Analyzing the Digital Society by Tracking Mobile Customer Devices

42

Lorenz Schauer

Abstract

Nowadays, most people use smartphones or tablets for personal or commercial purposes in their daily life. Such mobile devices are electronic all-rounders equipped with several sensors and communication interfaces, e. g., Wi-Fi and Bluetooth. Both communication systems leak information to the surroundings during operation which can be used for monitoring customers and analyzing their behavior in an area of interest. This article shortly describes techniques for tracking mobile customer devices and identifies potentials and limitations for analyzing the digital society based on mobile tracking data. Both scientific papers and commercial projects are investigated focusing on trends for the digitalization of the retail industry. Furthermore, different start-ups currently working in the field of retail analytics are presented and compared in terms of their unique selling point (usp) and future oriented projects. Overall, this book chapter presents a compact overview of state-of-the art techniques and future works for analyzing the digital society by tracking mobile customer devices.

42.1 Introduction

The ongoing digitalization is not only changing business and marketplaces, it is also changing our complete society. One of the most evident observation of this trend can be made in our life every day, e. g. when we go to work, when we meet friends, or even when we have dinner: people use their smartphones or other modern mobile devices for making business, chatting with friends, buying new products, or reading the newspapers

L. Schauer (✉)
Ludwig-Maximilians-Universität München
Munich, Germany
e-mail: lorenz.schauer@ifi.lmu.de

C. Linnhoff-Popien et al. (eds.), *Digital Marketplaces Unleashed*,
https://doi.org/10.1007/978-3-662-49275-8_42

on their way. Hence, the increasing usage of these electronic all-rounders in nearly all situations of today's life is an obvious characteristic of our digital society. Technically, the permanent and ubiquitous connection to data networks plays a key role in this process rendering digital mobile applications and services very powerful. Overall, without Internet, most services are not able to provide full functionality.

Therefore, together with the immense diffusion of smartphones and tablets, the usage of Wi-Fi as state-of-the-art wireless communication standard, has increased dramatically. Wi-Fi infrastructures have been installed in many public spaces and buildings providing Internet access and local services to mobile clients. Both facts lead to a high percentage of Wi-Fi enabled mobile devices which can be used to analyze our digital society by tracking mobile customer devices and without the users' consent or even awareness. The extracted information from such tracking data might be very valuable and helpful for different kind of use cases, such as retail analytics, crowd control, emergency situations, or just commercial purposes. On the other hand, tracking mobile customer devices without asking for users' compliance represents a privacy attack.

This book chapter firstly describes the technical background of tracking mobile devices using Wi-Fi signals which are automatically sent out by any Wi-Fi enabled smartphone, or tablet. Secondly, both scientific and commercial projects are presented and compared using such tracking data for different purposes. Overall, we discover potentials, risks, and limitations of this analyzation technique and focus on trends for the digitalization of the retail industry. In this context, some start-ups are presented and evaluated in terms of their unique selling point (usp) and future oriented projects. The aim of this article is to give a compact overview of state-of-the-art methods nowadays, and how Wi-Fi tracking can be used in the near future, when even more people use more than one device and MAC-Address randomization is integrated in common phones.

42.2 Technical Background

As already mentioned, we firstly give a short description of why and how Wi-Fi tracking can be realized technically. Wireless local area networks, commonly known as Wi-Fi, are standardized in IEEE 802.11 [1]. The communication range varies from about 35 m for indoor to over 100 m for outdoor scenarios. The standard defines three individual frame types:

- Control frames, to support the delivery process of data frames and to manage the medium access
- Data frames, to transport user data for higher layers
- Management frames, to exchange management information for connection establishment and maintenance

For Wi-Fi tracking, only management frames are of interest being involved in the 802.11 network discovery and association process as shown in Fig. 42.1.

From the view of a mobile device, the discovery process can be either passive by just listening on beacon frames which are periodically transmitted by the access point (1) or it can be active by sending out probe request frames (2). The latter is preferred in mobile context, due to lower energy-consumption and shorter discovery time of access points which could come into reach while moving [2].

Hence, Wi-Fi enabled mobile devices periodically perform an IEEE 802.11 active scan, in order to discover available access points in their surroundings more quickly. The scanning interval depends on the used chipset and the Wi-Fi driver, but not on the association status. Our own investigations show that an active scan is performed at least once within two minutes on average for Android and iOS devices. Furthermore, we also found a maximum idle time of less than 5 min where no probe requests were sent out during a 10 h test phase, despite the case that the test device was associated to an access point or not.

Generally, a device starts an active scan by sending out probe requests and listens for probe responses (3). This is done for each channel iteratively. Each probe request frame contains the device specific MAC address of sender and receiver, supported rates, the destination's network name (SSID) and other management information. If the SSID field is left empty, then the probe request addresses all access points in range which is seen as broadcast. If the SSID field is filled with a specific network name, only the corresponding access point with the same SSID will answer with a probe response frame when it's within range. These directed active probe requests are the consequence of hidden networks, broadcasting beacons with an empty SSID field which makes a directed probe necessary. In practice, various mobile devices broadcast directed probes for each SSID, which is saved in the preferred network list (PNL). In combination with other information from periodical active probes, such as the device MAC address, this can be a serious privacy issue [3].

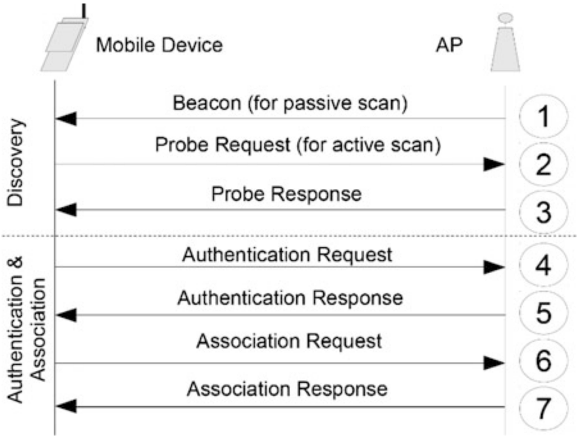

Fig. 42.1 IEEE 802.11 Network Discovery and Association Process

All of the mentioned Wi-Fi management frames can be easily captured by any Wi-Fi card within range which is set into a special monitor mode. Hence, it is very simple to implement this technique on almost any stationary device containing a Wi-Fi interface, e. g., access points, laptops, pcs, etc. The aggregation and analyzation of captured packets in an area of interest is also quite simple, due to the fact that management frames contain the essential information in plain-text, without any encryption. With the usage of advance algorithms in data analytics, one is able to gather useful information from the digital society in a very efficient and easy way. This information can be of high interest for different kind of purposes. Some of these will be presented in the sequel, where we describe scientific and commercial investigations based on captured Wi-Fi data from the digital crowd.

42.3 Wi-Fi Tracking as Emerging Research Field

Due to the increasing percentage of Wi-Fi enabled devices in our digital society, the topic of Wi-Fi tracking has gathered high interest in the scientific world since recent years. Some of the most relevant papers are presented in the following subsections, clustered by the kind of extracted information.

42.3.1 Crowd Data and Social Information

As already mentioned, probe request frames transport different types of management data which can be used to gather some general information about mobile users passing by a Wi-Fi monitor.

For instance, on the basis of the first three Bytes of a captured MAC-address, Barbera et al. [4] determine the manufacturer ID of the sender by performing an OUI – organizationally unique identifier – lookup. One observation of this investigation is the remarkable dominance of Apple devices, which was also detected by our tests at a major German airport [5]. However, these results have to be treated carefully, due to the fact, that Apple devices perform active scans more often, and thus, they might be detected more frequently than other devices.

Beside this, Barbera et al. focus on social relationships in their work and use captured Wi-Fi probes to uncover the social structure of the set of people in the crowd. They determine the similarity of users' context by comparing the SSIDs in the probes and performed a thorough social analysis in terms of social links, user languages, and vendor adoptions in different real-world scenarios.

Cunche et al. [6] also investigate social links based on captured Wi-Fi probes by comparing SSIDs fingerprints using different similarity metrics. On the basis of two large datasets, partly collected with the help of volunteers, the authors conclude that the detection of relationships by analyzing captured Wi-Fi probes is very easy and also a huge privacy risk.

Ruiz-Ruiz et al. [7] present several analysis methods for extracting knowledge from Wi-Fi tracking data. They perform a huge real-world study in a hospital and calculate various features, such as vendor adoptions, arrival and stay times, frequented places, densities, flows, and so on. The authors conclude that they could extract realistic information reflecting real behavior of people in such a complex environment.

42.3.2 Density and Pedestrian Flow Information

The current user density is quite easy to determine by the amount of captured unique devices being within a Wi-Fi monitor's coverage range for a certain time interval. Flow information can then be extracted out of the density information from more than one monitor node supervising an area of interest, as it is schematically illustrated in Fig. 42.2. The pedestrian flow is computed as the amount of people moving one way through this area which can be determined by comparing captured MAC-addresses at all of the installed monitor nodes [5].

Schauer et al. [8] used this procedure and deployed two monitor nodes in the public and security area of an airport divided by a single security check-in counter. With the access to corresponding boarding pass scans, they were able to compare their density and flow estimations with ground truth data. Overall, they determined a strong correlation of 0.75 between the Wi-Fi estimations and the real amount of people passing through the security check.

Fukuzaki et al. [9] claim that pedestrian flow sensing using Wi-Fi monitors is one of the most promising technique for smart cities. They conducted a two-month experiment with 20 Wi-Fi monitors deployed in a shopping mall and determined a coefficient to estimate the number of people. An error rate of 260 persons for weekdays has been achieved.

Li et al. [10] presented a system called *SenseFlow* for monitoring people density and flows based on Wi-Fi tracking data. The system was evaluated in four different application scenarios focusing on various parameters which may have an influence on the tracking accuracy e. g., the device type, the device's operational mode, or the underlying human walking behavior. Overall, the system showed an accuracy of up to 93% in case of Android and 80% for Apple devices in best case.

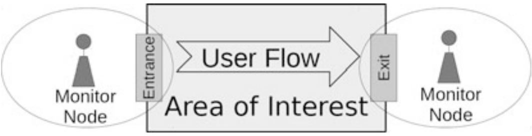

Fig. 42.2 Density and Pedestrian Flow in an Area of Interest

42.3.3 Location and Trajectory Information

One of the most interesting but also very challenging topic in the field of Wi-Fi tracking is the detection and determination of users' current locations and their trajectories. Due to arbitrary probe transmissions form moving mobile devices and significant fluctuations in the Wi-Fi based received signal strengths indicator (RSSI), simple positioning methods are not sufficient for achieving accurate localization results. Bonné et al. [11] confirm this statement claiming that several empirical tests have indicated that the RSSI value is not feasible in crowded environments for tracking the device's location. The authors conducted two large real-world experiments at their university campus and at a music festival.

A more sophisticated solution for tracking complete trajectories of unmodified smartphones is presented by Musa and Eriksson [12]. They used a probabilistic method based on Hidden Markov Model and Viterbi's algorithm and performed real-word experiments on a road network. Their Wi-Fi based trajectory estimations are compared to ground truth data provided by GPS resulting in a mean estimation error of under 70 m.

Chon et al. [13] performed a complete urban mobility monitoring project based on Wi-Fi tracking. They used the well-adopted fingerprinting technique and distinguished between stationary and moving users, in order to detect logical and revisited places. Their experiment was conducted with 25 students over a seven week period in Seoul.

Wi-Fi based trajectory estimations for indoor scenarios were also performed by Schauer et al. [14]. They investigated several probabilistic methods and introduced a modification to a common particle filter implementation in order to improve the tracking accuracy and its performance. Overall, a mean error of 11.65 meters for complete trajectories have been achieved indicating that highly accurate localizations of users based on Wi-Fi tracking data remain challenging.

42.3.4 Other Context Information

Beside the mentioned types of extracted information, there is still a lot of research inferring other context information from Wi-Fi tracking data.

For instance, Wang et al. [15] proposed a method for measuring human queues using a single Wi-Fi monitor. Such queues can be found in different business scenarios, such as retail stores, or at state departments. The authors infer typical and significant time spans, e. g., waiting in the queue, being attended, or leaving the queue, just by Wi-Fi signal readings form mobile devices. Their approach was tested within several experiments at different places, such as coffee shops, laboratory, or at an airport, reaching an estimation error of about 5 s for short and normal service times and under 10 s for longer service times.

Another interesting work is introduced by Maier et al. [16] who use Wi-Fi management frames for a privacy-preserving proximity detection for mobile users. The authors use a variation of the well-adopted cosine similarity to measure the degree of spatial closeness of mobile targets listening on probe requests from their environment. The idea behind is, that the collections of Wi-Fi probes in the surrounding of a mobile user depends on both spatial and temporal criteria. If two users capture a similar amount of probes, they can be seen in a spatial closeness at this moment. The results derived from conducted experiments at different scenarios yield to the conclusion, that a short-range and privacy preserving proximity detection is possible when using Wi-Fi tracking data.

Based on the presented scientific works, we conclude that Wi-Fi tracking involves high potentials for analyzing our digital society without requiring any active user participation nor any device or hardware modification. We have shown different aspects of extracting essential information from the crowd which can be very valuable for various use and business cases. Considering the ongoing digitalization with the increasing usage of Wi-Fi enabled devices, this technique becomes even more promising for innovative business cases in the near future.

42.4 Wi-Fi Tracking as Innovative Business Model

We have just demonstrated the potentials of Wi-Fi tracking and the kind of investigations which are performed in an experimental and scientific context. In this section, however, we highlight the business context and show how Wi-Fi tracking can be used economically.

Due to the increased attention of this technique, a lot of smaller and bigger companies exists offering products and special business services based on Wi-Fi tracking. Most customers of such products are retail shop managers who search for adequate analytic tools in order to analyze the behavior of their customers, like it is well-established in online shops. Hence, they require valuable insights about locations, interests, and all interactions of customers inside their shops. In the sequel, we present and compare some of the companies trying to solve this problem by Wi-Fi tracking:

42reports[1] is a Berlin Start-up focusing on Wi-Fi tracking to monitor customers in retail stores. It was founded in December 2012 and bought by DILAX Intelcom GmbH in April 2016. Beside Wi-Fi, they use other sensors, such as cameras and Bluetooth Beacons, and offer both the infrastructure and tools for retail analytics. Their services are divided into three packages and can be used to access different levels of information about customers' behavior and the shop's situation. Hence, shop managers get the possibility to see how their marketing performs and can make data-driven decisions. Some important features from the provided services are listed below:

- Detection and recognition of customers (new and old)
- Counting, frequency and success rates
- Forecasts

[1] https://42reports.com.

- Return of investment (ROI) analyzations
- Dwell times, density and flow information
- Visualization tools for different platforms in responsive design

Another important topic for 42reports is the protection of users' privacy. The start-up claim to be one of the leaders in security and protection of data privacy. Therefore, they perform 256-bit SSL encryption and a MAC-address anonymization for their retail analytic tools. Hence, third parties and shop owners don't get access to real MAC-addresses which belong to personal information (like IP-addresses).

sensalytics[2] provides similar services for retail shops, events and public buildings. Again, they offer different sensors, such as infrared, Wi-Fi, 3D-cameras, and a particular revenue sensor. Their basic concept is to measure all kind of customer and user interactions, in order to provide thorough analyzation possibilities for manager to make operational and strategic decisions. Based on Wi-Fi tracking, sensalytics extract similar information as 42reports, such as dwell times, detection and recognition of visitors, etc. On their website, they specify the counting accuracy between 40 and 70%. Note here, that other Wi-Fi tracking companies do not publish any data about accuracies and precisions of their services. Beside in-store analytics, sensalytics also focus on fairs and events, and offers a solution for human queue analysis which is, unlike to Wang et al. [15], based on 3D-camera sensors. Overall, with the fusion of the named sensors and the proposed software, they give retailers and event managers some of the possibilities which are quite common and well-adopted in e-commerce: the analyzation of customers. In this context, other German business rivals have to be mentioned, such as Infsoft[3], Crosscan[4], or RetailReports[5], providing similar analytic tools and services for retail shops.

Within the European market, walkbase[6] is one of the most famous retail analytics providers. Some of their key partners are IBM, Samsung, or Cisco. Beside the services we already mentioned above, walkbase also provides marketing optimization tools, queue management, passenger flow optimization, and location based services. They claim that "Wi-Fi is the most versatile technology for modern retail analytics". Using Wi-Fi and Bluetooth enabled devices, they even provide indoor positioning for opt-in passengers at travel hubs.

Euclid Analytics[7] is another company from the US using Wi-Fi probes from mobile devices for customer analytics. They offer "three distinct products to meet the needs of retailers, restaurants and malls". Their services include among others: visitor counts, evaluation of marketing campaigns, identifying visitor patterns, analyzation of visitor behavior, and understanding entire customer buying journeys. Like walkbase, Euclid was

[2] https://sensalytics.net/de.
[3] https://www.infsoft.de.
[4] http://crosscan.com/de.
[5] https://www.retailreports.de.
[6] http://www.walkbase.com.
[7] http://euclidanalytics.com.

founded in 2010 and states that it is nowadays “monitoring hundreds of millions of events daily”.

Based on the introduced examples of companies and start-ups from above, one can get an adequate overview of the potentials of Wi-Fi tracking for innovative business models in our digital world where mobile devices are more and more popular. Hence, on the one hand, this technique renders digital analytic tools possible for retailers and offline marketplaces. On the other hand, we have to look carefully on social restrictions, such as users’ privacy, and consider technical changes in the near future which may degrade these potentials and cause negative impacts. Thus, we will discuss these points in the following section.

42.5 Social and Technical Consequences of Wi-Fi Tracking

As we have demonstrated, Wi-Fi tracking combined with big data algorithms creates the ability to track and analyze mobile users without their consent or even awareness. No complex hard- or software is required, and thus, it is very easy for companies or even malicious persons to use this technique for their intents. Hence, anyone who carries a Wi-Fi enabled mobile device risks to be tracked all the time involuntarily. This fact is a major issue for users’ privacy and their implicit rights on personal data.

So what are the consequences for our more and more digitalized society where a stable and fast connection to the Internet is treated as a valuable asset? Sure, the easiest and most effective way is just to disable Wi-Fi interfaces and use more mobile data connections. However, inside huge buildings, e. g., shopping malls, or airports, only Wi-Fi may provide a stable connection. Furthermore, we suppose that only a few people are willing to enable or disable the Wi-Fi adapter several times per day.

Stricter laws and penalties which prohibit passive Wi-Fi sniffing in public spaces would be a political way trying to reduce the risk of being involuntarily analyzed. However, this would probably not prevent malicious persons from sniffing Wi-Fi traffic, and would definitively destroy all the innovative business models we mentioned in the previous section.

Users could also actively remove network names from their PNL which are not going to be used anymore. This would at least decrease the number of SSIDs sent out by probe requests and thus, social profiling becomes more difficult and inaccurate. However, most users never delete their saved networks and furthermore, this method does not protect users from being analyzed by Wi-Fi sniffers.

A more sophisticated and technical method to protect users against efficient Wi-Fi tracking is provided by Apple’s current mobile operating System (iOS 9). Since iOS 8, a mechanism for automatic MAC-address randomization is integrated in the OS which fakes the real hardware identifier of the device. Hence, continuous tracing or recognizing an iOS device by distributed Wi-Fi sniffers becomes more difficult. When Apple introduced this feature in 2014, it was hardly criticized as impractical, due to the fact that the new randomization process only worked for devices which entered into full sleep mode which was only in case of both disabled cellular data connection and disabled location services [17]. Hence, most users didn't really had MAC-randomization activated in their daily life. Thus, Apple recently improved and extended the mechanism to location and auto-join scans, meaning that MAC randomization is now available also for active devices and during IEEE 802.11 active scans [18]. Note, that the randomization process is not activated for associated devices.

So for the first time, Apple as one of the leading providers for mobile devices, has established an automatic method for protecting users' privacy against Wi-Fi sniffing which is directly integrated in the operating system. However, MAC-randomization makes Wi-Fi based analyzations more complicate, but it doesn't fulfill a complete privacy protection, as it is stated in [19]. Furthermore, Pang et al. [20] have already demonstrated in 2007 that so-called implicit identifiers and certain characteristics of 802.11 traffic can be used to identify many users with high accuracy and without knowing the device specific MAC-address. Hence, Apple's mechanism is just a first but also important step to react on the needs for complete privacy protection in our digital society. Overall, it has to be observed in the near future, how companies and people deal with this topic and how retail analytics can be performed when Wi-Fi tracking becomes inaccurate due to more sophisticated privacy-preserving mechanisms. Probably, the fairest and best way would always be to ask people for compliance before tracking them.

42.6 Conclusion and Future Impacts

In this book chapter, we have demonstrated the possibilities, risks and limitations of tracking mobile customer devices in our more and more digitalized world. Technical backgrounds to standard IEEE 802.11 Wi-Fi tracking have been described. Furthermore, both scientific and commercial works have been presented focusing on the type of crowd information which can be extracted from Wi-Fi tracking data. It was seen that this technique has gathered a high interest also for innovative business models and shows great potentials for the near future, due to an increasing amount of Wi-Fi capable mobile devices. On the other hand, the technique includes serious risks for users' privacy and people should be aware of the fact, that their phone is sending data without their awareness.

We have also demonstrated, that new privacy-preserving mechanisms are developed and partially integrated in current mobile operating systems. However, they still do not guarantee a complete protection against being tracked in public spaces, due to implicit identifiers. Hence, if users want to be sure they just have to switch off the Wi-Fi interface of their device.

For the near future, we assume that Wi-Fi tracking will even spread in public spaces, due to low cost, more mobile devices, and more sophisticated data mining algorithms. Especially retailers who require similar analytic tools as in online-shops will install such a technique in their business. The highest uncertainty for our prediction will be the prospective user acceptance and the development of more advanced privacy-preserving mechanism. Overall, voluntary tracking of mobile users will always be possible, which is the fairest way in our opinion.

References

1. IEEE Computer Society, "IEEE Std 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 3 Park Avenue, NY 10016-5997, USA, June 2007.
2. S. Lee, M. Kim, S. Kang, K. Lee and I. Jung, "Smart scanning for mobile devices in wlans," *IEEE International Conference on Communications (ICC),* pp. 4960–4964, 2012.
3. J. Lindqvist, T. Aura, G. Danezis, T. Koponen, A. Myllyniemi, j. Mäki and M. Roe, "Privacy-Preserving 802.11 access-point discovery," *Second ACM Conference on Wireless Networks Security,* pp. 123–130, 2009.
4. M. V. Barbera, A. Epasto, A. Mei, V. Perta and J. Stefa, "Signals from the crowd: uncovering social relationships through smartphone probes," in *Proceedings of the 2013 conference on Internet measurement conference*, ACM, 2013, pp. 265–276.
5. L. Schauer and M. Werner, "Analyzing Pedestrian Flows Based on Wi-Fi and Bluetooth Captures," in *EAI Endorsed Transactions on Ubiquitous Environments*, ICTS, 2015.
6. M. Cunche, M. A. Kaafar and R. Boreli, "I know who you will meet this evening! linking wireless devices using wi-fi probe requests," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a*, IEEE, 2012, pp. 1–9.
7. A. Ruiz-Ruiz, H. Blunck, T. Prentow, A. Stisen and M. Kjaergaard, "Analysis methods for extracting knowledge from large-scale WiFi monitoring to inform building facility planning," in *Pervasive Computing and Communications (PerCom), 2014 IEEE International Conference on*, IEEE, 2014, pp. 130–138.
8. L. Schauer, M. Werner and P. Marcus, "Estimating crowd densities and pedestrian flows using wi-fi and bluetooth," in *Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, ICST, 2014, pp. 171–177.
9. Y. Fukuzaki, M. Mochizuki, K. Murao and N. Nishio, "Statistical analysis of actual number of pedestrians for Wi-Fi packet-based pedestrian flow sensing," in *Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers*, ACM, 2015, pp. 1519–1526.
10. K. Li, C. Yuen, S. Kanhere, K. Hu, W. Zhang, F. Jiang and X. Liu, "SenseFlow: An Experimental Study for Tracking People," arXiv, 2016.
11. B. Bonné, A. Barzan, P. Quax and W. Lamotte, "WiFiPi: Involuntary tracking of visitors at mass events," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops on a*, IEEE, 2013, pp. 1–6.
12. A. Musa and J. Eriksson, "Tracking unmodified smartphones using wi-fi monitors," in *Proceedings of the 10th ACM conference on embedded network sensor systems*, ACM, 2012, pp. 281–294.
13. Y. Chon, S. Kim, S. Lee, D. Kim, Y. Kim and H. Cha, "Sensing WiFi packets in the air: practicality and implications in urban mobility monitoring," in *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, ACM, 2014, pp. 189–200.

14. L. Schauer, P. Marcus and C. Linnhoff-Popien, “Towards Feasible Wi-Fi based Indoor Tracking Systems Using Probabilistic Methods,” in *Indoor Positioning and Indoor Navigation (IPIN), 2016 International Conference on*, IEEE, 2016.
15. Y. Wang, J. Yang, Y. Chen, H. Liu, M. Gruteser and R. Martin, “Tracking human queues using single-point signal monitoring,” in *Proceedings of the 12th annual international conference on Mobile systems, applications, and services*, ACM, 2014, pp. 42–54.
16. M. Maier, L. Schauer and F. Dorfmeister, “ProbeTags: Privacy-preserving proximity detection using Wi-Fi management frames,” in *Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on*, IEEE, 2015, pp. 756–763.
17. M. Beasley, “More details on how iOS 8’s MAC address randomization feature works (and when it doesn’t),” 9to5mac.com, 26 09 2014. [Online]. Available: http://9to5mac.com/2014/09/26/more-details-on-how-ios-8s-mac-address-randomization-feature-works-and-when-it-doesnt/. [Accessed 29 07 2016].
18. K. Skinner and J. Novak, “Privacy and your app,” in *Apple Worldwide Dev. Conf. (WWDC)*, 2015.
19. M. Vanhoef, C. Matte, M. Cunche, L. Cardoso and F. Piessens, “Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms,” in *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, ACM, 2016, pp. 413–424.
20. J. Pang, B. Greenstein, R. Gummadi, S. Seshan and D. Wetherall, “802.11 user fingerprinting,” in *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, ACM, 2007, pp. 99–110.