IoT Geofencing for COVID-19 Home Quarantine Enforcement

Jiajie Tan, Edmund Sumpena, Weipeng Zhuo, Ziqi Zhao, Mengyun Liu, and S.-H. Gary Chan

Abstract

Containment is the first-priority measure in infection control to curb the spread of highly infectious diseases such as COVID-19. Home quarantine is one such measure to keep people at their accommodations for the incubation period (typically 14 days). Compared to dedicated monitoring centers, home quarantine is a more cost-effective and comfortable approach to isolate a large number of low-risk people. However, efficient monitoring of confinees inside their accommodations is a challenging problem because the quarantined locations are scattered throughout the city. We propose and study SignatureHome, an automated IoT-based geofencing algorithm to cost-effectively monitor confinees. The core principles of SignatureHome was adopted by the Hong Kong government and implemented as an app to enforce home quarantine order in March 2020 for hundreds of thousands of entrants from other regions.The system employs waterproof Bluetooth Low Energy wristbands that are uniquely paired with the confinees' smartphones. SignatureHome uses the identifiers of the environmental network facilities (Wi-Fi access points and cellular networks) as the home signature. By comparing the current observed signals of the phone with the home signature, the algorithm can efficiently determine whether the user is within the geofenced area. SignatureHome is computationally efficient, responsive, privacy-preserving, cost-effective, and adaptive to home diversity and changing environments. Our experimental results validate its design and high accuracy in terms of precision, recall, F-measure, and false alarm rate.

Introduction

The highly infectious disease COVID-19 has become a pandemic with profound impacts on our life and economy [1]. To effectively curb its spread, infection containment is the first-priority measure. In many countries or regions, people who recently have traveled from high-risk areas or have had physical contact with confirmed cases are required to be quarantined for the virus incubation period (typically 14 days). For example, Hong Kong has enforced a mandatory quarantine order either at home or at a monitoring center for people arriving from overseas since February 2020 [2].

In contrast to quarantine in dedicated facilities (so-called centralized quarantine), *home quarantine* allows people to stay in their apartments or rental rooms. It is a more cost-effective approach for containing a large number of low-risk people, greatly relieving the effort of facility management and security monitoring. Furthermore, home quarantined people often feel more comfortable and at ease when staying at the places of their choice.

Any violation of home quarantine (i.e., the confinee's leaving home within the quarantine period) can present a huge risk and cost to public health. Since quarantine places are scattered over the city, how to efficiently and continuously monitor the confinees becomes a challenging problem. One approach is to require the confinees to regularly report their satellite-based (e.g., GPS and Beidou) geo-locations for remote checking [3, 4]. Such regular manual reporting, however, disrupts the normal lives of the confinees, drains government resources, and functions unreliably in crowded buildings where satellite signals are weak or even absent.Another approach is to conduct surprise visits to make sure the confinees are at home. This is inefficient due to its large manpower requirement and intrusive nature. Because of privacy concerns, these measures cannot be conducted in a frequent manner of, say, once every minute, hence posing the risk of the confinee's leaving the quarantine place between inspection/report points.

Due to the prevalence and penetration of IoT technology, researchers and developers employ smartphones to transparently, automatically, and digitally *geofence* quarantined people over time. A common approach is to estimate a confinee's position using Wi-Fi fingerprinting [5, 7], and then check whether it falls within the predefined confined area. Although accurate, the approach requires much effort on prior calibration of signal patterns both inside and outside the quarantine region. This is costly and not scalable for highly scattered quarantine places.

We propose and study a novel and simple IoT geofencing technology called *SignatureHome*, which leverages the distinctive characteristics of the identifiers (IDs) of network facilities (e.g., Wi-Fi and cellular network) to determine the in/out status of the confinees. It requires neither fine-grained user locations nor intensive computational power, making it suitable for large-scale mobile deployment.

The basic and core principles of SignatureHome have been developed as a public app named *StayHomeSafe*, operated and maintained by the Hong Kong government to support distributed home quarantine monitoring. It has been successfully deployed to hundreds of thousands of entrants to enforce home quarantine orders since March 2020 [8]. SignatureHome has the following strengths:

- *Accuracy*: SignatureHome detects whether the IoT device with the app (phone in this case) is inside or outside the designated area with high precision and recall.
- *Adaptiveness to home environment and diversity*: SignatureHome works in homes of different layouts and sizes and adapts to changing signal environments.
- *Responsiveness*: SignatureHome can quickly detect whether the confinee has left the quarantine location or not. The latency is as low as half a minute.
- *Automation and non-intrusiveness (ease of use)*: The system is "plug and play," fully automated, easy to use, and requires little manual interaction.
- *Privacy by design*: SignatureHome respects user privacy with data minimization. It makes the in/out decision without needing the exact position of the confinee. Personal data (location history, user activities, cameras, photos, voice, etc.) is not collected or used. The publicly available network IDs are the only required data. They are collected solely on the device and do not leave the phone without user consent.
- *Lightweight (low power consumption)*: SignatureHome is simple to implement and lightweight. Due to its computational efficiency and minimal use of device sensors, power consumption is low. Running the app does not negatively affect the normal operation of the device or user experience.

Digital Object Identifier: 10.1109/IOTM.0001.2000097

- *Cost effectiveness to deploy and maintain*: The system does not require special devices beyond the Bluetooth Low Energy (BLE) wristbands. The wristband is low-cost, and may be simply cut and disposed of at the end of the quarantine period.

System Overview

We show in Fig. 1 the operation workflow of the IoT-enabled quarantine monitoring system. The system consists of a low-cost waterproof wristband using BLE and a smartphone owned by the confinee. The confinee is first attached with a wristband, which periodically broadcasts BLE beacons with its unique ID. The wristband is worn by the confinee for the entire quarantine period and cannot be taken off without cutting the circuit and terminating beaconing permanently. Once wearing the wristband, the confinee then installs the geofencing app on the phone, which pairs with the wristband. By detecting the beaconing signals, the smartphone ensures its proximity to the wristband, and hence the confinee. The phone also collects environmental signals such as Wi-Fi and cellular to make the geofencing decision (i.e., whether the phone itself is inside the quarantine location). The phone has to be on at all times and periodically sends heartbeats to the control center. If the wristband is far from the phone (and hence no beacon is detected by the phone) or the phone is not inside the geofenced area, the confinee is likely out of the quarantine place. In such a case, the control center will be immediately notified. Figure 2 shows the wristband and a smartphone with the Hong Kong StayHomeSafe app for a home confinee.

The core of the quarantine monitoring system is SignatureHome, an efficient and practical algorithm for geofencing. Two types of network IDs, ambient ID and connection ID, are used in SignatureHome, together forming the unique *home signature* of the quarantine environment. Signals detected by the confinees' devices are compared with the home signatures of the geofenced regions to determine their in/out status.

Home Signature

The home signature reflects the unique signal pattern of the quarantine location. We introduce two types of ID components (ambient ID and connection ID) in the home signature for efficient geofencing.

Ambient IDs

Due to heterogeneous settings of network facilities (e.g., locations, transmission power) and various indoor layouts (walls, household appliances, etc.), different locations are usually covered by unique sets of ambient networks. We regard the IDs of those networks as an important component in the home signature.

Wi-Fi networks usually use service set identifiers (SSIDs) as their names. A wireless network consists of one or more network sections, each of which is covered by a base station such as an access point (AP) or a wireless router. The network section is identified by the basic service set identifier (BSSID) [9]. By convention, the BSSID is globally unique because it is synonymous with the base station's medium access control (MAC) address. In addition, we can easily obtain nearby BSSIDs by scanning Wi-Fi services on mobile devices. Due to its uniqueness and availability, we regard Wi-Fi BSSIDs as ambient IDs. Note that we do not consider cellular networks for ambient IDs because most off-the-shelf phones do not provide users access to the information of unconnected cellular base stations.

Connection IDs

Modern smartphones are able to connect to known networks (e.g., Wi-Fi at home) automatically without manual operation. Since the settings of the home network are rarely changed, such connection preference can be leveraged to recognize if the user is inside the quarantine place. Connection IDs involve both the connected Wi-Fi network and the connected cellular network. For the Wi-Fi network, we consider the following connection IDs:

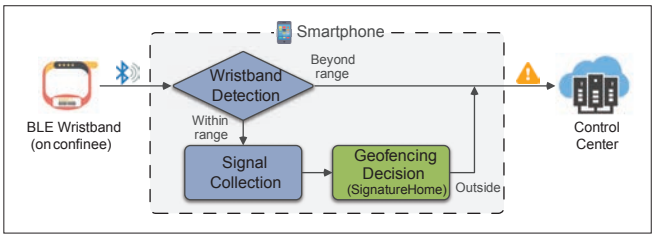


FIGURE 1. The operation workflow of the IoT-based home quarantine monitoring system.

FIGURE 2. The home quarantine monitoring system StayHomeSafe deployed in Hong Kong.

- *SSID*: As mentioned above, an SSID is the name of the Wi-Fi network. Although a unified Wi-Fi network can be composed of multiple APs with different BSSIDs, they usually share the same SSID. We hence use the connected SSID rather than BSSID to represent the unique home environment.
- *Local IP address*: The local IP address is assigned by the dynamic host configuration protocol (DHCP) service in the local area network (LAN). A DHCP server tends to assign the same IP address to the same device if the address resource is available. We leverage this convention to infer whether the device connects to the same LAN or not.
- *External IP address*: The external IP address of the home network is assigned by the Internet service provider (ISP). As the address is rarely changed, we can use it to infer whether the connected network is indeed that of the home or not.

In cellular networks, a base station is identified by its location area code (LAC) and cell ID (CID). We use the combination of LAC and CID to represent its unique connection ID.

It is worth noting that we employ multiple simultaneous IDs to verify the connected networks. If we use only a single ID, say, SSID, an attacker can easily deceive the system by using a portable hotspot with the same network name. The multimodal IDs cross-verify the connection and hence greatly improve the security, accuracy, and robustness.

SignatureHome: Efficient ID-Based Geofencing

Workflow

The workflow of SignatureHome consists of two phases: a training phase that constructs the home signature and an operation phase that makes geofencing decisions during the quarantine period. The training phase takes place when a confinee arrives at the quarantine accommodation for the first time. He/She is required to walk around at home with his/her smartphone for

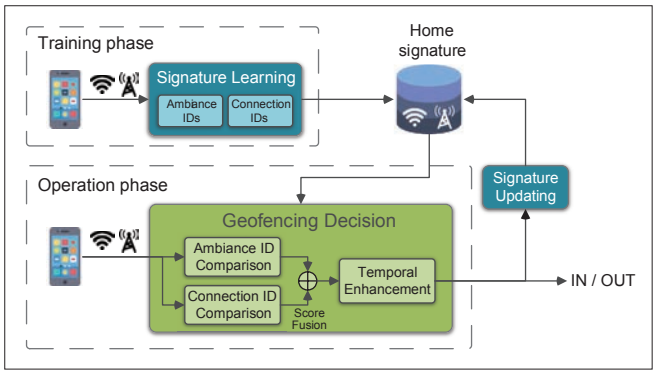


FIGURE 3. The workflow of SignatureHome, which consists of a training phase and an operation phase.

several minutes. The phone collects the IDs of both ambient networks and connected networks to construct the home signature. In the operation stage, SignatureHome determines the confinee's in/out status based on the current sensed signals. It compares the observed ambient and connection IDs with the home signature and leverages temporal information to make the in/out decision. Additionally, SignatureHome identifies the trustworthy at-home IDs obtained in operation to update the home signature. The algorithm can be deployed on mobile devices for efficiency improvement and privacy protection.

Training Phase: Signature Learning

In the training phase, a home signature is constructed using Wi-Fi and cellular signals collected at home. This signature is synonymous with a virtual geofence for the quarantine accommodation.

One strategy is to store all the training IDs in a database. It is widely applied in fingerprint-based localization [10]. The confinee's in/out status can be obtained by comparing the similarity between the observation and all the entries in the database. Although the approach performs well for localization, it has two critical issues in home quarantine scenarios. One is that the fingerprinting model lacks generalizability for the environments since the constructed model always fits tightly to the training samples. In practice, however, the signal collection is a casual process for the confinees. They may not walk to every location in the quarantine accommodation and cannot collect signals outside the region, affecting the model's accuracy. Another challenge is the need for large storage to contain the training data and high computational power to search for the matched results, resulting in the burden of processor and battery on mobile devices.

In SignatureHome, we propose a simplified and unified representation for home signature. The ambient IDs in the home signature are the union of the observed BSSIDs in the training phase. The connection IDs in the home signature involve multiple types of connections. For each kind of connection, we use the union of the corresponding connection IDs in the training samples as the ID. Generally speaking, the IDs in any observed sample inside the geofence are expected to be a subset of the corresponding part in the home signature.

Operation Phase: Geofencing Decision

In the operation phase, SignatureHome decides whether the confinee is inside the geofence. Given an observed signal sample, it first determines the probability of being inside the geofence by comparing the ambient IDs and the connection IDs with the home signature. The algorithm then fuses the scores and leverages temporal information to enhance the final decisions.

The modules in the geofencing decision are explained below.

Ambient ID Comparison: Since the home signature has included all the sensible network IDs inside the geofence, any signal at home should have a large proportion of IDs that are also in the home signature. We hence define the score of ambient ID as the ratio of the number of intersection IDs (between the targeting sample and home signature) to the total number of IDs in the targeting sample. The score is a real number between 0 and 1. If all the ambient IDs appear in the home signature, the highest score, 1, can be obtained. On the contrary, the score becomes 0 if none of them matches the home signature.

Connection ID Comparison: To compare connection IDs, we check whether the observed connection IDs exist in their corresponding home signature ID sets in the home signature. For any type of connection ID, the score will be 1 if the result is positive, and 0 otherwise. Based on that, we are able to obtain the scores of different kinds of connection IDs (SSID, local IP, etc.).

Score Fusion: We use weighted averaging to fuse the scores of ambient and connection IDs. Weights are assigned to the ID scores to represent their importance and reliability. To constrain the fused score between 0 and 1, all the weights must be positive and add up to 1. The weights can be determined by empirical settings or an offline learning process. The learning alternative can be interpreted as a linear regression problem [11], where the scores of different IDs form a feature vector and the weights are the parameters to be estimated. The parameters can be computed by minimizing the total prediction error based on an extra set of labeled samples (both in and out). In the case when certain IDs are missing (e.g., the phone does not connect to Wi-Fi, and hence there is no SSID and local IP), we exclude those IDs in computation and normalize the scores based on the weights of the remaining IDs. Finally, we set a decision threshold T to convert the score to the in/out decision. Samples whose scores are greater than T are regarded as insiders, while the others are outsiders.

Temporal Enhancement: Since an individual sample is vulnerable to the signal fluctuation and ambiguity, we introduce a post-processing module that leverages temporal information to enhance the robustness of the system and user experience. Our intuition is that users do not switch regions frequently, and hence we can cross-verify the decisions among temporally neighboring samples to mitigate the decision error. To determine the geofencing decision at time t, we look at the observed samples within the time window from $t - \tau$ to $t + \tau$, where τ is the parameter controlling the window width. The in/out decision at time t follows the majority voting on all the independent decisions within the time window.

In the process above, SignatureHome visits each sensed ID once to determine the intersection between the sensed IDs and the home signature. The modules of score fusion and temporal enhancement have constant complexity by caching the previous results. Therefore, the overall time complexity is linear to the amount of sensed IDs, which is low in reality.

Signature Update

Network connections can be changed on user devices. For instance, a smartphone will switch to another Wi-Fi network when the previous connection is not stable. The geofencing accuracy will be affected if the new connection ID is not recorded in the training stage. To address this, we discuss an optional process of updating home signature in operation.

The general principle of updating signature is to identify the valid and trustworthy at-home signals and add their connection IDs to the home signature. To approach this, we set up three criteria to make sure the sample is indeed at home:

- The sample should be classified as an insider.
- The score of its ambient IDs should be greater than ϕ, where ϕ is a predefined threshold.
- The BSSID of the new connection should be in the ambient IDs of the home signature.

For every online observed signal, we check whether it satisfies the criteria above. If all the criteria are met, the sample is

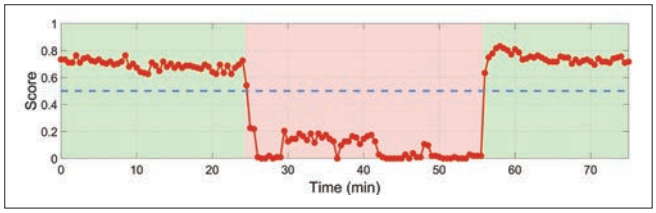


FIGURE 4. A fragment of the geofencing scores in the example of tester A. The red line shows the scores over time. The dashed line in blue represents the decision threshold (T = 0.5). The colored background indicates the actual location status, where green is inside and red is outside.

qualified to update the signature. We can thus add its connection IDs into the corresponding sets of the home signature if the IDs have not appeared before.

Implementation and Experimental Study

To study and validate the performance of SignatureHome, we have implemented a prototype system and conduct extensive experiments in the scenario of home quarantine.

The prototype system consists of a client app built on the Android platform and a server to receive and process the leaving-region notifications. The app works as a background service in the general operation, reducing disturbance to the users' normal usage. Meanwhile, we develop an experimental mode that allows testers to label their in/out status at ease (used for collecting the ground truth). The geofencing decision is computed locally on the phone. The testing devices include Mi MIX 3, Huawei P20, Samsung Galaxy S7, Google Nexus 5, LG Q7+, and so on. The versions of the operating system range from Android 5 to 10. To balance the responsiveness and power consumption, we set the signal sampling interval to 30 s.

We recruit eight volunteers to participate in the testing. Testers follow the common quarantine procedure. They first conduct the training process to construct the home signatures. During the period, they walk around at home for 3 to 5 minutes and stay in different rooms for a while. After that, testers start the simulation of home quarantine. They stay at home for several hours (~2 hours) as the normal at-home case, and leave home for a while at an arbitrary time to simulate leaving-home cases. To obtain the actual locations as the ground-truth labels, testers are required to record the in/out status if it is changed (e.g., leaving home or coming back). Table 1 lists the test settings of different quarantine places (e.g., apartment, dormitory and house) and sizes (ranging from 6 m^2 to 250 m^2). Note that, due to the pandemic, testers are scattered in different cities around the world. This also helps to validate the adaptiveness in heterogeneous quarantine environments.

To quantitatively evaluate the performance of SignatureHome, we view the geofencing task as a binary classification and thus apply classification metrics such as precision and recall [12]. In particular, our evaluation focuses on the leaving-home cases since the main objective is to detect whether the confinees leave their places or not. Precision is defined as the ratio of the number of cases that are correctly recognized as outsiders to the total number of outside predictions. Recall is the fraction of correct outside predictions among all the cases when users are actually out of the home. Precision reflects the goodness of the leaving-home alarms, while recall indicates whether all the leaving-home cases can be detected. F-measure evaluates the comprehensive performance of precision and recall, which is defined as their harmonic mean. On the other hand, false alarms (i.e., reporting that the confinee leaves while he/she does not) is also important in the quarantine monitoring as they may affect the user experience and disturb the normal operation of the control center. We define the false alarm rate as the ratio of the number of false alarms to the total number of at-home samples.

Table 1 also describes the geofencing performance in terms of precision, recall, F-measure, and false alarm rate. We can see that SignatureHome achieves high precision (0.972 on average) and recall (0.928 on average) in general, as well as a low false alarm rate (0.014 on average). The data validates SignatureHome's high applicability in real-world scenarios and excellent adaptiveness to heterogeneous environments.

To give an intuitive demonstration of how SignatureHome geofences the confinee, we plot in Fig. 4 the geofencing scores of tester A over time. The tester initially stays at home and randomly moves in different rooms. He then leaves the apartment to imitate a quarantined user leaving the accommodation. After wandering around the building and the residential district for a while, the tester returns home. We can see that the trend of scores matches the tester's trajectory accurately. When the tester is inside the apartment, the scores fluctuate around 0.7. As he leaves home, the scores dramatically decline to a low level (under 0.2). By setting the appropriate decision threshold (T = 0.5 in our prototype), SignatureHome is able to adapt to heterogeneous environments and make geofencing decisions with high accuracy.

We further investigate the impact of ID choices in the home signature. In Fig 5a, we plot the F-measure against different types of IDs when temporal enhancement is applied (labeled with "w/T.E.") or not (labeled with "w/o T.E."), respectively. The colored bars represent the mean F-measure among all the tests, and the error bars show their minimum and maximum values. We observe that the ambient ID alone does not have as good performance as the connection ID, as shown by the lower mean F-measure. However, it shows more stable results in terms of the smaller variance. The reason lies in the different characteristics of the IDs. Connection ID provides trustworthy at-home information, but it does not have sufficient discriminability in ambiguous zones such as doorways and lobbies. Ambient IDs, on the other hand, are able to distinguish between fine-grained regions but is vulnerable to signal noise. This can also be verified by the observation that temporal enhancement contributes more to the ambient ID than the connection ID, since the temporal information is helpful to mitigate the influence of signal noise. SignatureHome fuses the two types of IDs and applies temporal enhancement, hence achieving the most accurate and robust performance.

Figure 5b illustrates the impact of window widths in the temporal enhancement. We can observe that a suitable choice of window width (60 s) leads to the highest F-measure. When the window width is zero, no temporal enhancement is applied, and the system hence becomes sensitive to signal fluctuation (with low F-measure). On the other hand, an overly large window width does not improve the performance since users may have long-range movement during the large interval, and the inconsistency of the individual results within confuses the final decision.

To validate the computational efficiency of SignatureHome, we study its power consumption on commercial smartphones (LG Q7+). We also implement a GPS-based approach on the same device. The battery drain without any geofencing app is recorded as a baseline. Figure 5c shows the battery curves within 90 minutes (all the tests start with 90 percent battery life). We can see that the power consumption in SignatureHome remains close to the baseline (5 percent), while the battery declines much quicker in the GPS case (exceeding 10 percent under the baseline). This is because SignatureHome uses only low-energy network interfaces as sensors, and the algorithm is designed with low computational complexity. The minimized energy consumption makes it possible to deploy geofencing on users' phones without affecting the normal operation.

Conclusion

Home quarantine is an effective way to contain the spread of infectious diseases such as COVID-19, where the confinees are isolated in their accommodations for the virus incubation period. We propose and study SignatureHome, an automated

Tester	Quarantine location			Geofencing performance			
	Location	Type	Area	Precision	Recall	F-measure	False alarm rate
A	Hong Kong, China	Apartment	~60 m^2	1.000	0.971	0.986	0.000
B	Hong Kong, China	Apartment	~40 m^2	1.000	0.995	0.997	0.000
C	Hong Kong, China	Dormitory	~6 m^2	0.955	0.984	0.969	0.012
D	Shanghai, China	Apartment	~100 m^2	1.000	0.939	0.968	0.000
E	Changchun, China	Apartment	~120 m^2	0.992	1.000	0.996	0.003
F	Shantou, China	Apartment	~100 m^2	0.875	0.848	0.862	0.019
G	Shenzhen, China	Apartment	~50 m^2	1.000	0.800	0.889	0.000
H	San Diego, U.S.	House (2 floors)	~250 m^2	0.953	0.885	0.918	0.077
Mean	–	–	–	**0.972**	**0.928**	**0.948**	**0.014**

TABLE 1. The experimental settings and geofencing performance.

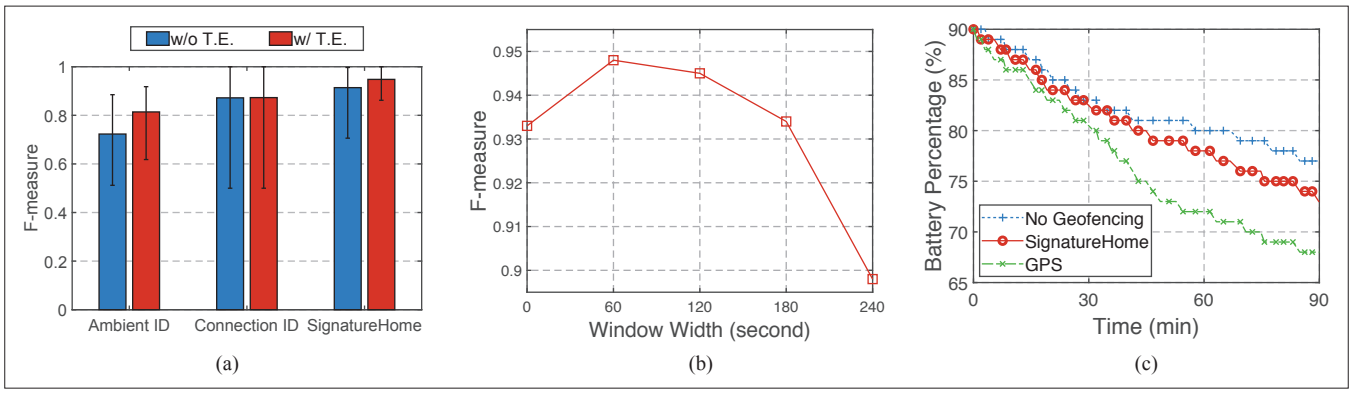


FIGURE 5. The experimental results: a) geofencing performance under different categories of IDs; b) geofencing performance under different window widths; c) power consumption under different geofencing approaches.

IoT-based geofencing algorithm to cost-effectively monitor the confinees. The basic principles and core ideas of SignatureHome have been implemented as a publicly available home quarantine app called StayHomeSafe by the Hong Kong government to enforce the home quarantine order. Paired with a BLE wristband, the system has been serving hundreds of thousands of entrants into Hong Kong since March 2020.

SignatureHome leverages the IDs of Wi-Fi and cellular networks to create a home signature. By comparing the observed signals of the confinee with the home signature, SignatureHome can efficiently detect the in/out status of the confinee. The algorithm is lightweight, responsive, adaptive, privacy-preserving, and cost-effective to deploy and maintain. Our extensive experimental results validate its design and high accuracy in terms of precision, recall, F-measure, and false alarm rate.

Acknowledgment

This work was supported, in part, by Hong Kong General Research Fund (16200120).

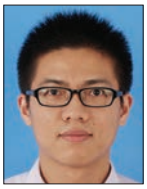
References

[1] WHO, "WHO Director-General's Opening Remarks at the Media Briefing on COVID-19 — 11 Mar. 2020," Mar. 11, 2019; https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19—11-march-2020, accessed July 5, 2020.
[2] Hong Kong Government, "Cap. 599C Compulsory Quarantine of Certain Persons Arriving at Hong Kong Regulation," Feb. 8, 2020; https://www.elegislation.gov.hk/hk/cap599C, accessed July 12, 2020.
[3] F. Reclus and K. Drouard, "Geofencing for Fleet Freight Management," *Proc. 9th Int'l. Conf. Intelligent Transport Systems Telecommun.*, Oct. 2009, pp. 353–56.
[4] R. R. Oliveira *et al.*, "SWTRACK: An Intelligent Model for Cargo Tracking Based on Off-the-Shelf Mobile Devices," *Expert Systems with Applications*, vol. 40, no. 6, May 2013, pp. 2023–31.
[5] P. Bahl and V. N. Padmanabhan, "RADAR: An In-Building RF-based User Location and Tracking System," *Proc. 19th Annual Joint Conf. IEEE Computer and Commun. Societies*, Tel Aviv, Israel, 2000, vol. 2, pp. 775–84.
[6] M. Youssef and A. Agrawala, "The Horus WLAN Location Determination System," *Proc. 3rd Int'l. Conf. Mobile Systems, Applications, and Services*, Seattle, WA, 2005, pp. 205–18.
[7] S. He and S.-H. G. Chan, "Tilejunction: Mitigating Signal Noise for Fingerprint-Based Indoor Localization," *IEEE Trans. Mobile Computing*, vol. 15, no. 6, June 2016, pp. 1554–68.
[8] HKUST Press Release, "HKUST Researchers Develop Smart Geo-fencing Technology for Home Quarantine amid COVID-19 Pandemic," Mar. 19, 2020; https://www.ust.hk/news/research-and-innovation/hkust-researchers-develop-smart-geo-fencing-technology-home-quarantine, accessed July 15, 2020.
[9] M. S. Gast, *802.11 Wireless Networks: The Definitive Guide*, 2nd ed.. O'Reilly Media, 2005.
[10] S. He and S.-H. G. Chan, "Wi-Fi Fingerprint-Based Indoor Positioning: Recent Advances and Comparisons," *IEEE Commun. Surveys & Tutorials*, vol. 18, no. 1, 1st qtr. 2016, pp. 466–90.
[11] C. Bishop, *Pattern Recognition and Machine Learning*, Springer, 2006.
[12] J. Davis and M. Goadrich, "The Relationship Between Precision-Recall and ROC Curves," *Proc. 23rd Int'l. Conf. Machine Learning*, Pittsburgh, PA, 2006, pp. 23–40.

Biographies

Jiajie Tan (jtanad@cse.ust.hk) received his Bachelor of Engineering degree from Zhejiang University, Hangzhou, China, in 2012, and is working toward a Ph.D. degree in the Department of Computer Science and Engineering, Hong Kong University of Science and Technology (HKUST), China. His research interests include indoor localization, people sensing, and mobile computing.

Edmund Sumpena (edsumpena@gmail.com) is an 11th grader attending Westview High School in San Diego, California. He is interested in the intersection between machine learning and medicine, particularly issues related to cancer, neurological disorders, and pathogenic diseases. In 2020, he was a winner of the Microsoft Imagine Cup Junior AI for Good Challenge. He was also selected as a delegate to the World Food Prize Global Youth Institute to present his research on food security at the Norman Borlaug Dialogue International Symposium. He was the captain leading a FIRST Tech Challenge robotics team, which qualified for the FIRST World Championship.



Weipeng Zhuo (wzhuo@cse.ust.hk) is a third year Ph.D. student advised by Prof. Gary S.-H. Chan in the Department of Computer Science and Engineering, HKUST. He also got his Bachelor's and M.Phil. degrees from HKUST. His research focuses on indoor localization, more specifically, indoor geofencing, path recovery, and pathways learning via implicit crowdsourcing.

Ziqi Zhao (zzhaoas@connect.ust.hk) received his B.S. degree in computer science from HKUST in 2020. He will pursue an M.S degree in computer science from École Polytechnique Fédérale de Lausanne starting in 2020. His current research interests include indoor localization, machine learning, and data mining.

Mengyun Liu (amylmy@cse.ust.hk) is currently a postdoctoral fellow at the Department of Computer Science and Engineering, HKUST. She received her B.E., B.B.A (minor), and Ph.D. degrees from Wuhan University, China, in the School of Geodesy and Geomatics (2009–2013), Economics and Management School (2011–2013), and State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing (LIESMARS, 2013–2019), respectively. Before joining HKUST, she was also an intern at Microsoft Research Asia, Beijing, China, and a research assistant in the Department of Land Surveying and Geo-Informatics, Hong Kong Polytechnic University. Her research interests include indoor localization, wireless computing, multimodal machine learning, and the Internet of Things.

S.-H. Gary Chan (gchan@cse.ust.hk) is currently a professor in the Department of Computer Science and Engineering, HKUST. He is also the director of the Entrepreneurship Center and chair of the Committee on Entrepreneurship Education Program, Center for Education Innovation, HKUST. He received M.S.E. and Ph.D. degrees in electrical engineering from Stanford University, California, in 1994 and 1999, respectively, with a minor in business administration. He obtained his B.S.E. degree (highest honor) in electrical engineering from Princeton University, New Jersey, in 1993, with certificates in applied and computational mathematics, engineering physics, and engineering and management systems. His research interests include smart sensing and IoT, cloud and fog/edge computing, indoor positioning and mobile computing, video/location/user/data analytics, and IT entrepreneurship. He has been an Associate Editor of *IEEE Transactions on Multimedia* (2006–2011) and a Vice-Chair of the Peer-to-Peer Networking and Communications Technical Sub-Committee of the IEEE Comsoc Emerging Technologies Committee (2006–2013). He is and has been a Guest Editor of Elsevier *Computer Networks* (2017), *ACM Transactions on Multimedia Computing, Communications and Applications* (2016), *IEEE Transactions on Multimedia* (2011), *IEEE Signal Processing Magazine* (2011), *IEEE Communication Magazine* (2007), and Springer *Multimedia Tools and Applications* (2007). He was the TPC Chair of IEEE Consumer Communications and Networking Conference 2010, the Multimedia Symposium of IEEE GLOBECOM (2007 and 2006), IEEE ICC (2007 and 2005), and the Workshop on Advances in Peer-to-Peer Multimedia Streaming at ACM Multimedia Conference (2005). He has co-founded and transferred his research results to several startups. Due to their innovations and commercial impacts, his startups and research projects have received local and international awards (2012–2018). He is the recipient of the Google Mobile 2014 Award (2010 and 2011) and the Silver Award of Boeing Research and Technology (2009). He has been a visiting professor and researcher at Microsoft Research (2000–2011), Princeton University (2009), Stanford University (2008–2009), and the University of California at Davis (1998–1999). He was undergraduate programs coordinator in the Department of Computer Science and Engineering (2013–2015), director of the Sino Software Research Institute (2012–2015), co-director of the Risk Management and Business Intelligence program (2011–2013), and director of the Computer Engineering Program (2006–2008) at HKUST. He was a William and Leila Fellow at Stanford University (1993–1994), and the recipient of the Charles Ira Young Memorial Tablet and Medal and the POEM Newport Award of Excellence at Princeton (1993). He is a member of honor societies Tau Beta Pi, Sigma Xi, and Phi Beta Kappa, and a Chartered Fellow of The Chartered Institute of Logistics and Transport (FCILT).