An Adaptive Sensor Network for Home Intrusion Detection by Human Activity Profiling

Masahiro Tokumitsu, Masashi Murakami and Yoshiteru Ishida

Department of Knowledge-Based Information Engineering,
Toyohashi University of Technology, Tempaku, Toyohashi 441-8580, Japan
(Tel : +81-53-244-6895; Fax : +81-53-244-6873)
(ishida@tutkie.tut.ac.jp)

Abstract: An adaptive sensor network for home intrusion detection has been proposed. The sensor network combines a profile-based anomaly detection and an adaptive information processing based on Hidden Markov Models (HMM) that allows the system to train and tune the profiles automatically. The trade-off between miss-alarm and false-alarm has been experimentally studied. Several types of hypothetical intrusion have been tested and successfully detected. However, hypothetical anomalies supposing a fall down of a resident due to sudden illness have been difficult to detect.

Keywords: sensor network, adaptive information processing, human activity profile, home intrusion detection.

I. Introduction

On the one hand sensor technology has been developed and many sensors are available to detect several quantities in the environment. These sensors range from the ones with low-cost but low resolution to the expensive ones with high precision. One the other hand, recent rapid progress on the wireless technology and information network allows aggregating and organizing many sensors distributed in a space of the environment [1]. The space ranges from a small one within a room to a large-scale covering an entire buildings and production plants.

With the advent of both low energy-consuming sensors and networking technology, sensor networks have been attracting attention [2]. What is required is synthesizing large-scale data collected from the sensor network to the meaningful information in real time. We have studied a design framework for an adaptive sensor network based on the immune systems analogy [3]. However, here we focus on another sensor network involving the Hidden Markov Model (HMM) (e.g., [4]) to attain an adaptive system while using the similar framework of profiling the human behavior.

Even when restricted to statistical methods, there have been many methods such as Support Vector Machine (SVM) [5]. For human activity monitoring, sensors can be mounted to the body [6]. We have focused on the adaptability that allows the sensor network (installed in a room) adapt to the environment.

Section 2 explains the intrusion detection based on profiling. Section 3 presents how the profiles are constructed and used for detection. Section 4 presents the experimental results. Section 5 discusses performance analysis comparing two experimental data acquired from the two homes.

II. Adaptive Intrusion Detection based on Profiling

2.1 Profiling Human Activity and Anomaly Detection

Profiling on agents has been widely studied and used even restricted to human. When restricted to human, DNA profiling may be most popular to find and identify evidences and to narrow down the scope of suspects in the criminal acts such as murder.

Here, we focus on the profiling on human activity and behavior in their daily life, particularly in their homes. Profiles of the residents are used to detect anomaly in their daily life such as housebreaking by an intruder, fall down and lost mobility due to sudden illness (e.g., heart attack), and long absence due to prowl caused by an illness (e.g., Alzheimer disease). In this paper, we deal with the first two: the housebreaking and the fall down.

2.2 Profiling Time Series Data by Hidden Markov Models

The sensor network monitors usual resident's behavior, extracts normal activities, and updates the normal activity profile. A deviation from the profile can be used as an evidence of anomaly. In this note, we use a collection of parameters of the HMM as a profile (Fig.

1). The HMM is suited for a task of handling time series data such as speech recognition and gesture recognition systems [7]. Since the HMM assumes that states are not directly observable, the parameters include output probabilities and initial distribution of probabilities, other than state transition probabilities. These parameters are estimated from the data monitored by the sensors.

The data of the first few days (up to five days) sampled from the sensors monitoring the resident's activity in his/her home are used for estimating the parameters, and the collection of the parameters is regarded as the profile of the resident to identify his/her normal life in the home. We call the period of few days a training period and the data collected in these days a training data. After the training period, the detection will be carried out by calculating a likelihood that the current data are within the range expected from the normal life, testing against the profile of a normal life (Fig.1).

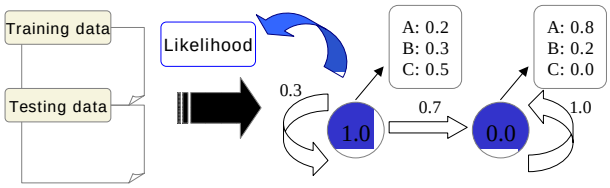

Fig. 1. Anomaly Detection by HMM parameters as profiles.

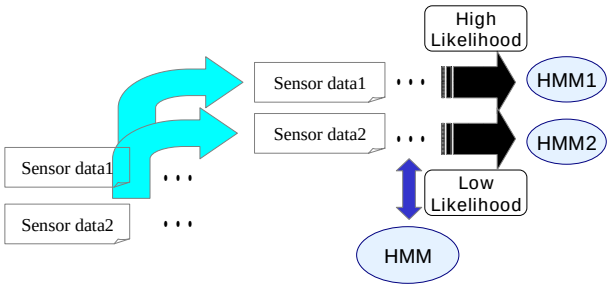

Fig. 2. Generating process of HMM profiles..

III. Sensor Network for Home Intrusion Detection

3.1 A Framework for Home Intrusion Detection by Sensor Networks

In our detection framework, we used multiple HMMs (Fig. 2) even for a single resident for detection accuracy, since even one man can have multiple patterns of activities. In a detection mode, a likelihood is calculated from the current monitoring data and the HMM to judge whether the current activities are within the expectation. If all the likelihoods calculated from corresponding HMMs are not greater than the predetermined thresholds, then anomaly will be concluded. These thresholds are acquired in a training phase.

Tuning of the thresholds plays a critical role in setting alarms, since any alarming systems are under a trade-off between miss-alarm and false-alarm. Too high thresholds turn out to be too many false-alarms, while too low thresholds lead to too many miss-alarms.

3.2 Processing of Sensor Data for Hidden Markov Models

Sensor data are sampled from the Infra-Red (IR) sensors installed to a room in a home as shown in Fig. 3. The detection system processes the data obtained through a sensor net interface.

Sensor data must be coded to input sequence of symbols for HMM. In the experiment, sensor data are sampled and transformed to 1 (reacted, or ON) / 0 (not reacted, or OFF) sequence of four bits (Fig. 4) in every five seconds. One minute collection of the 1/0 data is coded into one symbol sequence (Fig. 4).

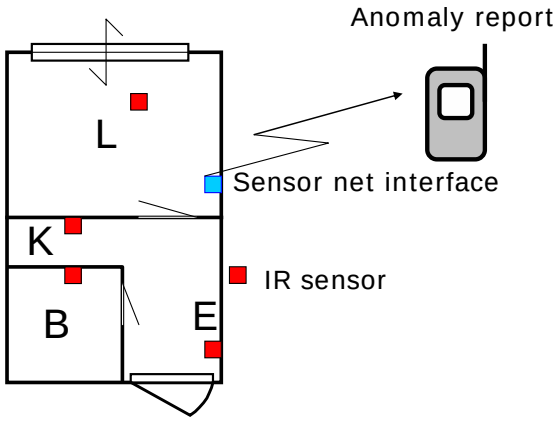

Fig. 3. Layout of sensors in a room for the experiment.

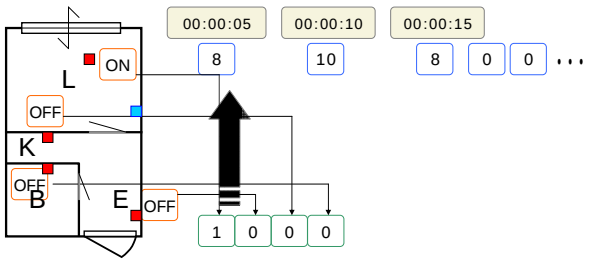

Fig. 4. Sensor Data Coding for HMM.

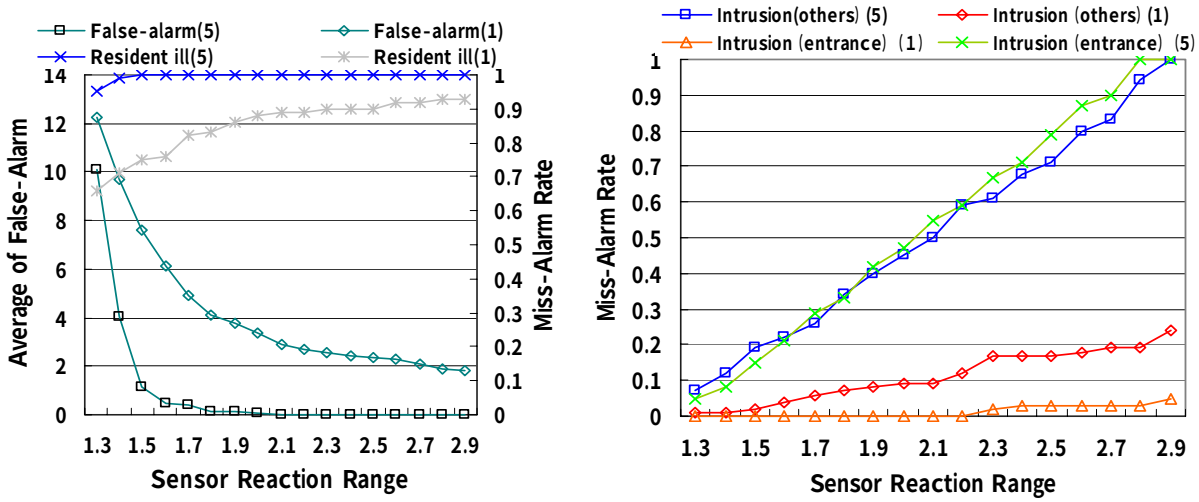

Fig.5. Average of False-Alarms (left) and Miss-Alarm Rate (right) when Sensor Sensitivity is varied in a home A. The number in parenthesis indicates the number of days used for the training of the system.

IV. Experiments and Performance Analysis

4.1 A Framework for Home Intrusion Detection by Sensor Networks

The sensor networks have been installed to a room in a home. Sensor layout in one room was shown in Fig. 3. Activities of a resident are monitored for three months. Since the actual anomaly would not happen, virtual anomalies have been set for performance analysis of the system. The following three types of anomalies are presented to the system:

1) Housebreaking from the entrance,

2) Housebreaking from other than the entrance (e.g., from the window), and

3) Resident falls down due to sudden illness.

4.2 Performance Analysis on the Adaptive Sensor Network

Among the monitored data, up to five days are used as learning data to train the HMM. The rest of data are used to test the performance in detection. The number of false-alarms (i.e., the system gave to alarm even when anomaly did not occur) in a day (Fig. 5 left) as well as the rate of miss-alarms (i.e., the system failed to alarm even when anomaly actually occurs) (Fig. 5 left) are plotted with the reactive range on which the sensitivity depends varied.

When the detection sensitivity decreases by lowering the thresholds for each HMM, the number of false-alarms decreased (Fig. 5 left) while the miss-alarm rate increased (Fig. 5 right). As expected, this trade-off holds for two data sets from two different homes. The events of resident fall down are difficult to detect. Indeed, missalarm rate for the resident fall down is higher than that for housebreaking.

V. Discussions

We have conducted the above experiments for two homes whose floor plan differs (Fig. 6) to compare the performances and to make performance analysis in more detail. That is, we want to investigate and narrow down the factors that affect the performance.

Fig. 7 shows the plots of average of false-alarms and miss-alarm rate for both homes. It can be first observed that the performance of the system for both homes is similar, even though the floor plan and hence the sensor layout differs from each other. This means that the adaptability of the system offered an adaptation to the sensor layout as long as the number of sensors and coverage to the room are adequately set. In this experiments also, the number of IR sensors are equal (four) and at least one IR sensor is installed to each room: living (L), kitchen (K), bedroom (B), and the entrance (E).

Again, the events of resident fall down are difficult to detect in both experiments. Since the events of resident fall down occurs in the middle of some normal activities, it may be difficult to discriminate them from normal activities in the coded profiles. It would be expected if the activities were monitored more frequently by sampling the data from the sensors in less than five minutes; the miss-alarm rate would be

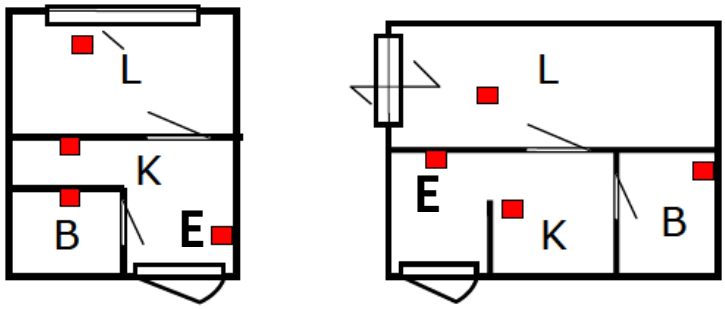

Fig.6. The IR sensor layout in the room of the home A (left) and B (right) for the experiment. The living (L), kitchen (K), bedroom (B), and the entrance (E) are shown.

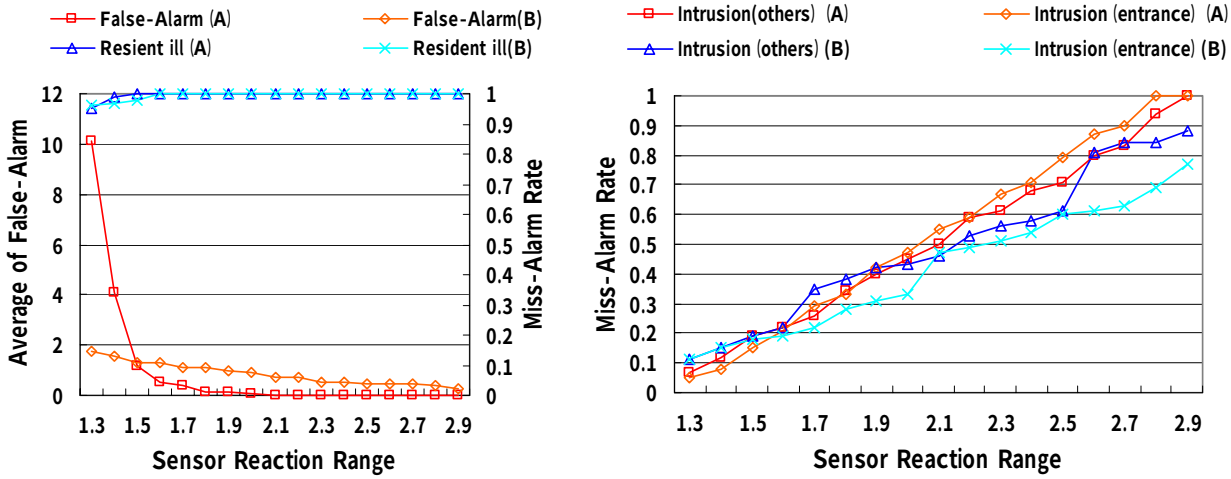

Fig.7. Average of False-Alarms (left) and Miss-Alarm Rate (right) of two homes A and B when Sensor Sensitivity is varied. A and B in the legend indicate the data from the home A and B, respectively.

improved. As a future work, the sampling time should be adapted to the environment.

VI. Conclusion

Experiments demonstrated that anomaly detection based on adaptive updates of resident's normal behaviors allows not only detection anomaly in the behaviors but also adaptation of the system to the environment. Here, the environment includes dynamic and diverse patterns of abnormal and normal behavior, dynamic but periodic life pattern. Reflecting the periodic conditions in short-terms such as hours and in longterms such as months and seasons to the profiles would improve the performance of detection success rate.

Acknowledgments. This work was supported by The Global COE Program "Frontiers of Intelligent Sensing", from the ministry of Education, Culture, Sports, Science and Technology. This work was also supported in part by Grants-in-Aid from Toyohashi University of Technology and CASIO Science Promotion Foundation.

REFERENCES

[1] Culler, D.E., Mulder, H.: Smart Sensors to Network the World, *Scientific American*, June (2004)
[2] Culler, D.E., et. al.: Overview of Sensor Networks, *IEEE Computer, Special Issue in Sensor Networks*, Aug (2004)
[3] Ishida, Y.: *Immunity-Based Systems: A Design Perspective*. Springer (2004)
[4] Rabiner, L.R.: A tutorial on Hidden Markov Models and selected applications in speech recognition". Proceedings of the IEEE 77-2 (1989) 257-286
[5] Preece, S.J. et al: Activity identification using body-mounted sensors—a review of classification techniques, *Physiol. Meas.* 30 (2009) R1-R33
[6] Jie Yin; Qiang Yang; Pan, J.J.: Sensor-Based Abnormal Human-Activity Detection, *IEEE Transactions on Knowledge and Data Engineering*, 20-8 (2008) 1082 – 1090
[7] Wilson, A.D., Bobick, A.F.: Parametric Hidden Markov Models for Gesture Recognition. IEEE Transaction Pattern analysis and machine intelligence, 21-9 (1999) 884-900