HuMAn: Human Movement Analytics via WiFi Probes

Georgios Pipelidis, Nikolaos Tsiamitros, Malte Kessner and Christian Prehofer
Technical University Of Munich,
Faculty of Informatics, Research Group for Software &
Systems Engineering, Munich, Germany

***Abstract*—In this paper, we describe our approach that enables spatial human analytics using WiFi probes. Our approach works as follows: we first set up our beacons in the area. Then, we use our novel localization method, which operates in a smart-phone, to broadcasts probe requests in a high frequency. Our beacons collect these probe requests and relate them to locations, as estimated from our localization method in the smartphone. The combined WiFi probes with locations are then used to generate a radio map and enable tracking even of devices that are not equipped with our smartphone application.**

***Index Terms*—WiFi Probes, Indoor Localization, Indoor Tracking, Indoor Mapping, Movement Analytics.**

I. Introduction

WiFi Probe requests are network packets which are broadcasted periodically by most devices in order to detect nearby Access Points (AP), even when the device is not in active use [13].

*a) **Hypothesis**:* It is natural to assume that each detected device is associated with one person and each device location approximately matches the location of this person, given the fact that smartphone users keep their phones within arm's reach for 58% of the time [3]. Hence, using WiFi probes we could potentially monitor the movement of humans even in indoor places.

*b) **Motivation**:* Today, there is a tremendous effort on tracking smartphones, since they can provide location information related to phone owners that can enable crowd dynamics monitoring.

*c) **Goal**:* Usually, WiFi sniffers are installed at the entrance of a place and aim to provide information about visitors entering and leaving this place. Our goal is to provide a more sophisticated approach, where multiple sniffers will be placed in various locations indoors, and they will be used to acquire the precise location of the source from an incoming probe.

*d) **Novelty**:* Our approach has several advantages over other technologies, since it provides low battery consumption, low cost, passive monitoring capabilities and widespread presence of contributing WiFi chipsets [10]. Additionally, to our knowledge, our approach is the only approach able to provide precise localization using WiFi sniffers and the only approach that uses this information to localize users.

*e) **Potential Impact**:* The WiFi probing based monitoring approach can enable energy savings in smart buildings, for example by dynamically scheduling Heating, Ventilation, and Air Conditioning (HVAC) activity based on real-time occupancy levels at different areas [2]. Additionally, it can provide benefits for public transport by enabling scheduling based on measured occupancy levels [9] and for smart traffic guidance systems by considering real-time traffic density on the road [5]. Moreover, search and Rescue operations would be facilitated by the automatic localization of persons in need [12], [1]. Finally, following our approach the indoor navigation industry could be bootstrapped, since there would be a clear economic motivation behind analytics of human motion in areas such as malls or airports, where consumers interact with products.

*f) **Contribution**:* The contribution of this paper can be summarized as follows: (1) We provide a method that enables WiFi probe request sniffing with off-the-shelf Internet of Things (IoT) devices. (2) We provide a novel approach for aggregating data sensed from multiple devices and use them to precisely localize smartphones. (3) We use those devices to enable localization on the user side and encourage their use for indoor navigation.

II. Related work

Barbera et. al. [11] use WiFi probes following an exploratory approach, attempting to identify the crowd dynamics as well as whether this process can be automated. Hong et. al. [6], use WiFi probes for detecting traces of people in museums. However, they do not perform localization but rather they infer trajectories through presence sensing. Finally, Hu et. al. [7], provide a study of the implications WiFI probes have at the energy consumption and throughput on both phones and access points, in small and large scale environments. They provide several thoughts on balancing WiFi discovery speed and ultra-dense network interactions.

978-1-5386-9151-9/19/$31.00 ©2019 IEEE

III. Approach

Our approach can be described in four simple steps, as can be seen in Figure 1: (1) The first step is to setup infrastructure and **Collect Data** that is going to be used in (2) for training our model in order to **Enable Localization**. Once our localization model has been trained, we are able to (3) provide more precise localization, which is going to boost the localization accuracy, via the enhancement of the data collection process and due to the increase of precision of the collected information. Finally, we (4) **Provide Analytics**, which implies that location pattens of users can be now revealed.

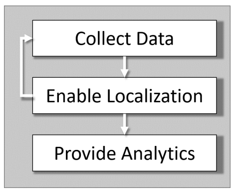

Fig. 1: General Architecture of our System.

A. Collect Data

As a first step of our approach, we set up infrastructure in the space. Our beacon devices have approximately 70m range, while the ideal distance between each device is approximately 10m, since the signal, strength attenuation follows a logarithmic curve, and longer distance would increase the localization uncertainty. Once all of the devices have been set up, the data collection process is executed with the help of a smartphone application. As can be seen at the bottom of Figure 2, the smartphone is equipped with our localization method, which operates following a novel particle filter approach that enables the fusion between the Inertial Motion Unit (IMU) sensor of the smartphone and a map of the indoor place.

B. Train the Localization Model

Once everything is in place and location data have been collected with the help of our smartphone application, the Unique User IDentifier (UUID) of the smartphone is used to filter the only dataset tagged with precise location. At this step, we generate histograms, as can be seen at the top of Figure 2, which contain the Received Signal Strength (RSS) that each IoT device senses from the smartphone. Once each histogram has been generated for every location estimated at the previous step, we cluster this data using the K-Nearest Neighbores algorithm and the Elbow method [8], in an attempt to identify the optimum number of clusters in the space. Once the optimum number of clusters is identified, we label the data and use it to train our localization algorithm and enable localization predictions.

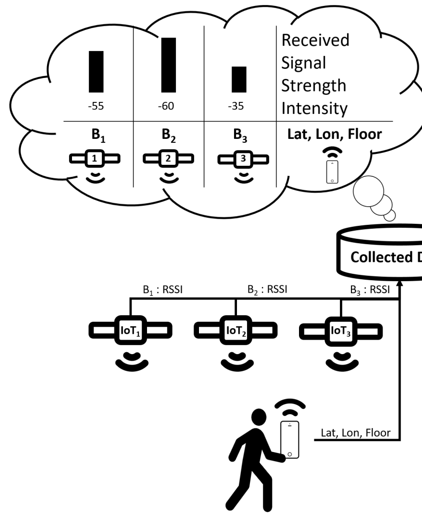

Fig. 2: An example of the data collection and the training process.

C. Enhance Localization Precision

At this step, the initial localization model is used to enhance the localization process in a Simultaneously Localization And Mapping (SLAM)-like approach [4]. This step, aims to introduce a higher precision localization and acts as enabler for collecting more precise data and hence improve the analytics procedure.

D. Provide Analytics

At this step, users' positions are marked on the map in real time, while they are moving freely around the space. Each user's walking pattern is presented in the context of a heatmap, where dark red areas indicate the most visited places and light red areas the less visited ones. The user can interact with the data having the possibility to visualize individual routes or a selected group of routes.

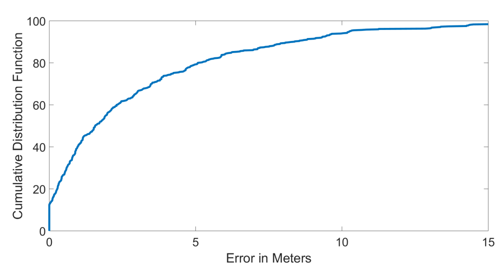

Fig. 3: Localization Results.

IV. Localization Results

We have evaluated our framework in an office space building. We used 8 beacons in a $65.1m^2$ space. The average distance between each beacon was 7.5m. The error was estimated following the Accumulated Distribution Function, as can be seen in Figure 3, our median error is 1.56m, the 75^{th} percentile is 4.22, while the 95^{th} percentile is 10.25m.

V. Demo Case

During our demo we will enable complete indoor navigation to smartphone users via our application, similar to Figure 4.(a). More specifically, we will enable the users to be routed from and to destination at the conference venue and be localized on their way.

(a) (b)

Fig. 4: Indoor Navigation Demo Case.

Additionally, we will equip the place with our beacon devices that will be used for tracking user locations. The users will be able to watch in real time, traces of people inside the venue, while they will be able to watch clusters being formed in real time, similar to Figure 4.(b).

VI. Discussion

WiFi probes have caused a lot of discussion recently, since capturing probe requests is completely passive and hence it does not require any user cooperation. Device owners have no means of noticing that they are being tracked. As a result, lawyers, authorities, and the population tend to take a skeptical position [7]. In 2013 a network of publicly placed bins was banned from the city of London after it was revealed that the bins recorded probe requests of pedestrians walking by [16]. Back then the British media labeled the setup as a legal 'grey area'. In fact, a respective network of scanners would enable the operator to create extensive movement profiles without the people's consent. However, on the devices' side, tracking can be prevented by changing its MAC address periodically and randomly. A device can for instance use a different randomly generated source address for every probe request sent, making it impossible to relate two captured probe requests to the same device when just considering the source address. Most developers of WiFi drivers have adopted address randomization by now. However, none of the major manufacturers use it in a persistent manner, allowing devices to broadcast their identity on a frequent basis. In addition, various studies investigating the effectiveness of address randomization were able to identify regularities in the timing of probe requests, making it still possible to relate frames with different addresses to the same device.

References

[1] V. Acuna, A. Kumbhar, E. Vattapparamban, F. Rajabli, and I. Guvenc. Localization of wifi devices using probe requests captured at unmanned aerial vehicles. In *Wireless Communications and Networking Conference (WCNC), 2017 IEEE*, pages 1–6. IEEE, 2017.

[2] Y. Agarwal, B. Balaji, R. Gupta, J. Lyles, M. Wei, and T. Weng. Occupancy-driven energy management for smart building automation. In *Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building*, pages 1–6. ACM, 2010.

[3] A. K. Dey, K. Wac, D. Ferreira, K. Tassini, J.-H. Hong, and J. Ramos. Getting closer: an empirical investigation of the proximity of user to their smart phones. In *Proceedings of the 13th international conference on Ubiquitous computing*, pages 163–172. ACM, 2011.

[4] H. Durrant-Whyte and T. Bailey. Simultaneous localization and mapping: part i. *IEEE robotics & automation magazine*, 13(2):99–110, 2006.

[5] P. Fuxjaeger, S. Ruehrup, T. Paulin, and B. Rainer. Towards privacy-preserving wi-fi monitoring for road traffic analysis. *IEEE Intell. Transport. Syst. Mag.*, 8(3):63–74, 2016.

[6] H. Hong, G. D. De Silva, and M. C. Chan. Crowdprobe: Non-invasive crowd monitoring with wi-fi probe. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(3):115, 2018.

[7] X. Hu, L. Song, D. Van Bruggen, and A. Striegel. Is there wifi yet?: How aggressive probe requests deteriorate energy and throughput. In *Proceedings of the 2015 Internet Measurement Conference*, pages 317–323. ACM, 2015.

[8] D. J. Ketchen and C. L. Shook. The application of cluster analysis in strategic management research: an analysis and critique. *Strategic management journal*, 17(6):441–458, 1996.

[9] W. Pattanusorn, I. Nilkhamhang, S. Kittipiyakul, K. Ekkachai, and A. Takahashi. Passenger estimation system using wi-fi probe request. In *Information and Communication Technology for Embedded Systems (IC-ICTES), 2016 7th International Conference of*, pages 67–72. IEEE, 2016.

[10] P. Robyns, B. Bonné, P. Quax, and W. Lamotte. Noncooperative 802.11 mac layer fingerprinting and tracking of mobile devices. *Security and Communication Networks*, 2017, 2017.

[11] M. V. Barbera, A. Epasto, A. Mei, V. C. Perta, and J. Stefa. Signals from the crowd: Uncovering social relationships through smartphone probes. pages 265–276, 10 2013.

[12] W. Wang, R. Joshi, A. Kulkarni, W. K. Leong, and B. Leong. Feasibility study of mobile phone wifi detection in aerial search and rescue operations. In *Proceedings of the 4th Asia-Pacific Workshop on Systems*, page 7. ACM, 2013.

[13] G. Wilkinson. Digital terrestrial tracking: The future of surveillance. *DEFCON*, 22, 2014.