Embedded Action Detector to Enhance Freedom from Care

*Kyohei Koyama[*1], Kouichi Nakagawa[*2], and Hiromitsu Shimakawa[*1]*

[*1] Computer Science, Ritsumeikan Univ. 1-1-1, Noji-Higashi, Kusatsu, Shiga, Japan

[*2] Advanced Technology R&D Center Mitsubishi Electric Corp. 8-1-1, Tsukaguchi-Honmachi, Amagasaki, Hyogo, Japan

kyohei@de.is.ritsumei.ac.jp Nakagawa.Koichi@wrc.melco.co.jp simakawa@cs.ritsumei.ac.jp

Abstract

The Tagged World project provides services to make our life more safe and easy by recognizing and reasoning the human behavior. In the project, appropriate personalized services are provided for each person. RFID tags are attached with all objects around us. A user brings a wearable computer to record the access logs to tags. The wearable computer is equipped with RFID reader. The access logs are used in the recognition and the reasoning. We use the Bayesian network methodology for the probability statistics in the recognition and the reasoning. Fundamental experiments have done to represent the human activity using Bayesian networks. In this paper, we propose an approach to recognize and reason the human activity keeping the computation load small. We show the approach is suitable for wearable computer having the limited power resources.

1 Introduction

In a daily life, we handle more than one works at the same time. So, many people sometimes forget to do important things carelessly. The careless miss occasionally brings people into a dangerous situation. For example, a man who has his attention caught by a train departure time is likely to fail to check the fire and to lock a window and a door. These kinds of dangers exist everywhere in our lives. We have begun the Tagged World project. An aim of the project is to provide a safer and easier life. The Tagged World makes computers to recognize and reason human activities to eliminate risky factors form our lives.

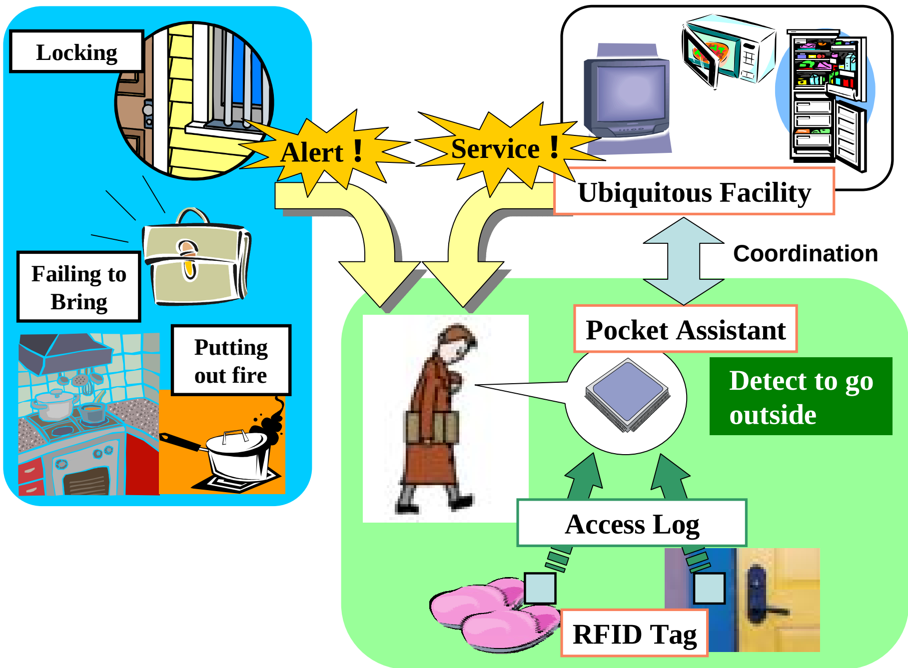

Figure 1: Tagged World

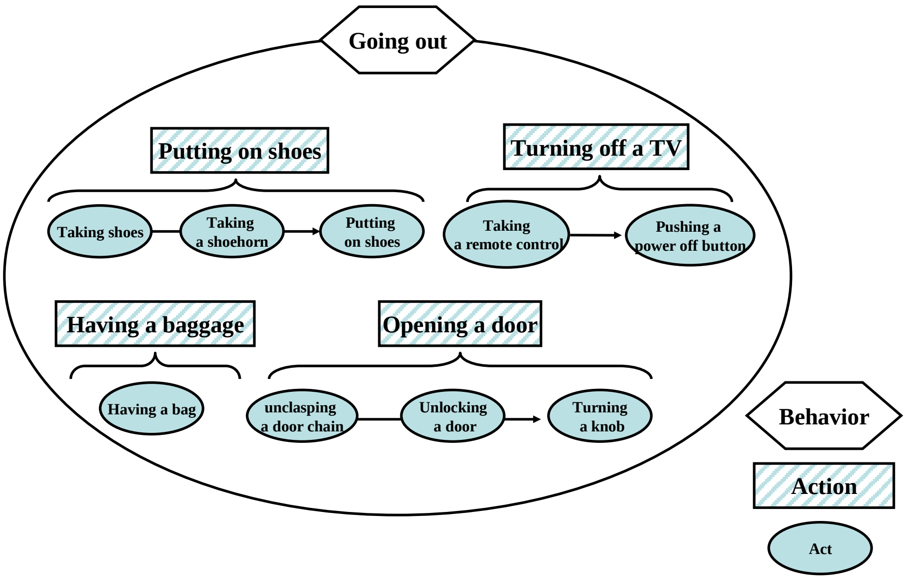

Figure 2: An Example of Human Activity

Some researches try to provide services by the recognition of human behavior[3][5]. However, they use many kinds of sensors for the recognition, which costs high. Our project employs an RFID system because of its low cost. As shown in figure 1, all objects existing around us are tagged and a user brings a wearable computer to record the access logs of the user to tags. The wearable computer is equipped with 13.56 MHz RFID reader. Since the reader can detect tags within 1 inch, we can collect only close accesses to the tag such as grasping and touching an object to which a tag is attached. The Tagged World Project refers to the wearable computer as the Pocket Assistant. The Pocket Assistant compares an access log with patterns to recognize human activities. Though a research group recognizes predefined activities using RFID tags[8], our project addresses to recognize activities without constrains. To detect a behavior as soon as possible, an access log must be compared with specific patterns every access. It would be a huge load for the Pocket Assistant that is a wearable computer with a limited power.

In this paper, we pay a special attention to objects that are important to detect a specific behavior. The Pocket Assistant compares an access log with a pattern corresponding to the behavior only when the user makes an access to the important objects. It contributes to reducing the load dramatically. This paper shows a way to reduce the load keeping the correctness of the comparison.

2 Recognition of Human Activity

2.1 Definitions of Human Activity

In this section, human activity is modelled. The human activity is composed of three elements; act, action and behavior. An act is the minimum unit of human activity. In the Tagged World, we regard an access to an object as an act such as touching an object and holding an object. An action is a sequence of acts. A behavior is a set of actions, but it is not necessary to consider the order of the actions.

For example, figure 2 shows that a user goes outside from his own house. The "*going outside*" behavior is composed by several actions such as the "*putting on shoes*" action, the "*opening a door*" action, the "*turning off a TV*" action and so on. There is no particular order in which the user takes actions. Figure 2 includes an example easy to understand. The order of the "*having a baggage*" action and the "*turning off a TV*" action doesn't have an effect on going outside. Each action can be divided into several acts. For example, the "*opening a door*" action is composed of the "*unclasping a door chain*" act, the "*unlock a door*" act, and the "*turning a knob*" act. The order of acts is fixed in an action.

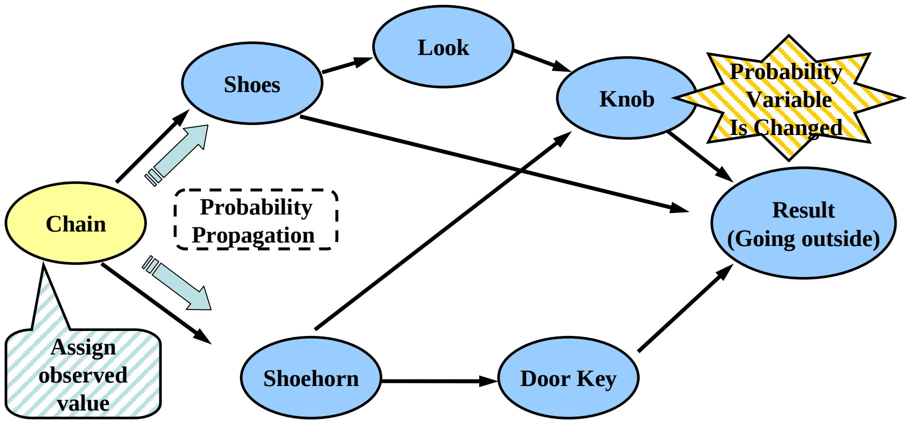

Figure 3: An Example of Bayesian network

2.2 Bayesian network and ECA Model

Our aim is to provide an appropriate service by recognition of a user behavior from a log of access to object around him. The Event-Condition-Action (ECA) Model[6] is convenient to provide the service when a specific behavior is detected. The ECA model abstracts systems that efficiently execute specified services when specified conditions hold. When an event rises up, a condition is inspected, and an action method is executed in accordance with the result of the inspection. In this research, we regard every act as an event. When a user does an act, the record of acts in a fixed term is retrieved as an access log. The log is inspected to determine whether a specified behavior may occur in the term. A service is triggered if the behavior does occur.

We apply the Bayesian network methodology for inspecting the record of acts. Figure 3 illustrates an example of the "*going outside*" behavior represented with a Bayesian network. Each node is corresponds to an act in the "*going outside*" behavior. The result node drawn on the right side of figure 3 is a node that shows the probability variable of the user going outside. By the value of the probability variable of the result node in the Bayesian network, we can deduce whether the user goes outside or not. At an initial state of the Bayesian network, no act has happened yet. In this state, all the values of probability variables are unspecified. If a user touches a door chain, for example, the observed value "1" is assigned to the probability variable of the *chain* node. The assignment causes the probability propagation where each posterior probability is calculated one after another. Eventually, the probability of the result node is calculated. Whenever the user does an act causes the retrieval of the record of acts in a term of predefined length. Probability variable corresponding to acts that occur in the record are set to "1" as observed values. The length of the term is determined so that it covers a behavior to be recognized, we refer to the term as the behavior term. Every act, the probability of the result node is calculated by the probability propagation.

2.3 Initial Approach

To detect the human behavior precisely, it is necessary to scrutinize the order and the duration of each act in the record of acts. However, it is difficult to scrutinize the temporal properties of all acts in the access log in detail, because its inspection becomes a high load factor.

To avoid a heavy load method, the process to recognize a behavior is divided into the two stages. Figure 4 shows an approach for providing some services in the Tagged World. In the first stage, a Bayesian network as mentioned in section 2.2 is adopted for detecting candidates that includes the behavior to be recognized. The function of the first stage is to reason the probability of the behavior occurrence from the sets of acts during the behavior term. In the second stage, a more detailed inspection is executed against the candidates detected by Bayesian network.

This paper discusses the efficiency of the inspection using a Bayesian network, that is, the one in the first stage. We adopt K2 algorithm[1] as a method to construct a Bayesian networks. Fundamental experiments to recognize a target behavior are done in advance. The access logs in the experiments are used to construct a Bayesian networks using K2 algorithm.

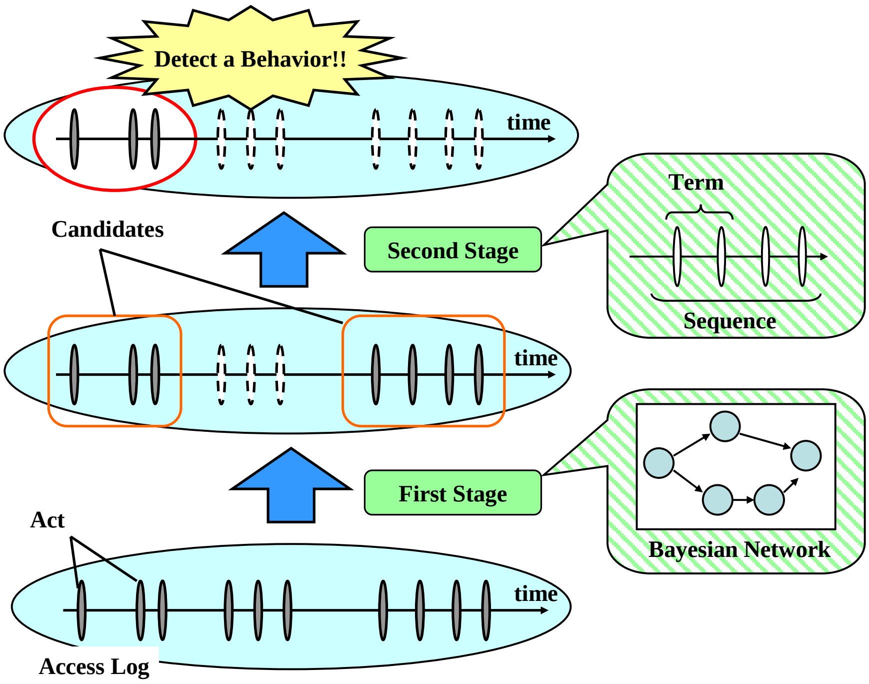

Figure 4: Initial Approach

3 Idea from Experiment

3.1 General Description of Experiment

We have experimented to obtain human behaviors. We focus on, in particular, the "*going outside*" behavior. The aim of this experiment is to represent human behaviors by a Bayesian network from the access log. We analyse specific characteristics of Bayesian networks that represent human behaviors.

Assume an apartment where a user lives alone. RFID tags are attached to various objects in the entrance. A user brings a PDA equipped with an RFID Reader/Writer. A user does some kind of cases prepared in advance. In this time, nine cases are prepared; six cases are true cases which mean going outside, while a user does not go outside in false cases though they look like the *going outside* behavior. The nine acts in table 1 are prepared and true cases and false cases are constructed by these acts as table 2 shows.

Nine users have done six true cases three times, and three false cases six times. In total, 324 cases have been sampled.

Table 1: Description of Acts

Act	Description
Taking shoes	A user takes shoes from shoe box.
Putting on shoes	A user puts on shoes without using a shoehorn.
Shoehorn	A user puts on shoes using a shoehorn.
Door key	A user has a door key.
Chain	A user unclasps a door chain.
Lock	A user unlocks a door.
Knob	A user turns a knob.
Broom	A user takes a broom.
Dustpan	A user takes a Dustpan.

Table 2: Description of True and False Cases

Case ID		Action(alignment of the acts)
True Cases	TC1	Take shoes → Shoehorn → Key → Chain → Lock → Knob
	TC2	Chain → Lock → Take shoes → Shoehorn → Door Key → Knob
	TC3	Chain → Door Key → Take shoes → Shoehorn → Knob
	TC4	Door Key → Take shoes → Chain → Lock → Shoehorn → Knob
	TC5	Door Key → Take shoes → Chain → Lock → Shoehorn → Knob
	TC6	Take shoes → Lock → Shoehorn → Door Key → Knob
False Cases	FC1	Chain → Lock → Knob (Greeting a visitor)
	FC2	Broom → Dustpan → Lock → Chain → Knob (Sweeping a entrance)
	FC3	Take shoes (Polishing shoes)

Bayesian networks whose nodes correspond to the nine acts in table 1 are generated from the access log of two users sampled at the experiment based on the K2 algorithm. The Bayesian networks recognize the *"going outside"* behavior for the access logs of seven users.

3.2 Threshold Value and Key Event

The Bayesian network works as a sieve to detect candidates from access logs. Each access to the object has some potential to change the probability value of the result node. For example, when a user takes the action which is a sequence of unclasping a door chain, unlocking a door, and touching a knob, the probability value that he goes outside may increase step by step on the Bayesian network to detect the *"going outside"* behavior. If the probability value is over a threshold value, the access log should be inspected minutely in the second stage. The threshold value is particularly important. If the threshold value is too large, the candidate might be missed. On the contrary, if the threshold value is too low, the requests which are to be inspected by the second stage might be trigged unnecessarily. Thus, the quality of the sieve depends on the threshold value.
In this experiment, we get the following two ideas;

- An effective threshold value can be determined for a Bayesian network
- Some object increases the probability value dramatically.

Figure 5 presents the transition of the probability which is calculated by a Bayesian network to detect the "*going outside*" behavior. As shown in the graph, a distinct gap of the probability exists between true cases and false

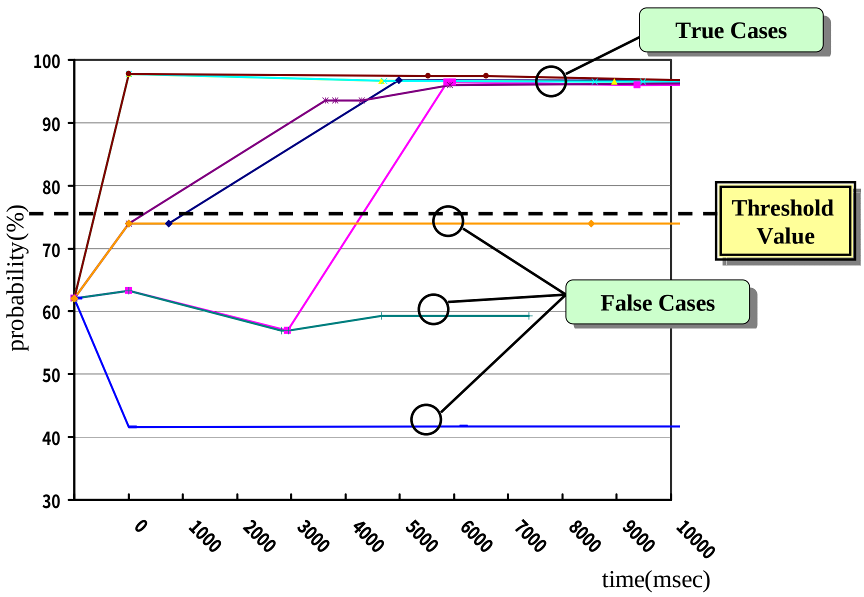

Figure 5: A Graph of the Probability

cases. In true cases, the probability increase step by step as time goes on, and the final probability converges into a value over than 90%. At the same time, the max probability of false cases never surpasses the probability of true cases. A threshold value should be set up as a value which is more than the probability of any false case in order to request second stage inspection.

When a user takes the "*going outside*" behavior, the occurrence probability calculated with the Bayesian network increases every access to an object. It is noteworthy that the breadth of upsurge is different for each of the access. An access to a specific object raises the occurrence probability to a value over the threshold value. We refer the access to the object as to a *key event*. The graphs shown in figure 6 represent the transition of the probability for four true cases. The probability of the "*going outside*" behavior increases dramatically due to a touch to shoes and a shoehorn as shown in graph 6-1. Moreover, in graph 6-2 and 6-3, a set of accesses to the shoes and the lock significantly raises the probability. In the same way, the door key raises the probability. As a result, the key event in the Bayesian network is a set of the shoes and the shoehorn, a set of the shoes and the lock, and the door key.

The key event is effective to reduce the number of calculation for the probability of the Bayesian network. In the initial approach, the calculation of the probability should be executed whenever an act is taken because any act has potential for changing the probability. It would cause a huge number of the calculation. The occurrence probability does not change when accesses other than the key event occur. It is reasonable to calculate the probability only when the key event occurs.

It is conceivable that the key event can be identified by analyzing the structure of the Bayesian network and the conditional probability table (CPT). It, however, requires the special knowledge on the Bayesian network.

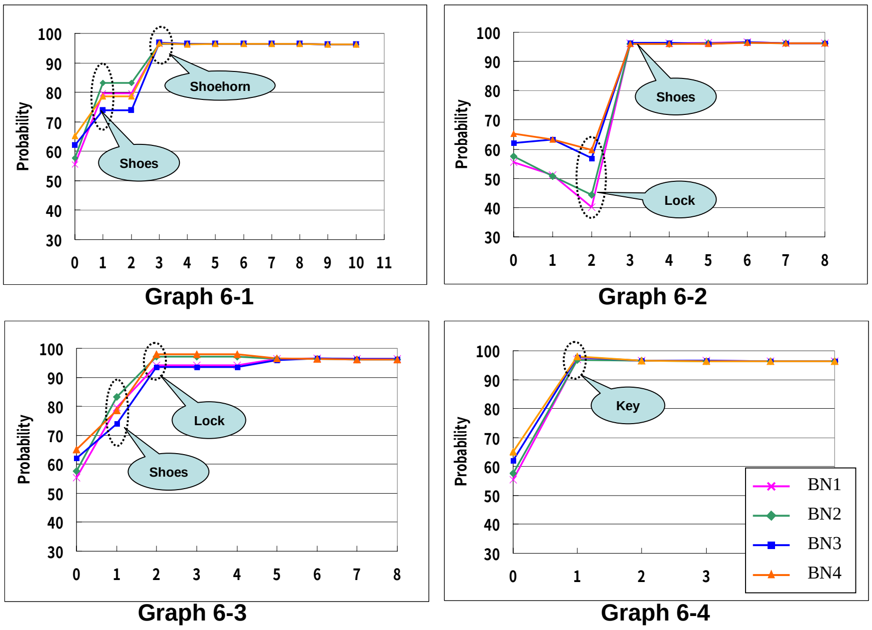

Figure 6: Graphs of the Probability

4 Revised Approach

We consider the two stage inspection to detect the behavior of a user in the initial approach. The result of the experiment indicates that another inspection should be executed before the initial approach. It is an inspection to detect a key event. We regard the discovery of a key event as a trigger to execute the probability of Bayesian network. Figure 7 presents our revised approach where the three stage inspection is executed for detecting a behavior. The first inspection checks whether a key event occurs or not. The occurrence triggers to carry out the two stage inspection of the initial approach.

In the revised approach which introduces a key event, the computation is drastically reduced as compared with the one in the initial approach. There are two reasons. The first reason is that the number of calculation times is reduced. Second, it contributes to decreasing the number of times that acts are retrieved from access log. The calculation of the probability with the Bayesian network requires to track back to a term of behavior while checking up the act. In the initial approach, the retrieval is required frequently because the probability is calculated every act is occurred. On the contrary, revised approach retrieves the acts when a key event occurs. Though the load of the observation of a key event is added in the revised approach, reduced processes brings far more reduction of the load.

We propose that the revised approach should introduce a layoff as shown in Figure 7. The result of the experiment shows that it takes at least 0.5~1.0 sec to change from one act to next. It is meaningless to set the period to calculate the probability of a Bayesian network less than 0.5~1.0 sec. In other words, we can cease the calculation of the probability for 0.5sec from the last calculation. It reduces the computation time.

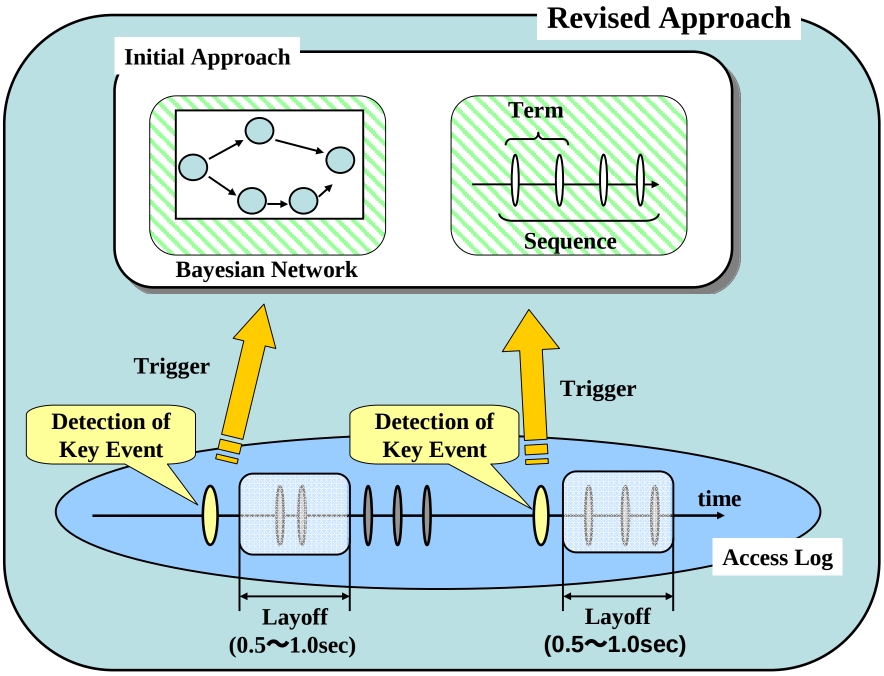

Figure 7: Revised Approach

5 Evaluation

In this section, four methods are compared in the viewpoint of the number of the calculation to gain the probability represented by a Bayesian network. The differences are the timing for the calculation. We compare the following four methods;

- Method 1 : starts the calculation when an act occurs.
- Method 2 : starts the calculation every 0.5 sec.
- Method 3 : starts the calculation when a key event occurs.
- Method 4 : starts the calculation when a key event occurs, and ceases it for 0.5 sec after the key event.

The method 1 is the identical with the initial approach and the method 4 equals to the revised approach. Each method is applied to access log of the experiment. The elements of table 3 shows the number of times the probability is calculated, accompanied with the ratio compared with the number of calculation times in the method 1. In a case of the method 2, the calculation times is reduced by approximately 20 ~ 30 percent. The decrease of calculation is remarkable in the method 3 and the method 4 that adopt in an idea of the key event. It is reasonable that key events are rare in false cases. From these results, the revised approach reduces the number of calculation by 14.8% compared with the initial approach.

Table 3: The result of Evaluation

Case ID		Method 1		Method 2		Method 3		Method 4	
		Number of Times	(%)	Number of Times	(%)	Number of Times	(%)	Number of Times	(%)
True	TC1	114	-	62	(54.39)	74	(64.91)	27	(23.68)
	TC2	78	-	49	(62.82)	64	(82.05)	21	(26.92)
	TC3	53	-	37	(69.81)	43	(81.13)	15	(28.30)
	TC4	66	-	50	(75.76)	46	(69.70)	18	(27.27)
	TC5	59	-	38	(64.41)	43	(72.88)	16	(27.12)
	TC6	37	-	29	(78.38)	6	(16.22)	4	10.81
False	FC1	18	-	14	(77.78)	0	(0.00)	2	(11.11)
	FC2	67	-	63	(94.03)	0	(0.00)	2	(2.99)
	FC3	76	-	34	(44.74)	0	(0.00)	2	(2.63)
Total		-		69.12%		32.24%		14.80%	

6 Concluding Remarks

The Tagged World aims to provide the services for a more safe and easy life. For the aim, we try to recognize and reason human activities using the RFID technology. In this research, a Bayesian network is used to recognize the human behaviors. According to the fundamental experiment, we introduce a key event. We propose the three stage inspection to utilize key events. The paper discusses the efficiency of the key event.

Experiments for various kinds of cases are left as a further work. A systematic method should be developed to find a key event.

References

[1] Gregory F. Cooper et al.：“A Bayesian Method for the Induction of Probabilistic Networks from Data”, Machine Learning, Vol.9, pp.309-347 (1992).

[2] Satoko Fujiwara and Hiromitsu Shimakawa：“Behavioral Pattern Considering Object Groups and Access Time Control”, Forum on Information Technology (FIT2004), pp.23-24 (2004), (in Japanese).

[3] Cory D. Kidd et al.：“The Aware Home: A Living Laboratory for Ubiquitous Computing Research”, Proceedings of CoBuild'99, pp.191-198 (1999).

[4] Panu Korpipää et al.： “Bayesian approach to sensor-based context awareness”, Personal and Ubiquitous Computing, Vol.7, Issue2, pp.113-124 (2003).

[5] Jani Mäntyjärvi et al.：“Sensor Signal Data Set for Exploring Context Recognition of Mobile Devices”, Workshop of Benchmarks and a Database for Context Recognition in conjunction with the 2nd Int. Conf. on Pervasive Computing (PERVASIVE 2004), pp.18-23 (2004).

[6] Dennis R. McCarthy and Umeshwar Dayal：“The Architecture Of An Active Data Base Management System”, Proc. of ACM SIGMOD International Conf. on Management of Data, pp.215-224 (1989) .

[7] Yoichi Motomura：“Bayesian network Softwares”, Journal of Japanese Society for Artificial Intelligence Vol17, No5, pp.559-565 (2002), (in Japanese).

[8] Mike Perkowitz et al.：“Mining Models of Human Activities from the Web”, Proceedings of the 13th international conference on World Wide Web, pp.573-582, (2004).