Probr – A Generic and Passive WiFi Tracking System

Joel Scheuner, Genc Mazlami, Dominik Schöni, Sebastian Stephan, Alessandro De Carli,
Thomas Bocek, and Burkhard Stiller
Communication Systems Group CSG, Department of Informatics IfI, University of Zurich
CH-8050 Zurich, Switzerland
Email: {firstname}.{lastname}@uzh.ch

***Abstract*—WiFi-enabled devices broadcast a vast amount of data without being associated to any access points. To study and analyze this data, a generic passive WiFi tracking system called *Probr* was developed. Probr manages various types of WiFi capturing devices, collects captured WiFi traces, 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. Thus, Probr is the first system of that kind known, enabling full device administration and provided completely as Open Source.**

A case study conducted demonstrates the capabilities of Probr for use cases such as room utilization estimation, indoor device localization, tracking a person's presence between multiple Probr-equipped locations, and analysis of device vendor preferences.

I. Introduction

Industry, as indicated by [19], and research [29], [18], [20], [34], [17] 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). 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 *Device localization*: Where are devices located in a room?
U3 *Person tracking*: Is it possible to reproduce the daily routine of a person?
U4 *Device statistics*: Can the data expose device vendor preferences for different communities?

This paper is structured as follows: Section II discusses related work. Section III is dedicated to the architecture and design of the Probr system and its components. Section IV presents a case study where Probr analyzes patterns during a meeting. Finally, Section V draws conclusions and depicts future steps of relevance.

II. 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. A first passive WiFi tracking approach was presented in [26], which allowed to capture WiFi packets from any WiFi-enabled device. 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

 The definitive Version of Record was published in *2016 IEEE 41st Conference on Local Computer Networks (LCN), November 7–10, 2016, Dubai, United Arab Emirates*, https://doi.org/10.1109/LCN.2016.30

work about privacy in the field of WiFi tracking is discussed at the end of this section.

1) 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, [25] 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 ubiquity 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, [20] reported to have achieved very accurate (*i.e.*, $\approx$ 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, [33] analyzed WiFi traces from APs to track any object equipped with a WiFi tag. They reported results of similar accuracy (*i.e.*, $\approx$ 4 meters indoor) compared to [20]. WiFi traces from APs were analyzed in [24] but their goal was to construct a mobility model focusing on movements of devices among popular regions. [32] visualized campus-wide WiFi activity from AP traces in real time. Also based on WiFi traces from APs, [30] performed indoor density and flow estimation with the goal to support indoor facility planning in large buildings.

2) Passive WiFi Tracking: In passive WiFi tracking, a capturing device senses and tracks any WiFi traffic within its range. [26] 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 [34] 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, [21] 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. [23] performed real-time pedestrian flow analyses in indoor and outdoor environments by collecting and investigating probe requests. [31] focused on classifying human presence into different activity patterns (*e.g.*, engaged or outside). [16] showed 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. [17] demonstrated 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.

3) WiFi Tracking Tools: Several tools for passive WiFi tracking have been proposed in academia and industry. [35] presented a framework called *Snoopy*, developed by the Sense-Post [2] company, that has been extensively tested and was even deployed in extreme conditions such as aerial surveillance by placing capturing devices onto drones. [31] presented 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 other WiFi traffic to perform frequency analysis. [28] designed a cheap, distributed, and large-scale WiFi tracking system called *CreepyDOL* that was used to collect a comprehensive amount of WiFi traces (hundreds of gigabytes). In industry, there exist several commercial WiFi tracking solutions. [19] compiled a list of 15 major vendors of WiFi tracking systems including RetailNext [3] which was also mentioned by [35]. In addition, Wilkinson referred to numerous offerings in the military space (*e.g.*, Netline [4], Verint [5]).

Table I compares Probr with existing WiFi tracking tools using the following 5 dimensions. Device administration supports custom commands via its interactive terminal which makes Probr flexible to capture other signal types beyond WiFi and very suitable to perform ad-hoc experiments and scale them to larger studies. The capturing client is designed to run on minimal infrastructure, such as BusyBox [6], aiming to support a wide range of capturing devices without the need to setup additional runtime environments. The data presentation of Probr excels with a real-time Web interface that allows for flexible packet querying which includes user-definable tags in order to logically structure individual experiments. All supported use cases of Probr are available on-line, which means that analyses do not need to be triggered manually (*i.e.*, off-line) but instead are performed incrementally and the results are presented timely to the user. The Probr system is fully open source and available on Github [1].

4) WiFi Tracking and Privacy: A set of attacks aiming towards identifying the association between a person and its WiFi device were presented in [18]. He concluded 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, potential countermeasures against these threats were reported in [27]. An analysis how companies currently handle privacy policies for WiFi tracking systems was conducted in [19]. Additionally, they revealed weaknesses in hash-

TABLE I: Comparison of WiFi Tracking Tools

	Snoopy [35]	Mo-Fi [31]	CreepyDOL [28]	Probr
Device Administration	No	No	No	Yes
Capturing Client	Python	Python	Ruby	Portable Shell
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 [7]	No	Partially [8]	Yes [9]

based MAC address anonymization, demonstrated brute-force attacks against MAC address hashes, and briefly discussed a more secure implementation for anonymizing MAC addresses. However, MAC address pseudonyms are insufficient to prevent WiFi tracking because the majority of users (65%) can be profiled with high accuracy (90%) based on implicit identifiers (*e.g.*, SSID probes, MAC protocol fields, or timing and sizes of Web transfers) as studied in [29].

III. 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.

A. 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 to support distributed capturing across various networking topologies (*e.g.*, devices behind NAT). Furthermore, all device-server communication is secured via HTTPS and per device API key authentication. 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.

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 in order to attribute for different needs of various use cases (*e.g.*, InfluxDB [10] for time series analysis).

B. Probr-Analysis

The Probr-Analysis subsystem consists of a visualization Web interface for the user, a back-end providing a RESTful API for the Web interface, and a set of decoupled workers that process data-intensive workloads asynchronously. The user can browse and query collected packets, view utilization graphs (Fig. 2b top), explore the location heatmap (Fig. 6), view vendor device statistics (Fig. 8), and track persons based on their MAC address (Fig. 2b bottom). In the following, the foundations of the session-based utilization model, the signal strength-based localization process, and MAC address-based device identification will be presented.

1) Sessions: The notion of *sessions* defines device presence within a monitored area in a superior way than simple MAC address counting. Sessions are much less susceptible to overestimate device presence compared to simply counting the number of distinct source MAC addresses from observed WiFi packets. A session is defined as the time interval wherein a device with a certain MAC address was present. It is stored as a session entity that 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.

A packet represents a single WiFi probe request. It is identified by a UUID and contains the source MAC address, 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.

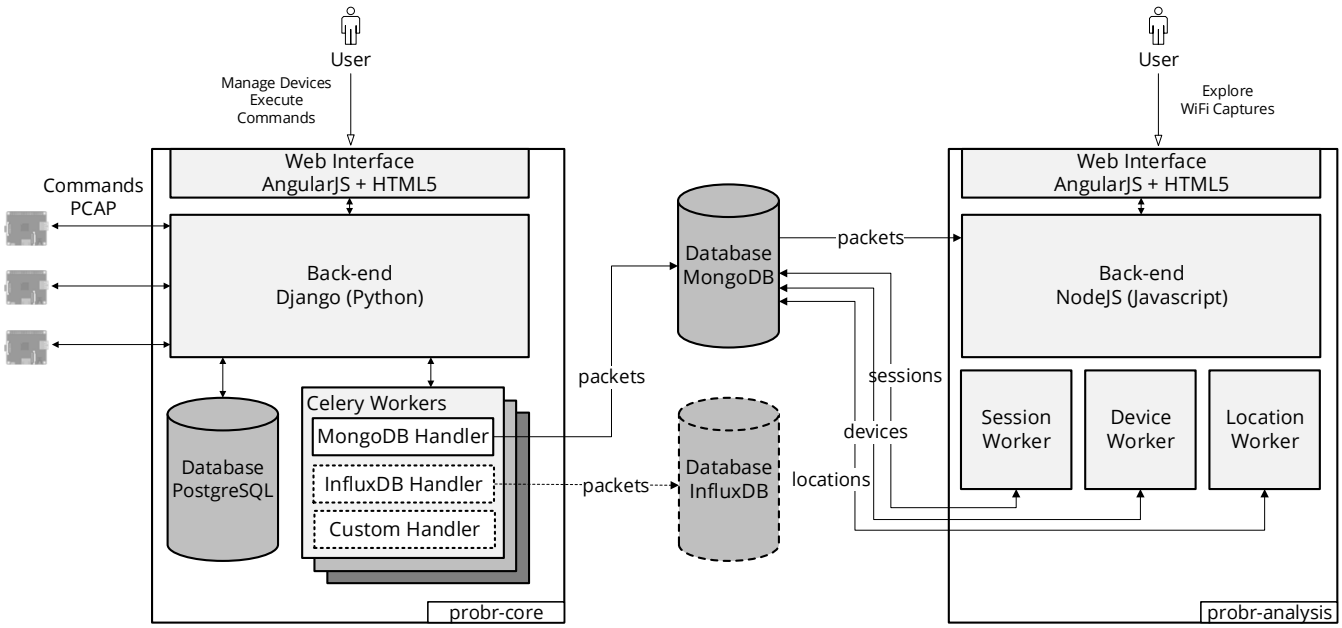
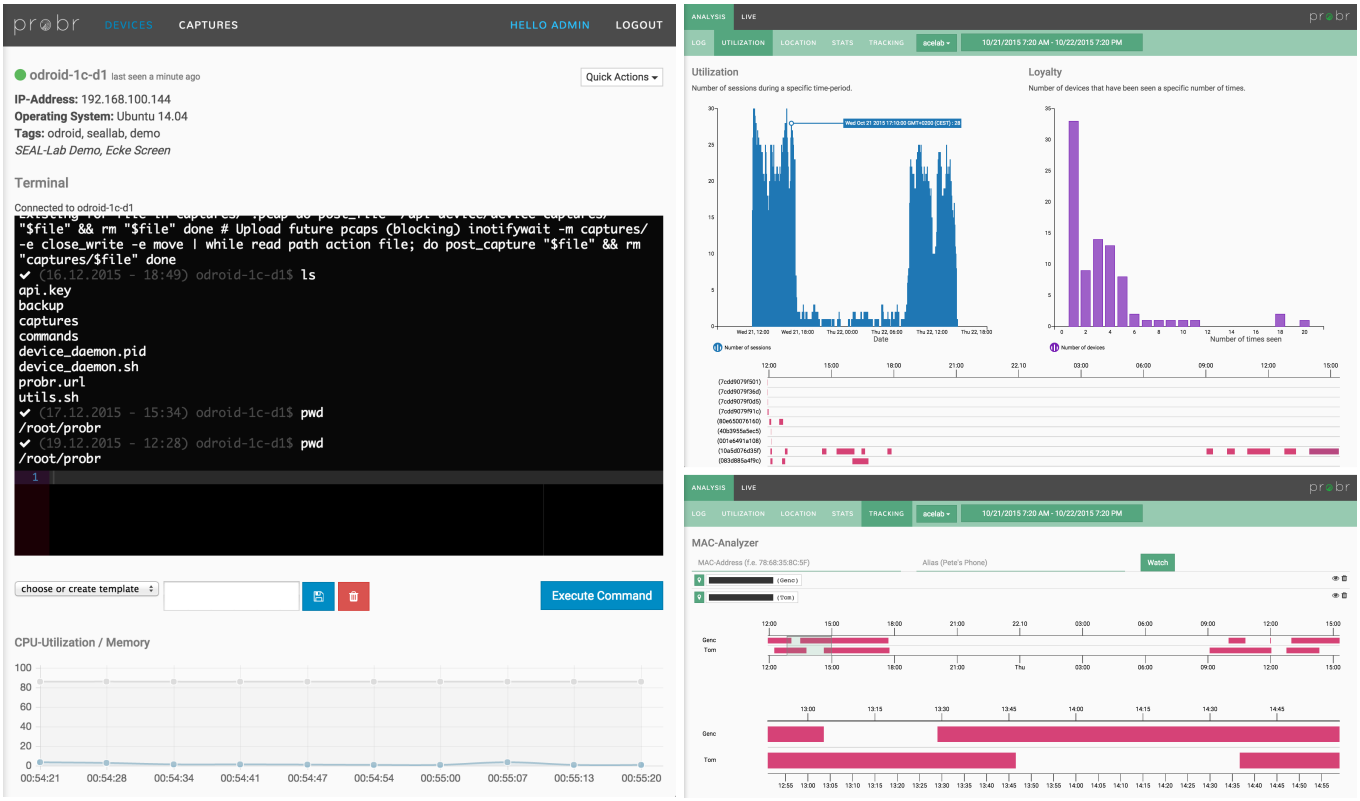


Fig. 1: Architecture Overview



(a) Probr-Core

(b) Probr-Analysis

Fig. 2: Probr Web Interfaces

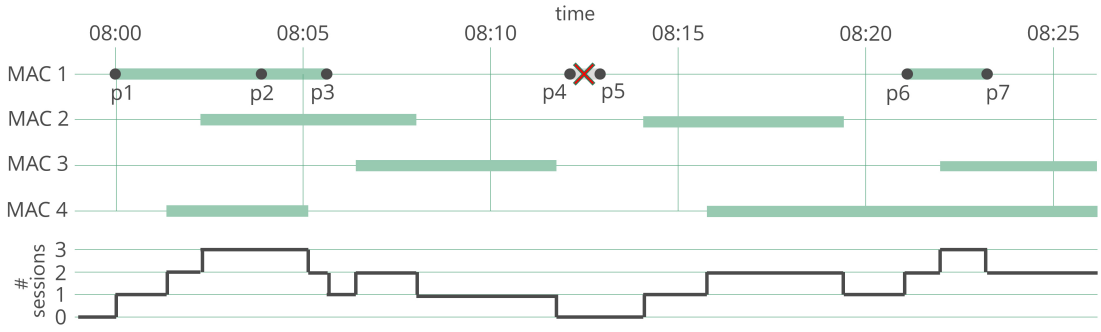


Fig. 3: Example of Session Definition

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 the specified threshold of 1 minute. This minimum threshold for session duration prevents that devices just passing by a capturing device are considered being present at this location. However, $p6$ and $p7$ exceed this timespan threshold, are more than 5 minutes apart from $p3$, 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 Fig. 3, directly translates to the number of seen devices at a time in the monitored location.

2) Localization Process: Probr-Analysis leverages the MapReduce programming model and asynchronous worker model to analyze captured WiFi packets and derive location estimates for each sender device identified. The Map function emits the location of the capturing device together with the received signal strength indicator (RSSI) for each WiFi packet that satisfies a specific noise reduction threshold (e.g., $RSSI > -60$). The emitted value is identified by a composite key consisting of the packet's MAC address and a timestamp rounded off to the nearest minute. Subsequently, the Reduce function pairs each location with its RSSI value for the same MAC address per minute. Multiple observations for the same location are combined by averaging their RSSI values. The resulting list of location-RSSI pairs per MAC address per minute is then persisted into an intermediate MongoDB collection. For each of these entries, a worker job incrementally computes a location estimate using multilateration.

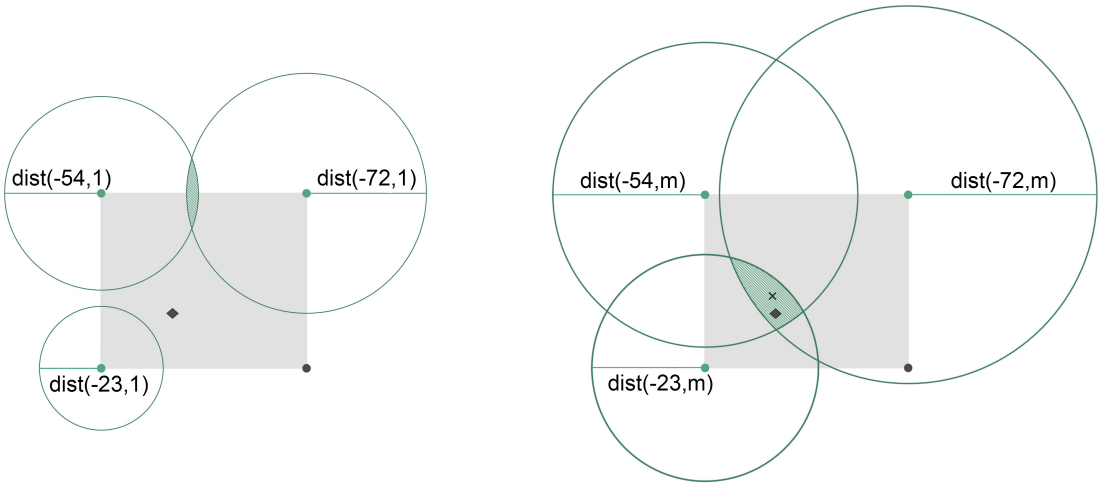
The proportional growth multilateration algorithm takes the RSSI as an indicator of the physical distance between the sender device and the capturing device to obtain a location estimate for the sender device. The formula expressing the general relationship between RSSI and physical distance (1), experimentally derived in [36], was adjusted slightly to the incremental nature of Probr-Analysis (2) by introducing the additional multiplier m. As starting with m=1 might be insufficient to achieve at least three intersecting circles (Fig. 4a), the algorithm exponentially increases m for all RSSI values (resulting in larger circles) until the three smallest circles intersect (Fig. 4b). Notice that a larger circle represents weaker signal strength, indicating that the sender device (depicted by the diamond ⬥) is located further away from a capturing device (green bullet •). The centroid (cross ×) of the intersection area (hatched area) constitutes the final location estimate. The deviation between the estimated (×) and the actual (⬥) sender location is caused by interference factors such as obstacles or reflecting walls that influence the measured RSSI.

$$RSSI = -15.08 * log(dist) - 38.45 \tag{1}$$

$$dist(RSSI, m) = 10^{\left(\frac{RSSI*m+38.45}{-15.08}\right)} \tag{2}$$

3) Device Identification: MAC addresses are used to identify individual devices and their 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 [11]. 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.

Device vendors have started to introduce MAC address randomization to protect the privacy of their users. Such a device uses a random MAC address when scanning for APs. Thus, for each scan, Probr sees a new device. Therefore, Probr automatically detects and ignores such device candidates caused by MAC address randomization. This is achieved by inspecting a flag, specified by IEEE 802 [15], in the MAC address that indicates whether an address is administered universally or locally (i.e., randomized). 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.



(a) Initial Intersections

(b) Final Trilateration

Fig. 4: Example of Multilateration

IV. Case Study

For the case study, a 2 days 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 [13] single-board computers equipped with the standard ODROID WiFi Module 4 [14]. Probr was used to setup and configure 6 capturing devices placed in the room's corners and monitor the room during the experiment. In total, Probr captured over 200 000 probe requests originating from 1 705 unique MAC addresses out of which 371 could be attributed to MAC randomization. This case study answers the questions with respect to the use cases **U1** (room utilization), **U2** (device localization), **U3** (person tracking), and **U4** (device statistics).

A. 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 utilization 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. On the contrary, a cause for under-estimated utilization is the sleep mode of devices that suppresses WiFi activity. 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.

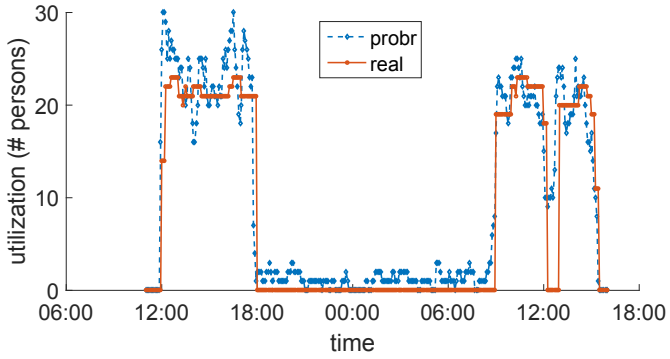


Fig. 5: Room Utilization

B. Indoor Localization

Fig. 6 shows the changes in the heatmaps for the first day of the case study from 11.30 hours to 14.00 hours. These 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.

Accurate localization through multilateration of WiFi signals is difficult due to interference, effects of noise, obstacles, and reflections [20], [33]. 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 (*e.g.*, some device locations were reported slightly outside the room as illustrated by the second heatmap in Fig 6). A limitation of the study setup is that exact position recording of each device was not feasible and thus quantitative analysis of the localization accuracy will be part of future work.

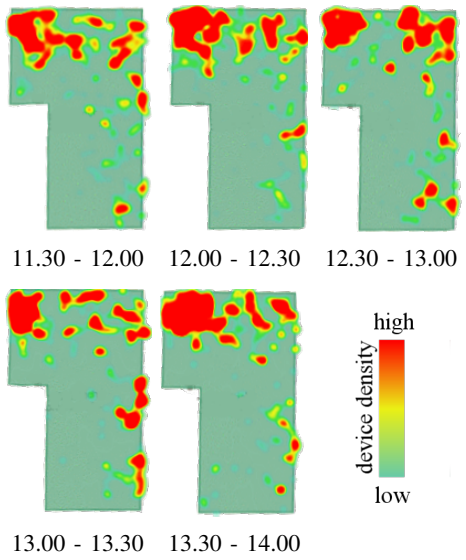


Fig. 6: Sample Localization Results

C. 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 home and traveled 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.

D. 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 30 GB data set of continuous operation over 4 months including almost 30 million probe requests that were captured within a student lab at the IfI of the UZH (Fig. 8b).

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*.

V. Summary, Conclusions, and Future Work

This paper introduced the generic, real-time, and passive WiFi tracking system Probr, which was designed with the two subsystems Probr-Core and Probr-Analysis. To our best knowledge, Probr is the first passive WiFi tracking system that supports real-time use cases, full device administration, and that is provided completely as Open Source. It has been shown how existing localization techniques were adapted to work with incremental MapReduce resulting in the proportional growth multilateration algorithm. Additionally, the case study demonstrated that Probr is able to display relevant information for several use cases including:

U1 *Room utilization*: Section IV-A and Fig. 5
U2 *Device localization*: Section IV-B and Fig. 6
U3 *Person tracking*: Section IV-C and Fig. 7
U4 *Device statistics*: Section IV-D and Fig. 8

Probr was able to estimate a room's utilization tolerating slight overestimation **U1**, present a room's heatmap indicating the device density distribution **U2**, track specific MAC addresses across multiple Probr-equipped locations **U3**, and reveal differences in vendor distributions between communities **U4**.

The generic operational capabilities might be limited due to environmental interferences, noisy devices, and device-specific probing behaviors. Therefore, parameter calibration, such as the session timeout or the cut-off for weak signal strength, can be required when deployed.

To prevent from being tracked, users of WiFi-enabled devices have to turn off WiFi on their devices or setup intrusive tools, such as Pry-Fi [12], for active protection. These cumbersome countermeasures raise the need for alternative protection mechanisms against passive WiFi tracking systems. In the future, it is expected that device vendors continue their efforts in developing preventive measures against privacy leaks exploitable by passive WiFi tracking systems such as Probr. Therefore, Probr will consider alternative identification methods such as device fingerprinting shown in [29] or device re-identification based on probe request sequence numbers [22]. An additional challenge in capturing systems that rely on probe requests is the variance of probing frequency and behaviour among different devices [22]. To tackle these challenges, future work will extend the scope of WiFi capturing, which is currently limited to probe requests.

Acknowledgment

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: Aug 2016
[2] https://www.sensepost.com/, last visited: April 2016
[3] http://retailnext.net/, last visited: April 2016
[4] http://www.netlinetech.com/, last visited: April 2016
[5] http://www.verint.com/, last visited: April 2016
[6] https://www.busybox.net/, last visited: April 2016
[7] https://github.com/sensepost/snoopy-ng, last visited: Aug 2016
[8] https://github.com/ussjoin/reticle, last visited: Aug 2016
[9] https://github.com/probr, last visited: Aug 2016

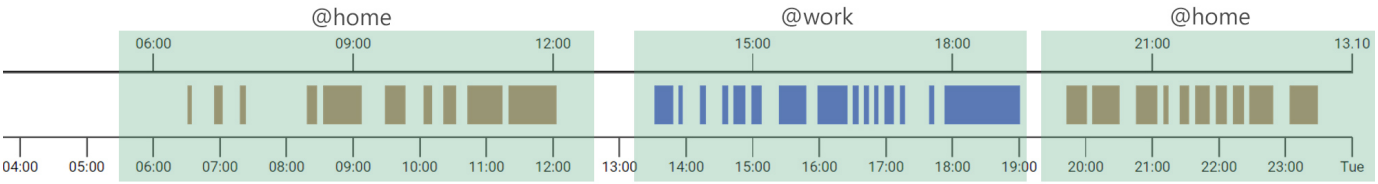
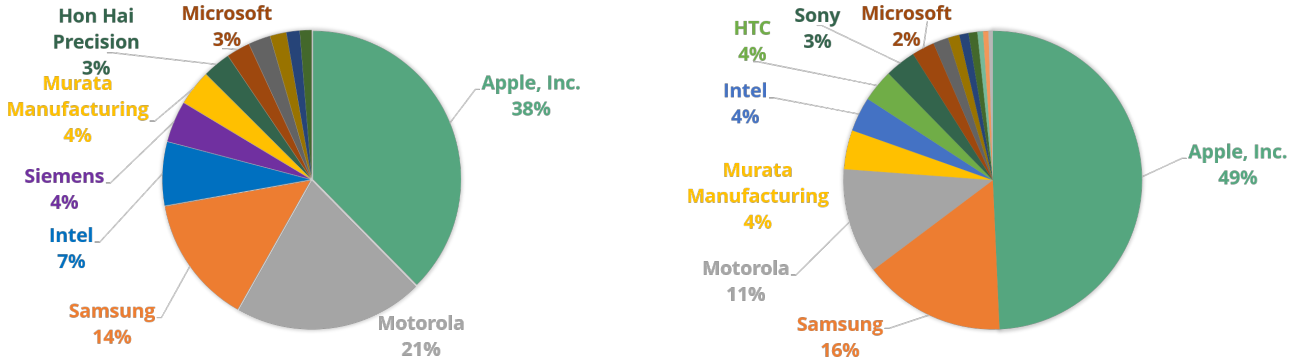


Fig. 7: Example of a Person Tracking



(a) Distribution during Case Study

(b) Distribution over 4 Months

Fig. 8: Vendor Distributions

[10] https://influxdata.com/, last visited: April 2016

[11] http://standards-oui.ieee.org/oui.txt, last visited: April 2016

[12] https://play.google.com/store/apps/details?id=eu.chainfire.pryfi&hl=en, last visited: April 2016

[13] http://www.hardkernel.com/main/products/prdt_info.php?g_code=G141578608433, last visited: Aug 2016

[14] http://www.hardkernel.com/main/products/prdt_info.php?g_code=G141630348024, last visited: April 2016

[15] IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture. IEEE Std. 802-2014 (2014)

[16] 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)

[17] 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)

[18] 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)

[19] L.Demir, M.Cunche, C.Lauradoux: Analysing the Privacy Policies of Wi-Fi Trackers. Workshop on Physical Analytics pp. 39–44 (2014)

[20] 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)

[21] 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)

[22] 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)

[23] 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)

[24] 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)

[25] 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)

[26] 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)

[27] 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)

[28] B.O'Connor: CreepyDOL: Cheap, Distributed Stalking. Technical Paper by Malice Afterthought, Inc (June 2013)

[29] 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)

[30] 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)

[31] 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)

[32] 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)

[33] 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)

[34] 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)

[35] G.Wilkinson: Digital Terrestrial Tracking: The Future of Surveillance. DEFCON 22 (2014)

[36] 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), 17–34 (Aug 2013)