Ambient Intelligence Application of Bayesian Networks in a Home Security System

Gustavo López, Ramón Brena

ITESM, Campus Monterrey
Av. Eugenio Garza Sada 2501 Sur, Monterrey, N.L., México
gustavo.alh@gmail.com, ramon.brena@itesm.mx

Abstract. The abundance of sensors in daily life infrastructures and mobile devices can allow to determine what the users are doing, which is the situation of the environment they are in, and therefore what needs they can have and take action accordingly. Artificial Intelligence techniques are applied in order to give the users the functionality that best suits their needs. This is what is called "context-aware computing". The term "Ambient Intelligence" refers to this technology and emphasizes the incorporation of local intelligence to computing components. Ambient Intelligence is a huge field that goes from the acquisition of data from the environment, to fusioning the gathered information and data, to extracting situation characteristics, and to finally selecting and providing adequate information and services based on the extracted context. There are many applications of this technology. In this research paper, we focus in the use of bayesian networks techniques to intelligently use the information about the location and situation of persons and their surrounding environment, registered by the use of sensors, in order to deliver appropriate actions in a home security system and improve the adequacy of this kind of commercial systems.

Key words: ambient intelligence, ami, context awareness, bayesian networks, home security systems

1 Introduction

Advances in the miniaturization of electronics are allowing technological devices with various capabilities and interfaces to become part of our daily life. Sensors, actuators, and computing components can now be purchased at very affordable prices. This technology can be networked and used with the coordination of highly intelligent software to understand the events and relevant context of a specific environment and to take sensible decisions in real-time or *a posteriori*. [1]

This is related to several current technological trends. For example, Home Automation has been around for years, and applications include simple things like turning lights on and off depending on the user's location in the house, but too rigid systems have limited the possibilities of this area. The term "Ambient Intelligence", or AmI, refers to a situation where devices work in concert in order to relate to human needs. In "Ubiquitous Computing", computing devices "disappear" and integrate to the world people live in.

As it is stated in the Ubiquitous Computing manifesto [2]:

Advances in Computer Science and Electronic Systems
Research in Computing Science 52, 2011, pp. 97-106

Received 23/01/11
Accepted 20/02/11
Final version 07/03/11

"The emergence of powerful digital infrastructures, wireless networks and mobile devices has already started to move computing away from the desktop and embed it in the public spaces, architectures, furniture and personal fabric of everyday life."

The Ubiquitous Computing paradigm and, most recently, the Ambient Intelligence paradigm, are the visions in which technology becomes invisible, embedded, present whenever we need it, enabled by simple interactions, attuned to all our senses and adaptive to users and contexts [3]. From a technological point of view, Ambient Intelligence builds on early innovation concepts such as Ubiquitous Computing [4] and Pervasive Computing [5]. The major new things in Ambient Intelligence are the user involvement and situation modeling.

The algorithmic techniques and methods that apply to design for intelligence in Ambient Intelligent systems are rooted in the field of Artificial Intelligence. AI is the scientific and technological pursuit that aims at designing and analyzing algorithms that upon execution give electronic systems intelligent behavior. [6]

One of such techniques are the Bayesian Networks [7]. They are graphical structures for representing the probabilistic relationships among a large number of variables, present in real-world phenomena, and doing probabilistic inference with those variables.

A relevant real life problem for the application of AmI and Situation Modeling theory is that of a Home Security System. Common security systems are rigid, stimulus-response systems. There is an area of opportunity for implementing AmI systems, procedures and techniques in this real scenario.

The basic idea behind Home Security Systems based on Ambient Intelligence is to integrate current technological infrastructure (sensors, actuators, etc) with recent research in AmI's field focused toward personal security. This brings systems with intelligence that take situations into account (e.g. implicated users' position, habits, interpretation of activities, pertinence of notifications, etc) and act based on them.

This kind of intelligent security systems integrate the following technological components:

- Intelligent software (Identification of situations)
- Sensors (Doors, Windows, Movement, Smoke, etc)
- Communication networks
- Actuators (Notifications, Alarms, Lights, etc)
- Portable devices

Ambient Intelligence is a huge field that goes from the sensor acquisition of data from the environment, to fusioning the gathered information and data, to extracting situation characteristics, and to finally selecting and providing adequate information and services based on the extracted context. Each of these areas, or components of the process, have underlying theory and concepts of their own.

The focus of this research work, is in the Intelligent Software that implements *Situation Modeling in Ambient Intelligence* taking information from the system's sensors

and providing services using the system's actuators. The problem of this Case Study is approached using the Bayesian Networks Artificial Intelligence technique. With the use of Bayesian Networks, we examine how the information provided by the security sensors along with other parameters in the users' environment can allow to determine which is the state of the environment, which is the situation they are in, and therefore perform the corresponding action with the actuators.

2 Proposed Solution Model

In this work several sensors are distributed in the important locations of a house (possible access locations, proper measurement locations, etc). These sensors are considered to be forming a sensor network connected to a central intelligent system that takes appropriate actions. Each sensor pass its information to the system in real-time. The intelligent system makes use of a Bayesian Network to take these input parameters and decide the most pertinent action to take.

A Bayesian Network was chosen to address the problem due to its properties. Its most important advantages are the following [8]:

- By exploiting conditional independences entailed by influence chains, we are able to represent a large instance in a Bayesian network using little space.
- We are often able to perform probabilistic inference among the features in an acceptable amount of time.
- The graphical nature of Bayesian networks gives us a much better intuitive grasp of the relationships among the features.

A typical distribution of security sensors and actuators in a house is used in this case study. The schematic for the configuration of the sensors and actuators is as in Figure 1. The symbols in the figure represent the following:

- D1: Door sensor
- W1,W2,W3,W4: Window Glassbreak sensors
- M1,M2,M3,M4: Motion detectors
- S1,S2: Smoke detectors
- G1: Carbon Monoxide detector
- L1: Luminance sensor
- T1: Temperature sensor
- C1,C2: Cameras
- SI1: Siren
- LI1: Light alarm
- AC1: Central Air Conditioner

2.1 Bayesian Network Design and Implementation

A Bayesian Network was used as the solution model for this case study. It provides an important way to solve the problem and implement the AmI paradigm. The solution model, its design and implementation using this technique is shown in this section.

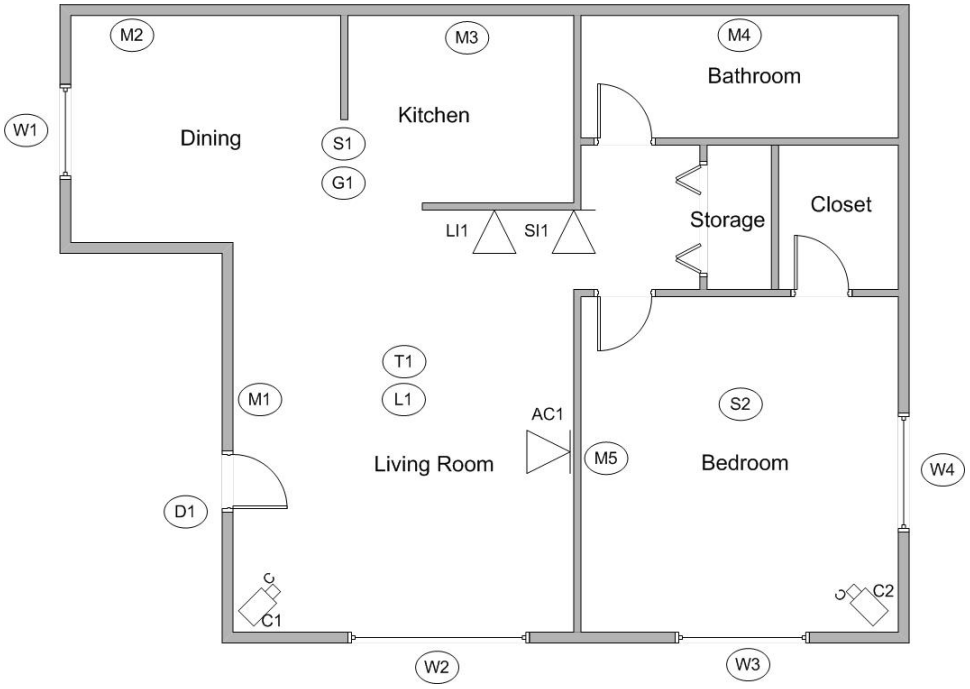

Fig. 1. Sample configuration of sensors in home

Concepts from the Ambient Intelligence and Situation Modeling framework are implemented.

For the design of the network, the AmI awareness concepts are applied. The five types of context-awareness of this application are addressed as follows:

1. *Identity-awareness (IAw)*: a simple user module is implemented to hold what kind of user(s) are in the system. In this case, four kinds of user were to be modeled: House residents, Guests, Intruders, and Animals.
2. *Location-awareness (LAw)*: the different sensors provide the location of the users in the house. In this scenario, five locations inside the house were to be modeled: Kitchen, Living Room, Bathroom, Bedroom, and Dining Room.
3. *Time-awareness (TAw)*: the time is taken directly from the system and provides valuable information. For this implementation, seven time periods represent hours with common activities: 1-5am, 5-8am, 8-1pm, 1-3pm, 3-7pm, 7-10pm, 10-1am.
4. *Activity-awareness (AAw)*: the task which the user carries out is inferred from the sensors. The activities to be modeled are: Having a Meeting, Sleeping, Cooking, Eating, and Watching TV.
5. *Objective-Awareness (OAw)*: this type of awareness is not considered in this implementation due to the nature of the problem. Most of the security system's functionality is obtained through the previous types of awareness.

All these types of awareness answer the five basic questions ("Who", "Where", "What", "When" and "Why") which provide the guidelines for context modeling. This kind of information allows us to adapt or build the needed technology to disperse throughout the environment and to model the human behavioral support. [9]

As a result from the previous guidelines, we obtain what are the middle layers of the Bayesian Network, which answer the important main questions of an AmI system. Now, the next step is to introduce the physical configuration of the home security system into the Bayesian model. This is done by introducing each one of the sensors as the input, first layer, to the system and each one of the actuators as the output, final layer, that provides a service. By doing this, we get the required nodes for the desired functionality of the network.

What follows is to establish the relationships between the nodes. There are three main design points that are relevant to mention, those are:

- One important design point in doing this is to establish the relationships so as to minimize the number of connections, and by that, minimizing the size of the conditional probability tables of the Bayesian Network.
- Another important point is to consider real-world causal relationships (i.e. cause-effect relationships between the variables in the nodes), as this usually minimizes the size of the conditional probability tables.
- A recommendation point is to exploit conditional independences entailed by influence chains, as this allows to represent a large instance in a Bayesian Network using little space.

For this particular problem, the relationships between the nodes are established following a cause and effect pattern. This is implemented as follows:

1. The activation of the *sensors* is an effect of the different *kind of users* being in an specific *location* in the house. This relationship generates causal arrows going from the users and location nodes to the sensors.
2. Different *hours of the day* cause the *users* to be in the house or not, and also to be in a different *location* of the house. This relationship generates causal arrows going from the time node to the location and users' nodes.
3. The fact that a certain *kind of users* are in a certain *location* of the house implies they are doing a certain *activity*. This relationship generates causal arrows going from the users and location nodes to the activity nodes.
4. Risk *situations* happen when specific *events* occur implying a specific kind of *user* in a specific *location* of the house. This relationship generates causal arrows going from specific combinations of sensors, location and users nodes to the risk situation nodes.
5. The different *activities* and *situations* in the house make more pertinent for certain *actions* to be carried out. This relationship generates causal arrows going from activity and risk situation nodes to the actuators.

As a result from the previous node relationship implementation, we obtain the interconnected network representing the model of the problem. Figure 2 shows this Bayesian Network. The different types of awareness are highlighted. This solution model takes

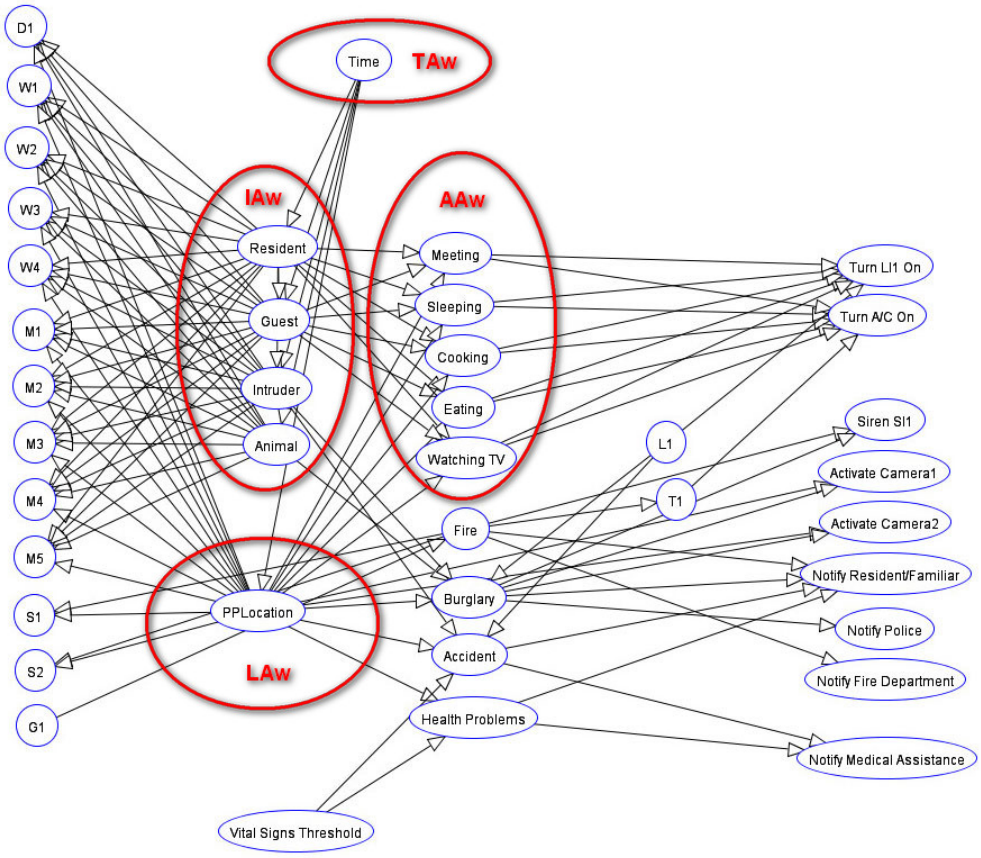

Fig. 2. Bayesian Network for sample home configuration

into account the configuration of sensors and actuators in the house as well as the previous mentioned types of awareness.

Finally, to complete the Bayesian Network so that it can be used as a proper solution model, conditional probability tables have to be introduced. For each of the nodes, values to the probability tables are filled out according to how the relationships between them behave in the real world. The size and complexity of the table for a particular node depend on the number of arrows entering the node. In general, the proposed network is neither very complex nor very simple.

The description of the solution model presented in this section gives an overview of the concepts from the AmI theoretical framework as well as the procedures implemented to make it work. The result is a Bayesian Network model of a Home Security System that works with the Ambient Intelligence paradigm at its core.

3 Experimentation and Results

In this section the functionality and performance of the model is evaluated. There can be several performance measures, but the ones of interest at this moment are the values of the outputs of the security system given a certain configuration of the input sensors. Experiments are carried out to test this. In these experiments, different values of the main sensor parameters are tested. This is done in order to see if the model provides the desired functionality, based on its design and expected behavior.

The experiments are set up in this way: a scenario of a state of the house is supposed and the state of the sensors under this scenario is fed to the system, the system then calculates the value probabilities for the output actuators. These output values are analyzed according to each scenario. The following four scenarios are considered:

- **Scenario 1**: The first scenario is a normal night at 2 am, with the resident at home in his bedroom activating sensor M5. The state of the system is as shown in Figure 3 a).
- **Scenario 2**: The second scenario is minutes afterwards with the resident at home in his bedroom when the W1 sensor detects the dinner room glass breaking. The state of the system is as shown in Figure 3 b).
- **Scenario 3**: The third scenario is the same as Scenario 2, but with the clock pointing at 8pm. The state of the system is as shown in Figure 3 c).
- **Scenario 4**: The fourth scenario continues from scenario 3, but guests arrives at home and are in the dinning room. The state of the system is as shown in Figure 3 d).

The outputs shown in Figure 3 present the changes in the probabilities of the actuators according to each scenario. These outputs are a result of the Bayesian Network probabilities propagation [8] given the inputs stated in each particular scenario. The main changes are the following:

- From Scenario 1 to Scenario 2, it can be seen how the probabilities of activating the alarm and send notifications to the resident and police increase due to the overall configuration of the situation (2 am hour of the day, dinner room glassbreak sensor activated with no residents around, resident located at bedroom, etc).
- Scenario 3 shows the effects of a subtle change in the hour of the day. The same things happening in Scenario 2, while happening at another time produce different probabilities because the prior information of the system points that burglary is more probable at certain hours than at others. Nonetheless, if a certain important event configuration of the sensors occurs, the hour could possibly not have as much effect in the probabilities.
- Scenario 4 gives another pointer. If the system detects there are users in the room where a certain sensor becomes activated, it is more probable to have been activated by accident, and therefore output probabilities change accordingly.

Thus, it can be seen from the results generated by the model that following the AmI paradigm proposed in the solution model shows to be beneficial for the Home Security System application. Clearly, the information provided by the sensors give us

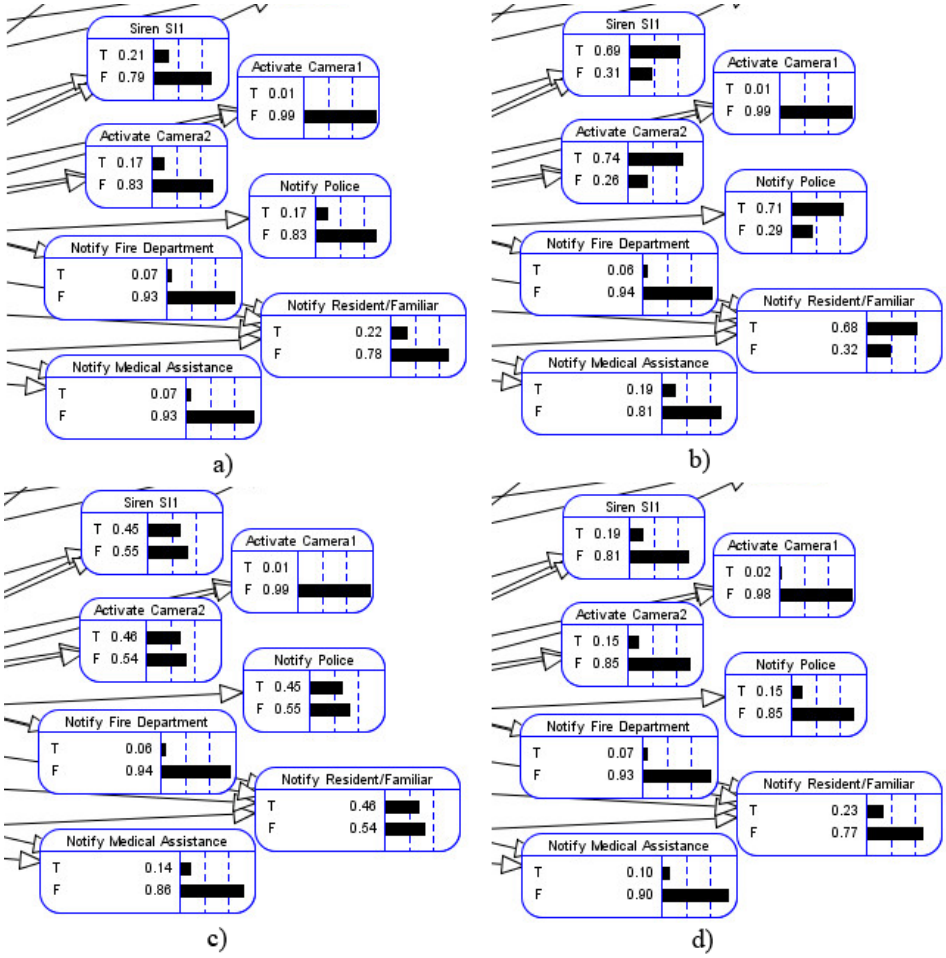

Fig. 3. Output for the four Scenarios configuration. **T** = true and **F** = false

important data to make inferences, obtain conclusions, and act accordingly. Also, the presented results show the power of only a particular implementation of the problem by using Bayesian Networks, which is very interesting as it can be explored using other Artificial Intelligence techniques such as the presented in [7] and [10].

4 Summary and Discussion

The overall results of the experiments carried out allow to actually make conclusions about the quality of the developed model as a solution to the intelligent home security system problem. The following is a summary of the obtained results:

- It can be seen from the experiments that following the Ambient Intelligence paradigm proposed in the solution model can help in identifying potential risky situations for the persons.
- The experiments demonstrated that the Bayesian Network solution model presented the potential for modeling security situations in a house.
- The information gathered by the sensors can be processed intelligently in order to produce useful inferences about the context.
- Results can get very accurate depending on the actual accuracy of the situation modeling, i.e. the better the model represents the actual system, the better the accuracy of the results.
- The experiments also show the flexibility of introducing new features to the network but also the complexity that is added by doing so.

5 Conclusions and Future Work

The solution model presented here took advantage of a whole variety of concepts such as: Context-Awareness, Probability Reasoning, Situation Modeling, Stochastic Processes, Security Systems, among others. It interconnects all those concepts into an integrated model that receives environmental input and produces results according the interpreted situation. The result is a model of an intelligent home security system that works with the AmI paradigm at its core.

Future work includes introducing the concept of *sequential behaviors*, expanding the model to recognize and interpret more complex situations, introducing important features such as a *user profile* and *activity history*, and implementing other Artificial Intelligence techniques. All of these would contribute to taking the AmI problem solution to a more useful level.

References

1. Nakashima, H., Aghajan, H., Augusto, J. C., Eds.: Handbook of Ambient Intelligence and Smart Environments. Springer, New York (2010)
2. Chalmers, D., Chalmers, M., Crowcroft, J., Kwiatkowska, M., Milner, R., O'neill, E., Rodden, T., Sassone, V., Sloman, M: Ubiquitous computing: Experience, design and science. Tech. rep. (2006)
3. Dey, A. K., Abowd, G. D.: Towards a better understanding of context and context awareness. In Proceedings of the Workshop on the What, Who, Where, When and How of Context-Awareness, affiliated with the CHI 2000 Conference on Human Factors in Computer Systems (2000)
4. Weiser, M.: The computer for the twenty-first century. Scientific American, vol. 265(3), pp. 94104. (1991)
5. Satyanarayanan, M.: Pervasive computing, vision and challenges. IEEE Personal Communications (August 2001), pp. 10-17. (2001)
6. Weber, W., Rabaey, J., Aarts, E., Eds.: Ambient Intelligence. Springer, New York (2005)
7. Hopgood, A. A.: Intelligent Systems for Engineers and Scientists. CRC Press (2001)
8. Neapolitan, R. E.: Learning Bayesian Networks. Prentice Hall (2003)

9. Mikulecky, P., Liskova, T., Cech, P., Bures, V.: Ambient Intelligence Perspectives: Selected Papers from the first International Ambient Intelligence Forum 2008 - Volume 1 Ambient Intelligence and Smart Environments. IOS Press, Amsterdam, The Netherlands, The Netherlands (2008)
10. Russell S., Norvig, P.: Artificial Intelligence: A Modern Approach. Prentice Hall (2002)