A Novel Approach for Meeting the Challenges of the Integrated Security Systems

MOEIN KASEM [1] NADIM CHAHIN [2]
1 Researcher, department of electronics and telecommunication engineering
2 Professor and head of the department of electronics and telecommunication engineering
Damascus University
SYRIA

Abstract: - This study aims to build a general mathematical model in integrated security systems to overcome the remaining challenges in this domain, due to the heterogeneity, the uncertainty, the bad quality, and the conflict resulting from the information provided by the information sources (i.e. sensors) by taking account of the constraints, the scalability, and the architecture of the security system. The proposed model is fundamentally based on the proportional conflict redistribution fusion rule developed by Arnaud Martin under the framework of Dezert-Smarandache model. This combination permits to extend the utility of Dempster-Shafer model, and assures the generality of the proposed system.

Key-Words: - Dezert-Smarandache Theory (DSmT), Dempster-Shafer Theory (DST), Proportional Conflict Redistribution (sixth version) PCR6, Integral Security System Challenges.

1 Introduction

In spite of the great interest and the significant number of the applications and researches carried out in the field of the security systems, there is still a considerable number of challenges and needs that must be rapidly solved within a unified simple framework due to the increasing grow of threat, terrorism, destructive actions, …etc., all around the earth with the aim to survive the life of men, governments, economics, etc, from one side, and to ameliorate the life of each breathing soul from the other side.

The remaining main challenges and needs in security systems, particularly pointed out and discussed recently in detail [9] along with other requirements and difficulties collected from the literature [1] [3] will be summed up and discussed in the following section followed by the mathematical model that we propose to fulfill these needs and to solve the described problem in section 3. The manner in which the proposed model can step in here to tackle these problems and to overcome the difficulties will be presented in section 4 followed by an illustrative numeric example in section 5. Afterwards, we conclude and resume the paper in the last section.

2 Problem Description

In this section, the main remaining challenges in the domain of security systems will be resumed from the information processing and engineering point of view, while the other challenges resulting from the physics and electronics of the devices of the system will be presented in another article so as not to aviate from the main scope of this article.

The first challenge is the quality of data. Images or audio recordings of a CCTV sensor for example are not always perfect in such systems, objects of interest can be partially obscured; camera lenses maybe covered or damaged, the person (object) being recognized may have deliberately covered itself up. Even when these problems do not exist, there are other factors causing quality concerns, such as, poor illumination, sensor noise, particularly in poor lighting conditions and low resolution of the cameras.

The second challenge is the uncertainty of recognized events from a source (e.g., a camera) due to the poor quality of data provided. For instance, it can be very difficult to judge if a person is a male or female if the person wearing a heavy coat is entering a bus with its back deliberately leaning towards a camera. Therefore, adequate mechanisms shall be deployed to model such uncertainty and ignorance associated with the detected events (multiple explanations of events).

The third challenge is the inconsistency or conflict among multiple sources. A typical scenario is that from a camera with poor visibility a male can be detected while the audio recording strongly indicates a female. So adequate methods must be applied to resolve this inconsistency.

The fourth challenge is the adequate modeling of events information. For real-time surveillance involving multiple sources, the representation of events is particularly important, since it influences fundamentally the ways to merging detected events from multiple sources and the uncertainty and inconsistency handling during the fusion process.

The fifth challenge is the scalability of the system. What should be the manner that we revise/update rules for events composition if rules are used? How much change is needed if new types of equipment are brought into the system?

Along with the modification of the sources, the output of the security system must be appropriate for the following systems (like a data mining or machine learning system used to extract knowledge from the decisions based on the previous knowledge). These systems may be fuzzy, probabilistic, possibilistic, etc. Consequently, the proposed system must provide us with results that match these systems.

The sixth challenge is the evaluation of a surveillance system. In any security system, it is important to be able to evaluate the system entirely and all its parts. In other terms, it is fundamental to know if the performance of the system will be improved or worsened by adding new sensors or other sources, and when there is a conflict between the sources, it is fundament to know the sources of conflict and which source will improve the informative content and decrease the conflict by augmenting the coherence of the extracted knowledge.

The seventh challenge is the heterogeneity and the imperfection of data. As we use different types of sensors in such systems (laser, radar, CCTV, ANPR, etc), and each type supplies us with different kinds of data (images, video, audio, signals, parameters, etc), the proposed algorithm must be able to easily transform all these data types to a unified representation in order to find the solutions within an integrated platform. Besides, as the information elements could be imperfect (missing data, imprecise values, probabilistic distribution of the element coming from another precedent system, ..etc), the proposed technique ought to be able to represent this imperfection.

The eighth challenge is the time. Alarms, reactions, decisions, classification, etc must be achieved in the real time, since there is no utility of the security system if it is not capable to react in the appropriate moment. Accordingly, the proposed method must have a small executing time.

The ninth challenge concerns the memory space and the information

management. Security systems generally have a notable amount of tasks to achieve like face recognition, target tracking and classification, outlier detection, etc. if all these tasks can be solved within a unified integrated framework, then the management of the whole system will be accessible and feasible on the one hand, and the economy in data storage space is certain since we use the same technique to deal with all the required tasks of the integral system. This last point is also very indispensable in such systems, given that we deal with a large size of data since we use many sensors in the system.

The tenth challenges concerns the prior knowledge of the experts and the constraints of the system. Sometimes we know a priori that two or more actions cannot happen simultaneously, or two contradictory decisions cannot be taken together in the set of decisions. For example it is not possible that the detected target will be friend and enemy at the same time, or that the recognized person will be a male and a female. Therefore, all the evident types of constraints and conditions must be considered during analyzing the system to improve its efficiency and robustness.

3 Problem Solution

We propose to use a system like the one schematized in figure (1) presented at the end of the article. This system consists of multiple sensors (laser, radar, IP cam, CCTV, speedometer, etc), to capture the information from the observed region. Using multiple sensors in security systems has the following potential advantages [12]:

1. Multiple sensors would provide redundancy which, in turn, would enable the system to provide information in case of partial failure, data loss from one sensor - i.e., fault tolerance capability - robust functional and operational performance.

2. One sensor can look where other sensors cannot look and provide observations - enhanced spatial or geometrical coverage, and complementary information is made available.

3. Measurements of one sensor are confirmed by the measurements of the other sensors, obtaining cooperative arrangement and enhancing the confidence - increased confidence in the inferred results.

4. Joint information would tend to reduce ambiguous interpretations and hence less uncertainty.

5. Increased dimensionality of the measurement space, say measuring the desired quantity with optical sensors and ultrasonic sensors, the system is less vulnerable to interferences providing a sustained availability of the data.

6. Multiple independent measurements when fused would improve the resolution - enhanced spatial resolution.

7. Extended temporal coverage - the information is continually available.

8. Improved detection of the objects because of less uncertainty provided by the fusion process.

The information elements provided by the sensors must be saved on suitable supports (hard disks, databases, etc.), for example the data coming from the CCTV cameras must be saved on Digital Video Recorders DVRs, while the elements coming from IP CAMs will be saved on Network Video Recorders NVRs.

These storage supports represent the body of the security system. In order to give it the life, suitable programs to track the objects, to recognize the persons, to detect the danger, etc, must be installed on these disks.

Depending on the output of these systems, information can be represented and modeled using any suitable representational model. We propose to process the information elements using the evidence theory under the framework of *Dezert-*

Smarandach model (DSm Model) using the proportional conflict redistribution rule of fusion in order to combine the different information of the sensors. A basic mathematical background of this model will be represented in the following sub-section. We will show afterwards the advantages and the strong points of using such model to tackle the problem and to overcome the challenges explained in section 2. Actually, this is the first time that this theory is proposed and used in this domain under the platform of Dezert and Smarandache (Dsm model). In [9], the authors have implicitly proposed the evidence theory as a solution to the challenges, but under Dempster-Shafer's framework (DS model). Unfortunately, the latest model cannot take account of all the possible constraints of the system as is proved by Dezert in [13-14], and many problems can arise from such system in some special cases as explained by numeric examples in [13]. In addition, this rule of fusion is the worst concerning the conflict mass, especially when there is a notable conflict and contradiction between the information sources [14]. For the aforementioned issues, we recommend to extend this model by working under Dezert-Smarandache Model and to fairly redistribute the conflict by using the sixth version of the fusion rule proposed by Arnaud Martin [14] (chapter 2). This rule is called the proportional conflict redistribution fusion rule, denoted as PCR6, and it is considered as an improvement of the first five versions developed by Dezert and Smarandache.

3-1. Evidence Theory

Information can be defined mathematically as a function called the informative function described by means of a model, which maps the information definition set that represents the object of our description (denoted as Θ) to the information content set (denoted as Ω) that represents the manner used to describe the information (figure 2, at the last of the paper) [15]. The set of all the subsets of Ω is called the power set of Ω and is denoted $\rho(\Omega)$ or 2^{Ω}, since its cardinality is equal to $2^{|\Omega|}$.

Evidence theory permits to allocate the total belief normalized to the unity value over all the possible subsets of the information content set, through what is called the Basic Belief Assignment denoted as *m* or *BBA*, defined as:

$$m : \rho(\Omega) \rightarrow [0,1]$$
$$A \in \rho(\Omega) \rightarrow m(A)$$

with

$$m(\phi) = 0 \quad \text{(eq. 1)};$$
$$\sum_{A_i \subseteq \Omega} m(A_i) = 1 \quad \text{(eq. 2)}$$

The subsets A of Ω for which $m(A) > 0$ are called the focal sets of *m*. Each focal set *A* is a set of possible contents associated with $O \in \Theta$ and the number $m(A)$ can be interpreted as a fraction of a unit mass of belief, which is allocated to *A* on the basis of a given evidential corpus. Complete ignorance corresponds to put all our belief in the information content set Ω ($m(\Omega) = 1$), and the perfect knowledge of the content of the object $O \in \Theta$ is represented by the allocation of the whole mass of belief to a unique singleton of Ω (*m* is then called a certain *BBA*). Another particular case happens when all focal sets of *m* are singletons. In this situation, *m* is equivalent to a probability function and is called a Bayesian *BBA*. A basic belief assignment *m* can be equivalently represented through two non-additive belief functions; the **belief function (*Bel*)** and the **plausibility function (*Pl*)**.

The belief function of an event *A* for which ($\inf(O) \in A$) is the minimum belief mass that can be associated to the realization of this event, whereas the plausibility function of an event *A* for which ($\inf(O) \in A$) is the maximum belief mass that can be associated to the realization of this event.

$$Bel(A) = \sum_{B \subseteq A} m(B) \quad \text{(eq. 3)}$$
$$Pl(A) = 1 - Bel(A^C) = \sum_{A \cap B \neq \phi} m(B) \quad \text{(eq. 4)}$$

where A^C is the complement set of A.

The functions of belief and plausibility respectively represent the inferior and the superior bounds (limits) of the probability allocated to an event $A \subseteq \Omega$. These two functions boil down to a unique probability measure when *m* is a Bayesian *BBA*. Consequently, any probability distribution that realizes ($Bel(A) \leq \Pr(\{A\}) \leq Pl(A)$ for $\forall A \subseteq \Omega$) is said to be compatible with the given mass distribution. The pignistic probability

$$\Pr_{pignistic}(\{\omega_i\}) = \sum_{\substack{A \subseteq \Omega \\ \omega_i \in A}} \frac{m(A)}{|A|} \quad \text{(eq. 5)}$$

(where $|A|$ stands for the cardinality of the subset *A*) is a very well-known example of such compatible distributions.

For a given distribution of belief masses, and supposing that the uncertainty has a probabilistic nature, the uncertainty of the occurrence of an event $A \in \rho(\Omega)$ can be qualified by the confidence interval ($[Bel(A), Pl(A)]$) while the uncertainty degree of the value of the probability of *A* can be represented by ($\Delta = Pl(A) - Bel(A)$).

3-2 Evidential Information Fusion

One of the most well-known applications of evidence theory is information fusion. Combining two BBAs m_1 and m_2 representing distinct items of evidence coming from two different sources concerning the content of the object $O \in \Theta$ could be achieved using any fusion rule proposed in the literature [13] [14], . We give in the following three examples of three very widely-used rules:

- **Dempster-Shafer rule**: is the most widely used commutative and associated rule of combination, though it fails sometimes to provide coherent results due to the normalization procedure it involves.

$$m_{12_{DS}}(A) = \frac{1}{1-K} \sum_{\substack{k,l \\ B_k \cap C_l = A}} m_1(B_k) \cdot m_2(C_l)$$

(eq. 6)

where $K = \sum_{\substack{k,l \\ B_k \cap C_l = \phi}} m_1(B_k) \cdot m_2(C_l)$ (eq. 7)

is called the conflict degree between m_1 and m_2. It may be seen as the degree of disagreement between the two information sources.

- **Yager rule**: This rule admits that in case of conflict the result is not reliable, so that the conflicting mass plays the role of an absolute discounting term added to information content set Ω:

$$\forall A \in \rho(\Omega),\ A \neq \Omega,$$
$$m_{12_{Yager}}(A) = \sum_{\substack{k,l \\ B_k \cap C_l = A}} m_1(B_k) \cdot m_2(C_l) \quad \text{(eq. 8);}$$

and $m(\Omega) = m_1(\Omega) \cdot m_2(\Omega) + K$ (eq. 9).

- **Dubois-Prade rule**: This combination rule admits that the two sources are reliable when they are not in conflict, but one of them is right when a conflict occurs. Then if one observes a value in set B_k while the other observes this value in a set C_l, the truth lies in $B_k \cap C_l$ as long $B_k \cap C_l \neq \phi$;. If $B_k \cap C_l = \phi$; then the truth lies in $B_k \cup C_l$:

$$m_{12_{DB}}(A) = \sum_{\substack{k,l \\ B_k \cap C_l = A}} m_1(B_k)\cdot m_2(C_l) + \quad \text{(eq. 10).}$$
$$+ \sum_{\substack{k,l \\ B_k \cap C_l = \phi \\ B_k \cup C_l = A}} m_1(B_k)\cdot m_2(C_l)$$

3-3- Evidential Reasoning and Decision Making

Based on the basic belief assignments, the essential evidence tools like the belief and the plausibility functions, and after combining the information coming from different sources, one and only one decision ($\{\omega_i\} \in \rho(\Omega)$) has to be adopted (uncertainty). In the following, we present three well-known criteria used in making this decision:

- **Maximum plausibility criterion (optimistic solution):** the decision can be taken based on the superior limit of probability of the singletons under consideration, since the maximum plausibility assures a minimum conflict.

  $$(\inf(O) = \omega_{n_0}$$
  $$\textit{if and only if}$$
  $$Pl(\{\omega_{n_0}\} = \max_{n=1,2,\ldots,N} Pl(\{\omega_n\}) \text{ (eq. 11).}$$

- **Maximum belief criterion (pessimistic solution):** the decision can be taken based on the inferior limit of probability of the singletons under consideration. This means that we intend to choose the singleton whose belief mass is the greatest.

  $$(\inf(O) = \omega_{n_0} \quad \textit{if and only if}$$
  $$Bel(\{\omega_{n_0}\} = \max_{n=1,2,\ldots,N} Bel(\{\omega_n\})$$
  (eq. 12).

- **Maximum pignistic probability:** as a compromised solution between the optimistic and the pessimistic criterion, we can consider the maximum of the pignistic probability as:

  $$(\inf(O) = \omega_{n_0} \quad \textit{if and only if}$$
  $$\Pr_{pignistic}(\{\omega_{n_0}\} = \max_{n=1,2,\ldots,N} \Pr_{pignistic}(\{\omega_n\})$$
  (eq. 13).

3-4-Dezert-Smarandache Theory of Plausible and Paradoxical Reasoning

The basis of this approach is the refutation of Shafer's model's limitations [4] [6] [11] as the principle of the third middle excluded (i.e. the existence of the complement for any elements or propositions belonging to information content set Ω), the exclusivity constraints imposed upon these elements, and the redistribution of the conflicting mass to the non-empty sets using the normalization; on the ground that for a wide spectrum of fusion problems, the intrinsic nature of hypotheses can only be vague and imprecise in such a way that precise refinement of information content set is just impossible, and consequently, the exclusive elements ω_i cannot be properly identified and precisely separated. Depending on the nature of the elements of the fusion problem under consideration, it can also happen that some subsets of Ω may contain elements known to be truly exclusive and even possibly non-existing at a given time, particularly in dynamic fusion problems where the information content set changes with time with revision of the knowledge available. These integrity constraints must be considered in the model in order to fit with the reality. This has been achieved by Dezert-Smarandache combination rule (called the hybrid model) [13-14] given as:

$$m_{HybridDSm}(A) = \chi(A)\left[S_1(A) + S_2(A) + S_3(A)\right]$$
(eq. 14)

Where all the sets involved in formulas are in the canonical form and $\chi(A)$ is the characteristic non-emptiness function of the set A; i.e. $\chi(A)=1$ if $A \notin \varphi$ and $\chi(A)=0$ otherwise, given that $\varphi=\{\varphi_{\mathrm{M}}, \phi\}$. φ_{M} is the set of all the elements of the hyper power set of Ω denoted as D^{Ω} (Dedekind's lattice) which have been forced to be empty through the constraints of the model and ϕ is the classical universal empty set. $S_1(A)$, $S_2(A)$, and $S_3(A)$ can be evaluated for k sources as:

$$S_1(A)=\sum_{\substack{B_1,B_2,\dots,B_k\in D^{\Omega}\\ B_1\cap B_2\cap\dots\cap B_k=A}} \prod_{i=1}^{k} m_i(B_i) \qquad \text{(eq. 15)}$$

$$S_2(A)=\sum_{\substack{B_1,B_2,\dots,B_k\in \varphi\\ [\mu=A]\vee[(\mu\in\varphi)\wedge(A=I_t)]}} \prod_{i=1}^{k} m_i(B_i) \qquad \text{(eq. 16)}$$

$$S_1(A)=\sum_{\substack{B_1,B_2,\dots,B_k\in D^{\Omega}\\ B_1\cap B_2\cap\dots\cap B_k\in\varphi\\ B_1\cup B_2\cup\dots\cup B_k=A}} \prod_{i=1}^{k} m_i(B_i) \qquad \text{(eq. 17)}$$

with $\mu=u(B_1)\cup u(B_2)\cup\ldots\cup u(B_k)$ where $u(B)$ is the union of all ω_i that compose B, $I_t=\omega_1\cup\omega_2\cup\ldots\cup\omega_n$ is the total ignorance. $S_1(A)$ corresponds to free Dezert-Smarandache model of combination when the system has no constraints or restrictions; $S_2(A)$ represents the mass of all relatively and absolutely empty sets which is transferred to the total or relative ignorance associated with non-existential constraints; $S_3(A)$ transfers the sum of relatively empty sets directly onto the canonical disjunctive form of non-empty sets.

Instead of the normalization procedure utilized in Shafer's model to redistribute the conflicting mass to all the non-empty sets, Dezert and Smarandache have proved through different examples that it is more reasonable and logic to only redistribute this mass to the evidence sources involved in the conflict proportionally to their belief masses [13-14]. Thus, they established five different versions of proportional conflict redistribution approach (*PCR1, PCR2, ..., PCR5*) and they have shown that this redistribution (except *PCR1*) satisfies the three main properties of good combination rule: the coherence, the commutativity and the neutral impact of the vacuous belief assignments *VBA*. In addition to these properties, *PCR6* proposed by Martin and Osswald [10] is quasi-associative, stable in terms of decision, and more coherent than the other versions when there are more than two evidence sources [14]. It can be computed as [10]:

$$m_{PCR6}(A)=$$
$$m_c(A)+$$
$$\sum_{l=1}^{t} m_l(A)^2 \sum_{\substack{\bigcap_{k=1}^{t-1} Y_{\sigma_l(k)}\cap A=\phi\\ (Y_{\sigma_l(1)},\dots,Y_{\sigma_l(t-1)})\in(D^{\Omega})^{t-1}}} \left(\frac{\prod_{j=1}^{t-1} m_{\sigma_l(j)}(Y_{\sigma_l(j)})}{m_l(A)+\sum_{j=1}^{t-1} m_{\sigma_l(j)}(Y_{\sigma_l(j)})} \right)$$

(eq. 18)

where σ_l counts from 1 to t avoiding l:

$$\begin{cases} \sigma_l(j)=j & if \quad j<l,\\ \sigma_l(j)=j+1 & if \quad j\geq l, \end{cases} \qquad \text{(eq. 19)}$$

As Y_l is a focal element of the source l, then $m_l(A)+\sum_{j=1}^{t-1} m_{\sigma_l(j)}(Y_{\sigma_l(j)})\neq 0$.

It has been shown [10] [14] that all the proposed versions can properly work for any degree of conflict, for any models (Shafer's model, free DSm model or any hybrid DSm model) and for any type of fusion (statical or dynamical).

Dezert and Smarandache have shown in the three volumes that they published [13-14] that the probability, the possibility, the fuzzy set theories represent special cases of their proposed model.

4 Advantages of the Proposed System

The model that we proposed to deal with the information in security systems has the following strong points regarding the challenges introduced in section 2:

Concerning **the first two challenges**, the evidence theory has been come to existence to mainly deal with information uncertainty and quality, and we cannot find any work in uncertainty without introducing this theory that tries to extract the valid information of each sensor by removing the redundancy, and fusing the useful elements.

Regarding **the third challenge**, there is no other mathematical model until now capable to outperform the PCR 6 by fairly dealing with the conflict mass resulting from the contradictory between the sensors of the system [14]. This last reference contains a remarkable number of numeric illustrative examples and applications that prove this issue.

For the forth and the seventh challenge about the modeling of information elements, this model represent the information using basic belief assignments that assure a unified framework to represent the information whatever type they have and regardless of their forms and they also present a simple framework to combine the information elements, and to take the suitable decision by considering the maximum belief as a pessimistic solution, the maximum plausibility as an optimistic solution, or the maximum of the pignistic probability as a compromising solution between the last two ones.

Concerning the scalability (**the fifth challenge**), as is shown, supported by numeric examples in [1-2], the basic belief assignments can easily be transformed to probability degrees (for the probabilistic systems), to membership degree (for fuzzy systems), to possibility degrees (for possibilistic systems) etc, since these theories are particular cases of the evidence theory. Accordingly the output of our system is appropriate for any following system. Generally, the following systems are used to have deeper insight in the information, to extract potential trends and patterns, or to visualize or to represent the output (Data Mining systems). Thierry Denorex [WEB, 1] has offered to the researchers in this domain several packages to mine the evidential information elements in order to extract knowledge from information. In the following we give some examples of these packages:

- Relational Evidential c-means (RECM)
- Evidential c-means (ECM)
- Evidential distance-based classifier (k-NN version)
- Evidential distance-based classifier (neural-network version)
- Evidential distance-based classifier (arbitrary class labels)
- Evidential distance-based classifier with adaptable metric (beta version)
- Evidential regression
- Interval-valued belief structures
- Clustering approximation of belief functions
- Coarsening approximation of belief functions
- EVCLUS: evidential clustering of proximity data
- Fuzzy Principal Component Analysis
- Multidimensional Scaling (MDS) of interval-valued dissimilarity data

Adding any information source to the system or taking account of the updating information as is the case in the dynamic fusion is completely possible and simple within Dezert-Smarandach model [13]. Besides, the failure of any information source in the system can easily be considered by assigning all the unity mass to the information content set (total ignorance case). All these points affirm the large scalability of our system.

Regarding **the sixth challenge**, Dezert has shown in [5] using practical numeric examples, the way to evaluate and to analyze the security system (Threat assessment of a possible Vehicle-Born Improvised Explosive Device using the same mathematical model that we proposed in this particular case). In his example, there is a conflict between the information elements coming from the physical systems like the ANPR (Automatic Number Plate Recognition) and the elements provided by two experts, and the question that he stresses in this example is to choose between the experience and the physics to handle the conflict resulting from both of them. Then, between the experts themselves (an expert with 10 year experience and another expert new in his post.

The solution is carried out by calculating two quantities: the **uncertainty degree** (the difference between the plausibility degree and the belief degree) that must be as small as possible when the conflict between the sources is small, then the **Probabilistic Information Content** (PIC) proposed by John Sudano [16] is calculated. The PIC is the dual of normalized Shannon entropy. PIC is in [0, 1] and PIC = 1 if the probability measure assigns a probability equals to one only on a particular singleton of the frame, and PIC = 0 if all elements of the frame are equi-probable. So, in order to know the most reliable system between the experience and the physics, we choose the system that gives the less uncertainty degree (more precise) and the greatest PIC of the systems (the most informative and coherent). Actually there are many other tools and measures to evaluate the system in evidence theory.

For the eighth challenge, this theory has a small executing time since it fundamentally depends on the basic operations of the microprocessor like the maximum, minimum, union, intersection, etc. besides, the same technique can be used to achieve different security tasks like face recognition, target tracking, etc. this issue ensure a speed executing time on the one hand and a small storage space (**the ninth challenge**) on the other. The generality of the proposed model and its multistage property can provide us with efficient, simple, and robust management and stability of the entire system [13-14]. Therefore, we can overcome the ninth challenge.

At last, in security systems, some constraints and conditions resulting from our priori knowledge must be considered to improve the performance of the system. It has been shown [13] that Shafer's model and all the other models proposed by Yager, Dubois, Prade, etc. cannot take account of these conditions [13]. On the contrary, Dsm model can easily adapt these constraints giving coherent and robust results, and overcoming **the tenth challenge**.

5 An Illustrative Example

To clarify the aforementioned discussion, let us explain the proposed model with a simple illustrative example. Let us consider the information content set Θ = {A, B, C} that contains 3 alarms. Our a priori knowledge of the system tells us that the alarm A cannot simultaneously take place with the alarm B (i.e. A∩B = Φ), while the alarms A and C as well as C and B can be activated at the same time (i.e. A∩C ≠ Φ and B∩C ≠ Φ). Because of this type of constraints and conditions, Shafer's model stands incapable to solve this type of problems since its exclusivity conditions are not satisfied [14].

Let us consider now two sources of evidence with the following belief assignments:

$$m_1(A) = 0.50$$
$$m_1(B) = 0.30$$
$$m_1(C) = 0.20$$
$$m_2(A) = 0.60$$
$$m_2(B) = 0.30$$
$$m_2(C) = 0.10$$

Using the table representation, we get the table 1 schematized at the end of this article.

To combine these two evidences using PCR6 under Dezert-Smarandache model, we firstly compute the conjunctive consensus:

$$m_{12}(A \cap B) = 0.50 \times 0.30 + 0.30 \times 0.60 = 0.33$$

$$m_{12}(A \cap C) = 0.50 \times 0.10 + 0.20 \times 0.60 = 0.17$$

$$m_{12}(C \cap B) = 0.30 \times 0.10 + 0.30 \times 0.20 = 0.09$$

As one may notice, $m_{12}(A \cap B) = 0.33$ must be redistributed to A and B proportionally with the respect to $m_1(A) = 0.50$ and $m_2(B) = 0.30$ and then with respect to $m_2(A) = 0.60$ and $m_1(B) = 0.30$, as follows:

$$\frac{x_1}{0.50} = \frac{y_1}{0.30} = \frac{0.15}{0.50 + 0.30} = 0.1875$$

Consequently:

$$x_1 = 0.09375$$

$$y_1 = 0.05625$$

And

$$\frac{x_2}{0.60} = \frac{y_2}{0.30} = \frac{0.18}{0.60 + 0.30} = 0.20$$

Consequently:

$$x_2 = 0.12$$

$$y_2 = 0.08$$

where *x* is the part of conflict redistributed to A and *y* is the part of conflict redistributed to B.

Then the final result will be given by:

$$m_{PCR}(A) = 0.30 + 0.09375 + 0.12 = 0.5137$$

$$m_{PCR}(B) = 0.09 + 0.05625 + 0.08 = 0.2262$$

$$m_{PCR}(C) = 0.02$$

$$m_{PCR}(A \cap C) = 0.17$$

$$m_{PCR}(B \cap C) = 0.09$$

As is notable here, Dempster-Shafer model cannot find solutions for such simple problem because of the constraints of the system resulting from our prior knowledge that opposites Dempster-Shafer's assumptions ($A \cap B = \Phi$ and $A \cap C = \Phi$ and $C \cap B = \Phi$).

6 Conclusions

In this article, we proposed to extend Dempster-Shafer model in order to overcome the remaining challenges in security systems by using the proportional conflict redistribution rule proposed by Martin [10] under the fusion framework developed by Dezert-Smarandache [14]. We showed that the proposed mathematical model is able to fulfill the essential needs in the system and to overcome the integrity of challenges within a unified simple and integrated platform capable to process, to combine, and to handle the information in a meaningful manner, even in very complex conditions where uncertainty, heterogeneity, conflict, etc. must be entirely considered.

It is useful to mention at last that one can find all the necessary software tools and algorithms of PCR6 in [WEB, 2] (the official site of Arnaud Martin), and those of Evidence theory in [WEB, 3] (the official site of the great researcher Philippe Smets) explained in detail along with Dezert-Smarandache model in [13-14] (downloadable at the official site of Jean Dezert). These algorithms are programmed under Matlab as open sources. In [17-19], some examples of applying these tools in data mining and machine learning applications can be found in the medical domain.

7 References

[1] Dahabiah A., PUENTES J., SOLAIMAN B., *Fusion of Possibilistic Sources of Evidences for Pattern Recognition*, International Journal of Integrated Computer-Aided Engineering, IOS Press, (2010), vol. 17, No 2, pp. 117-130, ISSN: 1069-2509.

[2] Denoeux T., Masson M.H., EVCLUS: *Evidential Clustering of Proximity Data, IEEE Transactions on Systems*, Man and Cybernetics, 34 (1) (2004), 95-109.

[3] Denoeux T., *Neural Network Classifier Based on Dempster-Shafer Theory*, IEEE Transactions on Systems, Man, and Cybernetics, 30 (2), (2000), 131-150.

[4] Dezert J., *Foundations for a New Theory of Plausible and Paradoxical Reasoning*, International Journal of Information & Security, 9, (2002), 90-95.

[5] Dezert, J., *Threat assessment of a possible Vehicle-Born Improvised Explosive Device using DSmT*. 26 pages. Fusion'10 Conference, (2010).

[6] Inagaki, T., *Interdependence between Safety-Control Policy and Multiple-Sensor Schemes via Dempster-Shafer Theory*, IEEE Trans. on reliability, 40 (2), (1991), 182-188.

[7] Lee, M.D., *Determining the Dimensionality of Multidimensional Scaling Representations for Cognitive Modeling*, Journal of Mathematical Psychology, 45 (1), (2001), 149-166.

[8] Liu, W.Z., White, A.P., Thompson S.G., *Techniques for Dealing with Missing Values in Classification,* LNCS Springer, 1280, (1997), 527- 536.

[9] Lie, L., Miller, P., Ma, J., Challenges of Distributed intelligent surveillance system with heterogeneous information, (2009)

.

[10] Martin A., Osswald C., *Une Nouvelle Règle de Combinaison Répartissant le Conflit - Applications en Imagerie Sonar et Classification de cibles Radar*. Revue Traitement de Signal. 24 (2), (2007), 71-82.

[11] Murphy, C.K., *Combining Belief Functions when Evidence Conflicts, Decision Support Systems*, Elsevier Publisher, 29, (2000), 1-9.

[12] Raol, J., *Multi Sensor Data Fusion with Matlab*, CRC Press, Chapter 1, (2010).

[13] Smarandache F., Dezert J., *Advances and Applications of DSmT for Information Fusion*, American Research Press Rehoboth, 1, (2004), Chapters 1-6.

[14] Smarandache F., Dezert J., *Advances and Applications of DSmT for Information Fusion*, American Research Press Rehoboth, 2, (2006), 1-106.

[15] Solaiman, B., *Information Fusion Concepts: From Information Elements Definition to the Application of Fusion Approaches*, SPIE proceedings series, 4385, (2001), 205-212.

[16] Sudano, J., *The system probability information content (PIC) relationship to contributing components, combining independent multi-source beliefs,hybrid and pedigree pignistic probabilities*, Proc. of Fusion 2002, Vol.2, pp. 1277-1283, Annapolis, MD, USA, July 2002.

[17] Dahabiah A., PUENTES J., SOLAIMAN B., *Digestive database evidential clustering based on possibility theory.* WSEAS transactions on biology and biomedicine, september 2008, vol. 5, n° 9, pp. 239-248

[18] Dahabiah A., PUENTES J., SOLAIMAN B., Possibilistic Pattern Recognition in a Digestive Database for Mining Imperfect Data. WSEAS Transactions on Systems, february 2009, vol. 8, n° 2, pp. 229-240

[19] Dahabiah A., PUENTES J., SOLAIMAN B., *Gastroenterology dataset clustering using possibilistic Kohonen maps.* WSEAS transactions on information science and applications, april 2010, vol. 7, n° 4, pp. 508-521

8 Internet References

(@ 08.06.2011)

[WEB, 1]
http://www.hds.utc.fr/~tdenoeux/dokuwiki/doku.php?id=en:software

[WEB, 2]
http://www.arnaud.martin.free.fr/

[WEB, 3]
http://iridia.ulb.ac.be/~psmets/#G

9 Figures and Tables

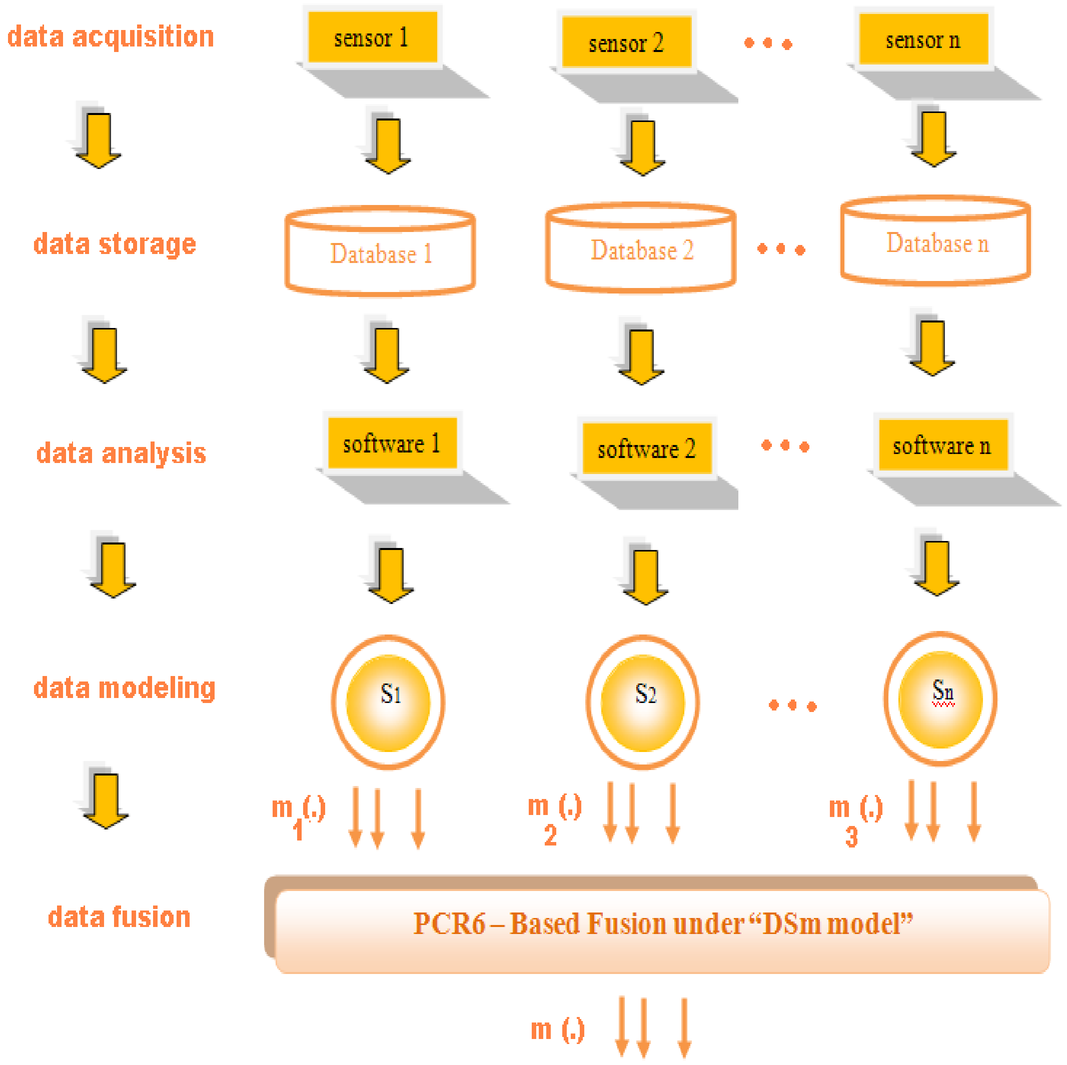

FIG 1. The integrated security system

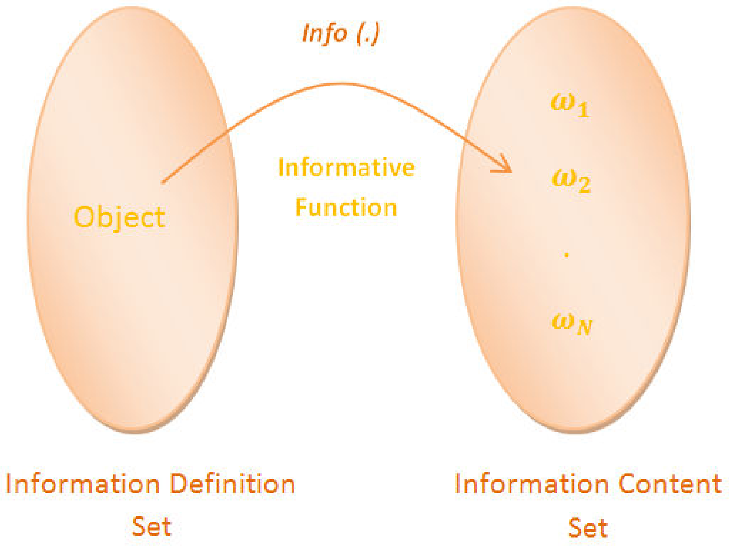

FIG 2. A general scheme of information structure

	A	B	C	$A \cap B$	$A \cap C$	$B \cap C$
m_1	0.50	0.30	0.20			
m_2	0.60	0.30	0.10			
m_{12}	0.30	0.09	0.02	0.33	0.17	0.09

Table 1. An illustrative example (section 5)