DOI: 10.1051/ro/2010022

DYNAMIC ESTIMATION OF EVIDENCE DISCOUNTING RATES BASED ON INFORMATION CREDIBILITY*

M.C. Florea¹, A.-L. Jousselme² and É. Bossé²

Communicated by M.C. Florea

Abstract. Information quality is crucial to any information fusion system as combining unreliable or partially credible pieces of information may lead to erroneous results. In this paper, Dempster-Shafer theory of evidence is being used as a framework for representing and combining uncertain pieces of information. We propose a method of dynamic estimation of evidence discounting rates based on the credibility of pieces of information. The credibility of a piece of information $Cre(I_n)$ is evaluated through a measure of consensus (corroboration degree) between a set of belief functions, and this measure serves as a basis for quantifying the credibility of the source (sensor or fusion node) itself, $Cre(S_k)$, used then as a discounting factor for all further belief functions provided by S_k . The process is dynamic in the sense that the credibility of the source is revisited in the light of new incoming piece of information. The method proposed relies on a hybrid fusion topology in which the sensors are grouped according to the feature they measure (similar and dissimilar sensors), allowing to select different kinds of measure for estimating the corroboration degrees. Through simulations, we compare (a) the hybrid-combination using the source credibility and the robust combination rule (RCR-L) accounting automatically for sensors's credibility; (b) the hybrid-combination, with different membership degrees and corroboration degrees used to estimate the sources credibility. We show that the new hybrid topology together with the credibility-based evidence discounting estimation algorithm provide a faster identification of the observed object.

 ${\bf Keywords.}$ Dempster-Shafer theory, evidence theory, discounting, credibility, fusion architecture.

Mathematics Subject Classification. 68T37, 68T05, 97R50.

Received December 31, 2009. Accepted November 8, 2010.

^{*} A preliminary version of this paper was presented in 2009 at the conference on Cognitive Systems with Interactive Sensors (COGIS'09) [6].

¹ Thales Canada Inc., Land & Joint Systems Division, Québec, Canada. Mihai.Florea@ca.thalesgroup.com

 $^{^2}$ Defence R & D Canada – Valcartier, Decision Support Systems for Command and Control Section, Québec, Canada. {Anne-Laure.Jousselme;Eloi.Bosse}@drdc-rddc.gc.ca

1. Introduction

In information fusion systems, considering information quality is of crucial importance [19]. For instance, granting equal weights to both reliable and unreliable sources may completely invalid the results of any information fusion process. Modeling uncertainty with belief functions allows to account for only one aspect of information quality, namely the uncertainty of the source regarding the piece of information it emits. However, other higher-order aspects of information quality need to be considered, in particular the reliability of the source that provides the information as well as the credibility of the piece of information. In [1,2,16], three main independent features have been identified to characterize the information evaluation: (1) the source's reliability, $Rel(S_k)$; (2) the number of independent sources that support a piece of information; and (3) the conflict factor of a piece of information with some other ones.

According to the NATO Standardization Agency, the reliability of a source relies on an evaluation of its past use. Thus, estimating the reliability of a source requires a training sequence where the information provided by the source can be compared to the ground truth. Then, the more correct pieces of information are provided, the more reliable the source is. The credibility of a piece of information relies on the relation between the other pieces of information provided by other independent sources of information, that if the pieces of information are either concurring or conflicting. Then, the more stored pieces of information confirming the given piece of information, the more credible this piece of information.

Both reliability of the source and credibility of the information influence the trust we should have about the piece of information. In [26], a degree of trustworthiness is defined denoting "the degree to which information from a source is perceived as conforming to a fact and therefore worthy of trust or belief". Two main factors influence thus the degree of trustworthiness and justify the discounting of a belief function before combination: (1) either the source is known to be not fully reliable; (2) or the information provided by the source is not fully credible. In both cases, the information should not be taken for granted and weakening it is reasonable, "discounting at higher rates those belief functions one particularly distrusts and whose influence one wants to reduce" as argued by Shafer [20]. The degree of trustworthiness t of a piece of information should be used to inversely discount the corresponding belief function such that a fully trusted information will not be discounted (t = 1) and a fully untrusted information will be discarded (t = 0). The question remaining is how to compute the discounting rate to be applied to a given belief function.

Discounting belief functions relatively to the reliability degrees of the source providing it is quite natural [15,21]. However, prior knowledge of sources's reliability is required and unfortunately often missing in practice. Unlike reliability, credibility can be estimated without any reference to ground truth and requires then no training sequence. Rather, an estimation of a credibility degree for a given piece of information can be based on a degree of agreement between pieces of information. For instance in [26], a degree of trustworthiness is computed as

a "measurement of corroboration derived by assessing the level of conformity to existing beliefs". The idea has been originally put forward by Yager [25] who states that "[a] characteristic of credibility qualification is that in some cases the credibility assigned to a piece of evidence can be a function of its compatibility with other, higher priority evidence". Approaches for discounting rates estimation based on consensus between several belief functions have been proposed in [4,9,14]. A measure of "relative reliability" is computed based on a membership degree of a source S_k to the others in a given set $S = \{S_1, \ldots, S_K\}$: if the piece of information provided by S_k is "close" to the ones provided by the $S \setminus S_k$, then S_k is considered as "reliable". If the piece of information from S_k is "far" from the others, then the source is "unreliable". Referring to the discussion above and regarding the distinction between the reliability and credibility concepts, it seems that the "relative reliability" in the above-mentioned works is simply the credibility of the source of information.

The underlying key concept for this kind of approach is the quantification of the interactions of two pieces of information, in particular the "closeness" between belief functions. In [4,9], computation is based on a similarity measure deduced from a distance between the pieces of information. Often used to quantify interaction between belief functions, Demspter's conflict factor does not reflect adequately the dissimilarity between two pieces information [12,14] as the internal conflict (or auto-conflict) is in general not null for a belief function. Indeed, Dempster's conflict rather represents a covariance measure [10]. Distances measures on the other hand may also incorrectly represent the disagreement between two belief functions.

We propose in this paper a method of dynamic estimation of evidence discounting rates based on the credibility of pieces of information. The credibility of a piece of information $Cre(I_n)$ is evaluated through a measure of consensus between a set of belief functions, and this measure serves as a basis for quantifying the credibility of the source (sensor or fusion node) itself, $Cre(S_k)$, used then as a discounting factor for all further belief functions provided by S_k . The process is dynamic in the sense that the credibility of the source is revisited in the light of new incoming pieces of information.

The method proposed relies on a hybrid fusion topology introduced in [7] in which the sources of information (sensors) are grouped according to the feature they measure. For instance, all sensors reporting information about the attribute Color are gathered in a group. This topology allows a greater flexibility in the choice of the measures of consensus (or agreement) between belief functions.

The paper is organized as follows: Section 2 presents background information on Dempster-Shafer evidence theory (DST). Section 3 shows the algorithm for discounting rate estimation and also different choices of interaction measures to be used either within a group of similar sensors or between groups of sensors. Section 4 presents the hybrid fusion topology together with the algorithm of discounting rate estimation. Section 5 provides simulation results on a vehicle identification scenario and compare the behavior of the proposed algorithm to other ones. We conclude in Section 6 on possible extensions of this work.

2. Background

Let Θ be the frame of discernment, containing N exclusive and exhaustive hypotheses, and let denote by 2^{Θ} its power set, containing all the subsets of Θ . A Basic Probability Assignment (BPA) is a mapping $m: 2^{\Theta} \to [0,1]$ that must satisfy the following conditions: (1) $m(\emptyset) = 0$ and $(2) \sum_{A \subseteq \Theta} m(A) = 1$, where $0 \le m(A) \le 1, \forall A \in 2^{\Theta}$. m(A) is called the mass of A and represents the degree of belief strictly assigned to A. A subset A with a non-null mass is called a focal element of m. Let \mathcal{F} designate the set of focal elements of m. A vacuous BPA has the frame of discernment itself as only focal element, i.e. $m_0(\Theta) = 1$. Θ is sometimes abusively called the ignorance.

A belief function Bel can be defined from $m, \forall A \subseteq \Theta$ as:

$$Bel(A) = \sum_{B \subseteq A} m(B). \tag{1}$$

The pignistic probability is defined $\forall A \subseteq \Theta$ as:

$$BetP(A) = \sum_{B \subseteq \Theta} m(B) \frac{|A \cap B|}{|B|}, \quad \forall A \subseteq \Theta.$$
 (2)

BetP defines a probability distribution over Θ .

2.1. Some combination rules

Dempster's combination rule of two BPAs m_1 and m_2 is defined as the normalized conjunctive combination as:

$$m_{\cap}(A) = \frac{1}{K} \sum_{B \cap C = A} m_1(B) m_2(C), \quad \forall A \subseteq \Theta$$
 (3)

where $K = m_{12}(\varnothing)$ is the weight of conflict (or simply conflict) between m_1 and m_2 and is equal to the mass of the empty set after the conjunctive combination and before any normalization step. If K is close to 0, the BPAs are not in conflict, while if K is close to 1, the BPAs are in conflict.

A class of Robust Combination Rules (RCR) has been introduced in [8] as adaptive combination rules for automatically account for the relative reliability of the sources. Within this class, the RCR with logarithmic weightings, called RCR-L, has been shown to perform the best in most of the situations (see [8] for details) and will be used for comparison in Section 5. The combination of two

BPAs m_1 and m_2 by the RCR-L is defined for all $A \subseteq \Theta$ by:

$$m_{RCR-L}(A) = \frac{\log[(1+x)^K (K+x)^{1-K}/x]}{\log[(1+x)/x]} m_{\cup}(A) + \frac{\log[(1+x)/(K+x)]}{\log[(1+x)/x]} m_{\cap}(A), \quad A \neq \emptyset$$

$$m_{RCR-L}(\emptyset) = 0$$
(4)

where $m_{\cup}(A) = \sum_{B \cup C = A} m_1(B) m_2(C)$ is the disjunctive combination rule, and x is a real value between 0 and 1 representing the distribution of the conflict K. In the following, we will use this rule to automatically account for the credibility of the pieces of information: If the conflict is low (high), the piece of information is credible (non-credible).

When we do not trust a particular BPA to a certain degree (of trustworthiness) $t \in [0,1]$, a discounting rate can be applied to the BPA resulting in for all $A \subseteq \Theta$:

$$m^*(A) = tm(A), \quad A \neq \Theta$$

 $m^*(\Theta) = 1 - t + tm(\Theta)$ (5)

t can represent either a degree of reliability associated to the corresponding source of information (t=1, meaning that the source is fully reliable), or a degree of credibility of the BPA itself when comparing it to others. When t=1, the mass function remains unchanged while when t=0, the mass function becomes the vacuous BPA $m_0(\Theta)=1$. The discounted BPA can be combined through Dempster's rule.

2.2. DISTANCES AND INNER-PRODUCTS

Let us introduce by $\mathbf{m} = [m(A_1) \dots m(A_{2^{N-1}})]'$ the vector notation of a BPA. \mathbf{W} is a $2^{N-1} \times 2^{N-1}$ square matrix whose elements W(A, B) quantify the interactions between the focal elements of m_1 and m_2 . W(A, B) is either a similarity or a dissimilarity measure. In [10], two main kinds of measures for quantifying the interaction between belief functions have been identified:

(1) Inner-products of the form

$$\sigma(m_1, m_2) = \mathbf{m_1}' \mathbf{W} \mathbf{m_2} \tag{6}$$

where $\mathbf{m_i}$ is the vector notation of the BPA m_i and $\mathbf{m'}$ is the transpose of \mathbf{m} . Inner-products measure a kind of *covariance* between m_1 and m_2 , the variance being the norm of m. Dempster's weight of conflict K is of this kind.

Distance name [Ref.]	$d(m_1, m_2)$	Comments
Tessem [22] d_T	$\max_{A\subseteq\Theta} \left \operatorname{BetP}_1(A) - \operatorname{BetP}_2(A) \right $	
Jousselme [11] d_{BPA}	$\sqrt{\frac{1}{2}(\mathbf{m}_1 - \mathbf{m}_2)' \mathbf{D}(\mathbf{m}_1 - \mathbf{m}_2)}$	$D(A,B) = \frac{ A \cap B }{ A \cup B }$
Euclidean [17] d_E	$\sqrt{\sum_{A\subseteq\Theta} \left[m_1(A) - m_2(A) \right]^2}$	
Euclidean (Bel) [3] $d_E^{(Bel)}$	$\sqrt{\sum_{A\subseteq\Theta} \left[\operatorname{Bel}_1(A) - \operatorname{Bel}_2(A) \right]^2}$	
Bhattacharyya [17] d_B	$\left 1 - \sum_{A \subseteq \Theta} \sqrt{m_1(A)m_2(A)} \right ^p$	$p \in \mathbb{R}^{*+}$
Diaz [5] d_{Di}	$\sqrt{\frac{1}{2}(\mathbf{m}_1 - \mathbf{m}_2)'F(\mathbf{S}, R)(\mathbf{m}_1 - \mathbf{m}_2)}$	$R = \frac{ A \cup B }{ \Theta }$
Cosine [23] σ_{\cos}	$\frac{\sum_{A\subseteq\Theta} m_1(A)m_2(A)}{\sqrt{\left(\sum_{A\subseteq\Theta} m_1^2(A)\right)\left(\sum_{A\subseteq\Theta} m_2^2(A)\right)}}$	

Table 1. Some dissimilarity measures between belief functions.

(2) Distances of the form

$$d(m_1, m_2) = (\mathbf{m_1} - \mathbf{m_2})' \mathbf{W} (\mathbf{m_1} - \mathbf{m_2})$$

$$\tag{7}$$

d is the quadratic form associated to the bilinear form σ and measures then the *variance* of the difference between m_1 and m_2 .

The main difference between distances d and inner-products σ is that while the property d(m,m)=0 always holds, in general $\sigma(m,m)=0$ does not hold. Table 1 summarizes some distances traditionally used.

3. Credibility-based estimation of discounting rate

3.1. Membership degrees

Let $\mathcal{M} = \{m_1, \dots, m_M\}$ be a set of BPAs. We call membership degree MD of a particular BPA, any measure that quantifies how close the specific BPA is to the rest of the group. The higher MD(m), the more it belongs to \mathcal{M} . In [7], some techniques to compute the membership degree of a BPA to a group of BPAs are reviewed¹. These measures proposed by Deng et al. [4], Martin et al. [14], Xu et al. [24] and Florea et al. [7] are all based on a distance measure between BPAs. The idea is that the farthest a BPAs from the other, the lower its membership to

 $^{^{1}}$ These measures have been given different names that we gather under the term "membership degree" in this paper.

Measure name [Ref.] Formula Comments $R'(m_i) = \frac{\operatorname{Sup}(m_i)}{\sum_{1 \le j \le N} \operatorname{Sup}(m_j)}$ Absolute reliability $R(m_i) =$ $\max_{1 \le j \le N} R'(m_j)$ $Sup(m_i) = \sum_{1 \le j \le N, i \ne j} s(m_i, m_j)$ s = 1 - d, similarity measure, [9]d in Table 1 $\alpha(m_i) = \left[1 - \operatorname{Conf}^{\lambda}(m_i)\right]$ $Conf(m_i) = d(m_i, m_{\oplus}^i)$ Relative reliability $m_{\oplus}^i = \bigoplus_{j,i \neq j} m_j$ [14] $ATR(m_i) = \frac{|\overline{A(m_i, \tau)}|}{M}$ $A(m_i, \tau) = \{m_j | s(m_i, m_j) \ge \tau\},\$ Above Threshold Ratio [7] $\tau \in]0,1[$ No-Conflict $NCR(m_i) =$ $B(m_i) = \{m_j | s(m_i, m_j) = 1\}$ Ratio [7] Reliability (Xu et al.'s modified method) [7,24]

Table 2. Membership degrees based on a distance measure d.

the group, and hence the lower the credibility of the source that has provided it. Table 2 summarizes these measures.

Although a distance measure can be used in some cases to quantify the "conflict" between BPAs, it may not be adequate in other cases as a high distance between two BPAs may be due to the natural complementarity of sources rather than to a real conflict, as it will be detailed in the rest of this section.

3.2. REDUNDANT AND COMPLEMENTARY INFORMATION

Four fundamental aspects are identified in [13] for multisensor integration and fusion: redundancy, complementarity, timeliness, and cost of the information. The redundancy and complementarity of sensors allow to obtain more precise information by accessing to features not available to individual sensors. Redundant pieces of information are obtained by sensors perceiving the *same* features in the environment whereas complementary pieces of information are obtained by sensors perceiving different features.

Hereafter, sensors whose reports concern the same features will be called *similar* and sensors providing information about different features will be called *dissimilar*. Thus, similar sensors provide redundant information while dissimilar sensors provide complementary information.

3.3. Example of a vehicle identification scenario

We consider the problem of vehicle (car) identification with a set of sensors. The list of possibly observable cars is provided in the information table of Table 3 together with their corresponding 4 features in $\mathcal{F} = \{\text{Model, Color, Class, Country}\}$

Table 3. Information table.

#	Model	Color	Class	Country
θ_1	BMW	red	sedan	Germany
θ_2	Honda	red	sedan	France
θ_3	Honda	black	SUV	Ontario
θ_4	Dodge	white	sedan	Quebec
θ_5	Dodge	red	coupé	Florida
θ_6	Toyota	blue	coupé	Ontario
θ_7	Toyota	blue	sedan	Quebec
θ_8	Porsche	black	SUV	Quebec
θ_9	Porsche	red	sport	Germany
θ_{10}	Audi	gray	sedan	France

Table 4. Feature domains.

	Feature f_i	Domain F_i
1	Model	{BMW, Honda, Dodge, Toyota, Porsche, Audi}
2	Color	{Red, Blue, Black, White, Gray}
3	Class	{Sedan, SUV, Coupé, Sport}
4	Country	{Germany, France, Ontario, Quebec, Florida}

(or state/province)}. The corresponding frame of discernment is $\Theta = \{\theta_1, \theta_2, \dots, \theta_{10}\}$. Each feature f_i has its own domain F_i detailed in Table 4.

Let $S = \{S_1, \ldots, S_9\}$ be a set of 9 sensors reporting information about (1) feature f_1 (model) that are S_1, S_2 , (2) feature f_2 (color) that are S_3, S_4, S_5 , (3) feature f_3 (class) that are S_6, S_7 and (4) feature f_4 (country) that are S_8, S_9 . For instance, S_1 and S_2 are similar sensors, while S_1 and S_4 are dissimilar sensors.

Each piece of information I_n is modeled by a dichotomous BPA such that

$$m_n(A_n) = 0.8 \quad m_n(\overline{A_n}) = 0.1 \quad m_n(\Theta) = 0.1$$
 (8)

where A_n is the set of objects of Θ whose feature is specified by I_n . Table 5 lists examples of pieces of information together with their corresponding main focal element A_n . The set S of sensors provides a set $\mathcal{M} = \{m_1, m_2, \ldots, m_M\}$ of BPAs. We denote by $\mathcal{M}(S_k)$ the set of BPAs from \mathcal{M} generated by S_k^2 . Also, $S_k(m_i)$ is the sensor associated to the BPA m_i .

 I_1 and I_5 are examples of redundant pieces of information while I_2 and I_3 are examples of complementary pieces of information. We intend to quantify the credibility of a given sensor based on the membership degree (or consensus degree) of its reported BPAs to a given group of BPAs. This involves thus the characterization of the interaction between the BPAs. In the two cases above, dissimilarities between the corresponding BPAs can arise but we argue that it should not be

²Note that the number of BPAs does not necessarily match the number of sensors.

Table 5. Pieces of information I_n and associated main focal element A_n .

	I_n	A_n
1	The car is a BMW	$\{\theta_1\}$
2	The car is red	$\{\theta_1, \theta_2, \theta_5, \theta_9\}$
3	The car is from Quebec	$\{\theta_4, \theta_7, \theta_8\}$
4	The car is a sedan	$\{\theta_1,\theta_2,\theta_4,\theta_7,\theta_{10}\}$
5	The car is a Dodge	$\{\theta_4, \theta_5\}$
6	The car is blue	$\{\theta_6, \theta_7\}$
7	The car is dark	$\{\theta_3, \theta_6, \theta_7, \theta_8, \theta_{10}\}$

Table 6. Examples of distance and covariance measures between redundant and complementary pieces of information.

	Redur		indant Complementary		ementary
		Agreeing	Conflicting	Agreeing	Conflicting
		m_{6}, m_{6}	m_{2}, m_{6}	m_1, m_2	m_{2}, m_{3}
σ	σ_W	0.16	0.64	0	0.64
	$\sigma_{ m cos}$	1	0.0152	0.0152	0.0152
	d_T	0	0.7667	0.5833	0.75
d	d_J	0	0.7611	0.6916	0.7492
	d_{Di}	0	0.7728	0.7060	0.7584

interpreted in the same way. Indeed, the fact that I_1 and I_5 are distinct reveals a conflict between the two sources as their intersection is null in their common domain (a car cannot be both a BMW and a Toyota). However, the dissimilarity between I_2 and I_3 is natural as both pieces of information concern different features (complementary information). Thus in this latter case, the sources should not be identified as being in conflict.

In order to characterize adequately the dissimilarity between two BPAs we select different measures for the two classes of sensors (either similar or dissimilar).

3.4. Choice of the measure

We agree that the interaction between for example m_1 and m_2 (dissimilar sensors) on the one hand and between m_2 and m_6 (similar sensors) on the other hand is not of the same nature and as such, should be quantified in different ways. The question is then "what measure should be used to quantify the interaction between two BPAs corresponding to either redundant or complementary information?".

Let us consider the examples of Table 6 where several cases have been considered: (1) redundant and agreeing pieces of information; (2) redundant but conflicting pieces of information; (3) complementary and agreeing pieces of information; and (4) complementary but conflicting pieces of information.

We note that although m_6 and m_6 are obviously agreeing³, σ_D is not equal to 0. On the other hand, the distances are obviously all null. While m_1 and m_2 are agreeing, $\sigma_D(m_1, m_2) = 0$ but their distances are not null which is natural since the sensors report about different features. In this case, the distance has no sense, and σ_D is more suitable for computing the membership degree.

The cosine measure σ_{\cos} has been introduced for comparison: Although it is of the same nature than σ_D , it is useless here since the interaction between the focal elements of the respective BPAs are not taken into account. The three distances selected provide equivalent results and the choice of one of them requires obviously a deeper study.

In light of this example, we argue that the interaction between BPAs for quantifying membership degree to a group should be based on:

- A distance measure if the sensors are similar (e.g. the target is red and the target is blue). One of the distance measures proposed for example in [5,11,14,18,22] can be used.
- A covariance measure if the sensors are dissimilar (e.g. the target is red and the target is a Dodge). Dempster's conflict σ_D is a good candidate.

3.5. Credibility as a corroboration degree

For a given sensor S_k and from the membership degrees associated to the pieces of information it generates, we propose to define the credibility estimation as a corroboration degree Corr and introduce two definitions:

(1) as the ratio between the number of corroborative BPAs inside $S_k(\mathcal{M})$ and the number of BPAs generated by S_k :

$$Corr_1(S_k) = \frac{|A_k|}{|S_k(\mathscr{M})|} \tag{9}$$

where $A_k = \{m_i | MD(m_i) \geq \beta, m_i \in S_k(\mathcal{M})\};$

(2) as the ratio between the overall membership degree and the number of BPAs generated by S_k :

$$Corr_2(S_k) = \frac{\sum_{m_i \in S_k(\mathcal{M})} MD(m_i)}{|S_k(\mathcal{M})|}$$
(10)

The overall algorithm for credibility estimation is depicted in Figure 1. After similar sensors have been gathered, the membership degrees are computed for each BPA within each cluster. The credibility of each sensor is then deduced as a corroboration degree of the BPAs within a cluster. Based on the credibility degree, the corresponding BPAs of the sensor are either discarded or discounted.

 $^{^{3}}$ This case illustrates the case where the same BPA is reported by different sensors.

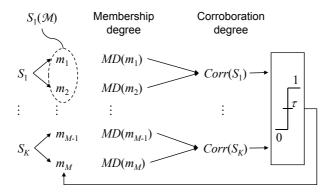


FIGURE 1. Sensor's credibility estimation based on membership degrees.

4. Information sources topology

If the use of multiple sensors has been acknowledged to increase the capabilities of fusion systems, the need for developing methods to integrate and combine the pieces of information from these sensors becomes more and more challenging. Indeed, the diversity of information provided by several types of sensors requires special care when combining the different pieces of information. As introduced in the previous section, dealing with redundant or complementary information may involve different processing regarding the fusion process in general, and the credibility estimation in particular.

4.1. Fusion topology

To adequately account for the similarity or dissimilarities between sensors, we proposed in [7] a hybrid sensor fusion (HSF) topology depicted in Figure 2. In this HSF topology⁴, groups of similar sensors are first built as a SSF (similar sensor fusion) node in which pieces of information from similar sensors will be combined. The combination results of the SSF nodes are further combined at a central DSF (dissimilar sensor fusion) node. Such a topology allows some flexibility in the selection of the combination rules to be used either at the different SSF nodes or at the DSF node, as the rule can differ from one node to another one. Our particular interest in this paper, is to have an estimation method of the credibility of the sensors and nodes based on different choices of dissimilarity or conflict measures.

⁴Note that an equivalent topology has been proposed in a parallel work in [1], for the evaluation of the information extracted from reports written in natural language.

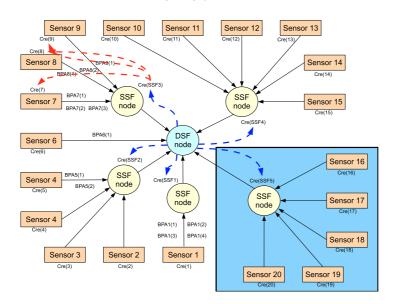


Figure 2. Information sources topology.

4.2. Algorithm for credibility estimation

The algorithm for credibility estimation is depicted in the flowchart of Figure 3.

Step (1): At the Sensors-level, consider the credibilities of all Sensors (in the interval [0, 1] or unknown). At the DSF-Level, we consider the credibilities of all SSF nodes (in the interval [0, 1] or unknown).

Move FORWARD from the Sensors-level to the SSF-level.

Step (2): At each SSF node, compute the corroboration degrees Corr of the sensors of the node, based on the BPAs obtained from each sensor (which are not discounted by the credibilities of the sensors). The corroboration degrees must be independent from the credibilities of the sensors, since they only measure the compatibility between the measures of sensors.

Move BACKWARD from the SSF-level to the Sensors-level.

Step (3): Based on the credibilities of the sensors and their corroboration degrees, compute a revisited credibility for all sensors, such that

$$Cre(S_k) = \frac{1}{2} \Big[Cre(S_k) + Corr(S_k) \Big].$$

If the credibilities of the senors are unknown, then the credibilities are set to be equal to the corroboration degrees:

$$Cre(S_k) = Corr(S_k).$$

Move FORWARD from the Sensors-level to the SSF-level.

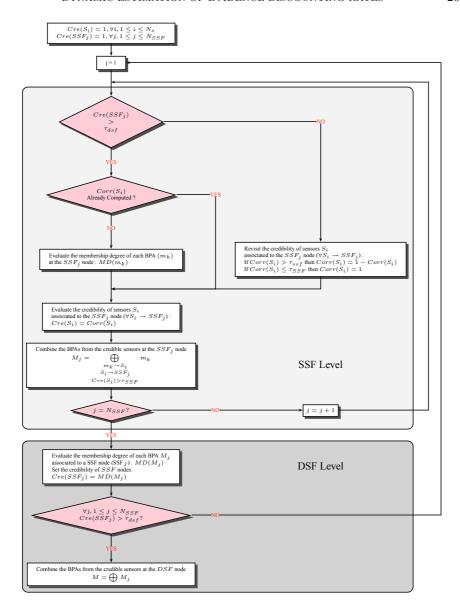


FIGURE 3. Flowchart for credibility estimation and combination.

Step (4): At each SSF node, combine the BPAs provided by the sensors of the SSF node, either with a hard discounting (combine only the BPAs from credible sensors, *i.e.* above a given threshold) or with a soft discounting (use the credibility degrees to discount all the BPAs before combination). Move FORWARD from the SSF-level to the DSF-level.

Step (5): Compute the membership degrees MD associated to the SSF nodes. Revisit the credibilities of the SSF nodes, using the membership degrees:

$$Cre(SSF_i) = \frac{1}{2} \Big[Cre(SSF_i) + MD(SSF_i) \Big].$$

If the initial credibilities of the SSF nodes are unknown, then the credibilities of the SSF nodes are set to be equal to their membership degrees

$$Cre(SSF_i) = MD(SSF_i).$$

Compare the credibilities of the SSF nodes to a given threshold and identify the incompatible SSF nodes (if any).

For each incompatible SSF node, move BACKWARD to the SSF-level.

Step (6): Revisit the corroboration degrees of the sensors of the SSF node. A corroborative sensor of an incompatible SSF node becomes un-corroborative:

$$Corr(S_k) = 1 - Corr(S_k)$$

and an un-corroborative sensor of an incompatible SSF node become corroborative $\,$

$$Corr(S_k) = 1.$$

Move BACKWARD to the Sensors-level and go to Step 3.

Credibility revisited

One major drawback of the consensus-based approaches for credibility estimation, is that a source may be discarded although it is the only correct one among a set of sources. The hybrid topology proposed offers the way to revise a decision (identify a sensor as non-credible) and reverse it through the process described at Steps 3 and 6 of the algorithm above.

The solution proposed here in order to revisit the corroboration degrees of the sensors based on the credibility of the SSF nodes is based on the assumption that at each SSF node there are at most 3 sensors. Thorough investigations should be conducted in order to develop a new algorithm taking into account groups of more than 3 sensors at each SSF node.

Corroboration degrees for sensors

At a given time step, a SSF node collects all the BPAs received until then, and computes for each BPA a membership degree. However, each sensor feeding the SSF node had provided one or more BPAs, each of them having a different membership degree. From the set of MD associated to each sensor, a corroboration degree can be computed in order to measure the credibility of the sensor. Once the credibility of a sensor has been computed, all the BPAs previously provided by it can be discounted accordingly or even discarded from the future combination

Value Node Attr. Freq. Prob. $P(S_k)$ $P(v|S_k)$ Honda S_1 0.1 0.9 SSF_1 Model S_2 0.05 Honda 0.7 \overline{S}_3 Red 0.9 0.1 SSF_2 S_4 0.05 Red 0.9 Color 0.25 Blue 1 Sedan S_6 0.150.9 SSF_3 Class S_7 0.1 Random 0.25 S_8 0.05 France 0.8 SSF_4 Country S_9 0.15 0.7 France

Table 7. Statistical features of sensors.

process, which allows to compute the BPA associated to the SSF node. At the DSF node, to each SSF node has been associated one and only one BPA (at a given time step - obtained from the combination at the SSF level). In order to evaluate the credibility of the SSF nodes, a membership degree of each BPA can be computed. Since there is only one BPA associated to each SSF node, no corroboration degree is necessary.

5. Simulations

5.1. Settings

A set of 9 sensors described in Section 3.3 is used for this simulation. Table 7 shows the sensors and their associated SSF nodes, the frequency at which the sensors are providing the measurements with the corresponding value, and their associated probability. For example, Sensor S_3 reports with a frequency of 10% about the color of the observed object $(P(S_3))$, and over 100 reports of S_3 , 90 say that the car is Red $(P(Red|S_3))$. The BPAs are then built according to the method described in Section 3.3.

We randomly generate a set of 200 BPAs following the specificities of Table 7. Each sensor provides measurements at random time-stamps inside the interval [1, 200]. We use the Hybrid Sensor Fusion topology and the algorithm of Figure 3 to combine the pieces of information and we set the initial credibility thresholds for the SSF and DSF nodes to be $\tau_{SSF}=0.75$ and $\tau_{DSF}=0.65$ respectively. At each node of the topology (SSF or DSF), we use either Dempster's rule or the RCR-L rule in order to combine the BPAs.

5.2. Results

Most of the sensors agree on the fact that the observed object is θ_2 . Sensor S_7 is completely unreliable since it provides random values and sensor S_5 always

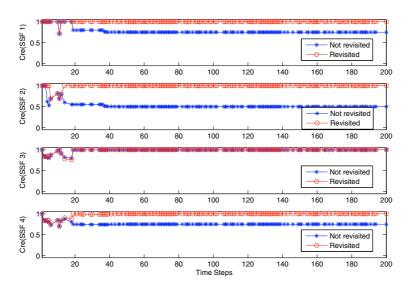


FIGURE 4. Credibility of the SSF nodes.

provides the same erroneous piece of information. Since the frequencies of sensors S_6 and S_7 are not so different and since sensor S_6 provides pieces of information in agreement (focused on a given value with a probability equal to 0.9) and S_7 provides pieces of information in a complete random manner, the algorithm should identify the sensor S_7 as non-credible at the SSF node.

Figure 4 shows the credibility of each SSF node. First, the credibility of each SSF node, computed as a compatibility measure (membership degree) between nodes is presented. When the SSF₂ node is identified as incompatible with the rest of the nodes, the credibility of all its sensors is revisited in order to look for compatibility at the DSF-level. Once the credibility of the sensors associated to the SSF₂ node is revisited, all the BPAs associated to the SSF₂ node change, their combination changes and thus, the compatibility of the SSF₂ node with the other SSF nodes changes too. Moreover, the compatibility of the other SSF nodes to the group changes too.

Figure 5 shows the credibility of Sensors 4–6 during the entire combination process. At each time step, the credibility of the sensor computed at the SSF node and the revisited credibility of the sensor (after the compatibility of the SSF nodes was processed at the DSF node) are both shown on the same graphic.

At the SSF₂ node, Sensor S_4 is identified as non-credible while Sensor S_5 is identified as credible. Meanwhile, when the SSF₂ node is identified as non-credible at the DSF node, the credibilities associated to all its sensors are revisited. And thus, Sensor S_4 becomes credible while Sensor S_5 becomes non-credible. This change produces also a change in all other SSF nodes, since they become more credible than previously. Sensor S_6 is identified as credible at the SSF₃ node and

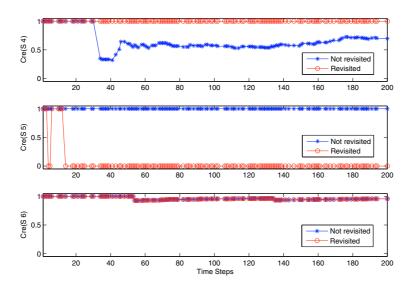


FIGURE 5. Credibility of the Sensors.

remains credible since the SSF₃ is detected to be credible and the credibility of its sensors is not revisited.

We call "blind" combination process, the process by which the BPAs are combined on the fly, without use of the HSF topology. Figure 6 compares the blind combination process and the hybrid combination process using a hard decision (only the BPAs from credible sources are combined). Both algorithms are used with Dempster's rule of combination and the RCR-L rule. The following parameters are used:

- Deng et al.'s membership degree using the d_{BPA} distance (at the SSF nodes):
- Deng *et al.*'s membership degree using the conjunctive conflict (at the DSF node);
- Corr₁ corroboration degree;
- $\tau_{ssf} = 0.75$ and $\tau_{dsf} = 0.65$.

The test-scenario provides pieces of information in agreement with the observed object only about 55% of the time. Therefore, we expect an oscillating behavior when the non-associative RCR-L rule is used in a blind combination process, since it provides more credibility to the last pieces of information. We notice also that in this case, the identification of singleton θ_2 as the observed object cannot be reached.

When comparing the hybrid topology used with Dempster's rule of combination and the blind Dempster's rule, the identification of singleton θ_2 is realized faster using the hybrid topology. When comparing the hybrid topology used with the RCR-L combination rule and the blind RCR-L rule, an improvement of the

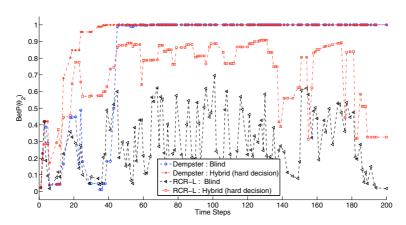


FIGURE 6. Blind Combination vs. Hybrid Combination (with Hard Decision).

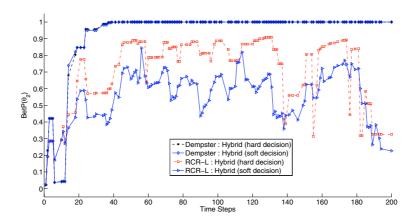


FIGURE 7. Hybrid Combination: Hard vs. Soft Decision.

identification of singleton θ_2 is observed when using the hybrid topology. The oscillating values of the BetP(θ_2) are attenuated. However, when comparing the hybrid topology using Dempster's rule of combination and the hybrid topology using the RCR-L rule, the identification is faster and without any doubt, when Dempster's rule of combination is used.

Figure 7 shows the impact of using a soft decision (by discounting the BPAs from non-credible sensors before the combination process) or a hard-decision (by filtering them from the combination process). The following parameters are used:

- Deng et al.'s membership degree using the d_{BPA} distance (at the SSF nodes);
- Deng *et al.*'s membership degree using the conjunctive conflict (at the DSF node);

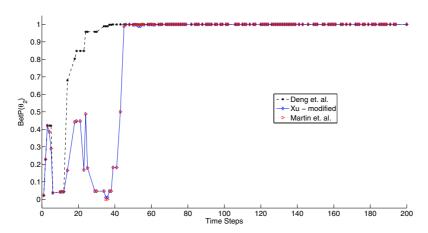


Figure 8. Comparison of different membership degrees.

- Corr₁ corroboration degree;
- $\tau_{ssf} = 0.75$ and $\tau_{dsf} = 0.65$.

We notice only a small difference between the hard and soft decision when using Dempster's rule. Meanwhile, when the RCR-L rule is used at both SSF and DSF nodes with the hybrid topology, the values of $BetP(\theta_2)$ are oscillating for both hard or soft decisions. However, the hybrid combination using soft decision can be seen somewhere between the blind combination and the hybrid combination with hard decision.

Figure 8 shows the impact of using different membership degrees at the SSF/DSF-levels on the pignistic probability of singleton θ_2 . The following parameters are used:

- hybrid Combination (with Hard Decision): Dempster's rule of combination at all SSF and DSF nodes;
- Corr₁ corroboration degree;
- $\tau_{ssf} = 0.75$ and $\tau_{dsf} = 0.65$.

Using Deng et al.'s membership degree at both SSF and DSF-levels allows to identify faster the singleton θ_2 as the observed object. The modified method of Xu et al. and Martin et al. method are providing similar results.

Figure 9 shows the impact of the corroboration degree on the pignistic probability of singleton θ_2 . The different parameters used for this test are the following:

- Deng et al.'s membership degree using the d_{BPA} distance (at the SSF nodes):
- Deng et al.'s membership degree using the conjunctive conflict (at the DSF node);
- Hybrid Combination (with Hard Decision): Dempster's rule of combination at each SSF and DSF nodes;
- $\tau_{ssf} = 0.75$ and $\tau_{dsf} = 0.65$.

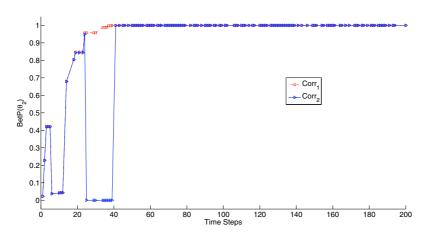


Figure 9. Comparison for different corroboration degrees.

 $Corr_1$ allows faster identification of singleton θ_2 than $Corr_2$. Moreover $Corr_2$ is unstable and can lead to incorrect identification (see time-steps between 25 and 40).

Figure 10 shows the impact of the SSF threshold on the combination process when Martin *et al.*'s membership degree is used at both the SSF nodes and the DSF nodes. The scenario test was generated using the following parameters:

- hybrid combination (with Hard Decision): Dempster's rule of combination at each SSF and DSF nodes;
- Martin et al.'s membership degree with Dempster's rule of combination, d_{BPA} and $\lambda = 4$;
- Corr₁ corroboration degree;
- $\tau_{dsf} = 0.65$.

When we use a higher threshold at the SSF nodes when Martin et~al.'s membership degree is used, the identification of Singleton θ_2 is slower. However, this should not be interpreted as the more the thresholds are low, faster the identification will be. In fact, the thresholds τ_{ssf} and τ_{dsf} should be adjusted to each different membership degree. If both thresholds are too high, the sensors and the SSF nodes will be considered as non-credible and then the BPAs associated to them will be discounted or discarded from the combination process. If the SSF threshold is too low, even the non-credible sensors will be considered credible and then the hybrid combination process will become close to the blind combination process. If τ_{ssf} is high and τ_{dsf} is low, the hybrid topology will favor the sensors from the SSF nodes which are in agreement. Even if in the previous simulations all the SSF nodes have the same threshold (τ_{ssf}) , a specific threshold could be defined for each particular SSF node.

From the previous tests we conclude that Deng *et al.*'s membership degree along with Dempster's rule of combination at both SSF and DSF nodes is the most appropriate configuration for our example.

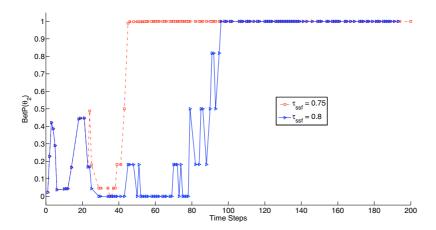


FIGURE 10. Comparison for Martin *et al.*'s membership degree when different threshold are used.

6. Conclusions

In this paper, we proposed a method of dynamic estimation of evidence discounting rates based on the credibility of pieces of information. We proposed a hybrid fusion topology in which the sensors are grouped according to the feature they measure (similar and dissimilar sensors), allowing to select different kinds of measure for estimating the corroboration degrees. We showed that the new hybrid topology together with the credibility-based evidence discounting estimation algorithm provide a faster identification of the observed object. We compared Dempster's rule of combination and RCR-L rule at both SSF and DSF levels in the hybrid topology. We have also compared several membership degrees to be used at both SSF and DSF nodes and several corroboration degrees to evaluate source credibility. Soft and hard decisions have been used with this hybrid topology in order to discount or discard the BPAs from non-credible sources. New combination rules at the different nodes as well as new dissimilarity measures will be explored in the future.

References

- J. Besombes, V. Nimier and L. Cholvy, Information Evaluation in Fusion using Information Correlation, in Proc. of the 12th International Conference on Information Fusion, Seattle, USA (2009).
- [2] L. Cholvy and V. Nimier, Information Evaluation: discussion about STANAG 2022 recommandations, in *Military Data and Information Fusion*, RTO-MP-IST-040, Prague, Czech Republic (2003).
- [3] F. Cuzzolin, A Geometric Approach to the Theory of Evidence. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews 38 (2008) 522-534.
- [4] Y. Deng, W. Shi, Z. Zhu and Q. Liu, Combining belief functions based on distance of evidence. Decis. Support Syst. 38 (2004) 489–493.

- [5] J. Diaz, M. Rifqi and B. Bouchon-Meunier, A similarity measure between basic belief assignments, in *Proc. of the 9th International Conference Information Fusion*, Firenze, Italy (2006).
- [6] M.C. Florea, E. Bossé and A.-L. Jousselme, Metrics, Distances and Dissimilarity Measures within Dempster-Shafer Theory to Characterize Sources' Reliability, in *Proc. of Cognitive* Systems with Interactive Sensors (COGIS '09) (2009).
- [7] M.C. Florea and E. Bossé, Crisis Management Using Dempster Shafer Theory: Using Dissimilarity Measures to Characterize Sources' Reliability, in Proc. of C31 in Crisis, Emergency and Consequence Management, RTO-MP-IST-086, Bucharest, Romania (2009).
- [8] M.C. Florea, A.-L. Jousselme, D. Grenier and E. Bossé, Robust combination rules for evidence theory. *Inform. Fusion* 10 (2009) 183–197.
- [9] H. Guo, W. Shi and Y. Deng, Evaluating Sensor Reliability in Classification Problems Based on Evidence Theory. *IEEE Transactions on Systems, Man, and Cybernetics. Part B:* Cybernetics 36 (2006) 970–981.
- [10] A.-L. Jousselme and P. Maupin, On some properties of distances in evidence theory, in Proc. of the Workshop on the Theory of Belief Functions, Brest, France (2010).
- [11] A.-L. Jousselme, D. Grenier and E. Bossé, A new distance between two bodies of evidence. Inform. Fusion 2 (2001) 91–101.
- [12] W. Liu, Analyzing the degree of conflict among belief functions. Artif. Intell. 170 (2006) 909–924.
- [13] R.C. Luo and M.G. Kay, Multisensor Integration and Fusion in Intelligent Systems. IEEE Transactions on Systems, Man, and Cybernetics 19 (1989) 901–931.
- [14] A. Martin, A.-L. Jousselme and C. Osswald, Conflict measure for the discounting operation on belief functions, in *Proc. of the 11th Annual Conference on Information Fusion*, Cologne, Germany (2008).
- [15] D. Mercier, B. Quost and T. Denœux, Refined modeling of sensor reliability in the belief function framework using contextual discounting. *Inform. Fusion* 9 (2008) 246–258.
- [16] V. Nimier, Information Evaluation: a formalisation of operational recommandations, in Proc. of the 7th International Conference on Information Fusion, Stockholm, Sweden (2004).
- [17] B. Ristic and P. Smets, The TBM global distance measure for the association of uncertain combat ID declarations. *Inform. Fusion* 7 (2006) 276–284.
- [18] B. Ristic and P. Smets, Global cost of assignment in the TBM framework for association of uncertain ID reports. Aerosp. Sci. Technol. 11 (2007) 303–309.
- [19] G. Rogova and E. Bossé, Information quality in information fusion, in Proc. of the 13th International Conference on Information Fusion, Edinburgh, Scotland (2010).
- [20] G. Shafer, A Mathematical Theory of Evidence, Princeton University Press (1976).
- [21] P. Smets, Belief functions: The disjunctive rule of combination and the generalized Bayesian theorem. *Int. J. Approxim. Reason.* **9** (1993) 1–35.
- [22] B. Tessem, Approximations for efficient computation in the theory of evidence. *Artif. Intell.* **61** (1993) 315–329
- [23] C. Wen, Y. Wang and X. Xu, Fuzzy Information Fusion Algorithm of Fault Diagnosis Based on Similarity Measure of Evidence, in *Advances in Neural Networks*, Ser. Lect. Notes Comp. Sci. 5264, Springer Berlin/Heidelberg (2008), pp. 506–515.
- [24] G. Xu, W. Tian, L. Qian and X. Zhang, A novel conflict reassignment method based on grey relational analysis (GRA). Pattern Recogn. Lett. 28 (2007) 2080–2087.
- [25] R.R. Yager, On considerations of credibility of evidence. Int. J. Approxim. Reason. 7 (1992)
- [26] S. Young and J. Palmer, Pedigree and confidence: Issues in data credibility and reliability, in Proc. of the 10th International Conference on Information Fusion, Quebec city (Qc), Canada (2007).