Fault Tolerance from Formal Analysis of a Data Fusion Mechanism

Kaci Bader, Benjamin Lussier, Walter Schön

Fault Tolerance from Formal Analysis of a Data Fusion Mechanism

BADER Kaci, LUSSIER Benjamin, SCHÖN Walter
Sorbonne Universités, Université de Technologie de Compiègne,
CNRS, UMR 7253, Heudiasyc CS 60 319, 60203 Compiègne, France
Email: {kaci.bader, benjamin.lussier, walter.schon}@hds.utc.fr

***Abstract*— Multi-sensor perception systems are starting to be used in critical applications, such as in drones and ADAS (Advanced Driver Assistance Systems). However, complete validation of complex perception systems is difficult to achieve. In this paper we examine these systems through the lens of an alternative dependability method, namely fault tolerance. We apply a formal analysis on a belief function data fusion mechanism to provide fault tolerance. By analyzing certain parameters related to the data fusion process, we show that it is possible to offer fault tolerance services suitable for multi-sensor perception systems, including detection, recovery, and fault masking.**

I. Introduction

Perception is a fundamental input in any robotic system. However, data perceived by robotic systems are often complex and subject to significant uncertainties and inaccuracies. Multi-sensor approaches seek to address this problem. In multi-sensor approaches data are acquired from multiple, complementary sensors, and redundancy between these sensors is used to increase the precision of perception. But the greater the number of sensors and underlying data fusion algorithms, the greater the likelihood of hardware and software faults occurring. Moreover, the open environments in which complex robotic systems operate can create a near-infinite execution context, which means that validating a multi-sensor approach might, for example, require thousands of hours' driving on roads, with no certainty that every possible situation has been encountered. Testing is therefore a lengthy, difficult, and costly operation. One alternative to this kind of exhaustive validation is to develop fault-tolerant mechanisms. Since it is difficult to remove all the faults in a system, the idea is instead to limit the impact of these faults on the system's operation. In this paper we show, via a simple theoretical case study, how fault-tolerant services may be derived from the formal analysis of data fusion parameters.

The paper is organized as follows: after this introduction, section II summarizes related works. Section III describes the architecture that we propose. Section IV presents our study and details the proposed fault tolerance services. The paper ends with prospects for future works.

II. Fault tolerance in data fusion: related works

To our knowledge, there have been few studies on fault tolerance in data fusion. The approaches we found in the literature mostly use the analysis of some internal parameters to provide fault tolerance. In [7] the authors discussed the detection of malfunctions through the temporal analysis of the conflict resulting from the fusion of data sources, based on Smets's TBM [9]. They suggested that once it is recognized that a source is defective, the influence of that source on the final decision should be weakened. In [4], an algorithm was proposed for detecting a defective source by analyzing the reliability of all the sources. This reliability serves as a discounting factor to weight belief masses given by the sources before they are combined. Where the conflict is due to a defective source, the authors analyzed the discounting factor to detect the erroneous source using a thresholding method. In [3] a similar approach was proposed by the same authors in the specific context of possibility theory.

Although these papers present effective solutions, it will be remarked that they focus only on hardware fault tolerance. Moreover, they detect and tolerate faults occurring in physical sensors providing input into data fusion processes that are difficult to design and validate, and that consequently may be considered untrustworthy for critical applications. It is our belief that fault tolerance in data fusion necessarily involves either trying to tolerate software faults in the data fusion process, or using formal methods to guarantee that the data fusion process is sound.

III. Fault tolerance through data fusion: proposed architecture

Our goal in this qualitative study is to analyze certain parameters from data fusion algorithms (Figure 1) to ensure fault tolerance services. Our architecture consists of two identical branches, each comprising two sensors and a fusion mechanism between those two sensors. In addition, there is a global fusion algorithm to merge the outputs of the two fusion mechanisms.

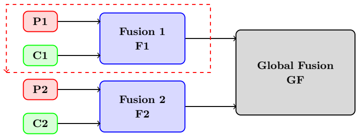

Fig. 1. Data Fusion Architecture

IV. Examination of the problem, proposed fault tolerance services

Our approach consists in formally analyzing the behavior of a data fusion mechanism based on belief function theory.

We illustrate this approach with an example application taken from [6], where it was proposed as part of a habitat perception architecture for communicating with and assisting elderly persons at home. The application detects whether or not someone is sitting on a chair. Two sensors are used: a pressure sensor (P) placed under the seat of the chair, and a camera (C) installed in front of the chair to detect a seated figure. In this case study, the sensors output 1 when there is someone on the chair, and 0 otherwise. Our analysis is separated into two parts: first we look at a simple case involving a single branch of the proposed architecture (the upper branch in Figure 1), then we study the complete architecture.

A. One branch case

Our data fusion mechanism is based on belief function theory [5][8]. In this section IV-A we look at a single set of sensors (camera, pressure) belonging to a single branch (P_1,C_1,F_1) of our architecture, as depicted in Figure 1.

1) Modeling:

- **Frame of discernment** Given the binary state assumption, the frame of discernment consists of the binary hypotheses that either one person is sitting on the chair ($\exists$), or that no-one is sitting on the chair ($\nexists$): $\Omega = \{\exists, \nexists\}$. From this Ω, we deduce the powerset 2^{Ω}: $2^{\Omega} = \{\{\exists\}, \{\nexists\}, \{\exists, \nexists\}, \emptyset\}$.
- **Assigning belief masses** Considering $p_i(\exists)$ the sensor output, we have:

$$\begin{cases} p_i(\exists) = 1 \text{ if someone is sitting on a chair} \\ p_i(\exists) = 0 \text{ otherwise} \end{cases} \quad (1)$$

  Each sensor i has a corresponding weakening factor $p^i_{trust} \in [0,1]$ that in our model represents reliability of the sensor. The masses assigned to the two hypotheses $\exists$ and $\nexists$ are the sensor outputs $p_i(\exists)$ weighted by this weakening factor p^i_{trust}, as defined in (2).

$$\begin{cases} m_i(\{\exists\}) = p^i_{trust} . p_i(\exists) \\ m_i(\{\nexists\}) = p^i_{trust} . [1 - p_i(\exists)] \end{cases} \quad (2)$$

  The masses $m_i(\{\exists\})$, $m_i(\{\nexists\})$ being defined, the remaining mass is assigned to Ω, which models the ignorance (3).

$$m_i(\{\exists, \nexists\}) = 1 - [m_i(\{\exists\}) + m_i(\{\nexists\})] \quad (3)$$

- **Combining belief masses** We combine the masses obtained from sensors P and C using the Dempster rule, as described in (4), to obtain the global belief on elements of 2^{Ω}:

$$\begin{cases} K = m_P(\{\exists\}) m_C(\{\nexists\}) + m_P(\{\nexists\}) m_C(\{\exists\}), \ \text{K: Conflict factor} \\ m_{P \oplus C}(\{\exists\}) = \frac{m_P(\{\exists\}).m_C(\{\exists\}) + m_P(\{\exists\}).m_C(\{\exists,\nexists\}) + m_P(\{\exists,\nexists\}).m_C(\{\exists\})}{1-K} \\ m_{P \oplus C}(\{\nexists\}) = \frac{m_P(\{\nexists\}).m_C(\{\nexists\}) + m_P(\{\nexists\}).m_C(\{\exists,\nexists\}) + m_P(\{\exists,\nexists\}).m_C(\{\nexists\})}{1-K} \\ m_{P \oplus C}(\Omega) = 1 - [m_{P \oplus C}(\{\exists\}) + m_{P \oplus C}(\{\nexists\})] \end{cases} \quad (4)$$

  Note that the conflict factor K is 0 when the two sensors are in agreement.
- **Decision** is based on the pignistic probability [10], obtained in this case by equi-distributing the mass of ignorance (Ω) over the two hypotheses $\exists$, $\nexists$. After calculating this probability, the decision is made according to a threshold value, strictly greater than 0.5: If $BetP(\exists) \geq th$, then we decide that there is a person on the chair. If $BetP(\exists) \leq 1$ - th, then we decide that no-one is sitting on the chair.

2) Principle of detection: This work examines the conditions that are required in this architecture's data fusion algorithm in order to formally guarantee an error detection service. In particular, we focus on three factors: the weakening factors p^P_{trust} and p^C_{trust}, and the decision threshold th. Under the single fault assumption, our principle of fault detection is as follows. Where both sensors have the same value, no error is present in the system and a decision is always reached. Where the two sensors have different values, there is an error and the system must not be able to decide either way. Consequently, when the system reaches at a decision, this means that no error is present, and when it fails to arrive at a decision, there is an error. To satisfy this principle, the following four conditions must hold.

1) In the absence of faults
   - **Condition 1:** Where someone really is sitting on the chair, we want the system always to decide that there is someone. This means that the two sensors (C, P) both output 1 if and only if the pignistic probability $BetP(\exists)$ is greater than or equal to the threshold decision.

$$\begin{cases} p_P(\exists) = 1 \\ p_C(\exists) = 1 \end{cases} \Leftrightarrow BetP(\exists) \geq th \quad (5)$$

   - **Condition 2:** Where no-one is sitting on the chair, we want the system always to decide that there is no-one. This means that the two sensors (C, P) output the same value 0 if and only if $BetP(\exists)$ is less than or equal to 1 - th.

$$\begin{cases} p_P(\exists) = 0 \\ p_C(\exists) = 0 \end{cases} \Leftrightarrow BetP(\exists) \leq 1 - th \quad (6)$$

2) In the presence of faults
   - **Condition 3:** Where there is someone on the chair and the two sensors give opposite results, we do not want the system to reach a decision. This means that when the sensors have opposite outputs and there is someone on the chair, the pignistic probability $BetP(\exists)$ is between 1 - th and th.

$$\begin{cases} p_P(\exists) = 1 \text{ and } p_C(\exists) = 0 \ \textit{with C failed} \\ \text{or} \\ p_P(\exists) = 0 \text{ and } p_C(\exists) = 1 \ \textit{with P failed} \end{cases} \Rightarrow 1 - th < BetP(\exists) < th \quad (7)$$

   - **Condition 4:** Where there is no-one on the chair and the two sensors give opposite results, we do not want the system to reach a decision. As in condition 3, we obtain:

$$\begin{cases} p_P(\exists) = 1 \text{ and } p_C(\exists) = 0 \ \textit{with P failed} \\ \text{or} \\ p_P(\exists) = 0 \text{ and } p_C(\exists) = 1 \ \textit{with C failed} \end{cases} \Rightarrow 1 - th < BetP(\exists) < th \quad (8)$$

3) Detection Service: For faults to be detected in the system, the four above conditions must be met simultaneously. In the following figures, we present the pignistic probability corresponding to the hypotheses $\exists$ and $\nexists$, depending on weakening factors p^P_{trust}, p^C_{trust}, to help us investigate the weakening factors meeting these four conditions. We first consider a threshold value of 0.8.

In Figure 2, the X axis represents the factor p^P_{trust} corresponding to the pressure sensor and the Y axis the factor p^C_{trust} assigned to the camera. The gray area represents the zone where the pignistic probability $BetP(\exists) \geq 0.8$ where both sensors are outputting 1 and thus meeting the first condition.

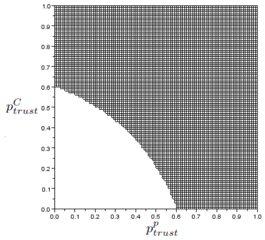

Fig. 2. Couples p^i_{trust} satisfying condition 1

Because of the symmetry of our problem, the couple (p^P_{trust}, p^C_{trust}) meeting condition 2 are identical to those in figure 2.

Figure 3 show the weakening factors (p^P_{trust}, p^C_{trust}) that meet the condition 3: the gray area of this figure is the zone where $0.2 < BetP(\exists) < 0.8$. It shows the situation where there is someone on the chair and the system does not reach a decision because the sensors are outputting different values. In this figure the white area on the upper left shows the area where the camera output decides the result of the fusion: the confidence accorded to the camera is such that its output determines the result of the fusion regardless of the pressure sensor output. Similarly, the area at the bottom right shows the area where the output of the pressure sensor alone decides the result of the fusion.

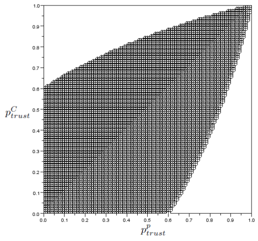

Fig. 3. Couples p^i_{trust} satisfying condition 3

As before, the symmetry of our problem means that the weakening factors (p^P_{trust}, p^C_{trust}) meeting the condition 4 are similar to those meeting condition 3, as shown in figure 3.

Finally, the couples (p^P_{trust}, p^C_{trust}) that detect an error for a threshold value of 0.8 are those that meet the four conditions above, and therefore the result of the intersection of the surfaces of figures 2, 3 shown in figure 4.

In the same way that we examined couples (p^P_{trust}, p^C_{trust}) for th = 0.8, we can consider other th values, and propose triplets (p^P_{trust}, p^C_{trust}, th) ensuring the detection service.

B. Complete Architecture

We saw in section IV-A how to ensure error detection with a single set of competitive sensors. To provide other services, such as system recovery or error masking, duplication of the hardware sensors is required. In the following section we study a complete data fusion architecture (Figure 1).

1) Modeling: In this architecture, the frame of discernment is the same as in the simple case, and the belief masses corresponding to the hypotheses are the results of both fusion blocks F_1 and F_2. These results are combined at the *global fusion block GF* using Demspter's rule as in equation 4, taking as input m_{F1} and m_{F2}.

2) Detection service: As in the simple case, we need to satisfy the four conditions above. For a threshold value of 0.8, Figure 5 shows the couples (p^P_{trust}, p^C_{trust}) that meet the first condition, that is the couples for which the system correctly decides that there is someone on the chair when all the sensors are outputting 1 and no sensors have failed.

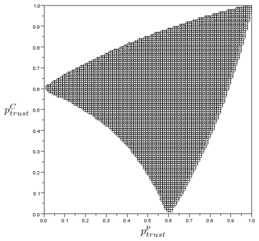

Fig. 4. Detection Service for th = 0.8

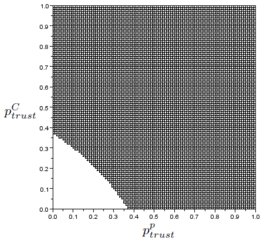

Fig. 5. Couples p^i_{trust} satisfying condition 1

Since the problems are similar, the couples (p^P_{trust}, p^C_{trust}) that meet the second condition are identical to those meeting the first condition, as shown in figure 5, but here we are interested in the couples for which the system correctly decides that there is no-one on the chair where all the sensors are outputting 0 and no sensors have failed.

Figure 6 shows the couples (p^P_{trust}, p^C_{trust}) that meet the third condition, that is to say the couples of weakening factors where the system is unable to decide that a person is present when exactly one camera has failed. The case where a pressure sensor is faulty gives a figure symmetrical to figure 6 with respect to the first bisector.

Finally, couples (p^P_{trust}, p^C_{trust}) meeting the fourth condition are the same as for the third condition, but in this case they represent the couples of weakening factors for which the system is unable to decide that a person is not present when exactly one sensor has failed. In figures 6, we remark that the white area represents the couples (p^P_{trust}, p^C_{trust}) where

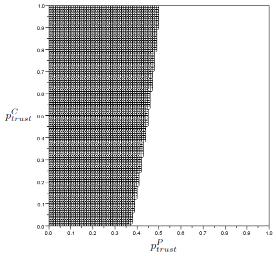

Fig. 6. Couples p^i_{trust} satisfying condition 3 with one failing camera

the system reaches the correct decision despite an error in one sensor. Here, however, we are seeking to detect the error rather than to reach the correct decision, and this area therefore excludes couples satisfying detection.

As in the simple case, for an error to be detected in the system the four conditions must be satisfied. The intersection of the figures shown in Figure 7 gives the couples (p^P_{trust}, p^C_{trust}) that ensure the detection service.

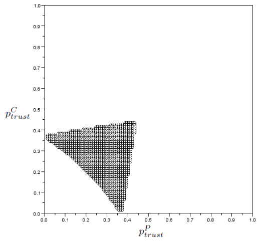

Fig. 7. Detection service for th = 0.8

3) Recovery service: The recovery service consists in using redundancy in the system to determine the correct result despite the presence of an error. To tolerate a hardware error, the complete architecture in Figure 1 must first detect the presence of an error, and then determine the correct output.

The detection is performed as before: we choose the parameters satisfying the error detection service in Figure 7. Once the error is detected, and under the assumption of a single error, we then find which branch (either F_1 or F_2) contains the defective sensor. When the two branches respect the criteria of error detection presented in section IV-A2, this is easy: the branch containing the defective sensor will not be able to decide, and the other branch will generate the correct output. The factors (p^P_{trust}, p^C_{trust}) ensuring the recovery service must therefore be able to detect an error in the complex case, and able to detect an error in the simple case. This corresponds to the intersection of figures 4 and 7, shown in Figure 8.

4) Masking service: The masking service consists in tolerating a hardware error without detection. In order to do so, two conditions have to be met: first, the system has the correct behavior where there is no error, which is equivalent to satisfying the first two conditions in Figure 5; second, the system delivers the correct result, despite there being a single error in one of the sensors. This corresponds to the couples (p^P_{trust}, p^C_{trust}) which complement the gray zone in figures 6.

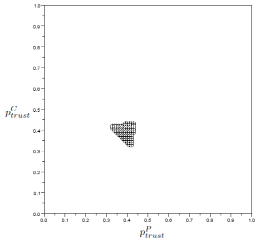

Fig. 8. Recovery service for th = 0.8

From these two constraints we find (p^P_{trust}, p^C_{trust}) for the fault masking presented in Figure 9.

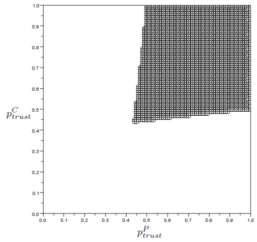

Fig. 9. Masking service for threshold 0.8

V. Conclusion and prospects

This paper presents a simple theoretical case study where data fusion mechanisms directly give rise to fault tolerance services. We have shown that from the analysis of a data fusion model and the careful choice of parameters it is possible to derive services of detection, recovery and fault masking.

In future work, we intend first to incorporate the results of this approach in a real application as in [1] and to explore other potential parameters such as combination operators. This kind of analysis is not always possible in complex cases, and where it is not possible, other complementary techniques (such as [1][2]) can be an alternative.

References

[1] Kaci Bader, Benjamin Lussier, and Walter Schön. A fault tolerant architecture for data fusion targeting hardware and software faults. In *The 20th IEEE, PRDC*, 2014.

[2] Kaci Bader, Benjamin Lussier, and Walter Schön. Functional diversification for software fault tolerance in data fusion: a real application on kalman filters for mobile robot yaw estimation. In *ESREL*, 2015.

[3] F. Delmotte. Detection of defective sources in the setting of possibility theory. *Fuzzy sets and systems*, 158(5):555–571, 2007.

[4] F. Delmotte and G. Gacquer. Detection of defective sources with belief functions. In *IPMU, Malaga*, pages 337–344, 2008.

[5] E. Lefevre, O. Colot, and P. Vannoorenberghe. Belief function combination and conflict management. *Inf Fusion*, 3(2):149–162, 2002.

[6] V. Ricquebourg, M. Delafosse, L. Delahoche, B. Marhic, AM Jolly, and D. Menga. Combinaison de sources de données pour la détection de dysfonctionnement capteur. LFA, 2007.

[7] V. Ricquebourg, M. Delafosse, L. Delahoche, B. Marhic, AM Jolly-Desodt, and D. Menga. Fault detection by combining redundant sensors: a conflict approach within the tbm framework. *COGIS*, 2007.

[8] K. Sentz and S. Ferson. *Combination of evidence in Dempster-Shafer theory*. Sandia National Laboratories SAND2002-0835, 2002.

[9] P. Smets. Data fusion in the transferable belief model. In *the 3rd Int Conf on Inf Fusion*, volume 1, pages PS21–PS33, 2000.

[10] P. Smets. Decision making in the tbm: the necessity of the pignistic transformation. *Int J Approx Reason*, 38(2):133–147, 2005.