KNUV 2015; 1(43): 5-15

Antoni Masiukiewicz
Akademia Finansów i Biznesu Vistula – Warszawa

THE METHODS OF USERS LOCALIZATION IN 802.11 NETWORKS

Summary

The location systems for 802.11 devices become important issue. There is a lot of new applications which require the asset tracking. The information about station location could also help in proper channel selection in small home networks.

Key words: 802.11 standard, station location, GPS, RF ID, fingerprinting.

JEL codes: C61, O33

Introduction

The WiFi applications market is continuously growing in many segments. Some of the new solutions require the information about the AP or station or both location. Location-based computing can be used by applications running in portable devices for taking better decisions and improving their performance as well as support different kind of activities e.g. a system supporting location-aware reminders would allow a user to set reminders relevant to their location, such as "pick up your documents" when near the printer closet (Liu 2004). Many new applications are dedicated to indoor use especially in office buildings. The samples of new location services are presented in Table 1.

It is worth to notice that presently a lot of devices were equipped with WiFi receivers. So the I Phones, Smart phones, Tablets and others dedicated to different applications devices are at the same time 802.11 standard devices. The market of RTLS (Real Time Location Systems) could reach the volume of 800 mln $ (Lansford 2010). The location info is one of the thing which is necessary to improve the QoS in small private and home 802.11 networks. Today the users of such networks usually have limited scope of information concerning neighborhoods AP's. Typical data include SSID, the outers AP's channel numbers and the signal power for each AP respectively (Masiukiewicz 2014). This is not enough for a sufficient channel selection. The information about location could release this problems especially in 2,4 GHz band where

the number of non–overlapping channels is far below the real needs and the interference calculation and optimization is crucial issue (Dolińska et al. 2013).

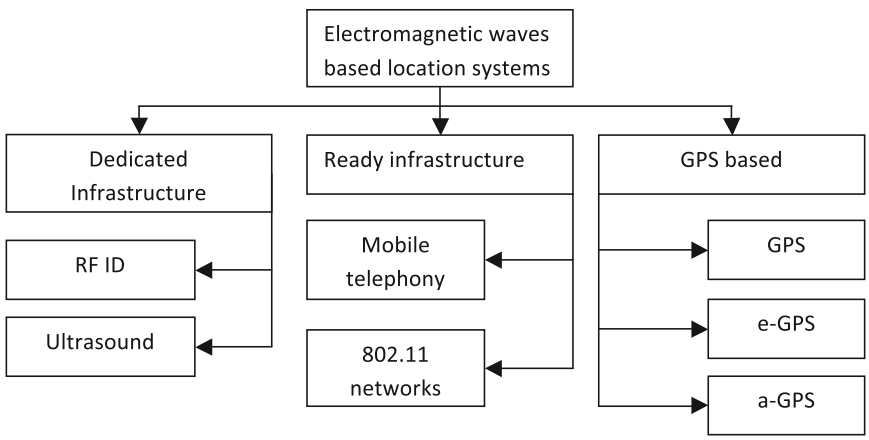
Table 1. Location services

No	Service	Accuracy	Terminal status
1	Terminal tracking and supporting user with additional information especially within the office buildings	Medium, the floor distinguishing could be essential	Moving
2	Terminal tracking and supporting with guide information	Medium or high within buildings	Moving
3	Location identification of objects using rescue number 911 e.g. E911	Medium	Static
4	TV white spaces	High	Static
5	Production	High	Moving

Source: own preparation.

Generally there are a lot of methods used for object location (Hightower, Barriello, 2001a; Hightower, Barriello 2001b; Burroughs 2012) The system classification is presented in fig. 1.

Fig. 1. Electromagnetic waves based location systems



Source: own preparation.

The basing principle is the use of different electromagnetic waves and the location system could be built as the infrastructure one with own senders, receivers, data bases, servers and processes. That is with popular RF ID (Radio Frequency Identification) systems or ultrasound systems. Both are wide use in the industry. The second solution is the location terminals using existing infrastructure and ready communication systems. Such situation is when we based on mobile telephony networks or 802.11 networks however the system parameters and a results the possible scope of location are quite different. While the global mobile telephony consist of many networks with mutual relations (due to roaming services) the 802.11 networks are rather separated island with the one joint element which is Internet. There are possibilities of station location using the 802.11 infrastructure. In this case knowledge about AP's location is necessary. such a method is presented by Kim (Kim *et al.* 2006). The real global system is the GPS with its versions dedicated to mobile devices (assisted -GPS and enhanced GPS). GPS have some disadvantages when it is use in the buildings. The location determination requires the visibility (LoS path) of a required number of satellites.

Author give an overview of basic location method together with the description of different algorithms used for location calculation. Then these methods are compared from the point of view of possibility of 802.11 stations location.

Three and Four Reference Point Algorithms

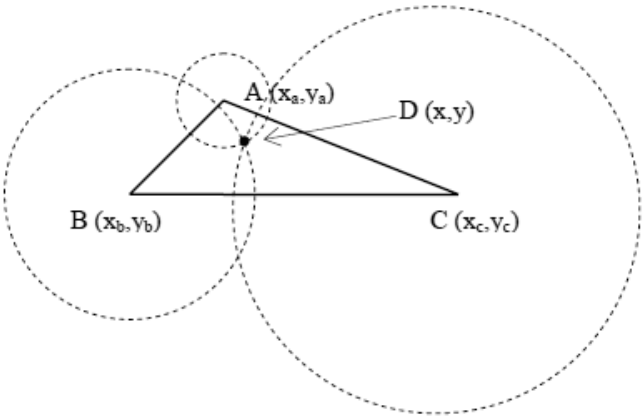
The triangulation location sensing technique uses the triangle properties to calculate object locations. There are two subcategories called respectively lateration, using distance measurements, and angulation, using primarily angle or bearing measurements.

Lateration calculates the position of an object by measuring its distance from multiple reference objects. Calculating an object's position in two dimensions plane requires measurements from 3 non-collinear points. If we would like to determine altitude distance measurements from 4 non-coplanar points are required. Some knowledge about the reference point/objects location may reduce the number of required distance measurements e.g. if one reference object is placed above all others reference objects and unknown object typically three measurements will be enough to locate unknown object in 3- dimensional space.

The triangulation method (Sanchez *et al.* 2006) is the centralized one and it base on distance measurements of RSS (received signal strength). This is a direct mode measurement sometimes we say the we measure the attenuation. The devices (e.g. WiFi stations) do not estimate theirs location, they only sent RSS to a server, which calculates the position of each device. Location information

could be distributed via a web interface. In this way, users remotely can know the location of WiFi stations. This method can be useful when we know the position of at least three access points. The location of D station is in the point of three circle with centers and A,B, and C (three known AP's) intersection what is shown in fig.2.

Fig. 2. Triangulation method concept



Source: Sanchez et al. (2006).

Therefore, given coordinates of each access point (x_i, y_i) and distances from the portable device to each of them (d_i), the position of a device can be obtained by the following nonlinear equations set:

$$(x - x_i)^2 + (y - y_i)^2 = d_i^2$$
$$i = a, b, \ldots, n \tag{1}$$

The distance from the station D to each access point is necessary to solve the above equations set. This is done on the base of RSS measurements. The signal power is measure by each AP and from the modified Friis formula d is derived. The obstacles such as walls and the proper power correction of the signal power versus distance characteristics (α is typically higher than 2 – when 2 is the power for FSL (Hodgkinson 2007; Freeman 2007)). This method however requires a whole infrastructure to carry the location process. The infrastructure includes the server, data bases and dedicated software. Direct mode is more suitable for determination of static objects.

In indirect mode instead of measuring signal power from an unknown WiFi station time-of-flight is measured. ToF (time of flight) is the time it takes

to travel between the object and point P at a known velocity. The station may be moving, This method require high resolution of time or frequency measurement so it can be difficult to fulfill with 2,4 or 5 GHz bands. This method is more suitable for lower frequencies e.g. ultrasound bands.

The angulation technique is similar to lateration but instead of distances, angles are measured for determining the position. Two angle measurements and one length measurement such as the distance between the reference points are necessary for plane analysis. Additionally one azimuth measurement, are needed to specify a precise position in three dimensional space. Phased antenna arrays are a good subject for the angulation technique. Such a MIMO antennas are used in new 802.11 standards such as n, ac and ad.

The objects which are transmitting any electromagnetic field could be also locate by the radars or spectrum analyzers but it need a very expensive equipment. Such method are called "scene analyze".

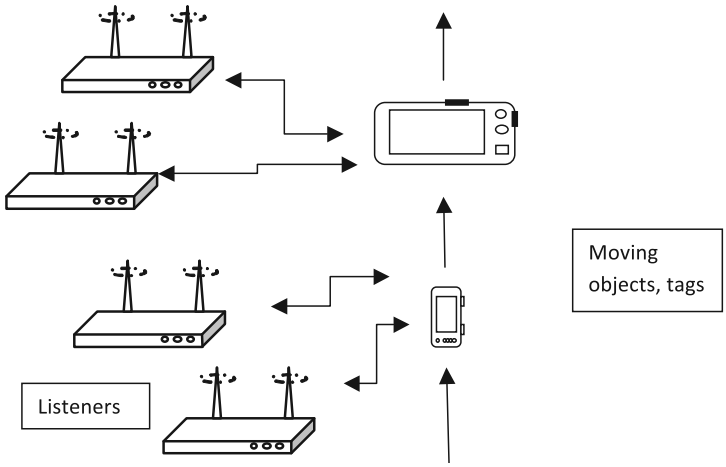
Other indirect method is proximity. The object is identified when it comes near to well known / well mark another object. There are three general approaches to sensing proximity:

- detecting physical contact which is the most basic type of proximity sensing. There are pressure sensors, touch sensors, and capacitive sensors,
- monitoring wireless cellular access points and associated with them mobile devices,
- using different ID systems such as credit card point-of-sale terminals, computer login histories, land-line telephone records, electronic card lock logs, and ID tags (RF or ultrasound technologies).

RF ID and Ultrasound Systems

Although RFID was not planned for indoor location of the wireless stations there are some developments which show that this method could be useful (Ni 2004). The basic nature of RFID techniques is lack direct contact and no need of LoS path between any active devices. RFID (RF Identification) is a tool of storing and conversion data through transmission of electromagnetic wave to an RF compatible reading circuit. An RFID system has a few basic components including a number of different RFID readers and RFID tags. The system structure is shown in fig. 3.

Fig. 3. RF ID system architecture



Source: like in fig. 1.

Generally the RFID devices can by classified as passive which can just reflect signals and active (able to send own signals). There is a lot of ready to use RFID systems which are used in production lines and to trace different objects.The system range depends on three main elements:

- the maximal signal power of the reader,
- the maximal signal power available within the tag to respond.
- the path structure and typical radio channel parameters (fast and slow fading, SNR, real room signal attenuation etc.).

Both the RF ID or ultrasound tags, beacons could be add to a 802.11 device,but efficient tracking need a whole system with reading/listening devices, computer system and data bases. Typical ToF measurements are the base for location calculation (Saha *et al.* 2002).

Fingerprinting

There are a few possibilities of tracking 802.11 standard devices. The WiFi device could be uniquely indentify by MAC address. The stations could use temporary names but is not enough to protect location privacy (Pang 2007). Generally the process of WiFi station tracking is called fingerprinting and very often there are commercial reasons for such activity. The fingerprinting is rather used for presence detection not a location however we often say that the station is localized.

Two factors let to 802.11 devices tracking increase. First the low cost of 802.11 hardware and its growing popularity and the second the large number

of WiFi commonly available network monitoring software (e.g. Net Stumbler 0.4.0, Xirrus WiFi Inspector).

Even without a unique address (e.g. MAC) , characteristics of users' 802.11 traffic can identify them and track them with high accuracy. Such an temporary ID is the IP address of a service that a user frequently accesses, such as his or her email server. In a population of several hundred users, this address might be unique to one individual; thus, the mere observation of this IP address would indicate the presence of that user. There are also other network or user activity parameters which could help to detect the user presence such as: network destinations, network names advertised in 802.11 probes, differing configurations of 802.11 options, and sizes of broadcast packets. If the 802.11 user is associated with access points we know that he is less than tens of meters away, and if we know the access point location new know a user coarse location (very coarse could means home or workplace).

Systems that can employ additionally or parallel any RFID, RSSI or radar location methods can obtain more accurate user's location.

Fingerprinting can be use can be use to find a user in 802.11 networks. The accuracy could be within the range from few to tens meters. The name fingerprint corresponding to the pairs of signature-location which form the known set of data. In case of high accuracy necessity typical fingerprinting system requires a lot of previously carried out measurements and temporary recalibration (it means more set of measurements).

GPS Based Location

The most recognized global positioning system is GPS. The use of satellites is free of charge and coverage is quite impressive. The location of WiFi AP's and stations needs however LoS (line of sight) path. In opinion of (Liu 2004) the accuracy of GPS supported by 802.11 standards are not sufficient for very precise location determination especially for indoors use when there is problem with LoS path to the satellites (at least three are required because the triangulation method is applied). The new amendments to the 802.11 std such as 802.11k and 802.11v give more support to GPS localization issue. The system of several satellites enable use of ToF techniques together with the triangulation method. The GPS system provides a very accurate time reference and time measurement possibilities (Czarnecki *et al.* 2000). The use of three satellites enables 3 dimensional location while the fourth reference satellite let us make a correction between clocks (receiver clock and GPS system time) what reduces the time errors and as a consequence improve location accuracy.

The 802.11 standard is continuously developed. The 802.11k and 802.11v amendments provide a framework for radio resource and network management,

respectively (Hiertz 2010). The 2008 approved 802.11k provides a lot of radio channel information. 802.11k measurement reports include a channel load and noise histogram, provide location information, give details on a wireless link and assist APs by means of a detailed neighbor AP report. While many vendors already use device statistics for channel selection, 802.11k delivers the first standardized solution. With traffic filtering, diagnosis and event reporting, 802.11v centers on device and network management and introduced WNM (Wireless Network Management).

802.11k approved in 2008 (IEEE 802.11k 2008) introduced 'Location Configuration Information (LCI)' which addresses following issues:
- initiation from AP or client,
- can be used for 'my location' or 'your location',
- format is geospatial, based on RFC 3825 (latitude, longitude, altitude).

The 802.11v (IEEE 802.11v 2011) adds respectively 2 new formats for location:
- 'Civic address' based on RFC 4776/5139,
- 'Identifier' (URI).

There some modification of GPS access. In e-GPS (enhanced GPS, EGPS) some new solutions are designed especially for mobile phones to improve GPS signals to deliver faster location fixes, lower cost implementations and reduced power and processing requirements. The a-GPS (assisted GPS) helps to decrease the time of obtaining the first coordination data set from satellites because the data are available at operator servers.

Conclusions

Theoretically at least a few methods can be used to locate the WiFi station. The most important issues are as follows:
- what for is the location needed,
- the station is moving or static,
- what accuracy is necessary,
- what cost could be accepted,
- the assets tracking is the single needs or continuous process.

The target of the analysis is to find the method of WiFi device location in small home or private network. This is a single measurement and accuracy of a few meters could be sufficient. The floor or the station altitude will be an advantage. The basic features of different system are compared in table 2.

Table 2. Features of different location methods

Method	Strength	Weaknesses
RF ID / ultrasound / proximity	Good accuracy	Dedicated infrastructure Not applicable for single measurement High cost
RSSI	Medium accuracy within the buildings Low cost	Needs a close cooperation of at least a few AP Administrator advisable
GPS	Low cost Implemented in 802.11 v and k standards amendments Possible data distribution via 802.11k and v options Two ways of introducing data-measurements or electronic maps data	Poor GPS signal inside buildings

Source: like in table 1.

The best solution for single measurement data location of WiFi station seems to be GPS based method. There is no additional cost and the standard amendments 802.11k and 802.11v let the processing of geographic data. Two formats of input data are accepted: data from digital maps or from GPS system. It helps to reduce the basic weaknesses of this method which is poor indoor signal. The data can be easily broadcast and received by all 802.11 users.

Bibliography

Burroughs K. (2012), *Discussion of Indoor Location Standards*, Qualcomm.

Czarnecki A., Lisowiec A., Masiukiewicz A. (2000), *GPS nie tylko do nawigacji*, „Infotel", nr 1.

Dolińska I., Masiukiewicz A., Rzadkowski G. (2013), *The mathematical model for interference simulation and optimization in 802.11n networks*, Workshop, Concurrency Specification and Programming 2013, CS&P, Warsaw University.

Freeman R.L. (2007), *Radio system design for telecommunication*, Wiley Interscience, IEEE, New Jersey.

Hightower J., Borriello G. (2001), *Location Sensing Techniques, Technical Report UW-CSE-01-07-01*, University of Washington, Computer Science and Engineering, July.

Hightower J., Borriello G. (2001), *Location Systems for Ubiquitous Computing*, "IEEE Communications Magazine", August.

Hodgkinson T.G. (2007), *Wireless communication – the fundamentals*, "BT Technology Journal", Vol. 25.

Hiertz G.R. (2010), *The 802.11 Universe*, "IEEE Communications Magazine", January.

IEEE Std 802.11k™-2008

IEEE Std 802.11v™-2011

Kim M., Fielding J.J., Kotz D. (2006), *Risks of using AP locations discovered through war driving*, "Lecture Notes in Computer Science", Vol. 3968.

Lansford J. (2010), *802.11 WNG Presentation on Location Awareness*, doc.: 802.11-10/1239r02, November.

Liu A., Robinson T. (2004), *Cost and Accuracy: Factors Concerning Various Indoor Location Estimation Methods*, https://courses.cs.washington.edu/courses/cse561/04au/projects/papers/A.Liu-Robison.pdf [access: September 2014].

Masiukiewicz A. (2014), *Channel selection in home 802.11 standard networks*, Digital Technologies 2014 Conference, Żylina, Slovakia.

Ni L. M., Liu Y.,. LauY. C, Patil A. P. (2004), *LANDMARC: Indoor Location Sensing Using Active RFID*, "Wireless Networks", No. 10.

Pang J., Greenstein B., Gummadi R., Seshan S., Wetherall D. (2007), *802.11 User Fingerprinting*, MobiCom'07, September 9–14, Montréal, Québec, Canada.

Sánchez D., Afonso S., Macías E. M., Suárez Á. (2006), *Devices Location in 802.11 Infrastructure Networks using Triangulation*, Grant TSI 2005-07764-C02-01, Contract PI042004/164.

Saha S., Chaudhuri K., Sanghi D., Bhagwat P. (2002), *Location Determination of a Mobile Device Using IEEE 802.11b Access Point Signals*, IEEE Wireless Communications and Networking Conference.

Metody lokalizacji użytkowników w sieciach 802.11

Streszczenie

Systemy lokalizacji terminali w sieciach 802.11 stały się istotną kwestią. Wiele nowych aplikacji bazuje na śledzeniu użytkowników. Informacje o lokalizacji punktów dostępowych mogą również pomóc we właściwym doborze kanałów w małych sieciach domowych.

Słowa kluczowe: standard 802.11, lokalizacja punktów dostępowych, GPS, RF ID, metody porównawcze.

Kody JEL: C61, O33

Artykuł nadesłany do redakcji we wrześniu 2014 r.

Afiliacja:
dr Antoni Masiukiewicz
Akademia Finansów i Biznesu Vistula
ul. Stokłosy 3
02-787 Warszawa
tel.: 22 457 23 00
e-mail: a.masiukiewicz_globalteam@op.pl