service set. Based on this data, a mobile device can calculate its current position without revealing its presence to the network since beacons can be monitored passively. Finally we introduce a data format that enables the transmission of necessary location data required by the positioning methods Fingerprinting and Proximity Sensing.**

***Index Terms*—positioning, indoor, wlan, beacons, privacy-friendly**

I. Introduction

In this day and age being online and up to date is a vital part of modern life. Essentially, the new person has become available anytime and anywhere causing network, service and content providers to put effort into offering context aware applications for all needs. One of the most important context information, and the foundation of location based services, is the current location of the user. With the vast amount of available data, e.g., weather predictions or restaurant guides, having an location estimation reduces the copious information to a small and manageable amount.

For outdoor positioning, GPS (Global Positioning System) [1] is a well established standard in the form of navigation systems for cars along with other GPS integrated smart devices available. However, GPS signals are very weak indoors and approaches using them need to be adapted and optimized for such regions [2]. In addition to GPS based methods, state of the art research also examines alternate techniques using Ultra Wide Band [4], Barcodes [5], Radio Frequency Identification [6] [7], Bluetooth [8] or hybrids of these signals [9]. In contrast to these techniques, WLAN [10] has the principle advantage that it is highly distributed in both businesses and homes.

The main research of this field focuses on improving the accuracy of the users position by adjusting various aspects of positioning methods or combining them to a hybrid positioning solution. However, little attention is paid to privacy aspects. State of the art location methods offer users the ability to learn their current position only with data exchange between themselves and the network. The location and movement information remain anonymous only to a certain extent, since each device communicating through WLAN with a network is uniquely identifiable with its MAC (Media Access Control) address. Furthermore, if additional databases are available and connected to the information of location, the provider not only gains movement patterns in the building but is also able to link personal data to the movements; in essence, people become trackable.

Our novel approach stems from the desire to have a privacy friendly location system in which network infrastructure operators are not actively involved in the positioning process allowing the user the possibility to decide who they want to reveal their position to. Our belief is that users should not be forced to exchange data with a network operating system in order to obtain their current position. The infrastructure provides some information to the users which they can use themselves to calculate their positions. As a result, the users have the power to decide what to do with these sensible data and who, if anyone, they want to offer the information to as they are the only ones to have it.

The remainder of this paper is structured as follows. The next section explains different positioning infrastructures and points out the issues of privacy friendly indoor positioning. This is followed by Section III, in which we introduce our concept of a privacy-friendly WLAN-positioning approach using enhanced 802.11 beacons, the influences on the methods Fingerprinting and Proximity Sensing and also a data format, which enables the transmission of necessary location data required by both methods. Finally, Section IV concludes and presents research directions.

II. Issues of privacy-friendly indoor positioning

As GPS is not applicable indoors, WLAN became a prevalent alternative for indoor positioning; however, WLAN positioning often requires the knowledge of the access points' positions in order to calculate locations. The provider of the network may have access to this information, but the common visitor to the building surely does not. As a result, spontaneous WLAN positioning cannot be achieved if desired. Hence, the need for communication between the provider of the mobile entity and the provider of the network is inevitable.

In terms of positioning, two different roles can be identified. The first role is as **Measurement Provider** (MP), which measures the signal strengths between access points and the mobile entity. The second role is as **Position Calculator** (PC), which is responsible for calculating the position of the target based on the measurements. Depending on which roles are taken by the mobile entity or the infrastructure, in [11] three positioning infrastructures are differentiated:

Infrastructure Based Systems. Both roles are located within the infrastructure. Only information which can be monitored and read out by the infrastructure is used. During the positioning process the mobile entity is not involved at all. The position of a mobile entity can be calculated based solely on the signals transmitted when the entity searches for available access points. The access point receives these signals and processes them to calculate the location via signal strength or incidents angles of the received signals. Such a system is ideal for tracking assets; however, in the case when these assets are in fact people, this concept of locating inherently compromises the privacy of each individual. The privacy of this person is completely unprotected since locating and even tracking is easily possible unbeknown to this person.

Terminal Assisted Systems. The terminal and the infrastructure split the positioning duties between themselves. The terminal takes over the role as *MP* and actively sends information to a given infrastructure (e.g., received signal strength (RSSI) values for the Fingerprinting method) in order to receive its own location or information from the infrastructure, which therefore takes over the role as *PC*. Using this method, the person is aware of releasing sensible data, but often has no other options than sharing these with the operator of the infrastructure.

Terminal Based Systems. Both roles are located on the mobile entity. It collects data from a network and calculates its position without the aid of the infrastructure. This technique seems to be privacy friendly since it doesn't need the infrastructure to calculate positions. However, in order to be able to calculate a position, the terminal needs private information of the underlying infrastructure (e.g., positions of the access points for Proximity Sensing, radio maps for Fingerprinting). In order to obtain this information, the mobile device must communicate with the infrastructure provider. In that moment, the provider can gain position information about the device. Although the position cannot automatically and immediately be tied to a human being, along with information about people entering and exiting a building, it does provide the capabilities to calculate sensitive data. In order to achieve a genuinely anonymous positioning system, the terminal based infrastructure must be enhanced. The goal is to enable a delivery of the needed information without forcing the mobile entity to reveal itself to the infrastructure provider.

Given the positioning infrastructure, different positioning methods can be used for indoor WLAN positioning. The two most established methods are as follows:

Proximity Sensing. The position of a mobile entity is determined based on the position of the closest known entity in the infrastructure. For example, the position of the access point with the highest signal strength is used to define the position of the mobile entity. Nowadays this method is primarily used to locate cell phones when GPS cannot be used either because signal reception is low or because a GPS receiver is not present.

Proximity Sensing requires the position of the known entity in the infrastructure. That means, a communication with a third party provider, who can transform the unique MAC address of an access point into a position, is necessary. There are several providers in the market today. These position providers build up databases containing the connection of a specific access point and its geographic position by carrying out (dedicated or via cell phones) series of measurements.

Fingerprinting. The goal of this method is to find the position whose stored signal strength values match the best with the measured values of the mobile entity. The basis principles are described in [11]. In the offline phase, WLAN signal strengths are measured at different positions. For every position, all measured signal strengths from different access points are put in one signal strength vector (SSV), and all SSV and their corresponding positions are stored into a database. This database, sometimes given as a radio map, is required by the *PC* to calculate the position.

Both Proximity Sensing and Fingerprinting require communication with a third party to obtain information about the infrastructure. Our concept now offers a new positioning approach that can be performed in buildings while still respecting privacy issues by transferring the needed information to the mobile device.

III. Enhanced WLAN Beacons

As described in the previous chapter, the state of the art WLAN positioning approaches cannot provide adequate privacy for the user because each approach requires a distribution of various information. That is, communication or at the minimum data exchange between the network structure and the client is necessary. Our goal is to avoid data exchange by providing the clients with all the essential information without demanding them to establish a connection to an access point or communicate with the network. Namely, the access points send their position within 802.11 MAC frames [10].

Each 802.11 MAC frame starts with 2 bytes containing the frame control which among other things defines the type of the MAC frame. The various types of frames are Management (Association, Probes, Authentication and Beacons), Control (RTS, CTS) and Data Frames. While Data Frames are used to send the payload, the Management Frame's primary purpose is to inform potential clients about the network characteristics. Some typical network characteristics are the used Extended Service Set ID and the network's underlying encryption.

Although the content of the fields within the MAC frame is fixed, it is possible to send additional data within the data field. These additional data are called Information Elements

IE Type	Value Length	*Value*	
		OUI	Vendor specific data

Fig. 1. Vendor specific Information Element

(IEs) and are represented in Type-Length-Value fields. Type describes the kind of the IE data and length specifies the size of the value field. Since the length field is limited to 1 byte, the value field has a maximum length of 255 bytes.

IEs are often used to realize certain extensions of the 802.11 standard, like international roaming extensions (802.11d, [12]) and quality of service enhancements (802.11e, [13]); however, this is not there sole utilization. Network chip manufacturer use IEs to transmit extended information about the state or the various options of the chip to enhance the communication of devices produced by the same manufacturer. This is achieved by using IEs with type *221*. This type number is used for vendor specific payload as it is not reserved by the IEEE and therefore can be used by all. When a MAC frame is parsed and an IE type *221* is read, it is understood that the containing data is in a vendor specific format. To enable the possibility to process this information and to support a variety of vendors, the data field includes a 3-octet OUI (Organizationally Unique Identifier), depicted in Figure 1, which identifies the vendor and is assigned by IEEE. As a result, the maximum payload size in such elements is reduced to 252 bytes.

The goal of our approach is to include all required information for positioning (positioning information) into the Information Elements. As previously stated, IEs are supported by all management frames, e.g., WLAN Probe Responses. After receiving a probe request from a client, access points transmit probe response packets that contain information about the wireless networks offered. By including positioning information about the network in the probe response frame, the client would have all the necessary information to calculate its position locally, or more precisely, terminal based. However, this procedure demands the transmission of probe requests from the client, and therefore, can still reveal the presence of the client.

For this reason our approach forgoes the usage of probe requests and instead proposes the usage of beacons. By default, beacons are sent by access points periodically as broadcasts making it unnecessary for clients to send requests to the infrastructure. Hence, the identity of the client remains protected. Furthermore the usage of Information Elements as information carrier causes no incompatibility problems, since all devices compliant to the IEEE 802.11 standard can handle IEs. If devices do not implement our new approach, they can simply discard these IEs.

A. Proximity Sensing using enhanced WLAN beacons

As already mentioned in Section II, Proximity Sensing requires the position of an access point. Compared to the flow described above, using our approach results in a shorter flow because the access point's position is sent in IEs within the beacons. After receiving a beacon, the mobile entity can parse and process the transmitted position. An additional communication with the position provider or any other third party is avoided meaning the user's position won't be revealed.

B. Fingerprinting using enhanced WLAN beacons

To enable a privacy-friendly positioning system using Fingerprinting, the radio map is transmitted to the mobile device via WLAN beacons. Consequently, a bidirectional communication between infrastructure provider and mobile entity isn't necessary. However, radio maps can be rather larger and the limited size of an information element might not be capable of storing the radio map. As a result, rather than sending the entire map, we choose to transmit only the SSVs with their corresponding positions. The radio map can then be calculated locally on the mobile device since mobile devices, in particular smartphones, have powerful processors capable of handling complex algorithms.

The accuracy of a calculated position is related to the amount of visible access points. That is, the more access points are visible at a certain position, the more precise the positioning results at this point will be. Therefore, it is advantageous to have a high access point coverage in buildings. However, this would mean that the SSVs for each position would grow and with it the total amount of data sent by one access point. Because of the limited size of IEs, it is necessary to reduce this data by removing redundant information.

Since the client is not interested in a position on the other far end of the building, it is unnecessary for each access point to transmit all pairs $(position,\ SSV)$ to the client, covering the whole building. Instead, it is sufficient for each access point AP_x to send only the pairs where its own signal strength values are involved. Because all other positions cannot be reached by the AP_x, it is not necessary to transmit those positions to a mobile entity in range of AP_x.

As mentioned previously, high coverage of access points is advantageous. The more access points per position there are in reach, the more relevant pairs $(position,\ SSV)$ a client receives at its current spot. Hence, the calculated radio map for the nearby area becomes more precise.

C. Proposed data format

Given the various positioning methods used in WLAN positioning, a data format is required to efficiently consolidate and transmit the required position information within beacons. For that purpose, the data format, depicted in Figure 2, implements a general approach that supports arbitrary methods. In our case, Proximity Sensing ($IDProxSensing$) and Fingerprinting ($IDFingerPrinting$) is used to demonstrate how the data format can be applied to different positioning methods to efficiently transmit all necessary data within WLAN beacons. By defining new IDs, additional positioning methods can be supported.

In every positioning system it is important to select the reference system in which positions or coordinates are presented.

<Data>	::=	<ProxSensing>|<FingerPrinting>
<ProxSensing>	::=	<IDProxSensing><Coordinate>
<FingerPrinting>	::=	<IDFingerPrinting><ListAP> {<Coordinate>{<AP><MV>}}
<IDProxSensing>	::=	0
<IDFingerPrinting>	::=	1
<ListAP>	::=	List of all access points used in fingerprints
<Coordinate>	::=	Coordinate in reference system
<AP>	::=	Index of an Access Point in ListAP
<MV>	::=	Measured signal strength value

Fig. 2. Data format for embedding positioning information in WLAN Information Elements; described in Extended Backus-Naur Form

In our case these coordinates are the positions of access points. Naturally, to achieve good results, it is desirable to use a reference system suitable for the target device. Additionally, if the target device can process the positions of the access points directly, complex transforming calculations can be spared. Although any reference system could be used with the specified protocol, the World Geodetic System 1984 (WGS84) was chosen as the reference system because it is supported by most of the smartphones and modern smartphone operating systems offer a wide range of algorithms and services to support coordinates given in WGS84. Coordinates are given as latitude and longitude values, normally described in decimal degrees format. However, as the size of an IE is limited, a WGS84 coordinate must be compressed. The compression procedure is as follows: Firstly, the coordinate must be available in a format as specified in NMEA-0183 (National Marine Electronics Association 0183), e.g., 45° 30.1234' written in NMEA format results in *4530.1234*. Next, longitude and latitude are treated like numbers without a decimal point. Each of these decimal numbers are now transformed into their binary representations which takes 27 bits (0 to $90 \cdot 10^6$) for latitude and 28 bits (0 to $180 \cdot 10^6$) for longitude. The orientation of both latitude (North or South) and longitude (East or West) can be represented by one bit each. By following this method, a WGS84 coordinate can be represented by 57 bits.

With Proximity Sensing ($ProxSensing$), the transmission of the access point's coordinate is sufficient. However, with Fingerprinting ($FingerPrinting$), additional information must be sent. The data format allows for sending deterministic measurement values by using one scalar value (MV) for each access point (AP) in sensing distance of each surveyed location. Since it is highly probable that nearby fingerprints consist of almost the same access points, the opportunity exists to save space by specifying these access points only once within an indexed list ($ListAP$). Subsequently, an access point only needs to be referenced by its index instead of its complete MAC address. Hence, a fingerprint can be defined by its coordinate, the indices of all visible access points and the corresponding signal strength value MV for each access point. If probabilistic positioning is required, MV has to be extended for multiple values. However, this extension can severely increase the data size, which makes it reasonable to instead use a combination of the expected value and the variance.

After receiving the coordinates and measurements for Fingerprinting, the smartphone is able to compute a radio map of the nearby area without communicating with a third party.

IV. Conclusion and Future Work

We have presented a novel concept of a network assisted positioning infrastructure. The goal of the approach was to support a privacy friendly solution for users to obtain their positions without revealing those positions to a network provider. As a result, we have shown that access points can broadcast all necessary data needed for positioning in their WLAN beacons by utilizing Information Elements. The presented data format implements a general approach that supports arbitrary positioning methods. This allows mobile entities to receive the data without exchanging information with the network and to calculate their positions locally.

Our next steps are to finalize the implementation and run tests to evaluate the impact both on a network structure and on the mobile device. We modified an access point to send out the data according to the specified protocol and are currently working on the receiving smart phones. The goal is to implement a location provider on an Android cell phone that uses our approach to provide location data and can replace the common android WLAN approach.

References

[1] E. D. Kaplan and C. Hegarty, Eds., *Understanding GPS: Principles and Applications, Second Edition*, 2nd ed. Artech House Publishers, 11 2005.

[2] K. Pahlavan, X. Li, and J. P. Makela, "Indoor geolocation science and technology," *IEEE Communications Magazine*, vol. 40, no. 2, pp. 112–118, Feb 2002. [Online]. Available: http://dx.doi.org/10.1109/35.983917

[3] B. Alavi, N. Alsindi, and K. Pahlavan, "Uwb channel measurements for accurate indoor localization," *MILCOM*, vol. 0, pp. 1–7, 2006.

[4] X. Yubin, J. Weilin, and S. Xuejun, "Toa estimate algorithm based uwb location," *Information Technology and Applications, International Forum on*, vol. 1, pp. 249–252, 2009.

[5] P. Ruppel and F. Gschwandtner, "Spontaneous and privacy-friendly mobile indoor routing and navigation," in *GI Jahrestagung*, 2009, pp. 2574–2583.

[6] L. M. Ni, Y. Liu, Y. C. Lau, and A. P. Patil, "Landmarc: indoor location sensing using active rfid," *Wirel. Netw.*, vol. 10, no. 6, pp. 701–710, 2004.

[7] B. Xu and W. Gang, "Random sampling algorithm in rfid indoor location system," *Electronic Design, Test and Applications, IEEE International Workshop on*, vol. 0, pp. 168–176, 2006.

[8] A. P. Patil, D. J. Kim, and L. M. Ni, "A study of frequency interference and indoor location sensing with 802.11b and bluetooth technologies," *Int. J. Mob. Commun.*, vol. 4, no. 6, pp. 621–644, 2006.

[9] A. M. Hossain, H. N. Van, Y. Jin, and W.-S. Soh, "Indoor localization using multiple wireless technologies," *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference*, vol. 0, pp. 1–8, 2007.

[10] "IEEE 802.11-2007, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," June 2007.

[11] A. Küpper, *Location-based Services: Fundamentals and Operation*. John Wiley & Sons, 2005.

[12] I. Board, "IEEE Std 802.11d-2001 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications amendment 3: Specification for operation in additional regulatory domains," IEEE, Tech. Rep., July 2001.

[13] S. Mangold, S. Choi, P. May, O. Klein, G. Hiertz, and L. Stibor, "IEEE 802.11e wireless lan for quality of service."