DESIGNING A HOME SECURITY SYSTEM USING SENSOR DATA FUSION WITH DST AND DSMT METHODS

A. Moussavi Khalkhali*

Telecommunication Infrastructure Company of Iran
Ministry of Information and Communication Technology
P.O. Box 14115-143, Tehran, Iran
arezou_moussavi@yahoo.com

B. Moshiri

Control and Intelligent Processing Center of Excellence
School of Electrical and Computer Engineering, University of Tehran
P.O. Box 14395-515, Tehran, Iran
moshiri@ut.ac.ir

H.R. Momeni

Department of Electrical Engineering, Tarbiat Modarres University
P.O. Box 14115-143, Tehran, Iran
momeni_h@modares.ac.ir

*Corresponding Author

(Received: October 9, 2006 – Accepted in Revised Form: September 25, 2008)

Abstract Today due to the importance and necessity of implementing security systems in homes and other buildings, systems with higher certainty, lower cost and with sensor fusion methods are more attractive, as an applicable and high performance methods for the researchers. In this paper**,** the application of Dempster-Shafer evidential theory and also the newer, more general one Dezert-Smarandache theory for implementing as a home security system and also using sensor data fusion have been considered. The benefits of multisensor fusion with direct connection to the control unit, in comparison with the traditional single sensor systems, have been shown.

Keywords Intrusion, Intelligent Housing System, Dempster-Shafer Reasoning, DSmT Approach, Information Fusion

چکیده امروزه به دلیل لزوم ایجاد امنیت و حفاظت از منازل، پیاده‌سازی یک سیستم حفاظتی با اطمینان بالا و هزینه کمتر از اهمیت بسزایی برخوردار است. در این میان روش‌های ترکیب اطلاعات سنسوری به عنوان روش‌های مطرح و کارامد، توجه بسیاری محققین را به خود جلب کرده است. در این مقاله کاربرد دو روش ترکیب اطلاعات تئوری Dempster-Shafer و Dezert-Smarandache، برای پیاده سازی یک سیستم امنیتی ساختمان بررسی می‌شود. در ذیل نشان خواهیم داد که نتیجه‌ای که از ترکیب اطلاعات چندین سنسور به دست می‌آید، چطور بر سیستم‌های تک سنسوری یا سیستم‌هایی که در آنها هر کدام از سنسورها مستقلاً به کنترل کننده مرکزی متصل است، برتری و ارجحیت دارد. از طرفی چنین سیستم‌هایی به دلیل قابلیت اطمینان بالایی که دارند مانع از صرف هزینه‌های بیهوده نیز می‌شوند.

1. INTRODUCTION

Having a security system in homes and other buildings, make the building intelligent and creates safety, assurance, and most of all security. Recent studies on sensor data fusion technologies persuaded researchers to look for better techniques with a higher assurance of fusion information.

In this paper, two theories of Dempster-Shafer (DST) and Dezert Smarandache (DSmT) were applied for fusing sensor information and making decision. The two said theories are among the

classical methods of information fusion. It could be said that DSmT is the general form of DST with the covering feature for deficiencies with the exceptions of DST.

The significant aim of this paper is to show the application of fusion methods in order to establish the security and detecting the precise location of the intruder at home, which are not viable through the traditional system, however in this application both of them cause the same results.

The following, home security system is simulated by MATLAB. In Sections 2 and 3, this paper will review the DST and DSmT and their combinational rules. Section 4 deals with the security system and applying the theories to a scenario, and finally Part 5 presents the conclusions obtained by simulating the attack scenarios.

2. DEMPSTER-SHAFER EVIDENTIAL THEORY BASIS

In Dempster-Shafer Theory (DST), there is a frame of discernment θ, in which the elements are all possible states of a system. So the DS fusion process is based on 2^{θ} elements called propositions.

To every subset in this frame a probability mass is assigned which is called basic probability assignment or basic belief assignment (bpa or m).

m; must satisfy the following conditions:

$$m: 2^{\theta} \rightarrow [0, 1], m(\emptyset) = 0, \sum_{A \in 2^{\theta}} m(A) = 1 \quad (1)$$

The probability that the true answer is a denoted by a confidence interval:

[Belief (A), Plausibility (A)] in which,

$$Bel(A) = \sum_{B \subseteq A} m(B) \quad (2)$$

$$Pl(A) = 1 - \sum_{B \cap A = \phi} m(B) \quad (3)$$

The width of the interval therefore represents the amount of uncertainty in A, given the evidence.

The belief function Bel (A) in a subset, entails belief in subsets containing that subset. The plausibility function measures the total belief mass that can move into A. For combining two belief functions over the same frame of discernment with different bpas (m1 and m2) and different sources, DS combination rule is used:

$$m(C) = [m_1 \oplus m_2](C) = \frac{\sum_{A \cap B = C} m_1(A)m_2(B)}{1 - \sum_{A \cap B = \phi} m_1(A)m_2(B)} \quad (4)$$

In which $k = \sum_{A \cap B = \phi} m_1(A)m_2(B)$ is interpreted as a measure of conflict among the various sources [1-3].

As an example consider a frame of discernment with three possible states H = {A,B,C}, then all subsets of H are 2^{θ} elements which are:

{A}, {B}, {C}, {A,B}, {A,C}, {B,C}, {A,B,C}, {Ø}.

Bel (B,C) = m ({B}) + m ({C}) + m ({B,C})

Pl (B,C) = m ({B}) + m ({C}) + m ({B,C}) + m ({B,A}) + m ({A,B,C}) + m {(C,A)}

Suppose that

m_1 (G) = 0.6, m_1 (V) = 0.3, θ_1 = (GUV) = 0.1,

m_2 (G) = 0.5, m_2 (V) = 0.35, θ_1 = (GUV) = 0.15

Then

m (G) = [(0.6*0.5) + (0.6*0.15) + (0.1*0.5)]/[1-(0.6*0.35)-(0.3*0.5)] = 0.6875

It could be seen that the combinational probability is more than the single probabilities of each source.

3. DEZERT-SMARANDACHE THEORY BASIS

The Dezert-Smarandache Theory (DSmT) is the generalization of DST. With DSmT any types of sources of information even those that have conflict among them, could be combined with each other.

Basic belief assignment, which is named here, generalized basic belief assignment or gbba, belief and plausibility functions defined here, are

like those in DST. Imagine $\Theta = \{\theta 1, \theta 2, \ldots, \theta n)$ is the frame of discernment of the system to be considered. So, m: $2^{\theta} \rightarrow [0,1]$ is defined as follows:

$$m(\emptyset) = 0, \ \sum_{A \in 2^{\theta}} m(A) = 1 \quad (5)$$

Then from gbba, belief and plausibility functions are defined by:

$$Bel(A) = \sum_{B \in 2^{\theta}, B \subseteq A} m(B) \quad (6)$$

$$Pl(A) = \sum_{B \in 2^{\theta}, B \cap A \neq \phi} m(B) \quad (7)$$

DsmT comes to overcome the two deficiencies in DST:

- In DST, the elements of the frame of discernment must be exclusive and exhaustive, but in DSmT they are not exclusive.
- In DST, bodies of evidence must be independent, but their belief functions have to be interpreted the same over different frame of discernment, if not the frame of discernments Θ1 and Θ2 could be mapped to the same frame of Ω. With DSmT, belief functions from two different frame of discernment can be combined without mapping them into the same frame. For more information, you could refer to [4,5].

The classical rule of combination of DSmT of two distinct sources of evidence over the same general frame of discernment Θ with belief functions associated with mass functions is given by:

$$\forall C \in D^{\theta}, m(C) = \stackrel{\Delta}{[} m_1 \oplus m_2](C) = \sum_{A,B \in D^{\theta}, A \cap B = C} m_1(A) m_2(B) \quad (8)$$

In this paper, DSmT classical rule of combination is used [6].

4. SIMULATION RESULTS

In order to simulate the security system, imagine a home with sensors located in different areas according to Figure 1. The security system utilized here is a system, capable of detecting intruders. If the home also needs to be protected from fire, smoke detectors and heat sensors should be used.

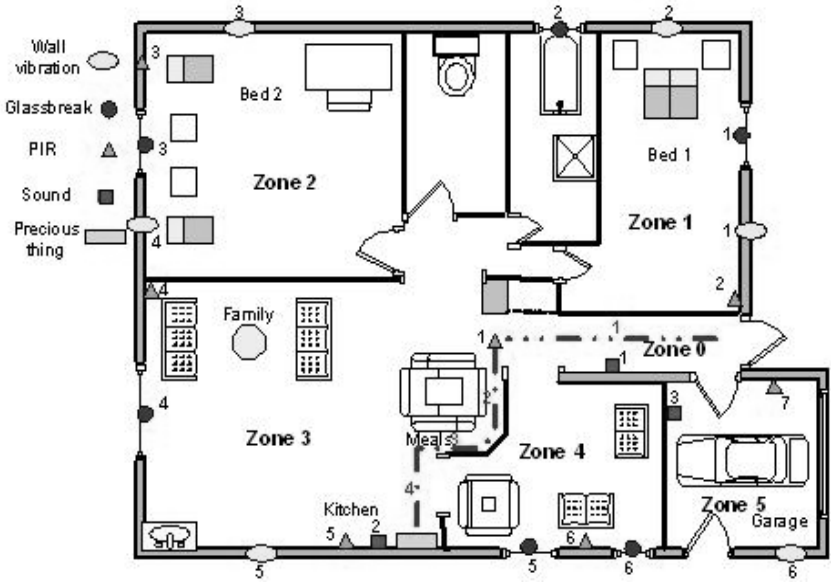

Figure 1. Home plan with sensors located in it.

Now four kinds of sensors are used to implement the system:

4.1. Wall Vibration Intended to detect mechanical vibrations caused by chopping, sawing, drilling, ramming or any type of physical intrusion.

4.2. PIR/Microwave In which microwave and PIR (passive Infrared) sensors are electronically connecting together with AND logic. Microwave sensors are active devices, which cover a zone or an area with electrical field and detect movement and PIRs are passive, which detect a heat-emitting source (human bodies).

4.3. Sound Detectors That "listen" to the noises produced by the intruder.

4.4. Glass-Break Detectors Which are sensitive to 5 kHz, shock and frequencies produced if a glass is broken.

It is tried to use almost maximum number of sensors, but it can be changed by the designer's opinion. In designing the home security system, it is tried to indicate the zone that the intruder attacks there. The home is divided into 6 areas as shown in Figure 1.

Considering Table 1, the probability of sensors detection is estimated as follow; [7].

TABLE 1. The Estimate Probability of Detection for Sensors.

Sensor Systems	Slow Walk	Walk	Run	Crawl	Roll	Jump
Sensor Lists-Estimate Probability of Detection-Very Low VL, Low L, Medium M, high H, Very High VH, N/A Not Applicable	-	-	-	-	-	-
Binary Sensors	N/A	N/A	N/A	N/A	N/A	N/A
Fix Barrier/Wall Sensor	N/A	N/A	N/A	N/A	N/A	N/A
Infrared Sensors						
Infrared Beambreak Detector	VH	VH	VH	M/H	H	H
Passive Infra-Red Sensor (PIR) Detector(Heat Sensor)	VH	VH	VH	M/H	H	H
Microwave Sensors						
Microwave Bistatic	H	VH	H	M/H	M/H	M/H
Microwave Monostatic	H	VH	H	M/H	M/H	M/H
Other Sensors						
Dual Technology Passive IR/Microwave	VH	VH	VH	M/H	H	H
Sound Sensors	L	M	M/H	VL	L	M

PIR/Microwave: VL = 0-0.2, L = 0.2-0.4, M/H = 0.4-0.6, H = 0.6-0.8, VH = 0.8-1

Sound Detector: VL = 0-0.3, L = 0.3-0.5, M/H = 0.5-0.7, H = 0.7-0.9, VH = 0.9-1

The worst condition for the system is when an intruder is crawling as given in Table 1. The threshold probability for detection of sound detectors set to 0.3 and for PIR/Microwaves, set to 0.45. The ignorance of the sensors is set to 0.1.

The system checks the 22 sensors' sample every 0.5 seconds. As soon as one sensor rises up the threshold, the system looks for another and combines their output to check if there is a real attack. If an intrusion has taken place, depending on which zone's sensors participate in combination, the alarm for the corresponding zone will be triggered.

The sensors are sensitive to delay between two detections and the system resets, if the intruder delays between two actions, so the system is programmed in a way that every time a sensor is triggered it increases the threshold value, the system holds it for 10 minutes. Unless the new value is greater than the last one, then the newer one is held.

First, consider a room with four sensors mentioned above, one sensor from each type. The mentioned system is simulated by the Monte-Carlo method in which, one mathematical experiment with random numbers is repeated for thousands of times [8].

As a sample calculation let's assume that "i" implies intruder and "s" means secure.

The four PIRs announce the following report:

m1 (i) = 0.6; m1 (s) = 0.3; m1 (θ) = 0.1

m2 (i) = 0.5; m2 (s) = 0.4; m2 (θ) = 0.1

m3 (i) = 0.5; m3 (s) = 0.4; m3 (θ) = 0.1

m4 (i) = 0.65; m4 (s) = 0.25; m4 (θ) = 0.1

and the two sound detectors informs the following:

m5 (i) = 0.2; m5 (s) = 0.65; m5 (θ) = 0.15

m6 (i) = 0.2; m6 (s) = 0.65; m6 (θ) = 0.15

Note that the ignorance of each sensor is indicated with the term $m_x(\theta)$.

The calculation process can be seen in the following tables, which are related to DST and DSmT methods respectively. (Tables 2 and 3)

Note that by fusion of the cell 1 and cell 2 of the tables, cell 3 is deduced.

The probabilities for detection produced by the sensors are random numbers. Applying the output value for the sensors is repeated for 1000 times, and the results are shown in Figure 2.

As shown in Figure 2 the frequency of the solid lines in two theories, the secure states in DST and DSmT, are the same, but the range of probability differs. This diversity is due to the normalization factor in the denominator of the DST combination rule.

Figure 3 indicates the function of detection by the sensors. It is assumed that the total time for traversing the path to reach the object shown in Figure 1 is 130 seconds. Another assumption is that, each sensor takes a sample every 0.5 seconds. The horizontal axis in Figure 3 shows the samples and the vertical one indicates the probability of the detection.

Considering the SD1 graph as an example, it is noticed that the sensor began to detect the thief around sample 57, where the sensors' detection peak appears.

This is due to the minimum distance between the intruder and the sensor. Afterward when the intruder receded the sound detector, the probability of the detection is also decreased.

It is assumed that it takes 60 seconds (120 samples) to pass the corridor (path 1), considering 30 seconds for passing the meal table (path 2), 10 seconds for crawling the path 3, and 30 seconds for reaching the object (path 4).

Figure 4 shows that at 208th sample the system realized the intruder and alarmed or called the local police station or locked the doors or any other security and prevention actions.

5. CONCLUSION

As shown in simulation results, the probabilities of the sensors to activate are very low. At least PIR's are more sensitive, which the sensors had to detect the intrusion with higher probability. Meanwhile

TABLE 2. Sensor Data Fusion in DST Method.

1 / 2 → 3	m1(i) = 0.6 m1(s)=0.3 m1(θ)=0.1	m3(i) = 0.5 m1(s)=0.4 m3(θ)=0.1	m4(i) = 0.65 m4(s)=0.25 m4(θ)=0.1	m5(i) = 0.2 m5(s)=0.65 m5(θ)=0.15	m6(i) = 0.2 m6(s)=0.65 m6(θ)=0.15
m2(i) =0.5 m2(s)=0.4 m2(θ)=0.1	k=0.61 m12(s)=0.3115 m12(i)=0.6721 m12(θ)=0.0164	k=0.5754 m123(s)= 0.2821 m123(i)= 0.7151 m123(θ)= 0.0028	k=0.6379 m1234(s)= 0.21559 m1234(i)= 0.8437 m1234(θ)= 4.4663e-004	k=0.4204 m12345(s)= 0.2973 m12345(i)= 0.7026 m12345(θ)= 1.5935e-004	k=0.4839 m123456(s)= 0.4917 m123456(i)= 0.5082 m123456(θ)= 4.9396e-005

TABLE 3. Sensor Data Fusion in DSmT Method.

1 / 2 → 3	m1(i) = 0.6 m1(s)=0.3 m1(θ)=0.1	m3(i) = 0.5 m1(s)=0.4 m3(θ)=0.1	m4(i) = 0.65 m4(s)=0.25 m4(θ)=0.1	m5(i) = 0.2 m5(s)=0.65 m5(θ)=0.15	m6(i) = 0.2 m6(s)=0.65 m6(θ)=0.15
m2(i) =0.5 m2(s)=0.4 m2(θ)=0.1	m12(s)=0.19 m12(i)=0.41 m12(θ)=0.01	m123(s)= 0.099 m123(i)= 0.2510 m123(θ)= 0.001	m1234(s)= 0.0349 m1234(i)= 0.1889 m1234(θ)= 0.0001	m12345(s)= 0.028 m12345(i)= 0.0661 m12345(θ)= 1.5000e-005	m123456(s)= 0.0224 m123456(i)= 0.0232 m123456(θ)= 2.2500e-006

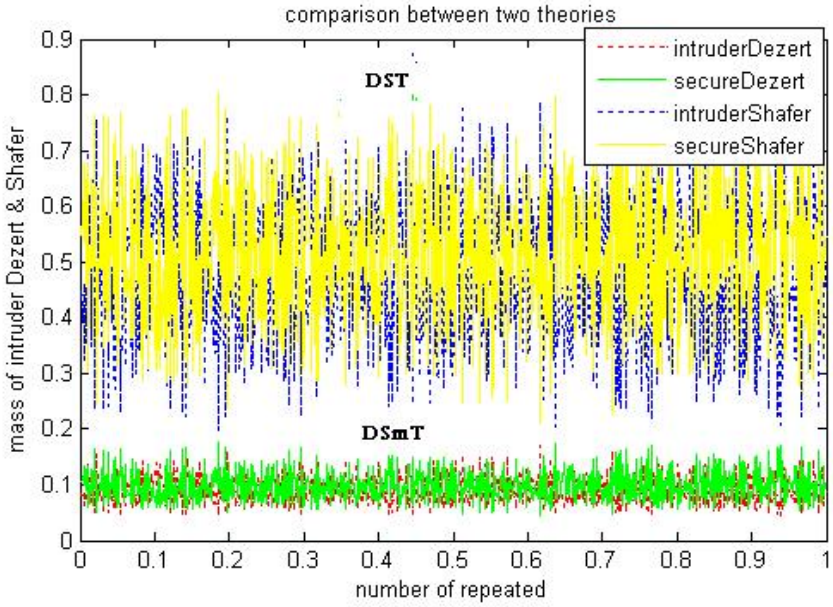

Figure 2. The result of combination of four sensors information with two methods (DST and DSmT).

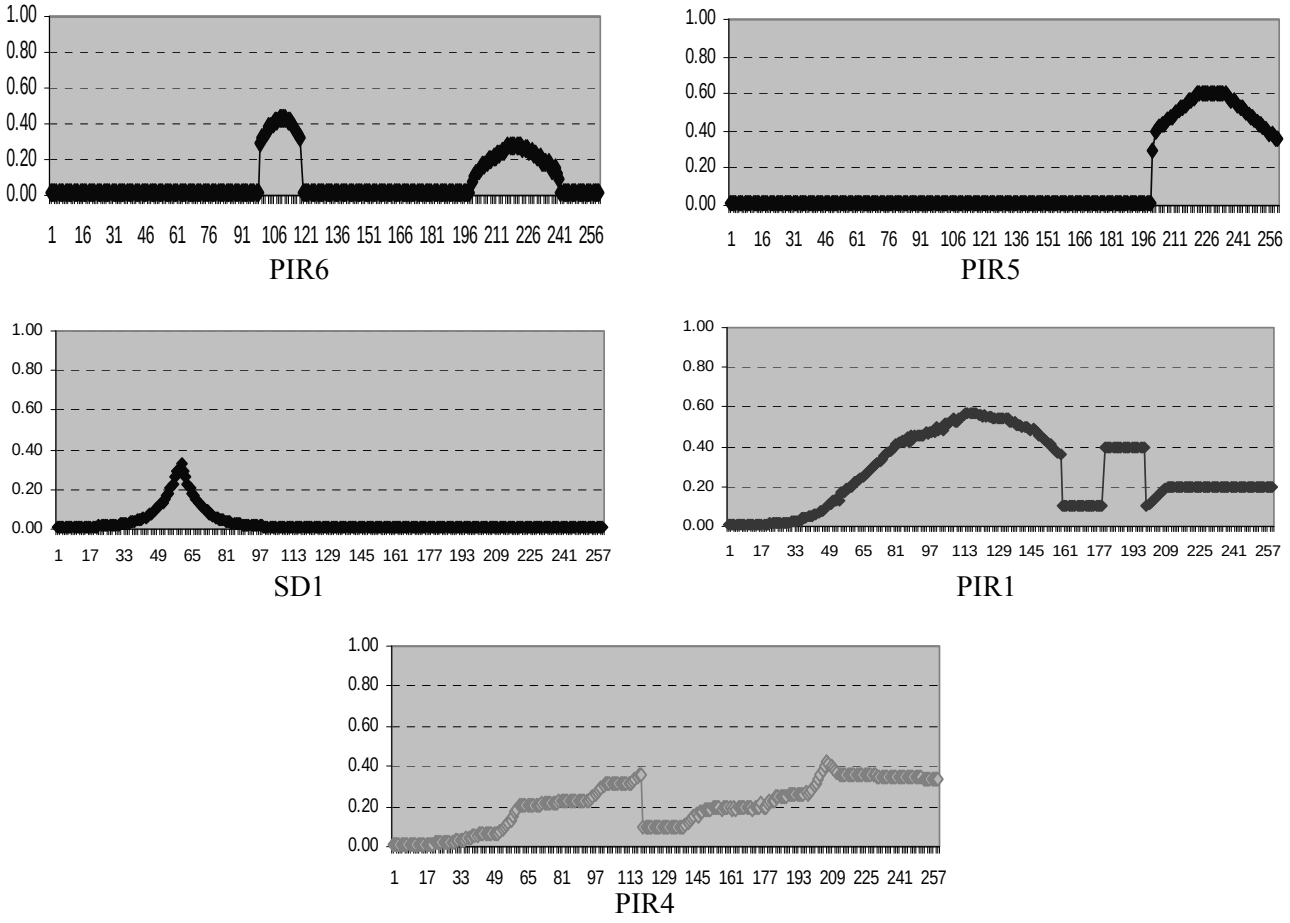

Figure 3. The output pattern of sensors.

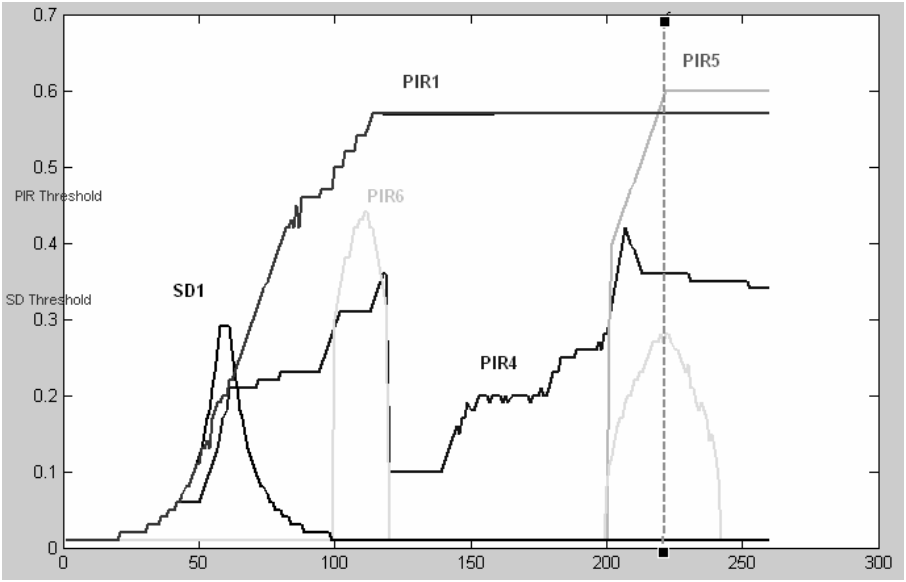

Figure 4. Detecting the intruder on 208th sample.

the worst conditions of the sensors have been considered. However, the proposed system based on data fusion concept could easily detect the intruder.

One of the advantages of using this system is detecting the zone where the intruder attacks, so based on the location in the house, the different mechanisms could be used in order to trap the intruder.

The higher reliability of the simulated security system was achieved due to the redundancy and complementary characteristics of the sensor fusion itself, and the nature of parallel data processing of sensor fusion approach provides less costly information processing. In this scenario the "m (intruder ∩ secure) = Ø", as a result, the DST and DSmT coincided each other. For further research work "m (intruder ∩ secure) ≠ Ø" could be considered and also the other fusion approaches using fuzzy integral operator or neuro-fuzzy method.

6. REFERENCES

1. Blaylock, N. and Allen, J., "Statistical Goal Parameter Recognition", ***14th International Conference on Automated Planning and Scheduling (ICAPS'04)***, Department of Computer Science, University of Rochester, Rochester, New York, U.S.A., (June 3-7, 2004), 297-304.
2. Sentz, K. and Ferson, S., "Combination of Evidence in Dempster-Shafer Theory", Sandia National Laboratories SAND 2002-0835, (April 2002).
3. Wu1, H., Siegel, M., Stiefelhagen, R. and Yang, J., "Sensor Fusion using Dempster-Shafer Theory", ***Instrumentation and Measurement Technology Conference, IMTC '03, Proceedings of the 20th IEEE***, Vol. 2, (May 20-22, 2003), 907-912.
4. Smarandache, F. and Dezert, J., "Advances and Applications of DSmT for Information Fusion, American Research Press, Rehoboth, U.S.A., (2004).
5. Dezert, J. and Smarandache, F., "On the Generation of Hyper-Powersets for DSmT", ***Proceedings of the 6th International Conference of Information Fusion***, Vol. 2, (July 2003), 1118-1125.
6. Dezert, J. and Smarandache, F., "Partial Ordering of Hyper-Powersets and Matrix Representation of Belief Functions Within DSmT", ***Proceedings of the 6th International Conference of Information Fusion***, Vol. 2, (July 2003), 1230-1238.
7. Rowshan, Sh. and Simonetta, R., "Intrusion Detection for Public Transportation Facilities Handbook", ***Transportation Research Board of the National Academies***, Washington D.C., U.S.A., (2003).
8. Henderson, T., Grant, E. and Luthy, K., "Precision Localization in Monte Carlo Sensor Networks", ***ISCA 18th International Conference on Computer Applications in Industr. and Engineering***, Sheraton Moana Surfrider, Honolulu, Hawaii, U.S.A., (November 9-11, 2005), 26-31.