IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 3, 2019, accepted June 16, 2019, date of publication June 27, 2019, date of current version August 7, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2925406

Mobile Device Detection Through WiFi Probe Request Analysis

LUIZ OLIVEIRA[1,2], (Member, IEEE), DANIEL SCHNEIDER[3], (Member, IEEE), JANO DE SOUZA[1], (Member, IEEE), AND WEIMING SHEN[4], (Fellow, IEEE)

[1]Systems Engineering and Computer Science Program/COPPE, Federal University of Rio de Janeiro, Rio de Janeiro 21941-590, Brazil
[2]IFRJ, Federal Institute of Rio de Janeiro, Niterói Campus, Niterói 24315-375, Brazil
[3]Tércio Pacitti Institute of Computer Applications and Research, Federal University of Rio de Janeiro, Rio de Janeiro 21941-901, Brazil
[4]State Key Lab of Digital Manufacturing Equipment and Technology, Huazhong University of Science and Technology, Wuhan 430074, China

Corresponding author: Weiming Shen (wshen@ieee.org)

The work of J. de Souza was supported in part by the Brazilian Research Council (CNPq) under Research Grant #311865/2017-8.

ABSTRACT Estimation of the presence of people in real time is extremely useful for businesses in providing better services while saving money. In this paper, we propose a technique for estimating the number of mobile devices present at a certain place and time, through analysis of WiFi probe requests from smart devices. Our goal is to address the problem through a solution that is immune to Media Access Control (MAC) address randomization strategies. The idea is to make use of information propagated in the environment, without the need to know the real MAC addresses of the devices. A state machine was modeled to detect the arrival, presence, and departure of devices in proximity to the sensors. A hardware prototype was developed for device detection, and its efficiency was evaluated in experiments that involved comparing the results of the proposed method with the manual measurements made by researchers. The proposed method provided very accurate correlations between the number of mobile devices detected and the real number of people in the environment.

INDEX TERMS Automatic people counting, occupancy estimation, building automation, WiFi probe request, MAC randomization, opportunistic sensing, passive tracking.

I. INTRODUCTION

Large urban centers have grown at a dizzying pace, which has often led to their disorderly growth. Accompanied by the rise in the number of inhabitants, the demand for services and energy consumption also increases, which leads to difficulties in the timely provision of services. Urban public transport infrastructure and commercial establishments are often burdened with long waiting times when meeting the demands of their respective publics. No less important an issue is the demand for energy in proportion to the population growth, whether in public spaces or in residential or corporate buildings.

The main problem to be addressed in this work is to estimate the number of people through the automatic detection of WiFi client devices. Occupancy detection can provide information to the building control systems to allow them to operate proportional to the number of occupants in the building [1], [2] and ultimately to optimize the building energy management through integrated optimal control of active and passive heating, cooling, lighting, shading, and ventilation systems [3]. This could lead to very positive impacts, either from a financial or environmental point of view.

The task of investigating probe requests is related to a challenge that has already been addressed in the literature [4]. In order to protect users' privacy, mobile operating systems usually hide the MAC address of the device when it is conducting probes. The main strategy adopted by manufacturers is randomizing MAC addresses, whose details can vary according to the device, manufacturer, and operating system version.

For example, from our observations, iPhone devices with iOS 10.1.1 execute a new MAC randomization every time the following occurs: (i) the device is locked or unlocked; (ii) a WiFi interface is activated or deactivated; or (iii) a connection to a WiFi access point is made or attempted. Thus, it can be stated that in some mobile devices it is not possible to estimate the time interval in which the same random MAC address is used, as this period depends on the way users interact with their smartphones.

The associate editor coordinating the review of this manuscript and approving it for publication was Tie Qiu.

Some efforts have been made to discover how to break this randomization [5]–[7]; however, the main drawback with these proposals is that the effectiveness can be disrupted whenever a new version of the mobile OS is released.

In the present study, our goal is to address the problem of detecting the presence of mobile devices located at a given place and time, through a solution that is immune to MAC randomization strategies. The idea is to make use of this information propagated in the environment, without the need to know the device's real MAC address. Occupancy detection can provide information to these building systems so that they operate in proportion to the number of occupants in the building [1], [2] and, ultimately, optimize the building's energy management through integrated optimal control of active and passive heating, cooling, lighting, shading, and ventilation systems [3].

The rest of the paper is organized as follows: sections II and III present the background and related work, respectively; section IV describes the proposed method for estimating the number of people at a given location and time; section V describes the new version of the hardware prototype developed; section VI discusses the current experiments and results; and section VII presents our conclusions and future work.

II. BACKGROUND

In this section we discuss the main topics covered in the present study, related to the area of Computer Networks. User devices that have a WiFi interface periodically perform a wireless probe procedure by actively sending a control frame, known as a ''probe request''. The purpose of this procedure is to have nearby wireless access points send information about wireless networks that are available for connection.

This scanning process is done whenever the WiFi interface is enabled, regardless of whether or not the user is connected to a wireless network. Client devices locally maintain a list called the Preferred Network List, which contains information about known networks to which the device has already connected at least once. Thus, the device is constantly searching for nearby wireless networks in order to find a known network to connect to automatically. Even when the device is already connected to a network, the scanning process continues, searching for networks with higher signal strength, thus always providing the best possible connection quality to the user.

Fig. 1 shows a simplified scheme of probe request messages. In this stream, the client sends a message that can be broadcasted or directed to a specific access point. Regarding the content, this message may mention a specific SSID or may not contain a value for the SSID field.

Table 1 shows some of the key fields that can be captured in probe request transmissions. Due to these transmissions being made prior to the process of associating a client to a wireless network, these data travel on the wireless medium without any type of encryption. The most important field for our study is the Source address, which states the physical address of

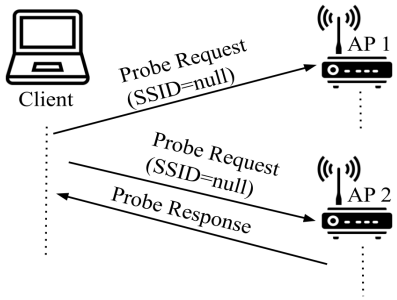


FIGURE 1. Simplified probe transmission scheme.

TABLE 1. Example with some fields for probe requests captured.

Source	Destination	BSSID	SSID
9a:31:87:22:fd:08	Broadcast	Broadcast	Broadcast
2a:15:c1:57:16:d8	Broadcast	Broadcast	wPESC

the device that scanned the networks. Another field widely used in other applications is the SSID searched for, which in many cases can compromise the privacy of users, as already reported in [8]–[11].

It should be noted that the aforementioned messages can be sent on the 14 different channels used by WiFi networks. Each channel represents a frequency spectrum used, and the distribution in channels is aimed at minimizing collisions in wireless transmissions.

Fig. 2 shows the 14 different channels used by WiFi networks, and also indicates the center of the frequency spectrum of each of the channels. The image highlights Channels 1, 6, and 11, which — because they do not have a frequency spectrum overlap between them — are the channels generally used by wireless routers. In this paper we also discuss strategies for monitoring the different wireless transmission channels.

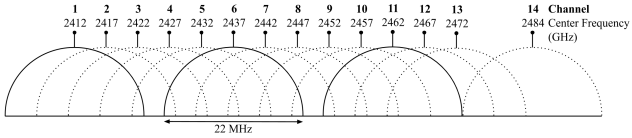


FIGURE 2. Communication channels used by WiFi networks.

III. RELATED WORK

In this section, a literature review on human presence detection initiatives that focus on different business needs is provided. Previous studies have proposed different methods for estimating the number of people present in a given area. To our knowledge, the first work to tackle this problem is from 1976 [12], in which the authors used time-stamped cards to monitor queues at an airport. Over the years, several other approaches have been used to address the problem of presence detection; for example: infrared sensors [13], [14]; cameras [15]; pressure sensors [16], [17]; visible light sensors [18]; Bluetooth [19]; WiFi [20]; RFID [21], [22]; UWB [23]; audio-processing [24]; and PC activity [1]. However, the use of the techniques mentioned above does not provide

satisfactory performance in relation to the cost of implementation and performance, as explored in [25].

In [4], the idea of capturing and analyzing frames of probe requests in order to deanonymize large clusters of people was discussed. The authors collected approximately 11 million probe requests at events of regional, national, and international relevance. It has been shown that by leveraging the information obtained from WiFi probes, it is possible to discover the provenience of the audience of each event to a high degree of accuracy. When generating probe requests, smartphones end up interchanging with each other the SSIDs of the networks to which the devices were previously connected.

Privacy risks associated with the leakage of SSIDs from networks already connected to by users were addressed in [9] and [10]. Even after several attempts to develop alternatives that preserve privacy, current mobile devices have continued to exhibit privacy-compromising behavior, by displaying previously used SSIDs, which could enable the identification of users.

The randomization of MAC addresses is a strategy that is intended to prevent potential observers from identifying which mobile devices are within reach of a sensor. In [5], Martin *et al.* reviewed the different techniques used, which varied according to device, manufacturer, and operating system version. The study also identified seven possible flaws in the current technological landscape. Firstly, the adoption rate — even though it is not necessarily a failure of the technology itself, it is not possible to ignore that the vast majority of devices currently in use, especially those with an Android operating system, do not implement randomization of MACs in any way. Secondly, the authors showed that, with one exception, all of the Android devices tested periodically transmit their global MAC addresses, which greatly impairs the effectiveness of randomization. Thirdly, UUID-E Reversal — a kind of attack, which was initially reported in [6] — was discussed. It makes Android devices transmitting probe requests with WPS data vulnerable, by exposing their global MAC addresses. Fourthly, the authors mentioned Device Signatures, which, in short, involve the use of sequence numbers in an attempt to assign — to a certain device that has disclosed its global MAC — other probes captured but with random origin MACs. Again, they found that Android devices are vulnerable to this tactic — unlike iOS devices, which do not transmit their global MAC information to probe requests. The authors also drew attention to the potential vulnerability in authentication and association frames, which always contain the global MAC, regardless of device. This can be exploited by analyzing sequence numbers of these packets and by establishing a relationship with probe requests captured with randomized MACs, similarly to the previous case. The problem with this approach is that it relies on the targeted device attempting to establish a network connection with a nearby access point, which is an event reasonably dependent on user activity. Karma Attack — also investigated in [6] — was the sixth method presented in [5]. It involves simulating an access point — that has the same SSID as a probe request captured from a certain device with randomized MAC — in order to identify its global address. The downside of this tactic lies in the fact that both Android and iOS have eliminated many of the so-called direct probes; that is, probes that have a specific target SSID as opposed to a probe in a broadcast that requests a response from all access points nearby. Finally, Martin *et al.* [5] proposed the Control Frame Attack, the aim of which is to send a Request to Send (RTS) to a device that is using a randomized MAC, thus prompting the device to respond with a Clear to Send. The RTS is sent to the previously known global MAC address, and if a response is received, it is possible to confirm that the device is within range of the sensor. The authors concluded that, regardless of manufacturer, in all of the tested devices, the operating system (or version thereof) is susceptible to this type of attack. Although very efficient, the need to know the MAC address in advance greatly limits the application of the technique. For practical purposes, this approach could be used only to monitor the presence of a reduced set of previously known devices. In Section IV we propose a solution based on a state machine that is able to monitor the presence of any devices even when using random MACs.

A number of efforts have been devoted to studying how to evaluate and classify approaches for detecting human presence. This classification can be done for dimensions such as resolution, accuracy, nature of infrastructure, diversity of sensors, applications, and user engagement, among other things. In [1], a model was proposed to measure the occupancy resolution in three dimensions, as can be seen in Fig. 3.

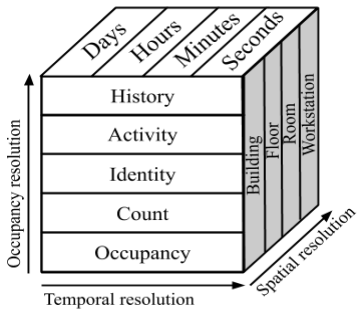


FIGURE 3. Occupancy resolution in three dimensions (modified from Melfi *et al.* [1]).

The model illustrated in Fig. 3 — derived from [1], [26] — evaluates the occupancy resolution in three dimensions: temporal, spatial, and semantic. The precision of the occupancy in days, hours, minutes, or seconds is informed for the temporal dimension. In the spatial dimension, the authors evaluated the scope of the occupancy measurement, from the more generic (i.e., a building) to the more specific (i.e., a workstation). The third and last dimension is related to semantic resolution of sensed occupancy:

- Level 1- Occupancy: at least one person in a zone
- Level 2- Count: number of people in a zone
- Level 3- Identity: who they are

- Level 4- Activity: what they are doing
- Level 5- History: movement history across different zones

The level of occupancy resolution required varies according to the application. For example, a building power control system will probably require less occupancy resolution than a building safety system. High resolution entails higher implementation costs, while appropriate levels of data granularity can provide the expected return on energy savings. Besides resolution, another important aspect is accuracy. Occupancy detection accuracy can be defined as the proximity of a measured value (usually based on a number of readings from a sensor) to the ground truth (actual) occupancy. Accuracy may also depend on the engagement of system users, because, in some cases, people may find ways to influence measurements; for example, by obstructing the view of the sensors [27]. Accuracy should be adjusted according to the application, and should take into account the consequences that false positives and false negatives for occupancy can generate in the decisions taken by a building's control system.

The nature of the infrastructure used for measurement is also an object of study. The extraction and utilization of occupancy information from systems that have been installed on a property for other primary purposes — rather than those explicitly designed to collect occupancy information — has been referred to as implicit occupancy detection [1], ambient sensing [28], or soft sensing [29], [30]. This potentially available information may have already been collected but not yet used for property control purposes; or, despite being available, it may not yet have been collected by any system. Melfi *et al.* [1] proposed a three-tier classification that evaluates the level of complexity of the modifications needed to promote the use occupancy sensors:

- Tier I requires no modification to existing systems other than a collection and processing point;
- Tier II involves the addition of software to existing infrastructure to make existing occupancy-related data available;
- Tier III involves the addition of software and hardware to introduce new sources of occupancy data to existing systems.

We must emphasize that all the three tiers require some sort of modification to the existing infrastructure. In Tier I, in which modification is less complex, only changes in the collection and processing of information that is already available are required. In Tier II, solutions that require some modification in the software are classified so that occupancy data is available. Finally, in Tier III it is no longer an implicit solution, as it is necessary to add more hardware and software infrastructure for occupancy sensing.

Proposed solutions for presence detection use either only one sensing approach or they aggregate information from more than one source. In [28], [31], and [32], the authors promoted the combination of data from multiple sensors — such as motion, sound, relative humidity, temperature, light, and CO2 — to monitor occupancy of environments. Hailemariam *et al.* [33] showed that the use of additional sensors does not necessarily increase detection accuracy. Khan *et al.* [34], in order to estimate occupancy, the authors investigated the combination of environmental sensing with contextual information, which yielded promising results. Among the contextual information used, the following can be mentioned: weather data, electricity consumption, meeting schedules, equipment usage, and PC activity data.

Occupancy monitoring techniques can be used for a number of different applications. Most reported efforts include solutions to optimize the operation of HVAC (heating, ventilation, and air conditioning) systems and the control of lighting [35], [36], as well as for targeted advertising [37]–[39], transportation [40]–[42], waiting-time estimation [15], [43], [44], indoor location [45]–[49], among other things.

IV. PROPOSED METHOD

In this paper, we propose a solution for estimating the number of people in a given location through the detection of wireless devices.

As discussed in Section II, a wireless client probes at all times, regardless of whether or not it is connected to a wireless network. Thus, monitoring the wireless environment turns out to be a good alternative for detecting human presence, considering the ubiquity of such devices. The main contributions of this present study include the following: the design of a WiFi presence detection device called Sherlock, which is specialized in detecting probe requests; and a method for estimating the number of people in a given location. This study is a follow-up of previous work [50] by the same research team.

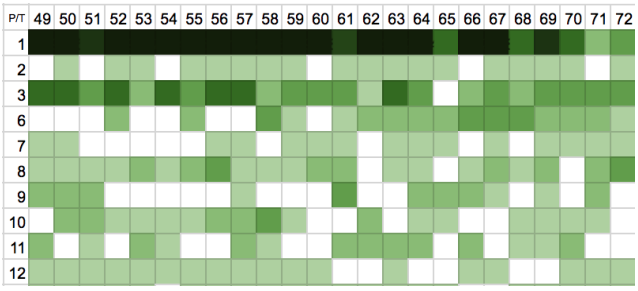


FIGURE 4. Bursts of probe request transmissions.

Fig. 4 depicts a partial visualization, based on data collected during one of the monitoring sessions conducted in a classroom. The rows describe 12 detected client devices that were part of the experiment. The columns represent one-minute time intervals, from the 49th to the 72nd minute, for a subset of the entire monitoring period. The color for each individual cell indicates the number of probes emitted by the corresponding participant and captured within that minute. White indicates that no probe was detected, while the shade of green gets darker as the number of probes increases. In this observation, the numbers ranged from zero to a few hundred

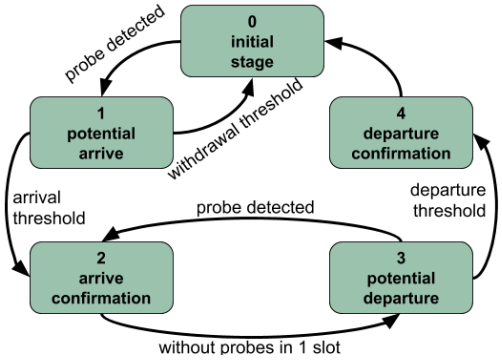


FIGURE 5. State transition diagram.

every minute, for each device. Different behavior patterns were observed; for example, some devices have continuous transmission bursts, while others have time intervals between one burst and another.

It should be noted that some devices that are in neighboring rooms or approach the monitored room for a few seconds may be detected during monitoring. Thus, it is necessary to design a mechanism that will handle these cases, filtering out unwanted detections and counting only people who actually enter and remain in the monitored environment. In order to deal with this problem, a state machine was modeled, based on [43], in which probe requests are submitted to an algorithm in order to detect the actual arrival and departure of people in the monitored room.

Fig. 5 shows the state transition diagram of the modeled state machine for detecting the presence of devices. The state machine is instantiated every time a new MAC address is perceived by Sherlock when performing transmissions. When a probe request from a given source is detected for the first time, the machine advances to stage 1 (potential arrival). The next detected transmissions are then grouped into one-minute slots to be evaluated on a consolidated basis. The potential arrival then needs to be confirmed, and this occurs when at least one probe request transmission from the same source is observed in the arrival threshold (A_T) slots, following the one in which the potential arrival was detected. Once this threshold is reached, the machine advances to stage 2 (arrival confirmation). It may happen that a potential arrival is not confirmed if consecutive withdrawal threshold (W_T) slots with no probes are detected during the arrival confirmation phase. In this case, the machine returns to the initial stage.

When a device's arrival is confirmed, it is also necessary to detect its departure. When no probe of a given source is detected in any slot, the machine advances to stage 3 (potential departure). Likewise, a potential departure event needs to be confirmed, and this occurs when it is not possible to observe at least one probe request transmission from the same source in the departure threshold (D_T) slots, following the slot in which the potential departure was detected. Once this threshold is reached, the machine advances to stage 4 (departure confirmation). A potential departure may not be confirmed in the situation in which the mechanism perceives some probe request from that source before the departure threshold is reached. In this case, the state machine returns to stage 2 (arrival confirmation). Once a device's departure has been confirmed, this device returns to the initial state of the state machine and is subject to a new detection.

As seen in Fig. 4, different values for the arrival, withdrawal, and departure threshold parameters have a strong influence on the arrival and departure of devices. The variation in values for these parameters will be detailed in Section VI.

V. PROTOTYPE

A new version of Sherlock, initially described in [50], has been developed. The current version is capable of capturing probe requests over multiple wireless interfaces, thus increasing the coverage of the capture mechanism on each of the transmission channels. The initial version of the device had only one wireless interface, and this interface was shared for monitoring the 14 transmission channels.

By leveraging multiple wireless interfaces, it is now possible to maximize the monitoring time on each of the wireless channels. Ideally, a device with 14 interfaces could monitor each channel 100% of the time. However, due to cost issues, it is generally not possible to design a device with such a large number of wireless interfaces. The Sherlock version presented in this paper has five network interfaces that can be used flexibly, scanning the transmission channels at different possible sharing settings.

In this new version, the mechanism has a more robust state machine (described in Section IV) that is capable of more accurately detecting the presence of wireless devices. The next section will present the experiments performed in order to validate the efficiency of the mechanism developed.

VI. EXPERIMENTS AND RESULTS

In this section, we describe the experiments and their results, in order to validate the mechanism proposed in Section IV.

Fig. 6 shows how the network interfaces were are allocated to perform the experiments discussed below. In all of the experiments reported in this section, Interface 0 was configured to cycle through Channels 1 to 13. Channel 14 was not included in this list because it has been homologated in hardly any countries. The device monitors a wireless transmission channel for 3 seconds and then tunes to the frequency of the next transmission channel. Data from Interface 0 is collected and processed separately for comparison purposes. Interfaces 1 through 4 are used in parallel, interleaving the monitoring of the 13 channels. Interface 1 monitors Channels 1, 2, and 3; Interface 2 monitors Channels 4, 5, and 6; Interface 3 monitors Channels 7, 8, and 9; and interface 4 monitors Channels 10, 11, 12, and 13. The results obtained in A were compared with the results obtained in B, as per Fig. 6.

A key issue that must be investigated in this work is the influence that the use of multiple antennas has on the effectiveness of the human detection mechanism. It is well known that a larger number of antennas maximizes the monitoring

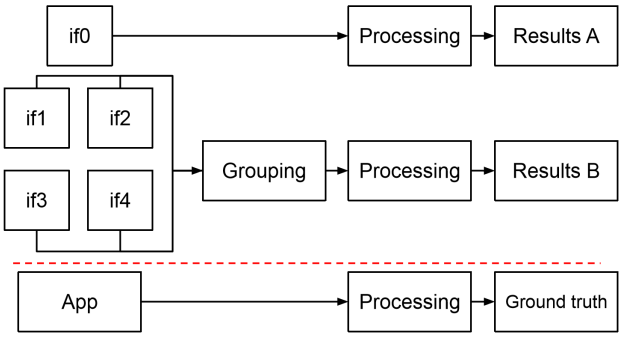


FIGURE 6. Scheme of use of the interfaces and workflow of the experiment.

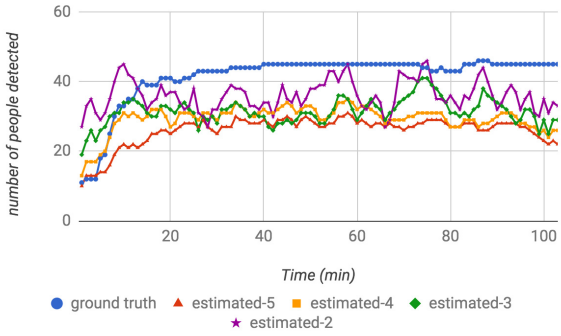


FIGURE 7. Detection of people through different time parameters, using only one network interface.

time for each channel, which leads to the detection of more probes. However, depending on the desired application, the increase in the number of probes does not necessarily lead to an improvement in the effectiveness of the mechanism, as will be discussed further below.

Fig. 4 shows bursts of probes from a number of sources. In some cases, a given source sent 602 probes in just 1 minute. In this and many other cases, it is not necessary to detect all of the probes — just a few, or even just one probe for each evaluation period. However, in other cases of devices that send much fewer probes, the presence of more antennas can determine if a particular device will be detected or not.

To answer this question, two results were produced for each experiment: Result A, with probes collected only by Interface 0; and Result B with probes collected by Interfaces 1 to 4. Since both results were collected by the same device and during the same time interval, the results can be compared with confidence. Finally, we have the ground truth measurement, which corresponds to the reading made through the visual observation of an expert (the researcher) during the experiment. We developed a mobile application to enable the production of a data series that expresses the manual counting of people in a place over time.

The researcher responsible for manually counting people used the mobile application by pressing the $+1$ and -1 buttons each time they observed someone entering or leaving the room, respectively. Thus, a data file was produced by recording the precise number of people (manually monitored) in the room at any point in the experiment. According to Fig. 6, the data produced by the mobile application enabled the generation of a ground truth measurement, which was used as a reference for comparison with results A and B.

A. INVESTIGATING THE USE OF MULTIPLE NETWORK INTERFACES

The first experiment was done during a lesson in a classroom of our university. Monitoring was done for 1 hour and 47 min, and the same device was used to capture probes in parallel in two configurations. In the first configuration, using only Interface 0 and switching between Channels 1 through 13, 42,169 probes were captured. In the second configuration, using Interfaces 1 through 4 and monitoring a subset of channels without any overlapping channels, 82,146 probes were captured. The first observation is that the use of multiple antennas did not lead to a proportional increase in the number of probes.

Fig. 7 shows the comparison between the ground truth result (used as a reference) and the estimates made by the proposed mechanism, with different values for the arrival and departure threshold parameters. During this analysis, the withdrawal threshold parameter had its value set to 1 (this parameter is the object of study in the next experiment). The arrival and departure threshold parameters are related to the number of consecutive slots of presence or absence of probes that must be observed in order to confirm a potential arrival or potential departure. The estimates are named according to the parameters used. For example, the "estimated-5" metric is calculated with the arrival and departure parameters set to 5; the "estimated-4" metric is calculated with the arrival and departure parameters set to 4, and so on. In Fig. 7, the ground truth result is shown in blue, the "estimated-5" metric — calculated with arrival and departure threshold parameters set to a 5-slot value — is shown in red, "estimated-4" is in orange, "estimated-3" in green, and "estimated-2" in purple.

As expected, lower values for the arrival and departure threshold parameters lead to more unstable estimates and tend to be less reliable. For higher values of these parameters, the estimates are more stable and follow the manual measurement tendency more faithfully. When observing the measure "estimated-2", with ($A_T = 2, D_T = 2$) configuration, that has low values for arrival and departure thresholds, it is noticed that the measure is very unstable and inaccurate, oscillating between values below and above the ground truth. This happens because, with these threshold values, the proposed mechanism confirms the arrival or departure of a device in a hasty manner. On the other hand, the "estimated-5" measure has a more conservative configuration ($A_T = 5, D_T = 5$) being more stable and stays closer to the ground truth line. In most of the time, all curves had lower values when compared to the visually monitored ground truth measurements, which is expected, because some devices may not have WiFi enabled and some people may not even be carrying wireless devices.

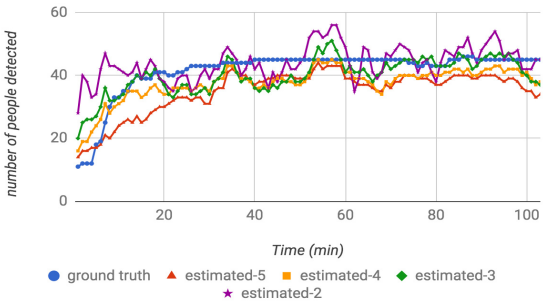


FIGURE 8. Detection of people through different time parameters, using four network interfaces.

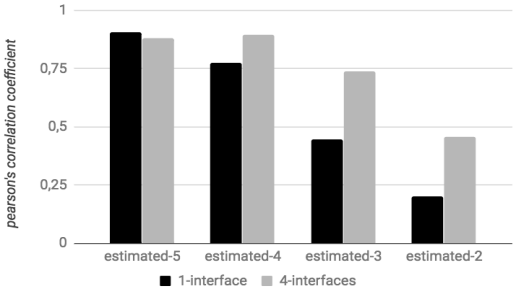


FIGURE 9. Pearson correlation coefficient between each estimate and its corresponding ground truth value.

Fig. 8 shows the same comparison, but takes into consideration probes collected from four antennas. The same stability trends observed in Fig. 7 for the metrics can also be seen in Fig. 8, with the difference being that the estimates in the four-antenna setup are closer to the ground truth values.

Fig. 9 shows the Pearson correlation coefficients for the ground truth measurements and the estimated value for each studied scenario — with either one or four interfaces and with different values for the arrival and departure threshold parameters. It can be seen that the "estimated-5" indicator achieved similar performance in scenarios with either one or four network interfaces. Due to the fact that it is a more conservative mechanism, it is stabler and more resilient, even in scenarios with a smaller sample of probes. The same behavior cannot be seen when using the other parameters: as the parameter values are reduced, the mechanism becomes less conservative and more responsive to external variations. This caused the correlation to decrease and resulted in differences between the one- and four-antenna scenarios.

Fig. 10 shows the mean relative errors between the ground truth value and the values estimated in each of the scenarios. It can be seen that in this evaluation, the one-antenna setup gave an error far greater than that in the four-antenna setup. In this case, we can see that the "estimated-4" indicator was the most accurate measure considering measure of association (0.896) and the "estimated-3" indicator with the lowest mean relative error (0.117).

B. INVESTIGATING THE ACCURACY OF THE PROPOSED MECHANISM USING DIFFERENT THRESHOLDS VALUES

As expected, the first analysis let us conclude that the use of multiple network interfaces in probings may provide better

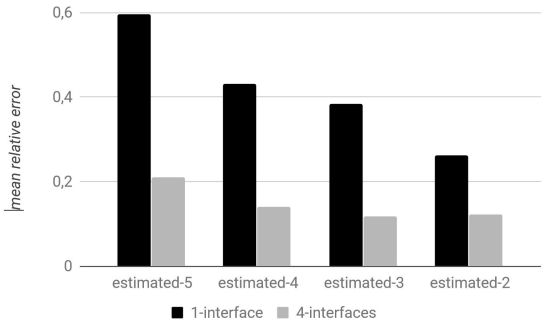


FIGURE 10. Mean relative error between each estimate and its corresponding ground truth value.

correlation and a smaller mean relative error, thus indicating better accuracy. A more detailed analysis of the influence that the three threshold parameters (A_T, W_T, and D_T) can exert on the mechanism is needed, and is given below. In this subsection we present the results of a new analysis made with the same data from the previous subsection. Unlike the first analysis, in which the withdrawal threshold parameter was set to one, the influence of this parameter is studied in this new analysis.

The withdrawal threshold parameter represents the number of slots without consecutive probes captured during the arrival confirmation phase for the state machine to return to the initial stage. When this parameter is set to one, it means that only one slot without probes during the arrival confirmation phase is sufficient for the process of confirming an arrival to be canceled. Even with this limitation, the mechanism can be efficient in detecting the presence of devices that have a high probe sending rate — devices that go no longer than 1 minute without sending probes during the arrival confirmation phase. This situation can be seen in Fig. 4 with participants numbered 1, 3, 8, and 12, who had an uninterrupted flow of probes from the beginning of the interval shown in the figure. This situation does not occur for participants numbered 2, 6, 7, 9, 10, and 11—although present, such devices go through periods without sending probes.

The ability of the algorithm to recognize the presence of a device, even if it fails to send probes through one or more slots during the arrival confirmation phase, ensures that more devices are detected by the mechanism. Thus, the raw data collected by the four network interfaces in the previous experiment were processed here using different values for arrival, withdrawal, and departure thresholds.

Table 2 shows the results obtained by varying the threshold parameters so that trends could be observed. When looking at this table, we can see that the best correlation occurs when the parameters A_T and D_T have a value of 5, 6, or 7. As observed in the previous subsection, high values for A_T and D_T provide more stability for the estimation, avoiding fluctuations that hinder the correlation of the series with the ground truth. The exact inflection point can be seen in the table, in which the Pearson's correlation coefficient tends to increase until it reaches its local maximum in the ($A_T = 6, D_T = 6, W_T = 2$) configuration.

TABLE 2. Thresholds values and results.

Thresholds			Results	
A_T	D_T	W_T	PCC	MRE
4	4	2	0.765	0.111
4	4	3	0.613	0.186
5	**5**	**2**	**0.868**	**0.103**
5	5	3	0.857	0.189
5	5	4	0,747	0.247
6	**6**	**2**	**0.869**	**0.087**
6	6	3	0.867	0.180
6	6	4	0.801	0.239
7	**7**	**2**	**0.811**	**0.131**
7	7	3	0.843	0.140
7	7	4	0.783	0.211

A_T = arrival threshold; D_T = departure threshold; W_T = withdrawal threshold; PCC = Pearson's correlation coefficient; MRE = mean relative error

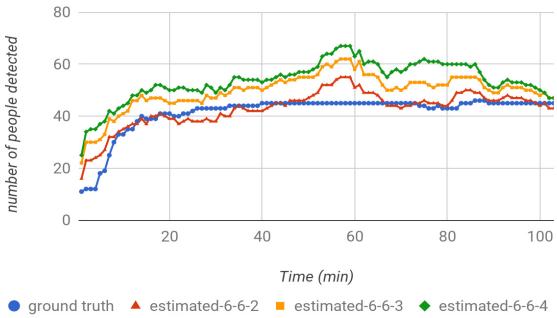


FIGURE 11. Influence of parameter W_T on detection of people.

With respect to the W_T parameter, we could see that high values for this threshold indicate significant increases in the mean relative error. We also observed that the three lines with $W_T = 2$ (highlighted in the table) are those with the smallest mean relative error. This is because a larger tolerance to slots without probes during the arrival confirmation phase implies an overestimated number of detected devices. Confirming the trend found with the Pearson's correlation coefficient, the exact inflection point of the downward trend of the mean relative error (i.e., when it reaches its local minimum) also occurs in the $(A_T = 6, D_T = 6, W_T = 2)$ configuration.

Four curves are shown in Fig. 11: the blue one indicates the ground truth; the red one indicates the estimate using the $(A_T = 6, D_T = 6, W_T = 2)$ configuration; the orange one shows the $(A_T = 6, D_T = 6, W_T = 3)$ configuration; and the red one depicts the $(A_T = 6, D_T = 6, W_T = 4)$ configuration. The high accuracy of the mechanism proposed here for estimating the number of devices can be seen when analyzing the graph, especially in the $(A_T = 6, D_T = 6, W_T = 2)$ configuration. We can also see in this same graph the influence that the W_T parameter exerts, so that the obtained values are overestimated in relation to the ground truth measurements.

VII. CONCLUSIONS AND FUTURE WORK

The experiments performed in this study were aimed at evaluating the effectiveness of a detection mechanism through evidence left by devices in the wireless transmission medium. In order to accomplish this verification, the ground truth number of people present in an environment (measured by an expert) and the estimated number of people computed by the mechanism were compared. Our goal was to produce an estimate that is as close as possible to the ground truth measurement observed, considering that the estimate can never be totally accurate due to the following reasons:

1) some people may not carry devices with a WiFi interface;
2) some devices may not have their WiFi interfaces enabled;
3) some people may have more than one device;
4) devices located in nearby rooms can be detected;
5) length of stay in the room may be insufficient for the detection of a number of devices; and
6) some transmissions may not be detected, as the monitoring device passes through different transmission channels.

The method proposed for estimating the number of devices by analyzing WiFi probe requests indicated a very strong correlation with the ground truth number of people in the environment, with a Pearson's correlation coefficient of 0.896. In addition to the high correlation, the mechanism was still able to achieve a low mean relative error of 0.087 — significant accuracy for the indicator.

The results obtained in this paper can be also compared with different approaches developed by other research groups that estimate the number of people in a given environment through evidence collected from the wireless environment. Table 3 summarizes the values of mean relative error obtained by number of approaches. The results indicate that the method based on the modeling of a state machine, called Sherlock, (proposed in this paper), proved to be more accurate than the Linear Regression (LR) and the Support Vector Regression (SVR) based methods, both proposed in [51]. The mean relative errors obtained by the LR-based and SVR-based methods were, respectively, 340% and 243% higher than those obtained through the mechanism embodied in Sherlock.

TABLE 3. Comparison with other related proposals.

Proposal	Mean Relative Error
Sherlock	0.087
LR-based method	0.383
SVR-based method	0.298

Despite the high correlation and low error rate observed with the proposed method, there is still further work to be done. The experiment needs to be replicated in other scenarios in order to reinforce the claims made in this study. Additionally, improvements should be made to obtain estimates closer to the ground truth values.

We believe that one of the answers to this problem may be in the use of machine learning techniques. The mechanism proposed in this work can monitor places for long periods of time, and the data collected can be used to detect spatial usage patterns. A new version of the method, which considers the

data collected before and after the monitoring moment, is currently under development. The dataset and source code used in this research are available in [52] so that other researchers can reproduce the experiments and verify the results.

REFERENCES

[1] R. Melfi, B. Rosenblum, B. Nordman, and K. Christensen, "Measuring building occupancy using existing network infrastructure," in *Proc. Int. Green Comput. Conf. Workshops*, Jul. 2011, pp. 1–8.

[2] Z. Wang and L. Wang, "Occupancy pattern based intelligent control for improving energy efficiency in buildings," in *Proc. IEEE Int. Conf. Automat. Sci. Eng. (CASE)*, Aug. 2012, pp. 804–809.

[3] B. Sun, P. B. Luh, Q.-S. Jia, Z. Jiang, F. Wang, and C. Song, "Building energy management: Integrated control of active and passive heating, cooling, lighting, shading, and ventilation systems," *IEEE Trans. Autom. Sci. Eng.*, vol. 10, no. 3, pp. 588–602, Jul. 2013.

[4] A. Di Luzio, A. Mei, and J. Stefa, "Mind your probes: De-anonymization of large crowds through smartphone WiFi probe requests," in *Proc. 35th Annu. IEEE Int. Conf. Comput. Commun. (IEEE INFOCOM)*, Apr. 2016, pp. 1–9.

[5] J. Martin, T. Mayberry, C. Donahue, L. Foppe, L. Brown, C. Riggins, E. C. Rye, and D. Brown, "A study of MAC address randomization in mobile devices and when it fails," *Proc. Privacy Enhancing Technol.*, vol. 2017, no. 4, pp. 365–383, 2017.

[6] M. Vanhoef, C. Matte, M. Cunche, L. S. Cardoso, and F. Piessens, "Why MAC address randomization is not enough: An analysis of Wi-Fi network discovery mechanisms," in *Proc. 11th ACM Asia Conf. Comput. Commun. Secur. (ASIA CCS)*, vol. 16, 2016, pp. 413–424.

[7] C. Matte, M. Cunche, F. Rousseau, and M. Vanhoef, "Defeating MAC address randomization through timing attacks," in *Proc. 9th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WiSec)*, vol. 16, 2016, pp. 15–20.

[8] M. Cunche, M.-A. Kaafar, and R. Boreli, "Linking wireless devices using information contained in Wi-Fi probe requests," *Pervasive Mobile Comput.*, vol. 11, pp. 56–69, Apr. 2014.

[9] A. B. M. Musa and J. Eriksson, "Tracking unmodified smartphones using Wi-Fi monitors," in *Proc. 10th ACM Conf. Embedded Netw. Sensor Syst. (SenSys)*, vol. 12, 2012, pp. 281–294.

[10] M. Cunche, M. A. Kaafar, and R. Boreli, "I know who you will meet this evening! Linking wireless devices using Wi-Fi probe requests," in *Proc. IEEE Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2012, pp. 1–9.

[11] N. Cheng, X. O. Wang, W. Cheng, P. Mohapatra, and A. Seneviratne, "Characterizing privacy leakage of public WiFi networks for users on travel," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2769–2777.

[12] J. P. Braaksma, "Time-stamping: A new way to survey pedestrian traffic in airport terminals," *Transp. Res. Rec.*, vol. 588, pp. 27–34, 2017.

[13] U. Stilla, E. Michaelsen, U. Soergel, S. Hinz, and H. J. Ender, "Airborne monitoring of vehicle activity in urban areas," *Int. Arch. Photogramm. Remote Sens.*, vol. 35, no. B3, pp. 973–979, 2004.

[14] R. H. Dodier, G. P. Henze, D. K. Tiller, and X. Guo, "Building occupancy detection through sensor belief networks," *Energy Buildings*, vol. 38, no. 9, pp. 1033–1043, Sep. 2006.

[15] D. Aubert, "Passengers queue length measurement," in *Proc. 10th Int. Conf. Image Anal. Process.*, Sep. 1999, pp. 1132–1135.

[16] D. Bauer, M. Ray, and S. Seer, "Simple sensors used for measuring service times and counting pedestrians: Strengths and weaknesses," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 2214, no. 1, pp. 77–84, 2011.

[17] Z. Yang, N. Li, B. Becerik-Gerber, and M. Orosz, "A multi-sensor based occupancy estimation model for supporting demand driven HVAC operations," in *Proc. Symp. Simulation Archit. Urban Design*, 2012, p. 2.

[18] J. Hao, X. Yuan, Y. Yang, R. Wang, Y. Zhuang, and J. Luo, "Visible light based occupancy inference using ensemble learning," *IEEE Access*, vol. 6, pp. 16377–16385, 2018.

[19] D. M. Bullock, R. Haseman, J. S. Wasson, and R. Spitler, "Automated measurement of wait times at airport security: Deployment at Indianapolis international airport, Indiana," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 2177, no. 1, pp. 60–68, 2010.

[20] Y. Wang, J. Yang, Y. Chen, H. Liu, M. Gruteser, and R. P. Martin, "Tracking human queues using single-point signal monitoring," in *Proc. 12th Annu. Int. Conf. Mobile Syst., Appl., Services*, 2014, pp. 42–54.

[21] N. Li and B. Becerik-Gerber, "Performance-based evaluation of RFID-based indoor location sensing solutions for the built environment," *Adv. Eng. Inform.*, vol. 25, no. 3, pp. 535–546, 2011.

[22] Z.-N. Zhen, Q.-S. Jia, C. Song, and X. Guan, "An indoor localization algorithm for lighting control using RFID," in *Proc. IEEE Energy Conf.*, Nov. 2008, pp. 1–6.

[23] Y. Xu, Y. S. Shmaliy, Y. Li, and X. Chen, "UWB-based indoor human localization with time-delayed data using EFIR filtering," *IEEE Access*, vol. 5, pp. 16676–16683, 2017.

[24] Q. Huang, Z. Ge, and C. Lu, "Occupancy estimation in smart buildings using audio-processing techniques," Feb. 2016, *arXiv:1602.08507*. [Online]. Available: https://arxiv.org/abs/1602.08507

[25] W. Shen, G. Newsham, and B. Gunay, "Leveraging existing occupancy-related data for optimal control of commercial office buildings: A review," *Adv. Eng. Inform.*, vol. 33, pp. 230–242, Aug. 2017.

[26] T. Labeodan, W. Zeiler, G. Boxem, and Y. Zhao, "Occupancy measurement in commercial office buildings for demand-driven control applications—A survey and detection system evaluation," *Energy Buildings*, vol. 93, pp. 303–314, Apr. 2015.

[27] H. B. Gunay, A. Fuller, W. O'Brien, and I. Beausoleil-Morrison, "Detecting occupants' presence in office spaces: A case study," *eSim*, vol. 2016, pp. 1–2, Oct. 2016.

[28] K. P. Lam, M. Höynck, B. Dong, B. Andrews, Y.-S. Chiou, R. Zhang, and J. Choi, "Occupancy detection through an extensive environmental sensor network in an open-plan office building," *IBPSA Building Simul.*, vol. 145, pp. 1452–1459, Jul. 2009.

[29] S. K. Ghai, L. V. Thanayankizil, D. P. Seetharam, and D. Chakraborty, "Occupancy detection in commercial buildings using opportunistic context sources," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops*, Mar. 2012, pp. 463–466.

[30] L. V. Thanayankizil, S. K. Ghai, D. Chakraborty, and D. P. Seetharam, "SoftGreen: Towards energy management of green office buildings with soft sensors," in *Proc. 4th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2012, pp. 1–6.

[31] B. Dong and K. P. Lam, "Building energy and comfort management through occupant behaviour pattern detection based on a large-scale environmental sensor network," *J. Building Perform. Simul.*, vol. 4, no. 4, pp. 359–369, 2011.

[32] A. Arora, M. Amayri, V. Badarla, S. Ploix, and S. Bandyopadhyay, "Occupancy estimation using non intrusive sensors in energy efficient buildings," in *Proc. 14th Conf. Int. Building Perform. Simulation Assoc.*, 2015, pp. 1–8.

[33] E. Hailemariam, R. Goldstein, R. Attar, and A. Khan, "Real-time occupancy detection using decision trees with multiple sensor types," in *Proc. Symp. Simulation Archit. Urban Design*, Boston, MA, USA, 2011, pp. 141–148.

[34] A. Khan, J. Nicholson, S. Mellor, D. Jackson, K. Ladha, C. Ladha, J. Hand, J. Clarke, P. Olivier, and T. Plötz, "Occupancy monitoring using environmental & context sensors and a hierarchical analysis framework," in *Proc. 1st ACM Conf. Embedded Syst. Energy-Efficient Buildings (BuildSys)*, vol. 14, 2014, pp. 90–99.

[35] Z. Nagy, F. Y. Yong, and A. Schlueter, "Occupant centered lighting control: A user study on balancing comfort, acceptance, and energy consumption," *Energy Build.*, vol. 126, pp. 310–322, Aug. 2016.

[36] S. Borile, A. Pandharipande, D. Caicedo, L. Schenato, and A. Cenedese, "A data-driven daylight estimation approach to lighting control," *IEEE Access*, vol. 5, pp. 21461–21471, 2017.

[37] T. Payne, E. David, N. R. Jennings, and M. Sharifi, "Auction mechanisms for efficient advertisement selection on public displays," in *Proc. ECAI*, 2006, pp. 285–289.

[38] J. F. McCarthy, T. J. Costa, and E. S. Liongosari, "UniCast, OutCast & GroupCast: Three steps toward ubiquitous, peripheral displays," in *Ubicomp 2001: Ubiquitous Computing* (Lecture Notes in Computer Science), vol. 2201, G. D. Abowd, B. Brumitt, and S. Shafer, Eds. Berlin, Germany: Springer, 2001. [Online]. Available: https://link.springer.com/chapter/10.1007/3-540-45427-6_28#citeas

[39] S. M. Bohte, E. Gerding, and H. L. Poutré, "Market-based recommendation: Agents that compete for consumer attention," *ACM Trans. Internet Technol.*, vol. 4, no. 4, pp. 420–448, 2004.

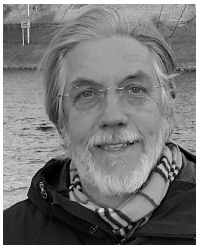
[40] W. Pattanusorn, I. Nilkhamhang, S. Kittipiyakul, K. Ekkachai, and A. Takahashi, "Passenger estimation system using Wi-Fi probe request," in *Proc. 7th Int. Conf. Inf. Commun. Technol. Embedded Syst. (IC-ICTES)*, Mar. 2016, pp. 67–72.

[41] T. Kusakabe, H. Yaginuma, and D. Fukuda, "Estimation of bus passengers' waiting time at a coach terminal with Wi-Fi MAC addresses," *Transp. Res. Procedia*, vol. 32, pp. 62–68, 2018.
[42] T. A. Myrvoll, J. E. Håkegård, T. Matsui, and F. Septier, "Counting public transport passenger using WiFi signatures of mobile devices," in *Proc. IEEE 20th Int. Conf. Intell. Transp. Syst. (ITSC)*, Oct. 2017, pp. 1–6.
[43] L. Oliveira, D. Schneider, F. Oliveira, S. Rodrigues, and J. de Souza, "Automatic detection of waiting times using smartphones," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2017, pp. 170–175.
[44] M. F. Bulut, Y. S. Yilmaz, M. Demirbas, N. Ferhatosmanoglu, and H. Ferhatosmanoglu, "LineKing: Crowdsourced line wait-time estimation using smartphones," in *Mobile Computing, Applications, and Services*. Berlin, Germany: Springer, 2012, pp. 205–224.
[45] V. Otsason, A. Varshavsky, A. LaMarca, and E. de Lara, "Accurate GSM indoor localization," in *UbiComp 2005: Ubiquitous Computing* (Lecture Notes in Computer Science), vol. 3660, M. Beigl, S. Intille, J. Rekimoto, and H. Tokuda, Eds. Berlin, Germany: Springer, 2005. [Online]. Available: https://link.springer.com/chapter/10.1007/11551201_9#citeas
[46] C. Wu, Z. Yang, Y. Liu, and W. Xi, "WILL: Wireless indoor localization without site survey," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 4, pp. 839–848, Apr. 2013.
[47] Y. Dobrev, P. Gulden, and M. Vossiek, "An indoor positioning system based on wireless range and angle measurements assisted by multi-modal sensor fusion for service robot applications," *IEEE Access*, vol. 6, pp. 69036–69052, 2018.
[48] Q. Li, W. Li, W. Sun, J. Li, and Z. Liu, "Fingerprint and assistant nodes based Wi-Fi localization in complex indoor environment," *IEEE Access*, vol. 4, pp. 2993–3004, 2016.
[49] Z. Li, Z. Xiao, Y. Zhu, I. Pattarachanyakul, B. Y. Zhao, and H. Zheng, "Adversarial localization against wireless cameras," in *Proc. 19th Int. Workshop Mobile Comput. Syst. Appl.*, 2018, pp. 87–92.
[50] L. Oliveira, J. Henrique, D. Schneider, J. de Souza, S. Rodriques, and W. Shen, "Sherlock: Capturing probe requests for automatic presence detection," in *Proc. IEEE 22nd Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, May 2018, pp. 848–853.
[51] T. Yoshida and Y. Taniguchi, "Estimating the number of people using existing wifi access point in indoor environment," in *Proc. 6th Eur. Conf. Comput. Sci. (ECCS)*, 2015, pp. 46–53.
[52] L. Oliveira. (2019). *Sherlock*. [Online]. Available: https://github.com/luizsoliveira/sherlock

LUIZ OLIVEIRA (M'15) was born in Três Rios, Rio de Janeiro, Brazil, in 1987. He receives the B.S. and M.S. degrees in computing from Federal Fluminense University, Niterói, in 2008 and 2013, respectively. He is currently pursuing the Ph.D. degree in computer engineering with the Federal University of Rio de Janeiro, Rio de Janeiro.

From 2009 to 2013, he was a Research Assistant with the UFF Midiacom Laboratory. From 2014 to 2016, he was a Research Assistant with the UFRJ Capgov Laboratory. Since 2017, he has been a Research Assistant with UFRJ Future's Laboratory. Since 2016, he has been an Assistant Professor with the Federal Institute of Rio de Janeiro, Niterói. His research interests include occupancy detection, mobile crowd sensing, participatory sensing, the Internet of Things, and the electronic prototyping of hardware.

DANIEL SCHNEIDER received the degree in computer science from IM–Federal University of Rio de Janeiro (UFRJ), in 2001, and the master's and Ph.D. degrees in computer engineering from COPPE–UFRJ, in 2004 and 2015, respectively. He is a Full Professor in computer science with UFRJ, focusing on the following subjects: databases, human–computer interaction, crowdsourcing, social computing, and CSCW.



JANO DE SOUZA graduated in mechanical engineering from the Universidade Federal do Rio de Janeiro, in 1974, the master's degree in computer science from COPPE-Universidade Federal do Rio de Janeiro, in 1978, and the Ph.D. degree in information systems from the University of East Anglia, in 1986. He was with Sabbatical leave at CERN from 1989 to 1993 (3 months a year). His researches and teaches in computer science, focusing on the following subjects: databases, knowledge management, social networks, CSCW, autonomic computing, and negotiation support systems.

WEIMING SHEN (M'98–SM'02–F'12) received the bachelor's and master's degrees from Northern (Beijing) Jiaotong University, China, in 1983 and 1986, respectively, and the Ph.D. degree from the University of Technology of Compiegne, France, in 1996. He is currently a Principal Research Scientist with the National Research Council Canada (on leave), a Professor with the Huazhong University of Science and Technology, China, and an Adjunct Professor with the University of Western Ontario, Canada. His research interests include intelligent software agents, service-oriented computing, wireless sensor networks, the IoT, and big data. He is a Fellow of Canadian Academy of Engineering and of the Engineering Institute of Canada, and a Licensed Professional Engineer in ON, Canada.