Defining posterior hypotheses in C2 systems

Ksawery Krenc[*], **Adam Kawalec**[**]

[*] OBR CTM S.A.
Dickmana 62, 81-109 Gdynia, POLAND
email: ksawery.krenc@ctm.gdynia.pl

[**]WAT Military University of Technology
Kaliskiego 2, 00-908 Warsaw, POLAND
email: adam.kawalec@wat.edu.pl

Abstract: *This paper describes the results of numerical experiments devoted to examination of influence of the target attribute hypotheses definitions on quality of information fusion. The main goal of the research works presented herein was to find answers to the subsequent questions: 'In the context of attribute information fusion in C2 systems, is it reasonable to extend the information scope of a sensor?' and 'Does the extension of the sensor information scope always provide tangible benefits in quality of fusion?'. In order to achieve that there have been defined two measures: decision robustness and decision deviation.*

In the experimentation Dezert-Smarandache Theory has been used as the main fusion engine.

1. Introduction

One of the most important requirements imposed on maritime Command & Control (*C2*) systems is to elaborate the so called Common Operational Picture (*COP*). In order to achieve that, the *C2* systems must be equipped with specific information fusion techniques, which enable to integrate both precise information as well as uncertain, incomplete or even conflicting information.

When the information is vague, sophisticated reasoning processes are performed to elaborate the final optimal decision [9], [10], [3], [4]. In such a case it is very important to create hypotheses upon the gathered evidence as much adequate as possible. Some of them (primary hypotheses) result directly from the sensors' resolution and may be regarded as the basis for constructing the frame of discernment. Others (posterior hypotheses) are created upon the primary hypotheses with usage of logical relations.

The definition of the posterior hypotheses is very important and should be a subject of the serious considerations. Certainly, one can imagine the posterior hypotheses may be regarded as completely different classes. However, that implies two problems: The first problem is evaluation of these new hypotheses, based on observation data, which is necessary if these hypotheses are intended to be utilised effectively. The second problem is that the reasoning system, which performs the fusion of the gathered information, does not have a 'notion' of the meaning of these new hypotheses unless they are defined based on the hypotheses that already exist.

2. Posterior hypotheses

Consider the following case of the *target threat* information fusion. It is assumed that *DSm* [10], [11], [12] free model holds and Bayesian *bba* is defined as follows:

$m_1(F) = 0.2, m_1(H) = 0.8;$

$m_2(F) = 0.9, m_2(H) = 0.1;$

Figure 1 shows the Venn's related to this case.

According to [5], [6], [7], [8] [12] $F \cap H$ hypothesis describes a training target, called FAKER (F_K), comprehended as a type of FRIEND (F), acting as HOSTILE (H) for exercise purposes. That means the target possesses features of both friendly and hostile target.

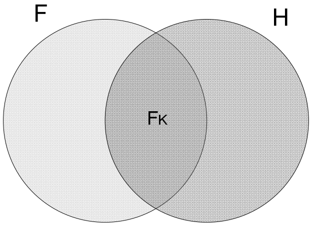

Figure 1 Venn's diagram for the Threat attribute

The corresponding evidence table has been presented at Table 1.

Table 1. Evidence table for two sensors discerning FRIEND and HOSTILE targets

m_2 \ m1	**F [0.2]**	**H [0.8]**
F [0.9]	F [0.18]	$F \cap H$ [0.72]
H [0.1]	$F \cap H$ [0.02]	H [0.08]

Application of the classical *DSm* rule of combination results in the following *bba*:

$m(F) = 0.18, m(H) = 0.08, m(F \cap H) = 0.74$

which in the consequence leads to subsequent values of belief functions:

$Bel(F) = m(F) + m(F \cap H) = 0.92$

$Bel(H) = m(H) + m(F \cap H) = 0.82$

$Bel(F \cap H) = m(F \cap H) = 0.74$

In that case the problem resides in the expression of $F \cap H$ which does not fully reflect the nature of FAKER. On one hand FAKER represents the target that encompasses the features of both targets: friendly and hostile. On the other hand it performs a specific type of FRIEND. Underlying the calculation of the belief functions is the assumption that FAKER supports both hypotheses: FRIEND and HOSTILE.

A simple correction of the calculation, by omitting the $F \cap H$ hypothesis support for HOSTILE, however incompatible with *DST* [9] and *DSmT*, may be regarded as a kind of instant solution. Thus:

$Bel(F) = m(F) + m(F \cap H) = 0.92$

$Bel(H) = m(H) = 0.08$

$Bel(F \cap H) = m(F \cap H) = 0.74$

Notice that this treatment may have some serious repercussions, since FAKER, with the biggest mass assigned in this case, is a posterior hypothesis, which means it has no direct support from the sensor data.

The described fusion case may be regarded as a follow-up of one of two possible events:

integration of information, originated from two sensors, which detect different features of the target or

integration of conflicting information, originated from two sensors one of which is reliable, and another is corrupted.

In the first event FAKER hypothesis seems to be highly appropriate. As a result of combination of evidence the biggest mass is assigned to it. Finally, due to the hypotheses hierarchy, according to which FAKER supports FRIEND, the corresponding belief function for a friendly target reaches the highest value. The lowest mass value is assigned to HOSTILE (0.08 after the correction).

In the second event the posterior hypothesis F$\cap$H, previously defined as FAKER should be regarded specifically. According to *DST* and *DSmT* the mass corresponding to that hypothesis is conflicting. Therefore omitting it in the belief function calculation may provide a serious corruption of the final decision, due to the fact the friendly target hypothesis would be fostered regularly.

For comparison, consider another target threat attribute fusion case, where every sensor provides additional information related to the training value (FAKER). That means the acquired *bba* is non-Bayesian. Similarly, as in the previous example, it has been assumed that *DSm* free model holds. The gathered evidence has been summarized with the following table:

Table 2. Evidence table for two sensors discerning FRIEND, HOSTILE and FAKER targets

m_2 \ m1	**F [0.2]**	**H [0.4]**	**F $\cap$ H [0.4]**
F [0.5]	F [0.1]	F $\cap$ H [0.2]	F $\cap$ H [0.2]
H [0.1]	F $\cap$ H [0.02]	H [0.04]	F $\cap$ H [0.04]
F $\cap$ H [0.4]	F $\cap$ H [0.08]	F $\cap$ H [0.16]	F $\cap$ H [0.16]

Application of the classical *DSm* rule of combination results in the following *bba*:

$m(F) = 0.1,\ m(H) = 0.04,\ m(F \cap H) = 0.86$

which in the consequence leads to subsequent values of belief functions:

$Bel(F) = m(F) + m(F \cap H) = 0.96$

$Bel(H) = m(H) + m(F \cap H) = 0.9$

$Bel(F \cap H) = m(F \cap H) = 0.86$

Applying the analogical correction as in the previous example leads to the following belief function values:

$Bel(F) = m(F) + m(F \cap H) = 0.96$

$Bel(H) = m(H) = 0.04$

$Bel(F \cap H) = m(F \cap H) = 0.86$

The fundamental difference between these two examples resides in the quantitative support for FAKER hypothesis. In the second case it is supported in three ways:

directly: when both sensors identify the target as FAKER (Table 2-2: the black-colored mass);

when only one sensor identifies the target as FAKER (Table 2-2: the green-colored mass);

indirectly: as a combination of FRIEND and HOSTILE hypotheses, similarly as in the first example (Table 2-2: the purple-colored mass);

This means that (in the second example) the risk of allocating the FAKER hypothesis inappropriately high mass value, while one of the sensors delivers false information, was significantly reduced.

Discerning these two cases underlies an alternative correction method, which may be regarded as less 'invasive'. Namely, in the second case it is possible to apply a decomposition of FAKER for particle hypotheses: SPECIFIC FAKER and CONFLICTING FAKER, as follows:

$$m(F_K) = m(F_{SK}) + m(F_{CK}) \qquad (1)$$

where:

$$m(F_{SK}) = m_1(F \cap H) \cdot m_2(F) + m_1(F \cap H) \cdot m_2(H) +$$
$$+\ m_1(F) \cdot m_2(F \cap H)\,) + m_1(H) \cdot m_2\,(F \cap H) +$$
$$+\ m_1(F \cap H) \cdot m_2\,(F \cap H) = 0.2 + 0.04 + 0.08 + +0.16 + 0.16 = 0.64$$

$$m(F_{CK}) = m_1(H) \cdot m_2(F) + m_1(F) \cdot m_2(H)$$
$$= 0.2 + 0.02 = 0.22$$

Such decomposition enables to calculate the belief function values as follows:

$Bel(F) = m(F) + m(F_{SK}) + m(F_{CK}) = 0.1 + 0.64 + 0.22 = 0.96$

$Bel(H) = m(H) + m(F_{CK})$= 0.04 + 0.22 = 0.26

$Bel(F_K) = m(F_{SK}) + m(F_{CK})$ = 0.86

The correction above enables to utilize the complete information that resides in the descriptive definition of FAKER, while maintaining compliance of the belief function calculation with *DST* and *DSmT*.

3. Need for experimentation

An introductory analysis of the posterior hypotheses definitions has proven that defining these hypotheses in such a way FAKER is decomposed for two components (i.e. specific and conflicting) seems to be very useful. Due to the fact it enables to assess the tactical situation reasonably, the resulting *bba* and the respective belief functions are much more reliable than before the decomposition takes place. That performs justification for numerical experiments, necessary for further analysis, and the full verification of this method for miscellaneous measurement and decision scenarios.

In the next sections, descriptions of the numerical experiments, the results of these experiments, and the conclusions will be presented.

During the experimentation, the *target threat* attribute was the only one taken into consideration, due to the fact its *information expansion* (i.e. ability to create multiple posterior hypotheses) is significantly higher.

4. Quality measures

Within the numerical examination work there have been realized:

- *Decision robustness* examination and
- Changeability of the belief functions.

The *decision robustness* performs a kind of decision stability margin. That is the degree, to which extent the decision is resistant to obstacles caused by both types of uncertainty (random and deterministic).

The decision robustness is based on the quantitative and qualitative analysis of the fusion cases, where slight modification of the input (sensor) data determines the decision change.

The *decision robustness* may be expressed as follows:

$$R_D = 1 - \frac{n_C}{N} \tag{2}$$

where:

n_C – the number of conflicting theses;

N – the number of possible theses (measurement scenarios).

Another measure, very useful while examination, is a *decision bias*. The *decision bias* defines the tendency of the preference of one prior hypothesis, regarding the other one, under the assumption of symmetric mass distribution.

The *decision bias* may be expressed as follows:

$$b_D = 1 - \frac{\min\{n_H, n_F\}}{\max\{n_H, n_F\}} \tag{3}$$

$$\forall m_1(F|F) = m_2(F|F) = m_1(H|H) = m_2(H|H)$$

where:

n_H – the number of HOSTILE theses;

n_F – the number of FRIEND theses;

$m_x(F|F)$ – the mass (originated from the x-th sensor) of the FRIEND hypothesis, on condition the data from the x-th sensor indicate the target is FRIEND.

The belief functions changeability examination performs a complement to the *decision robustness* study. Its general idea is to define the pace of the belief function change, while modification of the selected sensor data.

5. Comparison of fusion quality for diverse *bba*s

Due to the space restrictions of the paper, the authors decided to constrain the considerations to discussion of the obtained results of the numerical experiments, rather than their presentation.

Application of the introduced measures enables to notice that one of the most important disadvantages of *narrow information scope sensors* (NISS) information fusion is poor *decision robustness*. In about 30% of cases making decisions whether the target was FRIEND or HOSTILE was impossible. The only way the target could be identified as FAKER, was typically conflicting (by the combination of FRIEND from one sensor and HOSTILE from the other sensor). This conflicting mass is also problematic to manage, due to the fact that, according to *DST* and *DSmT* it should support both FRIEND and HOSTILE, while FAKER is also a subtype of FRIEND.

Extended information scope sensors (EISS) information fusion enables to deal with the problem of conflicting mass, since in such kind of fusion, the conflicting mass is not the only one indicating FAKER. The discussed cases of two-element decomposition and three-element decomposition differ from each other in terms of the defined measures. Even though, in both cases, the decision robustness values, calculated with the zero error, are equal to unity, which is an undoubted advantage in comparison with NISS fusion, the decision robustness values, calculated with the error of 0.01 differ significantly, providing better results for the two-element decomposition.

However, the *decision bias* is the key measure for the discussed comparison. For the two-element FAKER decomposition case the *decision bias* is relatively high. That means the results obtained with this method are tendentious in the consequence fostering FRIEND thesis. This also affects the *decision robustness* value, mentioned above, making it falsely high. Particularly, the difference in the *decision robustness* values is caused by existence of one case, where the decision change from FRIEND to HOSTILE is possible with error of 0.01. However, it is worth of notice, that this very case holds only if the evidence from both sensors shows no preference of any the types (i.e. FRIEND and HOSTILE are equally probable, according to data from both sensors). Anyway the decrease of the decision robustness is the high price that needs to be paid in three-element decomposition fusion, for this specific case. On the other hand, an arbitral acceptance of FRIEND in two-element decomposition fusion for this very case may seem to be a bit suspicious.

It is very important to notice that in all of the considered cases of fusion, the respective values of belief functions were close. The reader might find it counterintuitive: Since EISS better fits the real world, combination of evidence based on these sensors should probably provide higher values of the respective belief functions. This is not exactly the truth. The reliability of the results obtained for EISS is comparably higher, not the belief functions. This is due to the fact the respective belief functions encompass more focal elements, supported directly by sensor data.

6. Conclusion

The results of the numerical experiments have proven that taking into account the reliability of the elaborated decisions, application of EISS sensors is much more appropriate. Particularly, the best benefits may be achieved by applying three-element decomposition of FAKER hypothesis. This mechanism enables to decrease significantly the risk the resulting posterior hypothesis has been caused by fusion error, sensor damage or intentional introduction of false data.

It is worth of notice, that the specific features of the presented mechanisms, demonstrated in the target threat attribute, may also be applied to other attributes. In the worst case, an application of the decomposition, described herein, may cause the creation of posterior hypotheses that refer to the targets that do not exist.

That, in turn, should be verified by mechanisms of information evaluation [3] to eliminate such cases from the further analysis. On the other hand, remaining these cases will not degrade the quality of fusion, since the masses assigned to the improbable hypotheses are relatively small. However that will make the posterior hypotheses creation process less cost-effective.

As a direction for the forthcoming research works, related to the basic belief assignments the authors look forward to combination of ontological and evidential approaches, particularly an application of the former for creation of the posterior hypotheses.

7. Acknowledgement

This work was supported by the National Centre for Research and Development for the years 2009-2011 under Commissioned Research Project MNiSW-OR00007509.

References:

[1] Chmielewski M., Kasprzyk R.: Usage and characteristics of ontology models in Network Enabled Capability operations, MCC Conference, Cracow, ISBN 83-920120-5-4, 2008.

[2] Hyder A.K. et al. (eds.): *Multisensor Fusion*, ISBN 1-4020-0722-1, 99-124, 2002.

[3] Krenc K., A. Kawalec: An evaluation of the attribute information for the purpose of DSmT fusion in C&C systems, Fusion2008, Cologne, ISBN 978-3-00-024883-2, 2008.

[4] Krenc K., A. Kawalec: *An application of DSmT in ontology-based fusion systems*, Fusion2009, Seattle, ISBN 978-0-9824438-0-4, 2009.

[5] NATO Standardization Agreement, *Identification Data Combining Process*, STANAG No. 4162, Ed. 2.

[6] NATO Standardization Agency, *Tactical Data Exchange – Link 16*, STANAG No. 5516, Ed. 3.

[7] NATO Standardization Agreement (STANAG 5511): *Tactical data exchange – Link 11/Link 11B*, Ed 6 2004

[8] Navy Center for Tactical Systems Interoperability, Operational specification for over-the horizon targeting gold revision D, 2000.

[9] Shafer G.: *A mathematical theory of evidence*, Princeton U.P., Princeton, NJ, 1976

[10] Smarandache F., Dezert J., *Advances and Applications of DSmT for Information Fusion*, Vol 1, American Research Press Rehoboth, 2004.

[11] Smarandache F., Dezert J., *Advances and Applications of DSmT for Information Fusion*, Vol 2, American Research Press Rehoboth, 2006.

[12] Smarandache F., Dezert J., *Advances and Applications of DSmT for Information Fusion*, Vol 3, American Research Press Rehoboth, 2009

[13] The Joint C3 Information Exchange Data Model, Edition 3.1b, 2007