Sensor Management by using Bayesian Networks

Nuri Yilmazer and Lisa Ann Osadciw

Department of Electrical Engineering and ComputerScience
Syracuse University, Syracuse, NY- 13244-1240
Phone : 315-443-3366/Fax: 315-443-2583
nyilmaze@syr.edu/laosadci@syr.edu

Abstract - This paper introduces the sensor management problem and uses Bayesian networks as a scalable approach to handling the operational decisions concerning the sensor network. In general, single sensor systems only provide partial information on the state of the event or environment while multisensor systems provide a synergistic effect, which improves the quality and availability of information. Data fusion techniques can effectively combine this environmental information from similar and/or dissimilar sensors. Until recently, the operator could manage these multiple systems easily, but current systems are more complex and produce data more quickly than earlier versions. A sensor manager becomes necessary when this occurs to assist the operators. Researchers have developed many single point sensor management solutions.

I. INTRODUCTION

Sensor management can be described as a system or process that provides automatic or semi-automatic control of a group of sensors. In general, sensor management approaches can be divided into normative and descriptive methods[1]. Bayesian Network (BN) models, also called graphical models, have emerged as a powerful tool for representing and computing complex probability distributions. Hence they provide a compact representation as more of a normative method than descriptive method. This paper presents a unique approach to sensor management by using BN to assist in making decisions impacting global performance and, thus, individual sensor operation.

The sensor operating parameters are selected to achieve the desired global performance goals requested by the sensor manager. The sensors are, therefore, controlled indirectly through their performance. In this paper, performance parameters such as the false acceptance rate, FAR, or increasing accuracy are used. This approach, however, can be applied to any sensor network that can be measured in terms related to these performance parameters. In this study, a general BN algorithm is designed to solve the sensor management problem.

Systems that automatically or semi-automatically control a suite of sensors are defined as Sensor Management Systems [2]. In general, single sensor systems provide only partial information, while multisensor systems provide more complete information by using the synergistic effect of combining different data types. As the sensor networks become larger with either many sensors or more complex sensors, the task of managing the network becomes overwhelming for an operator.

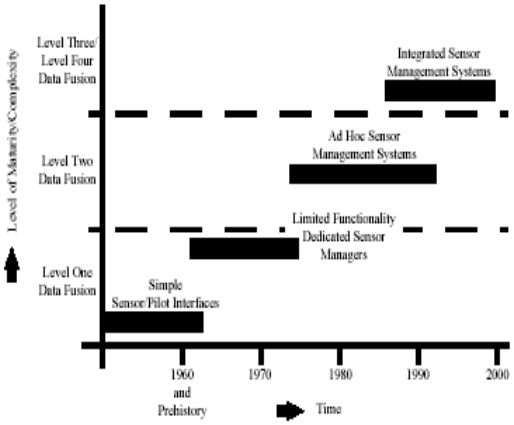

Fig. 1.R&D in Sensor Management Systems

Sensor management can simply defined as the efficient control of sensor resources [3]. Alternatively, the goal of sensor management is to perform the right task at the right time on the right object. Issues making the job tough include:

1. Environment is highly dynamic,
2. Sensor resources are insufficient,
3. Sensors have limited capability,
4. Sensor failures,

5. Interference and spoofing [4].

Research and development in the sensor management area are summarized in Figure 1. In the 1960s, systems were managed by pilots or operators, and sensor management was very immature (i.e. level 1 maturity). In the late 1960s through the 1970s, a few dedicated sensor managers were built that concentrated on specific functions to ease the burden on the pilots (i.e. still level 1 maturity). Ad-hoc sensor management systems emerged in the 1980s and reach a level 2 in maturity and complexity. By the 1990s, fully integrated sensor management systems emerge and are at a level 3 in maturity. However, these systems lack a general methodology that can easily be applied to any type of sensor network (level 4 in maturity). Thus, each sensor network employs its own special sensor manager.

Recent systems are even more complicated, and operators find it impossible to manage the whole system. The sensor manager (SM) should reduce the operator's workload by automating sensor allocation and reconfiguration. Sensor management can be thought of as a feedback control system, which maintains a required level of system performance. SM dynamically updates the sensor's operating parameters based on the system's current performance, the dynamically changing situations, and current sensor capabilities. Most of the research in sensor management to date has focused on tracking, detection and identification of the target[5]. These sensor managers are not easily applied to other sensor networks. This paper's algorithm, however, supports most sensor management problems.

Different methods such as neural networks, linear programing, heuristic or rule based systems have been applied to solve the SM problem[6][7]. We present a sensor manager based on Bayesian Networks, BN, also called graphical models. At the heart of the SM problem is determining the underlying probability distributions of the performance parameters given the state of the world, sensors, and events. The designer can use a priori knowledge to initialize these random variables but the SM must be able to learn and adapt the distributions as the system operates. The BN approach has recently emerged as a powerful tool for representing and computing complex probability distributions [8]. Hence, BNs will be used to assist in the decisions surrounding the choice of performance parameter requirements such as reducing the error rate or increasing accuracy. This study describes a general BN algorithm designed to solve the SM problem. It can handle a wide variety of sensor manager problems with minimal redesign.

1.1 Bayesian Network Review

Bayesian Networks were introduced in the 1980s for representing and reasoning problems by modelling the elements of uncertainty and, thus, adopting probability theory as a basic framework. A BN consists of the following elements [9].

1. A set of variables and a set of directed edges between variables.
2. Each variable has a finite set of mutually exclusive states.
3. The variables together with the directed edges form a directed acyclic graph (DAG).(A directed graph is acyclic if there is no directed path $A_1 \rightarrow \ldots \rightarrow A_n$ s.t. $A_1 = A_n$).
4. To each variable A with parents $B_1 \ldots B_n$ there is associated the potential table of conditional probabilities $P(A|B_1 \ldots B_n)$.

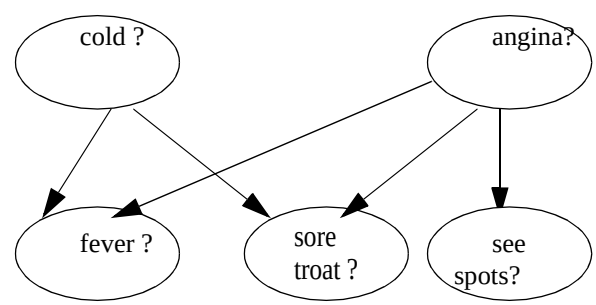

Fig. 2. A Simple Bayesian Network

A simple example of Bayesian Network is shown in Figure 2. The arrows represent the causal relationship between the variables. The fever is caused by a cold or angina. Each node is a random variable. Cold and Angina, which are defined by a priori probabilities, do not have parent nodes because they are the root causes. Fever, "sore throat", and "see spots" are defined by conditional probability distributions.

BNs are easy to modify and create by a good knowledge engineer. Their structure and parameters can be learned from the data through efficient algorithms. Once a BN is created it can be used in decision-making. Uncertainty about the state of world is represented by a probability distribution over the states. Probability can be considered a rational agent's degree of belief about the uncertain states of the world. By using a BN, beliefs are updated by conditioning on new information about the world's state.

2. Definition Of the Problem

The security of buildings is an increasing concern nowadays. One critical problem is assuring employees safety within their employer's building. In this building access

application, employees need varying levels of access to various regions of a building. The access requirements depend on an employee's daily tasks. Specific employees must handle security, finances, and sensitive information, which may be done in exclusive regions of the building. Clients or customers must move through other regions of the building all day.

Currently, this problem is either ignored resulting in a lack of security, or people are given something to carry like an identification card or key. Another option is to use codes and passwords. Both of these approaches to the problem are very prone to errors resulting in granting access to imposters and denying access to a genuine employees or customers. Sensor networks consisting of biometric sensors interfaced to door locking mechanisms is a better solution in terms of security and ease of use. Some more common biometric sensors include an optical or ultrasonic fingerprinting system, a face recognition sensor, iris scanning sensor, voice recognition sensor, or a hand geometry sensor. In this section, the BN that manages this network is provided as an example of an SM.

Performance of the biometric sensor network is based on decision error rate, user acceptability, and user circumvention[10]. The decision error rate is how often an imposter is granted access or, conversely, a genuine user is rejected access. User acceptability is the level that the user feels his/her privacy or physical space is invaded. Retinal scanning is rarely used, currently, because users do not want to place their heads on a device and have light beams scanning their retinas. These systems are frequently avoided. User circumvention results if the system takes too long or rejects the user too often.

A sensor manager can be used to manage the biometric sensors as well as fuse the decisions from the sensors [10]. One complex issue in this building accessibility system is how to quantitatively and automatically vary an individual's security level while taking into account the building's safety status, the individual's job, and the uniqueness of the employee's biometric features [10]. Uniqueness is a measure of how different one's biometric data is from the rest of the population. Some people have indistinct features rendering that biometric modality useless. The accessibility requirements for an individual can be based on their job description. Figure 5 illustrates the network's functions and how a sensor manager would interface with the network. The SM accepts the uniqueness of that individual's biometric features, his/her job description, and the security status of the building. The SM outputs the costs associated with each sensor's decision errors, and any needed sensor operating parameters such as decision threshold.

The security level corresponding to the job description and biometric features constitute the information gathered when an employee is enrolled into the system. Biometric features include any data that a biometric system requires to verify a person's identity. For voice recognition, this includes the voice samples required for comparison. In a face recognition system, an image of the face must be collected. The biometric data usually requires some processing before a comparison template is produced. This additional processing of the reference data is done at the time of enrollment as well. The biometric features are collected and matched against the enrollment features when the individual requests access. When the employee accesses the system, one of four consequences occurs

1. the genuine employee is accepted,
2. the genuine employee is rejected,
3. the imposter is accepted,
4. the imposter is rejected.

The system performance is based on the total error rate or the rate consequence 2 and 3 are made. The errors described in 2 and 3, the false rejection rate (FRR) and false acceptance rate (FAR), respectively. The sensor manager assigns a cost to each error type, which results in varying security levels for different employees. We define the error rates as

$$F_{AR_i} = P(d_g = 1|H_0) \text{ and} \quad (1)$$

$$F_{RR_i} = P(d_g = 0|H_1) \quad (2)$$

where H_0, the person is an imposter, H_1, the person is genuine, and the global decision made by the fusion system is

$$d_g = \begin{cases} 0, \text{ the person is an imposter} \\ 1, \text{ the person is genuine} \end{cases}. \quad (3)$$

The total error including costs is

$$E_t = C_{FA}F_{AR_i} + (2 - C_{FA})F_{RR_i} \quad (4)$$

where F_{AR} is the false acceptance rate, F_{RR} is the false rejection rate, and C_{FA} is the cost associated with the false acceptance rate[11]. A cost of 1 results in the total error rate being composed equally of the FAR and FRR. Accuracy, which is the focus of this paper, is equal to the total error rate when defined by Equation (4) with a C_{FA} of 1.

The conditional probability density functions are $p(d_i|H_1)$ and $p(d_i|H_0)$ where d_i is the decision output of the ith biometric sensor given the genuine person and the imposter, respectively. In this example, the sensor decisions are fused. The sensor decision is the likelihood ratio test given by

$$\frac{p(d_i|H_1)}{p(d_i|H_o)} \underset{d_i=0}{\overset{d_i=1}{\gtrless}} \lambda_i \tag{5}$$

where λ_i is an appropriate threshold. The optimum Bayesian fusion rule ([10]) allowing access to a building for N sensors is

$$\sum_{i=1}^{N}\left[d_i \log\left(\frac{1-F_{RR_i}}{F_{AR_i}}\right)+(1-d_i)\log\left(\frac{F_{RR_i}}{1-F_{AR_i}}\right)\right] \underset{d_g=0}{\overset{d_g=1}{\gtrless}} \log\left(\frac{C_{FA}}{2-C_{FA}}\right) \tag{6}$$

where N is the number of sensors.The rule in Equation (4) assumes an equal a priori probability of an imposter and genuine user. There are a total of 2^{2^N} possible fusion rules if all possible combinations of the sensor decisions are considered. Since F_{AR}, F_{RR}, and C_{FA} are set by SM, the SM controls the fusion of the individual sensor decisions.

Each node for the BN that handles this building security application represents a random variable. An example BN controlling the main entrance to the building is given in Figure 4. The node (High Security Building State) has three mutually exclusive states which are high, medium and low level. The High Security Job node also has these same three mutually exclusive states. Uncertainty about the state of the world is represented by the probability distribution over states for the nodes in Figure 4. The BN is used to update beliefs, which are represented by the node's conditional probability distribution and updated by conditioning on new information or evidence about the world. After the beliefs are updated, the error cost in Equation (4) is updated. Thus, the global decision is modified by the new information. The 5 actions to be taken correspond to the 5 arrows exiting Figure 4. These include disabling/enabling sensors 1,2, and 3, and increasing/decreasing the false acceptance rate cost and false rejection rate cost.

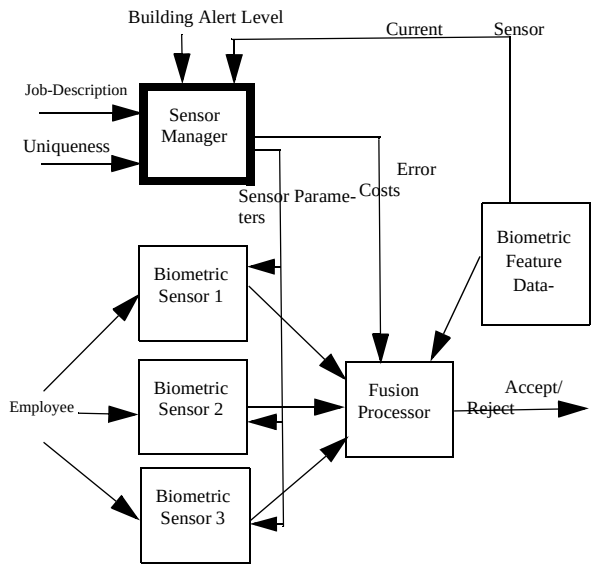

Fig. 3.f Overview of Building Security System

In this study, it is assumed that the Security Guard has the highest probability of requiring access to restricted rooms. Imposters will most likely try to steal the identity of these individuals. Identifying security guards must have the lowest error rate and is set high at 0.56. All the values are exaggerated for demonstration purposes. Typical values of false acceptance rates are around 0.001 but these are so low that it is difficult to demonstrate variations between systems. The company president also requires a lower identification error rate; the false acceptance rate for this employee is 0.12. The average employee is 0.36.

The extended BN simulation is shown in Figure 5. The conditional probability distributions are either entered by a knowledge engineer or learned from data. For this simulation, they were entered. For varied uniqueness values in node 3, the resulting output FAR is adjusted as can be seen in Figure 6 and Figure 7. Table I shows how the FAR changes for different scenarios.As the confidence in Uniqueness in 3 node increases, this will decrease the FAR. Two different situations are examined in here for different values of confidences in (uniqueness 3, 2, and 1 nodes), the result can be seen in Table2.

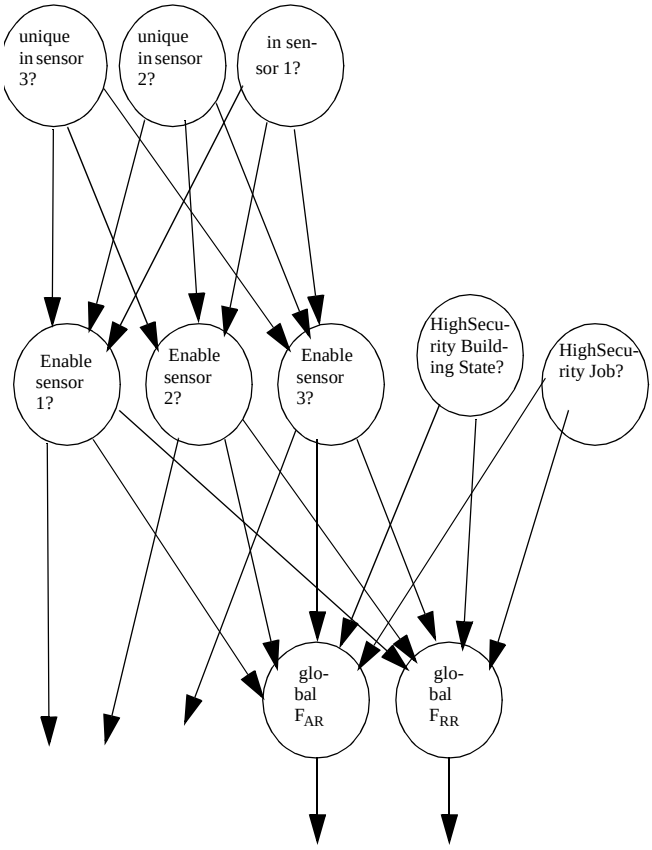

Fig. 4.Bayesian Network for the Sensor Manager at the Main Entrance

TABLE I.

Uniqueness in 3 (%)	FAR (%)	FRR(%)
90	42.4	55.6
80	43.1	55.0
70	43.9	54.4
60	44.6	53.8
50	45.3	53.2
40	46.1	52.6
30	46.8	52.0
20	47.5	51.4
10	48.3	50.8

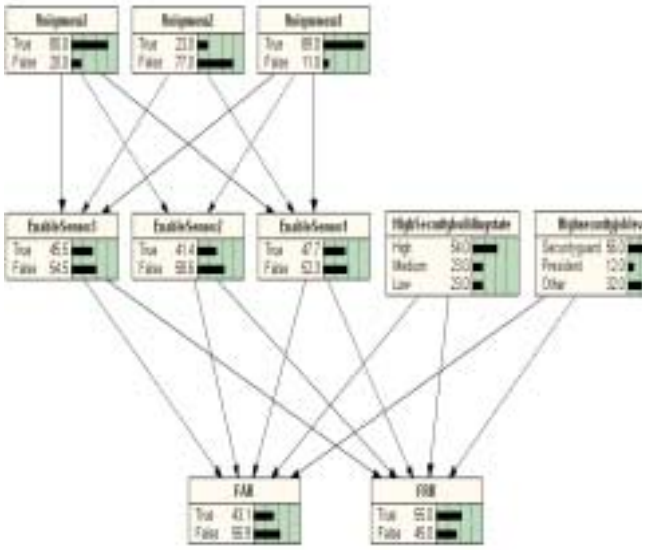

Fig. 5.BN for the sensor manager

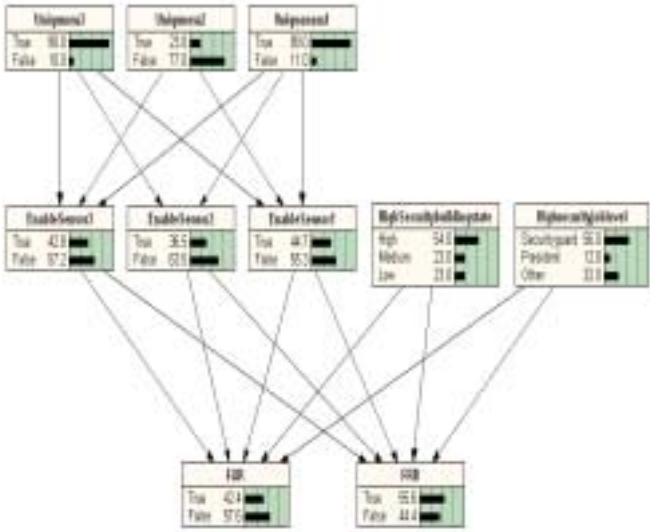

Fig. 6.BN for the sensor manager

TABLE II.

Uniqueness in 3 (%)	Uniqueness in 2 (%)	Uniqueness in 2 (%)	FAR (%)	FRR(%)
20	10	15	51.7	48.3
90	85	95	42.6	55.7

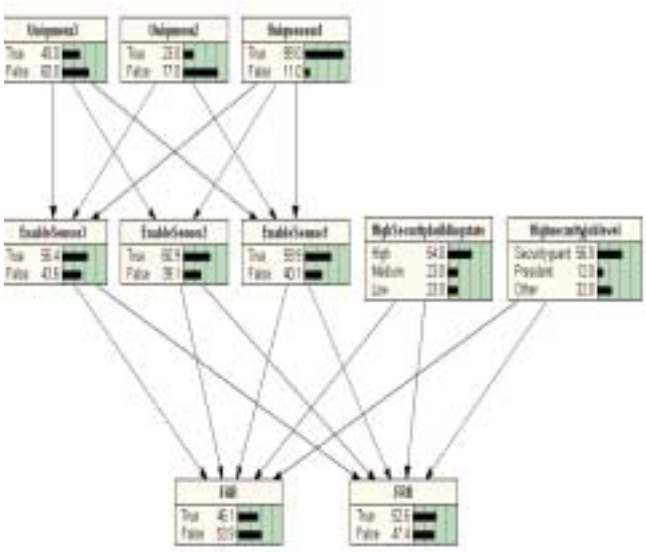

Fig. 7.BN for the sensor manager

3. Conclusion

In this study, an extended BN algorithm is designed to solve sensor management problem of building security. Different confidence values were presented for this sensor management problem demonstrating the possibilities of this approach. Depending on the changing state of the world such as, the security level and job title, BN updates the error cost and sent it to Fusion center to make the correct decision. Every time the situation changes, BN updates the system.

This paper illustrates how easily the extended BN can be applied to the general sensor management problem. The graphical nature of the influence diagram assists the system designer. The utility function can reflect the design parameters used by the system designer. Utility is so closely coupled to the resulting decisions that the utility and decisions must be designed together. The extended BN helps systems make more accurate decisions concerning the operating parameters. The advantages of automation and learning also follow an extended BN implementation.

IV. References

1 G. A. McIntyre, “Comprehensive Approach to Sensor Management, Part I: A Survey of Modern Sensor Management Systems”, *IEEE Transactions on SMC*, April 1999

2. G. A. McIntyre, “A Comprehensive Approach to Sensor Management and Scheduling”, Ph.D. Dissertation, Fall 1998, George Mason University, Fairfax, VA.

3.V. Denton, E. I. Alcaraz, J. Llinas, and K. J. Hintz, “Towards Modern Sensor Management Systems,” Chapter 13 in *Science of Command and Control: Part III Coping With Change*, AFCEA International Press: Fairfax, VA, 118-134, 1994.

4. L. Rothman and S. Bier, "Evaluation of Sensor Management Systems," *Proceedings of the IEEE 1989 National Aerospace and Electronics Conference*, NAECON 1989, 4, IEEE: New York, NY, 1747-1752, 1989.

5. S. Music and R. Malhotra , “Chasing The Elusive Sensor Manager”, *Proceedings of IEEE 1994 National Aerospace and electronics Conference*”, NAECON, Dayton, OH, 606-613, 1994.

6. D. M. Buede and E. L. Waltz, “Issues in Sensor Management”, *Proceedings. 5th IEEE International Symposium on Intelligent Control*, vol. 2, Philadelphia, PA, September 5-7 1990, pp. 839-842

7.T. A. Brownell, “Neural Networks for Sensor Management and Diagnostics,” *Proceedings of the IEEE 1994 National Aerospace and Electronics Conference, NAECON 1992*, vol. 3, Dayton, OH, May 18-22 1992, pp. 923-929.

8.Jenssen, F. , “ An Introduction to Bayesian Networks”. New York, Springer, 1996

9.Finn V Jensen, “Bayesian Networks and decision Graphs”, Springer, 2001

10.Lisa Ann Osadciw, Pramod K Varshney, Kalyan Veeramachaneni, “Improving Personal Identification Accuracy Using Multisensor Fusion for Building Access Control Applications”, *International Conefernce on Information Fusion*, July 7 -11, 2002, Annapolis, Maryland

11.Ramanarayanan Viswanathan and Pramod K. Varshney, “Distributed Detection With Multiple Sensors: Part I - Fundamentals”, *Proceedings of the IEEE*, Vol. 85, No. 1, Jan., 1997, pp. 54 - 63

12. J.Pearl, “Probabilistic Reasoning in Intelligent Systems*:* Networks of Plausible Inference”, Morgan Kaufmann, 1988.