Detecting Faulty Percepts in a Context-Aware Ubiquitous System

Bilal Ahmed, [1]Young-Koo Lee, [*]Sungyoung Lee
RTMM Lab, Department of Computer Engineering, Kyung Hee University, Korea.
{bilal,sylee}@oslab.khu.ac.kr, [1]yklee@khu.ac.kr

Abstract — **Perception of a ubiquitous system is based solely upon sensor and device readings. The system decides to provide adequate services based upon these readings. We define a system of fault detection in the perception mechanism of a ubiquitous system based upon Bayesian Networks and the combination of beliefs from independent networks. The proposed scheme is distributed and adequately suits the functioning of a large multi-domain ubiquitous system. Eradicating faulty percepts and identifying the malfunctioning device would improve the quality of service, and make the system more reliable.**

Keywords — **Ubiquitous Systems, Context-Awareness, Fault-Detection, Bayesian Networks.**

1. Introduction

Advances in embedded technology and computing power have made the vision of ubiquitous computing [6] a reality. As the devices become much smaller and powerful, the desired user ubiquity can be achieved. Taking the dream of ubiquitous computing to another level we see the development of context-aware ubiquitous systems. Systems which take into account a great amount of information before interacting with the environment, and dynamically cater to user needs based on the situation at hand.

Achieving context-awareness is not an easy task; the system must decide which information to model as context and which information to discard. The system has to maintain intense interaction with the environment to gather this information. At the same time the system should possess a very strong perception mechanism consisting of a number of versatile devices. The task of such perceiving devices becomes more complicated as they have to be deployed in a real environment which is very dynamic and from the system's point of view is partially observable.

Recent research has been aimed at making such context-aware ubiquitous systems more autonomous [11]. Autonomy on the part of the system requires it to continuously monitor all its resources and implement policies which can deal with situations of faults and failures. In order to be completely autonomic the system should incorporate the essential four features; self-optimization, self-healing, self-protection, and self-reconfiguration [11][12]. Self-healing and self-reconfiguration require that the system's perception mechanism should have a reliable fault-detection mechanism so that in case of any fault or failure in any device, its behavior does not deteriorate and there is no loss of information.

The perception mechanism of a context-aware ubiquitous system is made up of a number of disparate devices and sensors. It is through the state of these components the system assesses the current situation and decides upon the best service to provide. Moreover this information also forms the context which is used by the system for better situation assessment. If any of these devices or sensors develops a fault and provides faulty data to the system, the overall system performance would deteriorate.

This work is aimed at providing a mechanism which can exploit the prior domain knowledge a context-aware ubiquitous system has, in order to devise a fault detection method for its perception mechanism. In the next section we provide the related work and the third section briefly explains the working of a ubiquitous system's perception mechanism, and context formation. It also explains the effect of a faulty percept on the context formed and system behavior. Finally in the fourth section we present the proposed scheme and some simulation results.

2. Related Work

Fault detection and diagnosis in sensors and sensor networks has been the focus of much research in current years. Some well-established models for fault tolerance in sensors include the celebrated Marzullo model [3] and Iyengar's model [3]. These models have proven very useful in large and distributed sensor networks.

Online fault-detection of sensor measurements has also been done using function minimization and non-parametric techniques [4]. The approach uses function minimization and application of non-parametric statistical methods to weed out the most probable faulty sensors in a sensor network. Optimization is achieved by using Powell non-linear function minimization method. Whereas the above mentioned techniques have been applied successfully for fault tolerance and fault-detection in distributed sensor-networks, they do not involve much prior domain knowledge apart from that of the sensors. In a context-aware ubiquitous environment the prior domain knowledge is useful in predicting sensor behavior and modeling complex scenarios which can constrain the behavior of sensors and actuators. This additional knowledge needs to be incorporated for more reliable fault-detection techniques.

Sensor and actuator fault-detection in large dynamic systems has also been done using stochastic automaton [4]. The addressed systems include those which have discrete valued inputs and outputs. The approach is based on the generalized observer scheme and extends it to deal with discrete valued variables.

Sensor fault detection and identification for chemical processes using Bayesian Belief Networks has been explored thoroughly in [17]. The model applied is similar to the one presented here. It achieves fault detection through simple evidential reasoning and the identification is done through an analysis of the most probable state of the sensor over a long period of time. The main difference between this work and our work is the fact that we are trying to identify the faults in sensors and devices which form the complete perception mechanism of a ubiquitous system, whereas the work mentioned deals only with sensor faults.

Bayesian Networks have been used in fault detection and diagnosis of dynamic systems [5]. The work has been focused on domains related to the control and supervision of large industrial processes involving mixtures of continuous and discrete variables. The main technique in this work includes hybrid dynamic Bayesian networks which capture the stochastic nature of the process and accommodate all types of system variables both discrete and continuous. The application of learning Bayesian networks from system data has also been used for fault detection in large dynamic systems. This method explores the learning capability of Bayesian networks from measurements of the relevant signals that are present in the dynamic system by the use of a learning algorithm [7]. As opposed to our technique these techniques capture the temporal relations of various process components. Such temporal knowledge is not so critical for the context-aware ubiquitous system to be used efficiently for fault-detection.

Bayesian networks have been successfully used in anomaly detection. Naïve Bayesian networks have been employed for detecting anomalies in active networks for providing intrusion detection services [2]. Similarly Bayesian networks have also been used for developing self-aware services which use Bayesian networks to detect any anomaly in their behavior while functioning on the internet [1].

A complete classification of the various types of faults in a ubiquitous system is given in [13]. It goes on to propose an architecture for a fault-manager inside a ubiquitous system. The main focus of the work is on fault-tolerance in large and context-aware ubiquitous systems, dealing with application and device failures. Our proposed scheme deals specifically with the perception mechanism of a context-aware ubiquitous system and addresses in detail the faults which can occur in the hardware components such as the disparate sensors and actuators.

3. Context-Aware Ubiquitous Systems

Ubiquitous systems have been designed to facilitate the interaction of humans with computers so that instead of being distinct objects in a user's environment, computers become a part of it by embedding the computations into the environment. In order to achieve this goal the system would have to maintain a very intense interaction with its environment [10]. It needs prior knowledge about the domain, the user and the devices with which it interacts.

3.1 Perception Mechanism of a Ubiquitous System

In a context-aware ubiquitous system the entire perception mechanism of a system is composed of a number of diverse sensors deployed in the environment to monitor various physical quantities. A number of controllers or actuators are used by the system to respond to various changes which take place in the environment. The detection of such changes and the formation of context based on these changes is dependent on the data sensed from the monitored environment [10].

In any particular scenario the steps taken by the system can be defined as sensing some data from the environment and acting on its basis. The action taken in the light of the sensed data is determined through various factors such as available resources, the contextual contents, and user preferences. Every such decision step taken by the system also involves sensing data which is needed for validating if the action has indeed succeeded. The complete interaction cycle in a scenario is shown in Figure 1; taken from [14].

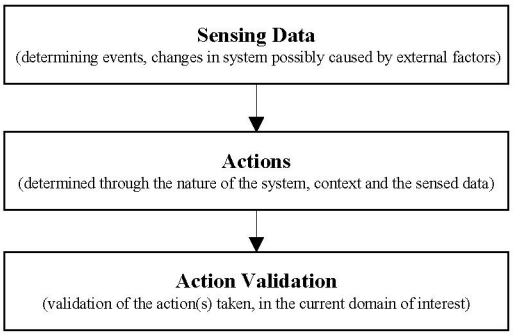

Figure 1. The complete interaction cycle of a context-aware ubiquitous system.

3.2 Context Formation

In large context-aware ubiquitous systems, the formation of context plays the most important role in their functionality. Context formation is done, using some prior domain-specific knowledge and the sensed data [10]. Prior domain knowledge can be represented using any feasible knowledge representation technique such as ontology etc [10]. Context is formed by fusing together sensed data and this prior domain knowledge. Sensed data plays the most important part in context formation. The current context is responsible for determining system decisions such as the type of service to be provided to the user and if through any sequence of events the sources of sensory data get corrupted the context formed would be incorrect. As the contextual knowledge plays the central role in the interaction cycle of a ubiquitous system, incorrect contextual information would result in erroneous system behavior.

4. Fault Detection using Bayesian Networks

A pervasive environment defines constraints on the behavior of devices and sensors with changing situations. These constraints can be used to model a single interaction-cycle of the system; accommodating all the participating devices and sensors. This model can then be used for detecting any fault in the system and identifying the faulty device or sensor.

Deducing the state of a single component from a single interaction-cycle would seem inappropriate because the device or sensor in question could be a part of another interaction-cycle where it interacts with a different set of devices. Considering the role of each device in an interaction-cycle different from its role in another interaction-cycle creates a sensor or device role replication. Thus, in order to exploit all the relevant evidences that we can get about a single device, we need to define a mechanism which can take this role replication into account and identify a faulty component with more confidence. In order to achieve this goal, we can define a single Bayesian Network [8] [9] which can absorb all the devices and their interactions. Maintaining a single Bayesian Network of this magnitude would be computationally infeasible. Most of the algorithms for exact inference in Bayesian Networks are exponential with the tree width [15], detecting and identifying faults would consume much system resources and time.

Separate Bayesian Networks can be used to model all the interaction cycles as mutually independent Networks, having some nodes in common.

4.1 Sensor and Actuator Models

We use the sensor and actuator models as described in [14]. For future use the models are described in figure 2.

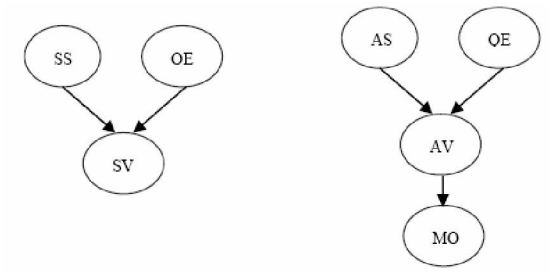

Figure 2. A Bayesian network representing a sensor (SS: Sensor State, QE: Physical Quantity/Event, SV: Actual Sensor Reading) on the left and a Bayesian network representing an actuator (AS: Actuator State, QE: Physical Quantity/Event, AV: Actuator Reading, MQ: controlled quantity) on the right.

According to the chain rule for Bayesian networks the joint probability distribution for the sensor model is given by the equation:

$$P(SS,QE,SV) = P(SV \mid SS,QE) \times P(SS) \times P(QE) \ldots (1)$$

and for the actuator model it is given as:

$$P(AS,QE,AV,MQ) = P(MQ \mid AV) \times P(AV \mid AS,QE) \times P(AS) \times P(QE) \ldots (2)$$

4.2 Sensor and Actuator Models

Each scenario can be described through a single Bayesian Network, by connecting the sensor and actuators which participate in it, as shown in figure 3.

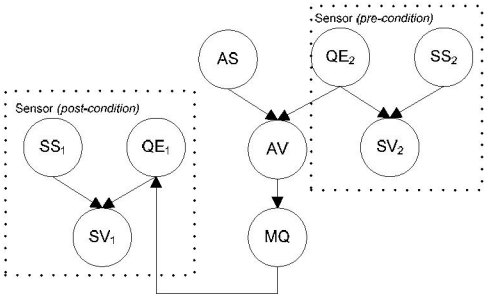

Figure 3. A complete scenario specified according to the selected models, for single sensors at the pre-condition and post-condition levels and a single actuator at the action level.

Thus in the representation of a scenario we find pseudo-causal relations among the participating devices. These relations impose constraints on their behavior, and any deviation from this would lead to an anomaly, which could be identified. The anomaly makes itself visible through the state variable of the participating devices. This inference is local to the scenario, inferences from other scenarios which contain the device should also be taken into account for the formation of a more reliable global belief.

Representing every scenario as an independent Bayesian Network, would distribute the number of devices present in the system among several networks. In case one of the devices has been recognized as being faulty it is needed that the beliefs currently assigned to this variable in other networks should also be taken into account. Thus we need a mechanism to combine probability estimates from separate sources.

We propose to use a scheme of combining probabilities from different sources based upon the amount of information they have. The combination is done using (3) which has been taken from [16].

$$p^* = \sum_{i=1}^{n} \beta_i p_i \ldots\ldots (3)$$

Where 'i' indicates the number of scenarios considered for forming the belief, 'β' is the amount of information each scenario has and 'p^*' denotes the global probability about the state of the device. 'β' is estimated using equation (4).

$$\beta_i = \frac{Devices\ in\ Scenario\ i}{\sum Devices\ in\ each\ scenario} \ldots\ldots (4)$$

Thus, a scenario which involves more devices would have more contribution in the overall belief formation, as it has more information about the system as compared to others.

5. Results

In the experiment which were simulated we considered three scenarios having one device in common. In order to

show the effectiveness of the technique we show the belief from each scenario and the overall combined belief.

1) "Whenever the user enters his bedroom, the inside temperature is adjusted according to the temperature outside the room. The user has defined his preferences "

2) "Within the bedroom the user has also given his preferences for setting the humidity level according to the current temperature of the room"

3) "The bedroom contains an area which the user uses as his study, and its tem-perature is also to be kept according to the temperature of the room, it has a separate actuator for adjusting the temperature, and the user has specified his preferences for this task."

The devices used in the described scenarios are:

- Internal Temperature Sensor
- Room Air Conditioner
- Movement Detector
- External Temperature Sensor
- Humidifier
- Humidity Sensor
- Study Air Conditioner
- Study Temperature Sensor

and the corresponding Bayesian Networks are depicted in figures 4 and 5

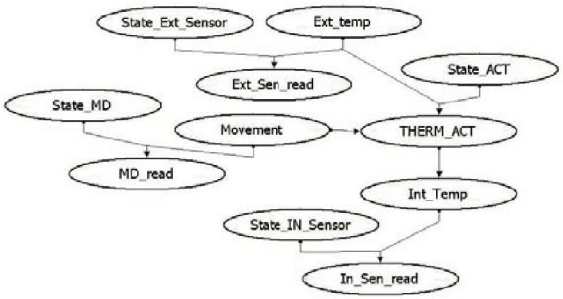

Figure 4. Bayesian Network for the first scenario.

It is impossible to list all the probability distributions here, for the sake of simplicity we provide the probability distribution of the movement-sensor from the first scenario. This is listed in Table-1.

For the test run consider that the internal temperature sensor is faulty. As it is present in all the three scenarios we need to evaluate each scenario independently and then combine the belief of the possibly faulty devices. The evidences entered into the system are listed in Table-2.

Table 1. Conditional Probability distribution for the movement detector from scenario 1 P(MD_read | State_MD, Movement)

		MD_read	
State_MD	**Movement**	*Yes*	*No*
Correct	*Yes*	1.0	0.0
	No	0.0	1.0
Incorrect	*Yes*	0.65	0.35
	No	0.35	0.65

Table 2. Device and Sensor Values for the simulation

Device	Scenario1	Scenario2	Scenario3
Internal Temperature Sensor	16-20	11-15	11-15
Room Air Conditioner	11-15		
Movement Detector	Yes		
External Temperature Sensor	31-40		
Humidifier		16-20	
Humidity Sensor		16-20	
Study Air Conditioner			16-20
Study Temperature Sensor			16-20

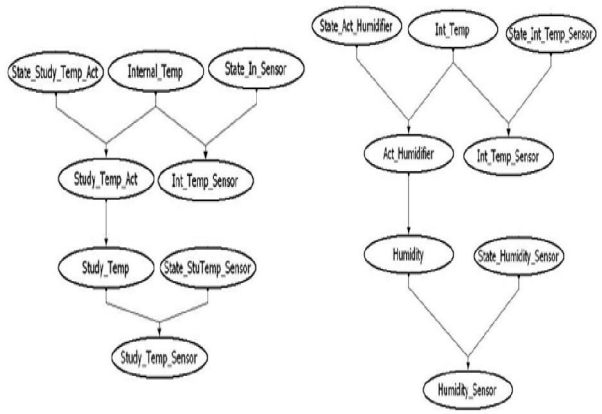

Figure 5. Bayesian Networks for scenario2 and scenario3.

The resulting state-probability for the devices are shown in Table-3.

Table 3. Resulting probability for the devices from each scenario. P(Device=Incorrect)

Device	Scenario1	Scenario2	Scenario3
Internal Temperature Sensor	0.8146	0.6663	0.7656
Room Air Conditioner	0.0508		
Movement Detector	0.2871		
External Temperature Sensor	0.1		
Humidifier		0.4891	
Humidity Sensor		0.2683	
Study Air Conditioner			0.2872
Study Temperature Sensor			0.0488

The combined belief for the internal sensor and the humidifier are calculated according to (3), and P(state_int-temp_sensor=Incorrect)=0.7554 and P(state_humidifier=Incorrect)=0.1467. Thus it is clear that the internal temperature sensor of the room is faulty and its readings should be corrected or discarded.

5. Conclusion and Future Work

We have proposed a scheme for fault detection using Bayesian Networks and the combination of beliefs from independent sources. The technique utilizes the prior

knowledge that the system possesses such as user-preferences and device and sensor descriptions. Bayesian Networks are created for each possible interaction cycle with the assumption that even with overlapping nodes the networks are mutually independent and the device replication in these scenarios is used to form a global belief about the state of the device or sensor. The proposed scheme not only helps in filtering out faulty percepts but it forms a vital component needed for making the system more autonomic, specially in the case of self-healing and self-optimization [11].

As our future work we would like to validate the theoretical aspects associated with our main assumption about the mutual independence of Bayesian Networks which have some nodes in common.

REFERENCES

[1] Alexandre Bronstein, Joydip Das, Marsha Duro, Rich Friedrich, Gary Kleyner, Martin Mueller, Sharad Singhal, Ira Cohen1, "Self-Aware Services: Using Bayesian Networks for Detecting Anomalies in Internet-based Services", HP Labs Technical Reports HPL-2001-23R1, 2001.

[2] Abdallah Abbey Sebyala, Temitope Olukemi, Dr. Lionel Sacks, "Active Platform Security through Intrusion Detection Using Naïve Bayesian Network for Anomaly Detection", proceedings of LCS 2002.

[3] Cheryan Jacob and Ranjit John Mathai, "Fault Tolerance in Sensor Networks, A Survey of Fault Tolerant Sensor Network Algorithms and Techniques".

[4] Koushanfar, F.; Potkonjak, M.; Sangiovanni-Vincentelli, A.; "On-line fault detection of sensor measurements" Sensors, 2003. Proceedings of IEEE Volume 2, 22-24 Oct. 2003 Page(s):974 - 979 Vol.2

[5] Uri Lerner, Ronald Parr, Daphne Koller, Gautam Biswas, "Bayesian Fault Detection and Diagnosis in Dynamic Systems", Proceedings of the Seventeenth National Conference on Artificial Intelligence (AAAI-00), pages 531-537, Austin, Texas, August 2000

[6] M.Satyanarayanan, "Pervasive Computing: Vision and Challenges", IEEE Personal Communications, pp.10-17, Aug. 2001.

[7] Jackson P. Matsuura and Takashi Yoneyama, "Learning Bayesian Networks for Fault Detection", 2004 IEEE Workshop on Machine Learning for Signal Processing.

[8] Jensen, Finn V., "Bayesian Networks and Decision Graphs", Springer-Verlag 2001, ISBN 0-387-95259-4.

[9] Pearl. Judea, "Probabilistic Reasoning in Intelligent Systems: Networks of plausible inference", Morgan Kaufmann publishers 1988, ISBN 1-55860-479-0.

[10] Hung Q. Ngo, Anjum Shehzad, Kim Anh Pham, Maria Riaz, Saad Liaquat, and S. Y. Lee, "Developing Context-Aware Ubiquitous Computing Systems with a Unified Middleware Framework".

[11] Roy Sterritt, Dave Bustard, "Autonomic Computing - a means of achieving dependability?", Proceedings of the 10th IEEE International Conference and Workshop on the Engineering of Computer-Based Systems (ECBS'03).

[12] Jeffrey O. Kephart and William E. Walsh, "An Artificial Intelligence Perspective on Autonomic Computing Policies", Proceedings of the Fifth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'04).

[13] Shiva Chetan, Anand Ranganathan and Roy Campbell, "Towards Fault Tolerant Pervasive Computing".

[14] Ahmed, Bilal. Lee, Young Koo. Lee, Sung Young, "Scenario Based Fault Detection in Context-aware Ubiquitous System", Proceedings of CIMCA 2005.

[15] Xiang, Yang, "Probabilistic Reasoning in Multiagent Systems: A Graphical Models Ap-proach", Cambridge University Press (2002).

[16] Clemen, Robert T. Winkler, Robert L., "Combining Porbability Distributions from Experts in Risk Analysis", Risk Analysis, Vol. 19, Springer-Verlag (1999).

[17] Nasir Mehranbod, Masoud Soroush, and Chanin Panjapornpon, "A method of sensor fault detection and identification", Journal of Process Control, Vol. 15(3), Elsevier, April 2005: pp 321-339.