Know Thy Quality: Assessment of Device Detection by WiFi Signals

Tim Rütermann
University of Bamberg, Germany
tim-daniel.ruetermann@stud.uni-bamberg.de

Aboubakr Benabbas
University of Bamberg, Germany
aboubakr.benabbas@uni-bamberg.de

Daniela Nicklas
University of Bamberg, Germany
daniela.nicklas@uni-bamberg.de

***Abstract*—Broadcasted WiFi traffic of mobile devices is the foundation of several estimation techniques like location tracking or crowd counting. Many pervasive applications use these techniques to infer the current state of an environment allowing better planning of resources. A vast majority of techniques use WiFi probe request frames, which contain the unique MAC address of a mobile device. This MAC address allows counting of unique devices and thus, their carriers. To ensure privacy, device manufacturers introduced MAC randomization as anonymization technique. This causes a considerable impact on the data quality of many pervasive applications as randomizing devices create fake MAC addresses. Previous works show that randomized MAC addresses can be linked to their origin device using different derandomization techniques. However, these approaches are not feasible in practice as novel randomization techniques are designed to prevent derandomization. Moreover, the frequency of WiFi probe request frames varies significantly on several factors making it difficult to estimate device presence in a timely manner. This paper assesses the challenges with probe request frames using a new data quality framework for device detection. Additionally, alternative detection methods that do not rely on probe request frames are presented. This includes a recently publicized WiFi device detection technique and a new way of detecting devices associated with a third-party network using a feature of the 802.11 protocol.**

I. Introduction

With the emergence of different sensor types and their increasing capabilities, pervasive computing has become the major topic over the past years to revolutionize the management of resources, like required working staff [4] or public transport [5]. This management relies heavily on knowledge about the real world which is provided by a set of sensors. For instance, by monitoring an area, it is possible to create a multitude of useful insights about a population like movement patterns or the number of occupants. These insights can be used by private and public facilities to provide more efficient and reliable services, like recommendation systems for evacuation scenarios [6], [15] or physical as in public transport optimization by anticipating pedestrian volume and flow [5]. Moreover, retailers can organize their stores and improve business by evaluating which spots were visited by more customers and whether a visitor returned [7].

Although crowd counting has been the topic of numerous scientific works, there exists no state-of-the-art approach [1]. One explanation is that the method of choice is highly dependent on the constraints of the deployment scenario. For example, counting people with cameras requires many installations, does not allow monitoring through walls and may raise privacy concerns. Less invasive alternatives like crowd counting using light inferences [14] can be very precise for small crowds in indoor environments but do not perform well on scenarios with larger crowds.

A promising approach which overcomes these challenges is WiFi-based crowd counting. WiFi signals can not only pass through walls but monitoring sensors are also cost-effective to install. With the continuous adoption of mobile devices like smartphones or smartwatches it has never been easier to track people and create useful insights about crowds. The method of choice for crowd counting with WiFi signals can be either device-free methods or device-based. Device-free methods measure the variance in received signal strength caused by people blocking the signal path between a sender and receiver [8], [16]. These methods are very privacy-protective but become imprecise with increasing size of the crowd and are dependent on the movement of persons.

In contrast, device-based methods measure and analyze the emitted WiFi traffic of devices, assuming they are carried by people [4]. I.e., a wide range of works successfully used broadcasted probe request frames to count and track devices [4], [6] [10]. However, this poses major privacy issues which have to be considered by including anonymization techniques or Privacy by Design principles on application side [11].

The protection of privacy has only recently resulted in mandatory laws like the data protection law of the European Union by declaring MAC Addresses as personal data. Instead of entrusting the application side with privacy measures, many device manufacturers introduced MAC randomization as preemptive privacy technique [1] [11]. Furthermore, manufacturers made efforts to conceal device presence by reducing the frequency of probe requests. As a result, this paper focuses on the impact of current MAC randomization implementations and varying probe frequency on data quality and proposes alternative methods for device detection.

Problem Statement

Privacy protection techniques for WiFi traffic lead to specific problems when trying to track or estimate the number of devices in an area. In order to build a robust crowd counting application, the following problems need to be considered:

Fake Devices: How can we relate monitored probe requests to devices? Before MAC randomization, each MAC address

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

could be mapped to its source device in a 1:1 relationship. However, a device with active randomization scheme can produce multiple probe requests with different MAC resulting in a 1:N relationship between device and probe request MACs. This produces a significant error when trying to count the number of unique devices based on probe requests.

Detection Latency: When do we detect a device? The frequency of probe requests is dependent on WiFi connection status, manufacturer, energy mode and level of user interaction resulting in a wide range of probing behaviors. At worst the device is never seen even if it stayed for a reasonable amount of time in the sensing area. Additionally, some devices reduce the number of probe requests to a minimum when connected to a network. Furthermore, probe requests do not allow the determination of device absence which requires systems to estimate when a device supposedly has left the area. Since probe frequency varies considerably, this approach can cause either an over- or underestimation error of device presence.

Device-Person Mapping: How can we relate detected devices to people? Depending on their context some persons might not have their WiFi activated or do not carry a device at all making them invisible to mobile WiFi detection. Moreover, one person can carry a multitude of different WiFi capable devices like business phones, laptops, smartwatches or reading pads. Hence some persons and their devices are never sensed while others are recognized as multiple actors. This problem can be solved by comparing ground truth data with sensed devices and creating a model for estimating the error. Since this model relies on the correctness of the sensed devices its accuracy is highly dependent on the solution of Fake Devices and Detection Latency problems.

The influence of MAC randomization on the Fake Devices problem can be minimized by using derandomization techniques as presented in several recent works [1] [11]. Nevertheless, the success of such techniques is highly dependent on the randomization degree used by manufacturers and remains ineffective considering state-of-the-art randomization. It also does not solve the problem of Detection Latency as the frequency of probe requests cannot be influenced by a third party. Hence this paper focuses on solutions which improve data quality even when randomization is implemented correctly and probing frequency is low.

In this paper, we take a close look at the impact of MAC randomization on the data quality for crowd counting applications. We provide the following contributions for pervasive applications based on WiFi traffic:

- Introduction of data quality metrics for the task of WiFi-based device counting
- Insights on the behavior and impact of state-of-the-art MAC randomization
- Evaluation of a recently publicized approach for active device detection despite randomization
- Presentation and evaluation of a feature in the 802.11 protocol allowing real-time detection of devices connected to a third-party network

We provide explanations on how these findings solve problems with Fake Devices and Detection Latency using experimental data. Moreover, we make real-world assumptions often overlooked by other crowd counting papers such as different device contexts. For instance, the estimation of devices and crowds is highly dependent on whether devices are associated with a network. To the best of our knowledge, we are the first to show how a particular feature of the 802.11 standard can be used to detect devices in an associated state. Furthermore, we present a novel way to assess data quality for device counting purposes within different contexts.

II. Related Work

Although multiple works used WiFi traffic to count crowds [4], [6], none of them explore the impact of MAC randomization on data quality in depth. In practice, most applications focus on solving the Device-Person Mapping directly by using ground-truth data and raw probe request observations instead of trying to solve the Fake Devices and Detection Latency problems first. This works only as long as devices with MAC randomization represent a minority. This seems unlikely considering the continuous adoption among device manufacturers [11]. Hence, analyzing and defeating MAC randomization was covered by various recent papers.

The work of Musa et al. [17] presents first passive and active methods for device detection. Unfortunately, their work does not cover MAC randomization as it was only in recent years widely adopted among manufacturers. A comprehensive study on probing behavior was conducted by Freudinger [2] in various experimental settings. He showed that probing frequency is dependent on a multitude of factors like manufacturer, battery level, user interaction and number of stored access point SSIDs. Although MAC randomization was not widely established across manufacturers during the time of the experiments he observed randomized probe requests by an Apple IOS 8 device. Furthermore, he explored the first possibilities for relating a randomized probe to its original device by using particular packet fields like Sequence Numbers or WiFi Protected Setup (WPS) information. Vanhoef et al. [3] explored different methods for relating a single or multiple observed randomized MAC to its source device enabling location tracking and counting. The proposed methods make use of different packet fields which provide useful information about device identity. For instance, the WiFi Protected Setup (WPS) field of a probe request can be used to link randomized probe requests to their source device. Additionally, they provided a method using the Sequence Number Field which is increased for every new probe request creating a link between two probes from the same device. To prevent such derandomization methods, privacy-protective device manufacturers removed the WPS content field and the incrementation of sequence numbers. The work of Martin et al. [1] and Matte [11] provide a good overview of both active and passive derandomization techniques. Moreover, Martin et al. claim to have found a way to actively derandomize 100% of devices across all manufacturers using customized

WiFi control frames. Their remarkable findings have been picked up by several computer and security blogs without further investigations. Since this method could enable location tracking and counting of devices despite randomization, it would be perfectly suitable for improving data quality in crowd counting applications. As a result, this paper assesses the proposed method thoroughly with regards to its applicability.

III. Preliminaries

In order to assess the effectiveness of certain methods, one must first define how data quality can be measured. As a first step, we decided to focus solely on the task of crowd counting as possible application scenario. Generally, a crowd counting application will be evaluated by the error α between estimated crowd size γ and true crowd size θ at a certain point of time. Therefore, such applications try to reduce α in:

$$\theta = \gamma + \alpha \tag{1}$$

Whereas, γ is estimated by counting the number of WiFi-enabled devices δ multiplied with a device distribution ratio β. This ratio reflects the fact that people carry either single, multiple or no detectable devices. As a result, γ is defined as:

$$\gamma = \delta \cdot \beta \tag{2}$$

Usually, β is acquired through learning with ground-truth data or representative surveys. As β belongs to the device-mapping problem it will not be explored further in this work. Instead, δ will be the key metric to assess data quality as it is strongly affected by the fake devices and detection latency problems. For instance, a device might use multiple randomized MAC addresses which could be interpreted as multiple devices but actually belong to a single device. These false devices are defined as ϵ_{rand} and cause an overestimation of counted devices as shown in Fig. 1. The detection latency problem addresses errors with the timeliness of detection. Since packets are only proof of presence for a single point of time, it might be the case that a device has been present but not detected yet. This causes an underestimation error of counted devices. Likewise, a device may have already left the sensing area and is still considered to be present resulting in an overestimation error. Both of these timely estimation errors belong to the detection latency problem and are defined as ϵ_{lat}. Assuming that μ is the set of devices that are present and correctly detected and thus do not belong to ϵ_{rand} or ϵ_{lat} the estimated number of devices δ can be defined as:

$$\delta = \mu + \epsilon_{rand} + \epsilon_{lat} \tag{3}$$

This data quality definition allows us to examine the impact of each data quality improving method on different aspects of device estimation. A problem occurs when using these data quality metrics for an experiment over time as they hold only for a single instance of interest. To solve this problem, we extended the definition by averaging each metric resulting in:

$$\overline{\delta} = \overline{\mu} + \overline{\epsilon_{rand}} + \overline{\epsilon_{lat}} \tag{4}$$

At last, we additionally defined τ as the true amount of WiFi-enabled devices in our experiments. This enables us to calculate the overall accuracy of device estimation with the Root Mean Square Error (RMSE) between δ and τ.

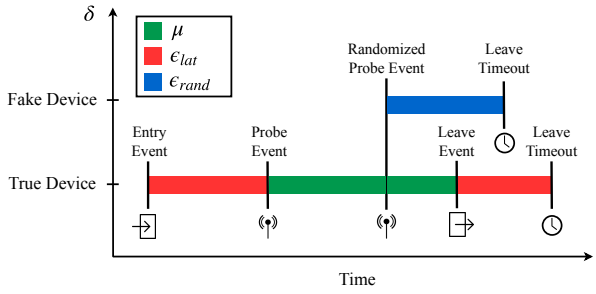


Fig. 1: Visualization of Data Quality Metrics

IV. Novel Detection Methods

To overcome the challenges of MAC randomization and low probe request frequency, new detection methods should be considered. As a result, we present novel ways to detect devices based on additional WiFi packets that are yet not affected by privacy measures.

Control Frame Attack. Martin et al. [1] presented the Control Frame Attack for detection of devices with and without active randomization. It is based on the idea that by sending WiFi frames to the universal MAC one can elicit a broadcasted response. This response is proof that the targeted device must be present in the vicinity of the monitoring station. The only requirement for this ping technique is the prior retrieval of the target universal MAC. This is achieved by monitoring probe requests which occasionally contain the universal MAC of the device. This method would allow active scanning for previously seen devices. As a result, the overestimation error ω of device presence is reduced because no more responses will be monitored after the device has left the area.

According to Martin et al. [1] this attack can be carried out by targeting devices with Request-To-Send (RTS) frames and listening to corresponding Clear-To-Send (CTS) responses. The RTS/CTS technique as specified by the IEEE 802.11 [9] was initially designed to reduce possible collision of WiFi frames (the so-called Hidden Node Problem). This occurs when two nodes communicate with an AP in their range but are too far away to sense the presence of the other node.

In order to avoid transmission collisions, each node may request with an RTS message a transmission permit from the AP. The AP can grant this permit by responding with a CTS frame. Both RTS and CTS frames contain a target MAC Address which can be used to detect the presence of devices similar to probe requests. Interestingly, RTS messages can also be sent to nodes or mobile devices in general to induce a CTS response. Devices can be tricked into revealing themselves by creating an RTS frame that contains the target device MAC as source and destination. In theory, a device should respond to that RTS frame with a CTS frame containing the device's own universal MAC as destination field. By monitoring these

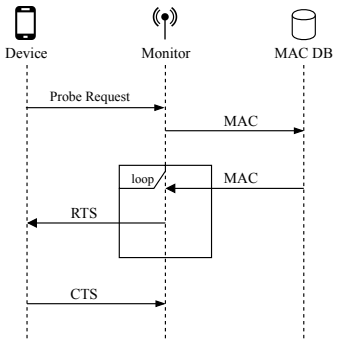


Fig. 2: RTS/CTS Device Scan

CTS messages the presence of a previously targeted device is proven despite active MAC randomization. An overview of this approach is shown in Fig. 2. We tested this approach with three different randomizing devices Motorola 5s+, IPhone SE and LG Nexus 5X using the packet sniffing and crafting libraries Scapy and Libtins as proposed by Martin et al. [1]. They confirmed the attack to be 100% successful independent from association state to a WiFi network without giving a definition for success. We define this success with their proposed attack purpose which is to "*elicit a specific response from them at any time if they are within wireless range*" [1, p. 15]. Regarding this definition, we have to conclude that the attack does not work as devices will not respond at any time but only under certain conditions. We conducted our tests for this attack at different places like the university laboratory and private living spaces where other WiFi networks were present.

We observed during our tests that a device only responds to RTS messages targetting its MAC upon sending out a probe request with that MAC. As a result, an RTS targetting the universal MAC is ignored when the device sends out a probe request with a randomized MAC. Interestingly, the device will answer RTS targetting the randomized MAC. We conclude from this behavior that the randomized MAC overwrites the universal MAC in the Network Interface Controller (NIC) for a short time, thus ignoring RTS targetting the universal MAC even during active probing.

Aside from these technical limitations, this approach may interfere with privacy protection regulations as MAC addresses have to be stored and sent out again. I.e., under the new European data regulation law [12] it seems unlikely that we can use previously seen MAC addresses in such an unintended way.

Protective Mode Monitoring. Protective Mode Monitoring is a new method for detection of devices that are associated with an AP by monitoring additional frames besides probe requests. We can detect devices that have a very low probing frequency or do not probe at all. During our experiments, we tried to find packets other than probe requests to detect device presence. To our surprise, we were able to see frequently RTS/CTS and acknowledgment (ACK) frames containing the universal MAC of devices. In order to elaborate why these frames were sent only in certain locations we checked if there were different compositions of available WiFi networks. We identified the coexistence of networks with different 802.11 WiFi standards as a trigger condition for the exchange of RTS/CTS and ACK messages.

The IEEE 802.11 norm evolved to different development standards a/b/h/g/n/ac [9]. The latest release was the ac standard in 2013 with the goal of providing high-throughput rates on the 5 GHz band and is therefore also known as Very High Throughput (VHT) mode. In contrast, older standards are described as High Throughput (HT) modes. During our experiments, we noticed that the vast majority of WiFi networks in our university and different public spaces belong to the HT mode type. We explain this distribution with the lack of demand for VHT mode and the resulting slow adoption of supporting routers. Without going further into detail on the fundamental differences between HT and VHT transmissions, it should be noted that a router with VHT mode can not process HT transmissions. To prevent issues with data frame transmissions in mixed environments with VHT and HT networks, devices can be prompted to operate in a so-called protected mode. By setting protection fields in probe responses and beacon frames, a VHT access point announces its presence and triggers the protected mode in nearby associated devices if an HT AP is also present. Upon operating in protected mode, an AP or device will use an RTS-CTS-ACK handshake for data transmissions as depicted in Fig. 3.

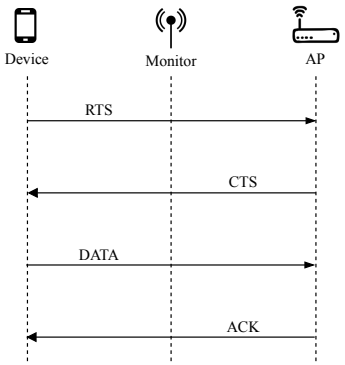


Fig. 3: RTS/CTS/ACK Handshake Initiated by Device

During our experiments, we observed that this handshake can be initiated by both parties. As a result, the device MAC will always appear in either the source or destination of an RTS message. Since CTS and ACK messages have only a destination MAC, the device MAC will only appear in them if the device initiated the handshake. Although CTS and ACK messages can also be used for device detection, we found the frequency of RTS messages enough for real-time location tracking purposes which also saves packet processing overhead on the application side.

To use this detection method, a monitoring application must assure that the conditions for protected mode are fulfilled. We achieved this by setting up an 802.11ac (VHT) network in an environment where 802.11 a/b/g/n (HT) networks already exist. Likewise, an HT network must be created if only

VHT networks are present. Since APs advertise their presence with beacons and probe responses it should be also possible to simulate such networks using only crafted WiFi frames. This would allow triggering the protected mode and detection of devices associated with third-party networks without the installation of additional hardware. Finally, this method of detection cannot be countered with techniques like MAC randomization as the RTS/CTS handshake only works with the true device MAC. Furthermore, in an associated state, no MAC randomization is employed due to possible WiFi communication problems in general. The only option would be to disable the protection mode by the manufacturer which seems unlikely since it is defined in the 802.11 standard itself.

V. Evaluation

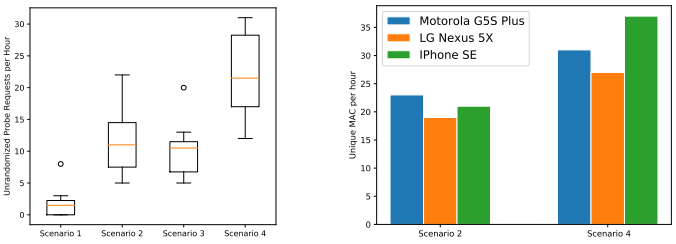
The goal of our evaluation was to show how the quality of device counting with probe requests is affected by MAC randomization and varying probing frequency. We used a controlled setting with a limited amount of devices to highlight how a small subset of devices can influence the estimation accuracy. In contrast to other works, we specifically focus on four different scenarios which are dependent on the deployment environment and strongly impact the estimation process but are often overlooked.

Experimental Design. The scenario metrics are the WiFi association states of mobile devices and whether the carrier interacts with a device as shown in Table I. These four different scenarios systematically cover the main contexts of devices. We simulated device usage by unlocking the screen every 5 minutes for 30 seconds and opening an app. For example in Scenario 1, the user interacts with the device regularly and the device is associated with a present WiFi.

To examine the impact of different probing frequencies and MAC randomization we evaluated the detection accuracy in a 40 minutes experiment with our devices. Entry and leave events of devices were simulated by adding and removing two devices every 5 minutes to the monitoring area. The experiment was initiated with zero devices. Then, devices were iteratively added until all devices were present. After the entry phase, devices were again repetitively removed. This approach allows us to examine the different errors regarding device over- and underestimation ϵ_{lat} and randomization error ϵ_{rand}. The overall detection accuracy was measured as RMSE between the true and estimated number of devices.

Results. As a first step, we analyzed the variation of probing frequency for each scenario to highlight the impact of association state and user interaction on probing behavior. As presented in Fig. 4a, Scenario 1 had the least probes per hour as devices tend to probe less without interaction and during an associated state. The impact of the association state is highlighted by the plot for Scenario 2 as user interaction remains the same and association state is changed to unassociated.

In Scenario 3, the probing frequency is similar to that of Scenario 2 as user interaction increases probing frequency and the associated state reduces it. Generally speaking, association state and user interaction can either boost or decrease probing



(a) Unrandomized Probe Request Frequencies

(b) Randomized Unique MAC per Hour

Fig. 4: Overview of Probe Request Behaviour

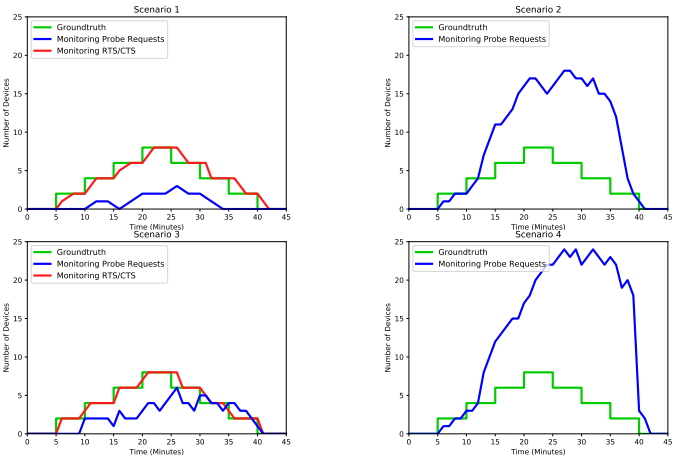


Fig. 5: Device Detection Experiments

frequency. As a result, the probing frequency in Scenario 4 is the highest due to the increasing effect of user interaction and devices being in an unassociated state. From these results, we infer that the detection of single devices and their carriers is strongly dependent on their environmental context.

Next, we present the magnitude of randomizing MAC in Fig. 4b which shows that devices can create a large set of unique MAC. In order to minimize the error ϵ_{rand} which represents randomized MAC in the data quality definition this would require either filtering or further processing of such MAC. As there exist no state-of-the-art approaches that are capable of identifying randomized MAC in the first place, it is unclear how they can precisely filtered or processed. Fig. 4b shows only Scenario 2 and 4 as devices in an associated state did not produce any randomized MAC. Interestingly, user interaction significantly increased the number of randomized MAC. We assume that devices interpret user activity as an indicator for a possible change of location and thus need to probe more often for new networks.

In Table I and II, we present the data quality (DQ) metrics for all scenarios using either probe requests or the CTS/RTS based approach for device detection. Please note that protective mode monitoring only works for devices in an associated state and is therefore only applied in Scenario 1 and 3. Additionally, in Fig. 5 we provide the device estimation for all scenarios.

In Scenario 1 the number of devices was constantly underes-

timated as the decreased probing frequency reduces the overall detection accuracy. Not only are some devices never seen but also late detected or it is falsely assumed that they have left after the chosen leave timeout of 5 minutes. Increasing the leave timeout will lead to overestimation and increase error further in environments with different scenario types. In contrast, using additional frames in the improved method results in a far better device estimation. The RMSE was reduced by 35% using the CTS/RTS approach due to the increase in correct detected devices $\overline{\mu}$ from 2.3 to 7.1. The detection latency error $\overline{\epsilon_{lat}}$ was also reduced by 87% from 5.47 to 0.93 as devices could be detected in a more timely manner. The metric $\overline{\epsilon_{rand}}$ was zero for both approaches devices do not use randomization in an associated state. Compared to the results of Scenario 3, the metrics slightly improve for both approaches solely due to the increased probe frequency. Especially, the probe request approach benefits much more from increased packet frequency as RTS/CTS message frequency is already high enough even without user interaction.

The data quality metrics for Scenario 2 and 4 highlight the issues with MAC randomization as $\overline{\epsilon_{rand}}$ clearly outweighs $\overline{\epsilon_{lat}}$. Although correct device detection $\overline{\mu}$ is with 5.27 for Scenario 2 and 5.88 for Scenario 4 higher than for all other scenarios, the RMSE is significantly increased because of $\overline{\epsilon_{rand}}$. The simulation of user interaction had the biggest impact on the RMSE in Scenario 4. This can be explained by the additional randomized probe requests that are sent out upon screen unlock resulting in a higher randomized probe frequency and $\overline{\epsilon_{rand}}$ compared to Scenario 2.

VI. Conclusion & Future Work

We have shown that the data quality of device detection is highly reliant on the context of crowd counting environment. In scenarios where devices are connected to WiFi infrastructures, like universities and shopping malls it is more difficult to detect devices unless our proposed protected mode monitoring method (PMM) is used. Likewise, the absence of WiFi structures leads to more devices in an unassociated state increasing the probing frequency but also creating a lot of noise due to randomized probe requests. As PMM does not work in unassociated state, crowd counting systems can only rely on probe requests and need to take care of randomized MAC addresses. Although the RTS/CTS attack did not work as intended it shows that there are ways to actively search for devices by taking advantage of 802.11 protocols.

Regarding data quality, we hope to see a clearer focus on the different scenarios in crowd counting and device detection. Our presented data quality metrics and scenario types allow a clear comparison regarding the effectiveness of different methods and approaches. Additionally, the metrics can be extended to reflect additional factors that not have been considered yet. We strongly believe that WiFi crowd counting requires such metrics to assess error sources and find proper detection methods. After all, only if you know thy quality you may be able to find appropriate strategies.

TABLE I: DQ Metrics for Probe Request Monitoring

scenario	WiFi state	usage	RMSE	$\overline{\mu}$	$\overline{\epsilon_{rand}}$	$\overline{\epsilon_{lat}}$
1	associated	no	3.43	2.3	0	5.47
2	unassociated	no	7.39	5.27	13.4	1.97
3	associated	yes	2.25	4.12	0	3.4
4	unassociated	yes	12.52	5.88	18.58	1.6

TABLE II: DQ Metrics for Protective Mode Monitoring

scenario	WiFi state	usage	RMSE	$\overline{\mu}$	$\overline{\epsilon_{rand}}$	$\overline{\epsilon_{lat}}$
1	associated	no	1.23	7.1	0	0.93
3	associated	yes	0.94	7.32	0	0.86

References

[1] J. Martin, T. Mayberry, C. Donahue, L. Foppe, L. Brown, C. Riggins, E. Rye and Dane Brown, "A Study of MAC Address Randomization in Mobile Devices and When it Fails," Proc. on Privacy Enhancing Technologies, 2017 (4), 365-383

[2] J. Freudinger, "How talkative is your mobile device?: an experimental study of Wi-Fi probe requests," Proc. of the 8th ACM Conf. on Security & Privacy in Wireless and Mobile Networks, ACM, 2015.

[3] M. Vanhoef, C. Matte, M. Cunche, L. Cardoso, and F. Piessens, "Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms," ACM AsiaCCS, 2016.

[4] A. Ruiz-Ruiz, H. Blunck, T. Prentow, A. Stisen and M. B. Kjaergaard, "Analysis methods for extracting knowledge from large-scale WiFi monitoring to inform building facility planning," IEEE PerCom, 2014.

[5] M. Elhamshary, M. Youssef, A. Uchiyama and T. Higashino, "CrowdMeter: Congestion Level Estimation in Railway Stations Using Smartphones," IEEE PerCom, 2018.

[6] N. Ahmed, A. Ghose, A. Agrawal, C. Bhaumik, V. Chandel and A. Kumar, "SmartEvacTrak: A people counting and coarse-level localization solution for efficient evacuation of large buildings," IEEE PerCom Workshops, 2015.

[7] O. Perdikaki, S. Kesavan and J. Swaminathan, "Effect of traffic on sales and conversion rates of retail stores," Manufacturing and Service Operations Management, 14/1, pp.2012.

[8] S. Depatla and Y. Mostofi, "Crowd Counting Through Walls Using WiF," IEEE PerCom, 2018.

[9] 802.11ac-2013 - IEEE Standard for Information technology– Telecommunications and information exchange between systemsLocal and metropolitan area networks– Specific requirements–Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications–Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz.

[10] M. Wirz, T. Franke, D. Roggen, E. Mitleton-Kelly, P. Lukowicz and G. Tröster, "Probing crowd density through smartphones in city-scale," EPJ Data Science, 2013.

[11] C. Matte, "Wi-Fi Tracking: Fingerprinting Attacks and Counter-Measures," Université de Lyon, 2017.

[12] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

[13] M. Cunche, J. Zuniga, M. Vanhoef and C. Matte. "Privacy issues in 802.11 networks," doc. IEEE 11-16-1492-00-0wng, 2016.

[14] Y. Yang, J. Hao,J. Lua and S. Pan, "CeilingSee: Device-Free Occupancy Inference through Lighting Infrastructure Based LED Sensing," IEEE PerCom, 2017.

[15] M. Murata, D. Ahmetovic, D. Sato and H. Takagi, "Smartphone-based Indoor Localization for Blind Navigation across Building Complexes," IEEE PerCom, 2018.

[16] R. Lim, M. Zimmerling, and L. Thiele, Passive, "Privacy-preserving Real-time Counting of Unmodified Smartphones via ZigBee Interference," Intl. Conf. on Distributed Computing in Sensor Systems, pp. 115-126, 2015.

[17] A. Musa, J. Eriksoson, "Tracking Unmodified Smartphones Using Wi-Fi Monitors," Proc. of the 10th ACM Conf. on Embedded Network Sensor Systems, pp. 281–294, 2012.