Probr – A Generic and Passive WiFi Tracking System

Joel Scheuner, Alessandro De Carli, Genc Mazlami, Sebastian Stephan,
Dominik Schöni, Thomas Bocek, and Burkhard Stiller

University of Zurich, Department of Informatics IFI, Zurich 8050, Switzerland,
{firstname}.{lastname}@uzh.ch|bocek,stiller@ifi.uzh.ch

Abstract. WiFi-enabled devices broadcast a vast amount of data without being associated to an access point. To study and analyze these data, a generic passive Wifi tracking system - Probr - was developed. Probr manages different types of capturing devices and its WiFi packets, processes collected WiFi traces, and visualizes WiFi activities via its Web interface. Probr supports several on-line analysis use cases and is extensible with respect to custom storage solutions to fit further use cases.
A case study conducted demonstrates the capabilities of Probr and shows that passive WiFi tracking is very suitable to provide many insights valuable for use cases in facility management, tourism, security solutions, or a wide range of behavioural research. Thus, possible applications include estimates of a room's utilization, an approximation of the location of a device within a room, a person's daily commuting routines between multiple Probr-equipped locations, and vendor preferences of devices utilized within different people's communities. As an example of exploitation data captured, WiFi traces are analyzed in the case study and respective countermeasures against passive WiFi tracking are presented.

Keywords: WiFi tracking, probe request, room utilization

1 Introduction

Industry as indicated by [16] and research [26,15,17,31,14] have shown interest in collecting and analyzing WiFi traces. Such traces are generated by WiFi-enabled devices even when they are not associated with an Access Point (AP) by capturing probe requests sent for AP discovery. This allows a device to be tracked in a non-intrusive way without installing additional software. The large amount of trackable devices within our daily environment holds a larger potential in revealing interesting patterns about their owners as many people utilize smartphones all day. However, collecting and analyzing such large amounts of data is difficult. Additionally, with the advent of affordable mini computers, such as the Raspberry Pi, potentially many WiFi capturing devices are available nowadays but must be managed by a capable system.

This paper introduces Probr [1], a generic, extensible, and open source system for passive WiFi tracking that supports several on-line analysis use cases. Probr separates device administration and WiFi data analysis into two subsystems called *Probr-Core* and *Probr-Analysis*. Probr-Core supports the configuration of WiFi interfaces, the capturing of WiFi traces, and the collection of results on groups of distributed devices through a graphical Web interface. Probr-Analysis processes and visualizes WiFi traces that are collected with Probr-Core.

While in principle two alternative methods to associate with an AP can be identified, especially AP-initiated WiFi beacons and client device-initiated probe requests, Probr exploits the latter. In the first method, APs periodically announce (*e.g.*, every 100 ms) their presence by broadcasting beacon management frames, which contain network-information such as the supported data rates and the SSID (Service Set Identifier). To detect APs, client devices listen for beacons and reply with WiFi association frames to initiate a connection. Within the second method, client devices actively discover APs by broadcasting WiFi probe requests on potentially multiple channels. Probe requests contain information about the client (*e.g.*, Media Access Control (MAC) address) and the preferred AP (*e.g.*, SSID) with which the client device wishes to associate. Although this work focuses on probe requests, Probr is also able to support capturing any publicly receivable WiFi activities. Instead of dealing with highly sensitive encrypted WiFi packets, the publicly broadcasted probe requests turned out to be sufficient to address the questions posed in the conducted case study. This case study demonstrates the capabilities of Probr and reveals interesting patterns with the following use cases:

U1 *Room utilization*: How many people are in a room at any given time?
U2 *Person tracking*: Is it possible to reproduce the daily routine of a person?
U3 *Device statistics*: Can the data expose differences in communities?

Finally, countermeasures, such as MAC randomization, and its impact on privacy and on the Probr system are discussed, since they tend to be more widespread with the recent efforts by mobile device vendors toward's improved privacy [19].

This paper is organized as follows. Section 2 discusses related work in the fields of active and passive WiFi tracking, existing tools, and privacy concerns regarding WiFi tracking while Section 3 is dedicated to the architecture and design of the Probr system and its components, Section 4 presents a case study where Probr analyzes patterns during a meeting. Section 5 concludes the work and discusses ideas for future work.

2 Related Work

Traces of WiFi activities have been captured and analyzed in research for many years. Many rely on active participation of the device being tracked or on traces being taken from APs. [23] present a first approach employing passive WiFi tracking, thus allowing to capture WiFi packets. This idea was pursued by further research and also lead to the development of tooling for WiFi tracking studies. Collecting and analyzing WiFi traffic raises questions regarding privacy of potential sensitive data. Therefore, related work about privacy in the field of WiFi tracking is discussed at the end of this section.

Active WiFi Tracking – Active or non-passive WiFi tracking relies on active device participation by installing additional software or configuring a device for a specific AP. In 2005, [22] proposed a device localization system called *Place Lab* using different kinds of radio beacons, including beacons from WiFi APs, to overcome limitations of existing systems. In particular, the ubiquitousness of WiFi systems allows for maximized coverage and easy deployment while simultaneously achieving fairly accurate localization results around 20 to 40 meters in urban areas. Similarly, also relying on a custom application installed on the device being localized, [17] reported to have achieved very accurate (*i.e.*, ≈ 3 meters) real-time localization results in their indoor experiment by using a path loss based estimation model. Instead of relying on client-side computation, [30] analyzed WiFi traces from APs to track any object equipped with a WiFi tag. They reported results of similar accuracy (*i.e.*, ≈ 4 meters indoor) compared to [17]. [21] also analyze WiFi traces from APs but their goal was to construct a mobility model focusing on movements of devices among popular regions. [29] visualized campus-wide WiFi activity from AP traces in real time. Also based on WiFi traces from APs, [27] performed indoor density and flow estimation with the goal to support indoor facility planning in large buildings.

Passive WiFi Tracking – In passive WiFi tracking, a capturing device senses and tracks any WiFi traffic within its range. [23] reported to be "the first study of using WiFi transmissions for passive tracking of WiFi clients". They presented a system comprising of common, off-the-shelf WiFi AP hardware that captures probe requests and implements several techniques to prompt devices for additional transmissions in order to obtain more valuable data. The collected data is then used to estimate the trajectory (*i.e.*, spatio-temporal path) of monitored devices. The authors propose a solution based on the Viterbi algorithm and Hidden Markov Model to overcome limitations of simple interpolation based approaches. Although [31] have employed passive WiFi traffic capturing before for tracing movements of mobile users, their scenario was limited to periodic MAC address scans of APs for the purpose of device localization and thus did not include tracking unmodified devices. In a similar way, [18] present a crowdsensing approach by leveraging commodity smartphones and exploiting the natural mobility of people to gather information (*e.g.*, bandwidth distribution) about the existing AP infrastructure in a specific area.

In the following, passive WiFi tracking approaches are discussed that aim towards tracking unmodified mobile devices. [20] perform real-time pedestrian flow analyses in indoor and outdoor environments by collecting and investigating probe requests. [28] focus on classifying human presence into different activity patterns (*e.g.*, engaged or outside). [13] show that probe request traces can reveal insightful information about the social structure and socioeconomic status of device owners. On large-scale datasets, graph-based models were used to derive relationship graphs and were combined with further features such as the owner language guessed from known service set identifiers (SSIDs) or the device vendor inferred from commonly known MAC address prefixes. [14] demonstrate

Table 1: Comparison of WiFi Tracking Tools

	Snoopy [32]	**Mo-Fi [28]**	**CreepyDOL [25]**	**Probr**
Device Administration	No	No	No	Yes
Capturing Client	Python	Python	Ruby	Portable Shell
Signal Types	WiFi, Bluetooth, ANT, ZigBee, GSM/UMTS, NFC, RFID	WiFi	WiFi	WiFi (Extensible via Templates and Plugins)
Data Presentation	Maltego (Data Visualization and Graphing Engine)	Web Interface with Visualizations	Unity (3D Game Engine)	Web Interface with Visualizations
Supported Use Cases	Room Utilization, Device Localization, Device Statistics, Person Tracking, all off-line	Human Presence	Device Localization, Web Traffic Analysis	Room Utilization, Device Localization, Device Statistics, Person Tracking, all on-line
Open Source	Mostly [6]	No	Partially [7]	Yes [8]

a crowdsensing system that captures WiFi packets in the air using the monitor mode of mobile devices. They concluded that crowdsensing can be used for efficient mobility estimation (*i.e.*, coarse-grained device localization) but it is also subject to privacy invasion because surrounding users expose their location without granting any permission.

WiFi Tracking Tools – Several tools for passive WiFi tracking have been proposed in academia and industry. [32] presents a framework called *Snoopy*, developed by the SensePost [2] company, that has been extensively tested and was even deployed in extreme conditions such as aerial surveillance by placing capturing devices onto drones. [28] present a WiFi monitoring and data aggregation system called *Mo-Fi* that was optimized with WiFi channel detection and selection algorithms, and client-side data filtering and compression. In addition to probe messages, *Mo-Fi* also captures data packages to perform frequency analysis. [25] designed a cheap, distributed, and large-scale WiFi tracking system called *CreepyDOL* that was used to collect a comprehensive amount of WiFi of traces (hundreds of gigabytes). In industry, there exist several commercial WiFi tracking solutions. [16] compiled a list of 15 major vendors of WiFi tracking systems including RetailNext[3] which was also mentioned by [32]. In addition, Wilkinson referred to numerous offerings in the military space (*e.g.*, Netline [4], Verint [5]). Table 1 compares Probr with existing WiFi tracking tools.

WiFi Tracking and Privacy – [15] presents a set of attacks aimed towards identifying the association between a person and its WiFi device. He concludes that "any individual equipped with a WiFi enabled device, such as a smartphone, can be easily tracked in its daily life". In addition to summarizing different types of privacy violating WiFi attacks, [24] reported potential countermeasures against these threats. [16] analyzed how companies currently handle privacy policies for WiFi tracking systems and reveal weaknesses in hash-based MAC address anonymization. They criticize the insufficient entropy of MAC addresses, demonstrate brute-force attacks against MAC address hashes to support their claim, and briefly discuss a more secure implementation for anonymizing MAC addresses. Beyond seeking for appropriate MAC address anonymization, [26] show that MAC address pseudonyms are insufficient to prevent WiFi tracking because users can be accurately profiled based on implicit identifiers. Their study on three real WiFi traces have shown that implicit identifiers (*e.g.*, SSID probes, MAC protocol fields, or timing and sizes of Web transfers) were able to track the majority of WiFi devices with high accuracy (90%).

3 The ***Probr*** System

The Probr system is divided into two subsystems: *Probr-Core* and *Probr-Analysis*. Probr-Core is a generic remote device administration system to manage WiFi capturing devices, while Probr-Analysis is an analytical application. Fig. 1 illustrates the interaction between the two subsystems. While Probr-Core writes the collected packets from the capturing devices to the storage, Probr-Analysis accesses this storage to retrieve the raw packet data for analyzing or showing captured data in real-time.

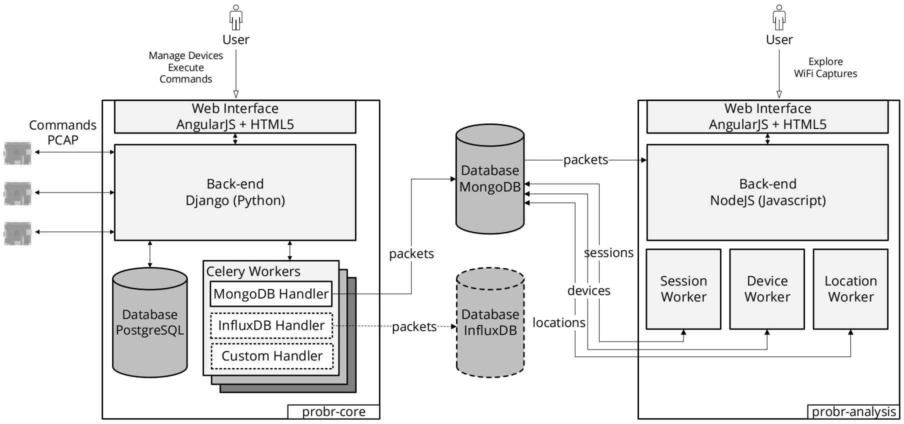
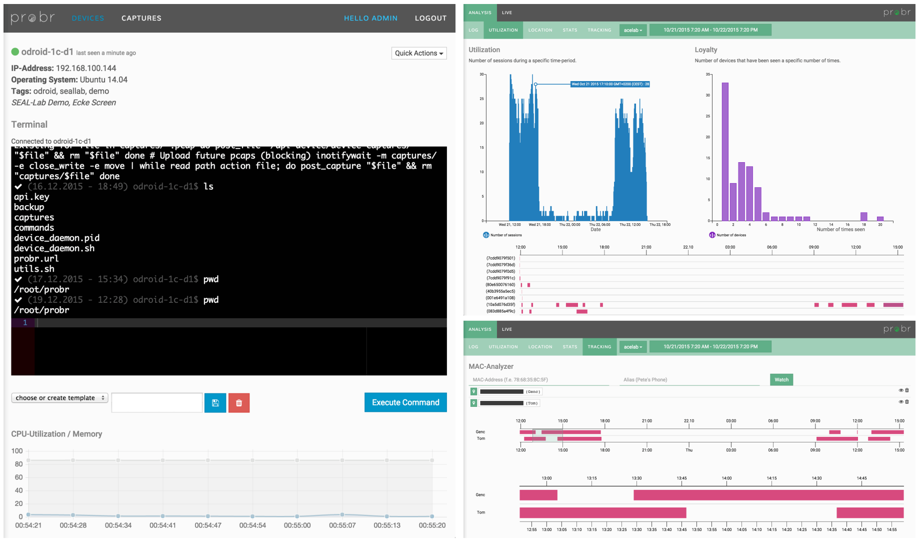


Fig. 1: Architecture Overview

3.1 Probr-Core

Probr-Core consists of a device management Web interface, a back-end service that provides a RESTful API for communicating with capturing devices, and a worker service that stores the data. Probr-Core users can manage (*i.e.*, setup, monitor, remove) devices and execute arbitrary remote commands via the Web interface. The wizard-guided setup to add a new device can be completed by executing a shell command on the device to register. Subsequently, further administration tasks can be accomplished solely via the Web interface. The remote command execution is pull-based and NAT friendly. Fig. 2a shows the view of a managed device with its interactive terminal. Pre-configured command templates for common actions, such as setting a device into monitor mode or starting WiFi capturing, are supported as well. Each managed device continuously runs a shell script in an infinite loop that periodically announces status updates (*i.e.*, CPU and memory usage) to the back-end server and checks for pending remote commands to execute. The shell code is designed to be fault-tolerant regarding erroneous remote commands and the script will automatically recover after rebooting a managed device. Furthermore, the device script is portable across various devices and *NIX flavored operating systems.



odroid-1c-d1 last seen a minute ago
IP-Address: 192.168.100.144
Operating System: Ubuntu 14.04
Tags: odroid, seallab, demo
SEAL-Lab Demo, Ecke Screen

Terminal

Connected to odroid-1c-d1

```
"$file" && rm "$file" done # Upload future pcaps (blocking) inotifywait -m captures/
-e close_write -e move | while read path action file; do post_capture "$file" && rm
"captures/$file" done
✓ (16.12.2015 - 18:49) odroid-1c-d1$ ls
api.key
backup
captures
commands
device_daemon.pid
device_daemon.sh
probr.url
utils.sh
✓ (17.12.2015 - 15:34) odroid-1c-d1$ pwd
/root/probr
✓ (19.12.2015 - 12:28) odroid-1c-d1$ pwd
/root/probr
```

CPU-Utilization / Memory

(a) Probr-Core

(b) Probr-Analysis

Fig. 2: Probr Web Interfaces

The back-end server provides RESTful APIs for the Web interface and capturing devices. It allows capturing devices to announce their status (including CPU and memory usage), retrieve and update remote commands, and submit captured WiFi traces via a *.pcap file. The task of transforming pcap files into a packet representation for a given storage solution is abstracted by the handler interface. New handler implementations for alternative storage solutions can be registered in the application configuration.

3.2 Probr-Analysis

The Probr-Analysis subsystem consists of a visualization Web interface for the user, a back-end that provides a RESTful API for the Web interface, and a set of decoupled workers that process data-intensive workloads asynchronously. Probr-Analysis provides the user with the possibility to browse through the collected packets and query them according to attributes. Probr-Analysis needs to process very high amounts of data in an efficient manner. Thus, the asynchronous workers use techniques such as the MapReduce programming model or the MongoDB aggregation pipeline. The mentioned asynchronous processing tasks work on custom data structures and algorithms, such as the *Session* model. In the following, those concepts will be discussed.

Sessions – A packet represents a single WiFi probe request. It is identified by a UUID and contains the source and destination MAC address, a timestamp, an SSID, the signal strength, a list of Probr-defined tags, and optionally the location (*i.e.*, latitude and longitude) of the capturing device. All these attributes are measured and set in the Probr-Core subsystem and then stored in the connecting database which is accessed by Probr-Analysis.

The use cases **U1** and **U2** depend on the information whether a device with a specified MAC address is present in the monitored area or not. The notion of a *session* defines said presence in a concise manner. It is defined as the time interval that a device with a certain MAC address was present. A session entity contains the MAC address, a start and end timestamp of the interval, the number of packets that contributed to the interval, the duration of the interval, and a list of Probr-defined tags.

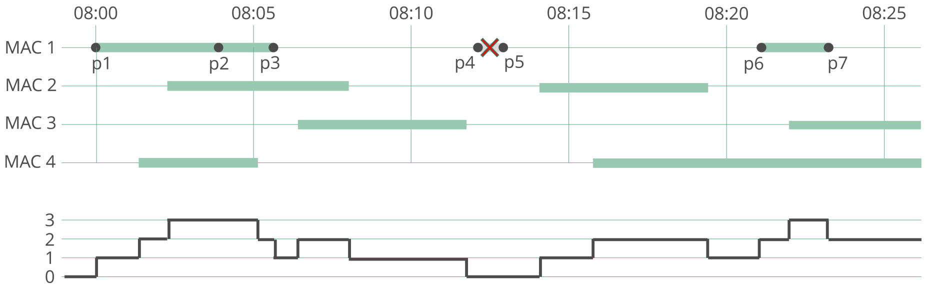
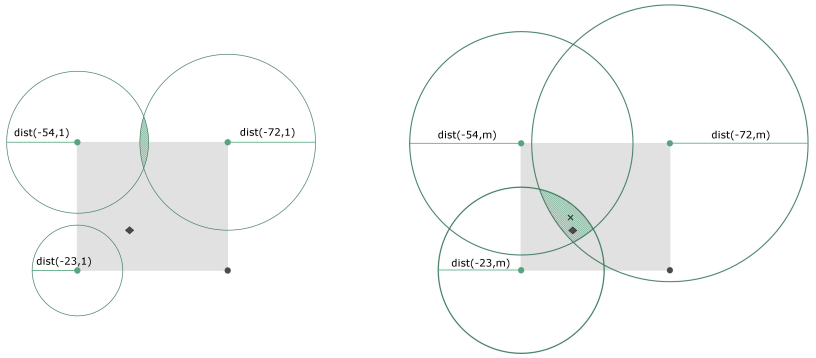


Fig. 3: Example of Session Definition

A session covers multiple packets that originate from the same MAC address and have an inter-packet time of less than 5 minutes (other session times can be configured as well). Fig. 3 illustrates the construction of a session: The packets $p1$, $p2$ and $p3$ belong to the same session because they are less than 5 minutes apart from each other. The next packet $p4$, although from the same MAC address, does not belong to the same session anymore because the time between $p3$ and $p4$ is too long. Packet $p4$ also does not form a session together with $p5$ because the timespan of this candidate session is below a specified threshold. However, $p6$ and $p7$ exceed this timespan threshold and are thus considered as a separate session. Counting the number of overlapping concurrent sessions at all times, as indicated in the lower part of figure 3, directly translates to the number of seen devices at a time in the monitored location.

Multilateration – Probr-Analysis provides a heatmap view, which requires the system to compute geographical locations for the collected data. The location algorithm used in Probr-Analysis is based on the usage of the signal strength as an indicator for the physical distance between the sender device and the receiving capturing devices. [33] derive a relation between the RSSI and the distance for pedestrian location systems, which was slightly adopted to the needs of Probr-Analysis: $dist(r,m) = 10^{\frac{r*m+38.45}{-15.08}}$. The factor r represents the signal strength value, while m was introduced as an additional multiplier during the multilateration process in the algorithm.

The process starts with creating location entries. A location entry contains a list of (location, signal strength) pairs. To reduce noise, packets with signal strengths lower than a certain threshold are ignored. The multilateration algorithm then processes the collection of locations and MAC address. For each raw location in the iteration, multilateration requires signal strength measurements from at least 3 differently placed capturing devices, otherwise it is discarded. This is illustrated in Fig. 4a). The diamond shape (♦) in the Fig. 4 indicates the actual device location. The measured signal strength of the locations from each of the capturing locations is used to compute the radius of the corresponding circle. As indicated in Fig. 4, the algorithm then computes the intersections between all the circles. In some cases, exemplified by Fig. 4a, not all of circles will intersect. As a consequence, the algorithm iteratively increases the multiplier m for all locations, thus proportionally increasing the radius of the circles until there is an intersection of at least 3 circles.



(a) Initial Intersections

(b) Final Trilateration

Fig. 4: Example of Multilateration

The intersection results in a polygon, as indicated by the shaded area in Fig. 4b. The last step computes the centroid of this polygon, indicated by x in Fig. 4b, which leads to the final result for a given MAC address. This information is persisted and available to display the location view. The deviation between the estimated (⧫) and the actual (x) location is caused by interference factors (*e.g.*, reflecting walls or obstacles) that influence the measured signal strength.

Device Identification – For the use case **U3**, MAC addresses are used to identify individual devices and its vendor. The MAC address of each device is specified by the vendor, which in turn is required to register at the IEEE Standards Registration Authority [9]. A MAC address is composed of a 3 Byte Organizationally Unique Identifier (OUI) which identifies the vendor and another 3 Byte long Network Interface Controller (NIC) specific identifier. This enables Probr-Analysis to query the vendor for each of the captured devices found in the packet data.

4 Case Study

For the case study, a 2 days lasting experiment was conducted in a meeting room ($\approx 35\ m^2$) at UZH during a scientific project meeting attended by 20 to 25 people. The capturing devices were ODROID-C1 [10] single-board computers equipped with the standard OROID WiFi Module 4 [11]. Probr was used to setup and configure the capturing devices and monitor the room during the experiment. This case study aimed to answer questions with respect to the use cases **U1** (room utilization and localization), **U2** (person tracking), and **U3** (device statistics).

4.1 Room Utilization

Fig. 5 illustrates the Probr utilization estimates compared to the actual number of people present in the room that were manually recorded every 15 minutes during the experiment. The Probr estimates are generally higher (peak at 30 people) than the actual utilization (with a peak at 22 people) due to the fact that Probr reports the number of probing devices which often exceeds the actual number of people. One can explain this divergence with a high percentage of people having more than one WiFi-enabled device in the room (*e.g.*, smartphone and laptop). Outside of meeting hours (*e.g.*, between 18.00 hours and 9.00 hours), Probr overestimated the actual zero utilzation by up to 3 people. This noise is caused by devices that are not tied to any people carrying them such as routers or network printers. However, Probr correctly reflects major changes in room utilization as happened at the end of the first meeting day (18.00 hours) or at lunchtime (12.00 hours) on the second day. Notice the smaller utilization decrease than actual in the latter case due to laptops being left in the room over lunchtime.

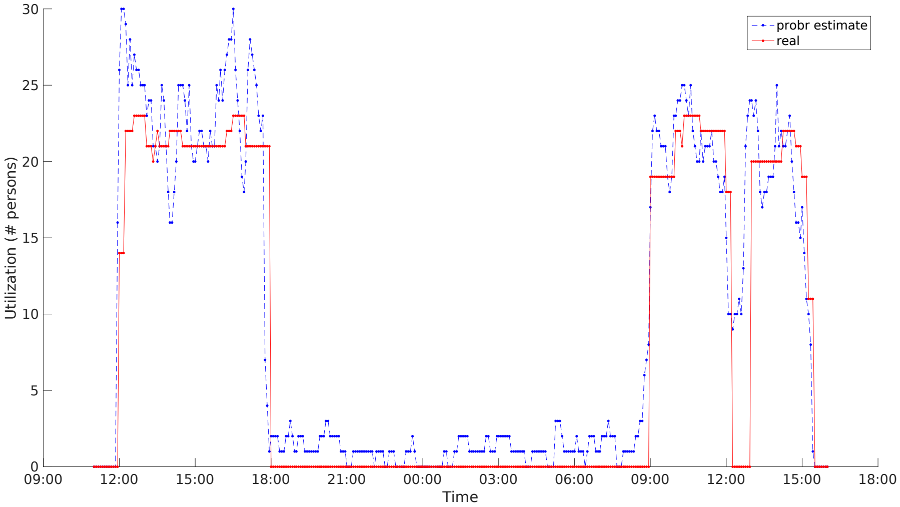


Fig. 5: Room Utilization

4.2 Indoor Localization

Fig. 6 shows the changes in the heatmap for the first day of the case study from 11.30 hours to 18.30 hours. Generally, heatmaps give an indication about where the majority of people were located at that corresponding time within the L-shaped meeting room. The participants of the meeting were located mostly in the upper part of the room, while the lower part was used for coffee breaks which corresponds to the Probr-reported heatmaps.

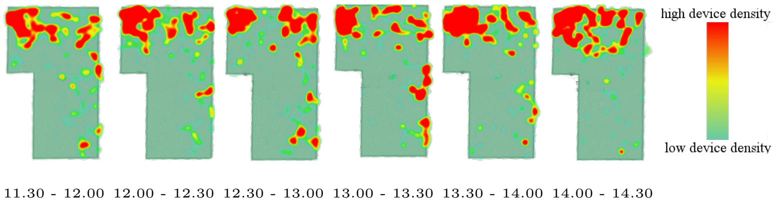


Fig. 6: Sample Localization Results

Accurate localization through multilateration of WiFi signals is difficult due to interference, effects of noise, obstacles, and reflections [17,30]. Probr shows that WiFi-based multilateration as a localization tool works well enough to be able to display the general distribution of people in a room or area. Therefore, a heatmap representation was chosen in order to attribute for slight inaccuracies.

4.3 Person Tracking

Probr allows to monitor specific MAC addresses which can be used to identify behavioral patterns of specific people across multiple Probr-equipped locations.

To demonstrate this ability, a mobile phone of a Probr team member was selected and his home location and workplace was equipped with capturing devices. Fig. 7 shows a day of monitored WiFi data as produced by Probr-Analysis for the person under surveillance. The green boxes together with the above-noted annotations were added to indicate his real locations. The example shows that the person under surveillance started the day approximately at 6.30 hours. At midday, he left his apartment in Baden and travelled to the university. After the arrival at approximately 13.30 hours, he stayed until 19.00 hours and arrived back home shortly afterwards. During nighttime, no activity has been registered. This matches with our subject's behavior of leaving his phone in airplane mode while asleep.

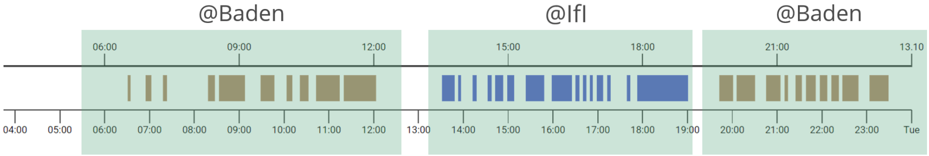
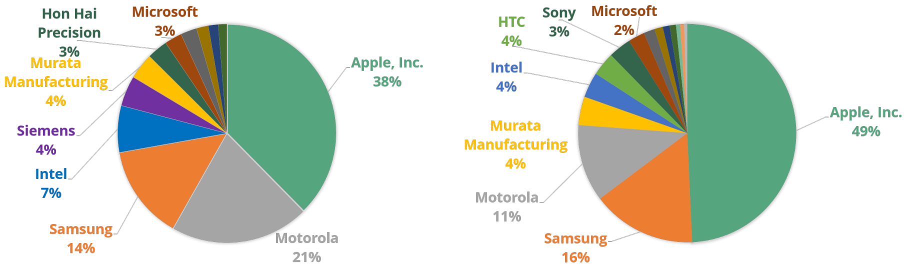


Fig. 7: Example of a Person Tracking

4.4 Device Statistics

To illustrate the differences in communities, we present the device vendor statistics for two data sets: The WiFi data captured during the 2 day use case introduced before (Fig. 8a) and a much larger data set captured during a semester at the IfI of the UZH (Fig. 8b).



(a) Distribution during Case Study

(b) Distribution over 4 Months

Fig. 8: Vendor Distributions

The comparison of both distributions exhibits very clear differences in vendor preferences of the spaces and communities monitored. While Fig. 8b illustrates data from a wider and more heterogeneous community (including students, employees, and professors), the case study community consisted mainly of senior researchers and was hence much more homogeneous (*cf.* Fig. 8a). This leads to clear differences in vendor preferences for the two groups: The case study group shows a lower dominance of *Apple* devices than the general group and a higher concentration of other vendors such as *Motorola* and *Samsung.*

5 Summary, Conclusions, and Future Work

This paper introduced the generic and passive WiFi tracking system Probr, which was designed with the two subsystems Probr-Core and Probr-Analysis. Additionally, a case study was run on the analysis and visualization system Probr-Analysis. Passive WiFi tracking systems are able to reveal information of people who carry WiFi-enabled devices. With the current trends towards IoT, the amount of information is increasing. To handle the large amount of traffic, a scalable architecture for Probr was presented. Based on the conducted case study, this paper concludes that Probr is able to handle the traffic load and is able to display relevant information for several use-cases including **U1** room utilization (Section 4.1-4.2 and Fig. 5-6), **U2** person tracking (Section 4.3 and Fig. 7), and **U3** device statistics (Section 4.4 and Fig. 8).

Besides these insights gained, Probr serves as a representative of passive WiFi tracking systems. Thus, with respect to environmental interferences, noisy devices, and device-specific probing behaviors respective technical concerns may arise. Thus, parameter calibration (such as a session timeout or a cut-off for weak signal) is required when deployed.

To prevent from being tracked, users of WiFi-enabled devices have to turn off WiFi on their devices. Furthermore, vendors have started to introduce MAC randomization to protect the privacy of its users. Probr reported that 51 889 out of the unique 72 652 MAC addresses identified during the 2 day case study originated from MAC randomization. That means that a device uses a random MAC address when scanning for an AP. Thus, for each scan, Probr sees a new device. While this helps to protect the privacy of users, it can be filtered by Probr, as a flag is set in the MAC address indicating a locally administered MAC address as specified by IEEE 802. While vendors have to follow this standard, additional tools such as Pry-Fi [12] can be used to generate true random MAC addresses and spam the Probr system. Furthermore, Pry-Fi also can change the MAC address for each new WiFi connection, offering a good privacy protection.

In the future, it is expected that device vendors continue their efforts in developing countermeasures against privacy leaks exploitable by passive WiFi tracking systems such as Probr. Therefore, Probr will consider alternative identification methods, such as device fingerprinting (as shown in [26]). Probe request sequence numbers can be used to re-identify devices that employ MAC randomization [19]. An additional challenge in capturing systems that rely on probe requests is the variance of probing frequency and behaviour among different devices [19]. To tackle these challenges, future work will extend the scope of WiFi capturing, which is currently limited to probe requests.

Acknowledgments – This work was partially supported by the FLAMINGO project funded under the EU FP7 Program (Contract Nr. FP7-2012-ICT-318488).

References

1. http://probr.ch/, last visited: Jan 2016
2. http://www.sensepost.com/, last visited: Jan 2016
3. http://retailnext.net/, last visited: Jan 2016
4. http://www.netlinetech.com/, last visited: Jan 2016
5. http://www.verint.com/, last visited: Jan 2016
6. https://github.com/sensepost/snoopy-ng, last visited: Jan 2016
7. https://github.com/ussjoin/reticle, last visited: Jan 2016
8. https://github.com/probr, last visited: Jan 2016
9. http://standards-oui.ieee.org/oui.txt, last visited: Jan 2016
10. http://www.hardkernel.com/main/products/prdt_info.php?g_code=G141578608433, last visited: Jan 2016
11. http://www.hardkernel.com/main/products/prdt_info.php?g_code=G141630348024, last visited: Jan 2016
12. https://play.google.com/store/apps/details?id=eu.chainfire.pryfi&hl=en, last visited: Jan 2016
13. M.V.Barbera, A.Epasto, A.Mei, V.C.Perta, J.Stefa: Signals from the Crowd: Uncovering Social Relationships Through Smartphone Probes. Proceedings of the Conference on Internet Measurement Conference (IMC'13). pp. 265–276 (2013), http://doi.acm.org/10.1145/2504730.2504742
14. Y.Chon, S.Kim, S.Lee, D.Kim, Y.Kim, H.Cha: Sensing WiFi Packets in the Air: Practicality and Implications in Urban Mobility Monitoring. ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp'14) pp. 189–200 (2014), http://doi.acm.org/10.1145/2632048.2636066
15. M.Cunche: I know your MAC Address: Targeted Tracking of Individual using Wi-Fi. Journal of Computer Virology and Hacking Techniques 10(4), 219–227 (2014), http://dx.doi.org/10.1007/s11416-013-0196-1
16. L.Demir, M.Cunche, C.Lauradoux: Analysing the Privacy Policies of Wi-Fi Trackers. Workshop on Physical Analytics pp. 39–44 (2014), http://doi.acm.org/10.1145/2611264.2611266
17. M.Emery, M.Denko: IEEE 802.11 WLAN Based Real-Time Location Tracking in Indoor and Outdoor Environments. Canadian Conference on Electrical and Computer Engineering (CCECE'07) pp. 1062–1065 (April 2007), http://dx.doi.org/10.1109/CCECE.2007.271
18. A.Farshad, M.Marina, F.Garcia: Urban WiFi Characterization via Mobile Crowdsensing. IEEE Network Operations and Management Symposium (NOMS'14) pp. 1–9 (May 2014), http://dx.doi.org/10.1109/NOMS.2014.6838233
19. J.Freudiger: How Talkative is Your Mobile Device?: An Experimental Study of Wi-Fi Probe Requests. 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec'15) pp. 8:1–8:6 (2015), http://doi.acm.org/10.1145/2766498.2766517
20. Y.Fukuzaki, M.Mochizuki, K.Murao, N.Nishio: A Pedestrian Flow Analysis System Using Wi-Fi Packet Sensors to a Real Environment. ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (UbiComp'14 Adjunct) pp. 721–730 (2014), http://doi.acm.org/10.1145/2638728.2641312
21. M.Kim, D.Kotz, S.Kim: Extracting a Mobility Model from Real User Traces. 25th IEEE International Conference on Computer Communications (INFOCOM'06) pp. 1–13 (April 2006), http://dx.doi.org/10.1109/INFOCOM.2006.173

22. A.LaMarca, Y.Chawathe, S.Consolvo, J.Hightower, I.Smith, J.Scott, T.Sohn, J.Howard, J.Hughes, F.Potter, J.Tabert, P.Powledge, G.Borriello, B.Schilit: Place Lab: Device Positioning Using Radio Beacons in the Wild. H.W.Gellersen, R.Want, A.Schmidt (eds.) Pervasive Computing, Lecture Notes in Computer Science, Vol. 3468, pp. 116–133. Springer Berlin Heidelberg (2005), http://dx.doi.org/10.1007/11428572_8
23. A.B.M.Musa, J.Eriksson: Tracking Unmodified Smartphones Using Wi-fi Monitors. 10th ACM Conference on Embedded Network Sensor Systems (SenSys'12) pp. 281–294 (2012), http://doi.acm.org/10.1145/2426656.2426685
24. P.Najafi, A.Georgiou, D.Shachneva, I.Vlavianos: Privacy Leaks from Wi-Fi Probing. Report of the MSc Information Security course at University College London (2014)
25. B.O'Connor: CreepyDOL: Cheap, Distributed Stalking. Technical Paper by Malice Afterthought, Inc (June 2013)
26. J.Pang, B.Greenstein, R.Gummadi, S.Seshan, D.Wetherall: 802.11 User Fingerprinting. 13th Annual ACM International Conference on Mobile Computing and Networking (MobiCom'07) pp. 99–110 (2007), http://doi.acm.org/10.1145/1287853.1287866
27. T.S.Prentow, A.J.Ruiz-Ruiz, H.Blunck, A.Stisen, M.B.Kjærgaard: Spatio-temporal Facility Utilization Analysis from Exhaustive WiFi Monitoring. 12th IEEE International Conference on Pervasive and Mobile Computing (PerCom'14) pp. 305–316 (2015), http://www.sciencedirect.com/science/article/pii/S1574119214001953
28. W.Qin, J.Zhang, B.Li, H.Zhu, Y.Sun: Mo-Fi: Discovering Human Presence Activity with Smartphones Using Non-intrusive Wi-Fi Sniffers. 10th IEEE International Conference on High Performance Computing and Communications (HPCC'13) pp. 2143–2150 (Nov 2013), http://dx.doi.org/10.1109/HPCC.and.EUC.2013.307
29. A.Sevtsuk, S.Huang, F.Calabrese, C.Ratti: Mapping the MIT Campus in Real Time using WiFi. Handbook of Research on Urban Informatics: The Practice and Promise of the Real-Time City pp. 326–336 (2009)
30. N.K.Vinh, T.Q.Long, N.A.Viet, D.M.Tien, V.P.Hau, T.de Souza-Daw, T.Dang, L.H.Ngoc, T.M.Hoang, N.T.Dzung: Efficient Tracking of Industrial Equipments using a Wi-Fi based Localization System. International Conference of Soft Computing and Pattern Recognition (SoCPaR'13). pp. 129–133 (Dec 2013), http://dx.doi.org/10.1109/SOCPAR.2013.7054114
31. L.Vu, K.Nahrstedt, S.Retika, I.Gupta: Joint Bluetooth/Wifi Scanning Framework for Characterizing and Leveraging People Movement in University Campus. 13th ACM International Conference on Modeling, Analysis, and Simulation of Wireless and Mobile Systems (MSWIM'10) pp. 257–265 (2010), http://doi.acm.org/10.1145/1868521.1868563
32. G.Wilkinson: Digital Terrestrial Tracking: The Future of Surveillance. DEFCON 22 (2014)
33. Z.Xu, K.Sandrasegaran, X.Kong, X.Zhu, J.Zhao, B.Hu, C.C.Lin: Pedestrain Monitoring System using Wi-Fi Technology and RSSI based Localization. International Journal of Wireless & Mobile Networks (IJWMN) 5(4) (Aug 2013), http://dx.doi.org/10.5121/ijwmn.2013.5402