Crowding Detection Combining Trace Elements from Heterogeneous Wireless Technologies

Rúben Dias da Silva
Lisboa, Portugal
ruben02b@gmail.com

Rui Neto Marinheiro
Instituto de Telecomunicações
Instituto Universitário de Lisboa (ISCTE-IUL)
Lisboa, Portugal
rui.marinheiro@iscte-iul.pt

Fernando Brito e Abreu
ISTAR-IUL
Instituto Universitário de Lisboa (ISCTE-IUL)
Lisboa, Portugal
fba@iscte-iul.pt

***Abstract*—Non-invasive crowding detection in quasi-real-time is required for a number of use cases, such as for mitigating tourism overcrowding. The present goal is a low-cost crowding detection technique combining personal trace elements obtained from heterogeneous wireless technologies (4G, 3G, GSM, Wi-Fi and Bluetooth) supported by mobile devices carried by most people. This work proposes detection nodes containing Raspberry-Pi boards equipped with several off-the-shelf Software Defined Radio (SDR) dongles. Those nodes perform spectrum analysis on the bands corresponding to the aforementioned wireless technologies, based on several open source software components. The outcome of this edge computing, performed in each node, is integrated in a cloud server using a Long Range Wide Area Network (LoRaWAN), a recent technology developed for IoT applications. Our preliminary results show that is possible to determine the number of mobile devices in the vicinity of each node, by combining information from several wireless technologies, each with its own detection range and precision.**

***Index Terms*—Crowding Detection, 4G, 3G, GSM, Wi-Fi, Bluetooth, SDR, LoRaWAN**

I. Introduction

According to [1], smartphones penetration in most western European countries during 2018 was in the range of 75% to 85% of the population. In these countries, the number of smartphones in a given area is, therefore, a good surrogate of the actual number of people in that area. Smartphones (and wearables, despite being still much less used) have a wireless footprint since, in their normal usage, they irradiate information due to the communication protocols they support. Even when that information is encrypted, it still can be used for crowding detection. In fact, we are not interested in the exchanged contents (voice or data) since we want to guarantee user privacy and anonymity, but solely on the detection of wireless trace elements that allow us to infer that a mobile device is operating in the vicinity. Those trace elements are generated by wireless protocols (4G, 3G, GSM, Wi-Fi and Bluetooth), each operating in specific bands of the electromagnetic spectrum. We detect the activity in each of those bands using off-the-shelf SDR dongles connected to a Raspberry Pi, where several spectrum analysis techniques are executed, based upon open-source software components. This corresponds to the edge computing phase of our distributed detection solution, bringing computation and data storage closer to the location where it is needed, to improve response times and save communication bandwidth. The cloud computing phase, performed in a cloud server, concerns how the detection data from multiple detection nodes is combined to provide a picture of the crowding distribution in the geographical area under observation.

The application domain that motivated our research was in tourism, where smart solutions are sought for mitigating the pressure felt, both by residents and visitants, due to overcrowding of some historic neighborhoods [2]. We are developing an alternative routing recommendation system for tourists that mitigates overcrowding trough their dispersion, while promoting the visitation of sustainable points of interest. Our solution innovates by having a crowding detection approach that combines trace data from heterogeneous wireless technologies, collected in real-time with off-the-shelf equipment and open source hardware and software.

This paper is organized as follows: section II describes related work in crowding detection; section III introduces the architecture of our solution; section IV describes the hardware and software used in our proposal; section V presents our validation and section VI addresses conclusions; finally, section VII presents ongoing and future work.

II. Related work

Crowd detection can be addressed using several approaches, such as image capturing, social networks, mobile operators data, and wireless spectrum analysis, with different capabilities in terms of range, precision and timeliness of detection 1. As for the latter, we consider a rough ordinal scale: “near real-time processing" (wireless spectrum analysis and sound capturing), “delayed results" (image capturing and mobile operators cell tower trace data, both requiring intensive computation, not amenable to produce immediate results) and “post facto analysis" (e.g. social networks based data analysis where, due to data capture delays and post processing of big data, results may take long hours, or even several days, to be produced).

Near real-time approaches are a prerequisite when immediate action is required. For retrospective analysis of the crowding phenomenon, all alternatives are acceptable, so only the range and precision aspects should be a concern. A brief review of each approach follows.

1) Image capturing approach: This approach may use a dedicated or existent network of cameras, usually required for

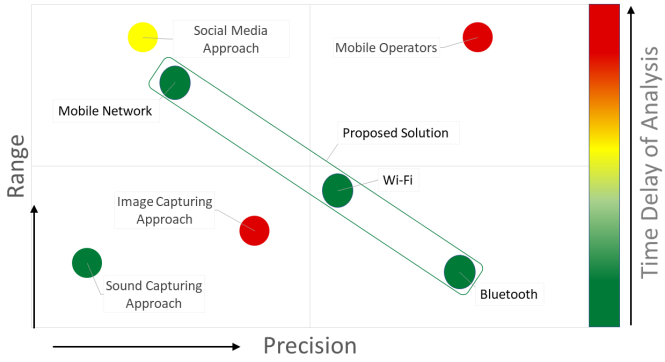

Figure 1. Quadrant analysis of the different approaches

security purposes in major cities (aka video-surveillance), to detect the number of individuals and their behaviour in the view range of cameras. Image processing and analysis is then performed using several techniques [3–5].
Besides requiring good quality cameras, this is a compute-wise demanding procedure, not amenable for edge computing. Communication costs between the sensor nodes and image processing servers (e.g. in the cloud) may be significant. Furthermore, this approach raises serious privacy concerns, requiring complex authorization procedures, since captured images of individuals can be used for identification purposes, either directly or indirectly (i.e. combined with other pieces of information).

2) Sound capturing approach: Another approach, already tested in some cities [6], uses a network of distributed sound sensors. Sensors gather ambience sounds including those emitted by people, cars, trains, etc. That information is then processed in the cloud, to generate heat maps. Preliminary analysis may be performed to isolate different sound sources [7] and then further processing takes place to determine people or cars density, in the sensor's range [8]. Compared to image processing, this approach is less demanding regarding computational power and network bandwidth. However, achieved precision and detection range is much lower (see Fig. 1) and it also raises similar privacy problems, since conversations may be recorded and transmitted to the cloud. A combination of image and sound processing has also been considered [3].

3) Using social networks activity: This approach uses information published in social networks [9–11]. Geo-location data of photos, tweets or other social media contents can be used to infer the number of individuals present in target areas. Instagram, for instance, is an interesting source of data used by researchers, because photos are usually posted along with location data. One of these kind of studies gathered info from posts in New York city in real-time and tried to aggregate them in clusters to analyze the flow of people in the city [11].
Another study combined, almost in real time, information gathered from Twitter and Instagram, using low-cost processing procedures [10], in order to analyzed it, using several filters, in the generation of several metrics for user distribution. This approach is dependent on data published by social media users. The fact that only a fraction of that data has public access permission, and not all of it is tagged with geo-location info, are strong validity threats regarding the representativeness of the actual crowding in target areas.

4) Using mobile operators' data: Mobile operators have at their disposal huge amounts of data regarding the usage of their networks, but the challenge presented in this type of approach is to generate relevant metrics using those big data sets. The real problem is to generate real time data that could, for example, detect crowds in confined areas.
Spanish's Telefonica [12] has invested in processing historical data, namely for prediction of future movement patterns. Vodafone Analytics[1] is a well-known example of this exploration of data and provides a set of metrics and their evolution over time. The metrics are usually presented in geo-referenced maps, where spacial-temporal evolution analysis is possible. Portuguese's operator NOS used data from roaming devices to build a Tourist Information Portal[2] that offers several indicators to allow business owners to identify potential target areas and municipalities across the country to analyze how to allocate resources more efficiently.

5) Using wireless spectrum analysis: Early works, such as [13], have analyzed the architecture of different indoor positioning systems and discussed the properties and drawbacks of solutions supported by smartphones. Most solutions used an active positioning approach and require willing users to install an app. Alternatively, passive monitoring is possible by the owner of the communication platform (see previous section). However, when that is not the case, third parties have resort to wireless spectrum and protocol analysis. The evolution and increasing affordability of SDR and open source hardware and compatible open source software has allowed for a more flexible spectrum and protocol analysis and has speed up research on wireless eavesdrop and active detection approaches. These approaches usually explore protocol characteristics and/or small security leaks of information. Previous research works were usually focused on a specific wireless technology, with its inherent trade-offs between range and precision. In our case we aim at mitigating those trade-offs, by combining several technologies, whose use for presence detection is thoroughly discussed in [14].
A few examples of the weaknesses, that can be exploited in some wireless technologies, will now be described.

GSM and 3G: In GSM, an attack may opportunistically take advantage of the lack of authentication of the base stations on the user equipment (UE) and IMSI[3] catchers or man-in-the-middle attacks are then possible [15]. Additionally, the communication may not be fully encrypted. The UE has to periodically transmit the current location, and this can be used to track and record usage and position [16]. In 3G, active attacks may also be performed by downgrading the connection to an insecure GSM link, and then explore its flaws.

[1] https://geographica.com/en/showcase/vodafone-analytics/
[2] http://customers.microsoft.com/en-us/story/nos-spgs-media-telco-azure-sql-r-server-portugal
[3] International Mobile Subscriber Identity

4G/LTE/5G: In 4G/LTE, the most interesting non-active exploit is a location leakage that occurs when the network has to respond to a paging request and decrypted information of users' location is exposed. Other active and passive attacks on 4G networks are also possible, as described in [17]. Although security features in 5G have been enhanced to prevent known protocol attacks, it is still possible to apply pre-authentication message-based exploits and to leverage Radio Network Temporary Identifier (RNTI) for user tracking [18].

Wi-Fi: UE with enabled Wi-Fi, periodically send messages, even when not attached to a network. These probe requests are an active mechanism to accelerate the connection process. This has been widely exploited to track user activities, using low-cost equipment, such as wireless-cards supporting monitor mode [19; 20]. Modern UE still continue to be very talkative regarding probe requests [21], although efforts have been made to develop privacy-preserving enhancements. One such initiative, whose adoption is not universal, is that probe requests are sent out with a randomized pseudonym identification that is changed periodically. This MAC address randomization also has some flaws [22] that can be exploited.

Bluetooth: With this technology, a variety of device discovery and fingerprinting techniques are possible [23]. Bluetooth classic is nowadays less viable for tracking UE. Nevertheless, it is still possible to track wearables using Bluetooth Low Energy (BLE). When compared to Wi-Fi, similar challenges regarding addresses randomization exist. Nonetheless, it is frequent to have a correlation between Wi-Fi and Bluetooth addresses, which may facilitate the merging of detections in counting people, our main objective.

III. Architecture of Proposed Solution

The development of this approach was driven by the tourism overcrowding problem faced by many historical neighbourhoods worldwide. The nature of these areas dictates the options that are most appropriate for the architecture. In particular, we need to: (i) have small-sized and non-intrusive detection nodes; (ii) deploy a large number of nodes, and so cost per node must be low; (iii) edge computing is required to merge and anonymize data from several radio sensors; (iv) keep communication costs low, by just sending the number of detected people every few minutes.

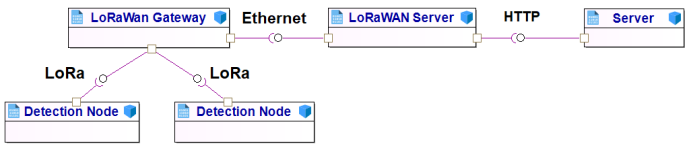

Figure 2. Component Diagram of Overall Architecture

Considering the above requirements, we propose the architecture of Fig 2, where light edge computing nodes communicate with the cloud server using LoRaWAN, a low management network with a very wide coverage, that reduces dramatically the cost of communications because its usage is free. Since the information to be passed on to the cloud server is small and the required sampling rate is low (consecutive messages will typically be a few minutes apart from each other), the low bandwidth characteristics of a LoRaWAN network is not a limitation for our architecture. Wi-Fi was not an option, because is not freely available in all areas of interest.

Each detection node, equipped with an IoT LoRa board and antenna, will upload data to a LoRaWAN gateway that, in its turn, will route the detection information to a cloud server, via a LoRaWAN server, for further processing and visualization of the crowding metrics generated in each node. Each detection node in the proposed architecture (Fig 3) contains a Raspberry-Pi based processing unit, with a set of connected sensors, such as a Wi-Fi dongle in monitor mode, a Bluetooth dongle or a GSM/3G/4G SDR dongle. Those USB dongles are responsible for capturing data in their respective technology, while the processing unit analyses and integrates locally all the captures, to compute one metric to estimate how crowded is the environment surrounding the node. A more detailed description of the solutions adopted for obtaining trace elements for each technology follows.

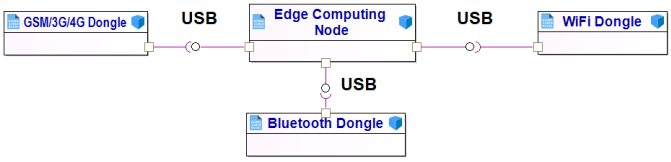

Figure 3. Component Diagram of Detection Node

IV. Tracking Wireless Technologies

Wireless technologies used by UE may have different limitations, but also potential, regarding detection. We advocate that detection nodes have to scrutinize several technologies simultaneously, to maximize detection opportunities. For instance, transmission power and frequency band (see Tab I) determines the potential range of detection. Low power and high-frequency such as Bluetooth has a low range detection, but a potentially higher precision when compared to GSM.

Table I
Operation Frequency Spectrum of Used Technologies

Technologies List				
GSM	3G	4G LTE	Wi-Fi	Bluetooth
900 MHz	900 and 2100 MHz	900, 1800 and 2600 MHz	2400 and 5000 MHz	2400 MHz

Additionally, different technologies have different security weaknesses that can be explored. In the next subsections we review the solutions adopted in each technology, for tracking and counting detected devices.

1) GSM 3G: GSM is the first digital iteration of the mobile network. In spite of its security risks, it is still in use, in particular by roaming tourists. One of those risks is the lack of authentication and full encryption in key functions of the communication between UE and the network. This allows for third parties to listen and get data from the users in the

network. With a SDR USB dongle, such as noolecSmartee[4] paired with a GSM receiver tool that explores security flaws, such as gr_gsm[5], it is possible to obtain relevant users' details. This type of data can be analyzed with software, such as the IMSI catcher[6] program in Python, to disclose not only the IMSI, but also to obtain other metrics such as roaming details, SNR ratio, and received power strength.

2) 4G/LTE: The 4G iteration of the cellular network technology focused not only on data transfer at greater speeds, but also enhanced security, improving user authentication and anonymity. Nevertheless, as previously stated, security flaws that can be exploited remain. In particular, there is a location leak that allow for the interception of decrypted paging messages that disclose the presence of users in the network. With a broadband SDR USB dongle, such as Lime-SRD[7], and a free and open-source LTE software suite, such as srsLTE[8], it is possible to analyze those paging requests.

3) Wi-Fi: Wi-Fi is widely used and enabled in UE in public areas, where they are usually more talkative[21] due to more frequent handovers or connection drops. In particular, clear probes are regularly sent to identify both the network and users. The probes containing MAC address can be intercepted and analyzed by a wireless USB dongle, configured in monitor mode. For this it is possible to use a Wi-Fi security auditing tools suite, such as aircrack-ng[9], to sniff probes and count how many UEs are present in an area. Presently, some devices use MAC address randomization for protecting their identity, but that randomization can be analyzed and by pattern detection it is possible to infer that a series of MAC addresses belong to just one device.

4) Bluetooth: Bluetooth uses a different architecture, when compared to Wi-Fi, but has a lot of similarities, and shares the same mechanism of probe request. These probes can also be intercepted with any appropriate sniffing USB dongle, specific for listening devices in undiscoverable mode, such as the open-source Bluetooth hardware Ubertooth One[10]. This can be paired with an open-source software[11] supported on the Kismet wireless network and device detector framework, and then it is possible to use the Ubertooth-Scan tool in conjunction with BlueZ, to detect the Bluetooth devices, either in undiscoverable or discoverable modes.

5) Combining trace elements: Our solution uses all of the aforementioned protocols and aims to unify all scavenged data into a relevant local crowding metric. Using this approach, we explored opportunities offered by security risks of those protocols. However, we guarantee users' privacy by only using passive techniques and anonymizing all sensible information that could identify a single user. A challenge for this solution is the calibration of each detection device, which depends on its local context, namely the topology of the surrounding environment. Each node will then require a learning period to calibrate how relevant is each technology to the crowding metric.

[4]https://www.nooelec.com/store/sdr/sdr-receivers/nesdr-smartee.html
[5]https://github.com/ptrkrysik/gr-gsm
[6]https://github.com/Oros42/IMSI-catcher
[7]https://myriadrf.org/projects/component/limesdr/
[8]https://github.com/srsLTE/srsLTE
[9]https://github.com/aircrack-ng/aircrack-ng
[10]https://greatscottgadgets.com/ubertoothone/
[11]https://github.com/greatscottgadgets/ubertooth

V. Validation

In order to validate our proposal, through preliminary field tests, we have developed a prototype of a detection node. Its case was designed to withstand harsh environmental conditions, including high temperatures and water splashes, such as rain. In its interior, several wireless sensor USB dongles, with their antennas, are connected to a processor board (see Fig 4).

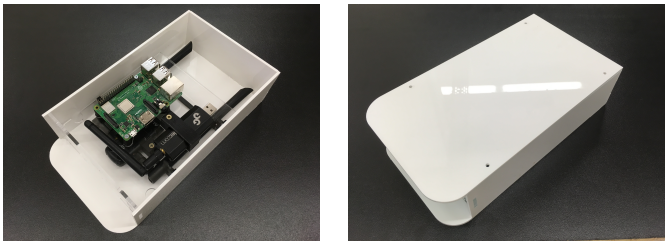

Figure 4. Open (left) and closed (right) case of detection node prototype

The hardware used in this prototype is described in Table II.

Table II
Components used in the detection nodes

COMPONENT	FUNCTION
Raspberry-Pi	Coordinate and Compute
Ubertooth One	Detect Bluetooth Devices
Alfa Network awus036ac	Detect Wi-Fi Devices
Nooelec NESDR SMArTee	Detect GSM/3G Devices
Lime-SDR	Detect 4G Devices

We foresee that the crowd sensor will be deployed in areas with different characteristics, and that a calibration period will be required. For this reason, we have opted for tests in typical usage scenarios, such as outdoor and indoor environments, in areas with high flow (narrow passages) and low flow (open spaces) of people. During these tests, we have measured the number of detections using different wireless technologies and compared it with direct observation of the number of people in the vicinity of the sensor.
This method allows to infer the effectiveness of our detection approach, but also presents some validation threats, such as human errors during counting (e.g. false negatives due to not being able to count people that is not in the line of sight).
The results in figure 5 were obtained with the sensor placed in a narrow passage with a high flow of people, in an indoor environment.

The plot of this graph uses a sliding window approach, where each data point represents how many people has passed in the capturing range of our sensor in the last 15 minutes. This sliding window approach was also used for plotting the graphs in figures 6, 7 and 8.
Results show that by merely capturing Wi-Fi data from devices

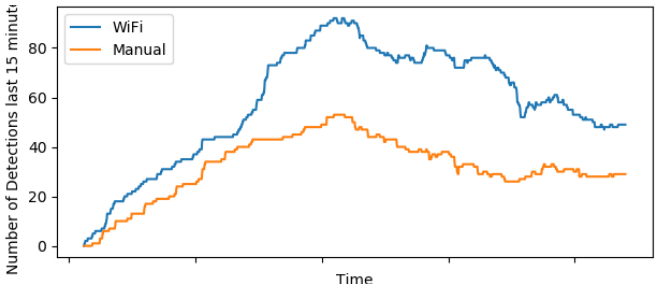

Figure 5. # of detected Wi-Fi vs manual detection in high flow

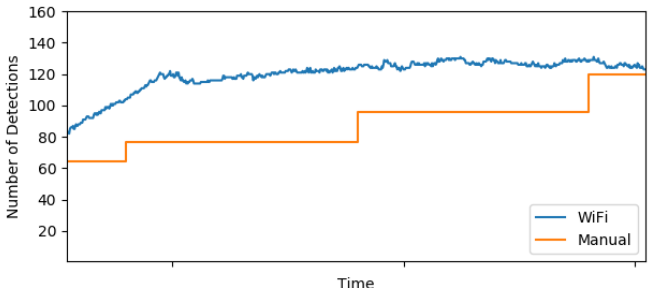

Figure 7. Outdoor # of detected Wi-Fi devices vs manual

it is already possible to obtain a good relationship between detected users and direct observations. The surplus in automatic detection face to the human (manual) counting, may be due to the 'noise' produced by random MAC generation; we plan to mitigate this problem in future work. The next two tests where both performed in an open space area, with a low flow of people, for indoor (Fig 6) and outdoor (Fig 7) environments. It is important to learn how our solution behaves in this type of scenarios, as it will be common in overcrowded situations, where people will to move slower or have longer periods of stay.

Fig 6 shows that the sensor takes some time to reach the number of devices present in the room. This is mostly due to how talkative are the devices in the sensor vicinity. After this initial period, detections follow closely the data observed via a manual counting. This indicates that the sensor, when exposed to a sudden crowding situation, may take some time to adjust but, nevertheless, providing a quasi-real-time estimate.

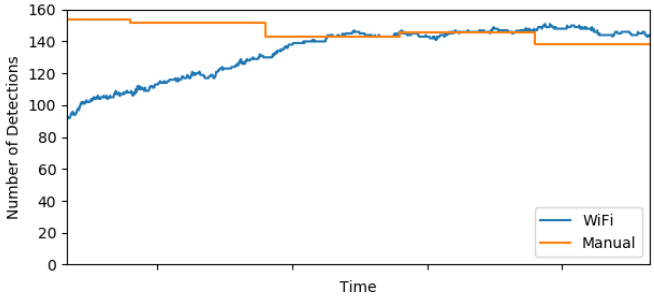

Figure 6. Indoor # of detected Wi-Fi devices vs manual

Fig 7 confirms that detections are a fair estimate for manual observations. The initial detection increase is also noticeable, but device detection via Wi-Fi data is higher than manual count. This difference confirms our suspicions regarding the characteristics of the outdoor environment used for the test: a courtyard surrounded by the main building of the campus. As such, the sensor is counting devices both in line-of-site (within the courtyard) and hidden (inside the building). Future iterations of our sensor should consider this during calibration.

Figure 8 shows detections using several technologies simultaneously, in an open space area. It is possible to notice that Wi-Fi detection presents a convincing result when compared to reality, matching the growth of people in the area. However, Bluetooth confirms our expectations and shows a much lower detection rate when compare to Wi-Fi. That is explained by the smaller range of this technology, and devices are detected only when they are a few meters apart from the sensor. In order to validate the use of Bluetooth, more tests are required with a manual count of users within a radius of few meters from the sensor. By fusing Wi-Fi and Bluetooth data, a sensor is possible with a significant recall provided by Wi-Fi (few false negatives), improved with the precision that is possible with Bluetooth (few false positives).

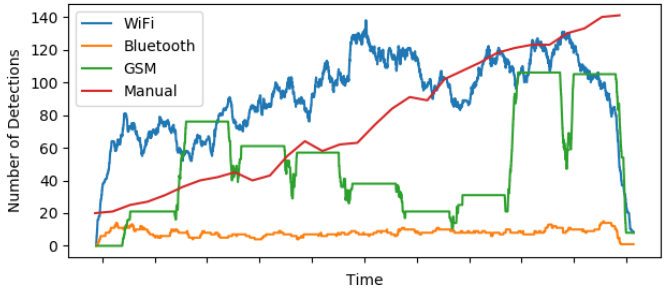

Figure 8. # of detected devices using several technologies

Due to limitations of hardware, that will be solved in future iterations of our solution, GSM data collection was done for a few minutes period in the nearest cell towers by round robin. The steps presented in the GSM data denote the detection handover from one cell tower to another and the number of devices detected during the detection period on each cell. For this reason, the obtained results are not yet conclusive.

VI. Conclusions

We conclude that it is possible to build a low-cost device to estimate crowding in its vicinity, by detecting the operation of multiple wireless technologies currently used by personal mobile devices. Based on open source software components and off-the-shelf hardware, it is possible to gather data simultaneously from those technologies and derive the number of devices in the area, in almost real-time. We recognize that several factors influence the detection process differently for each wireless technology under study, such as the space topology, the flow of people and local propagation characteristics. Therefore, further work is required to understand that influence and calibrate our detection algorithms, to guarantee the reliability of results.

Applications domains other then tourism overcrowding mitigation could benefit from our crowd detection technique.

The data we are collecting can be used to identify crowding patterns in near-real-time, which can be useful for several purposes, such as quick law enforcement actions (e.g. for dispersing sudden hostile purpose gatherings) or short-term, unplanned, urban cleaning actions, due to the arrival of cruise ships, or other unforeseen manifestations. By analyzing the geographical and temporal distribution of the crowding patterns, local authorities can also improve their planning and assign their resources more efficiently, in areas such as security patrolling or waste collection, thereby improving urban management with benefits for both residents and visitors.

VII. Ongoing and Future Work

We are now deploying our solution in the university campus for crowd detection during an extended period of time. The campus, with circa 9K "inhabitants", is a good surrogate of a touristic neighborhood affected by overcrowding, since during academic working days it has crowded narrow streets with high pedestrian traffic in some time periods, along with large open spaces where the occupation pace varies much slower. Our crowd detectors will be installed in several locations, each with different characteristics, in terms of space topology (e.g. passage alleys, leisure and working areas, both indoor and outdoor), flow of people and local propagation characteristics. To assess the influence of such diverse factors on the validity of this measurement approach, namely on its precision and recall, we will perform people counting by direct observation. For the calibration of our detection algorithms we plan to explore supervised machine learning techniques.

We also plan to combine the quasi-real-time data captured by our network of detectors with geo-referenced forecasts from surrounding areas, based on past data from other sources (e.g. mobile phone operators) with the aim of deriving dynamic heatmaps where crowd density will vary over space and time.

References

[1] Newzoo. Global mobile market report 2018.

[2] McKinsey&Company. Coping with success: Managing overcrowding in tourism destinations. Technical report, World Travel & Tourism Council, 2017.

[3] M. Andersson et al. Fusion of acoustic and optical sensor data for automatic fight detection in urban environments. In *13th Conf. on Information Fusion (FUSION)*, pp. 1–8. IEEE, 2010.

[4] P. Peng et al. Robust multiple cameras pedestrian detection with multi-view Bayesian network. *Pattern Recognition*, 48(5):1760–1772, may 2015.

[5] C. Stahlschmidt et al. Applications for a people detection and tracking algorithm using a time-of-flight camera. *Multimedia Tools and Applications*, 75(17):10769–10786, 2016.

[6] J. C. Farrés. Barcelona noise monitoring network. In *EuroNoise Conference*, pp. 218–220, 2015.

[7] A. Mesaros et al. Acoustic event detection in real life recordings. In *18th European Signal Processing Conference*, pp. 1267–1271. IEEE, 2010.

[8] R. Agarwal et al. Algorithms for crowd surveillance using passive acoustic sensors over a multimodal sensor network. *IEEE Sensors Journal*, 15(3):1920–1930, 2015.

[9] C. Anglano. Forensic analysis of WhatsApp Messenger on Android smartphones. *Digital Investigation*, 11(3):201–213, 2014.

[10] S. B. Ranneries et al. Wisdom of the local crowd. In *8th Conf. on Web Science (WebSci'16)*, pp. 352–354. ACM, 2016.

[11] D. R. Domínguez et al. Sensing the city with Instagram: Clustering geolocated data for outlier detection. *Expert Systems with Applications*, 78:319–333, 2017.

[12] S. Park et al. MobInsight: Understanding Urban Mobility with Crowd-Powered Neighborhood Characterizations. In *Int. Conf. on Data Mining Workshops (ICDMW)*, pp. 1312–1315. IEEE, 2017.

[13] A. Kashevnik and M. Shchekotov. Comparative analysis of indoor positioning systems based on communications supported by smartphones. In *12th Conf. of Open Innovations Association (FRUCT)*, pp. 1–6. IEEE, 2012.

[14] Q. Yang and L. Huang. *Inside Radio: An Attack and Defense Guide*. Springer, 2018.

[15] D. Fox. IMSI-Catcher. *Datenschutz und Datensicherheit (DuD)*, 21:539, 1997.

[16] D. Strobel. Imsi catcher. Technical report, Ruhr-Universitat Bochum, 2007.

[17] A. Shaik et al. Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. Technical Report 1510.07563, arXiv, 2016.

[18] R. P. Jover and V. Marojevic. Security and protocol exploit analysis of the 5G specifications. *IEEE Access*, 7:24956–24963, 2019.

[19] M. V. Barbera et al. Signals from the crowd. In *Internet Measurement Conf. (IMC'13)*, pp. 265–276, New York, USA, 2013. ACM Press.

[20] A. Musa and J. Eriksson. Tracking unmodified smartphones using wi-fi monitors. In *10th Conf. on Embedded Network Sensor Systems*, pp. 281–294. ACM, 2012.

[21] J. Freudiger. How talkative is your mobile device?: an experimental study of wi-fi probe requests. In *8th Conf. on Security & Privacy in Wireless and Mobile Networks*, pp. 8. ACM, 2015.

[22] J. Martin et al. A Study of MAC Address Randomization in Mobile Devices and When it Fails. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2017(4):365–383, 2017.

[23] M. Chernyshev. An overview of bluetooth device discovery and fingerprinting techniques – assessing the local context. In *13th Australian Digital Forensics Conf.*, Perth, 2015.