12th International Conference on Information Fusion
Seattle, WA, USA, July 6-9, 2009

An application of *DSmT* in ontology-based fusion systems

Ksawery Krenc
RS-SD
R&D Marine Technology Centre
Gdynia, Poland
ksawery.krenc@ctm.gdynia.pl

Adam Kawalec
The Institute of Radioelectronics
WAT Military University of Technology
Warsaw, Poland
Adam.Kawalec@wat.edu.pl

Abstract – *The aim of this paper is to propose an ontology framework for preselected sensors due to the sensor networks' needs, regarding a specific task, such as the target's threat recognition. The problem will be solved methodologically, taking into account particularly non-deterministic nature of functions assigning the concept and the relation sets into the concept and relation lexicon sets respectively and vice-versa. This may effectively enhance the efficiency of the information fusion performed in sensor networks.*

Keywords: Attribute information fusion, *DSmT*, belief function, ontologies, sensor networks.

1 Introduction

Ontologies of the most applied sensors do not take into account needs of sensor networks [1]. Sensors, in particular the more complex ones, like radars or sonars are intended to be utilized autonomously.

The foundation of the sensor networks (*SN*), comprehended as the networks of cooperative monitoring, is *understanding* information obtained from some elements by another ones. Thus the question of *the common language* is very important. The ontology of sensor network should be unified and structured.

The key problem in this paper is neither a direct application of existing solutions in the field of ontologies for the sensor networks nor a design of a new ontology, ready to implement. The aim is to propose the ontology framework for networks, consisting of preselected sensors, due to the sensory needs, to perform a specific task, such as recognizing the target threat.

The selection of the sensors will be taken in four particular steps, namely:

1. Describing, what particular pieces of information are required to define the target threat;

2. Describing, what particular sensors enable to gain the mentioned pieces of information;

3. Identification of all information possible to acquire by preselected sensors;

4. The specific sensor selection;

2 Sensor type selection

This section focuses on creating the ontology of a sensor network, processing information related to the target threat attribute. Mentioned information may be classified, according to its origin, as:

- Observable – originated directly from sensors or visual sightings;
- Deductable (abductable) – designated by the way of deductive reasoning, based on the other observable attributes, gathered previously;
- Observable and deductable – designated both: on the basis of observation and by the way of deductive reasoning;
- Confirmed – verified by other information center or external sensor network;

The observable attributes may be defined based on information originated from diverse sensors. For the purpose of this paper the scope of sensors (possible to utilize) will be constrained to the set, which in the authors' opinion fully reflects the required information about the target in the real world.

It is a very important assumption that the selection of sensor types is conditioned ontologically. That means neither any particular sensor model nor communication protocol nor any other element of the *SN* organizations will be discussed.

From the observer's point of view (whose main duty is to assess the target threat) it is important to define the following features of the target:

- Key attribute of the target: the threat (based on observations);
- Additional target attributes (as the basis for deduction reasoning about the threat) i.e. the platform, (frigate, corvette, destroyer) and the activity (attack, reconnaissance, search & rescue);
- Auxiliary characteristics: target position;

2.1 Types of sensors

Preselected target features may be registered by various means of observation, namely:

- Position: Radar (all spatial dimensions), sonar, IR sensor (mostly to define target azimuth and elevation);
- Threat: IFF, visual sightings (human), video camera (daylight or noctovision);
- Platform: visual sightings, video camera, thermo-vision camera;
- Activity: visual sightings.

The above statement may be regarded as a pre-selection of sensor set, used in the following considerations of this paper. It is important to notice, that some of the mentioned sensors may acquire information related to more than one attribute. Therefore, a reversed assignment (sensors to attributes) seems to be more adequate.

2.2 Sensor-originated information

Figure 1 presents the preselected target features and their inclusion relations. Additionally, it was pointed out the example sensors, which enable to acquire the mentioned information.

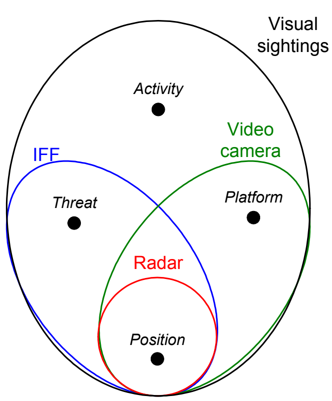

Figure 1 Information scope originated from diverse types of sensors.

It should be noted that although some of these sources allow for obtaining information on more than one attribute, it is possible to identify a hierarchy of relevance of this information. That means that some of the attributes, however, possible to reveal from multiple sources, for some sources perform the primary information while for others the secondary information:

- Radar: position[1];
- IFF: position, threat;
- Video camera: position, platform, threat;
- Visual sightings: position, threat, platform, activity;

For visual sightings, where the human plays the role of the sensor, it is difficult to identify the primary information. Among the above sources the visual recognition is the most reliable way of defining the target activity. Therefore, taking into account the fact that it allows to identify the target threat and platform, the visual recognition may be considered as a specific source of information.

These observations are highly important for future considerations, which will be effectively used in creation of the hierarchy of the concept lexicons as well as in defining the relations among concepts of *SN* ontology.

Some of these sensors perform very complex devices and require the introduction of certain interfaces, allowing the automatic acquisition of useful information (in terms of sensor networks). An example of such a sensor is a video camera. In order to make effective use of an image from the video camera a specific module is necessary to interpret the taken picture, identifying the significant features of the object of interest. In that case, the ontology, the video camera is defined in that very module and it is modifiable as long as there is access to the configuration of that module. This leads to another possible classification of sensors:

- Constant (invariant) ontology sensors, e.g. IFF;
- Variant ontology sensors, e.g. video camera equipped with interpretation module or visual sightings;

Guided by the principle of maximum information growth, in next stages of creating the *SN* ontology the following sources of attribute information will be taken into account: IFF, video camera (*VC*) and visual sightings (*VS*).

3 Defining sets of *SN* ontologies

Referring to a taxonomy of the term of *ontology* [1] the authors would like to notice that the problem of *SN* ontology concerns, in particular, the so-called *method and task ontologies*.

There have been effectively utilized concept lexicons of *Joint C3 Information Exchange Data Model*

[1] Underline means the prime information.

[2], constraining the considerations to three of the *JC3* model attributes:

- threat: *object-item-hostility-status-code*;
- platform: *surface-vessel-type-category-code*;
- activity: *action-task-activity-code*;

While defining the attribute relation functions, the Dezert-Smarandache Theory (*DSmT*) of plausible and paradoxical reasoning has been utilized [3].

3.1 Rules for sensor network ontologies selection

In section 2.2 there was proposed a sensor distinction for variant and invariant ontology sensors. Considering this division is fundamental while creating *SN* ontology, which takes place in four stages:

1. Creating the fundamental concept lexicon for a sensor network, based on invariant concept lexicons of particular sensors;
2. Creating the auxiliary concept lexicon for sensor network, based on variant concept lexicons of particular sensors;
3. Extending the fundamental concept lexicon with the auxiliary lexicon;
4. Defining relations among the concepts in sensor network;

According to the definition of ontology, given in [4], [5], *SN* ontology may be formulated as follows:

$$O = \left\langle L, F, G, \overline{F}, \overline{G}, C, R \right\rangle \tag{1}$$

where:

L – is either concept or relation lexicon;
F – lexicon elements to concepts assigning function; G – lexicon elements to relations assigning function; $\overline{F}$ – a function reversed to F, assigning concepts to elements of the concept lexicon; $\overline{G}$ – a function reversed to G, assigning relations to elements of the relation lexicon; C – a set of the whole concepts used in *SN*; R – a set of the whole relations used in *SN*.

According to the lexicons of *JC3* model, the above mentioned concepts and functions will be defined in the following subsections.

3.1.1 Concepts

Concepts are representations of a certain group of objects of the same characteristics, which may be directly identified by selected subset of elements of the concept lexicon [5]. That means, that assigning for example an attribute ‘hostile target’ to a target uses the concept of the ‘hostile target’, which is the element of the set (C) of all possible concepts for a given sensor network.

Another question is a representation of the concept ‘hostile target’ in the language of the particular source. For instance: for IFF device it will be the value of ‘FOE’, and for a video camera the value, defined in the interpreting module as ‘HOSTILE’.

Mathematically, the F assignment is not a bijection in general, moreover: it is not a function. In case multiple sources are utilized, the F is not an injection, whereas if the concept set is ‘rich’, comparably to the ‘poor’ lexicon the $\overline{F}$ is not injective. This may occur if the *SN*, prepared for defining fully target threat, is used for deciding whether the target is either friend or hostile. Then, the $\overline{F}$ will interpret concepts of ‘training hostile’, ‘training suspect’ and ‘assumed friend’ as ‘friend’ assigning the lexical value of ‘FRIEND’ [6].

In order to illustrate F and $\overline{F}$ assignment it is suggested to consider the following example.

<u>Example 1</u>: Let the set of concepts be defined as follows:

$$C = \{\text{‘friend’}, \text{‘assumed friend’}, \text{‘assumed hostile’}, \text{‘hostile’}\} \tag{2}$$

and the concept lexicon is defined as follows:

$$Lc = \{FRIEND, HOSTILE, ASSUMED\} \tag{3}$$

Thus, it is possible to define subsets of the concept lexicon elements in such a way that the F assignment would be a bijection (Figure 2).

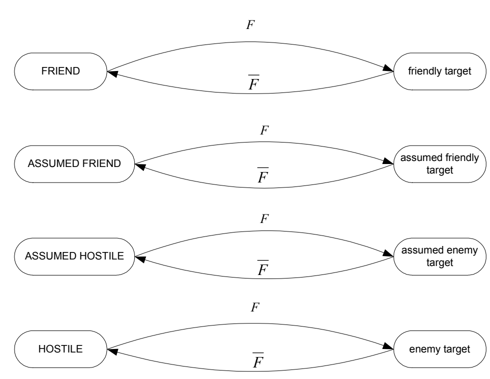

Figure 2 F-assignment as a bijection.

Defining subsets of lexical elements as singletons leads to non-function *F* assignment (Figure 3).

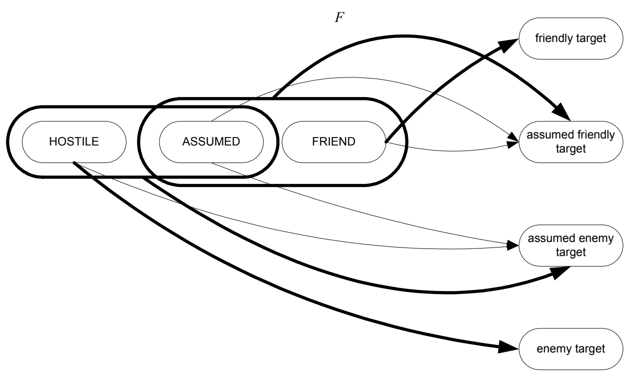

Figure 3 *F* as a non-function assignment.

In case of 'rich' concept lexicon sets it is important to express subsequent target types as conjunctions of their distinctive features.

Example 2:

Table 1 Example definitions of surface platforms

Transporter	AUX $\wedge$ AIR $\wedge$ D $\wedge$ TRAN
Command	AUX $\wedge$ S&MCAL $\wedge$ AIR $\wedge$ C2

where:

AUX – auxiliary vessel;
S&MCAL – equipped with artillery of small and medium caliber;
AIR – against the air targets;
D – performs landing operations;
C2 – command & control;
TRAN – transport of landing forces;

3.1.2 Relations

Relations define the relationships among concepts. Relation may be hierarchical or structural. Moreover, for the purpose of sensor networks, they may be classified as:

- Relations I, among the observable attributes of a diverse type;
- Relations II, among attributes of miscellaneous origin;
- Relations III, among the identical attributes, originated from diverse sources;

Relations among the observable attributes of a diverse type enable a deduction of some attributes values based on observable values of another ones. For instance: the relations between the threat and the platform of the target enable the deduction of target activity. Linking the subsequent observable attributes is performed according to mentioned in previous section distinctive features of the target. This means that for example: defining (based on observations) the target platform is equal to assigning to the target some of distinctive features, which the target, performing the particular activity, has to possess.

Relations among attributes of miscellaneous origin: observable and deductable result in so-called observable-deductable attribute. The effective information fusion from multiple sources is performed according to the rules of combination and conditioning, obtained from *DSmT* [7], [8]. This process is going to be described in details in section 3.2.

Relations among the identical attributes, originated from diverse sources are the type of relations, where the key question is a lexical variety of concepts used by particular sources. For instance: the threat attribute value acquired from IFF may be either FRIEND or FOE, whereas the same attribute obtained from visual sightings may be of {FRIEND, HOSTILE, UNKNOWN, JOKER, FAKER,…}. In such a case a value of FRIEND, gained from IFF, corresponds to the exact value of the visual sightings. The value of FOE is equal to HOSTILE, whereas the relations among values of FRIEND, gained from IFF and FAKER (or JOKER), gained from the visual sightings are not so obvious and they must be defined, according to the definitions of these training types (JOKER, FAKER).

3.2 Proposition of sensor network ontology

This section presents a proposition of an ontology framework for a sensor network, dedicated to monitor the target threat. In the solution there were utilized concepts and concept lexicons of *JC3* model. The authors' intention was to show the way relations of three attributes (threat, platform and activity) should be defined, rather than to present the complete *SN* ontology.

Table 2 presents a bijective assignment of concepts to elements of a concept lexicon. As it was mentioned before, this assignment need not be a bijection, however it is desirable especially if sets of values for attributes of platform and activity are numerous.

Table 2 *SN* ontology: concepts and concept lexicon.

Concepts		**Concept lexicon**	
Threat	An OBJECT-ITEM that is assumed to be a friend because of its characteristics, behavior or origin.	***object-item-hostility-status-code***	ASSUMED FRIEND
	An OBJECT-ITEM that		HOSTILE

	is positively identified as enemy.		
	…according to JC3		… according to JC3
Platform	General designator for aircraft/multi-role aircraft carrier;	***surface-vessel-type-category-code***	AIRCRAFT CARRIER, GENERAL
	Craft 40 meters or less employed to transport sick/wounded and/or medical personnel.		AMBULANCE BOAT
	… according to JC3		… according to JC3
Activity	To fly over an area, monitor and, where necessary, destroy hostile aircraft, as well as protect friendly shipping in the vicinity of the objective area.	***action-task-activity-code***	PATROL, MARITIME
	Emplacement or deployment of one or more mines.		MINE-LAYING
	… according to JC3		… according to JC3

The assignment of relations among attributes to relation lexicons (Table 3) is a surjection. In order to define the relations among attributes *DSmT* combining and conditioning rules have been applied. The preferred rule for conditioning is the rule no. 12. When combining evidence, there is a possibility to use many combination rules, depending the particular relation. However, for simplicity, it is suggested to apply the classic rule of combination (*DSmC*), which has properties of commutativity and associativity.

Table 3 *SN* ontology: relations and relation lexicon.

Relations		**Remarks**	**Relation lexicon**
Rel. I:	*cond(.)*	Based on *DSmT*	*Conditioning*
	$\rightarrow$	According to distinctive features	*Implication*
Rel. II:	*cond(.)*	Based on *DSmT*	*Conditioning*
	$\oplus$	Based on *DSmT*	*Combination*
Rel. III:	*cond(.)*	Based on *DSmT*	*Conditioning*
	$\oplus$	Based on *DSmT* (combination rule need not be identical with one in Relations II)	*Combination*

Below, there have been presented examples of particular types of relations. In case of the relation of type I it is possible to reason about a value of a certain attribute, based on the knowledge about the other ones. However, if the unambiguous deduction of the third attribute is not possible, due to the majority of possible solutions, an application of abductive reasoning (selection of the optimal variant) seems to be justified.

Relations I:

(Threat, Platform) $\rightarrow$ *Activity: (FAKER, FRIGATE TRAINING)* $\rightarrow$ *TRAIN OPERATIONS*;
(Threat, Activity) $\rightarrow$ *Platform: (FAKER, TRAIN OPERATIONS)* $\rightarrow$ *TRAINING CRAFT*;
(Platform, Activity) $\rightarrow$ *Threat: (HOUSEBOAT, PROVIDE CAMPS)* $\rightarrow$ *NEUTRAL*;

Relations II:

$FAKER = cond(obs(FAKER) \oplus ded(FAKER) \oplus obs(FRIEND))$;

Relations III:

$FAKER = cond(obs(FAKER) \oplus VS(FAKER) \oplus IFF(FRIEND))$;

The abductive reasoning process may be systemized by application of *DSmT*, where the selection of the optimal value takes place after calculating the basic belief assignment.

<u>Example 3:</u>

(Threat, Activity) $\rightarrow$ *Platform: (FRIEND, MINE HUNTING MARITIME)* $\rightarrow$
MINEHUNTER COASTAL (MHC) $\vee$
MINEHUNTER COASTAL WITH DRONE (MHCD) $\vee$ *MINEHUNTER GENERAL (MH)* $\vee$
MINEHUNTER INSHORE (MHI) $\vee$
MINEHUNTER OCEAN (MHO) $\vee$
MINEHUNTER/SWEEPER COASTAL (MHSC) $\vee$
MINEHUNTER/SWEEPER GENERAL (MHS) $\vee$
MINEHUNTER/SWEEPER OCEAN (MHSO) $\vee$
MINEHUNTER/SWEEPER W/DRONE (MHSD)

Applying *DSmT*, for each of possible hypothesis a certain mass of belief is assigned, e.g.:

$m(MHC) = 0.2$, $m(MHCD) = 0.3$, $m(MH) = 0.1$, $m(MHI) = 0.1$,$m(MHO) = 0.1$, $m(MHSC) = 0.05$, $m(MHS) = 0.05$, $m(MHSO) = 0.05$, $m(MHSD) = 0.05$

Based on the obtained *basic belief assignment* (*bba)* belief functions, referring to particular hypotheses, may be calculated. In the simplest case, assuming all of the hypotheses are exclusive, the subsequent belief functions will be equal to respective masses, e.g. $Bel(MHC) = m(MHC)$, $Bel(MHCD) = m(MHCD)$, etc.

More complex case, where relationships among hypotheses are taken into account will be considered in the next section.

4 Verification of the usefulness of elaborated ontology sets

The presented framework of the *SN* ontology, for the purpose of the target threat assessment, requires a verification. Particularly, it is important to verify the correctness of reasoning processes and a combination of the reasoning results with observation information.

The proposed solution substantially differs from the existing deterministic ontology-based methods because it introduces explicitly the uncertainty of the relations among target attributes. Therefore this section was meant to focus on the verification of these relation reasoning mechanisms rather than the completeness of the target representation by the sensor network.

4.1 Assumptions

In order to verify the usefulness of the proposed ontology framework, a specially designed demonstrator application for evaluation of the target threat information has been used. This application enables a simulation of acquiring of information from diverse sources, like: radar, video camera and visual sightings.

It is assumed that the visual sighting is also a source of information about a target platform and a target activity. The *bba* values for platform and activity attributes have been assigned arbitrary. During experimentation the observable attributes as well as deductable attributes have been taken into account. Frames of discernment for observation and deduction may differ in general. For the purpose of verification of proposed ontology sets, an example from the section 3.2 is to be considered. Additionally it is assumed:

- Application of the hybrid *DSmT* model:
    - The hypotheses are not exclusive;
    - The hypotheses correspond to the JC3 model terminology;
- In relations of type II and III the hybrid rule of combination (*DSmH)* has been applied;
- The conditioning rule no. 12 has been used for updating evidences;

4.2 Numerical experiments

Figure 4 shows a randomly generated trajectory of the target of which the threat value is at stake. Observations are taken from three sources (visual sightings, radar system - IFF and video camera) synchronously.

The green color means successively acquired observations for each of the sources. The red color means the observations impossible to acquire because the target was outside of the detection zone for a particular source [3].

Taking for example the last sample, the respective *bba* are as Table 4 shows.

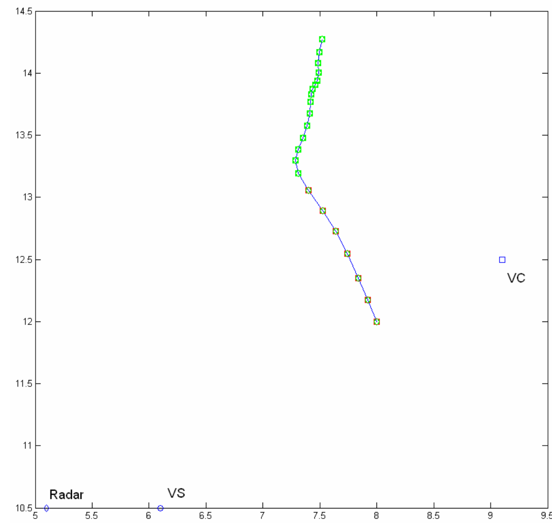

Figure 4 Randomly generated target trajectory and its threat evaluation based on radar, *VS* and *VC* observations.

Table 4 *Bba* gathered from diverse sources: visual sightings, video camera and radar.

Threat	Visual Sightings	Video Camera	Radar/IFF
HOS	0.0024	0.0004	0.0008
UNK	0.0060	0.0012	-
NEU	0.0068	0.0015	-
JOK	0.0109	-	-
FRD	0.2400	0.4368	0.8773
FAK	0.0292	0.0049	0.0119
SUS	0.0032	0.0005	0.0011
AFR	0.0215	0.0046	0.0088
PEN	0.6800	0.5500	0.1000

A relation of type III of combining information from IFF and the visual sightings results in acceptance the target is friendly:

$$Threat_{VS} \oplus Threat_{IFF} \equiv FRIEND \tag{4}$$

From the visual sightings it is also acquired that the target activity is mine-hunting (*MINE HUNTING MARITIME*). Thus, the relation of type I, between the threat and the activity attribute results in selection of the target platform, related to searching for mines.

$$(FRIEND,\ MINE\ HUNTING\ MARITIME) \rightarrow platform \tag{5}$$

In the considered case it is assumed the frame of discernment of the *platform* attribute originated from the video camera is defined as follows:

$$\Theta_{VC} = \{MHC, MHI, MHO, MSC, MSO, D\} \quad (6)$$

where:

MHC – MINEHUNTER COASTAL;
MHI – MINEHUNTER INSHORE;
MHO – MINEHUNTER OCEAN;
MSC – SWEEPER COASTAL;
MSO – SWEEPER OCEAN;
D – DRONE;

Additionally, with $\cup$ and $\cap$ operators the secondary hypotheses may be created, which refer to another values of the *platform* attribute (*surface-vessel-type-category code*) of *JC3* model:

$MHC \cup D$ = *MHCD (MINEHUNTER COASTAL WITH DRONE);*

$MHI \cup MHO \cup MHC \cup D$ = *MH (MINEHUNTER GENERAL);*

$MHO \cap MSO$ = *MHSO (MINEHUNTER/SWEEPER OCEAN);*

$(MHC \cap MSC) \cup D$ = *MHSD (MINEHUNTER/SWEEPER W/DRONE);*

$(MHO \cap MSO) \cup (MHC \cap MSC) \cup D$ = *MHS (MINEHUNTER/SWEEPER GENERAL);*

The basic belief assignment for the video camera observation may be defined as follows:

$m_{VC}(MHC) = 0.1$, $m_{VC}(MHCD) = 0.1$,
$m_{VC}(MSC) = 0.2$, $m_{VC}(MHI) = 0.3$,
$m_{VC}(MHO) = 0.2$, $m_{VC}(MSO) = 0.1$,

Due to the implication (5) the above *bba* may be modified according to BCR12 with a following condition:

$$Cond : Truth = MHC \cup MHO \cup MHI \quad (7)$$

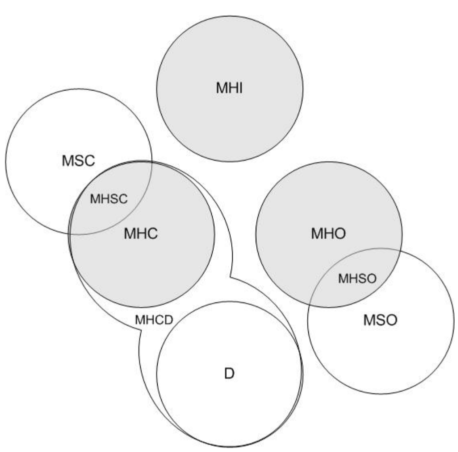

Figure 5 Venn's diagram for the platform attribute. The truth is grey colored.

Thus, the resulting *bba* for the platform attribute is updated, as follows:

$m_R(MHC|Cond)=m_{VC}(MHC)+m_{VC}(MHCD)=0.2,$
$m_R(MHSC|Cond)=m_{VC}(MSC)=0.2,$
$m_R(MHI|Cond)=m_{VC}(MHI)=0.3,$
$m_R(MHO|Cond)=m_{VC}(MHO)=0.2,$
$m_R(MHSO|Cond)=m_{VC}(MSO)=0.1,$

which, after calculating the respective belief and plausibility functions, leads to acceptation of the hypothesis of *MHC (MINEHUNTER COASTAL)* for the platform attribute of the whole sensor network.

It is worth of notice that the belief function for *MHC* before updating is of the least value since:

$$Bel_{VC}(MHC) = m_{VC}(MHC) = 0.1 \quad (8)$$

After updating, due to the fact that $m_{VC}(MHSC)$ supports the belief in *MHC* hypothesis, this hypothesis becomes the most credible since:

$$Bel_R(MHC) = m_R(MHC) + m_R(MHSC) = 0.4 \quad (9)$$

5 Conclusions

The results of the numerical experiments, presented in the previous section, have proven that the application of *DSmT* for the purpose of defining relations among target attributes, gives the possibility of unification of information acquired from sensors as well as obtained based on the deductive reasoning. That influences effectively the whole *SN* ontology, due to the fact the *SN* concept lexicon becomes substantially modified. It does not provide a union of lexicons for each sensor, which would be expectable in the deterministic case. The *SN* concept lexicon becomes extended with intersections and unions of the hypotheses created upon the lexicons of particular sensors.

During the experiments it has been utilized the *JC3* model's lexicon of *surface-vessel-type-category-code* attribute. It is important to notice, that despite its large volume, the lexicon is not structured. Thus, an emerging conclusion occurs, that setting *JC3* lexicons in a hierarchy would bring tangible benefits due to the fact that the hierarchy enables creating the hypotheses using $\cup$ and $\cap$ operators more effectively, and this in turn increases the precision of the reasoning processes based on information acquired from sensors.

Acknowledgements

The research work described in this document is a part of extensive works devoted to sensor networks in NEC environment. It was financed with science means from 2007 to 2010 as an ordered research project.

References

[1] K. Krenc: *An introductory analysis of the usefulness of sensor network organizations,* MCC Conference, Cracow, ISBN 83-920120-5-4, 2008.

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

[3] K. Krenc, 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] http://www.aifb.uni-karlsruhe.de/WBS/meh/publications/ehrig03ontology.pdf

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

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

[7] Florentin Smarandache, Jean Dezert, *Advances and Applications of DSmT for Information Fusion*, Vol 1, American Research Press Rehoboth, 2004.

[8] Florentin Smarandache, Jean Dezert, *Advances and Applications of DSmT for Information Fusion*, Vol 2, American Research Press Rehoboth, 2006.