EasyChair Preprint

№ 3902

Using WiFi Signals in Combination with GPS to Track Human Traffic in a Space

James Roetman

July 18, 2020

Using WiFi Signals in Combination with GPS to Track Human Traffic in a Space

James Roetman
Flinders University

Roet0008@flinders.edu.au

Abstract

In large, open spaces, GPS can be used to show your current location with relatively high accuracy, but this accuracy drops significantly in areas with limited GPS signal, such as when surrounded by buildings or in a location without direct line of sight to GPS satellites. Another limitation of GPS is that it cannot show where you are vertically in a space such as a building with multiple floors. Combining GPS with an understanding of the WiFi devices in an area and how they work can resolve these issues in applicable situations.

1 Introduction

While GPS has many limitations in terms of accuracy due to its use of satellites to provide the users location, most of these can be overcome by using knowledge of the WiFi access points in the area. As defined by the United States government, it is committed to providing a GPS accuracy of <7.8m, with 95% probability when under open sky (National Coordination Office for Space-Based Positioning, 2017). This can become significantly worse when in an enclosed space or surrounded by many tall structures. If you know where all the access points in a given area are, you can, using various methods, find their location to within 0.5m to 2m(Zandbergen, 2009). There are many different techniques which can be used, such as, Received Signal Strength Indicator (RSSI) and Lateration, Fingerprinting, Angle of Arrival, SpotFi and Time of Flight. Often a combination of the above is used to play to the different strengths of each method. For example, angle of arrival is highly accurate but requires a large amount of processing power in the user's end to provide results, whereas fingerprinting uses past results as a starting point and combines with another method with low processing overhead, usually RSSI, to provide accurate results without much burden on the end users device or the system. This type of tracking has been in use for many years in large shopping complexes where it is used to give accurate directions to particular locations; in museums, so that they can show extra information about the pieces around you based on your location and sporting stadiums where it is used to determine the amount of people coming and going through areas to try and increase the efficiency of entrances and exits, reducing queue times and congestion. This paper will discuss the different types of WiFi signal tracking, their strengths, weaknesses and in which situations they should be used.

2 Types of WiFi Signal Tracking

2.1 RSSI

RSSI uses the strength of WiFi signals which can be detected in the end user's device to triangulate their location. This can either be used in real-time or to create a fingerprinting system. Real-time RSSI tracking requires much more processing power at the time of tracking but is very simple to setup and is therefore the most used RSSI system. Fingerprinting initially uses real-time tracking but then keeps a log called a fingerprint database. The database can then be looked upon in the future for a similar case to provide results without a connection to a processing system. Fingerprinting is not as accurate as real-time tracking, requires an order of magnitude more setup work and does not cope well with changed to the physical environment which change the way WiFi signals travel. RSSI is often combined with fingerprinting to create an always updating database with less downtime (Paul & Wan, 2009).

2.2 Simple Network Management Protocol (SNMP)

SNMP is a method which is often used in large areas with hundreds of access points, and usually thousands of daily users. By logging the number of users connected to each access point at a given time and repeating at a regular interval. It is then possible to create a heatmap of where people are in the physical space. These access points also keep track of the Media Access Control (MAC) Address of each device. A MAC address is a 'unique' identifier, baked into a device which can be used to identify a device, although it does not include any other identifiable data. While a MAC Address shouldn't change or appear on multiple devices, there are many cases in which it can. Over time, this collected data can be used to learn which areas have higher and lower traffic and at which times of the day. SNMP is not capable of tracking a singular person in real-time with high accuracy although it can technically be used to track someone's movements through an area in a broad sense (Meneses & Moreira, 2012) by checking to see which access points their device has connected to via its MAC address. Although, as discussed above, this is not always an accurate indicator of a unique device(Chilipirea, Petre, & Dobre, 2016).

3 Ethics

There are many topics to be taken into consideration when discussing the ethics of GPS and WiFi tracking. The largest of which are the consent of the person/s who is/are being tracked and why they are being tracked. The reasons for tracking an individual or group range from the government tracking a parolee, to a caregiver tracking a mentally ill person in case they get lost and a car rental company tracking their vehicles in case of theft(Michael, McNamee, & Michael, 2006). In the case of tracking a person for navigation there are many applications which already do this, such as Google Maps which is by far the most common, boasting more than 154.4 million unique users each month as of May 2018 (Statista, 2018) and over one billion searches per month (Russel, 2019). These types of applications provide the user with an End User Agreement which, amongst other things, gives your consent for the company to track you and usually store the data generated for analysis. Best practise is to store this data without any of the end users' identifying information such as age, but more and more often in the information age, this is not the case. For example, the Facebook–Cambridge Analytica data scandal. In 2018, Facebook was caught allowing Cambridge Analytica to access the user data of millions of users, without their consent, for use in targeted political advertising (Cadwalladar & Graham-Harrison, 2018).

New laws in the European Union's General Data Protection Regulation (GDPR) as of May 2018 state that any time a company wishes to collect and store user data it is required to get explicit consent from the user. For most applications and websites, this is in the form of a one-time prompt when first accessing the service. The GDPR also states that service providers must provide a method for the end user to revoke their consent at any time and to be able to access all the personalized data which has been collected and stored about them in a human friendly format. While these rules technically only apply to users within the European Union, many companies have changed their global policies to match as many other nations look to adopt similar regulations (European Union, 2018). With maximum fines for breaching the regulations from 20 million to 4 percent of the company's global turnover (whichever is higher) (European Union, 2018, Article 83, Section 5), these are not rules which any company would want to come close to breaching.

4 Conclusion

In conclusion there are many different methods which can be used for tracking people. Some are used for personal tracking/navigation. Some used for tracking large groups of people. Some are aimed at giving real time results and others are designed to take in data over a longer period. RSSI and fingerprinting is the most popular method for real time tracking although is an extra step which can be used with nearly all real time algorithms. SNMP is used to track foot traffic over a period in order to provide data on how many people are coming and going. This can then be used to change building layouts etc. While there are many different reasons to track a person. In the case of tracking for navigation or statistical analysis, if the person/s being tracked are aware, there should not be any negative ramifications.

References

Cadwalladar, C., & Graham-Harrison, E. (2018, March 18). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. Retrieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Chilipirea, C., Petre, A.-C., & Dobre, C. (2016). Presumably Simple: Monitoring Crowds Using WiFi. *IEEE International Conference on Mobile Data Management*, 220-225. doi:10.1109/MDM.2016.42

General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 C.F.R. (2018).

Meneses, F., & Moreira, A. (2012, 13-15 Nov. 2012). *Large scale movement analysis from WiFi based location data.* Paper presented at the 2012 International Conference on Indoor Positioning and Indoor Navigation (IPIN).

Michael, K., McNamee, A., & Michael, M. (2006). The Emerging Ethics of Humancentric GPS Tracking and Monitoring. *International Conference on Mobile Business*, 34-34. doi:10.1109/ICMB.2006.43

National Coordination Office for Space-Based Positioning, N., and Timing. (2017). GPS Accuracy. Retrieved from https://www.gps.gov/systems/gps/performance/accuracy/

Paul, A. S., & Wan, E. A. (2009). RSSI-Based Indoor Localization and Tracking Using Sigma-Point Kalman Smoothers. *IEEE Journal of Selected Topics in Signal Processing, 3*(5), 860-873. doi:10.1109/JSTSP.2009.2032309

Russel, E. (2019). 9 things to know about Google's maps data: Beyond the Map. Retrieved from https://cloud.google.com/blog/products/maps-platform/9-things-know-about-googles-maps-data-beyond-map

Statista. (2018). Most popular mapping apps in the United States as of April 2018, by monthly users. Retrieved from https://www.statista.com/statistics/865413/most-popular-us-mapping-apps-ranked-by-audience/

Zandbergen, A. P. (2009). Accuracy of iPhone Locations: A Comparison of Assisted GPS, WiFi and Cellular Positioning. *Transactions in GIS, 13*, 5-26. doi:10.1111/j.1467-9671.2009.01152.x