BLEDoorGuard: A Device-Free Person Identification Framework Using Bluetooth Signals for Door Access

Article *in* IEEE Internet of Things Journal · September 2018

DOI: 10.1109/JIOT.2018.2868243

5 authors, including:

Wei Shao
RMIT University

Thuong Nguyen
Trusting Social Co.

Kyle Kai Qin
RMIT University

Moustafa Youssef
Alexandria University

BLEDoorGuard: A Device-Free Person Identification Framework Using Bluetooth Signals for Door Access

Wei Shao, Thuong Nguyen, Kai Qin, Moustafa Youssef, and Flora D. Salim

***Abstract*—Recently, door access control with Internet of Things (IoT) has become increasingly popular in the field of security. However, conventional approaches such as video-based or biological information based cannot satisfy the requirements of personal privacy protection in the modern society. Hence, a wireless signal based technique which does not need users to carry any devices, called device-free have been introduced in recent years to detect and identify persons. In this paper, we present BLEDoorGuard, a wireless, invisible and robust door access system which leverages received signal strength indicator (RSSI) from Bluetooth Low Energy (BLE) beacons to recognise a person who accesses a door. We evaluated BLEDoorGuard in two real world scenarios: the first is an office with a key lock, and the second is a meeting room with swipe card access. We exploit the characteristics of use of BLE for person identification and propose a two-step algorithm with multiple classifiers. We demonstrate that BLEDoorGuard is capable of identifying the actual user during door access with an accuracy of 69% and 62% among groups of 6 and 10 people, respectively.**

***Index Terms*—Device-free, Access control, Bluetooth, Activity recognition**

I. Introduction

Person identification is a key area in mobile and ubiquitous computing [1] [2]. When an individual is identified in a context-aware and personalised system, the application content can be customised. Additionally, the task of identifying the person forms the groundwork for security monitoring solutions, to provide authenticated access to a secure facility or resource [1]. Traditional approaches use Internet of Things (IoT) devices (e.g, on-body sensors, mobiles) to track and identify the user who wears them. Recent research on human detection and localisation using wireless signals provides a more flexible solution to the person identification problem [3]. This device-free technique outperforms traditional person identification methods in various ways. It employs wireless signals generated from environmental devices such as WiFi, radio-frequency identification (RFID) generators or Bluetooth beacons, to detect, localise and recognise the person in a particular region.

One state-of-the-art approach called WiWho using WiFi was proposed by Zeng et al. [2]. This framework used channel state information (CSI) for person identification, showing that RF-based techniques can identify persons in specific areas from a small group of people (from 2 to 10 people). WiFi techniques can be applied in places such as smart homes and offices where there is an active WiFi connection. However, in places with door access and other temporary constructions, it is not reasonable to assume that WiFi system and electrically charged systems exist because WiFi systems need at least one router to establish a connected network, and this may not be available in the above scenarios. Sugino et al. [4] proposed a human motion detector with low energy Bluetooth beacons, based on the assumption that human activities can be detected using Bluetooth beacons. Compared with other popular device-free techniques such as WiFi and RFID, Bluetooth beacons are more portable and energy efficient. For example, Bluetooth beacons called iBeacon, use Bluetooth 4.0 techniques, which can run for more than one year without changing the batteries. The size of the Bluetooth beacons can be smaller than a coin and therefore, they can be deployed anywhere. Despite these advantages, Bluetooth signals have some limitations such as low sampling rates and unstable signal strength. The other drawback is that the coverage range of Bluetooth signals is smaller than the range of WiFi. According to our preliminary study and technical document, the valid range of Bluetooth beacons in a room is less than 10 meters. Although the range of standard beacons has been expanded to 70 meters, such signals are too weak to distinguish changes caused by obstacles. To the best of our knowledge, there is no work on exploring the potential use of Bluetooth Beacons for person identification problem.

Based on our preliminary studies, we aim to solve the person identification problem using Bluetooth signals. Moreover, we focused on a real application of identifying a person out of n known people in a door access system, using only Bluetooth signals in the environment. In this scenario, Bluetooth beacons are preferable. Bluetooth beacons do not require pre-installed infrastructure such as a power system, exchange routers or a network system. Bluetooth-based person identification only requires a couple of portable Bluetooth beacons and a battery operated receiver which can run for years. They can also be reused if the system is moved to other places. Additionally, low energy Bluetooth techniques can save more energy compared

W. Shao, K. Qin and F. D. Salim are with the School of Science (Computer Science), RMIT University, Melbourne, VIC 3001, Australia (e-mail: wei.shao@rmit.edu.au).

Thuong Nguyen is currently a research scientist at Trusting Social, Melbourne, Austrlia (e-mail: thuong@trustingsocial.com).

Moustafa Youssef is a professor at Alexandria University and Egypt-Japan University of Science and Technology (E-JUST) (e-mail: moustafa.youssef@gmail.com)

with other device-free approaches.

It is challenging to identify a person who enters a room using RF signals generated by Bluetooth beacons [5]. For example, in a key based door access system, people enter the room following a sequence of activities: walking to the door, getting the key from their pocket and standing in front of the door, inserting the key and opening the door, and finally, closing the door. Coarse-grained device-free techniques cannot distinguish every activity of every different person. However, through a series of experiments outlined in Section IV, we observed that the behavioural patterns of each different person in the door access process are slightly different. Further, the same individual is likely to adopt a similar pattern each time when accessing the door. For instance, some people tend to open the door with their hands, someone prefer to use their shoulder, and some even like to kick the door open. Though some people may open the door in the same way, the speed of opening and, the body angle varies among people, which presents an opportunity to identify people by their behaviours during the door access.

Inspired by our observations, we proposed a two-step identification process to identify a person during door access. The first step aims to recognise actions of each participant especially the length of each action. The second step is to identify the person using the temporal information of the actions. In the first step, we use Bluetooth signals to extract features for action recognition. As the recognised labels can be in any order and may not be an appropriate sequence of action, we align them using a dynamic programming technique to assure the order of the actions. In the second step, we use the recognised labels in the first step to compute temporal features of the actions. Since different person usually spend different amount of time on each action during door access, it is possible to identify each person with extracted temporal features. Another challenge associated with Bluetooth signals are the low sampling rate and noise. Compared with WiFi and RFID signals, the sampling rates of Bluetooth Beacons are much lower, which can undermine the ability to recognise people's actions during door access. To manage this problem, we applied a sinc interpolation method and a Kalman filter to remove the noise and compensate for the sampling rate.

We evaluated the BLEDoorGuard framework using two real-world cases: a door with a key lock and a door with a smart card lock. For each case study, we recruited two groups of volunteers (6 and 10 volunteers, respectively) to access doors. They were asked to conduct each action during door access as they usually did. Each participant repeated the door access procedure 10 to 20 times. A camera was used to capture the data collection process and to extract the action time and person identity for each door access process.

In short, our main contributions in this paper are:

- We conducted the preliminary studies to reveal the potential use of Bluetooth beacon in the person identification study.
- Based on a preliminary study, we designed a two-step algorithm to identify people. We employed the temporal features and activity recognition results to identify who opened and closed the door in the framework.
- We conducted an evaluation of BLEDoorGuard in real world scenarios and achieved acceptable performance. We recruited two groups of people, with the groups differing in the number of participants and designed a practical experiment. We built a complete dataset of videos and RF signal files. We applied the proposed framework to this dataset and identified the person from the groups with 6 and 10 people respectively, in two different scenarios.

The remainder of the paper is organised as follows. Section II introduces the related work. Section III provides an overall picture of the system design and goals. We conducted a preliminary study of Bluetooth characteristics for person identification in Section IV. The techniques used in data preprocessing and detection are shown in Section V. We designed and proposed a two-step algorithm in Section VI and conducted related experiments in Section VII. In Section VIII, we discuss the limitations of this paper and briefly propose some solutions in the future. We conclude in Section IX.

II. Related Work

Person Identification: Person identification is attracting widespread interest in ubiquitous computing research community. Cornelius proposed an approach which employed coherence between accelerometers on body to identify persons with on-body sensors [1], [6]. In their study, users were required to wear sensors for long periods in order to collect the data. It was highly invasive and annoying for the users to wear the devices for a long time, especially for elderly participants [4], [7]. There are some non-invasive approaches for user modelling leverage specifically designed infrastructure sensors which area embedded into the environment. For example, Orr and Abowd [8] used a force sensor installed under the floor to sense the ground reaction force of footsteps. Features were then extracted from signals of the force sensor and used to recognise people. Another line of work used a capacitive sensing system installed under the floor to track user's mobility trajectories, and identified users by recognising the patterns of their trajectories [9], [10]. These approaches, however, require installation of specifically designed infrastructure, which usually extremely expensive.

Device-Free Techniques: Device-free is a pervasive technique that can detect, localise, and recognise activities using radio signals. Device-free systems leverage radio-based wireless devices to capture the transmitting signals in the environment. As an object or a person may interfere with the signal, the mobility of this subject or person can be captured by the changes in signals. In device-free systems, the user does not need to carry any devices or sensors [11]. Device-free techniques have been used in many ubiquitous applications, such as indoor localisation [12]–[14], gesture recognition [15]–[17] and activity recognition [3], [18], [19]. Youssef outlines several challenges in the device-free area [20]. The main challenges include human detection, tracking and identification.

Device-Free Activity Recognition Human activity recognition is one of the most important applications of device-free technology. WiBreath [21] used the RF-based techniques to measure the respiration rate of users. WiSee [22] [23] claims that wireless signals enable gesture recognition in the whole room, which can be applied to non-line-of-sight and through-the-wall scenarios. They extracted gesture information by employing the Doppler shift effect. One of latest work proposed by Aljumaily [24] also used wireless networks to recognise human gestures. The magnitude of radio signals has been used for human activity recognition for many years. Since the magnitude of signals is easy to be influenced by environmental noise, WiFi CSI is introduced to activity recognition area and is widely used in many activity recognition applications [25], [26]. Kim et al. summarised some important works on device-free activity recognition with CSI data [27]. Bo et al. [28] recognised static and non-static activities with high accuracy using WiFi CSI. They extracted the weighted average value of the signals as the main feature for classification [29]. Another important sub-area in activity recognition is the motion detection. The RASID system [30] used a number of RF generators and a laptop as the receiver to detect the motion of users. Compared with existing work, their system is non-parametric and robust.

Device-free Person Profiling There are few studies on person identification using device-free techniques [31], [32]. WiDisc [33] is able to distinguish three different subjects by leveraging radio signals. It uses traditional fingerprint methodology and only needs few training data. However, this system, to some extent, cannot identify users as it only uses three classes of people– tall, medium and small. Nevertheless, this study provides useful preliminary work for attempting to identify a user profile using wireless signals. The state-of-the-art device-free technique involved person identification using WiFi CSI based gait recognition. Both WiWho and WiFi-ID attempt to recognise person in smart places such offices and rooms using WiFi CSI together with gait recognition approach [2], [34]. In these two works, their systems were evaluated using groups of 6 and 10 people. Interestingly, WiWho [2] and WiFi-ID [34] achieved a close accuracy with similar experimental settings and algorithm. WiWho removes the distant multipath noise and high frequency noise with FFT techniques while WiFi-ID remove the noise with a Butterworth filter and a median filter. WiWho detected the walking cycle of each person and extracted features of each step. It establishes a gait pattern profile by analysing step features. WiFi-ID separates signals with specific frequency and chooses the most distinguishable band as the unique sign of each person. Inspired by this work, we go further beyond user profiling to person identification, and investigate the feasibility of recognising user actions and explore the identity of users who access the door.

III. Overview

In this section, we define the problem of person identification during door access. We also describe the design goals and scenarios. Challenges and assumptions are also discussed, provides a clear overall view of BLEDoorGuard.

A. Preliminary

Definition 1: (Person during door access) A volunteer is a tuple $u =< f_t(\overrightarrow{a}), t_s, t_e >$, where $f_t(\overrightarrow{a})$ is the time person spend on each activity during door access and t_s and t_e are the start time and end time.

Definition 2: (Task) An access door task T is a sequence of activities associated with different time intervals. The order of each activity for each person is fixed but the time interval for each activity for each person can be different. Therefore, $T = a_1, a_2, ..., a_m$, where m denotes the number of activities during door access.

Definition 3: (Sensed data) The sensed information is represented as multiple channel time-series data $D = C_1, C_2, ..., C_d$, where d is the number of channels and C is the signal strength generated from Bluetooth beacons.

B. Problem Definition

Given volunteers $U = \{u_1, u_2..., u_n\}$ with a start location L_s and end location L_e, the person identification during door access problem is to recognise u_i from U with D generated from the door access task T performed by person u_i. Each volunteer u_i perform the same task and the associated data D is labelled with the ID of each person u_i.

C. Usage Scenarios

The Bluetooth beacons need to be located around the door noting that people walking up block the line-of-sight between the receiver and the beacons. The door can be key-based or card-based. Each person takes similar actions and follows the same order to open and close the door. The design goals of the system are low cost, device-free and privacy protected. The system should not be used in places where an error in person identification can lead to severe consequence since the accuracy cannot achieve 100 percentage. Though applicable scenarios therefore are limited, our system could also be useful in many privacy-orientated locations that do not require ultra high accuracy and where there is no complete infrastructure system such as a WiFi access point. More conveniently, such a system can be installed and unset effortlessly. Bluetooth beacons and receivers can be placed almost everywhere and no specific knowledge is required.

D. Challenges

Using Bluetooth beacons for person identification is challenging. First, although some studies [4] show that Bluetooth signals can detect and localise a person, it is not clear whether this can be applied to person identification problems. Secondly, the sampling rate of multiple beacons are lower than WiFi or RFID, which increases the difficulty in addressing the problem. Thirdly, impulse noise and multipath fading problem need to be addressed. Finally, human labelling errors have negative effects on the accuracy of classification, hence labels need to be aligned. We propose corresponding solutions to the above challenges in the following sections.

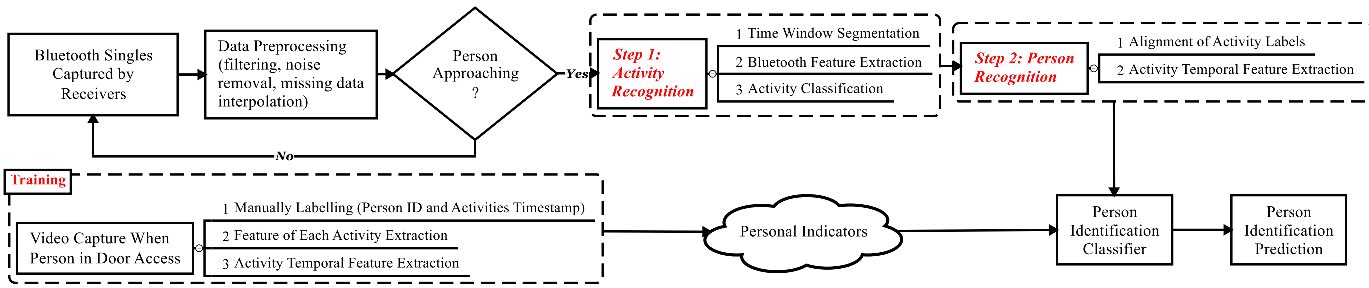


Fig. 1. BLEDoorGuard architecture.

E. Framework

Fig. 1 presents the framework of our person identification system which is comprised of three main components: data collecting and preprocessing, training and a two-step algorithm.

In the first component, as illustrated in the top left of Fig. 1, the Bluetooth receiver can obtain signals from Bluetooth beacons in the environment. In the first step, we placed multiple Bluetooth beacons inside and outside of the door. Each beacon periodically transmits Bluetooth signals corresponding to a preset frequency. Multiple channel time-series data was collected and stored in a database. In the second step, a Kalman filter [35] was applied to this data to solve the multipath fading and impulsive noise problem. Compared with other RF signals from WiFi and RFID, the sampling rate of Bluetooth signals is much lower (2 - 10 Hz). In addition, multiple Bluetooth beacons compete with each other, which leads to a further decrease in the sampling rate. The low sampling rate undermines the ability of predictive models to estimate the activities of person, and are likely to cause missing data problem in a short time window. Moreover, the signals from different channels are not synchronised due to propagation path length and competition. Therefore, an adequate method needs to be considered as a compensatory approach to increase the sampling rates and synchronise the channels. Sine interpolation is a sound interpolation method applicable to Bluetooth signals [36].

In the training session, a camera was used to capture videos during door access. For each task, we manually labelled corresponding time-series data with person ID u_i and timestamps for each action. The features are calculated for each time window where the window covers the entire actions during door access. The last step aims to analyse the temporal features of each person and build a training model with machine learning methods.

The proposed two-step algorithm consists of the action recognition aspect and the person identification aspect. In the action recognition aspect, the first step was to divide time-series data into fixed length non-overlapping time windows. In the second step, features were extracted from each time window. Finally, a classifier was used to recognise action of each time window. In the person identification aspect, the labels of action first are needed to be aligned, because the classifier does not take the order of activities into account. Therefore, we applied a dynamic programming alignment method to revise the labels of each time window. Finally, the time windows with the same label were combined and temporal features were calculated from each action. With the training data and temporal features extracted from testing sets, person ID can be recognised using machine learning classifiers.

F. Assumptions

BLEDoorGuard assumes everyone accesses the door with the same set of actions and that all actions are conducted in the same order. This is consistent with our observation that most people access the door with the same actions but with different time cost and all actions follow the same order. For example, standing in front of the door should always be undertaken after walking to the door. BLEDoorGuard system cannot track multiple person at the same time. The current BLEDoorGuard system can only identify a single person during door access. Multiple person identification has a significant effect on Bluetooth signals and requires more study. Bluetooth signals vary with any moving obstacle in the coverage area. Hence any other moving objects make the prediction more difficult. In summary, BLEDoorGuard is designed to identify a single person who accesses door with a set of fixed order activities detected by environmental Bluetooth signals at any given time.

IV. Feasibility Study

Although researchers have used WiFi or RFID to identify people in a device-free environment and have explored the characteristics of these two techniques, the properties of Bluetooth Beacons in such scenario are still unknown. Compared with RFID tags and WiFi generators, Bluetooth has its own unique features such as shorter range, lower tolerance of spatial density, orientation sensitivity, lower reading rate and occlusion effect. Therefore, we perform a series of experiments on Bluetooth Beacons which are similar to the experiments conducted in [2], in order to address the following questions:

- **Occlusion:** Is there any noticeable pattern in the Bluetooth signals when a person enters the Bluetooth coverage area? Does the orientation of the human body have a significant effect on signals strength?
- **Differences in Temporal Features Extracted from Activities Among People:** Can we only use temporal features of each action to distinguish them during a door access environment?

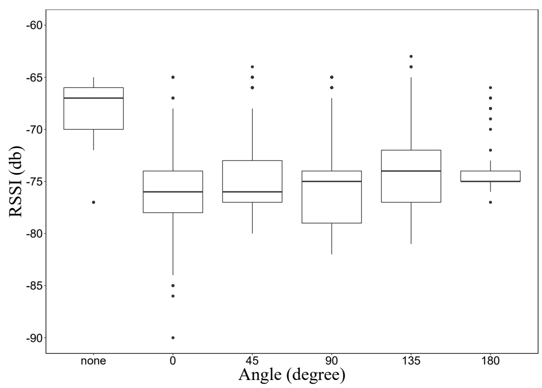


Fig. 2. Overall RSSI patterns for different rotation angles.

- **Consistency of Temporal Features of Each Action for the Same Person:** Do the temporal features extracted from actions during door access by the same person remain the same over time?

A. Occlusion with Human Body Orientation

We aim to identify people through signal variation. Hence, it is necessary to explore the correlation between the occlusion situation and signal strength. We asked 10 volunteers to stand in a different orientation relative to the mobile beacons and we measured RSSI when the subject rotated their body. The mobile device was positioned at 1 metre high and 2 metres away from the beacons. The location of people was on the line-of-sight between the receiver and beacons. Zero degree means the subject is facing the Beacon while 180 degree means the subject is facing to the mobile device. Additionally, the body of the subject rotates counter-clockwise during the process. In the experiment, we observe that the RSSI varies for each person in the case of 10 subjects. A box-plot graph of these results is shown as Fig. 2.

Fig. 2 illustrates the RSSI variation for different rotation angles of the 10 volunteers. The median RSSI value of the group with no occlusion in Fig. 2 is much higher than any other group, which suggests that RSSI values drop significantly if any subject blocks the line-of-sight between the Bluetooth beacons and the receiver. Additionally, the medians (which generally will be close to the average) of those groups with different occlusion values are all at similar levels, although the box plots in these groups show different distributions. The groups with 0 and 180 degree rotation angles tend to have higher signal strength. In contrast, groups with the other three rotation angles (45, 90 and 135 degrees) had lower RSSI results. The conclusion drawn from Fig. 2 related to the first question above, suggests that it is possible to detect a person during the door access area with signal strength alone, and that different occlusion angles lead to variations in RSSI.

B. Actions during Door Access

One assumption of our system is that each person accesses the door via a series of actions of fixed order. Therefore, it is important to verify that it is possible to recognise activities

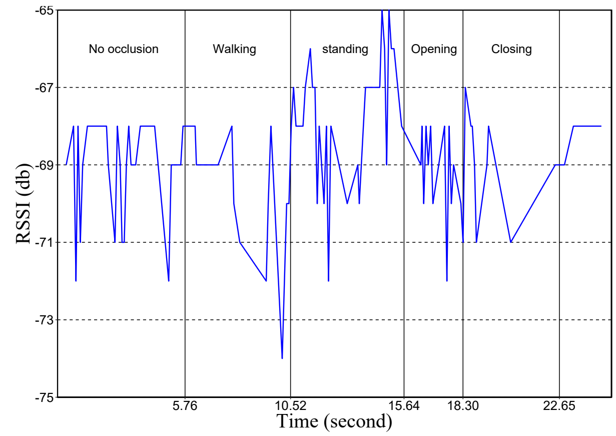


Fig. 3. Signal strength for activities during door access.

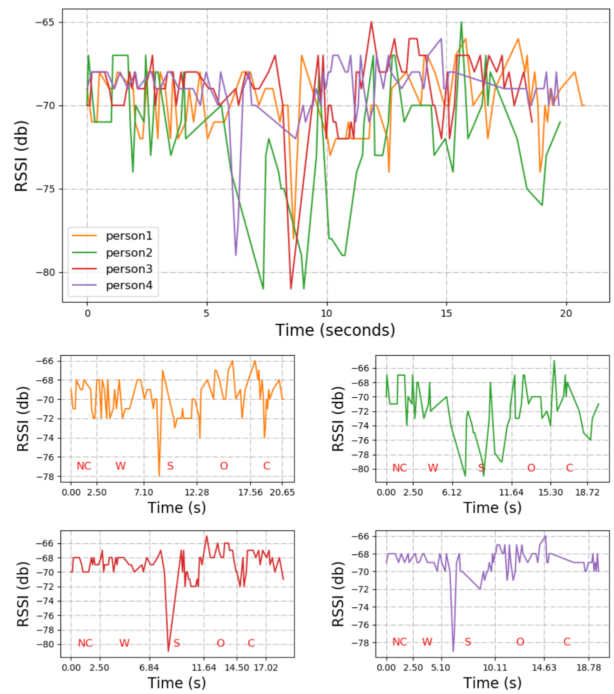


Fig. 4. Signal strength for activities of multiple people.

from signal strength, and that temporal features extracted from those actions are different for each person. The door access actions consist of walking to the door, standing in front of the door, pushing the door and closing the door. Each action has its own unique identity in the shape of the signals. Therefore, we deployed a single mobile device and four Bluetooth beacons within a reasonable range of the mobile device and collect signals from them. In the preliminary study, We choose the beacon which was located behind the door as an example and draw the variation of signal during door access and each action time window of this beacon in Fig. 3.

We divided whole signal session into four parts. In the first part, the person is walking towards the door without any limitations or particular requirements. That is, the person walked the same way as they did in everyday life. In the second step, the person is standing in front of the door and inserting the key. Then the person tries to open and close the door. All labels of actions reflected the typical pattern people follow to access the door. We set a start point and end point for the scenario. The start point was around 2 meters outside the door. The end point was positioned inside the door. The volunteers were required to walk from the starting point to the ending point without any on-body device.

From Fig. 3, it can be observed that the signal strength fell when people approached the door because the person blocked the line-of-sight from the Bluetooth beacons and the receiver. In the standing phase, signal strength does not vary much because the person does not move. A static subject has a small effect on signal strength, which has been tested in the occlusion part of the experiment. When the subject opens the door, this lead to a rise in signal strength because the door cannot block the line-of-sight any more. Finally, the door is closed and the signal strength returns to the original level. Fig. 3 shows that the action of people during door access can be observed from variation in signal strength.

We repeated same experiments for four different people and illustrated the RSSI variation during the process in Fig 4. In the Fig 4, we observe that RSSI profile from each person are significantly different in each action. Nevertheless, it is still difficult to distinguish people only with RSSI profile. Therefore, we propose a two-step algorithm in this paper to transform the RSSI profile to temporal features. In the next subsection, we will show that temporal information is a more effective sign to distinguish persons.

C. Differences in Temporal Domain of Actions Between Two People

Although we are able to detect a person and recognise their actions from Bluetooth signals. More experiments are required to confirm whether temporal features extracted from actions during door access are sufficient to distinguish different people. In order to investigate these differences, a multiple person comparison experiment was conducted. We randomly chose two volunteers from the group and asked them to access the door 20 times. For each round, the temporal features were extracted from each action. As a result, two 4×20 matrices compose of time cost for each action were generated. We conducted a two sample unpaired t test to examine whether these temporal features were statistically significant different. Table I shows that the p value of all actions were less than 0.05. It can be concluded that there is a statistically significant difference between the means of the two groups. That is, the temporal features such as the mean time taken for each action are different for different people. Consequently, it is possible to identify a small group of people with only temporal features of each action during door access.

D. Consistency of Temporal Features of Actions over Time

In this study, it was important to confirm that the temporal features of each action of the same person should remain the same over time in the same scenario. In order to verify the consistency problem, subjects were asked to repeat the door access procedure 20 times over two days. The subjects undertook four actions each time, and these were completed 10 times on each day. Prior to each round, they were asked to wait for three minutes. The box-plot graph of the results is illustrated in Fig. 5. It shows that the time elapsed for each action each time by the same person are similar even across the span of a day.

TABLE I
THE RESULTS OF TWO SAMPLE UNPAIRED T TEST FOR TEMPORAL FEATURES OF EACH ACTION OF TWO PEOPLE.

Action	p-value	$\mu(Person1)$	$\mu(Person2)$
Walking	1.742e−7	4.66	3.87
Standing	6.942e−12	4.86	1.20
Opening	1.833e−9	2.50	1.72
Closing	0.019 82	3.40	3.18

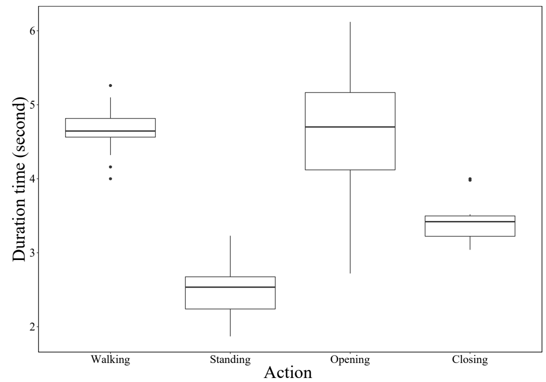


Fig. 5. The time cost for different action of the same person.

E. Summary of Preliminary Study

From the above preliminary study, we can conclude that Bluetooth signals can detect door access activity and recognise activities based on the temporal features of each action. In addition, Bluetooth signals for each action for the same person remain similar over time. This motivated us to design a person identification system based on Bluetooth signals and the temporal features of each action.

V. BLUETOOTH SIGNALS PREPROCESSING

The signals were generated from Bluetooth low energy (BLE) beacons which employ Bluetooth 4.0 standard. There are numerous advantages of BLE beacons such as low energy consumption, small size and portability. However, compared with other device-free techniques, BLE beacons signal processing is more difficult due to its specific characteristics. We conducted a series of experiments to test the BLE Beacons we had at hand and also investigate other studies on Bluetooth signals. Finally, we summarize some key points we need to pay attention to in the system and approach design. Firstly, the sampling rate of BLE Beacons is lower than other device-free techniques such as WiFi CSI and RFID. The maximum sampling rate of BLE Beacons we have is 10 Hz. The real sampling rate we finally obtained is even lower than this setting frequency because the power of the receiver also plays an important role in sampling rates. Also, multiple beacons competition has a negative effect on sampling rates and quality of signals. As a consequence, the signal data we obtained are sparse in temporal domain and the timestamps were likely to be shifted. Hence, We need a signal interpolation methodology to compensate. Secondly, multipath fading problem affects the RF signals [37]. Multipath fading problem is caused by reflection from a distant object or person. The Bluetooth Beacons propagate signals in environment and signals are reflected by the obstacles in different position, which results in multipath inference and causing multipath fading problem. Lastly, the normal noise such as impulse noise is common appeared in the Bluetooth signals, which has a negative effect on the accuracy of action recognition. Due to these factors, we need to consider two important issues in data preprocessing – (1) noise filtering and (2) signal interpolation.

A. Noise Removal

There are two primary types of noise data in Bluetooth signals, multipath fading and impulse noise. To address this, we applied Kalman filter and median filter to the signals processing. The Kalman filter is a conventional method used to handle multipath fading problems [38] and the median filter is good at removing impulse data. Based on our observation, we set the time window with 1 second length. We used the robust adaptive online repeated median filter package [39] which is good at processing low frequency time-series signals to remove impulse noise. The Kalman filter [40] with default settings was applied to fix the multipath fading problem.

B. Sinc Interpolation

To address the issue of low sampling rates in the Bluetooth signals, we need to compute signals values at an arbitrary continuous time from existing discrete-time samples of the signal amplitude. Sinc aims to resample the signals using sine cardinal function. Before sinc interpolation, the sampling rates varies from 2 Hz to 10 Hz, and it is difficult to extract features with fixed length time windows. This is because sometimes a window contains no data points. Interpolation method is capable of fill the window which contains no any data points. The other advantage to use the interpolation is the synchronisation between different Bluetooth beacons. In our experiment, multiple Bluetooth beacons with different time systems are used for transmitting signals. Although each Bluetooth beacon transmits signals at the same sampling rate, the receiver tends to obtain data selectively. That is, the sampling rates of each beacon in the receiver terminal are different. Consequently, if we apply a fixed length window to time-series signals from different beacons, some may only have data from a subset of beacons. The sinc interpolation method solves this problem as signal data from all channels is continuous after the resampling.

VI. A Two Step Person Identification algorithm

With the hypothesis that people take the same actions with different time during the door access, we implemented the recognition algorithm in two steps (shown in algorithm VI). In the first step, we recognised the actions during door access by classifying the Bluetooth signals. Then in the second step, we used the actions recognised in the first step to derive temporal features of each action. The person who accesses the door can be identified by these temporal features with classifiers. The details of these steps are described in algorithm VI.

Algorithm 1 Two - Step Person Identification Algorithm

Input: The set of RSSI records for all the activities, R_n;
Output: Predicted result of different persons' ID, I_n;

```
Step 1 (Action Recognition):
Apply time segmentation to R_n;
for each time segment s ∈ R_n do
    for each beacon b ∈ s do
        Calculate the number num, mean μ and standard
          deviation σ for the RSSI values;
        Create a new list l with b, num, μ and σ;
        Add l to the set T_n;
    end for
end for
Apply normalisation to T_n;
for each record r ∈ T_n do
    Predict action label through r via traditional classifiers;
end for
Build matrix P with each cell(i, j) that is the probability
  of assigning segment j to action i;
Obtain a new matrix D in which the elements are com-
  puted via Equation 1;
Arrange the action labels ∈ T_n in time order by tracking
  backward from D;
Step 2 (Person Identification):
for each action a ∈ T_n do
    Compute the time duration t for a;
    Add t and a as new row into set J_n
end for
Apply normalisation for t ∈ J_n;
Predict the persons' ID I_n through J_n;
return I_n;
```

A. Action Recognition Using Bluetooth Signals

In this step, we recognised the actions performed by the users during door access. These actions include walking, standing, opening the door and closing the door. We divided the sequences into one second segments and dealt with each segment as a sample for action classification. We used Bluetooth signals to derive the features. We considered each pair of a BLE beacon and a phone as a data channel. The total number of channels may vary in different settings. For example, in our case study 1, we used 4 BLE beacons and one mobile device, which established 4 channels. For each channel in a time window, we extracted three features: the number of readings, mean and standard deviation of signal strengths. We then normalised these features to a unit range and use them as input features for action classification. We tested our framework using some traditional classifiers: decision tree, simple artificial neural network and random

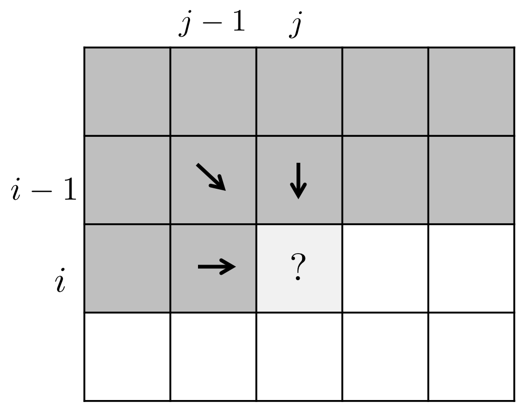


Fig. 6. An illustration of dynamic programming alignment of action labels to the segments.

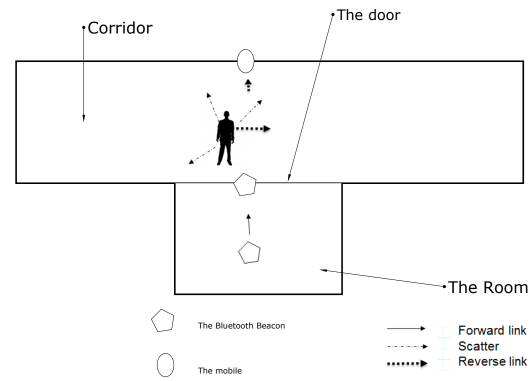


Fig. 7. A general layout of BLEDoorGuard.

forests. We also used some neuron networks-based methods such as multilayer perceptron(MLP), Long short-term memory (LSTM) and Gated recurrent unit (GRU) to solve this problem. For MLP, The input layer for each classifier consisted of features extracted from each time window. The output layer listed the actions during the door access process. For LSTM and GRU, as we interpolated Bluetooth signals, the frequency of signals are the same for all samples. Therefore, we can use the magnitude of signals as the input. In this experiment, we use an existing code to recognise each action [41]. We also modified the code to GRU-based version.

In the classification process, there is no constraint on the predicted labels in a sequence of segments, they can be in any order, e.g. open the door then insert the key. Therefore, we need to form them into an appropriate order. For this we perform a smoothing step using a dynamic programming technique. Input of this smoothing step is a matrix P with one dimension representing the segments in a sequence and the other one representing the action labels. Each cell (i, j) in the matrix is the probability of assigning segment j to action i. The aim of this smoothing process is to obtain a matrix D in which the elements are computed as:

$$D_{i,j} = P_{i,j} \times min\left[D_{i-1,j-1}, D_{i-1,j}, D_{i,j-1}\right] \tag{1}$$

where $P_{i,j}$ is the probability of assigning segment j to action i. This filling process is illustrated in Fig. 6. After filling the whole matrix D, we can find the appropriate action assignment by tracing backward from the bottom right corner.

After applying this smoothing, the predicted action labels are in a designated order. More importantly, the segments that are classified into a particular action are consecutive in time order. Therefore, we can use them to compute temporal features of action for user identification in the second step.

B. Person Identification Using Two Step Approach

Using the recognised labels of actions, we derived the temporal features, i.e, the time duration for each action. We computed the time interval for each action and normalized this to a unit sum. We use these normalised numbers as features for classification. Similar to the previous step, we employed three traditional classifiers: decision tree, neural networks and random forests. We also applied the MLP to this supervised classification problem. The input layer of each classifier consists of the temporal interval for each action of each time window. The output layer lists the ID of each person. In this step, LSTM and GRU are also used. The input is a series of temporal information of each action of one sample. The output is the identify of a specific person.

VII. Experiment Setting and Results

We evaluated our approach in two case studies corresponding to two popular types of doors: access using keys and access using smart cards.

A. The BLEDoorGuard System and Settings

We propose a framework to recognise each action in door access and use the temporal features of actions to identify person. Our BLEDoorGuard framework leverages 2.4 GHz wireless devices deployed in the environment to collect the data, and volunteers do not need to carry any devices. Multiple Bluetooth Low Energy (BLE) beacons are used as the signal transmitters, and a cheap Android phone with Bluetooth component is used as the signal receiver. These devices were deployed around the door area so that the person or the door can interfere the line of sight between the transmitter and receiver. This deployment can capture the interference of the user or the door via changes in RSSI. Fig. 7 shows a general scenario. The user is under the converge of Bluetooth signals. In different scenarios, the deployment of beacons are also different. For example, the deployment of beacons in case study 1 - the door with key lock is illustrated in Fig. 8. In this figure, two BLE beacons are attached to the door in order to capture the changes of door position and the presence of users when they stand in front of the door. Other beacons are deployed opposite to the door, behind the door and at the top of the door. The receiver (the mobile device) is placed opposite the door to capture the RSSI signals from each beacon. The phone and three beacons are placed at the same height at 1

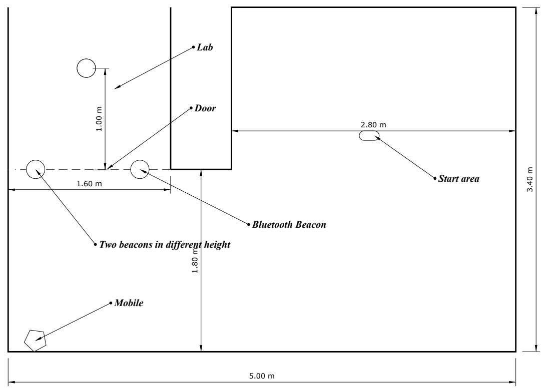


Fig. 8. Layout of beacon and phone setting in case study 1.

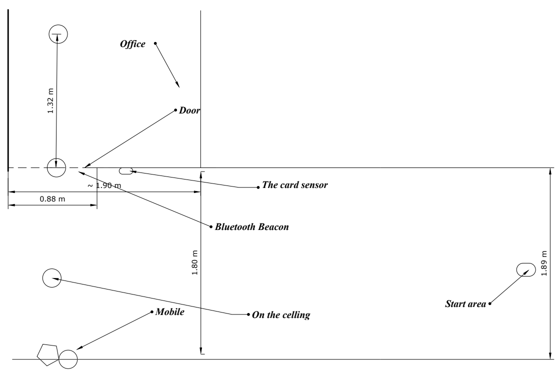


Fig. 9. Layout of beacon and phone setting in case study 2.

meter. An beacon is set at 1.8 meters height at the door as we want to also use the height of the people to distinguish them. This is because taller people are more likely to occlude the signals from that beacon. Fig. 9 shows another case which uses a smart card instead of the key. It takes less time than the first case, therefore the difficulty of the second case become much higher. The results also show that the accuracy is less than that in the first case.

An important aspect of this framework is the sampling rate of the devices. To identify this, we ran several tests on different types of phones and noted the difference at maximum sampling rates. For example, a HUAWEI P7 was able to capture around 10 Bluetooth samples per second, while an LG 40 could record only about 5 samples per second. The missing rate of Bluetooth samples could increase gradually when more beacons were deployed around the phone. Therefore, the number of beacons needs to be controlled properly in order to get an optimal recorded rate of recorded samples for data analysis. We finally decided to use a sampling rate of 8 Hz for our experiments.

To capture Bluetooth scans in the phones, we implemented an Android application that can regularly scan for surrounding Bluetooth signals and record the detected MAC address, RSSI and time stamp. We also need to record the ground-truth of time interval required for each action during door access. For this, we used a camera to record the whole process of the experiment and extracted the start and end time of each action which were observed from the video.

B. Case Study 1: Access Using Keys

1) Data Collection: In this first experiment, we applied our framework to a door which is accessed by a key. To capture the Bluetooth data, we deployed four beacons and one mobile device at different position facing the door. We set the sampling rate at 10 Hz. There were ten participants in the data collection procedure. Each participant was requested to perform the process of 4 actions described above, repeating the process several times. In total, we obtained 200 samples from ten users. The start and end time stamp of each action along with the identification of the users were recorded.

2) Person Identification Using Temporal Features: To first test our hypothesis on the unique manner of accessing the door, we evaluated user classification using temporal features derived from the ground-truth labels. For every door access (considered as a sample), we computed the time interval required for each action. We normalised these features to a unit sum, i.e. the sum of all features in a sample is equal to 1. We tested with three traditional classifiers (decision tree, simple neural networks and random forests) and deep learning methods (MLP, LSTM and GRU).

We randomly split the data into training and validating sets with equal numbers of samples. We fed the training data to the classifiers to obtain the trained model and used the trained model to classify the samples in the validation set. We computed the accuracy of the classifier by computing the rate of correct samples over the total number of samples in the validation set. We repeated the process 100 times and random forests were performed the best achieving a mean accuracy of 91 percent (See Table II). This high performance of user identification verify the feasibility of our hypothesis.

Motivated by the high performance obtained on the temporal features derived from ground-truth, we demonstrate the use of Bluetooth signals for user identification in a two-step process as below.

TABLE II
ACCURACY OF USER CLASSIFICATION USING TEMPORAL FEATURES OF ACTIONS ON KEY DATA

Classifier	Accuracy
Decision tree	0.79
Neural Network	0.82
MLP	0.85
LSTM	0.75
GRU	0.76
Random Forests	**0.91**

3) Action Recognition Using Bluetooth Signals: The aim of this step was to recognise the actions from Bluetooth signals. For this, we firstly segmented the data into 1.0 second time windows with 0.9 second overlaps. We then computed the number of readings, and the mean and standard deviation of each data channel during each time window. As there were four beacons and one mobile device in this experiment, we had four data channels. In total, we derived 12 features. We use $1/3$

TABLE III
ACCURACY OF ACTION CLASSIFICATION USING BLUETOOTH SIGNALS ON KEY DATA

Classifier	Non-smoothing	Smoothing
Decision tree	0.35	0.61
Neural network	0.42	0.62
MLP	0.49	0.64
LSTM	0.50	0.66
GRU	0.42	0.60
Random forests	0.50	**0.70**

TABLE IV
ACCURACY OF PERSON CLASSIFICATION USING TWO-STEP APPROACH ON KEY DATA

Classifier	Accuracy
Random guess	0.10
Decision tree	0.41
Neural Network	0.45
MLP	0.49
LSTM	0.36
GRU	0.32
Random Forests	**0.62**

of the data as the training set and evaluate using the remaining set. The reason for this split rate is that we will further split the validation set into a training and a test set to evaluate the user identification in the next subsection. The segments of a particular sequence (a door access) belong to either the training set or the test set. We fed the training data to the classifiers and used the trained model to classify the samples in the validation set. We repeated the whole process 10 times and report the mean accuracy obtained by three classifiers in the second column of Table III.

We then applied the smoothing step (cf. Fig. 6) on the classification results of the aforementioned classifiers and report the mean accuracy in the third column of Table III. As can be seen in the table, this smoothing step improves the accuracy of 26% for decision tree and 20% for random forests. Random Forest performed the best among all classifiers in this experiment.

4) Person Identification Using Two-Step Approach: In this step, we use the action labels given by random forests (the best classifier) to extract temporal features of the actions similar to that of Section VII-B2. We randomly split the validation set in the previous step into two sets that have equal number of samples to make the training set and test set. We feed the train data to the classifiers and use the trained model to classify the samples in test set. We repeat the whole process 10 times for each validation set of step 2 to make 100 pairs of training and test sets. We report the average accuracy in Table IV. The highest accuracy, about 62 percent, is obtained by random forests.

C. Case Study 2: Accessing Using Smart Cards

1) Data Collection: In this second experiment, we examined our framework on a door locked using a smart card lock. The series of actions performed during each door access was similar to the previous experiment, except that the unlocking action was performed using a smart card instead of a key. We tested our framework using a different setting of four BLE beacons and one phone. We recruited six participants, each performed the door access 10 times. In total, we recorded 60 samples for the six users.

2) Person Identification Using Temporal Features: Similar to case study 1, we firstly used temporal features derived from the ground-truth labels to identify the users. We randomly split the data into training and test sets with equal numbers of samples. We repeated this evaluation 100 times and report the average accuracy in Table V. The highest accuracy, about 93%, was again obtained by random forests, identifying six different users on average. The result shows that it is also feasible to distinguish person access the door using temporal features.

TABLE V
ACCURACY OF USER CLASSIFICATION USING TEMPORAL FEATURES OF ACTIVITIES ON SMART CARD DATA

Classifier	Accuracy
Decision tree	0.72
Neural network	0.87
MLP	0.90
LSTM	0.68
GRU	0.72
Random forests	**0.93**

3) Person Identification Using a Two Step Approach: We repeated the same process in the first case study. The mean accuracy for action classification is reported in Table VI. This table shows that the smoothing step improved the accuracy about 16% to 19%, and the highest accuracy was also obtained by random forests.

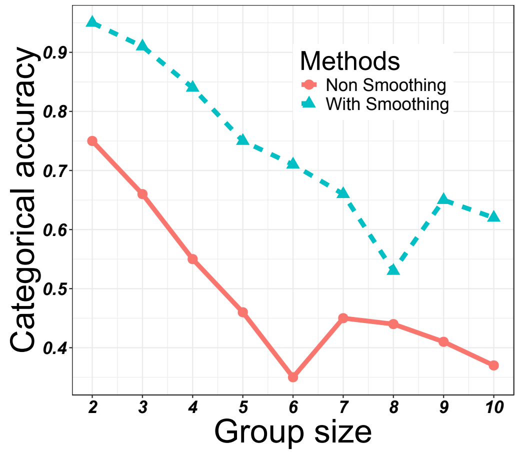
The average accuracy for user classification using recognised actions is reported in Table VII. We also report the accuracy of random guesses as a baseline method. As shown in Table VII, the accuracy obtained by our approach is much higher than that of random guesses.

TABLE VI
ACCURACY OF ACTION CLASSIFICATION USING BLUETOOTH SIGNALS ON SMART CARD DATA

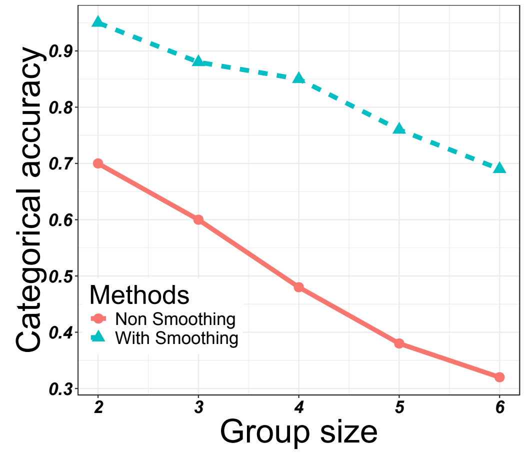
Classifier	Non-smoothing	Smoothing
Decision tree	0.42	0.61
Neural network	0.44	0.62
MLP	0.49	0.65
LSTM	0.38	0.58
GRU	0.42	0.61
Random forests	0.59	**0.75**

TABLE VII
ACCURACY OF USER CLASSIFICATION USING TWO-STEP APPROACH ON SMART CARD DATA

Classifier	Accuracy
Random guess	0.17
Decision tree	0.35
Neural network	0.23
MLP	0.65
LSTM	0.30
GRU	0.34
Random forests	**0.69**



(a) Door access with the key



(b) Door access with the card

Fig. 10. The accuracy in person identification with different group sizes. We compared methods with smoothing step and without smoothing step. The left figure shows the experimental result in case 1 and the right one shows the case 2.

D. Person Identification with Different Group Sizes

For each of the group sizes, we evaluated the BLE-DoorGuard with random forests. Fig. 10 shows the average accuracy of person identification with different group sizes for non-smoothing identification and smoothing identification in both scenarios. With increasing group size, person identification drops for both non-smoothing and with- smoothing methods. It is because that larger group increases the chances that people have similar temporal features in door access. We found that the smoothing method significantly boosted the accuracy of person identification across all group sizes. In summary, group sizes play an important role in person identification accuracy in our system. Since our system was applied to small groups of people who were accessing the same room, we believe it still practical and useful in these cases.

VIII. LIMITATIONS AND FUTURE WORK

In this section, we discuss several limitations of the current framework and algorithm, along with our ongoing work and potential future directions.

Firstly, the low accuracy of person identification in the large group undermines the capacity of this system. Higher accuracy is needed if we would like to apply the framework to more scenarios, especially for security monitoring. There are two potential solutions to improve the accuracy of the current system. Firstly, the size of the training set used in our experiment is limited. Larger training sets with more people and more samples is likely to boost the accuracy of person recognition. We can also conduct more experiments with different setting and different groups of people, which also can boost the accuracy. In our experiments, deep learning solutions did not perform better than some traditional classifiers. It is because that the number of training samples is too small for complicated networks. Underfitting problem is obvious in our experiments. The second solution is to use more advanced Bluetooth beacons. IoT techniques are booming in recent years, which provides more advanced hardware include new Bluetooth beacons. High frequency and more robust Beacons are likely to improve the accuracy because we can get richer information such as details of human activities.

Secondly, the case studies in this paper are specific. Applying our framework in varies scenarios such as human behaviour recognition, shopping habit profiling and working style identification is our next goal. All applications should be relevant to person identification and activities, and temporal features should have significant effect on distinguishing persons.

Thirdly, the system was not used in real life, but was only tested in controlled experiments. In the future, we will apply this system to more sophisticated environment with larger group of people. Additionally, our framework is not specific to Bluetooth. It can also be applied to other RF-based system such as WiFI or RFID. We plan to use other RF-based technique to evaluate our two-step approaches in the future.

IX. CONCLUSIONS

We have presented the BLEDoorGuard framework using Bluetooth beacons and receivers to recognise person during door access. We also explored the characteristics of the use of Bluetooth in person identification problems. We evaluated our framework on two different case studies: a door with a key lock and a door with a smart card lock. Using the recognised action labels to compute temporal features for user identification, we achieve 95 to 62 percent accuracy from 2 to 10 person respectively. Our experiments show that the BLEDoorGuard is feasible for person identification during door access with limited number of people. More complicated and real-world scenarios would be considered in the future experiments. Our framework is potentially to be extended to many similar person identification scenarios such as hotel check, hospital check and car driver identification. We plan to commercialise the system and collaborate with industrial partners in the future. More studies can be conducted with different real-world scenarios and more participants.

ACKNOWLEDGEMENT

We acknowledge the support for Wei Shao's scholarship from RMIT Sustainable Urban Precincts Program and Northrop Grumman Corporation. This research was also supported partially by the Australian Government through the Australian Research Council's Linkage Projects funding scheme (project LP150100246; CIs J Burry, S. Watkins, F. Salim, A. Mohammed).

REFERENCES

[1] C. T. Cornelius and D. F. Kotz, "Recognizing whether sensors are on the same body," *Pervasive and Mobile Computing*, vol. 8, no. 6, pp. 822–836, 2012.

[2] Y. Zeng, P. H. Pathak, and P. Mohapatra, "Wiwho: Wifi-based person identification in smart spaces," in *2016 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, 2016, Conference Proceedings, pp. 1–12.

[3] Y. Wang, J. Liu, Y. Chen, M. Gruteser, J. Yang, and H. Liu, "E-eyes: device-free location-oriented activity identification using fine-grained wifi signatures," in *Proceedings of the 20th annual international conference on Mobile computing and networking*. ACM, 2014, pp. 617–628.

[4] K. Sugino, Y. Niwa, S. Shiramatsu, T. Ozono, and T. Shintani, "Developing a human motion detector using bluetooth beacons and its applications," *Information Engineering Express*, vol. 1, no. 4, pp. 95–105, 2015.

[5] W. Shao, F. D. Salim, T. Nguyen, and M. Youssef, "Who opened the room? device-free person identification using bluetooth signals in door access," in *Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017 IEEE International Conference on*. IEEE, 2017, pp. 68–75.

[6] C. Cornelius, R. Peterson, J. Skinner, R. Halter, and D. Kotz, "A wearable system that knows who wears it," pp. 55–67, 2014.

[7] R. L. Shinmoto Torres, D. C. Ranasinghe, S. Qinfeng, and A. P. Sample, "Sensor enabled wearable rfid technology for mitigating the risk of falls near beds," in *RFID (RFID), 2013 IEEE International Conference on*, 2013, Conference Proceedings, pp. 191–198.

[8] R. J. Orr and G. D. Abowd, "The smart floor: a mechanism for natural user identification and tracking," in *CHI'00 extended abstracts on Human factors in computing systems*. ACM, 2000, pp. 275–276.

[9] M. Valtonen, L. Kaila, J. Mäentausta, and J. Vanhala, "Unobtrusive human height and posture recognition with a capacitive sensor," *Journal of Ambient Intelligence and Smart Environments*, vol. 3, no. 4, pp. 305–332, 2011.

[10] M. Valtonen, T. Vuorela, L. Kaila, and J. Vanhala, "Capacitive indoor positioning and contact sensing for activity recognition in smart homes," *Journal of Ambient Intelligence and Smart Environments*, vol. 4, no. 4, pp. 305–334, 2012.

[11] M. Scholz, S. Sigg, H. R. Schmidtke, and M. Beigl, "Challenges for device-free radio-based activity recognition," in *Proceedings of the 3rd workshop on Context Systems, Design, Evaluation and Optimisation (CoSDEO 2011), in Conjunction with MobiQuitous*, 2011, Conference Proceedings.

[12] N. Patwari and J. Wilson, "Rf sensor networks for device-free localization: Measurements, models, and algorithms," *Proceedings of the IEEE*, vol. 98, no. 11, pp. 1961–1973, 2010.

[13] M. Seifeldin, A. Saeed, A. E. Kosba, A. El-Keyi, and M. Youssef, "Nuzzer: A large-scale device-free passive localization system for wireless environments," *Mobile Computing, IEEE Transactions on*, vol. 12, no. 7, pp. 1321–1334, 2013.

[14] J. Wilson and N. Patwari, "A fade-level skew-laplace signal strength model for device-free localization with wireless networks," *Mobile Computing, IEEE Transactions on*, vol. 11, no. 6, pp. 947–958, 2012.

[15] Q. Pu, S. Gupta, S. Gollakota, and S. Patel, "Whole-home gesture recognition using wireless signals," pp. 27–38, 2013.

[16] S. S. Rautaray and A. Agrawal, "Real time multiple hand gesture recognition system for human computer interaction," *International Journal of Intelligent Systems and Applications*, vol. 4, no. 5, p. 56, 2012.

[17] L. Yao, Q. Sheng, W. Ruan, T. Gu, X. Li, N. Falkner, and Z. Yang, "Rf-care: device-free posture recognition for elderly people using a passive rfid tag array," in *MobiQuitous 2015: the way to foster research collaboration in Ubiquitous Computing*. Associaion for Computing Machinery, 2015, pp. 1–10.

[18] S. Sigg, M. Scholz, S. Shi, Y. Ji, and M. Beigl, "Rf-sensing of activities from non-cooperative subjects in device-free recognition systems using ambient and local signals," *Mobile Computing, IEEE Transactions on*, vol. 13, no. 4, pp. 907–920, 2014.

[19] S. Wang and G. Zhou, "A review on radio based activity recognition," *Digital Communications and Networks*, 2015.

[20] M. Youssef, M. Mah, and A. Agrawala, "Challenges: device-free passive localization for wireless environments," in *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*. ACM, 2007, pp. 222–229.

[21] R. Ravichandran, E. Saba, C. Ke-Yu, M. Goel, S. Gupta, and S. N. Patel, "Wibreathe: Estimating respiration rate using wireless signals in natural settings in the home," in *Pervasive Computing and Communications (PerCom), 2015 IEEE International Conference on*, 2014, Conference Proceedings, pp. 131–139.

[22] L. Garber, "Gestural technology: Moving interfaces in a new direction [technology news]," *Computer*, vol. 46, no. 10, pp. 22–25, 2013.

[23] Q. Pu, S. Gupta, S. Gollakota, and S. Patel, "Gesture recognition using wireless signals," *GetMobile: Mobile Computing and Communications*, vol. 18, no. 4, pp. 15–18, 2015.

[24] M. S. Aljumaily and G. A. Al-Suhail, "Towards ubiquitous human gestures recognition using wireless networks," *International Journal of Pervasive Computing and Communications*, vol. 13, no. 4, pp. 408–418, 2017.

[25] Z. Wang, B. Guo, Z. Yu, and X. Zhou, "Wi-fi csi based behavior recognition: From signals, actions to activities," *arXiv preprint arXiv:1712.00146*, 2017.

[26] B. Tan, Q. Chen, K. Chetty, K. Woodbridge, W. Li, and R. Piechocki, "Exploiting wifi channel state information for residential healthcare informatics," *arXiv preprint arXiv:1712.03401*, 2017.

[27] S.-C. Kim, "Device-free activity recognition using csi & big data analysis: A survey," in *Ubiquitous and Future Networks (ICUFN), 2017 Ninth International Conference on*. IEEE, 2017, pp. 539–541.

[28] B. Wei, W. Hu, M. Yang, and C. T. Chou, "Radio-based device-free activity recognition with radio frequency interference," pp. 154–165, 2015.

[29] J. Wright, A. Y. Yang, A. Ganesh, S. S. Sastry, and Y. Ma, "Robust face recognition via sparse representation," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 31, no. 2, pp. 210–227, 2009.

[30] A. E. Kosba, A. Saeed, and M. Youssef, "Rasid: A robust wlan device-free passive motion detection system," in *Pervasive computing and communications (PerCom), 2012 IEEE international conference on*. IEEE, 2012, pp. 180–189.

[31] Y. Chen, W. Dong, Y. Gao, X. Liu, and T. Gu, "Rapid: a multimodal and device-free approach using noise estimation for robust person identification," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 1, no. 3, p. 41, 2017.

[32] J. Lv, W. Yang, and D. Man, "Device-free passive identity identification via wifi signals," *Sensors*, vol. 17, no. 11, p. 2520, 2017.

[33] M. Scholz, L. Kohout, M. Horne, M. Budde, M. Beigl, and M. A. Youssef, "Device-free radio-based low overhead identification of subject classes," in *Proceedings of the 2nd workshop on Workshop on Physical Analytics*. ACM, 2015, pp. 1–6.

[34] J. Zhang, B. Wei, W. Hu, and S. S. Kanhere, "Wifi-id: Human identification using wifi signal," *Distributed Computing in Sensor Systems (DCOSS), 2016 International Conference on*, pp. 75–82, 2016.

[35] R. E. Kalman, "A new approach to linear filtering and prediction problems," *Journal of Basic Engineering*, vol. 82, no. 1, pp. 35–45, 1960.

[36] H.-l. DAI and M. ZHANG, "The embedded data acquisition system based on the bluetooth technology [j]," *Journal of Changchun University of Technology (Natural Science Edition)*, vol. 4, p. 008, 2007.

[37] A. Soltanian and R. E. Van Dyck, "Performance of the bluetooth system in fading dispersive channels and interference," in *Global Telecommunications Conference, 2001. GLOBECOM'01. IEEE*, vol. 6. IEEE, 2001, pp. 3499–3503.

[38] X. Liu, K. C. Teh, and E. Gunawan, "Blind adaptive kalman filter-based multiuser detector over a multipath fading channel," *IEEE communications letters*, vol. 8, no. 6, pp. 342–344, 2004.

[39] K. Schettlinger, R. Fried, and U. Gather, "Real-time signal processing by adaptive repeated median filters," *International Journal of Adaptive Control and Signal Processing*, vol. 24, no. 5, pp. 346–362, 2010.

[40] J. Durbin and S. J. Koopman, *Time series analysis by state space methods*. Oxford University Press, 2012, no. 38.

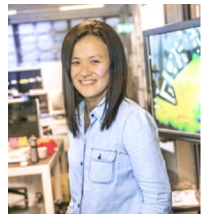
[41] G. Chevalier, "Lstms for human activity recognition," 2016. [Online]. Available: https://github.com/guillaume-chevalier/LSTM-Human-Activity-Recognition

Wei Shao Wei Shao is current a PhD student in the RMIT, Australia. His interest research area focused on optimisation, spatio-temporal data analysis and device-free activity recognition. He received the Master of Science in the University of Hong Kong. Previously, he received a BEng in Software Engineering from Xidian University, China.

Thuong Nguyen Thuong Nguyen is currently a research scientist at Trusting Social. He obtained his PhD from Deakin University in 2015. Before joining Trusting Social, he was postdoctoral fellow at RMIT University and CSIRO. His research interests are machine learning, big data, pattern recognition and context discovery in pervasive computing. He served as a TPC member of PerCom 2018. He is regularly invited to review papers for Pervasive and Mobile Computing Journal.

Kai Qin Kai Qin is a research assistant at the School of Science, RMIT University. His main areas of research interest are data analytics and artificial intelligence. He received the Master degree in Information Technology Engineering from RMIT University, Melbourne, Australia, in 2015. He also has about 5 years of experience in developing web-based systems or mobile applications.

Moustafa Youssef Moustafa Youssef is a professor at Alexandria University and Egypt-Japan University of Science and Technology (E-JUST) and founder and director of the Wireless Research Center of Excellence, Egypt. His research interests include mobile wireless networks, mobile computing, location determination technologies, pervasive computing, and network security. He has tens of issued and pending patents. He is the Lead Guest Editor of the upcoming IEEE Computer Special Issue on Transformative Technologies, an Associate Editor for ACM TSAS, served as an Area Editor of ACM MC2R as well as on the organizing and technical committees of numerous prestigious conferences. He is the recipient of the 2003 University of Maryland Invention of the Year award, the 2010 TWAS-AAS-Microsoft Award for Young Scientists, the 2012 Egyptian State Award, the 2013 and 2014 COMESA Innovation Award, the 2013 ACM SIGSpatial GIS Conference Best Paper Award, the 2107 Egyptian State Excellence Award, multiple Google Research Awards, among many others. He is an ACM Distinguished Speaker, an ACM Distinguished Scientist.



Flora Salim Flora Salim is a Senior Lecturer at the Computer Science and IT, School of Science, RMIT University. Her research interests are human mobility and behaviour analytic, context and activity recognition, and urban intelligence. She received her PhD award from Monash University in May 2009. She was awarded the Australian Research Council Postdoctoral Fellowship Industry in 2012-2015, the RMIT Vice-Chancellor's Award for Research Excellence - Early Career Researcher 2016, and RMIT School of Science HDR Supervision Excellence Award 2017. She is an Editorial board member and an Area Editor of Pervasive and Mobile Computing journal, a TPC vice chair of IEEE PerCom 2018, and a regular reviewer for ACM ToIT, IEEE THMS, IEEE TSC, IEEE TKDE, IEEE T-ITS, IEEE TCC, and Springer DMKD journal.