Estimating Crowd Densities and Pedestrian Flows Using Wi-Fi and Bluetooth

Lorenz Schauer
Mobile and Distributed
Systems Group
LMU Munich, Germany
lorenz.schauer@ifi.lmu.de

Martin Werner
Mobile and Distributed
Systems Group
LMU Munich, Germany
martin.werner@ifi.lmu.de

Philipp Marcus
Mobile and Distributed
Systems Group
LMU Munich, Germany
philipp.marcus@ifi.lmu.de

ABSTRACT

The rapid deployment of smartphones as all-purpose mobile computing systems has led to a wide adoption of wireless communication systems such as Wi-Fi and Bluetooth in mobile scenarios. Both communication systems leak information to the surroundings during operation. This information has been used for tracking and crowd density estimations in literature. However, an estimation of pedestrian flows has not yet been evaluated with respect to a known ground truth and, thus, a reliable adoption in real world scenarios is rather difficult. With this paper, we fill in this gap. Using ground truth provided by the security check process at a major German airport, we discuss the quality and feasibility of pedestrian flow estimations for both Wi-Fi and Bluetooth captures. We present and evaluate three approaches in order to improve the accuracy in comparison to a naive count of captured MAC addresses. Such counts only showed an impractical Pearson correlation of 0.53 for Bluetooth and 0.61 for Wi-Fi compared to ground truth. The presented extended approaches yield a superior correlation of 0.75 in best case. This indicates a strong correlation and an improvement of accuracy. Given these results, the presented approaches allow for a practical estimation of pedestrian flows.

Categories and Subject Descriptors

C.3 [**Special-purpose and application-based systems**]: Signal processing systems

General Terms

Measurement

Keywords

Crowd density; Pedestrian flow; Tracking; Wi-Fi probes; Bluetooth

1. INTRODUCTION

The organization of pedestrian flows in large public buildings like airports, train stations, shopping malls etc. is a big challenge for people working in these buildings. Systems with information about current crowd densities are able to support the control and management process of pedestrian flows and can reduce travel time and management cost. Such systems can react on the actual needs of the present people, e.g. by closing or opening additional doors, ticket shops, or control gates. Based on automatic flow information, people can be informed about the degree of capacity utilization in the desired destination and certain pedestrian flows can be led through less crowded areas for time-saving reasons. Furthermore, such crowd information is also very interesting and useful for commercial purposes. In oder to obtain this information automatically, optical approaches have been investigated for many years using cameras and image processing techniques, such as [14]. However, these techniques require special additional hardware components and suffer from high implementation cost in order to track people in huge areas. Furthermore, taking pictures or video surveillance of unknown people is always a privacy issue and has to be discussed carefully in certain scenarios [6].

In the last decade, Wi-Fi infrastructures have been widely installed in many public buildings offering Internet and local services to their visitors. With the immense diffusion of modern smartphones and tablets, more and more people use these services with their Wi-Fi enabled mobile device. The increasing usage of Wi-Fi as an ubiquitous communication technology also offers new possibilities to estimate current pedestrian flows without the need for expensive additional hardware installation. Due to the fact, that Wi-Fi enabled devices periodically broadcast certain management frames, an easy and low-cost implementation of monitoring units suffices to passively collect Wi-Fi data from surrounding people. Neither an active user's participation nor any modification of the involved hardware or software is needed. This readily available activity information has been exploited in literature for several purposes, such as locating and tracking people or for density and trajectory estimations.

However, and to the best of our knowledge, an estimation of current pedestrian flows based on Bluetooth and Wi-Fi captures has not been realized in a scenario where a reliable source of ground truth information is available. Thus, as a main contribution, we present a low-cost tracking system for pedestrian flow estimations and investigate its feasibility and

accuracy in detail with a known ground truth in a realistic scenario. Therefore, during a period of 16 days, management frames of both, Bluetooth and Wi-Fi have been collected at two particular monitor nodes inside a major German airport. One monitor node was placed in the public area and another one in the security area separated by a security check involving boarding pass scans. Based on the collected data, we compare the ability of Bluetooth and Wi-Fi for pedestrian flow estimations. Furthermore, we present three different approaches to improve the accuracy towards ground truth in comparison to a naive count of Wi-Fi captures. All approaches are evaluate with the Pearson's correlation indicating the degree of the linear dependence between our estimation and ground truth.

The remainder of this paper is structured as follows: In Section 2 we give a brief overview of current research in this topic. Section 3 presents the proposed methodology and explains the underlying technical properties exploited for detecting devices. The conducted experiment and its evaluation are presented in Section 4. Finally, Section 5 concludes the paper and gives hints on future work.

2. RELATED WORK

Tracking people by Bluetooth or Wi-Fi signals has been discussed previously in literature. Density estimation in crowded mass events has been studied using Bluetooth scans or Wi-Fi from collaborating smartphones inside the crowd [15, 17]. Furthermore, human behavior was extracted from similar data for a concert situation [4, 8]. For the case, that enough devices from the crowd are cooperating, the density and motion of surrounding people has been studied using devices building a Bluetooth ad-hoc network [12].

However, Bluetooth has a short transmission range and most modern smartphones operate Bluetooth in invisible mode per default. Therefore, researcher started to investigate information extracted from Wi-Fi activity and compare it to Bluetooth [1]. The authors sum up that Wi-Fi shows higher benefits for monitoring people, due to shorter discovery time and higher detection rates. According to their results, only five percent of all discovered unique devices at several locations are discovered via Bluetooth and over 90% via Wi-Fi. Several systems concentrating on Wi-Fi have been proposed in literature. Data extracted from Wi-Fi management frames has been used in order to estimate trajectories [11], social relationships [3], waiting times in human queues [16], and in order to calculate density estimations [4].

However, to the best of our knowledge, none of these works present detailed analysis of Bluetooth and Wi-Fi based density and flow estimations in real-life scenarios related to a known ground truth and, hence, an explicit evaluation of the reliability of such estimations is still missing.

3. METHODOLOGY

This section describes the methodology for crowd density and pedestrian flow estimations based on signal captures from unmodified mobile devices. At fist, the following definitions are presented:

Crowd density is defined by the amount of people per unit of area within a certain time interval.

Pedestrian flow is defined as the amount of people moving one way through an area of interest within a certain time interval.

For the detection of a mobile device, it has proven useful to look at the traffic generated from local area network technologies such as Bluetooth and Wi-Fi.

3.1 Bluetooth

Bluetooth is a wireless communication system designed for short range communication and operates in the license-free ISM band. It is defined as IEEE 802.15.1 Bluetooth. The typical range of Bluetooth-enabled smartphones is roughly ten meters. In order to organize Bluetooth connections, an inquiry mode has been defined. Basically, a device which wants to initiate a Bluetooth connection with another device sends out an inquiry packet and other devices listening for them can answer. Most devices only react to such inquiry packets, when made visible by the user through a user interface dialog. The inquiry response frame contains the Bluetooth MAC identifier of the discovered device and can contain additional information including the local name of a device. In order to track devices, the target has to answer inquiries, which has long been the default for phones. Therefore, we expect a specific amount of detectable devices, mainly from older generation.

3.2 Wi-Fi

The wireless local area network technology, commonly known as Wi-Fi, is defined in IEEE 802.11. Its communication range varies from about 35 meters for indoor scenarios to more than 100 meters for outdoor scenarios, depending on the environment, the Wi-Fi transmitter power, and the used 802.11 protocol extension [1]. The standard defines three different classes of frames: Control frames, management frames, and data frames. We focus on management frames, as these are involved in the network discovery and association process and performed by most smartphones in the public.

Wi-Fi discovery consists of two mechanisms: *Passive scanning* in which a mobile device listens for messages from access points advertising their presence. In order to become detectable, access points send out beacon frames roughly every 100 ms. However, these frames are only sent out on the channel, where the access point is operating. Therefore, the client has to listen to different channels in order to find access points passively. In contrast to that, *active scanning* is based on messages sent by the mobile device similar to a Bluetooth inquiry message. These messages are sent out on all channels one after another.

This is the preferred method for mobile devices due to lower energy-consumption and shorter discovery time of access points [9]. Empirical test with different mobile devices show that an active scan is performed at least once within two minutes, despite the case that the test device was associated to an access point or not [4]. Our own experiments with an iPhone 5 and a Galaxy S3 Mini confirm these results on average. Probe request frames contain the MAC address of the sender and, optionally, the SSID of the network of interest. If the frame's SSID field is left blank, all access points should answer the probe request. In practice, various

mobile devices broadcast directed probe requests for each SSID, which is saved in the preferred network list (PNL). In combination with other probe request information, such as the MAC address, which provides a device specific identifier, this common procedure of Wi-Fi active scans leads to serious issues concerning the privacy of mobile users.

In order to address these issues, researchers started to investigate and develop privacy preserving approaches for Wi-Fi, either with minimal modifications to standard 802.11 implementations [10], or as a new protocol version [7]. However, none of these approaches are applied in practice yet. Recently, Apple has integrated a mechanism to randomize the device specific MAC address in their new mobile operating system iOS 8. The purpose of this mechanism is, that it becomes more difficult to clearly recognize a phone by probe request captures and, thus, the privacy of iPhone users gets more preserved. However, only the randomization of MAC addresses does not preserve the user's privacy, due to implicit identifiers, or specific characteristics of Wi-Fi traffic [13]. Furthermore, the actual implementation of Apple's mechanism fails at a rigorous MAC address spoofing in practice, due to several conditions, which are not common in real-life, e.g. the device must be asleep for a long time, which is not given in case of cellular data connectivity [2]. In summary, a mobile device can still reliably be recognized in practice based on captured Wi-Fi active scans. This is the basis for the approaches presented in the subsequent section.

3.3 Approaches

Considering the definitions from above and assuming that a captured unique MAC address belongs to one person, the crowd density of one monitor node's coverage area is estimated by the amount of captured unique devices at the corresponding node during a certain time interval. Furthermore, a pedestrian's movement through an area of interest is measured by capturing the device specific MAC address at different monitor nodes located at the entrances/exits to this area of interest. According to the definition, the pedestrian flow in the desired area of interest is the amount of people moving from one entrance to one exit within a certain time interval. Thus, the pedestrian flow can be estimated by one of the following approaches, which are based on the captures made at one monitor node n_i covering the entrance and another monitor node n_j covering the exit of an area of interest.

3.3.1 Naive Approach

The naive approach just counts the unique MAC addresses which have been captured at both nodes n_i and n_j within a specific time interval t. This simple approach suffers from two major problems: First, the direction of a person's movement cannot be determined, and second, the detection of a device in an overlapping coverage area of monitor nodes is automatically seen as a pedestrian's movement, even if the person is not moving from one area to another. This increases the false-positive rate of the system. In order to overcome these problems, three extensions of this naive approach are presented in the sequel.

3.3.2 Time-based Approach

The time-based approach additionally considers the time when a MAC address was captured at a monitor node for the first or the last time, respectively. Thus, the pedestrian flow between n_i and n_j is expressed as the number of unique MAC addresses in t containing a positive time delay between the last (or first) capture at node n_i and the last (or first) capture at node n_j. Hence, the direction of a person's movement can be determined. However, the number of false positives in case of overlapping coverage areas cannot be completely reduced by this approach. Therefore, an RSSI-based solution is presented.

3.3.3 RSSI-based Approach

This method is an extension of the naive approach taking the received signal strength indication (RSSI) value of captures into account. The pedestrian flow between monitor n_i and monitor n_j is then expressed as the number of unique MAC addresses in t containing at least one capture with an RSSI value over a certain threshold ϵ for both nodes. With a well-chosen threshold, this approach can reduce the false-positives in case of overlapping coverage areas. However, an optimal and absolute RSSI based threshold is hard to find in realistic scenarios, due to the fact, that many factors have significant influences on the RSSI value, such as device characteristics, environmental circumstances or phone positions. Hence, the major issue is to find an adequate value ϵ for each scenario. If ϵ is chosen too small, many captures will not be considered and the false negative rate increases. If ϵ is too large, the problem of overlapping coverage areas is not solved. Furthermore, the direction of the pedestrian flow is hard to determine with a pure RSSI-based method. Therefore, we present a hybrid approach.

3.3.4 Hybrid Approach

The hybrid approach is a combination of the last two methods and considers both the RSSI value and the time when a MAC address was captured. Thus, the pedestrian flow from node n_i to node n_j is expressed as the number of unique MAC addresses in t containing a positive time delay between the nodes and at least one capture with an RSSI value over a certain threshold ϵ for both nodes. Besides the fact that an optimal RSSI based threshold is hard to find, the proposed method provides both the direction of the pedestrian flow and the possibility to reduce the false-positive rate in case of overlapping detection zones.

4. EVALUATION

In this section, a thorough evaluation of the described methodology and the proposed approaches is performed. The underlying data was collected with the following implementation and setup.

4.1 Implementation and Experimental Setup

Two identical and time-synchronized laptops were placed at two different locations at the Munich Airport in order to collect both, Wi-Fi frames and Bluetooth inquiry results. All Wi-Fi management frames excluding 802.11 Beacons (due to unnecessary processing overhead) were captured with a Wi-Fi interface in monitor mode. For Bluetooth measurements, the *BlueZ* stack of the Linux kernel was used performing one inquiry scan per minute in order to avoid negative influences on Wi-Fi transmissions. The corresponding responses including RSSI value, the address and a time stamp were collected.
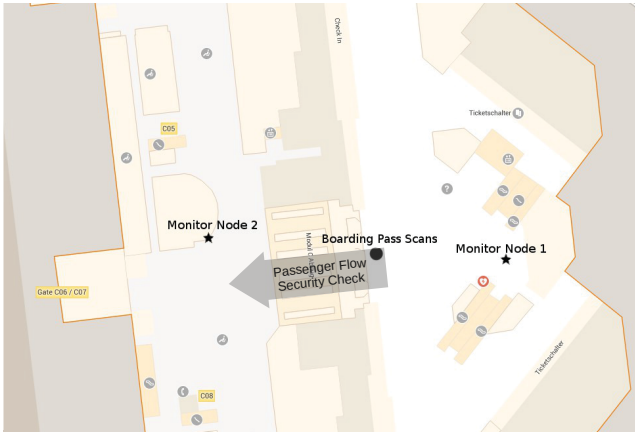
Figure 1: Map[2]of the testbed indicating the passenger flow through the security check, and the locations of monitor nodes, and boarding pass scans

As a reference information, we were given access to the boarding pass scan numbers reflecting the true flow of people through the security check. The experimental setup is shown in Figure 1 and is designed as follows: The first monitor node is installed at an info desk in the public area, located approximately 20 meters in front of the entrance to the mentioned security gate and 10 meters before the boarding pass scans. Thus, this node covers the entrance to the area of interest, which is the area of the security check in this case. The second monitor node is located at the desk of an airport takeaway restaurant in the security area, approximately ten meters behind the exit of the security check. The distance between both monitor nodes is roughly 40 meters. The proposed setup provides the following benefits:

- A minimal usage of additional hardware is required

- A deterministic one way pedestrian flow through the security gate is realized

- Access to ground truth from corresponding boarding pass scans is given

With the proposed implementation and setup, Bluetooth and Wi-Fi signals from passing mobile devices are captured during a 16-day period. Note that these captures include people who do not pass the security check, such as visitors, staff and other persons walking through the coverage areas. Thus, the following subsection firstly presents general crowd information based on the collected data, and then, an overall evaluation of the proposed methodology is given.

4.2 General Information from the Crowd
In general, we observed over 11 million probe requests and 6,600 unique SSIDs in the public and about 8.5 million probes and 4,000 unique SSIDs within the security area. The ratio of directed probes with transmitted SSID was nearly 37% in the public and about 47% in the security area, respectively. On average, we detected 6,211 unique Wi-Fi MAC

---

[2]Source: Google Maps – https://maps.google.de

addresses and 250 unique Bluetooth addresses per day in the public area which leads to a 4% Bluetooth/Wi-Fi ratio. Less traffic was captured within the security area, counting 3,784 unique Wi-Fi and 107 Bluetooth addresses, resulting in a Bluetooth/Wi-Fi detection ratio of 2.8%.

For unique MAC addresses, which were captured during the complete experiment, we perform an Organizationally Unique Identifier (OUI) lookup, indicating the manufacturer of the used Wi-Fi chip. The distributions for the most frequently tracked OUIs in the public area are shown in Figure 2(a) and 2(b) for Bluetooth and Wi-Fi, respectively. The results for the security area show nearly the same distributions.

As expected, newer mobile devices such as iPhones or Samsung phones are seldom detected via Bluetooth. Instead, more models of long established manufactures including Nokia or RIM's BlackBerry are detected by Bluetooth inquiry requests. In case of active Wi-Fi probes, we discover a significant dominance of Apple devices which has also been reported by other studies [3, 11]. In empirical tests, we found out that some Apple devices send out probe requests more often compared to some Android devices. Therefore, this unexpected high fraction of Apple devices is influenced by a higher probability of receiving a probe request in a given period of time. Furthermore, it can also indicate that Android devices have Wi-Fi turned off more often, possibly due to very easy access to the option in the energy management widget.

4.3 Density Estimation
We estimate the crowd density in both areas and for both techniques, separately. In this case, we do not have data representing ground truth. However, we assume that if there is a high frequency of boarding pass readings, we should observe a higher density in the public and security area before and after these readings, respectively. Figure 3 shows our density estimations compared to the frequency of boarding pass readings for a single day as an example of the experiment. In general, it can be observed, that the density of captured unique devices in the public area is higher than in the security area. This is to be expected taking into account that more people move through the public area including visitors.

Besides probe requests, we also take additional association and reassociation requests into account. However, this does not influence the Wi-Fi density estimation significantly. In contrast to Wi-Fi, Bluetooth density underestimates the frequency of boarding pass scans. This is because the quantity of trackable Bluetooth devices is small in comparison to the amount of people.

We also observe a positive time shift between the peaks of Wi-Fi density estimations from the public to the security area during a peak of boarding pass scans. This indicates an adequate result, due to the fact that the building introduced exactly this ordering: Visibility for the first sensor node followed by boarding pass scan and entering the range of the second node, followed by loosing contact to the first and later to the second sensor node.
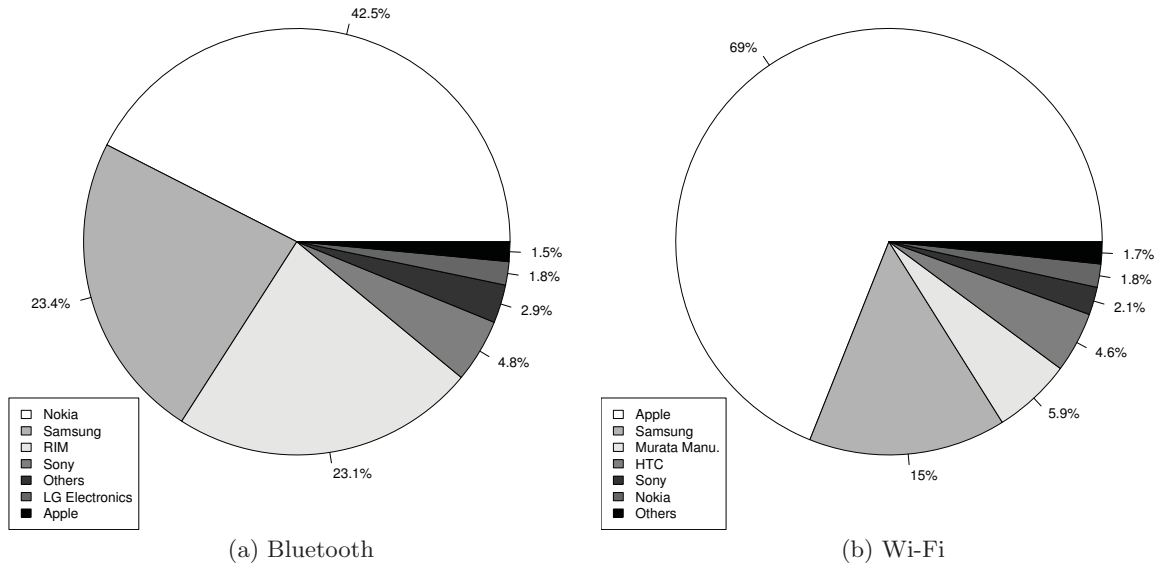
(a) Bluetooth

(b) Wi-Fi

Figure 2: Manufacturer distribution of unique captured devices in the public area
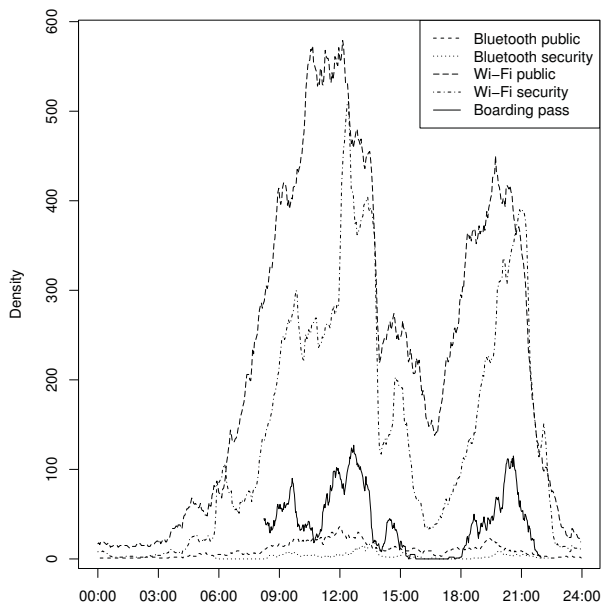

Figure 3: A single day including Wi-Fi, Bluetooth, and boarding pass readings

4.4 Pedestrian Flow Estimation

Based on corresponding boarding pass readings, we analyze the accuracy of our proposed methodology for pedestrian flow estimation. Figure 4 shows the obtained results for Bluetooth and naive Wi-Fi counts in comparison to boarding pass scans for one day of the study. It can be observed that Wi-Fi overestimates and Bluetooth underestimates ground truth. In case of Wi-Fi, this was unexpected, due to the fact that not every passenger carries a Wi-Fi enabled device. Beside the fact, that some airport staff members might be

included in the data and some persons may carry more than one device, we explain this observation by a high number of false-positives, due to the short distance between the monitor nodes which leads to an overlapping zone of both coverage areas. Hence, some Wi-Fi devices have been tracked at both areas without passing the security gate. According to Section 3.3, we evaluate if this effect can be limited by using one of the extended approaches. Figure 5 shows the results for the RSSI and the time based approach indicating an improvement towards ground truth in comparison to the naive method. Note that in case of Bluetooth, these extended approaches have no positive influence, due to the small quantity of captured Bluetooth devices and, hence, we will evaluate them for Wi-Fi based estimations only. It has to be mentioned that the presented estimations generally contain a positive time delay related to ground truth. This is because people scan their boarding pass and need longer time to exit the range of the monitor node of the public area while we consider the last timestamp when a MAC address was seen in the public area for our estimations.

For a more detailed analysis, we determine the Pearson's correlation, which is a widely used measure of the linear dependency between two observations, in our case between the estimation and ground truth. As result, the correlation coefficient r is returned, with $-1 \leq r \leq 1$. Positive values denote positive linear correlation and negative values denote negative linear correlation. The absolute value $|r|$ indicates the strength of the correlation and can be verbally described according to Dancey and Reidy's categorization [5]:

$\|r\| = 0.0$	zero
$0.1 \leq \|r\| \leq 0.3$	weak
$0.4 \leq \|r\| \leq 0.6$	moderate
$0.7 \leq \|r\| \leq 0.9$	strong
$\|r\| = 1.0$	perfect

	Bluetooth	Wi-Fi naive	Wi-Fi RSSI	Wi-Fi time	Wi-Fi hybrid
max	0.73	0.82	0.93	0.93	0.93
average	0.44	0.41	0.56	0.47	0.57

Table 1: Correlation coefficients for each approach based on an optimal time shift
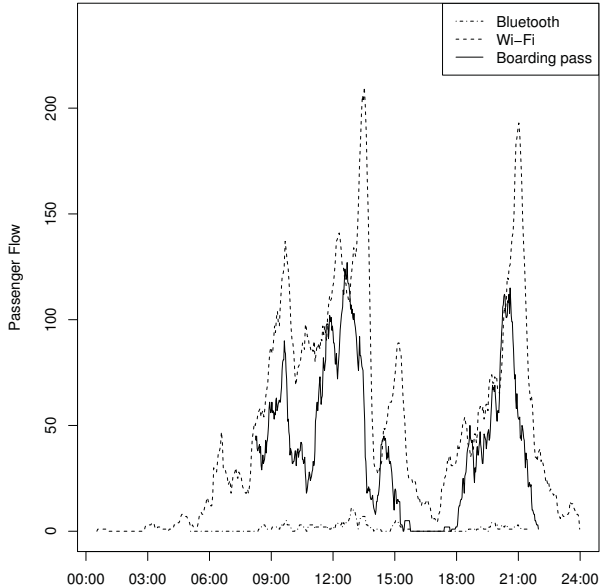

Figure 4: Results of naive Wi-Fi and Bluetooth based pedestrian flow estimations at a single day compared with boarding pass scans

Figure 5: Results of RSSI and time-based Wi-Fi pedestrian flow estimations at a single day compared with boarding pass scans

Due to the positive time delay, we first perform several time-shifts of our estimations and determine the correlation coefficient for each shift. The results for the complete experiment are indicated in Table 1 showing the maximal and average correlation coefficient for each approach based on an optimal time shift related to the average value. As expected, Bluetooth and the naive Wi-Fi based estimations show the lowest correlation, while the extended approaches reach a correlation coefficient of 0.93 in best case. This indicates a good result and shows the improvement of the estimation accuracy in comparison to a naive approach. However, such an adequate correlation cannot be observed for any approach on average, where the highest correlation of 0.57 is reached by the Wi-Fi hybrid method.

In order to improve these results, we investigate our methods for an abbreviated (focused) capturing time, namely from 6.00 to 22.00, when the security gate is open. This is due to the fact that during night, no boarding passes are scanned while some signals from passing mobile devices are captured, leading to a higher false-positive rate. This external information is available in many application scenarios. Again, Table 2 shows the results for the maximal and average correlation coefficient for each approach based on an optimal time shift and a focused estimation. The results indicate that a focused estimation increases the average correlation coefficient for every approach.
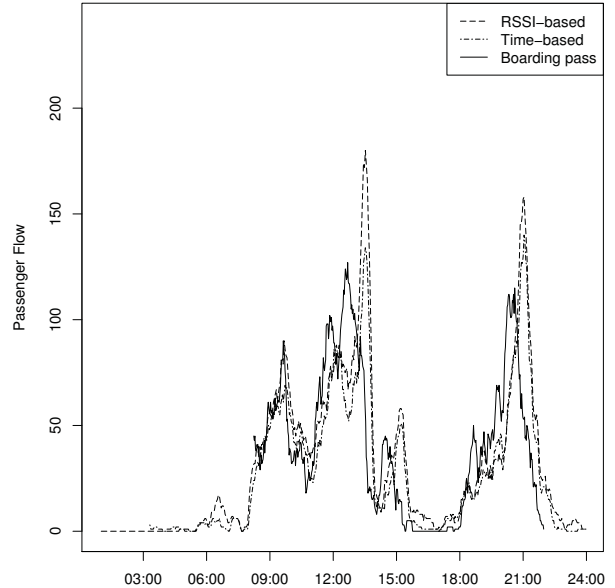
In case of the naive Wi-Fi method, the most significant improvement of about 48% is reached. Due to a higher false-positive rate in case of overlapping monitor ranges, this was expected. In contrast, Bluetooth shows the lowest improvement of only 20% indicating a smaller false-positive rate, due to its short communication range. Furthermore, only a moderate correlation of 0.53 could have been reached on average, due to the small quantity of detected devices. In case of Wi-Fi, the hybrid based method performs best on average showing a strong correlation of 0.75. Furthermore, it can be seen that in comparison to a naive count of captured MAC addresses, the extended methods improve the estimation accuracy of up to 23%. Note that all these results according to Wi-Fi are based on probe request captures only and could not have been improved further by considering additional frames, such as association requests.

5. CONCLUSION AND FUTURE WORK

In this paper, we have investigated the quality and feasibility of pedestrian flow estimations based on Wi-Fi and Bluetooth captures from unmodified mobile devices at a major German airport. Furthermore, we have presented three approaches to improve the accuracy of our Wi-Fi based estimations in comparison to a naive count of MAC addresses often proposed in related work. Based on the performed evaluation, we conclude, that both Bluetooth and Wi-Fi can be used to get approximations about the crowd without the awareness

	Bluetooth	Wi-Fi naive	Wi-Fi RSSI	Wi-Fi time	Wi-Fi hybrid
max	0.79	0.86	0.91	0.91	0.91
average	0.53	0.61	0.74	0.63	0.75

Table 2: Correlation coefficients for each approach based on an optimal time shift and a focused estimation

of its members. In summary, only a fraction of surrounding devices could have been tracked by periodical Bluetooth scans and thus, Bluetooth based estimations are less accurate showing a moderate average correlation to ground truth of only 0.53 in best case. This is not an adequate result for a reliable pedestrian flow estimation system.

In contrast to Bluetooth, Wi-Fi tracking provides a good approximation to crowd densities and pedestrian flows. By using one of the extended approaches, the accuracy of a naive Wi-Fi based estimation could have been improved. With additional information from the application scenario we have reached a strong correlation related to ground truth on average. These results lead to the general conclusion that the presented approaches allow for a practical estimation of pedestrian flows. Furthermore, external sources of information are needed in order to provide a reliable tracking system based on Wi-Fi probes. Even simple information such as the opening times of the security gate help a lot in increasing the average prediction quality. This should be addressed in future work for different external information. It has to be mentioned that the presented results are based on a single realistic scenario. The properties of this specific scenario with respect to communicational and social behavior of users could have influenced the experiment and other environments might have significant differences. Further experiments in other scenarios, e.g shopping malls, or train stations, are required in the future, in order to assess and compare our results. We plan to do so and want to enhance our research efforts in this topic, especially in terms of positioning, trajectory estimation and privacy aspects.

6. REFERENCES

[1] N. Abedi, A. Bhaskar, and E. Chung. Bluetooth and wi-fi mac address based crowd data collection and monitoring: Benefits, challenges and enhancement. In *Australasian Transport Research Forum (ATRF), 36th, Brisbane, Queensland, Australia*, 2013.

[2] N. Arnott. What's really happening with ios 8 mac address randomization? `http://www.imore.com/closer-look-ios-8s-mac-randomization`, Sept. 2014. Last access: 23.10.2014.

[3] M. V. Barbera, A. Epasto, A. Mei, V. C. Perta, and J. Stefa. Signals from the crowd: uncovering social relationships through smartphone probes. In *Proceedings of the conference on Internet measurement conference*, pages 265–276. ACM, 2013.

[4] 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), IEEE 14th International Symposium and Workshops on a*, pages 1–6, 2013.

[5] C. P. Dancey and J. Reidy. *Statistics without maths for psychology*. Pearson Education, 2007.

[6] D. M. Gavrila. The visual analysis of human movement: A survey. *Computer vision and image understanding*, 73(1):82–98, 1999.

[7] B. Greenstein, D. McCoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall. Improving wireless privacy with an identifier-free link layer protocol. In *Proceedings of the 6th international conference on Mobile systems, applications, and services*, pages 40–53. ACM, 2008.

[8] J. E. Larsen, P. Sapiezynski, A. Stopczynski, M. Mørup, and R. Theodorsen. Crowds, bluetooth, and rock'n'roll: understanding music festival participant behavior. In *Proceedings of the 1st ACM international workshop on Personal data meets distributed multimedia*, pages 11–18, 2013.

[9] S. Lee, M. Kim, S. Kang, K. Lee, and I. Jung. Smart scanning for mobile devices in wlans. In *Communications (ICC), IEEE International Conference on*, pages 4960–4964, 2012.

[10] J. Lindqvist, T. Aura, G. Danezis, T. Koponen, A. Myllyniemi, J. Mäki, and M. Roe. Privacy-preserving 802.11 access-point discovery. In *Proceedings of the second ACM conference on Wireless network security*, pages 123–130, 2009.

[11] A. Musa and J. Eriksson. Tracking unmodified smartphones using wi-fi monitors. In *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems*, pages 281–294, 2012.

[12] R. Nishide and H. Takada. Exploring efficient methods to extract pedestrian flows on a mobile adhoc network. In *UBICOMM 2012, The 6th International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, pages 29–34, 2012.

[13] J. Pang, B. Greenstein, R. Gummadi, S. Seshan, and D. Wetherall. 802.11 user fingerprinting. In *13th ACM international conference on Mobile computing and networking*, pages 99–110, 2007.

[14] H. Rahmalan, M. S. Nixon, and J. N. Carter. On crowd density estimation for surveillance. In *Crime and Security. The Institution of Engineering and Technology Conference on*, pages 540–545. IET, 2006.

[15] M. Versichele, T. Neutens, M. Delafontaine, and N. Van de Weghe. The use of bluetooth for analysing spatiotemporal dynamics of human movement at mass events: A case study of the ghent festivities. *Applied Geography*, 32(2):208–220, 2012.

[16] Y. Wang, J. Yang, H. Liu, Y. Chen, M. Gruteser, and R. P. Martin. Measuring human queues using wifi signals. In *Proceedings of the 19th annual international conference on Mobile computing & networking*, pages 235–238. ACM, 2013.

[17] J. Weppner and P. Lukowicz. Bluetooth based collaborative crowd density estimation with mobile phones. In *Pervasive Computing and Communications (PerCom)*, pages 193–200. IEEE, 2013.