PROCEEDINGS OF SPIE

SPIEDigitalLibrary.org/conference-proceedings-of-spie

Fusion of identification information from ELINT-ESM sensors

Tadeusz Pietkiewicz, Bronisław Wajszczyk

Tadeusz Pietkiewicz, Bronisław Wajszczyk, "Fusion of identification information from ELINT-ESM sensors," Proc. SPIE 10715, 2017 Radioelectronic Systems Conference, 107150F (19 April 2018); doi: 10.1117/12.2316489



Event: Radioelectronics Systems Conference, 2017, Jachranka, Poland

Fusion of identification information from ELINT-ESM sensors

Tadeusz Pietkiewicz^{*}, Bronisław Wajszczyk Institute of Radioelectronics, Military University of Technology Gen. S. Kaliskiego str. 2, 00-908 Warszawa, POLAND

ABSTRACT

This paper presents a method of fusion of identification (attribute) information provided by ELINT – ESM sensors (Electronic Intelligence – Electronic Support Measures). In the first section the basic taxonomy of attribute identification in accordance with the standards of STANAG 1241 ed. 5 and STANAG 1241 ed. 6 (draft) is adopted. These standards provide the following basic values of the attributes of identification: FRIEND, HOSTILE, NEUTRAL, UNKNOWN and additional values: ASSUMED FRIEND and SUSPECT. The last values can be interpreted as a conjunction of basic values. The basis of theoretical considerations is the Dezert-Smarandache theory (DSmT) of inference. This paper presents and practically uses combining identification information from different ELINT – ESM sensors one of the information fusion rules proposed by the DSmT - the Proportional Conflict Redistribution #5 rule (PCR5).

In the next section rules of determining attribute information by ESM sensor equipped with the data base of radar emitters are presented. It was proposed that each signal vector sent by the ELINT-ESM sensor contained an extension specifying a randomized identification declaration (hypothesis). This declaration specifies the reliability of the identification information - basic belief assignment (bba) for the identification information set. This paper presents a method of determining this belief assignment based on the distance between recognized signal features, vectors and centers of clusters grouping emitter patterns in the pattern data base. Results of the PCR5 rule of sensor information combining for two scenarios are presented in the final part of this paper. Conclusions are given at the end of this paper. They confirm the legitimacy of the use of the Dezert-Smarandache theory into information fusion for ESM sensors.

Keywords: identification information fusion, Dezert-Smarandache theory (DSmT) of inference, radar emitters recognition, ELINT, ESM

1. INTRODUCTION

ELINT – ESM (electronic intelligence – electronic support measures) electronic surveillance sensors consist of passive receivers and direction-finders, which allow them to capture emitter signals coming from different directions. In this way, the electronic recognition system can receive, among other things, information on radar emitters mounted on air platforms. Messages sent from ELINT - ESM sensors include, among other things, the features of the captured signal, the emitter azimuth and the identification information. The classification method depends on the organization that operates the ELINT – ESM sensors. This paper assumes that the identification classification of sensors is consistent with the NATO standard STANAG 1241 [1,2]. In addition, five identification classes are used - three primary and two secondary. This division is described in the next chapter. Sensors may send identification information in the form of a hard decision, otherwise referred to as non-randomized, or soft decision, otherwise referred to as randomized. It is assumed that sensors send identification information in a randomized form, i.e. in the form of basic belief assignment (bba) on a set of identification classes.

This assignment determines the sensor belief that the detected emitter belongs to the individual identification classes. Chapter four proposes a method for determining this assignment. It has been assumed that the procedure of recognizing a registered signal vector is to find such a signal pattern cluster center that lies closest to the recognized signal vector. This distance is the basis for determining the basic belief assignment value.

This paper also assumes that the sensors are equipped with a specialized database called the emitter database that stores information about previously captured, processed, analyzed, and described radar emitter signals along with additional information about the type and mode of the emitter work, the platform on which these emitters can be installed, and the

^{*} tadeusz.pietkiewicz@wat.edu.pl

²⁰¹⁷ Radioelectronic Systems Conference, edited by Adam Kawalec, Andrzej Witczak, Proc. of SPIE Vol. 10715, 107150F · © 2018 SPIE · CCC code: 0277-786X/18/\$18 · doi: 10.1117/12.2316489

national or organizational affiliation of these platforms. The detected signals are the subject of an analysis procedure which allows the determination of the distinctive features of the signal and then assigning this information to a particular electronic entity (already existing or created ad hoc). The basis for assigning distinctive information to a particular electronic entity is the azimuth angle of the incoming signal.

In the case of a high density of targets, identification information may fluctuate due to false assignments of signal information to an electronic entity [7]. Methods of estimating the position of electronic entities have been presented, among others, in papers [15,16,17]. Assuming that sensors send all reports on the tracked electronic entities to the superior operation center in the electronic recognition system, such a center can perform the fusion function of the identification information. In this paper, such a center has been called the information fusion center (IFC). The implementation of the identification information fusion will ensure the greater stability of this information - resistance to random sensor decision changes. The identification information fusion can be based on three basic theories – The Bayesian theory of inference, the Dempster-Shafer theory - called the theory of evidence, and the Dezert-Smarandache theory. The last theory previously mentioned has been used in this paper. Its application was due to the fact that two secondary identifications are the conjunctions (intersections) of basic identification.

ELINT-ESM sensors are deployed in the electronic recognition system at various locations of the responsibility area, hence sensor messages may be contradictory in some situations. The Dezert-Smarandache theory provides many tools for conflict redistribution in the context of the decision information fusion. These tools are called conflict redistribution rules. In this paper the Proportional Conflict Redistribution Rule # 5 has been used for combining identification information. It is presented in chapter 3.

The results of the identification information fusion for the simulation scenarios have been presented in the final part of this paper.

2. INTERPRETATION OF ATTRIBUTE IDENTIFICATION ACCORDING TO STANAG 1241

The set of possible values of attribute identification applied by the sensor can be determined on the basis of standardization documents of organizations exploiting these sensors [1,2,3,4,5,12].

This paper assumes a basic taxonomy of identification in accordance with the draft of STANAG 1241 ed. 6 [2]. To other similar documents one may include the following standards: STANAG 4420 and STANAG 1241 ed. 5, which provide the following basic values of the attribute identifications:

- FRIEND (F),
- HOSTILE (H),
- NEUTRAL (N),
- UNKNOWN (U).

Each of these documents contain their own definitions of the declarations.

The following definitions of these basic values of the attribute identification are used in the paper (in accordance with [2]):

- FRIEND an allied/coalition military track, object or entity; a track, object or entity, supporting friendly forces and belonging to an allied/coalition nation or a declared or recognized friendly faction or group,
- HOSTILE a track, object or entity whose characteristics, behaviour or origin indicate that it belongs to opposing forces or poses a threat to friendly forces or their mission,
- NEUTRAL a military or civilian track, object or entity, neither belonging to allied/coalition military forces nor to opposing military forces, whose characteristics, behaviour, origin or nationality indicates that it is neither supporting nor opposing friendly forces or their mission,
- UNKNOWN an evaluated track, object or entity, which does not meet the criteria for any other standard identity.

These standards bring additional values of the attribute identification:

ASSUMED FRIEND,

- SUSPECT.

One should pay attention on these two recent identities contained in [1] as well as their definitions [2]:

- ASSUMED FRIEND a track, object or entity which is assumed to be friend or neutral because of its characteristics, behaviour or origin,
- SUSPECT a track, object or entity whose characteristics, behaviour or origin indicate that it potentially belongs to opposing forces or potentially poses a threat to friendly forces or their mission.

From these definitions, it appears in the following graphic interpretation using the Venn diagram shown in Figure 1.



Figure 1. The interpretation of STANAG 1241 using the Venn diagram

3. BASICS OF DEZERT-SMARANDACHE THEORY

This section presents selected elements of the Dezert-Smarandache theory for plausible and paradoxical reasoning that have been used in this paper. They have been taken from [6,10,11].

Basic definitions:

• Basic set Θ . It's the set including every possible declaration θ_i . This set is exhaustive and its elements are not exclusive.

$$\boldsymbol{\Theta} = \{\boldsymbol{\theta}_1, \boldsymbol{\theta}_2, \dots, \boldsymbol{\theta}_n\}. \tag{1}$$

• Power set 2^{Θ} : represents the set of all possible sets using the declarations (singletons) of the basic set Θ . It includes the empty set and excludes intersections. With the basic set defined above, we get the power set:

$$\boldsymbol{2}^{\boldsymbol{\theta}} = \{ \emptyset, \{\theta_1\}, \{\theta_2\}, \dots, \{\theta_n\}, \{\theta_1 \cup \theta_2\}, \dots, \{\theta_1 \cup \theta_2 \cup \dots, \theta_n\}, \dots, \boldsymbol{\Theta} \}.$$
(2)

• Hyper-power set D^{Θ} : represents the set of all possible sets using the declarations of the basic set Θ and allowing intersections between singletons. It includes the empty set. For the basic set: $\Theta = \{\theta_1, \theta_2\}$, we get the hyper-power set

$$\boldsymbol{D}^{\boldsymbol{\Theta}} = \{ \emptyset, \{\theta_1\}, \{\theta_2\}, \{\theta_1 \cap \theta_2\}, \{\theta_1 \cup \theta_2\} \}.$$
(3)

When $\boldsymbol{\Theta} = \{\boldsymbol{\theta}_1, \boldsymbol{\theta}_2, \boldsymbol{\theta}_3\}$, we get $\boldsymbol{D}^{\boldsymbol{\Theta}} = \{\emptyset, \alpha_1, \alpha_2, \dots, \alpha_{18}\}$ and $\|\boldsymbol{D}^{\boldsymbol{\Theta}}\| = 19$.

Proc. of SPIE Vol. 10715 107150F-3

• Conjunctive Power set 2_{\cap}^{Θ} : represents the set of all possible sets using the declarations of Θ . It includes the empty set and excludes disjunctions. With the basic set $\Theta = \{\theta_1, \theta_2, ..., \theta_n\}$, we get the conjunctive power set:

$$\boldsymbol{2}_{\cap}^{\boldsymbol{\theta}} = \{ \emptyset, \{\theta_1\}, \{\theta_2\}, \dots, \{\theta_n\}, \{\theta_1 \cap \theta_2\}, \dots, \{\theta_1 \cap \theta_2 \cap \dots \cap \theta_n\} \}.$$
(4)

• Basic belief assignment (bba) *m*: function $2^{\Theta} \rightarrow [0,1]$, so the mass given to a set $A \subseteq \Theta$ obeying $m(A) \in [0,1]$.

Combining rules for data fusion

1) Conjunctive combining rule [8]: when we refer to the conjunctive combining rule, we will refer to the version described as:

$$m(\boldsymbol{A}) = m_1 \wedge m_2 = \sum_{\substack{\boldsymbol{B} \cap \boldsymbol{C} = \boldsymbol{A} \\ \boldsymbol{B}, \boldsymbol{C} \subseteq \boldsymbol{\Theta}}} m_1(\boldsymbol{B}) m_2(\boldsymbol{C}) \quad \forall \boldsymbol{A} \subseteq \boldsymbol{\Theta} \,.$$
(5)

2) Disjunctive combining rule [9]: When we refer to the disjunctive combining rule, we will refer to the version described as:

$$m(\boldsymbol{A}) = m_1 \vee m_2 = \sum_{\substack{\boldsymbol{B} \cup \boldsymbol{C} = \boldsymbol{A} \\ \boldsymbol{B}, \boldsymbol{C} \subseteq \boldsymbol{\Theta}}} m_1(\boldsymbol{B}) m_2(\boldsymbol{C}) \quad \forall \boldsymbol{A} \subseteq \boldsymbol{\Theta} \,.$$
(6)

3) Dezert-Smarandache rules of combination: the Dezert-Smarandache theory (DSmT) uses the hyper-power set thus being able to work with intersections. The DSmT possesses two rules of combination which are able to work around the mass redistribution problem of the DST in the presence of large conflicts:

• The Classical DSm (DSmC) rule of combination (DSmC);

• The Hybrid DSm (DSmH) rule of combination (DSmH).

• Instead of applying a direct transfer of partial conflicts onto partial uncertainties as with DSmH, the idea behind the Proportional Conflict Redistribution (PCR) rule [11] is to totally or partially transfer conflicting masses to non-empty sets involved in the conflicts proportionally with respect to the masses assigned to them by sensors as follows:

- calculation the conjunctive rule of the belief masses (1);
- calculation the total or partial conflicting masses;
- redistribution of the conflicting masses (total or partial) to the non-empty sets involved in the model proportionally with respect to their masses assigned by the sensors.

One of the PCR rules – PCR#5 [11] has been used in this paper. The PCR#5 rule is following:

$$m_{PCR5}(\emptyset) = 0.$$
⁽⁷⁾

2) $\forall A \in \mathbf{G} \setminus \emptyset$ occurs

1)

$$m_{PCR5}(A) = m_{12}(A) + \sum_{\substack{X \in G \setminus A \\ X \cap A = \emptyset}} \left[\frac{m_1(A)^2 \cdot m_2(X)}{m_1(A) + m_2(X)} + \frac{m_2(A)^2 \cdot m_1(X)}{m_2(A) + m_1(X)} \right]$$
(8)

Set *G* is a subset of the hiper-power set D^{Θ} ($G \subset D^{\Theta}$), in which there are no elements of the constraints power set D_c^{Θ} .

4. BASIC BELIEF ASSIGNMENT FOR ELINT-ESM SENSORS

An ESM sensor is a passive sensor that captures incoming electromagnetic signals initially generated by radar emitters mounted on air or maritime platforms. This sensor recognizes radar signals determining the values of their distinctive features [18,20]. In this paper we will not address the methods of radar signal recognition in details. However, we will use information about these methods to identify platforms that generate the signals according to STANAG 1241 – NATO Standardization Agreement and The Dezert-Smarandache theory. As previously it was described, we are interested in three basic values of identification: friend, hostile and neutral, and two secondary values: suspicious and assumed friendly. In addition, we will assume that in some situations it is not possible to determine the identification of the emitter carrier platform. To clarify this issue, we should briefly describe the method of determining the identification of the emitter carrier platform that generated the captured signal. The sensor recognition system is equipped with a database that can be divided into three components: a platform database, an emitter list and a geopolitical list [5,19,21]. The platform database (**PDB**) contains information about platforms that can be met in the area of interest along with their equipment with emitters. The emitter name list (**ENL**) includes all emitters corresponding to each platform of the PDB and contains the values of the distinctive signal features for each emitter. The values of distinctive features are the basis for the procedure of recognizing a captured signal. The geopolitical list (**GPL**) provides the allegiance of various countries and platforms and allows us to identify them in accordance with STANAG 1241.

The algorithm of signal recognition is realized in two stages:

- 1. Verification at the level of signal quality features. The second stage is executed after a positive assessment of the conformity of quality features.
- 2. The signal recognition procedure determines the distances between the distinctive features of the recognized signal and the distinctive features of all pattern signals stored within the emitter list.

Let us introduce the following notation:

 \boldsymbol{x}_{s} – vector of distinctive features of the recognized signal,

 \boldsymbol{x}_i - vector of distinctive features of *i*-th pattern signal (*i* - the number of the pattern signal, $i \in \overline{1, M}$),

 $d_{s,i} = d(\mathbf{x}_s, \mathbf{x}_i)$ - the distance between the distinctive features vector of the recognized signal and the distinctive features vector of *i*-th pattern signal; the distance $d_{s,i}$ is the Mahalanobis distance taking into account the correlations of the distinctive features.

The signal recognition classifier compares the distance $d(\mathbf{x}_s, \mathbf{x}_i)$ with the acceptable positive distance of the classification δ . The distance δ is the limit that we will interpret as a boundary of emitter pattern recognition. We will divide the set of pattern signals into two subsets: the patterns satisfying the positive classification condition in relation to the recognized signal $s - D_s^+$ and the patterns that do not satisfy the positive classification condition $-D_s^-$. The formal definition is as follows:

$$\boldsymbol{D}_{s}^{+} = \left\{ i \in \overline{1, M} : d_{s,i} \leq \delta \right\},\tag{9}$$

$$\boldsymbol{D}_{s}^{-} = \left\{ i \in \overline{1, M} : d_{s,i} > \delta \right\}.$$

$$(10)$$

In this paper we propose the following method of determining the basic belief assignment on a set of pattern signals, which is related to the distance between a signal and a pattern in the distinctive features space:

$$m_s(i) = e^{-d(\mathbf{x}_s, \mathbf{x}_i)}$$
 (11)

As one can see from the formula (14) if $d(\mathbf{x}_s, \mathbf{x}_i) = 0$ then $m_s(i) = 1$, whereas if $d(\mathbf{x}_s, \mathbf{x}_i) > 0$ then $1 > m_s(i) > 0$. The above measure is not normalized, hence we will standardize it

$$\widetilde{m}_{s}(i) = \frac{m_{s}(i)}{\sum\limits_{i=1}^{M} m_{s}(i)}.$$
(12)

The sum of the measures assigned to all the emitters, whose distinctive features lie outside the limit δ , will be treated as a measure assigned to the base hypothesis "unknown" (U)

$$\widetilde{m}_{s}(U) = \sum_{i \in D_{s}^{-}} \widetilde{m}_{s}(i).$$
(13)

To determine the belief measure of other base hypotheses (H, F, N) and secondary hypotheses (AF and S), we should introduce formal definitions of sets contained in the sensor database and used for recognition of captured signals. As it was mentioned above the set of all the necessary data for platform identification can be divided into three sets: PDB - a platform database, ENL - an emitter name list and GPL - a geopolitical list:

PDB – the platform database contains information about all platforms observed in the area of interest, including information on all emitters mounted on each platform; we assume that one platform can have many emitters and the same type of emitters can be installed on many platforms; the *PDB* also contains information concerning the national affiliation of each platform,

ENL – the emitter name list is a set of information about all recognized emitters in the area of interest; this set contains the mean values of the distinctive features of emitter signals (so-called signal patterns) and their standard deviations,

GPL – the geopolitical list contains the base values of identification attributes (H, F, N) assigned to the various countries.

We will also introduce additional notations used in this paper:

PDBL – the list of platform numbers that are stored in the **PDB**,

PL(i) – the set of numbers of platforms which have the emitter with number "i",

IPL(j) – the base identification attribute of the platform with number "j" determined on the basis of the information contained in **PDB** and **ENL** ($IPL(j) \in \{F, H, N\}$).

The set of signal patterns satisfying the positive classification condition in relation to the recognized signal *s* denoted as D_s^+ can be divided into disjunctive subsets according to the values of the carrier platforms identification features:

$$\boldsymbol{D}_{s}^{+} = \boldsymbol{D}_{s}^{+F} \cup \boldsymbol{D}_{s}^{+H} \cup \boldsymbol{D}_{s}^{+N} \cup \boldsymbol{D}_{s}^{+AF} \cup \boldsymbol{D}_{s}^{+S}, \qquad (14)$$

$$\boldsymbol{D}_{s}^{+k} \cap \boldsymbol{D}_{s}^{+l} = \emptyset, \ k \neq l, k, l \in \{F, H, N, AF, S\}.$$
(15)

Each subset of the set D_s^+ for the base identification is defined as follows:

$$\boldsymbol{D}_{s}^{+F} = \left\{ i \in \boldsymbol{D}_{s}^{+} : \forall j \in \boldsymbol{PL}(i) \ IPL(j) = F \right\},$$
(16)

$$\boldsymbol{D}_{s}^{+H} = \left\{ i \in \boldsymbol{D}_{s}^{+} : \forall j \in \boldsymbol{PL}(i) \ IPL(j) = \mathrm{H} \right\},$$
(17)

$$\boldsymbol{D}_{s}^{+N} = \left\{ i \in \boldsymbol{D}_{s}^{+} : \forall j \in \boldsymbol{PL}(i) \ IPL(j) = N \right\}.$$
(18)

In a similar way, one can define subsets of the set \boldsymbol{D}_{s}^{+} for the secondary identification (AF, S):

$$\boldsymbol{D}_{s}^{+AF} = \left\{ i \in \boldsymbol{D}_{s}^{+} : \exists \ j \in \boldsymbol{PL}(i) \ IPL(j) = F \land \exists \ j \in \boldsymbol{PL}(i) \ IPL(j) = N \right\},$$
(19)

$$\boldsymbol{D}_{s}^{+S} = \left\{ i \in \boldsymbol{D}_{s}^{+} : \exists \ j \in \boldsymbol{PL}(i) \ IPL(j) = \mathbf{H} \land \exists \ j \in \boldsymbol{PL}(i) \ IPL(j) = \mathbf{N} \right\},$$
(20)

Proc. of SPIE Vol. 10715 107150F-6

One can notice that in this paper we assume that no emitter type can be installed simultaneously on platforms with identifications F and H:

$$\left\{i \in \boldsymbol{D}_{s}^{+} : \exists j \in \boldsymbol{PL}(i) \ IPL(j) = F \land \exists j \in \boldsymbol{PL}(i) \ IPL(j) = H\right\} = \emptyset.$$
(21)

Introducing the definition of subsets of the set D_s^+ allows us to determine the belief masses for all identification features:

$$\widetilde{m}_{s}(F) = \sum_{i \in D_{s}^{+F}} \widetilde{m}_{s}(i), \ \widetilde{m}_{s}(H) = \sum_{i \in D_{s}^{+H}} \widetilde{m}_{s}(i), \\ \widetilde{m}_{s}(N) = \sum_{i \in D_{s}^{+N}} \widetilde{m}_{s}(i),$$
(22)

$$\widetilde{m}_{s}(AF) = \sum_{i \in D_{s}^{+AF}} \widetilde{m}_{s}(i), \widetilde{m}_{s}(S) = \sum_{i \in D_{s}^{+S}} \widetilde{m}_{s}(i).$$
(23)

One should emphasize that the method presented here is different than in [6,7]. These papers assume that ESM sensors can only generate basic declarations with attribute values FRIEND,HOSTILE and NEUTRAL but in this paper we assume, that ESM sensors can generate declarations from an extended set of attribute values (additionally ASSUME FRIEND, SUSPECT and UNKNOWN).

5. NUMERICAL EXPERIMENTS

5.1 Typical simulation scenarios

The paper [7] presents a typical simulation scenario for testing the identification information fusion. The authors formulated several requirements that should be met by such a scenario. It should:

- 1) adequately represent the known ground truth of the emitter identification,
- include sufficient numbers of incorrect associations to be realistic and to test the robustness of the rules to temporary incorrect sensor decisions,
- 3) provide only partial knowledge about the ELINT-ESM sensor declarations, and thus contain uncertainty,
- 4) allow to show stability in case of countermeasures,
- 5) allow to switch identification when the ground truth changes.

The authors [7] propose the following parameters of the scenario:

- 1) ground truth of identification is FRIEND (F) for the first 50 iterations of the scenario and HOSTILE (H) for the last 50 iterations,
- 2) the number of correct associations is 80% of all iterations, the number of incorrect associations caused by countermeasures is 20% of all iterations in a randomly selected moments of time,
- 3) ELINT-ESM sensor declarations have a mass of 0.7 for the most credible identification and 0.3 for the identification of UNKNOWN (U).

The assumption 5) has not been considered in this paper, assuming that the real object does not change its real identity while performing the mission. The following assumptions concerning the parameters of the scenario have been made:

- 1) the real value of identification is constant in each scenario and is equal to FRIEND (F) in the first scenario and HOSTILE (H) in the second scenario;
- 2) the above declarations are transmitted by sensor number 1 with the real identification mass equal to 0,7 and the mass of complementary identification (UNKNOWN) equal to 0,3;
- 3) the second sensor shall transmit its declarations in accordance with the tables 1 and 2 for the scenarios 1a and 1b and with the tables 3 and 4 for the scenarios 2a and 2b.

Table 1. Belief mass values for the second sensor for the scenario 1a

Type of identification	F	N	Н	$N \cap F$	$N \cap H$	U
Correct identification (80% of events)	0.6	0.1	0	0.2	0	0.1
Incorrect identification (20% of events)	0	0.1	0.6	0	0.2	0.1

Table 2. Belief mass values for the second sensor for the scenario 1b

Type of identification	F	N	Н	$N \cap F$	$N \cap H$	U
Correct identification (80% of events)	0.7	0.1	0	0.1	0	0.1
Incorrect identification (20% of events)	0	0.1	0.7	0	0.1	0.1

Table 3. Belief mass values for the second sensor for the scenario 2a

Type of identification	F	N	Н	$N \cap F$	$N \cap H$	U
Correct identification (80% of events)	0	0.1	0.6	0	0.2	0.1
Incorrect identification (20% of events)	0.6	0.1	0	0.2	0	0.1

Table 4. Belief mass values for the second sensor for the scenario 2b

Type of identification	F	N	Н	$N \cap F$	$N \cap H$	U
Correct identification (80% of events)	0	0.1	0.7	0	0.1	0.1
Incorrect identification (20% of events)	0.7	0.1	0	0.1	0	0.1









Figure.3. Scenarios 2a i 2b for the sensor 1





Proc. of SPIE Vol. 10715 107150F-8



One should note that scenario 1b differs from scenario 1a by the greater belief of mass assigned to the incorrect identification of the recognized emitter. Similar differences concern scenarios 2b and 2a.

Scenarios 1a, 1b and 2a, 2b for the sensor 1 have been presented in Figures 2 and 3 (respectively). All scenarios for the sensor 2 have been presented in Figures 4, 5, 6 and 7.

5.2 Simulation configuration

ELINT - ESM sensors work asynchronously in the electronic recognition system. In the same way, the simulator of the information fusion center (IFC) should work. It can be assumed that signal vectors, which are sensor messages, are processed in the information fusion center sequentially. The information fusion in IFC means combining a signal vector sent by any of the ELINT - ESM sensors with a generalized signal vector as a part of an electronic entity record in the IFC. The general diagram of the simulation system has as many inputs as ELINT - ESM sensors cooperate with the IFC. In this paper the number of sensors have been reduced to two - the first sensor sent the messages containing the actual identification values, while the second sensor sent the messages containing disrupted information. The simulation diagram of the test system is shown in Figure 8. The messages from the first and second sensors are sent to the IFC alternately.



Figure. 8. General diagram of signal vector processing from ELINT – ESM sensors in the information fusion center IFC. Notation in the figure: \boldsymbol{v}_s^i - signal vector from *i*-th sensor (*i*=1,2), \boldsymbol{v}_s^{IFC} - generalized signal vector - a part of an electronic entity record, EER – electronic entity record in IFC, PDB – pattern data base in IFC.

5.3. Numerical results

The results of simulation of identification information fusion are presented for scenarios 1a and 1b in Figures 5 and 6 and for scenarios 2a and 3b in Figures 7 and 8 respectively.

The presented results (Figures 9-12) show that the method of information fusion allows us to draw correct conclusions about the actual identification of the recognized object. The application of the decision threshold for the belief mass at the level m_{α} =0,45 allows us to properly evaluate the identification of the recognized object: for scenario 1a – FRIEND and for scenario 2a – HOSTILE. Applying the same decision threshold to scenarios 1b and 2b basically allows us to identify objects properly, but in one case for each of these scenarios such a threshold leads to incorrect decisions. This was due to the fact that the sensor 2 sent incorrect identification information with a high value of belief mass (0.7).



Figure 9. Values of the result belief mass for the scenario 1a



Figure.11. Values of the result belief mass for the scenario 2a



Figure.10. Values of the result belief mass for the scenario 1b



Figure 12. Values of the result belief mass for the scenario 2b

6. CONCLUSIONS

The proposed basic belief assignment model for ELINT-ESM sensors can be used to build identification information fusion systems. Practical meaning have, first of all, models conformable to STANAG 1241. It contains definitions of identification values corresponding to the intersections of basic identification declarations. Therefore in this work, the Dezert-Smarandache theory has been used to determine the basic belief assignment for declarations sent by ELINT-

ESM sensors. The presented method of determining randomized ELINT-ESM sensor declarations is based on the results of electronic signal measurements and the data contained in specialized hierarchical databases of signal patterns and their emitters. An extension of the standard reports on detected signals with randomized identification declarations allows us to use methods of identification information fusion in the information fusion center. The elaborated method of determining the basic belief assignment can also be applied directly in the information fusion center when the sensors send only randomized declarations for the basic identification values, and even when the sensors send only non-randomized declarations. The information fusion center should have a specialized database of signal patterns and their emitters so that the described information fusion can be implemented.

Further work in this area should include the development of other methods of determining the basic belief assignment on a set of possible identification declarations and the assessment of the effectiveness of other methods of combining identification information in the information fusion center.

REFERENCES

- [1] [NATO Standardization Agreement STANAG No. 1241 . NATO Standard Identity Description Structure for Tactical Use, Ed. 5], North Atlantic Treaty Organization (April 2005).
- [2] [NATO Standardization Agreement STANAG NO. 1241 AO. NATO Joint Standard Identification Description, Ed. 6, Ratification Draft 1], North Atlantic Treaty Organization (27 October 2009).
- [3] [NATO Standardization Agreement STANAG No. 5516, Tactical Data Exchange Link 16, Ed. 3], North Atlantic Treaty Organization.
- [4] [NATO Standardization Agreement STANAG No. 4162, Identification Data Combining Process, Ed. 2], North Atlantic Treaty Organization.
- [5] Valin, P., Bossé E., "Using A Priori Databases for Identity Estimation through Evidential Reasoning in Realistic Scenarios", RTO IST Symposium on Military Data and Information Fusion, RTO-MP-IST-040, Prague, Czech Republic, 12-1 – 12-12, (20-22 October 2003).
- [6] Djiknavorian P., Grenier D., Valin P., "Analysis of information fusion combining rules under the DSm theory using ESM input", 10th International Conference on Information Fusion, FUSION 2007, Québec, Canada,1-8 (9-12 July 2007). doi: 10.1109/ICIF.2007.4408128
- [7] Djiknavorian P., Grenier D., Valin P., "DSm theory for fusing highly conflicting ESM reports", 12th International Conference on Information Fusion, Seattle, WA, USA, 1211-1217 (July 6-9, 2009).
- [8] Smets PH., Kennes R., "The transferable belief model", Artificial Intelligence, Vol. 66, 191-234 (1994). doi.org/10.1016/0004-3702(94)90026-4.
- [9] Smets PH., "Belief functions: the disjunctive rule of combination and the generalized Bayesian theorem", International Journal of Approximate Reasoning, Vol. 9, 1-35 (1993). doi.org/10.1016/0888-613X(93)90005-X.
- [10] Smarandache F., Dezert J., editors, [Advances and Applications of DSmT for Information Fusion, vol. 1], American Research Press (2004).
- [11] Smarandache F., Dezert J., editors, [Advances and Applications of DSmT for Information Fusion, vol. 2], American Research Press (2006).
- [12] Krenc K., Kawalec A., Pietkiewicz T., "Definition of bba and quality of fusion in C2 systems", 14th International Conference on Information Fusion, FUSION 2011, Chicago, 1-8 (2001), ISBN: 978-1-4577-0267-9.
- [13] Pietkiewicz T., Kawalec A., "A method of determining the basic belief assignment for combined primary and secondary surveillance radars based on Dezert-Smarandache theory", The 17th International Radar Symposium (IRS), Kraków, 1-6 (2016). doi: 10.1109/IRS.2016.7497297.
- [14] Pietkiewicz T., Kawalec A., Wajszczyk B., "Analysis of Fusion Primary Radar, Secondary Surveillance Radar (IFF) and ESM Sensor Attribute Information under Dezert-Smarandache Theory", The 18th International Radar Symposium (IRS), Prague, Czech Republic, 1-10 (June 28-30 2017). doi: 10.23919/ IRS.2017.8008199.
- [15] Konatowski S., Kaczmarek B., "Effectiveness of position estimating in nonlinear filtering approximation", Przeglad Elektrotechniczny, Vol. 85, Issue 3, 15-21 (2009).

- [16] Konatowski S., Sosnowski B., "Nonlinear filtering effectiveness evaluation in the process of maneuvering object tracking". Przeglad Elektrotechniczny, Vol. 87, Issue 10, 208-213 (2011).
- [17] Kaniewski P., Gil R., Konatowski S., "Estimation of UAV Position with Use of Smoothing Algorithms". Metrology and Measurement Systems. Vol. 24, No. 1, 127-142 (2017) ISSN 0860-8229, eISSN: 2300-1941, DOI: 10.1515/mms-2017-0013.
- [18] Matuszewski J., "Specific emitter identification". Proceedings of International Radar Symposium (IRS), Wrocław, Poland, 302-305 (2008).
- [19] Matuszewski J., "The Radar Signature in Recognition System Database". Proceedings of 19th International Conference on Microwaves, Radar and Wireless Communications (MIKON-2012), Warsaw, Vols. 1-2, 617-622 (2012).
- [20] Matuszewski J., "The Analysis of Modern Radar Signals Parameters in Electronic Intelligence System". 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), Lviv-Slavske, Ukraine, 298-302 (2016).
- [21] Matuszewski J., Paradowski L., "The Knowledge Based Approach for Emitter Identification", Proceedings of 12th International Conference on Microwaves & Radar (MIKON). Krakow, Poland, Vols. 1-4, 810-814 (1998).