Robustness Analysis at the Technical Level of Situation Assessment*

Xuezhi Wang
xu.wang@ee.mu.oz.au

Gavin Thoms
gavin@cybernetics-international.com

Center for Sensor Signal and Information Processing (CSSIP),
Dept. Electrical & Electronic Engineering, University of Melbourne, Vic. 3010, Australia

Abstract – *In a typical air defence scenario, the probability of threat posed to an asset by an intruder can be calculated using tactical data received from a Tracking and Data Fusion unit [1]. However, the outcomes of the calculation can be considerably influenced by the accuracy of the input data and the system disturbance. In this paper, the robustness analysis of a situation assessment system built upon a Bayesian network is presented. The problem under consideration has two aspects: 1) Determine the maximum allowable data disturbance; 2) Establish a probabilistic procedure to estimate the input data accuracy online. An example of data accuracy estimation for demonstrating the effectiveness of our approach is presented.*

Keywords: Threat probability, Robustness analysis, Data quality assessment, situation assessment.

1 Introduction

Situation assessment is a critical component of many complex sensor systems, an example of which is a sensor network management system for air defence. A sensor control system is shown schematically in Figure 1, where each box

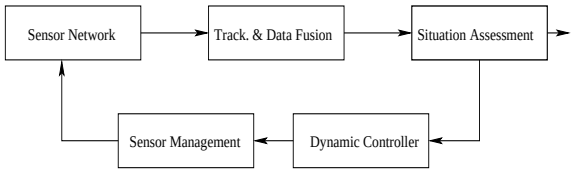

Fig. 1: Closed dynamic control system for sensor management.

represents a specific function in the system. The situation assessment function here is used to provide a measure of data quality and its output is fed into a controller which controls the operational behavior of the sensor network. This process results in the optimization of the output data quality of the tracking and data association (TDF) unit.

In an earlier air defence application, SA provided a probabilistic measure of threat from intruders based on TDF data [1]. In this approach, SA is an evidence-based inferential process. The uncertain nature determines the SA taking probability measure for its output objects even though all its input quantities can be "almost sure".

*This work is supported by RLM Systems, Australia.

In [1], a specified Bayesian network framework was used to describe the SA function and thus provide the stochastic based solution [2, 3], where a Bayesian network causally maps both kinematic and attribute data of the intruders and the location of an asset to be protected into the probability space in terms of threat probability. That is, the conditional probability of threat posed on the mth asset, given all intruders' data $X = \{x \in \mathbb{R}_n, x_p \in \mathbb{R}_p\}$ and asset location $a_m \in \mathbb{R}_n$, can be expressed mathematically as

$$P(T_{a_m}|X, a_m) \triangleq f\,(x, a_m, x_p) :\in \Omega \qquad (1)$$

where T_{a_m} denotes the threat function from intruders as described in [1] and $P(\cdot)$ is a probability ($\Omega \in [0, 1]$). $x \in \mathbb{R}_n$ is the intruder's kinematic state and $x_p \in \mathbb{R}_p$ is the intruder's identity state (type, weapon envelop, etc.).

As a component of a stochastic control system (Figure 1), the behavior of the SA function (1) is of interest. In particular, for the given SA function in [1], it is desirable that we 1) determine the maximum allowable data disturbance; 2) establish a probabilistic procedure to estimate the input data accuracy online.

Our interests include robustness analysis of the model (1) developed in [1] and the related data quality assessment. The former is about the SA output behavior with respect to the input data fluctuation, while the later ranks kinematic data quality/accuracy according to the random nature of the SA input.

In the next section, a quantitative study of the SA system relative error is presented. Subsequently, in Section 3, two approaches for online kinematic data quality classification are presented. An example of data quality assessment is then presented to demonstrate the merit of the proposed approaches. Finally, conclusions are drawn.

2 Relative Error Analysis

The objective of an air defence system is to protect a set of prioritized, high value assets. In Figure 2, appearance of an intruder implies a potential threat to each asset within the area of responsibility. The intruder t_i may effect its threat against asset a_m via any one of numerous paths. To obtain a single valued expression, the threat probability (1) implemented in [1] adopts a "worst case" approach in that

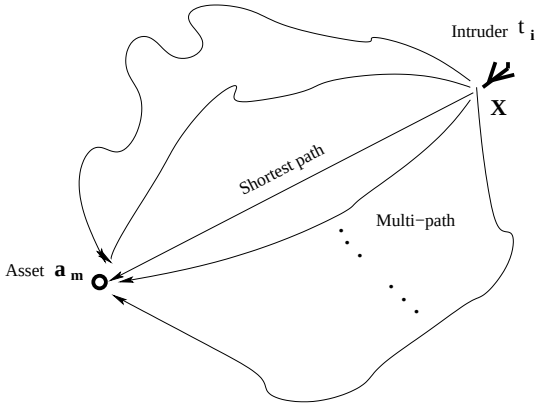

Fig. 2: Multiple value of a threat function Multiple routine attack

it is conditioned on the intruder's "shortest path ". Using such model, and assuming that all assets have equal priority, one may create a map of threat probability as a function of intruders' kinematic states across the entire surveillance region of responsibility. Figure 3 is an example of the threat probability distribution based on two intruders, where the intruders' states are assumed to be known exactly. However, if the data (of the intruder's kinematic

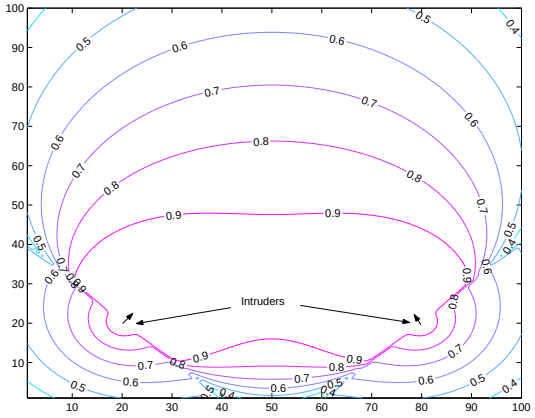

Fig. 3: Map of threat probability distribution (Surveillance region: $100 \times 100\ km^2$).

states) was corrupted by a Gaussian disturbance, the result (Figure 4) could differ significantly from that in Figure 3.

The input to the SA is typically the track data (X) from TDF output. In this paper, we will restrict the robustness analysis to the kinematic data input only.

A track from a TDF unit is often approximated as a Gaussian distributed PDF and thus is represented by a mean and its covariance. The input term may be represented by a fixed quantity x_k plus a disturbance $\triangle x_k$ as shown in Figure 5, where $\triangle x_k = \hat{x}_{k|k} - x_k$ and $\triangle P = \hat{P} - P$ are defined as track error and probability offset respectively. $\hat{x}_{k|k}$ is the track from TDF output and $\hat{P}$ is the SA output produced using $\hat{x}_{k|k}$. The object of the robustness analysis in this case is to quantify the variation of the SA output $\hat{P}$ with respect to the input $\hat{x}_{k|k}$. Furthermore, we seek an upper bound of the variation for the input such that the variation of the SA output is within a specified level. Many

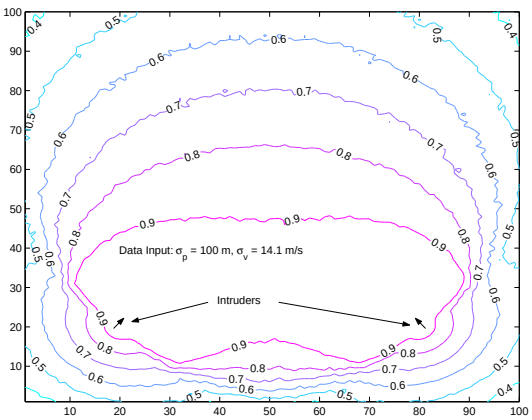

Fig. 4: Map of threat probability distribution in the presence of Gaussian disturbance (Surveillance region: $100 \times 100\ km^2$).

Fig. 5: SA model with disturbed data input.

analysis methods can be found in the system and control literature, for example [4, 5]. Since it is difficult to get the closed derivative expression of (1), we numerically evaluate its relative error via the Monte Carlo method.

We assume that the kinematic state of the intruder is known and the fluctuation term $\triangle x_k$ is a zero mean Gaussian random vector with variance Σ, i.e.,

$$\triangle x_k \quad \sim \quad \mathcal{N}(\ 0,\ \Sigma\ ) \tag{2}$$

where

$$\Sigma = \begin{bmatrix} \frac{\sigma_p^2}{2} & 0 & 0 & 0 \\ 0 & \frac{\sigma_v^2}{2} & 0 & 0 \\ 0 & 0 & \frac{\sigma_p^2}{2} & 0 \\ 0 & 0 & 0 & \frac{\sigma_v^2}{2} \end{bmatrix}$$

σ_p and σ_v denote the standard deviations of the intruder's position and velocity components respectively. The output measures considered in this experiment are the averaged error $\triangle \bar{P}$ and the relative error $(\triangle \bar{P}/P)\%$ of the threat probability respectively. Figures 6 and 7 illustrate the numerical statistics of the relative error $(\triangle \bar{P}/P)\%$ with respect to the uncertainties of the intruder's position data and velocity data respectively. All these results are averaged over 1000 runs.

Observations:

1. An input data error bound (or maximum allowable disturbance) can be identified from Figures 6 and 7. Thus, if input data error exceeds its error bound, the output relative error will grow exponentially fast.

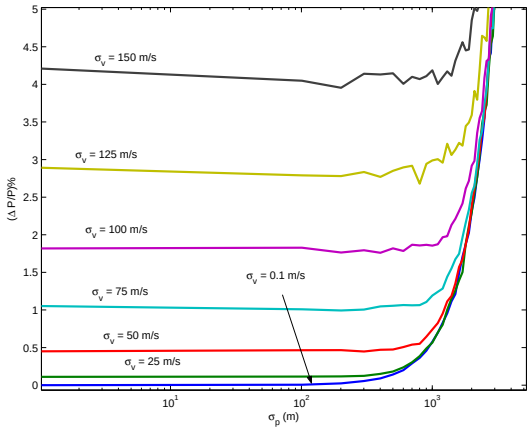

Fig. 6: Relative output error vs. (input) standard deviation of intruder's velocity.

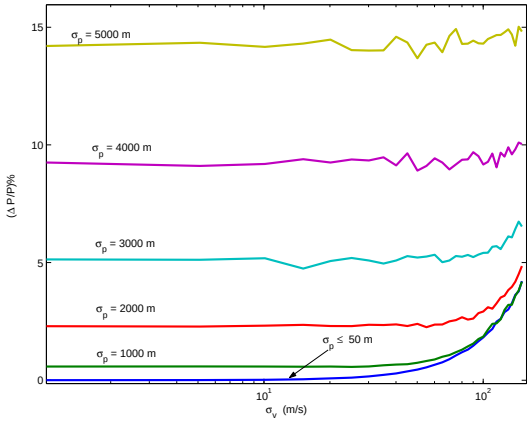

Fig. 7: Relative output error vs. (input) standard deviation of intruder's position.

2. The system will have a relative output error less than 5% if a data accuracy level $\sigma_p \leq 3000m$ and $\sigma_v \leq 150m/s$ can be maintained. This data accuracy requirement satisfies most of practical multisensor fusion surveillance network such as the Tactical Digital Information Links.

3 Data Quality Assessment

The relative error analysis performed in the last section confirms that for any feasible SA system like the one in [1] the quality of input data has a direct impact on the output of the SA. Assurance of inferential quality requires that we are able to perform estimation of data quality online. Data quality assessment is the process of classifying data according to a finite set of accuracy levels in a SA system. Two methods are available for data quality assessment. One is *knowledge-based data quality classification*, which is a probabilistic approach based on a priori data quality information. The other method is *virtual region based data quality classification*, which is based on online information alone. Both methods are derived within Bayesian frameworks.

3.1 Knowledge-based data quality classification

As shown in Figure 8, we assume that the underlying surveillance region covered by a sensor suite can be divided into a set of n sub-regions $\{A_1, A_2, \cdots, A_n\}$ such that the input data obtained through each of those sub-regions will possess an accuracy level $L_i, i = 1, 2, \cdots, n$, where n is a finite integer. Thus, when an intruder is inside the surveillance region means that 1) the intruder is in one of the sub-regions $A_i, i = 1, 2, \cdots, n$; 2) the track of this intruder from the TDF output is of at least accuracy level L_i. An example for data accuracy level specification corresponding to Figure 8 is given in Table 1.

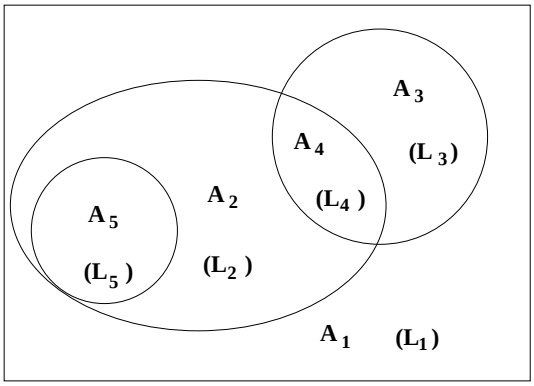

Fig. 8: Sub-regions of a sensor coverage area

Table 1: Data Accuracy Specification

Sub-region	Accuracy Level	Specification
A_1	L_1	< 5000 m
A_2	L_2	< 500 m
A_3	L_3	< 150 m
A_4	L_4	< 50 m
A_5	L_5	< 10 m

We have adopted on approach that is similar to that used for modelling uncertainties in the electronic support measures (ESM) [6]. The following models for data accuracy level classification process are proposed:

1. Modelling sensor network operational uncertainties.

   This uncertainty arises from the underlying data accuracy of the sub-region from which the data was acquired and is known in advance. In other words, the data accuracy level is probabilistically distributed within the surveillance region. A table (or matrix) of data accuracy level probability distribution can be pre-defined based on prior knowledge, which describes the probability of the received data accuracy given the sub-region from which the data originates, e.g., $P(L_i|A_j),\ i, j \in \{1, 2, \cdots, n\}$. An example of such a table for Figure 8 is presented in Table 2.

   A probability distribution of data accuracy in the form of a table or matrix may be estimated initially from a

Table 2: Data Accuracy Level Probability Distribution

Observed Sub-region	Data accuracy level probabilities				
	L_1	L_2	L_3	L_4	L_5
A_1	0.8	0.05	0.05	0.05	0.05
A_2	0.05	0.8	0.01	0.07	0.07
A_3	0.1	0.01	0.8	0.09	0
A_4	0.01	0.09	0.1	0.8	0
A_5	0.02	0.18	0	0	0.8

priori information and subsequently may be updated in real-time from cumulative outputs of the sensor communication network (Subsection 3.2). The matrix then provides a metric that may be used for real-time adaptation of the sensor network that should ensure optimal performance. Real-time adaptation may include scheduling of communication links, and scheduling of sensor focus and characteristics.

2. Modelling data geometric uncertainties.

   The data geometric uncertainties arise because 1) the underlying intruder is a moving object that may be passing over a sub-region boundary; 2) the boundary of those sub-regions cannot be exactly defined. Thus it is necessary to model the transitions between a finite number of sub-regions probabilistically. We model this transition process as a finite Markov chain process that is governed by a transition probability matrix Π. Its (i,j)th entry $\pi_{ij} = P(L_i|L_j)$ describes the probability that the current data accuracy level is of L_i given previous data accuracy level was of L_j. An example of transition probability matrix for Figure 8 is presented in Table 3.

Table 3: Data Accuracy Transition Probability Matrix

	L_1	L_2	L_3	L_4	L_5
L_1	0.8	0.09	0.09	0.01	0.01
L_2	0.05	0.8	0.05	0.05	0.05
L_3	0.12	0.01	0.8	0.07	0
L_4	0.01	0.1	0.09	0.8	0
L_5	0.01	0.19	0	0	0.8

Let H_k^i signifies the data accuracy event at time k. H_k is of accuracy level L_i, i.e., $H_k^i \Rightarrow H_k = L_i$ and $\hat{x}_k$ and $\hat{x}^k$ signify the track (kinematic data) and the track sequence $\{\hat{x}_1, \hat{x}_2, \cdots, \hat{x}_k\}$ respectively. We want to recursively compute the probability that the data is of accuracy level L_i at time k based on the all data $\hat{x}^k$, i.e., $P(H_k^i|\hat{x}^k)$. Using Bayes' rule, we have

$$P(H_k^i|\hat{x}^k) = \frac{P(\hat{x}_k|H_k^i,\hat{x}^{k-1})P(H_k^i|\hat{x}^{k-1})}{\sum_{j=1}^n P(\hat{x}_k|H_k^j,\hat{x}^{k-1})P(H_k^j|\hat{x}^{k-1})} \quad (3)$$

where $P(\hat{x}_k|H_k^i,\hat{x}^{k-1})$ is the likelihood function which is measurable from track kinematic data according to the underlying definition. In particular, if the kinematic data indicates that the intruder is in the sub-region A_j, we have

$$\begin{aligned} P(\hat{x}_k|H_k^i,\hat{x}^{k-1}) &\equiv P(\hat{x}_k \in A_j|H_k = L_i,\hat{x}^{k-1}) \\ &\equiv P(A_j|L_i) \end{aligned} \quad (4)$$

The value of $P(A_j|L_i)$ can be found in the pre-defined data accuracy level probability distribution table, e.g., Table 2. It turns out that for the example illustrated in Figure 8, the "measurement space" for computing (3) is the set of indexes of all sub-regions $\{A_1, A_2, \cdots, A_n\}$. The predicted data accuracy level probability $P(H_k^i|\hat{x}^{k-1})$ in (3) can be further derived (using total probability theorem) as

$$P(H_k^i|\hat{x}^{k-1}) = \sum_{j=1}^n P(H_k^i|H_{k-1}^j)P(H_{k-1}^j|\hat{x}^{k-1}) \quad (5)$$

where

$$P(H_k^i|H_{k-1}^j) \equiv P(H_k = L_i|H_{k-1} = L_j) = P(L_i|L_j)$$

is the transition probability defined by the Markov chain transition probability matrix Π, e.g., Table 3. The term $P(H_{k-1}^j|\hat{x}^{k-1})$ is the prior probability of data accuracy and is available from previous recursion.
Knowledge-based data quality classification has the advantages of being simple to implement and has a stable result when one is confident about the prior knowledge. Its main shortcoming is that it does not use online data to quantify data uncertainties and thus the result cannot reflect the variation of the uncertainties within a sub-region.

3.2 Virtual region based data quality classification

The virtual region approach uses only online information to assess data quality. The key is to partition the continuous uncertainty measure space into a finite set of n sub-regions. In each of these sub-regions, values taken by the uncertainty measure determine the data accuracy level. Denoted as $\{B_i\}_{i=1}^n$ the set of partitioned sub-regions corresponds to a set of n data accuracy levels $\{L_i\}_{i=1}^n$. Similar to the knowledge-based data quality classification, one can define a data accuracy level probability distribution table so that for any value taken by the uncertainty measure that corresponds to sub-region B_j, one can find a value of likelihood function conditioning on a data accuracy level L_i, i.e., $P(B_i|L_j)$.

$$\begin{aligned} P(\hat{x}_k|H_k^i,\hat{x}^{k-1}) &\equiv P(\hat{x}_k \in B_j|H_k = L_i,\hat{x}^{k-1}) \\ &\equiv P(B_j|L_i) \end{aligned} \quad (6)$$

We then use a Markov chain model to characterize the uncertainties that arise due to the data quality varying with time and the associated transition probability matrix can be designed in advance. Since all sub-regions are partitioned (non-overlapped and jointed), any uncertainties in a sub-region can only affect the adjacent sub-regions on both

Table 4: Data Accuracy Level Probability Distribution

Observed Sub-region	Data accuracy level probabilities				
	L_1	L_2	L_3	L_4	L_5
B_1	0.8	0.05	0.05	0.05	0.05
B_2	0.05	0.8	0.01	0.07	0.07
B_3	0.1	0.01	0.8	0.09	0
B_4	0.01	0.09	0.1	0.8	0
B_5	0.02	0.18	0	0	0.8

sides of this sub-region. Consequently, both data accuracy level probability distribution table and transition probability matrix will have the following structure

$$\begin{bmatrix} \pi_{11} & \pi_{12} & 0 & \cdots & \cdots & 0 \\ \pi_{21} & \pi_{22} & \pi_{23} & 0 & \cdots & 0 \\ 0 & \pi_{32} & \pi_{33} & \pi_{34} & 0 & \vdots \\ \vdots & \cdots & \pi_{(i,i-1} & \pi_{ii} & \pi_{i,i+1} & \vdots \\ \vdots & \cdots & \cdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & \pi_{n,n-1} & \pi_{nn} \end{bmatrix}$$

Therefore, we can straightforwardly compute the probability that data is of accuracy level L_i at time k using (3).

Remarks:

1. Since sub-regions in this approach are not related to the specified geometric area, they are called virtual sub-regions.
2. In SA environment, data is the output of the TDF unit. Under Gaussian assumptions, the covariance of the track can be used as the data uncertainty measure.
3. In our experience, the threat probability (the output of the SA) is more sensitive to the fluctuation of the intruder's velocity for the SA system implemented in [1]. Therefore, we take the standard deviation of the velocity component as the data uncertainty measure for data quality assessment.

4 Example of Online Data Quality Assessment

In reality, the accuracy of the track output from a TDF unit will vary with the intruder's geometric location since data handovers from sensor to sensor (with different accuracies) in a sensor network are always involved. Hence estimation of data accuracy in real-time and justification of outcomes of the SA system is essential. An example follows.

A target is observed via three sensors $S_i,\ i = 1, 2, 3$ with position accuracy levels L_4, L_3 and L_2 respectively (see Table 1). In the total 90 scans of target position measurements received by the fusion center, S_1 provided measurements from first 30 scans, S_2 the next 30 scans and S_3 the last 30 scans. The fusion center produces an estimate of the target state using a Kalman filter (KF) based on the noisy sensor measurement sequence and outputs the estimated target state (position & velocity) to a SA system at each scan. We assume that all sensors produce position only measurements with Gaussian zeros mean observation noise as shown in Figure 9. The Root

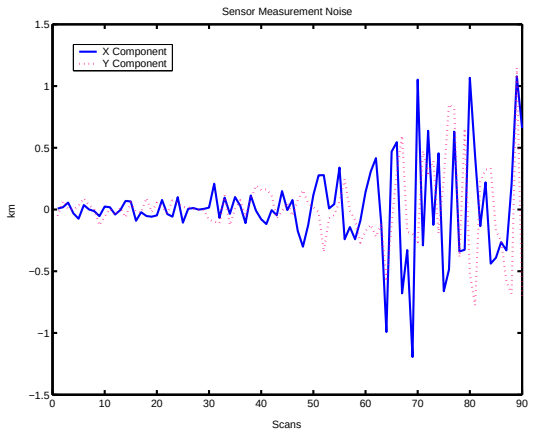

Fig. 9: Noise of sensor measurements

Mean Square (RMS) errors of the KF output are plotted in Figure 10. The figure confirms that the estimation errors are increased as sensor error increases. A virtual region

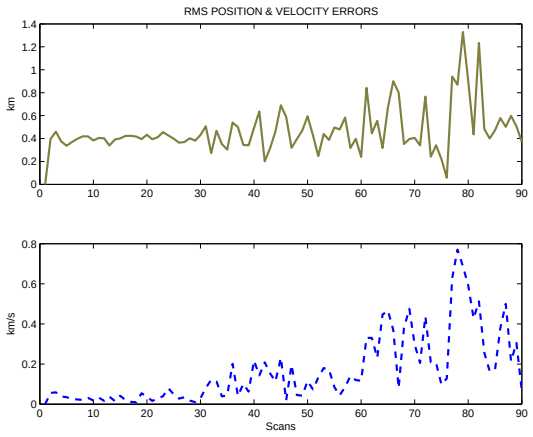

Fig. 10: RMS errors of the KF output

based data quality classifier described in previous section was used to estimate the data accuracy within 5 states of levels which are listed in Table 5. The matrix of the data

Table 5: Accuracy Level Specification in the Example

Accuracy Level	Specification
L_1	1000 m or above
L_2	$500 \sim 1000$ m
L_3	$50 \sim 500$ m
L_4	$1 \sim 50$ m
L_5	$0.1 \sim 1$ m

accuracy level probability distribution and the Markov

transition probability matrix used in our example are given in Tables 3 and 4 respectively. Figure 11 is the result of the estimated data accuracy level probabilities. Note that,

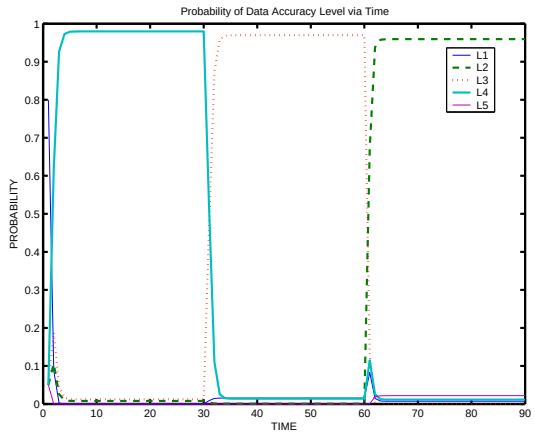

Fig. 11: Estimated data accuracy level probabilities

Figure 11 provides an accurate result since we assume that the errors of those sensors who provide intruder's position measurements are known exactly and thus the accuracy states are matched with sensor error levels.

5 Conclusion

In this paper, the robustness analysis of a situation assessment system built upon a Bayesian network is presented. The problem under consideration has two aspects: 1) Determine the maximum allowable data disturbance; 2) Establish a probabilistic procedure to estimate input data accuracy online. An example of data accuracy estimation for demonstrating the effectiveness of our approach is presented.
Attributes of sensor networks and real-time sensor data may be fused to provide a probability distribution (matrix) of network robustness.
Further research in the robustness analysis of the SA system is under consideration and the virtual region based data quality classification is recommended for building real-time implementable data quality indicators.

References

[1] G. A. Thoms, D. Musicki, N. Okello, X. Wang, T. Pham, R. Evans and I. Mareels. "Situation Awareness Using Bayesian Networks – Phase 2", in *Technical report to the center of sensor signal, information processing* , CSSIP CR 16/03, Melbourne, Australia, Jan. 2003.

[2] F. V. Jensen. *Bayesian networks and decision graphs*, Springer-Verlag, New York, 2001.

[3] N. Okello and G. A. Thoms. "Threat Assessment Using Bayesian Networks", in *Proceedings of the 6th International Conference on Information Fusion*, Cairns, Queensland, Australia, July, 2003, pp. 1102–1109. .

[4] J. Doyle, M, Newlin, F. Paganini, and J. Tierno. "Unifying robustness analysis and system ID ", *Proceedings of the 33rd IEEE Conference on Decision and Control*, vol. 4, pp. 3667–3672, Dec. 1994.

[5] X. Zhu, Y. Huang and J. Doyle. "Soft vs. hard bounds in probabilistic robustness analysis ", *Decision and Control, 1996., Proceedings of the 35th IEEE* , vol. 3 , pp. 3412–3417, 11-13 Dec. 1996. .

[6] X. Wang, S. Challa, and G. W. Pulford. "Target Tracking and Classification Using Radar and ESM Sensors", *Proc. of 8th International Aerospace Congress*, Adelaide, Australia, March 1999.