Designing a Home Security System Using Sensor Data Fusion with DST and DSmT Methods

Behzad_ Moshiri
Control and Intelligent Processing
Center of Excellence
University of Tehran
Tehran, Iran
moshiri@ut.ac.ir

Arezou_Moussavi Khalkhali
Faculty of Post Graduate
Islamic Azad University,
Southern unit
Tehran, Iran
arezou_moussavi@yahoo.com

Hamid Reza_ Momeni
Department of Electrical
Engineering
Tarbiat Modarres University
Tehran,Iran
momeni_h@modares.ac.ir

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

Keywords: intrusion, intelligent housing system, Dempster-Shafer reasoning, DSmT approach, information fusion

1 Introduction

Having a security system in homes and intelligent buildings that cause welfare and rest, is a substantial category in district of creating security systems. Recent studies on sensor data fusion technologies persuade researchers to look for the better techniques with a higher assurance of fusing 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 and 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.

In 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, which its 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 :

$$m : 2^θ \to [0, 1], \ m(Ø) = 0, \ \sum_{A \in 2^θ} m(A) = 1 \quad (1)$$

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, 2, 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 Θ= {θ1, θ2,…, θn) is the frame of discernment of the system to be considered. So, m: 2^{θ} → [0, 1] is defined as follows:

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

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

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

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

DsmT comes to overcome the two deficiencies in DST :
  1. In DST, the elements of the frame of discernment must be exclusive and exhaustive, but in DSmT they are not exclusive.
  2. 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 :

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

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 picture 1[7]. The security system discussed here is a system, capable of detecting intruders. If there is need to protect the home from fire, as a result the smoke detectors and heat detectors should be used. Now four kinds of sensors are used to implement the system :

- *Wall vibration* intended to detect mechanical vibrations caused by chopping, sawing, drilling, ramming or any type of physical intrusion.

- *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).

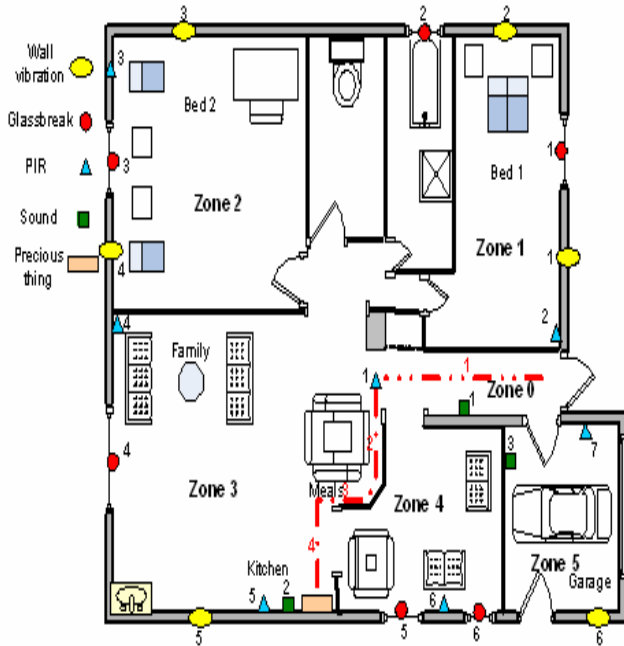 - *Sound detectors* that "listen" to the noises produced by the intruder.

- *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 picture 1.
Considering the table1, the probability of detection of sensors is estimated as following [8].

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

Picture1. Home plan with sensors located in it

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 for every 0.5 seconds. As soon as one sensor rises up the threshold, the system looks for another and combines the output of them to check if there is a real attacking. If an intrusion happened, depending on which zone's sensors participate in combination, the corresponding zone alarm will be triggered.

The sensors are sensitive to the delay between two detections and the system resets if the intruder delayed between two actions, so the system is programmed in a

way that each time one sensor's output 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.

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

First, consider a room with the 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 [9].

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 Fig.1.

As shown in Fig.1 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.
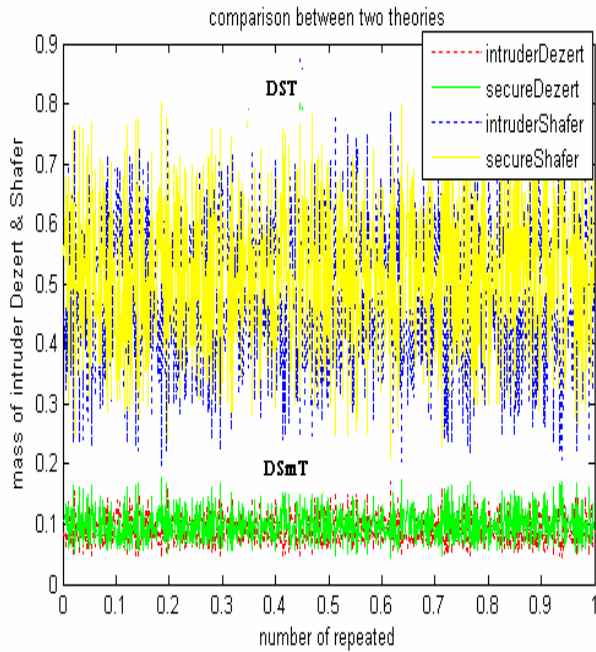

Fig.1. The result of combination of four sensors information with two methods (DST and DSmT)

Fig.2 indicates the function of detecting by the sensors. It is assumed that the total time for traversing the path to reach the object shown in picture 1 is 130 seconds. Another assumption is that each sensor takes a sample in every 0.5 seconds. The horizontal axis in Fig.2 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 until around the sample 57, where the peak of the probability of the detection of the sensor appears.
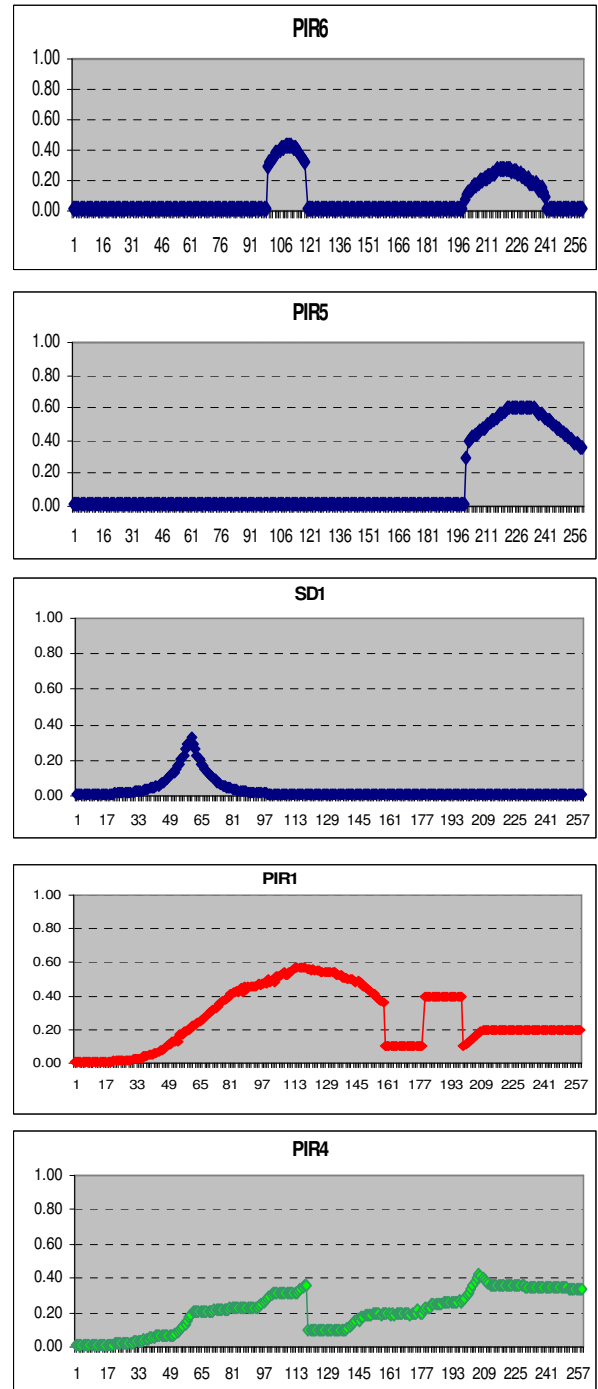

Fig.2. The output pattern of sensors

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 also decreased.

It was assumed that it takes 60 seconds (120 samples) to pass the corridor (path number 1), considering 30 seconds for passing the meal table (path2), 10 seconds for crawling the path 3, and 30 seconds for reaching the object (path4).

Fig.3 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.

One of the advantages of using this system is detecting the zone where the intruder attacked into it, so based on the location of 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 the parallel processing of sensor data 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.
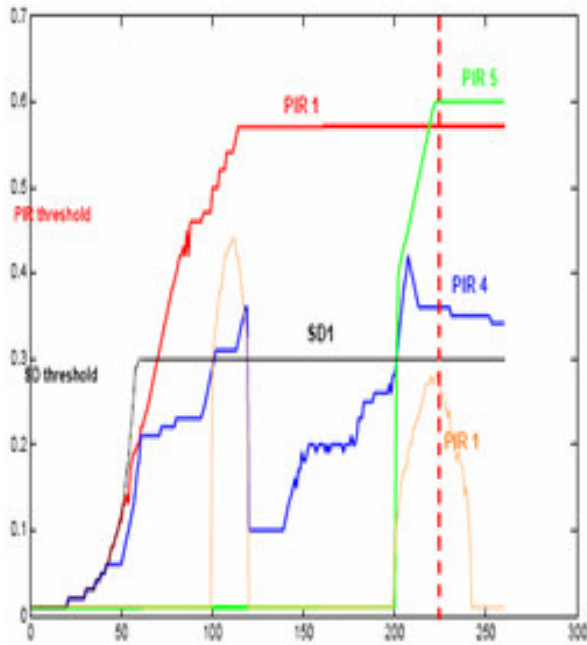

Fig.3. Detecting the intruder on 208th sample

5   Conclusion

As shown in simulation results the probabilities of the sensors for activating are very low. At least PIR's are more sensitive than what were supposed here and the sensors had to detect the intrusion with higher probability. Meanwhile the worst conditions of the sensors have been considered. However, the proposed system based on data fusion concept could easily detect the intruder.

References

[1] Nate_Blaylock, and James_Allen, "Statistical Goal Parameter Recognition", Department of Computer Science , University of Rochester, Rochester, New York, USA, 14th International Conference on Automated Planning and Scheduling (ICAPS'04), pages 297-304, Whistler, British Columbia, June 3-7 2004.

[2] Kari_Sentz, and Scott_Ferson, "Combination of Evidence in Dempster-Shafer Theory", Sandia National Laboratories SAND 2002-0835, April 2002.

[3] Huadong_Wu1, and Mel_Siegel, and Rainer_ Stiefelhagen, and Jie_Yang, "Sensor Fusion Using Dempster-Shafer Theory", IEEE Instrumentation and Measurement Technology Conference, Anchorage, AK, USA, 21-23 May 2002.

[4] Florentin_Smarandache, and Jean_Dezert, Advances and Applications of DSmT for Information Fusion, American Research Press, Rehoboth, 2004.

[5] Jean_Dezert, and Florentin_Smarandache, "On the generation of hyper- powersets for DSmT, " published in the Proceedings of The 6th International Conference on Information Fusion, FUSION 2003, Radisson Hotel, Cairns, Queensland, Australia, 8-11 July 2003.

[6] Jean_Dezert, and Florentin_Smarandache, "Partial ordering of hyper-powersets and matrix representation of belief functions within DSmT", published in the Proceedings of the sixth International Conference on Information Fusion, FUSION 2003, Radisson Hotel, Cairns, Queensland, Australia, 8-11 July 2003.

[7] www.rylebrown.com.au/securitybooklet.pdf.

[8] Shahed_Rowshan and Richard_J.Simonetta, "Intrusion Detection for Public Transportation Facilities Handbook", Transportation Research Board of the national academies, Washington D.C., 2003.

[9] Thomas_C.Henderson, and Edward_Grant, and Kyle_Luthy, "Precision Localization in Monte Carlo Sensor Networks", ISCA 18th International Conference on Computer Applications in Industry and Engineering, November 9-11, 2005, Sheraton Moana Surfrider, Honolulu, Hawaii, USA, 2005.