RFID-based human behavior modeling and anomaly detection for elderly care

Hui-Huang Hsu* and Chien-Chen Chen
Department of Computer Science and Information Engineering, Tamkang University Taipei, Taiwan

Abstract. This research aimed at building an intelligent system that can detect abnormal behavior for the elderly at home. Active RFID tags can be deployed at home to help collect daily movement data of the elderly who carries an RFID reader. When the reader detects the signals from the tags, RSSI values that represent signal strength are obtained. The RSSI values are reversely related to the distance between the tags and the reader and they are recorded following the movement of the user. The movement patterns, not the exact locations, of the user are the major concern. With the movement data (RSSI values), the clustering technique is then used to build a personalized model of normal behavior. After the model is built, any incoming datum outside the model can be viewed as abnormal and an alarm can be raised by the system. In this paper, we present the system architecture for RFID data collection and preprocessing, clustering for anomaly detection, and experimental results. The results show that this novel approach is promising.

Keywords: RFID, behavior modeling, anomaly detection, elderly care, clustering

1. Introduction

Elderly care is an important issue in an aging society. There are many elderly people who live alone. Even though some elderly people live with their children, they are at home alone most of the time since young people need to work or go to school. Quite a few systems have been developed for health care [1–3] in general and elderly care in specific [4,5]. To monitor the movements of the elderly at home is one of the major parts of elderly care. Mining meaningful information from human movement data is also an essential research issue [6–8]. This research would like to utilize information technology to unobtrusively detect abnormal behavior of elderly people at home according to their movements. Abnormal behavior includes not only emergencies like faints and falls, but also others like "not eating," "not going to toilet regularly," "lack of movement," and "trotting around." Since everyone can have very different behaviors at home, it is not possible to predefine the so-called abnormal behaviors. Thus machine learning technology is needed to build a personalized behavior model for each individual [9, 10].

To answer the two raised issues, first, we propose to use the RFID (Radio Frequency Identification) technology for movement detection of the elderly. The reason is that the RFID system is relatively cheap and easy to deploy in the home environment. Furthermore, RFID sensors are unobtrusive comparing to the popular solution by video cameras. Secondly, to deal with the behavior modeling, we propose to

---

*Corresponding author: Department of Computer Science and Information Engineering, Tamkang University, 151 Ying-Chuan Rd. Tamsui, Taipei, 25137, Taiwan. Tel.: +886 2 26215656 Ext. 3307; Fax: +886 2 26209749; E-mail: h_hsu@mail.tku.edu.tw.

use the clustering analysis [11,12] since presumably only positive data (normal behavior) are collected. Abnormal behavior is hard to define and a complete collection of such negative data is not possible. It is not feasible to use a classifier [13,14] which needs both positive and negative examples for training. Thus, clustering should be the way for modeling the user movements.

Sensor networks have been a popular research issue due to many useful applications [15–17]. Valuable information can be collected through various kinds of sensors. In this research, RFID sensors were chosen for monitoring human behavior at home. An RFID system includes two parts: tags and readers. The readers are used to detect the deployed tags which usually are attached to objects and store serial numbers corresponding to the objects. There are basically two kinds of RFID tags: passive and active. Passive tags simply reflect the signal sent from the reader for the transmission of the stored information. They draw power from the reader and need no battery. On the other hand, active tags have their own transmitter and power source (battery). RFID tags are designed to operate in different frequencies. General speaking, high frequency (HF) tags are used in a detecting distance shorter than 0.5 meter (usually passive tags); ultra high frequency (UHF) tags are used for a wider range (several meters to one hundred meters; usually active tags). In this research, active tags are used since they are of an ultra high frequency and can be detected in a wider range. When the reader detects the signals from the tags, received signal strength indication (RSSI) values can be obtained. The RSSI value has a negative relationship with the distance of the tag from the reader. Thus a relative distance of the tag and the reader in a measurement of signal strength can be obtained [18].

It is desired to build a behavior model (viewed as normal) for the elderly by the collected RSSI data. One or two week data are needed for such modeling. We then can use this model to detect subsequent abnormal behavior of the user. The system architecture includes deploying active tags in the living environment, e.g., the living room, the dining room, the kitchen, the rest room, and the bed rooms. The reader is to be carried by an elderly person. The detected RSSI values are recorded following the movement of the person. A clustering technique is then used to build a model of normal behavior, and the model can be used to determine if the subsequent behavior is normal or not. Since only data of normal behavior are collected, the behavior model can be build with only positive examples via clustering analysis. The key to a successful behavior modeling would be on the setting of cluster boundaries. Moreover, short-term behavior (for a few minutes) and long-term behavior (for a couple of hours) are quite different. So we actually need two models for short-term behavior and long-term behavior, respectively.

This novel approach, different from computer-vision-based approaches, not just detects predefined events like if the elderly person falls, but finds the living patterns of the person. The machine learning technique can be used to learn all the patterns without defining all of them in advance. Also, it is not necessary to install cameras at home. This can relieve the concern of personal privacy issues [1]. Researches related to using RFID and/or other sensors for elderly care and home safety can also be found in other researches [4,5,19]. But all of them do not focus on general behavior modeling as we do.

In the next section, we give an overview on related work. The third section illustrates behavior modeling, including environment settings, RFID data collection, data preprocessing, and clustering for normal behavior modeling. The fourth section shows experimental results of abnormal behavior detection. The final section draws a brief conclusion and discusses future development.

2. Related work

In this section, we first discuss a few papers related to using the RFID technology in elderly care and home care. Ho et al. gave a progress report in using RFID and sensor networks for elderly care in

2005 [4]. The goal was to build an in-home elderly care system that monitors the medication-taking behavior of the elderly. In their prototype system, a simulated HF RFID reader, a simulated UHF RFID reader, a weight scale and a base station PC were used. A HF RFID tag is attached to each medicine bottle which is placed on top of the scale within the detection range of the HF RFID reader. Each elder patient wears a UHF RFID tag. The UHF RFID reader is also placed near the medicine bottles. When a bottle is removed from the scale, the UHF RFID reader can identify which elder patient is taking the bottle and the HF RFID reader can decide which medicine bottle is removed. When the bottle is put back to the top of the scale, the scale can tell the system to record the amount of medicine the patient has taken. The system design is very interesting and the preliminary results showed that the system could record medication-taking behavior of the elder patient. Our system aims at understanding general behaviors/movements of the elderly at home, not just specifically in medication-taking behaviors.

Jih et al. intended to build a smart environment at home for the elderly in 2006 [5]. It presented a context-aware service integration system using multi-agent technologies. The system can provide context-aware healthcare services to the elderly at home and the remote caretaker can monitor and attend the elder's well-being at anytime from anywhere. It tracks the location and activities of the elderly via sensors like pressure-sensitive floors, cameras, smart furniture, and bio-sensors. The paper gave several context-aware service scenarios to demonstrate such a system can enhance the quality of care for the elder's daily life. However, the paper only showed the design of the proposed framework and discussed the usefulness of such a platform. It focused on using the agent technology in processing the sensor data from various sensors, but no real implementation and experimental results were given.

Lee and Kim proposed a context-aware home safety model which applied the RFID and sensor network in 2007 [19]. The model focused on surveillance and intrusion detection. Networking and privacy issues along with the RFID middleware were also presented. RFID as well as light and temperature sensors were used. The paper utilized the RFID technology for home safety. It is for general purpose, not just elderly care.

Quite a few researches can be found in the literature for RFID tracking/positioning [20–23]. However, we do not need such complicated systems since exact location of the elderly person is not needed. Time sequences of RSSI values collected from active tags deploying in various corners at home are a sufficient representation of the movement of the elderly person who carries the reader. Other indoor positioning systems used wireless LAN [24], floor pressure/load sensors [25], and infrared-based small motion detectors (SMDs) [26]. Furthermore, video tracking systems can also be used to monitor indoor human behavior [27] or outdoor traffic [28]. The RFID technology has become popular and the cost of the readers and tags are going down rapidly. This makes the RFID technology more appealing than the wireless LAN, SMDs, and video cameras for detecting the movements of the user. Furthermore, object tracking in video is a much more complex task. It also draws concern on personal privacy.

Another major issue of this research is the behavior modeling by only positive examples. The goal for such modeling is to detect abnormal behaviors. In the literature, we have found applications of anomaly detection in information security [29,30], credit fraud detection [31], and document selection [32]. All of them used a machine learning approach to build a classifier with both positive and negative examples. One-class SVM (support vector machines) that finds the hyperplane between the positive examples and the origin is used in [29]. The origin is used to represent the negative examples. Such a classifier is biased and not suitable in our system. On the other hand, artificial negative examples were used in [32]. This is also impractical since negative examples are difficult to define and generate. Therefore, clustering analysis is a much more feasible way for building a normal behavior model.
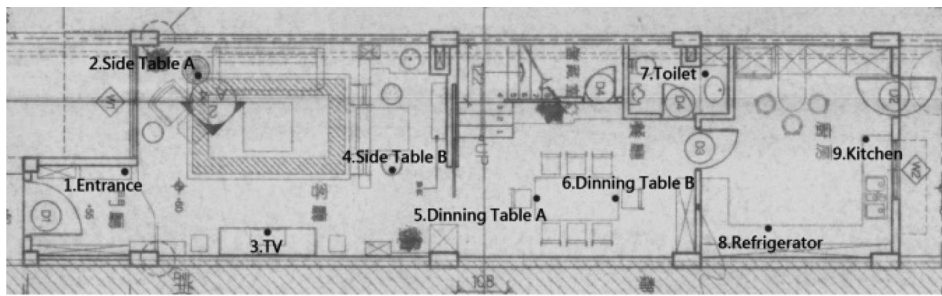
(a)
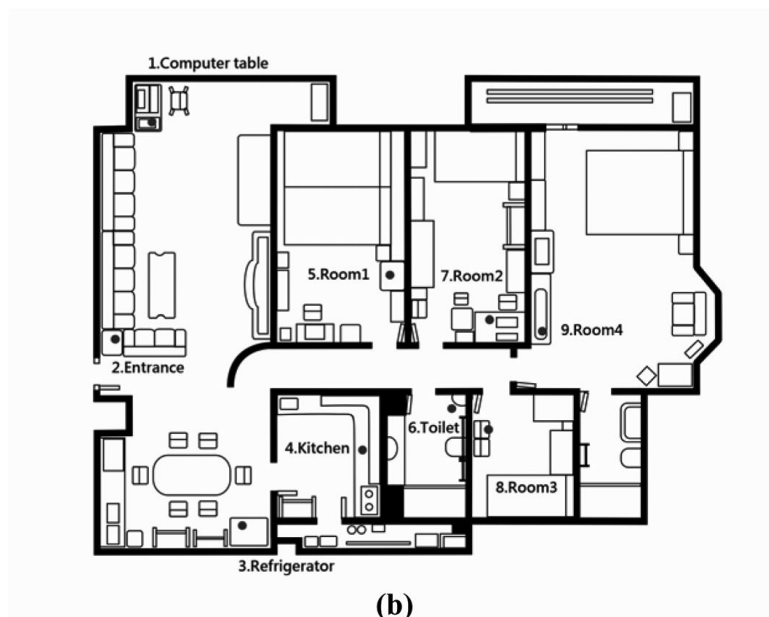
(b)

Fig. 1. Deployment of tags in testing environment: (a) Area A, (b) Area B.

3. Behavior modeling

In this section, behavior modeling by RFID is divided into three parts: environment settings and data collection, data preprocessing, and behavior modeling by clustering.

3.1. Environment settings and data collection

In our setting, a notebook PC, a wireless LAN access point (AP), a CF-card RFID reader, a PDA with a CF-card slot, and 10 active RFID tags with various sizes were used. The user carried the PDA with an RFID reader. The tags were deployed in the testing environment. Two areas were used in our tests. The first area was the first floor of a house (Area A) and the second one was an apartment (Area B). Please refer to Fig. 1. The dots in the Figure show the location of the deployed tags. Totally nine tags were deployed and the 10th tag was a bracelet tag carried by the user.

After the RFID and wireless environment were constructed, signals from 10 tags were transmitted to the reader, and the PDA transmitted the received RSSI values from the tags to the notebook PC every
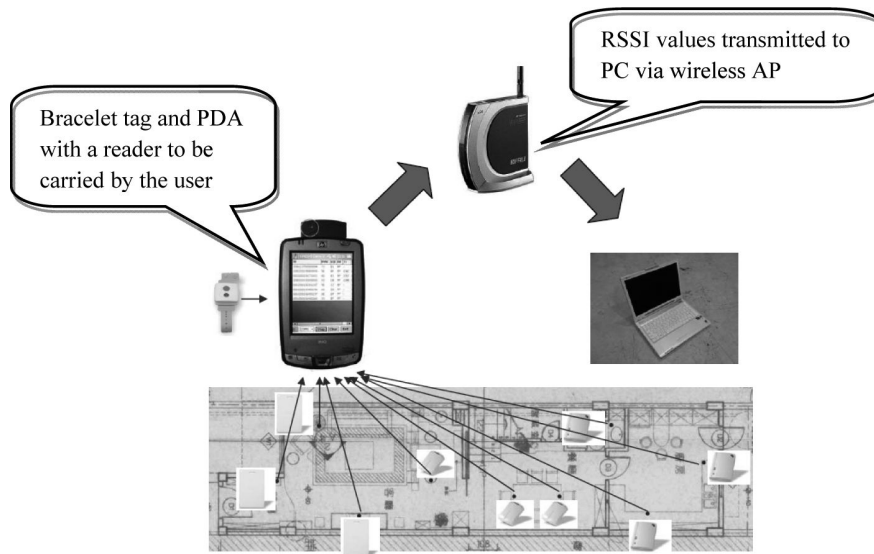
Fig. 2. System architecture for data collection.

```
ID:0001000107520133,RSSI:133,LQI:219,DI:255,T1:-,T2:-
ID:0001000107520125,RSSI:132,LQI:73,DI:255,T1:-,T2:-
ID:0001000107520124,RSSI:111,LQI:107,DI:255,T1:-,T2:-
ID:0001000107462018,RSSI:0,LQI:0,DI:0,T1:-,T2:-
ID:0001000107462016,RSSI:103,LQI:213,DI:255,T1:-,T2:-
ID:0001000107462011,RSSI:0,LQI:0,DI:0,T1:-,T2:-
ID:0001000107291249,RSSI:0,LQI:0,DI:0,T1:-,T2:-
ID:0001000107291246,RSSI:0,LQI:0,DI:0,T1:-,T2:-
ID:0001000107291241,RSSI:0,LQI:0,DI:0,T1:-,T2:-
ID:0001000107503013,RSSI:150,LQI:227,DI:255,T1:29.25,T2:29.87
```

Fig. 3. Samples of collected data.

second through the wireless AP. The collected data were then stored and preprocessed in the notebook PC for further analysis. We could have collected the movement data in a reverse way, meaning, the person carried a tag and readers were deployed in the environment. But the cost would be much higher. The system architecture for data collection can be seen in Fig. 2. In the system, active tags were deployed in the home environment. The user carried a PDA with the CF-card reader and wore a bracelet tag. (A custom-designed RFID reader which is light weighted and easy to carry should be used in real cases.) The bracelet tag can also measure and transmit body temperature of the user. This can help ensure that the reader is with the person at all times. This can also be integrated into the customized design.

The following data were transmitted: the tag ID number, the RSSI value, the connectivity quality (LQI), the battery indicator (DI) and detected temperatures (only for Tag #10 that has temperature sensors). At the current stages, only the first two items were used to build the behavior models. A set of sample data collected and transmitted in one second is shown in Fig. 3 for illustration.

To do a primary test, we collected the RSSI values for half an hour in Area A. During the test, the user stayed in the couch for 10 minutes, walked to the toilet in one minute, stayed in the toilet for 90 seconds, moved to the refrigerator in 15 seconds, stayed in front of the refrigerator for another 15 seconds, walked to the kitchen tag, stayed in front of the kitchen tag for 60 seconds, walked back to the couch in
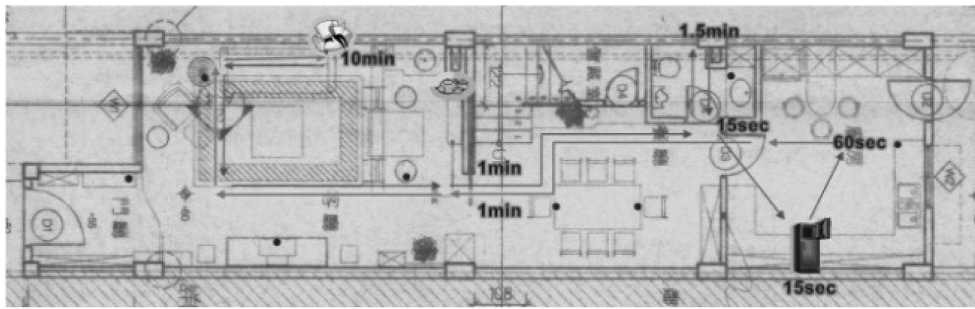
Fig. 4. Test moving route.

one minute, then repeated the whole process once (Fig. 4). The total time for this data collection was 30 minutes with 1800 data points. (The PDA transmitted detected data every second.) The user moved in the test environment alone with no interference from other people. The CF-card reader was held in an upright position at all time to ensure that signals from all tags could be more accurately detected.

The collected RSSI data sequences from five of the 10 tags are shown in Fig. 5. The five tags are *Side Table A*, *Side Table B*, *Dining Table B*, *Toilet*, and *Bracelet* (please refer to Fig. 1 (a)). In Fig. 5 (a), the tag was not detected (with an RSSI value of zero) in the two squared periods because the person was going away from the living room. Fig. 5 (b) is similar to Fig. 5 (a) except that the RSSI values are lower and noisier when the person was in the living room. The noisy signal was caused by the furniture existing between Side Table B and the couch. In Fig. 5 (c), the signal was even noisier than Fig. 5 (b) when the person was in the couch. This is because that there was a division between the living room and the dining room. On the other hand, the RSSI values of the Dining Table B tag were higher when the person moved to the toilet and the kitchen. From Fig. 5 (d), it is very obvious to know at what time the person was in the toilet. In Fig. 5 (e), it shows that the bracelet tag was with the person during the test. From these signals, we are sure that the collected RSSI values can represent the movement of the person. The RSSI values from the tags change with the distances between the tags and the reader (the person).

3.2. Data preprocessing

The RSSI values can be unstable and noisy sometimes. This is why we need to preprocess the collected data before they are sent to the clustering process. From Fig. 5, we see noises in the collected signals. Most importantly, the signals dropped to zero sometimes even when the person was not moving. The tags were not detected during that one second period. Also, furniture and divisions between rooms cause interference to the signals. Moreover, the reader is directional. Detected signals can be different when we point the reader in different directions. This is why the user had to keep the reader in an upright position to have more accurate data collection. Although this might seem to be quite inconvenient for the user, we believe a customized, miniaturized RFID reader can overcome this problem.

To provide a dataset with a better quality for clustering analysis, we need to preprocess the collected data. First, the sudden zeros are detected and smoothed out. Secondly, the RSSI values sometimes maybe unstable and noisy, so it is needed to smooth all collected data. Thirdly, the data should be sampled to reduce the total amount of data. In Fig. 6 (a), a sudden zero is shown and it can be smoothed out to 121 ($(124 + 124 + 118 + 118)/4 = 121$) as in Fig. 6 (b). Here we use a voting mechanism to decide if a zero is a sudden zero. If the majority of the previous samples and the subsequent samples are not zero, it means that the current zero should not be zero. Thus it is smoothed out by averaging the RSSI values
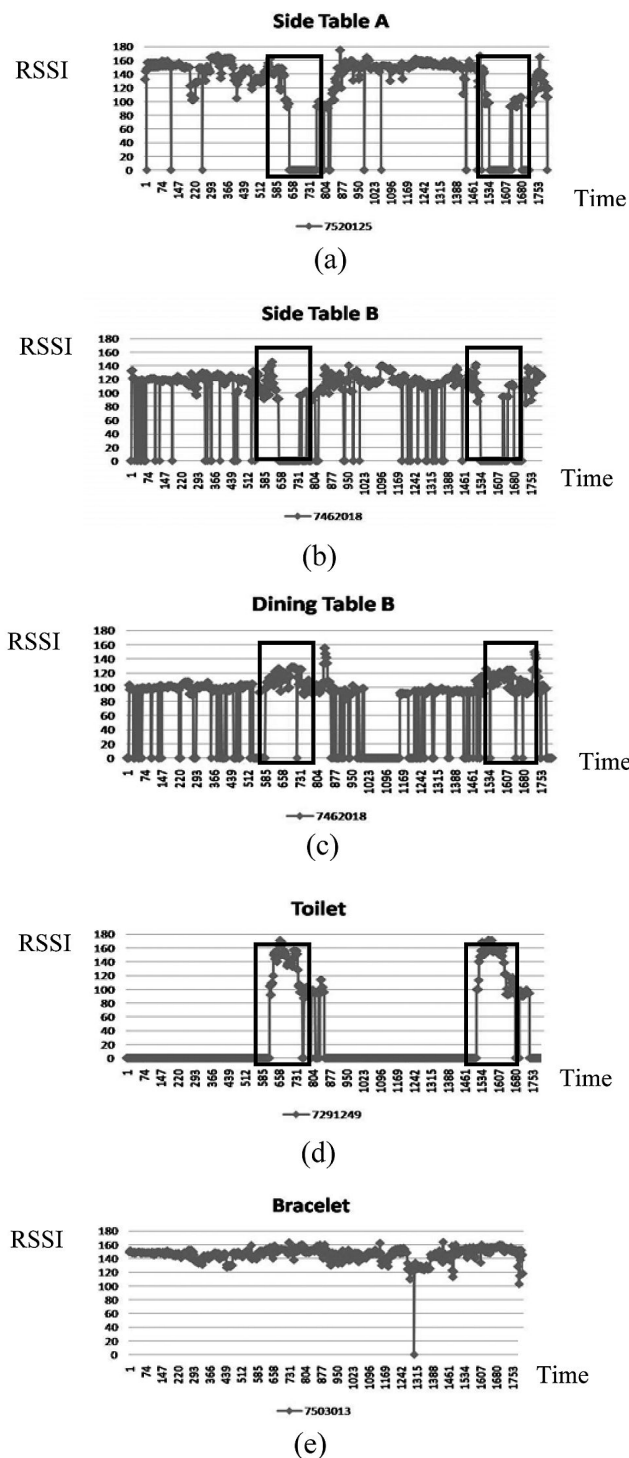
Fig. 5. Collected data from the 30-minute test movement: (a) Side Table A, (b) Side Table B, (c) Dining Table B, (d) Toilet, (e) Bracelet.

	A	B
129	124	115
130	124	115
131	122	117
132	122	117
133	122	117
134	124	117
135	124	117
136	124	117
137	124	131
138	124	131
139	0	131
140	118	131
141	118	131
142	118	131
143	120	107
144	120	107
145	120	107

(a)

	A	B
129	124	115
130	124	115
131	122	117
132	122	117
133	122	117
134	124	117
135	124	117
136	124	117
137	124	131
138	124	131
139	121	131
140	118	131
141	118	131
142	118	131
143	120	107
144	120	107
145	120	107

(b)

Fig. 6. RSSI values with a sudden zero (a) before smoothing (b) after smoothing.
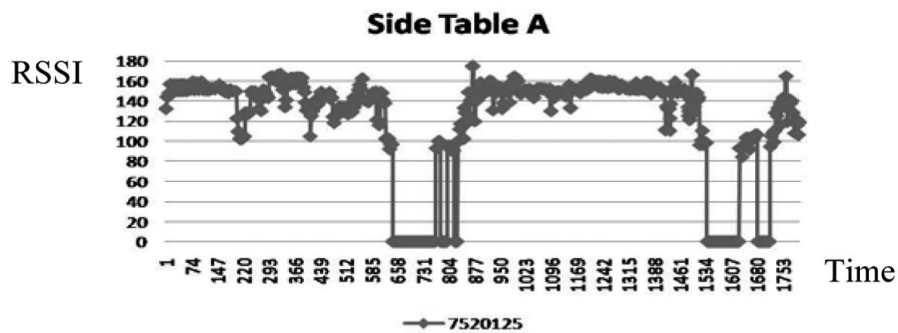

Fig. 7. Result with sudden zeros smoothed out for Side Table A.

of the neighbors. In our experiments, 10 neighbors were used to make the decision. In this example, only four neighbors were used for illustration. The sudden zeros in Fig. 5 (a) were smoothed out by this technique (Fig. 7). Next, we applied a general moving average technique to the rest of the data sequences to filter out the noises. Meaning, each data point is replaced by the average of its neighbors and itself.

For reducing the space and time complexity, it is needed to sample the collected data. This is to reduce the number of data points in a windowed data from the time sequences. The sampling interval cannot be large because the user may move from one point to another then back in a few seconds. The information of this movement may be lost if the data are sampled for a long period of time. From our experiments, it is suggested that the sampling interval is set to five seconds. Furthermore, we believe that it is better to retain the maximal RSSI value in the sampled interval so that movement information can be best preserved. Figure 8 shows an example for such a sampling process. 7520125 and 7520124 were the tag ID numbers. The data were sampled every five seconds and the maximal RSSI value during that five-second period was saved. For example, the maximal value of the 7520125 tag in the first five seconds was 144. It was 117 for the 7520124 tag in the same period.

7520125	7520124
132	111
132	111
144	111
144	117
144	117
144	117
144	111
144	111
132	111
148	98

7520125	7520124
144	117
148	117

Fig. 8. Data sampling with the maximum retained.

3.3. Behavior modeling by clustering

After the RFID data sequences are properly smoothed and sampled, the preprocessed data sequences are windowed by a sliding window. Since we want to analyze the movements of the user, a short segment of data (windowed data) from the data sequences should be assembled into a movement datum for behavior modeling, not just the data at a particular time. Two behavior (movement) models are then built. They are models for short-term behavior and long-term behavior. The short-term model is used to detect anomalies like falls (unusually staying in a place for too long) and anxiety (trotting around). On the other hand, the long-term model is used to detect anomalies like "not going to the toilet for all day" and "not opening the refrigerator for a few hours." The windowed datasets for short-term modeling and long-term modeling are different in window size and sampling interval. The dataset for long-term behavior modeling has a larger window to include more information and a larger sampling interval to reduce processing time.

The datasets for short-term modeling and long-term modeling are clustered respectively through standard clustering techniques like K-means [33]. The K-means algorithm randomly selects K centers. Each data point then chooses to join the cluster of a specific center if the distance between the data point and the center is the shortest (comparing to the distances to other cluster centers). It iteratively updates the cluster centers and members of each cluster until it is converged. Manhattan distance is used here to measure the similarity between data points.

$$d_M(x_i, x_j) = \sum_{d=1}^{N} |x_{id} - x_{jd}| \tag{1}$$

The number of clusters would be the number of different spaces in the environment. In Fig. 9, we have four clusters in the two-dimensional space. In real cases we should have more clusters in the 10-dimensional space (due to 10 RFID tags).

Since only data of normal behavior are collected, the model (a classifier) can be built with only positive examples. The key for this behavior modeling is to determine the boundaries of all clusters. Once the boundaries are properly determined, we can have a model to detect anomalies. In Fig. 9, point A is outside the boundary of either one of the four clusters. So it is viewed as an anomaly. In our experiments, the boundary of a cluster was set to the maximal distance from all member points to the cluster center.
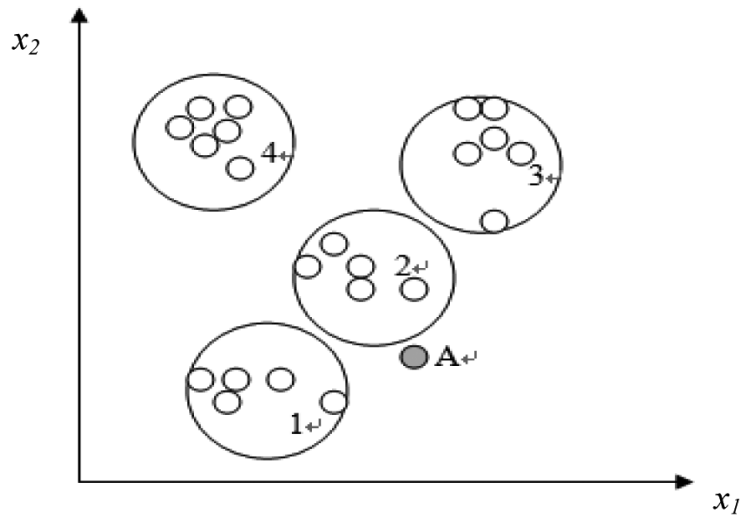
Fig. 9. Clustering for behavior modeling.

Fig. 10. Eight-hour training data of normal behavior.

4. Experimental results

In the following experiments, RFID RSSI data were collected in Area B (Fig. 1 (b)). An eight-hour dataset was collected as the training data for building the normal behavior models (Fig. 10). Two other test datasets were designed to simulate possible abnormal short-term behaviors, which will be shown later.

Before doing the tests, we need to first set the criteria for triggering the alarm. We cannot trigger the alarm simply by the appearance of one single abnormal data point because there would be too many false alarms. The number of continuous abnormal data points should be greater than a preset threshold, say five points, to be considered as an abnormal event. When an abnormal event occurs, it would generally last for a period of time. For example, if the user falls down at the entrance of the toilet, he/she would stay there for a period of time longer than he/she usually does. The alarm should be triggered in a short period of time after continuous abnormal data points are observed.

Table 1
Detected abnormal data points of Route 1

Abnormal points	Time interval	Number of points
160∼164	13m50s∼14m10s	5
445∼451	37m35s∼38m05s	7
460∼486	38m50s∼41m	28
491∼493	41m25s∼41m35s	3
501∼504	42m15s∼42m30s	4
518∼529	43m40s∼44m35s	12
545∼547	45m55s∼46m05s	3
566∼572	47m40s∼48m10s	7
577∼581	48m35s∼48m55s	5
589∼592	49m35s∼49m50s	4

Table 2
Detected abnormal data points of Route 2

Abnormal points	Time interval	Number of points
119∼120	10m25s∼10m30s	2
255∼257	21m45s∼21m55s	3
279∼285	23m45s∼24m15s	7
293∼298	24m55s∼25m20s	6
302∼320	25m40s∼27m10s	19

4.1. Short-term anomaly detection

The following two routes are the designed testing data for anomaly detection of short-term behaviors.

1. Living room (15 minutes) → 30 seconds → Room1 (15 minutes)→ 30 seconds → Refrigerator (20 minutes)
2. Room1 (10 minutes) → 30 seconds → Toilet (10 minutes) → 20 seconds → Toilet entrance (20 minutes)

The experimental results of Route 1 are shown in Table 1. In Route 1, the user stopped in front of the refrigerator for 20 minutes at the end. Since in the training data (Fig. 10) the user has stayed in front of the refrigerator for at most one minute, we would expect to receive an alarm from the system after 32 minutes 30 seconds (in Route 1, the sum of 15 minutes, 30 seconds, 15 minutes, 30 seconds, 1 minute, and 30 seconds). 30 seconds were added because the abnormal event criterion was set at six consecutive abnormal points and the time interval between two points is 5 seconds. From Table 1, abnormal events are detected at 38 minutes (37 minutes and 35 seconds plus 25 seconds). It is a few minutes later than expected, but still acceptable. A false alarm could have been raised at 14 minutes 10 seconds, but owing to the preset criterion (over five consecutive abnormal points), the alarm was not issued by the system.

In Route 2, the user stopped at the toilet entrance for 20 minutes at the end. From the training data (Fig. 10), the user has stayed in the toilet three times, for 15, 3, and 10 minutes respectively, but he/she actually never stopped at the toilet entrance. We would expect the system to issue an alarm a short time after 21 minutes and 20 seconds (in Route 2, the sum of 10 minutes, 30 seconds, 10 minutes, 20 seconds, and 30 seconds). In Table 2, an abnormal event is detected at 24 minutes and 10 seconds (23 minutes and 45 seconds plus 25 seconds). It is a bit later than expected. Abnormal points 255∼257 (3 points, ends at 21 minutes and 55 seconds) were viewed as normal because of the suppression from the alarm-triggering criterion. Otherwise, we could have got an alarm at a time even closer to the expected time (22 minutes and 10 seconds).

Table 3
Clustering analysis of long-term tes-
ting data

Clusters	Number of data
1.Computer	1251
2.Living room	3688
3.Restaurant	2006
4.Refrigerator	4206
5.Kitchen	1306
6.Room1	1874
7.Toilet	0
Abnormal points	5

4.2. Long-term anomaly detection

In the experiment for long-term behavior modeling, we intentionally removed the data, collected when the user was in the toilet, from the original training data (Fig. 10) for the purpose of testing. This is to simulate the situation that the elder person did not go to toilet for the whole day. We classified the testing data (without toilet data) by the long-term behavior model which was built by the training data with toilet data. The results in Table 3 show that no data point was classified into the toilet cluster. We can conclude from the results that the user did not go to the toilet. We cannot simply make this judgment from the RSSI values of the toilet tag because the threshold would be hard to set. With this long-term anomaly detection, long-term behaviors for not going to a certain place, e.g., the kitchen and the toilet, for hours or even a whole day can be detected. Not eating much and not going to toilet are both serious problems for the elderly.

5. Conclusion

In this paper, we present a novel RFID-based approach for modeling human behavior, which we believe has never been tried before. The aim is to detect abnormal behavior by the personalized behavior model. This can be very useful for elderly care at home since it is unobtrusive and easy to deploy. Only one custom-designed RFID reader and a dozen of active RFID tags are needed for detecting the movements of the user. The custom-designed device should certainly be light weighted and easy to carry. Moreover, the primary test results show that this approach is very promising. When the user stays at a location longer than he/she usually does (simulating falls and faints), the system can detect the situation and issue an alarm. If the user does not go to the toilet for hours, a warning message can also be issued.

References

[1] Y. Xiao, X. Shen, B. Sun and L. Cai, Security and privacy in RFID and applications in telemedicine, *IEEE Communications Magazine* **44** (2006), 64–72.
[2] A. Koyama, J. Arai, S. Sasaki and L. Barolli, Design, field experiments and evaluation of a web-based remote medical care support system, *International Journal of Web and Grid Services* **4** (2008), 80–99.
[3] A. Yamazaki, A. Koyama, J. Arai and L. Barolli, Design and implementation of a ubiquitous health monitoring system, *International Journal of Web and Grid Services* **5** (2009), 339–355.
[4] L. Ho, M. Moh, Z. Walker, T. Hamada and C.-F. Su, A prototype on RFID and sensor networks for elder healthcare: progress report, Proceedings 2005 ACM SIGCOMM Workshop on Experimental Approaches to Wireless Network Design and Analysis, 2005, pp. 70–75.
[5] W.-R. Jih, J.Y. Hsu and T.-M. Tsai, Context-aware service integration for elderly care in a smart environment, Proceedings 2006 AAAI Workshop on Modeling and Retrieval of Context Retrieval of Context, 2006, pp. 44–48.

[6] J.Y. Goh and D. Taniar, Mobile data mining by location dependencies, Proceedings of the 5th International Conference on Intelligent Data Engineering and Automated Learning, *Lecture Notes in Computer Science* **3177** (2004), 225–231.

[7] J. Goh and D. Taniar, Mining frequency pattern from mobile users, Proceedings of the 8th International Conference on Knowledge-Based Intelligent Information and Engineering Systems, *Lecture Notes in Computer Science* **3215** (2004), 795–801.

[8] D. Taniar and J. Goh, On mining movement pattern from mobile users, *International Journal of Distributed Sensor Networks* **3** (2007), 69–86.

[9] O. Daly and D. Taniar, Exception rules mining based on negative association rules, Proceedings of the International Conference on Computational Science and Its Applications, *Lecture Notes in Computer Science* **3046** (2004), 543–552.

[10] D. Taniar, J.W. Rahayu, V.C.S. Lee and O. Daly, Exception rules in association rule mining, *Applied Mathematics and Computation* **205** (2008), 735–750.

[11] T. Kwok, K.A. Smith, S. Lozano and D. Taniar, Parallel fuzzy c-means clustering for large data sets, Proceedings of the 8th International Euro-Par Conference on Parallel Processing, *Lecture Notes in Computer Science* **2400** (2002), 365–374.

[12] L. Tan, D. Taniar and K.A. Smith, A clustering algorithm based on an estimated distribution model, *International Journal of Business Intelligence and Data Mining* **1** (2005), 229–245.

[13] L. Tan, D. Taniar and K.A. Smith, Maximum-entropy estimated distribution model for classification problems, *International Journal of Hybrid Intelligent Systems* **3** (2006), 1–10.

[14] L. Tan and D. Taniar, Adaptive estimated maximum-entropy distribution model, *Information Sciences* **177** (2007), 3110–3128.

[15] A. Aikebaier, T. Enokido and M. Takizawa, Design and evaluation of reliable data transmission protocol in wireless sensor networks, *Mobile Information Systems* **4** (2008), 237–252.

[16] S. Kumar and S.-J. Park, Probability model for data redundancy detection in sensor networks, *Mobile Information Systems* **5** (2009), 195–204.

[17] W. Wu, X. Li, S. Xiang, H.-B. Lim and K.-L. Tan, Sensor relocation for emergent data acquisition in sparse mobile sensor networks, *Mobile Information Systems* **6** (2010), 155–176.

[18] R. Crepaldi, A.F. Harris, R. Kooper, R. Kravets, G. Maselli, C. Petrioli and M. Zorzi, Managing heterogeneous sensors and actuators in ubiquitous computing environments, *Proceedings International Conference on Mobile Computing and Networking*, 2007, pp. 35–42.

[19] B. Lee and H. Kim, A design of context aware smart home safety management using networked RFID and sensor, *Proceedings First IFIP WG6.2 Home Networking Conference*, 2007, pp. 215–224.

[20] R.S. Sangwan and R.G. Qiu, Using RFID tags for tracking patients, charts and medical equipment within an integrated health delivery network, Proceedings 2005 IEEE Networking, *Sensing and Control* (2005), 1070–1074.

[21] W. Jiang, D. Yu and Y. Ma, A tracking algorithm in RFID reader network, *Proceedings Japan-China Joint Workshop on Frontier of Computer Science and Technology*, 2006, pp. 164–171.

[22] E. Aydin, R. Oktem, Z. Dincer and I.K. Akbulut, study of an RFID based moving object tracking system, *Proceedings RFID Eurasia* (2007), 1–5.

[23] S. Jia, J. Sheng, D. Chugo and K. Takase, Obstacle recognition for a mobile robot indoor environment using RFID and stereo vision, *Proceedings 2007 International Conference on Mechatronics and Automation*, 2007, pp. 2789–2794.

[24] P. Prasithsangaree, P. Krishnamurthy and P.K. Chrysanthis, On indoor position location with wireless LANs, *Proceedings 13th IEEE International Symposium On Personal, Indoor, & Mobile Radio Communications* **2** (2002), 720–724.

[25] W.H. Liau, Inhabitant tracking and service provision in an intelligent e-home via floor load sensors, Master's Thesis, Department of Computer Science and Information Engineering, Nation Taiwan University, Taipei, Taiwan, 2005.

[26] K. Hara, T. Omori and R. Ueno, Detection of unusual human behavior in intelligent house, *Proceedings 12th IEEE Workshop on Neural Networks for Signal Processing*, 2002, pp. 697–706.

[27] P.-C. Chung and C.-D. Liu, A daily behavior enabled hidden Markov model for human behavior understanding, *Pattern Recognition* **40** (2008), 1572–1580.

[28] C.P. Lin, J.C. Tai and K.T. Song, Traffic monitoring based on real-time image tracking, *Proceedings 2003 IEEE International Conference on Robotics and Automation* **2** (2003), 2091–2096.

[29] Y. Wang, J. Wong and A. Miner, Anomaly intrusion detection using one class SVM, *Proceedings Fifth Annual IEEE SMC Information Assurance Workshop*, 2004, pp. 358–364.

[30] C.-H. Lin, J.-C. Liu and C.-H. Ho, Anomaly detection using LibSVM training tools, *Proceedings 2008 International Conference on Information Security and Assurance*, 2008, pp. 166–171.

[31] A.K. Ghosh and A. Schwartzbard, A study in using neural network for anomaly and misuse detection, *Proceedings 8th Conference on USENIX Security Symposium* **8** (1999), 12–12.

[32] J. Zizka, J. Hroza, B. Pouliquen, C. Ignat and R. Steinberger, The selection of electronic text documents supported by only positive examples, *Proceedings 8th International Conference on Statistical Analysis of Textual Data*, 2006, pp. 993–1002.

[33] P. Mitra, C.A. Murthy and S.K. Pal, Unsupervised feature selection using feature similarity, *IEEE Transactions on Pattern Analysis and Machine Intelligence* **24** (2002), 301–312.

Hui-Huang Hsu is an Associate Professor in the Department of Computer Science and Information Engineering at Tamkang University, Taipei, Taiwan. He received both his PhD and MS Degrees from the Department of Electrical and Computer Engineering at the University of Florida, USA, in 1994 and 1991, respectively. He has published over 80 referred papers and book chapters, as well as participated in many international academic activities. His current research interests are in the areas of machine learning, data mining, bio-medical informatics, ambient intelligence, and multimedia processing. Dr. Hsu is a senior member of the IEEE.

Chien-Chen Chen received his master's degree in Computer Science and Information Engineering from Tamkang University, Taipei, Taiwan in 2009. He worked on intelligent systems and RFID applications.