EAI Endorsed Transactions
on Ubiquitous Environments

Research Article ICST.ORG

Analyzing Pedestrian Flows Based on Wi-Fi and Bluetooth Captures

Lorenz Schauer[1,*] and Martin Werner[1]
[1]Ludwig-Maximilians-Universität München (LMU Munich), Mobile and Distributed Systems Group, Oettingenstr. 67, 80538 Munich, Germany

Abstract

The rapid deployment of smartphones has led to a wide adoption of wireless communication systems such as Wi-Fi and Bluetooth. Both techniques leak information to the surroundings during operation. This information has been used in literature for estimating pedestrian flows, b ut t he c orrelation t o g round truth has not yet been evaluated. Thus, a reliable deployment in real world scenarios is rather difficult. To fill in this gap, we use ground truth provided by the security check process at a major airport and evaluate the quality of crowd information gathered from Wi-Fi and Bluetooth captures. We analyze estimated pedestrian flows and present three approaches improving the accuracy compared 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. The presented approaches yield a better correlation and allow for a practical estimation of pedestrian flows.

Keywords: crowd density, pedestrian flow, tracking, Wi-Fi probes, Bluetooth

Received on 9 February 2014; accepted on 24 March 2015; published on 26 May 2015

doi:10.4108/ue.1.4.e4

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 to the actual needs of the present people, for example by closing or opening additional doors, ticket shops, or control gates. Based on automatically extracted 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 order to obtain this information automatically, optical approaches have been investigated for many years using cameras and image processing techniques, such as [15]. 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 people might be a privacy issue and has to be discussed carefully in most scenarios [7].

In the last decade, Wi-Fi infrastructures have been 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

*Corresponding author: Email: lorenz.schauer@ifi.lmu.de

several purposes, such as locating and tracking people or for density and trajectory estimation.

However, and to the best of our knowledge, the 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, selected management frames of both, Bluetooth and Wi-Fi have been collected at two particular monitor nodes inside a major 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 and the boarding pass scan 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 evaluated using the Pearson's correlation indicating the degree of the linear dependence between our estimation and the given 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 using 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 [17, 19]. Furthermore, human behavior was extracted from similar data for a concert situation [4, 9]. 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 [13].

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. Abedi et al. [1] 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 [12], social relationships [3], waiting times in human queues [18], and in order to calculate density estimations [4].

Wi-Fi based flow estimations are also performed by Ruiz et al. [16]. Using a classification approach based on RSS measurements, the authors estimate the amount of entries and exits from people entering or leaving a hospital. Their results are compared with ground truth provided by a person who manually counted the actual entries and exits of people at a specific entrance. In this aspect, their work is the closest related to our investigations. However, the used test set and the performed method differ from our approaches and a comparison to Bluetooth measurements is missing. Furthermore, we present an explicit evaluation of the reliability of such estimations performing correlation analysis with ground truth. With respect to related work, this has not been done so far.

3. Methodology

This section describes the methodology for crowd density and pedestrian flow estimations based on signal captures from unmodified mobile devices. 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. Most commonly, mobile devices use a class two radio which provides a communication range of about ten meters.

The device discovery process consists of two protocol parts which are called *Inquiry* and *Inquiry Scan*. The first part defines the active role and is used to discover other devices. Following this protocol, a device has to send an inquiry request on all possible inquiry scan physical channel frequencies and listen for an inquiry response message. The second protocol part *Inquiry Scan* defines, how a Bluetooth device shall behave in order to be detected by other devices. Commonly, a Bluetooth device following this protocol is said to be "discoverable" meaning that it remains passive and listens for inquiry requests on a selected single inquiry scan physical channel. The device will answer to inquiry requests received on this channel with an inquiry response [5]. The standard inquiry response frame contains the Bluetooth MAC identifier of the discovered device. Since Bluetooth 2.1 extended inquiry responses are sent providing more information about

the discovered device, such as local name, transmitter power, supported services or manufacturer specific values.

Modern smartphones are not in the inquiry scan state by default and thus, they will not be discovered on any inquiry scan physical channel. However, in public areas with heterogeneous crowds like on airports, it is suspected to capture a noticeable amount of discoverable Bluetooth 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, depicted in Figure 1 and performed by most smartphones in the public.

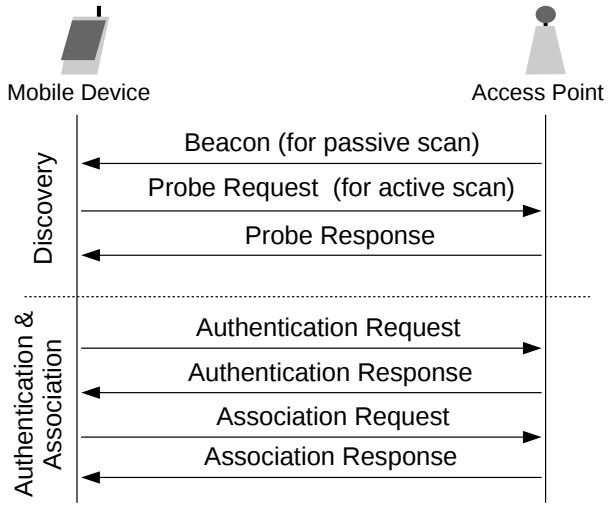


Figure 1. 802.11 network discovery and association process

Wi-Fi discovery also 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 [10]. 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 using 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 public 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 [11], or as a new protocol version [8]. 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 is slightly increased. However, the randomization of MAC addresses alone does not truly preserve the user's privacy, due to implicit identifiers, or specific characteristics of Wi-Fi traffic [14]. Furthermore, the actual implementation of the randomization in iOS fails 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 during short time periods. In other words, the MAC address randomization technique leads to the fact that measurements taken on different days are difficult to relate to each other while measurements taken in very short time frames in a Wi-Fi enabled environment are most likely showing the same MAC address.

3.3. Measurement Techniques

In order to estimate crowd densities and pedestrian flows, adequate data from mobile phones has to be captured at proper places. Generally, crowd density is defined to be the number of different people residing in

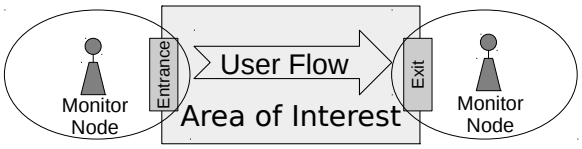


Figure 2. Schematic overview of pedestrian flow measurement

some unit of area during a certain time interval. Hence, the crowd density of one monitor node's coverage area is estimated as the amount of captured unique devices at the corresponding node during a certain time interval. We assume that a MAC address which is captured by a single monitor node belongs to one person. This has an effect on the total amount of our estimations, because some persons may carry more than one device while others do not carry any sending device at all. However, this does not affect the correlation between the estimations and ground truth, because the trend of the estimations is crucial, rather than the total amount of persons.

Beside crowd densities, which are measured by each monitor node, we are interested in the movement of crowds, respectively. Therefore, we define the pedestrian flow as the amount of people moving one way through an area of interest within a certain time interval. The area of interest can be of different type, e.g. hall, floor, room, etc. The pedestrian flow in the desired area of interest can then be measured by capturing and comparing the device specific MAC address at different monitor nodes located at the entrances and exits to this area of interest. Ignoring all sources of errors, the flow between two monitor node locations is given by the difference of their individual crowd densities. For a better illustration of this idea, Figure 2 depicts a schematic overview with one entrance and one exit door to the area of interest, while in general, there can be more entrances or exits.

Generally, the pedestrian flow is the amount of people moving from one entrance to one exit within a certain time interval. It 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.

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.

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.

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, phone positions and the crowd density itself. 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 due to the high amount of measurement noise in RSSI readings. Therefore, we present a hybrid approach.

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 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 strong impact on the ISM band and Wi-Fi transmissions. The corresponding responses including RSSI value, MAC addresses, and a time stamp were collected.

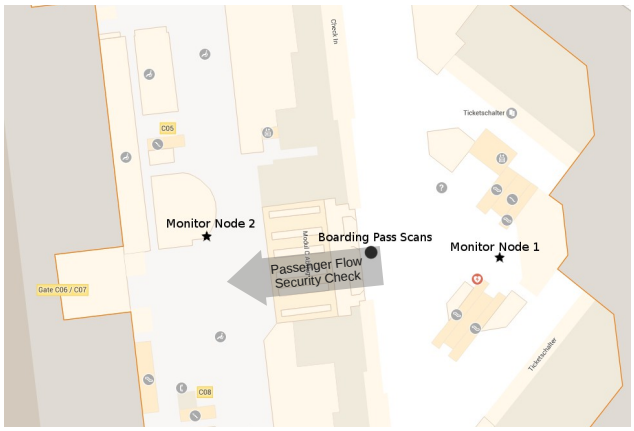


Figure 3. Map[1] of the testbed indicating the passenger flow through the security check, and the locations of monitor nodes, and boarding pass scans

As a reference information, we were given access to the exact boarding pass scan times reflecting the true flow of people through the security check. The experimental setup is shown in Figure 3 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 available

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.

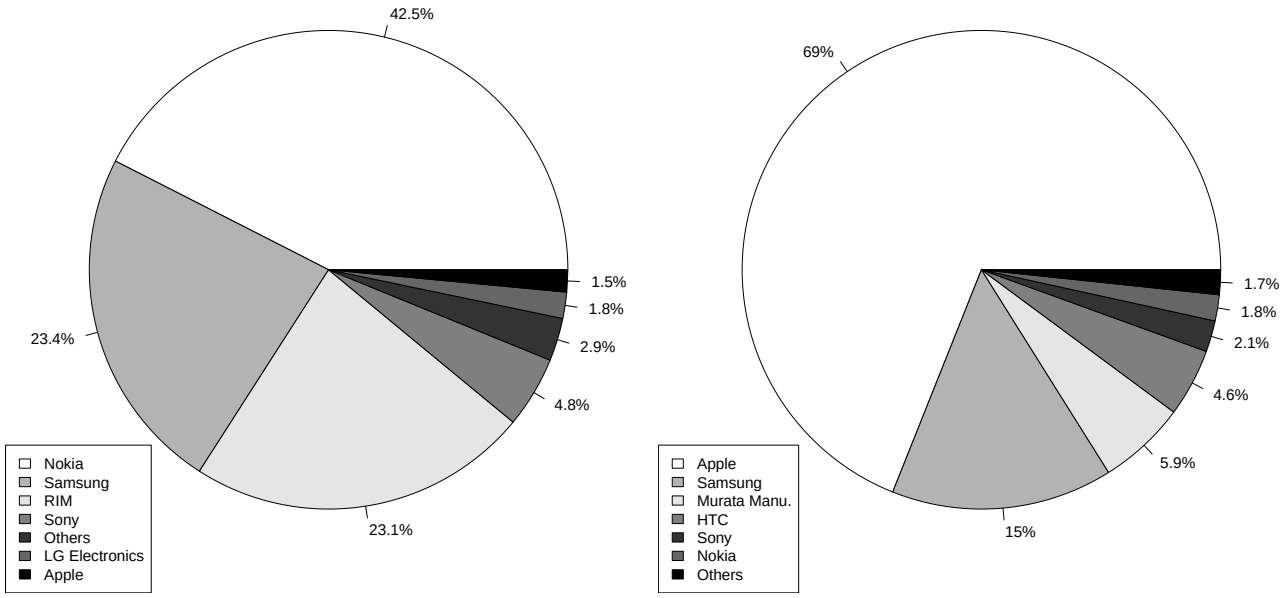
4.2. General Information from the Crowd

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 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 4a and 4b 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, 12]. 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,

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



(a) Bluetooth **(b)** Wi-Fi

Figure 4. Manufacturer distribution of unique captured devices in the public area

possibly due to very easy access to the option in the energy management widget. Finally, the crowd at an airport might have a skewed distribution of devices including a higher fraction of iPhones as compared to the current market shares of different smart phones.

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 5 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.

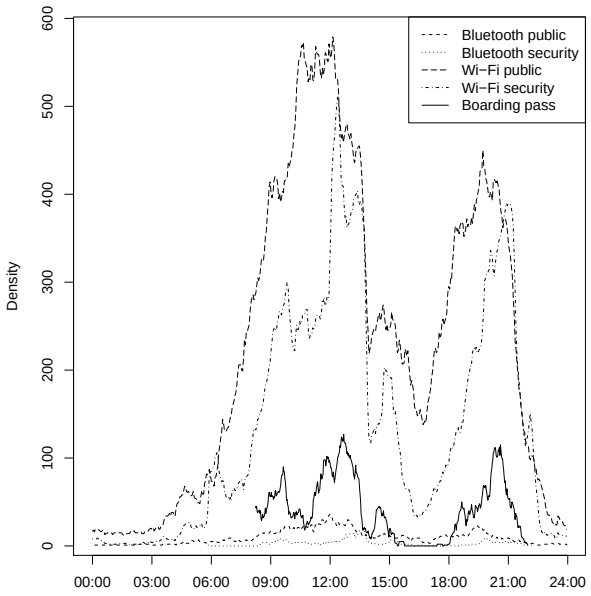


Figure 5. A single day including Wi-Fi, Bluetooth, and boarding pass readings

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.

4.4. Pedestrian Flow Estimation

Based on corresponding boarding pass readings, we analyze the accuracy of our proposed methodology for pedestrian flow estimation. Figure 6 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

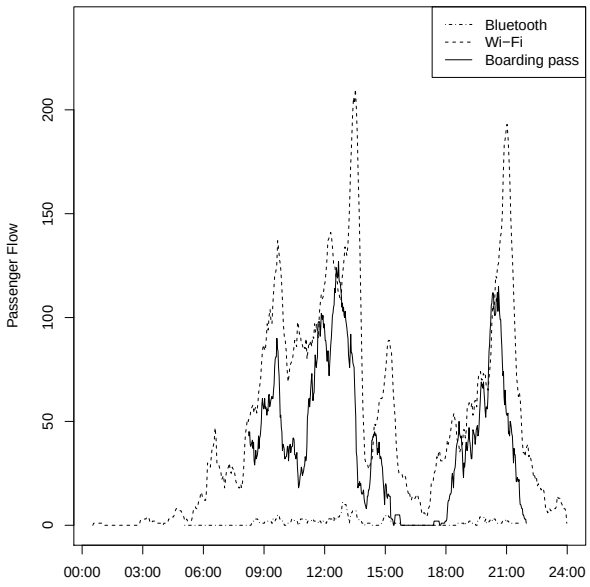


Figure 6. Results of naive Wi-Fi and Bluetooth based pedestrian flow estimations at a single day compared with boarding pass scans

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 actually passing the security gate. According to Section 3.3, we evaluate whether this effect can be limited by using one of the extended approaches. Figure 7 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

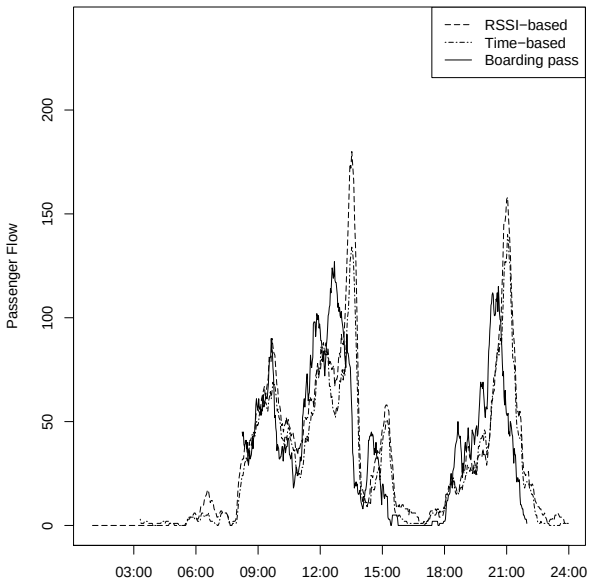


Figure 7. Results of RSSI and time-based Wi-Fi pedestrian flow estimations at a single day compared with boarding pass scans

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. Finally, Figure 8 depicts a general overview of the total amount of our flow estimations and ground truth for each day of the whole experiment. Considering the absolute amount of captured devices and real persons, the naive Wi-Fi counts perform better than the hybrid approach, expressed by a shorter Euclidean distance between both datasets. As already seen before, Bluetooth only shows a fraction of the real persons. However, the local maxima and minima are represented more precisely by the hybrid Wi-Fi based estimation.

For a more detailed analysis, we determine the Pearson correlation, which is a widely used measure of linear dependency between two observations, in our case between estimation and ground truth. The Pearson correlation is measured as a correlation coefficient $-1 \leq r \leq 1$. 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 the well-accepted categorization of Dancey and Reidy [6]:

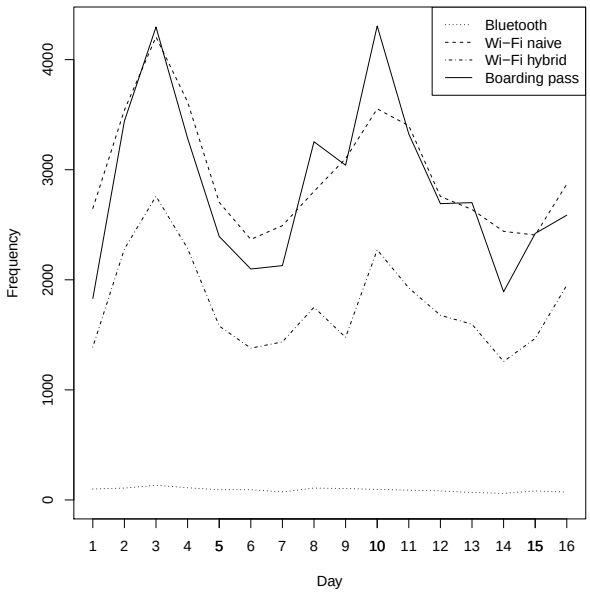


Figure 8. Overview of flow estimations and ground truth for each day of the experiment

$\|r\| = 0.0$	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

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 the system capturing only false-positives. Comparable 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 to be 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 has been reached for Bluetooth 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. Including additional information such as association requests did not improve the result. Consequently, we propose to limit data acquisition for Wi-Fi-based density estimation to probe requests reducing the amount of data per monitor node.

4.5. Security Check Duration Estimation

Based on the data from both monitor nodes, we estimate the security check duration for each passenger. The security check duration is defined to be the time it takes for each person to completely pass the security check procedure including the following steps:

1. Coming up to the security check area: In this step a person enters the range of the monitor node of the public area. Boarding passes are scanned at the entry to the waiting zone.

2. Standing in the waiting queue: The time it takes to pass this step depends on the amount of waiting persons, and thus, a correlation exists between the frequency of boarding pass scans and the length of waiting times.

3. Passing the security process: The passengers have to be checked by the security forces.

4. Exit the security check area: In this step a person leaves the range of the second monitor node.

From the data of each monitor node, we consider the timestamp when a MAC address was seen in the public and in the security area, respectively. The difference between these timestamps is seen as the estimated security check duration. For our purpose it has proven useful to consider the last timestamp of a captured MAC address at each node, due to the fact that there is a

	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

	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

higher probability for capturing persons standing in the waiting queue. Taking the time of the first occurrence of a MAC address would not cover the security check area, and considering the first of the public and the last timestamp of the security area would strongly overestimate the security check duration.

For the complete experiment, a mean security check duration of 26.6 minutes with a standard deviation of $\sigma = 3.5$ minutes is estimated in case of Wi-Fi, and 25.7 minutes with $\sigma = 12.5$ minutes in case of Bluetooth. Due to the fact, that these results cannot be compared with ground truth, we analyze the behavior of our estimation in comparison to the given boarding pass scans. Assuming that a longer waiting queue is indicated by an increased frequency of boardings pass readings, we compare our estimations with corresponding pass scans frequencies, depicted in Figure 9 for one example day. For this day, we observe a mean of 34.7 minutes and a median of 22.4 minutes for Wi-Fi based estimations. In case of Bluetooth, the mean is at 35.5 and the median at 27.5 minutes.

The results show the correctness of our assumption: During an increased frequency of boarding pass scans, we observe periods of higher security check duration estimations for both techniques. These periods suddenly start with a high value and decrease slowly over time. This indicates that a lot of passengers appear at the security check area at once, depicted in boarding pass scans, and thus, the waiting queue also increases suddenly at the beginning of one period. Then the security check duration decrease slowly over time, due to decreasing length of waiting queues.

However, real security check duration is hard to estimate on the basis of Wi-Fi or Bluetooth tracks only. It is not clear when a mobile device sends its probe requests or when people exactly leave the range of a monitor node. Thus, the last capture of a MAC address varies significantly which is expressed by a high number of outliers in the estimations indicating a very high security check duration.

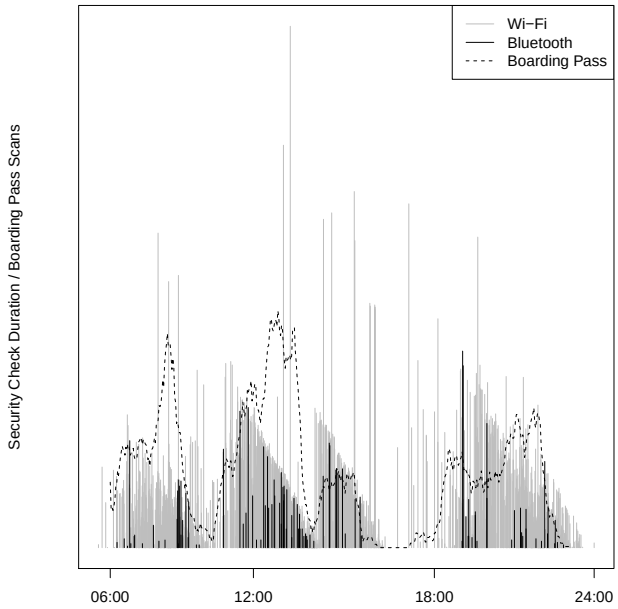


Figure 9. Estimated security check duration for passengers at one day compared with boarding pass scans

5. Conclusion and Future Work

In this paper, we have investigated quality and feasibility of pedestrian flow estimations based on Wi-Fi and Bluetooth captures from unmodified mobile devices at a major airport. Furthermore, we have presented three approaches to improve the Pearson correlation of our Wi-Fi based estimations to a known ground truth. A naive count of MAC addresses, as it is often proposed in related work, has only shown moderate results. 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 of its members. In summary, only a fraction of surrounding devices was tracked by periodical Bluetooth scans and, consequently, estimations based on Bluetooth 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 can be improved. With additional information from the application scenario, we 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 and possibilities of estimating a signal-to-noise ratio in pedestrian flow estimation. 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 show 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 the 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.

References

[1] Abedi, N., Bhaskar, A. and Chung, E. (2013) 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*.

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

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

[4] Bonné, B., Barzan, A., Quax, P. and Lamotte, W. (2013) 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*: 1–6.

[5] Chakraborty, G., Naik, K., Chakraborty, D., Shiratori, N. and Wei, D. (2010) Analysis of the bluetooth device discovery protocol. *Wireless Networks* **16**(2): 421–436.

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

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

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

[9] Larsen, J.E., Sapiezynski, P., Stopczynski, A., Mørup, M. and Theodorsen, R. (2013) 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*: 11–18.

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

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

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

[13] Nishide, R. and Takada, H. (2012) 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*: 29–34.

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

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

[16] Ruiz-Ruiz, A.J., Blunck, H., Prentow, T.S., Stisen, A. and Kjaergaard, M.B. (2014) Analysis methods for extracting knowledge from large-scale wifi monitoring to inform building facility planning. In *Pervasive Computing and Communications (PerCom), 2014 IEEE International Conference on* (IEEE): 130–138.

[17] Versichele, M., Neutens, T., Delafontaine, M. and Van de Weghe, N. (2012) 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.

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

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