Indoor Positioning Using CoLDE: An IEEE 802.11 Connectionless Extension

Osama ABU OUN, Christelle BLOCH and François SPIES
Emails: {oabuoun,christelle.bloch,francois.spies}@femto-st.fr
FEMTO-ST Lab (CNRS) - University of Franche-Comte, 1 Cours Leprince-Ringuet, 25200 Montbéliard, France

Abstract—**Acquiring current position information from the GNSS is a straightforward procedure outdoors. Any mobile device, equipped with a GNSS receiver, having a line of sight with enough numbers of satellites can calculate its location. The mobile device does not need a full connection with any of these satellites. In the indoor positioning using the Wireless Ethernet IEEE 802.11 (Wi-Fi) standard, some accurate methods require the mobile device to send some initial data from its environment to a server, the server utilizes the data to calculate the exact location. The mobile device should be able to connect to this server, either by having an association with a Wi-Fi access point or using 3G/4G if the server is accessible from the Internet. In some cases, having a connection to the Internet is not possible, either because of the absence of the 3G/4G, or the Wi-Fi access points and the server are not for the public. This study aims to make the Wi-Fi indoor positioning systems available to all the mobile devices, exactly as the GPS, without even the need to be connected, either to the Internet, or to any of the Wi-Fi access points. In order to achieve this goal, we developed an extension, CoLDE (Connectionless Data Exchange), for the protocol IEEE 802.11. CoLDE utilizes the management frames to allow Wi-Fi devices and access points to exchange small amounts of data without having an association. Using CoLDE, the access points can relay the initial data (which they) received from the mobile device to the server, and send the exact position back to the Wi-Fi device. CoLDE can be utilized regardless of the used Wi-Fi indoor positioning. This paper gives the description and the implementation of the protocol used and the proposed method, in addition to the experimental results gathered in a feasibility study to validate some of the basic concepts of this approach.**

keywords*: *indoor positioning,, indoor localization, Wi-Fi, beacons, management frames, optimization, GNSS information, colde.

I. Introduction

Indoor positioning using the IEEE 802.11 protocol has undergone considerable progress in the past decade. Indoor positioning became one of the essential technologies for many applications, such as disaster rescue, indoor navigation, and advertising. Indoor Positioning Systems (IPS) have been presented and implemented. These systems can be categorized into many groups according to their methods. One group is built on the use of the fingerprinting, which means a signature of environment features consistently and strongly depending on the physical location [1]. This group has many categories according to the feature used. One category is time-based methods, these methods include Time-of-Arrival (ToA), Time Difference-of-Arrival (TDoA) and Round Trip Time (RTT). Another category is the angle-based method (i.e. AoA)[2]. A third category uses (RSS) (Received Signal Strength) [3]. These categories are the three most representative measurements for position estimation. Compared to ToA and AoA measurements, the RSS can be more easily measured without any additional special hardware devices in current open public WLAN networks [4]. The other group uses triangulation. It is virtually impossible to use this method without a significant error, because this method does not take into consideration the interference or the obstacles in the area, such as walls, furniture, and even other people in the building.

In general, indoor positioning needs a number of calculations which differs according to the methods used. There are two ways to perform these calculations. One way is to perform them on a mobile device, while the other way is to perform them on a server. Performing the calculations on a mobile device consumes the device's battery, and since mobile devices are normally battery-driven, energy efficiency is a very important consideration in Wi-Fi localization systems [5]. Methods such as Wi-Fi fingerprint-based localization solves part of this problem by sending the needed parameters to a server in order to perform the calculations.

Sending the parameters to a server requires the mobile device to have an active connection to this server, either by having an association with a Wi-Fi access point or using 3G/4G if the server is accessible from the Internet. Such a condition limits the usability of the positioning and localization services to the mobile devices that are connected to the right network where the server is accessible. On the other hand, GPS (Global Positioning System) is a system accessible by any person with a GPS receiver. Our goal is to provide the needed method to make indoor positioning accessible by any mobile device equipped with a Wi-Fi network card, without requiring it to be connected to any network, and regardless of the localization system used. For this purpose, we present our solution to exchange positioning and localization data using the Connectionless Exchange Protocol (CoLDE). CoLDE uses the management frames in the IEEE 802.11 protocol to exchange small amounts of data [6].

The remainder of this paper is organized as follows: Section II presents the state of the art of this work and we survey related work in using connectionless protocols in positioning and localization. Section III introduces Connectionless Data Exchange protocol (CoLDE), in addition to our contribution on how to use it to exchange positioning and localization data without any association procedure. Section IV elaborates integration into embedded systems in details. The positioning by methods and applications which can benefit by CoLDE are discussed in Section V. Section VI provides the experiment scenarios and the results. And finally, some concluding remarks and future work are mentioned in Section VII.

II. State Of The Art

Beacon-Stuffing is one of the earliest attempts to use the management frame to exchange data. Beacon-Stuffing is a low bandwidth communication protocol for IEEE 802.11 networks that enables APs (Access Points) to communicate with clients without association. This enables clients to receive information from nearby APs even when they are disconnected or when connected to another AP[7]. It is possible to broadcast the AP position or the AP location using beacon-stuffing. When the Wi-Fi receives a beacon(s) from the surrounding AP(s), it extracts the position(s) from the beacon(s), it should perform the needed calculations with the help of other parameters like RSSI to get a more accurate position. In this method, the calculations depend on the Wi-Fi device itself. There are two concerns about this method, power consumption and the accuracy of the calculated location.

While beacon-stuffing provides a way to broadcast data from an AP to a client, in [8], the authors prove the possibility of exchanging any amount of data between two Wi-Fi clients using the management frames (probe request/response).
In [9], the authors utilize the NULL and the ACK frames to obtain the RTOF (Round-Trip-Time-Of-Flight), so the mobile can measure the distance from the AP. NULL frames represent a special type of IEEE 802.11 data frames, because they merely carry a power management bit while the data field is being left empty. NULL frames have to be acknowledged by the AP. A station sending a NULL frame to an access point does not have to be associated with the latter. NULL frames are unicast frames, so a null frame can be sent to an AP. That means a station should perform active or passive scanning, so the station can have a list of the APs.
In CoLDE, we send data simultaneously with the scanning frames. That means we send one frame to all the APs on the same frequency. We do not need to send a frame to each AP.
IEEE 802.11u was developed to improve internetworking with external non-802.11 networks[10]. IEEE 802.11u primarily focused on on-the-fly authorization between both the STA (Station) and the AP [11]. With the use of external network authorization, the AP also provides service to the previously unknown STAs.
In this paper, we present our solution which depends on CoLDE and uses the Wi-Fi networks which already exist, even the private ones, to provide indoor positioning services to any Wi-Fi device. The main three advantages in the proposed solutions are the following: firstly, the Wi-Fi clients do not have to be connected to any network at all. Secondly, they can use indoor positioning services from an AP_i while they are connected to AP_j, without the need to disconnect from

Frame Control	Duration	DA	SA	BSSID	HT Control	Sequence Control	Frame Body	FCS
Octets : 2	2	6	6	6	4	2	0-2312	4

Fig. 1. IEEE 802.11 Management Frame

Maximum Length = 2312								
	Element ID	Length	Service ID	Server's Address	Data Field Size	Data 1	...	Data N
	ID= [32→255]	X			Y			
Octet(s)	2	1	2	16	1	Y		Y

Fig. 2. CoLDE Frame

AP_j. Finally, it works with any indoor positioning system which needs to exchange a small amount of data between the client and the server. The Wi-Fi devices broadcast a localization request to the surrounding APs. The probe request contains the request along with the parameters needed by the positioning system. The parameters could be the information of the surrounding APs; such as the MAC (Media Access Control) address, SSID, RSSI, ...etc.
While IEEE802.11u improves interconnecting with external non-802.11 networks, CoLDE provides an easier way to exchange data with non-connected 802.11 networks.

III. ConnectionLess Data Exchange Protocol (CoLDE)

Our proposition CoLDE extension [6] allows exchanging data between two Wi-Fi entities without the need to have an alliance or establish a connection between them. The entities could be normal access points (infrastructure mode), ad-hoc devices, Wi-Fi Direct or even normal Wi-Fi clients. This extension allows broadcasting information to all Wi-Fi devices in particular areas, even if they are connected to different networks, or even if they are not connected to any network. CoLDE allows the Wi-Fi devices (i.e, mobile phones and laptops) to benefit from the new services with the help of the other devices that these services include. For example, some mobile phones do not include any localization systems, so they can get the current position from other devices (which include that localization system), if these devices exist in the same geographical area and most specifically in the Wi-Fi coverage area of the first device.
Examples and situations vary with localization functions, emergency evacuation, integration between Wi-Fi devices and VANET (Vehicular ad-hoc network), exchanging data with access points in the same area without the need to be connected to them or to use a service from another device.
In CoLDE the data will be carried into beacon frames for broadcasting the information, and into probe Request/Response Management Frames (Fig. 1.) to request a service. This approach more specifically uses the Information Elements (IEs) part of the management frame (in case of the probe Request/Response frames), which includes a variable length part, which the client usually uses to ask the access point for some extra information like the BSSID, (BSSID is the MAC address of the access-point), the supported rate,....

	Element ID	Length	OUI	OUI Sub-Type	Data
	221	L = (3 + 1) + X ≤ 251			
Octet(s)	1	1	3	1	X

Fig. 3. Vendor-Specific Information Element

Data, Length ≤ 251									
	System*	Time	Last Position	Count	AP 1			AP N	
					MAC	RSSI	....	MAC	RSSI
				N					
Octet(s)	1	11	20	1	6	1	....	6	1

*System : it means the indoor positioning/localization system

Fig. 4. CoLDE Indoor Positioning - Request Frame

Time, Length = 11 Octets									
	Year	Month	Day	Hour	Minutes	Seconds	Milli Seconds	Hours ±UTC	Min ±UTC
Octet(s)	3	1	1	1	1	1	2	1	1

Fig. 5. CoLDE Indoor Positioning - Time Format

Data, Length ≤ 251					
	System*	Time	Position	Msg Size	Msg
				Y	
Octet(s)	1	11	20	1	Y

*System : it means the indoor positioning/localization system

Fig. 6. CoLDE Indoor Positioning - Response Frame

Each request information element has a unique ID, the ID numbers between 32-255 have been reserved for future use. One of these IDs could be used to define a new Information Element (IE) to send a special request from a Wi-Fi entity to another Wi-Fi entity (broadcast if the SSID is unknown, unicast if the SSID is already known). The request can include some parameters, for example: the list of their access points with their RSSIs, their current location, extra information about an accident, road conditions (VANET).
Actually, the proposed extension is only software and needs no special hardware. Any Wi-Fi device, whatever its role in the network, can be provided with an extension, which means it can be provided by any access point, a mobile in an ad-hoc mode, a mobile in a direct Wi-Fi mode or even a normal mobile running in a pure client mode.

IV. Integration in Embedded System

CoLDE proposes a general structure frame which can contain any type of data (Fig. 2.). It depends on defining new information elements. In this paper we customized this method. Firstly, we use the vendor-specific information element (Fig. 3.). Because of the extensive importance and to allow some flexibility to the vendors, the 802.11 standard itself has a provision to carry non-standard, vendor-specific information in the ”vendor specific” Information Element (IE) field of management frame. This IE (with ELEMENT ID 221) is provisioned to be always present as a last IE in the frame body of beacon. Using it, up to 251 bytes of information can be embedded in each management frame[12]. Utilizing the vendor specific information simplifies the implementation, many Wi-Fi cards' drivers identify and send this information element to the application for it to be processed. Each vendor has its own OUI (Organizationally Unique Identifier). OUI is a 24-bit number that uniquely identifies a vendor, manufacturer, or other organization globally or worldwide. The following byte (OUI sub-type) is used as a vendor-specific sub-type.

The customizable information element (CoLDE-Request) (Fig. 4.) provides the needed data structure for the methods that use RSSI fingerprinting, collaborative localization or time based methods. By using only one probe request frame, it is possible to send the last position information, the time (Fig. 5.), the MAC address and the RSSI 31 of APs (the number of APs depends on the size of the *last position* field).
The main fields of CoLDE-Request are:

- **System** is a field of one byte with an unsigned integer, it specifies the ID of the positioning system that should process the followed data. System 0 means that there is no specific system, the data will be all available systems. Subsequently, the user could receive no response, one response or many responses.
- **Time** is a field of 11 bytes (Fig. 5.). The time is used in some positioning systems, such as OwlPS [23]
- **Last Position** contains the last position acquired by this client. It is a 20-byte length field. This field can be used to send the GNSS position (latitude: 8 bytes, longitude: 8 bytes and altitude: 4 bytes). Also, we can send a text or a code for relative location using all the bytes.
- **Count** is a field of one byte with an unsigned integer, it specifies the count of the data, in our case the count of APs gathered by the client, and the maximum number of APs is only 32.
- **AP MAC** is a field of 6 bytes containing the MAC address of the AP.
- **AP RSSI** is a field of one byte containing the RSSI, it indicates the power level being received by the AP.

A different structure has been built for the response (CoLDE-Response) (Fig. 6.) The main fields of CoLDE-Response are:

- **System** is a field of one byte with an unsigned integer, it specifies the ID of the positioning system that should process the followed data. System 0 means that there is no specific system, the data will be all available systems. Subsequently, the user could receive no response, one response or many responses.
- **Time** is a field of 11 bytes (Fig. 5.). It specifies the sending time of the position.
- **Last Position** contains the position provided by the Wi-Fi access point or by the positioning system. It is a 20-byte length field. This field can be used to send the GNSS position (latitude: 8 bytes, longitude: 8 bytes and altitude: 4 bytes). Also, we can send a text or a code for relative location using all the bytes.

- **Msg Size** is a field of one byte, it contains the size of the Msg field.
- **Msg** is a variable length field (The *Msg Size* field specifies the size of this field). It is a free structure field, the positioning system or the AP can send a text message to the client.

The time needed for processing a positioning request is a serious bottleneck. While the probe request has a timeout measured by hundred of milliseconds, indoor positioning systems need seconds (in the ideal circumstances) to calculate the client position. In normal cases, the active scanning process takes 2 to 3 seconds [13]. This time varies depending on the distance from the server's network, the link speed with this network, the server's capacity, and the most important parameter is the time needed by the positioning algorithm. In other words, when the client sends a probe request containing a positioning request, the timeout can be hit even before receiving the probe response. The same problem will arise when trying to send another request.

We present our solution which utilizes two levels of caching. By using the cache, the client will get the result of the positioning request in the following probe response frames.

We will cover the caching levels and the procedure followed in detail.

There are three main components in our solution. The Wi-Fi client device, the Wi-Fi access point and the CoLDE Proxy Server (CoLDE-Proxy).

CoLDE integration into the Wi-Fi client devices

The probe request is the main item needed to integrate client's CoLDE in the Wi-Fi client's devices. The probe request is used to perform "Active Scanning".

In active scanning, probe request frames are transmitted on all the channels. The responses received from APs in the form of probe response frames are then subsequently processed by the WNIC (Wireless Network Interface Card). Active scanning is the default-scanning technique for a WNIC, which enables it to implore an immediate response from an AP, without waiting for the beacon frames to be sent by the AP [14].

Considering that active scanning is the default technique in the Wi-Fi, we only need to add CoLDE-Request as an IE in the sent probe requests. Depending on the data needed by the positioning system, the client might need to use some data from the probe responses themselves. In this case, the system waits for the first scan to be done, it extracts the needed data, then it prepares the CoLDE-Request. The frame will be added as an IE to be sent in the next probe requests (only one time). Every positioning system can customize the CoLDE-Request to include the needed data. Each positioning system needs to have a unique ID to be used in the field *System* in the frame. By using the field *System*, the CoLDE-Proxy can call the functions of the right positioning system.

The iw is a new nl80211 [15] based on Linux CLI (Command Line Interface) configuration utility for wireless devices. It supports all new drivers that have been added to the kernel recently. It is an open-source library. We have used iw to add the CoLDE-Request as an IE in the probe requests, and to get the IE from the probe responses. As Wi-Fi clients, we are using an IPC (Internet Personal Computer) with Ubuntu and Arch linux operating systems, and a low-cost,compact Raspberry Pi with Arch linux.

CoLDE integration into the Wi-Fi access points

Access points play an important role in our solution. They have more tasks to do than just forwarding the frames from/to clients. We used Raspberry Pi as an access point. It has been equipped with Wi-Fi USB dongle. For the sake of testing we used three types of Wi-Fi dongles (Atheros, Ralink and Realtek). Arch linux (customized distribution for ARM architecture) has been used instead of Raspbian (based on Debian), the reason is related to the ability to control the Wi-Fi dongle driver by a 3rd-party application instead of the operating system itself.

The hostapd [16] has been selected as an access point application. Hostapd is a user space daemon for access point and authentication servers. It implements IEEE 802.11 access point management and it supports Linux (Host AP, madwifi, mac80211-based drivers) and FreeBSD (net80211). Hostapd is designed to be a "daemon" program that runs in the background. It can be distributed, used and modified under the terms of a BSD license.

The hostapd has been customized to process CoLDE frame. We used the code 0x0c01de (it has not yet been assigned to any vendor) as a temporary OUI, we will refer to this ID as CoLDE-OUI. Two sub-types have been added to further indicate the cache settings. The value 0x01 indicates that the client prefers to have instantaneous position (not from the cache). On the other hand, the value 0x02 shows that the client accepts cached position. Other values can be identified (254 values). These values can help to specify other settings. Whenever the hostapd receives a probe request with a CoLDE OUI in the IE part, it extracts the CoLDE-Request data. Then, it checks the OUI sub-type to decide whether it should check the local cache or not. In case of having the value 0x02, the AP searches the cache for any response stored for this client. If any response is found in the cache, the AP sends it directly in a probe response, otherwise it continues the procedure as if the sub-type were 0x01. If the OUI sub-type is 0x01, the AP forwards the data to CoLDE-Proxy as a unicast. Hostapd prepares the CoLDE-Response frame as soon as it receives the response from the CoLDE-Proxy. It adds the CoLDE-Response to a probe response to be sent to the client. The probe response has the same CoLDE-OUI as in the IE. Each entry in the cache has a timestamp and a timeout. The timeout is measured in seconds and it can be customized to fit different networks and different positioning systems. It is possible to send the timeout from the CoLDE-Proxy. The AP represents the 1st level of caching in our solution.

CoLDE Proxy Server (CoLDE-Proxy)

CoLDE-Proxy can be any linux or windows server, even it is

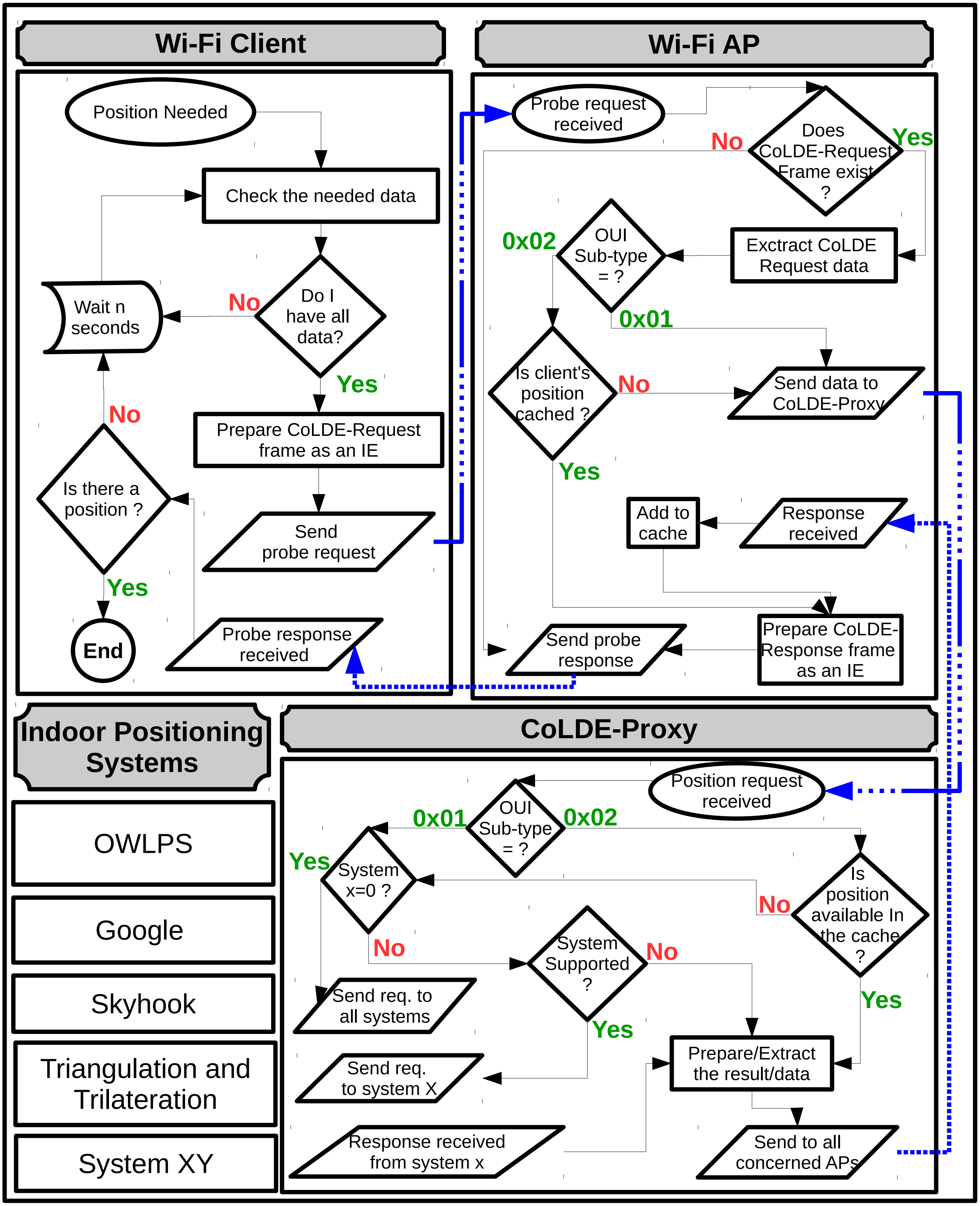

Fig. 7. CoLDE Indoor Positioning - Procedures and communications

possible to combine the access point and the CoLDE-Proxy in the same device. Actually CoLDE-Proxy is the interface between Wi-Fi clients and access points from one side, and the positioning system(s) from the other side. Such architecture facilitates the integration of CoLDE in any positioning system. CoLDE-Proxy acts as a proxy for Wi-Fi clients. At the same time, it acts as an Indoor-positioning cache (2nd level of caching) to speed up the positioning process, to reduce the traffic with the positioning system (in case it is located on a different server) and to be a temporary backup in case of losing connection with the positioning system. The possibility of using the caching varies depending on the positioning system itself.

CoLDE-Proxy can work with different positioning systems at the same time. Depending on the field *System* (CoLDE-Request) (Fig. 4.), CoLDE-Proxy can decide the format of the data and to which system they should be forwarded to. CoLDE-Proxy receives the data from the AP(s), it puts them into the appropriate format (according to the selected positioning system) and then it makes a call to the functions of that positioning system. It sends the result back to the access point(s) that sent the data. This procedure is repeated every time a client sends a positioning request. If the caching service is used, CoLDE-Proxy checks the cache before starting the session with the positioning system.

(Fig. 7.) summarizes the procedures of the three components in our solution and the communication between them.

V. Related Positioning Methods And Applications

Below we discuss some algorithms and methods which have been developed for indoor positioning, at the same time we will mention how they could be improved using our solution for connectionless.

Wi-Fi Localization Using RSSI Fingerprinting

Wi-Fi Fingerprinting creates a radio map of a given area based on the RSSI data from several access points and generates a probability distribution of RSSI values for a given (x,y) location. Live RSSI values are then compared to the fingerprint to find the closest match and generate a predicted (x,y) location[17]. We take two examples of the applications that use fingerprinting methods.

Google Maps [18] application can solve the problems of positioning navigation in open areas and indoors. It provides the possibility to calculate the route inside the building between several floors in addition to navigation [19]. For orientation it uses Wi-Fi and cellular networks with positioning accuracy ranges from 5 to 10 meters [20].

Skyhook Wireless [21] is one of the main companies in the domain of localization and positioning. Skyhook is a multiple source location system that uses Wi-Fi, GPS and cell towers which should work better in cities where Wi-Fi and cell tower signals are highly present[22]. Skyhooks Core Engine is a software-only location system. It uses a massive reference database comprised of the known locations of over 250 million Wi-Fi access points and cellular towers. Skyhook client software running on a Wi-Fi-enabled mobile device collects raw data from each of the location sources. The client needs to be connected on the Internet to send this data to the Location server.

It is possible to enhance these applications by using CoLDE, the users will be able to broadcast the gathered information to APs, which will forward them to the location server of the company(s) that support(s) this area. The response will be sent to the access point and then back to the client in a probe response.

Owl Positioning System (OwlPS)

OwlPS implements several positioning techniques and algorithms (RADAR[3], Interlink Networks [25], FBCM [26] and Basic FRBHM [27]), allowing to combine and compare them, even in a real-life experiment way [23]. The configuration where infrastructure executes all the processing needs several elements: mobile terminals equipped with Wi-Fi cards, access points or any capture device (listening for any positioning request transmitted by the mobiles), the aggregation server (which the APs forward the received positioning requests to) and the computation server (which computes the position of each mobile from information forwarded by the aggregation server) [24].

The system works as follows: the mobile airs a positioning request and capture devices (the infrastructure) capture it. This request consists of 10 to 20 UDP packets containing the local time. Each AP capturing the positioning request transmits it to the aggregation server along with additional data. The additional data consists of : the mobile MAC and IP addresses, the AP's MAC address, the time at which the packet was captured and the RSSI. The aggregation server gathers the data and forwards them to the computation server. The computation server analyzes the information received from the aggregation server and computes the mobile position. The computed position can be sent to the mobile by using direct connection between the computation server and the mobile.

OwlPS could use the CoLDE Indoor Positioning Frame (Fig. 4.), (Fig. 5.) to exchange data.

By using CoLDE, any Wi-Fi device can broadcast a probe request on a channel. The APs capture the probe request, each will forward it to CoLDE-Proxy along with the AP data. CoLDE-Proxy will relay the data to the aggregation server. The latter will process the data and forward it to the computation server. The computation server computes the position and sends it back to the APs. The APs send back the position in the probe response.

Using CoLDE would affect the mechanism of the system itself by adding the possibility to send the computed position to the mobile without having direct connection with it. Another advantage is the amount of data processed, while OwlPS depends on capturing and processing all frames (management and data frames), CoLDE processes the management frames only.

Collaborative Indoor Positioning
This kind of approach is the opposite of the localization methods that depend on the infrastructure. The collaborative localization proposes a model where clients may act as reference points in addition to their role as clients. People-Centric Navigation (PCN) provides an indoor localization solution by using the clients themselves as reference points. Clients with the PCN (i.e., mobile phones) continuously obtain accelerometer and digital compass readings to estimate step counts and direction. They also estimate a vector of each step called step vector, using the direction information and stride length. Since the stride length varies between individuals, it is approximated from the body height. Clients also record RSS from neighboring clients, which is collected through the device discovery process of Bluetooth. Step vectors and RSS are transferred to a centralized server called a PCN server via 3G or Wi-Fi. Then the PCN server estimates relative positions among users and the results are sent back to the clients to give them estimated positions[28].
Using CoLDE, PCN method can be enhanced to enable clients to broadcast their gathered data to the access point to be forwarded to the server without having any connection.

Emergency Evacuation
Emergency evacuation from buildings during catastrophic events need to be quick, efficient and distributed. Indoor localization with CoLDE can be used to optimize this process. In some cases, people could be trapped inside the building because of some obstacles or because of being injured or having a certain disability. Indoor localization using CoLDE can be used to have an updated database of mobile location tracking information. Indeed, they allow to determine the current location of the people present in a building. This permits rescue teams to find them by asking the approximate location.

VI. Experiments And Results

Our experiments and scenarios aim at demonstrating the improvement in indoor positioning systems by utilizing CoLDE. We evaluate and quantify the performance of the protocol in a real and congested environment. In this environment, there are more than 20 APs on different frequencies, the APs handle hundred of requests, and the clients receive hundred of broadcasting frames.
The experiments have been conducted using the following parameters:

- **Indoor positioning system**: we used a centralized trilateration indoor positioning system. The system maintains a database of the APs MAC addresses and their coordinates. It computes the client position by utilizing the APs coordinates, and their RSSI. In our experiment, the trilateration indoor positioning system was running on the same server with CoLDE-Proxy, so we eliminated the delay that could be caused by the network. The time needed to compute the position using the trilateration algorithm ranges between 5ms and 10ms. To simulate the delays in the other indoor positioning systems, we repeated the same trilateration algorithm with different delays. Each delay represents a different scenario, it simulates different indoor positioning system. We tested the following scenarios (the number after ”-” is the delay in milliseconds):
  - **(Scenarios-Group-I)**: Scenario-10, Scenario-100, Scenario-1k, Scenario-2k, Scenario-4k, Scenario-8k.
  - **(Scenarios-Group-II)**: Scenario-16k, Scenario-32k.
- **CoLDE-Client**: it is a Java application running on Linux. It utilizes the iw library (written in C). It uses the same architecture that we mention in Section IV. We customized it to collect the data needed for the trilateration indoor positioning system. A Wi-Fi client performs active scanning to collect the APs in its area and to send the data in a positioning request. The detailed functionality is described in (Fig. 8.).
- **CoLDE-Proxy and CoLDE-AP**: we have implemented one CoLDE-Proxy server and 3 CoLDE-APs as mentioned in Section IV.

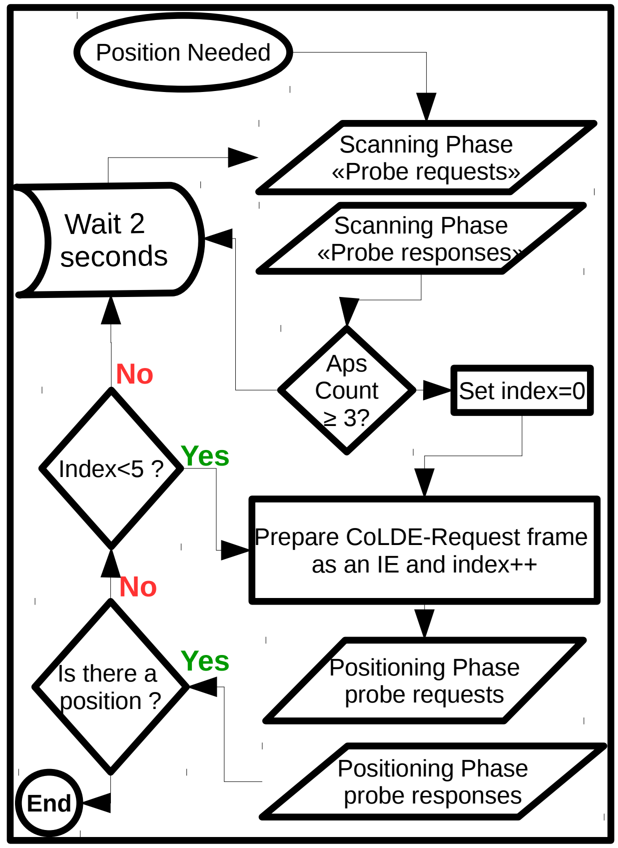

Fig. 8. CoLDE-Client - Trilateration

We installed the CoLDE-APs in different location. We configured them with different SSIDs and on multiple frequencies. All APs are connected to CoLDE-Proxy on the

TABLE I
EXPERIMENTS RESULTS

	Scenario-10	Scenario-100	Scenario-1k	Scenario-2k	Scenario-4k	Scenario-8k	Scenario-16k	Scenario-32k
Data Collecting Time (ms)	5300	5368	5657	5220	5120	5004	8677	9879
Position-obtaining Time (ms)	4568	4900	8126	8353	8283	11729	32545	32874
Data Collecting Scans	1	1	1	1	1	1	2	2
Position-obtaining Scans	1	1	2	2	2	3	9	9
Cache	Not Used	Not Used	Used	Used	Used	Used	Used	Used

same LAN. CoLDE-Client is installed on an IPC.

In our experiment, we studied the following aspects:

- **Frame size**: we assessed the effect of adding CoLDE data to the probe request/response frames. CoLDE adds up to 255 bytes into the probe request/response frames. (Table II) summarizes our results. It shows that, the round trip with CoLDE needed about 53% more than the same trip without CoLDE.
- **Data Collecting - Number of Scans**: number of active scans needed to collect the data. (Fig. 9) shows the number of scans needed for each scenario. We noticed that in Scenarios-Group-I, a client needs to scan the network only once. For Scenarios-Group-II, a client needs to scan the network 2 times to collect the data.
- **Position-obtaining - Number of Scans**: number of active scans needed to obtain the position. (Fig. 9) shows the number of scans needed for each scenario. We noticed that, a client needs to scan the network only once in Scenario-10 and Scenario-100, twice in Scenario-1k, Scenario-2k, Scenario-4k and 3 times in Scenario-8k. For Scenarios-Group-II, a client needs to scan the network about 9 times to obtain the position.
- **Data Collecting Time**: All infrastructure-based positioning systems require data sourced from various functions. For the data provided by the APs, We observed the time needed to collect this data using CoLDE. This time includes: time needed to send probe request by the client, time to process the request by the AP and time to send the probe response to the client. In (Fig. 10), we notice that data collecting time is about the same for Scenarios-Group-I. For Scenarios-Group-II, We found out that we needed double the time, because the client repeats the data collecting process after 5 failed tries, as described in (Fig. 8.).
- **Position-obtaining time**: it is the time between sending the positioning request in a probe request, and receiving the position in a probe response. For both of the scenarios group, the position-obtaining time is the sum of two values: the time required to compute the position (on the server), and a value ranges between (2000ms and 3000ms). This value represents the time needed to scan the network.

TABLE II
THE EFFECT OF ADDING COLDE INTO PROBE FRAMES

CoLDE	Probe	Size	Round-Trip Time
Without	Request	103 bytes	26 milliseconds
	Response	125 bytes	
With	Request	352 bytes	61 milliseconds
	Response	168 bytes	

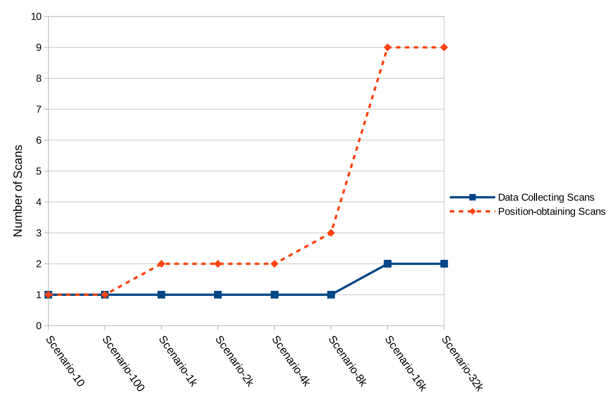

Fig. 9. Number of Scans

- **Position from the AP cache**: we observe the time when the client sends a second probe response, because it failed to obtain the position in the first one. In (Table II), clients obtained their positions without caching in Scenario-10 and Scenario-100. For all other scenarios, the positions have been cached in APs, the clients obtained them in the next probe response frame.

Experimental results prove that utilizing the management frames to send the data to the indoor positioning system does not change the protocol operation in any way. The delay resulted from adding data into the probe request/response frames is less than active scanning timeout. CoLDE needs about 3 seconds to exchange the data between the clients and the indoor positioning system. The AP caches are used for all indoor positioning that need more than 100ms to compute the position. Using the AP's cache gives an effective solution for the problems could be caused by the timeout of management frames.

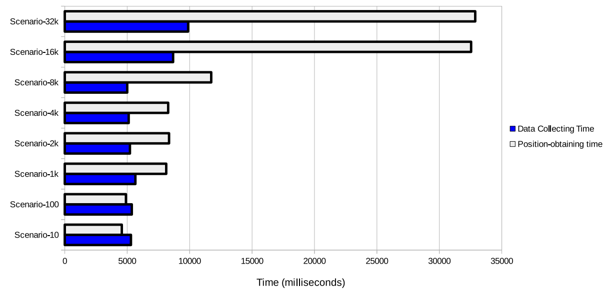

Fig. 10. Scan and Positioning Duration

VII. Conclusion and Perspectives

In this paper, we presented our solution to make indoor positioning functions available for public use. We proved that it is possible to change the way the service is provided by using the connectionless protocol CoLDE. We showed that CoLDE offers the needed mechanism for APs to be the bridge between Wi-Fi clients in their coverage areas, and the positioning systems that could be located on network different from the APs ones. We discussed the case where CoLDE can even improve some algorithms by providing them with more amount in data, where it would be impossible to have them using the traditional ways. We presented our component CoLDE-Proxy which is the interface between infrastructure devices and positioning systems. We showed that by using CoLDE-Proxy, clients in the same area can use different positioning systems, even without being connected directly to any of them. Integrating CoLDE into any positioning system does not interfere with the main functionality of the system, and it could even be transparent for the positioning system itself.

The experiments showed the ability to utilize CoLDE with a centralized trilateration positioning system. They proved the ability to have CoLDE working with indoor positioning systems that need more time to compute the positions, due to two levels of caching.

As for future work, our plans cover four aspects. Firstly, we plan to port CoLDE to different mobile platforms. Secondly, we plan to work to integrate CoLDE into an open-source operating system, such as OpenWrt. This step should facilitate upgrading the compatible access points to support CoLDE. Thirdly, we will work to develop CoLDE-Proxy so it can be integrated with different types of positioning systems. Finally, We are going to use the results of the three above-mentioned aspects to develop a standard for security in connectionless protocols.

Acknowledgment

This work has been supported by the European project G-navis (FP7 Collaborative Project, grant agreement No. 287203).

References

[1] K. Chen and K. R. Vadde, "Design and evaluation of an indoor positioning system framework" U.C. Berkeley course project for CS262A,2012.

[2] Da Zhang; Feng Xia; Zhuo Yang; Lin Yao; Wenhong Zhao: Localization Technologies for Indoor Human Tracking, Future Information Technology (FutureTech), 2010 5th International Conference, Page(s): 1-6

[3] P. Bahl and V. Padmanabhan. Radar: An in-building rf-based user location and tracking system. In INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, volume 2, pages 775-784. IEEE, 2000.

[4] Zengshan Tian, Xiaomou Tang, Mu Zhou, Zuohong Tan: Fingerprint indoor positioning algorithm based on affinity propagation clustering. EURASIP J. Wireless Comm. and Networking 2013: 272 (2013)

[5] Jianwei Niu, Banghui Lu, Long Cheng, Yu Gu. Lei Shu. ZiLoc: Energy Efficient WiFi Fingerprint-based Localization with Low-Power Radio. 2013 IEEE Wireless Communications and Networking Conference (WCNC 2013), Shanghai, China, April 7-10,2013.

[6] O. Abu Oun; W. Abdou; C. Bloch; F. Spies, Broadcasting Information in Variably Dense Environment Using Connectionless Data Exchange (CoLDE), WWIC 2014, LNCS 8458, pp. 283296, Springer International Publishing France, Paris 2014

[7] Ranveer Chandra, Jitendra Padhye, Lenin Ravindranath,Alec Wolman,"Beacon-Stuffing: Wi-Fi without Associations", Published in:Proceeding HOTMOBILE 07 Proceedings of the Eighth IEEE Workshop on Mobile Computing Systems and Applications, pages:53-57, 2007

[8] Muralidharan, K.;Software Eng. and Technol. Labs.,Infosys Technol. Ltd.,Bangalore;Dhanapal, K.B.;Chowdhury,A.R.,"BOWL: Design and implementation of a (connectionless) broadcasting system over wireless LAN", Published in:World of Wireless, Mobile and Multimedia Networks, WoWMoM 2008, pages:1-6, 2008

[9] Schauer, Lorenz; Dorfmeister, Florian; Maier, Marco, "Potentials and limitations of WIFI-positioning using Time-of-Flight," Indoor Positioning and Indoor Navigation (IPIN), 2013 International Conference on , vol., no., pp.1,9, 28-31 Oct. 2013

[10] Sourangsu Banerji; Rahul Singha Chowdhury,"ON IEEE 802.11:WIRELESS LAN TECHNOLOGY", International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol. 3, No.4,pages:45-64, August 2013

[11] D. Maniezzo, G. Villa, M. Gerla, "A smart MAC-routing protocol for WLAN mesh networks",UCLA-CSD Technical Report number 040032,2004

[12] Vishal Gupta; Mukesh Kumar Rohil, "Information Embedding in IEEE 802.11 Beacon Frame", National Conference on Communication Technologies & its impact on Next Generation Computing CTNGC 2012 Proceedings published by International Journal of Computer Applications (IJCA)

[13] Atul Adya, Paramvir Bahl, Ranveer Chandra, and Lili Qiu, Architecture and Techniques for Diagnosing Faults in IEEE 802.11 Infrastructure Networks, in ACM MobiCom, Association for Computing Machinery, Inc., September 2004

[14] Vaibhav Gupta, Raheem A. Beyah, Cherita L. Corbett: A Characterization of Wireless NIC Active Scanning Algorithms. WCNC 2007: 2385-2390

[15] Linux Wireless, nl80211 Documentation, [Online] Available: http://wireless.kernel.org/en/developers/Documentation/nl80211

[16] hostapd: IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/EAP/RADIUS Authenticator, URL: http://w1.fi/hostapd/

[17] Eduardo Navarro, Benjamin Peuker, Michael Quan, Dr. Christopher Clark, Dr. Jennifer Jipson, "Wi-Fi Localization Using RSSI Fingerprinting", URL:http://digitalcommons.calpoly.edu/cpesp/17

[18] R. Kim. (2011, November 29). Google turns on indoor mapping with Google Maps 6.0 for Android [Online].Available : http://gigaom.com/2011/11/29/google-turns-on-indoor-mapping-with-google-maps-6-0-for-android/

[19] Sagar V. Ramani, Yagnik N. Tank: Indoor Navigation on Google Maps and Indoor Localization Using RSS Fingerprinting, International Journal of Engineering Trends and Technology (IJETT) Volume 11 Number 4 - May 2014

[20] Alexey Kashevnik, Maxim Shchekotov. Comparative Analysis of Indoor Positioning Systems Based on Communications Supported by Smartphones. Proceeding of the 12th conference of fruct association.

[21] Skyhook Location SDK [Online]. Available:http://www.skyhookwireless.com/

[22] Rune A. Liljegren, Ulrik L. Jensen, "Performance Evaluation of the Skyhook Wireless Positioning System", Paper submitted for evaluation

in the Pervasive Computing Course, Fall 2010. The IT University of Copenhagen
[23] Matteo Cypriani, Frederic Lassabe, Philippe Canalda, and Francois Spies. Open Wireless Positioning System: a Wi-Fi-Based Indoor Positioning System. In VTC-fall 2009, 70th IEEE Vehicular Technologie Conference, Anchorage, Alaska, United States, pages 1-5, September 2009. IEEE Computer Society Press
[24] Cypriani, Matteo and Canalda, Philippe and Lassabe, Frédéric and Spies, François. Wi-Fi-Based Indoor Positioning: Basic Techniques, Hybrid Algorithms and Open Software Platform. IPIN 2010, 1st IEEE international conference on Indoor Positioning and Indoor Navigation. pages 116-125. ETH Zurich, Campus Science City (Hoenggerberg), Switzerland. Sep 2010.
[25] Interlink Networks, Inc., A practical approach to identifying and tracking unauthorized 802.11 cards and access points, Tech. Rep., 2002.
[26] F. Lassabe, O. Baala, P. Canalda, P. Chatonnay, and F. Spies, "A Friis-based calibrated model for WiFi terminals positioning" in Proceedings of IEEE Int. Symp. on a World of Wireless, Mobile and Multimedia Networks , Taormina, Italy, Jun. 2005, pp. 382-387.
[27] F. Lassabe, D. Charlet, P. Canalda, P. Chatonnay, and F. Spies, "Refining WiFi indoor positioning renders pertinent deploying location-based multimedia guide" in Procs of IEEE 20th Int. Conf. on Advanced Information Networking and Applications , vol. 2, Vienna, Austria, Apr. 2006, pp. 126-130
[28] Hirozumi Yamaguchi, Takamasa Higuchi and Teruo Higashino, Collaborative Indoor Positioning of Mobile Nodes, Proc. of ICMU2012, pp. 156-163, May 2012