Design of an Intelligent Housing System Using Sensor Data Fusion Approaches

Arezou_Moussavi Khalkhali, Behzad_ Moshiri, Hamid Reza_ Momeni
Telecommunication Infrastructure Company of Iran,
Ministry of Information and Communication Technology,
Control and Intelligent Processing Centre of Excellence, School of ECE,
University of Tehran
Department of Electrical Engineering, Tarbiat Modarres University
Tehran, Iran

1. Introduction

Today's security systems are expected to function more accurately and efficiently. Intelligent homes as a high demanded future technology need to become less expensive and more certain. These goals could be achieved by using fusion methods. In the following, two theories are applied to a home security system which are Dempster-Shafer evidential theory and Proportional Conflict Redistribution Rule no.5 (PCR5). The significant aim of this research is to show the application of fusion methods in order to establish the security system used in Intelligent Housing Systems (IHS) and detecting the precise location of the intruder at home, which are not viable through the traditional systems. The exactitude of PCR5 method to Dempster-Shafer Theory (DST) has been considered after applying them to the system. In the following, home security system is simulated by MATLAB. In sections 2 and 3, this research work will review the DST and PCR5 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. Therefore, the Dempster-Shafer (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 :

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

The probability that the true answer is A denoted by a *confidence interval*:
[Belief (A), Plausibility (A)] in which,

Source: Sensor and Data Fusion, Book edited by: Dr. ir. Nada Milisavljević,
ISBN 978-3-902613-52-3, pp. 490, February 2009, I-Tech, Vienna, Austria

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

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

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:

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

In which $k = \sum_{A \cap B = \varphi} m_1(A) m_2(B)$ is interpreted as a measure of conflict among the various sources (Blaylock & Allen, 2004; Sentz & Ferson, 2002; Wu et al., 2002).
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
m1 (G) = 0.6, m1 (V) = 0.3, θ1= (GUV) = 0.1,
m2 (G) =0.5, m2 (V) =0.35, θ1= (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. Proportional conflict redistribution rule no.5 (PCR5) basis

The basic idea of PCR rules is reallocating the partial conflicts to the non-empty sets that contribute in the conflict mass.
The process of applying PCR to calculating the total mass of several sources is as follows:

- Applying the conjunctive rule to calculate the belief masses of sources;
- Calculating the total or partial conflicting masses;
- Redistributing the total or partial conflicting masses to the non-empty sets contributed in the conflicts correspondingly to their original masses.

Several versions of PCR rules derived from the way in which the conflicting mass is reallocating to the non-empty sets.
According to the PCR5 rule the partial conflicting mass redistributes to the non-empty sets that involved in the partial conflict.
The PCR 5 formula for combining two sources is as follows (Dezert & Smarandache, 2006, (a)):

mPCR5 (Ø) = 0 and $\forall X \in G \setminus \{\theta\}$

$$\mathrm{mPCR5}(X)=\mathrm{m12}(X)+\sum_{\substack{Y\in G\setminus\{X\}\\ X\cap Y=\varphi}}\left[\frac{m_1(X)^2 m_2(Y)}{m_1(X)+m_2(Y)}+\frac{m_2(X)^2 m_1(Y)}{m_2(X)+m_1(Y)}\right] \tag{5}$$

Where $\mathrm{m12}(X)\overset{\Delta}{=}\sum_{\substack{X,Y\in G^{\Theta}\\ X\cap Y=X}} m_1(X)m_2(Y)$

Proof and complete explanation about PCR5 rule and other PCR rules could be found at (Dezert & Smarandache, 2006(a), Smarandache & Dezert, 2006(b)).
In this paper we use the above formula to combine the result of two sources with the third one and so forth.
PCR5 rule is more exact than Dempster's rule. This is because of how it redistributes the conflicting mass to the sets, which are involved in the conflict rather than redistributing to all non-empty sets like what happens in Dempster's rule.

4. Simulation results

In order to simulate the security system, imagine a home with sensors located in different areas according to Fig. 1. 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 IHS, 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 the table1, the probability of detection of sensors is estimated as following (Rowshan & Simonetta, 2003):
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. These values are supposed to be 0.25 for wall sensor and 0.4 for glass-break detectors. The ignorance of all 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 would be triggered.

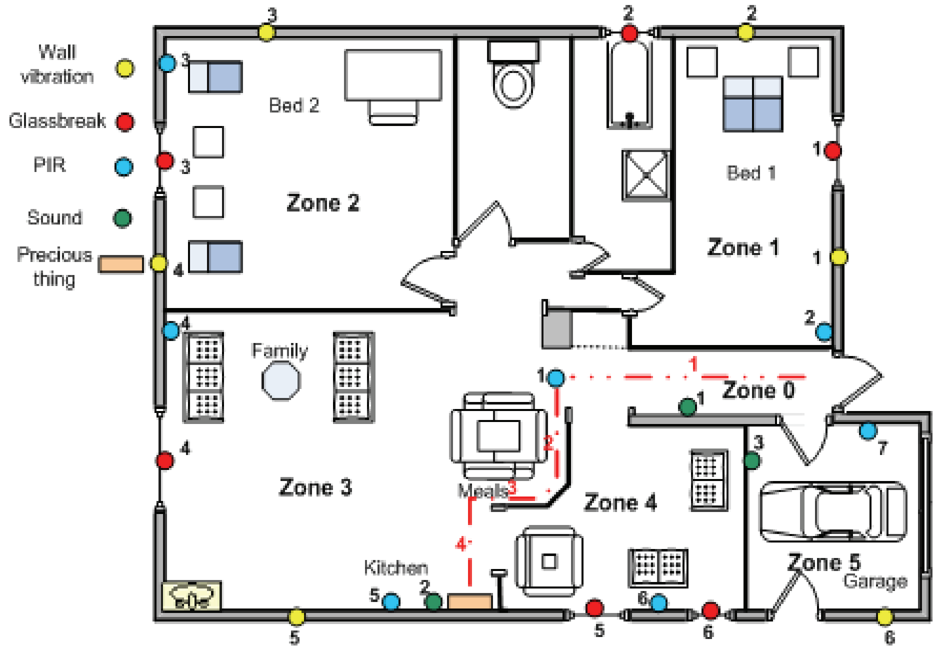


Fig. 1. House plan with sensors located in it

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. As soon as the new value becomes greater than the last one, the newer one will be held and subsequently this recent new value would be considered in the corresponding calculation process.

First, consider a room with the five sensors mentioned above: two glass-break detectors, two PIRs, and one wall sensor. The mentioned system is simulated by the Monte-Carlo method in which, one mathematical experiment with random numbers is repeated for thousands of times (C.Henderson et al., 2005).

The probabilities for detection produced by the sensors are random numbers. Applying the output value for the sensors is repeated for 1000 times. About 100 times out of 1000, the results of two methods contradicted each other. One of those contradictory conditions is considered below. The mass of intruder and secure for five sensors are as follows:

m1(i) = 0.17	m2(i) = 0.76	m3(i) = 0.16	m4(i) = 0.15	m5(i) = 0.89
m1(s) = 0.73	m2(s) = 0.14	m3(s) = 0.74	m4(s) = 0.75	m5(s) = 0.01

$\theta = 0.1$

With these probabilities, DST method considered the situation safe; however, PCR5 detects the condition as a dangerous one. The calculation process for DST and PCR5 is shown in table.2 and table.3.

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

Table 1. The estimate probability of detection for sensors

The step of calculation is according to the direction of arrows in the upper left cell of the tables. I.e. by fusing m1 and m2, m12 is achieved, then by fusing m3 and m12, m123 is deduced, and so forth.

Take note that although sensors number 2 and 5 display a high range of perilous situation, the DST method did not pay attention and announce the safe mode, however using PCR5 method by which conflict mass redistribute proportionally to the partial masses, danger mode is detected.

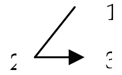
	m1(i)=0.17 m1(s)=0.73 θ1=0.1	m3(i)=0.16 m3(s)=0.74 θ3=0.1	m4(i)=0.15 m4(s)=0.75 θ4=0.1	m5(i)=0.89 m5(s)=0.01 θ5=0.1
m2(i)=0.76 m2(s)=0.14 θ2=0.1	K=0.4214 m12(i)=0.5273 m12(s)=0.4490 θ12=0.0237	K=0.5380 m123(i)=0.2619 m123(s)=0.7337 θ123=0.0044	K=0.6935 m1234(i)=0.0954 m1234(s)=0.9040 θ1234=6.36e-004	K=0.1945 m1234(i)=0.4883 m1234(s)=0.5113 θ1234=3.27e-004

Table 2. Calculation of the mass of intruder and secure with DST method

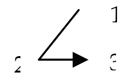
	m1(i)=0.17 m1(s)=0.73 θ1=0.1	m3(i)=0.16 m3(s)=0.74 θ3=0.1	m4(i)=0.15 m4(s)=0.75 θ4=0.1	m5(i)=0.89 m5(s)=0.01 θ5=0.1
m2(i)=0.76 m2(s)=0.14 θ2=0.1	m12(i)=0.5182 m12(s)=0.4718 θ12=0.01	m123(i)=0.3134 m123(s)=0.6856 θ123=0.001	m1234(i)=0.1662 m1234(s)=0.8337 θ1234=1e-004	m1234(i)=0.5493 m1234(s)=0.4507 θ1234=1e-004

Table 3. Calculation of the mass of intruder and secure with PCR5 method

The above situation can be mapped into a dining room with five sensors included two glass-break detectors, two PIRs, and one wall sensor. One of the glass-break detectors and one of the PIRs detect the intruder with the mass 0.89 and 0.76 respectively. The other sensors cannot detect anything according to their masses. Applying two methods implied that by using PCR5 rule, which is more exact than DST, the system could detect the dangerous situation. Now by implementing the main scenario to IHS with 22 sensors, there can be a better understanding between two theories by comparing the differences.
Fig. 2 (1 to 5) indicated the function of detecting by the sensors, i.e. it shows the sensors' detection status corresponding to the movement of an intruder.
It is assumed that the total time for traversing the path to reach the object shown in Fig. 1 is 130 seconds. Another assumption is that each sensor takes a sample in every 0.5 seconds.

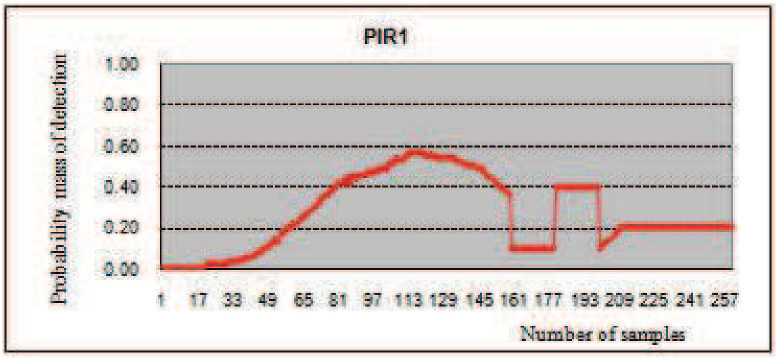


Fig. 2.1. Output pattern of PIR1 located in zone 0

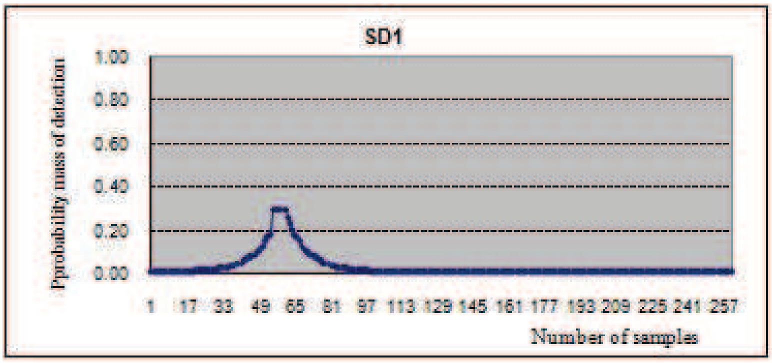


Fig. 2.2. Output pattern of SD1 located in zone 0

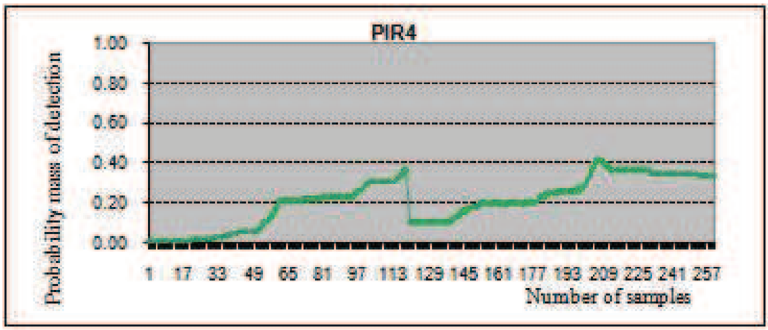


Fig. 2.3. Output pattern of PIR4 located in zone 3

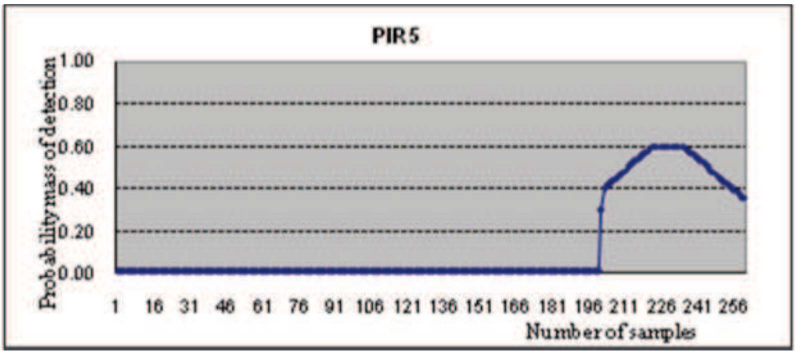


Fig. 2.4. Output pattern of PIR5 located in zone 3

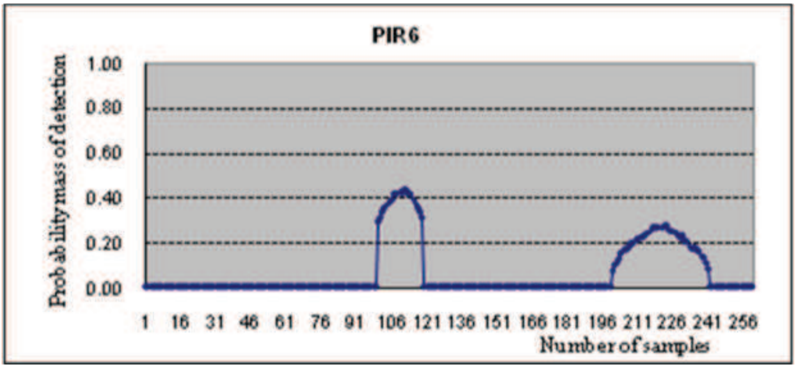


Fig. 2.5. Output pattern of PIR6 located in zone 3

Therefore, there are 260 samples in total. 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. This is due to the minimum distance between the intruder and the sensor. Afterward when the intruder receded from 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), 30 seconds to pass the meal table (path 2), 10 seconds to crawl the path 3, and 30 seconds to reach the object (path 4).

By simulating the security system with MATLAB, around sample 56 the PCR5 method announces the danger mode, but DST is safe yet until the 208 sample. At sample 208 DST alarms that the intruder attacks in zone 3. In sample 56 the mass of intruder and secure of PIR4, SD1, and PIR1 in the entrance of the home are as follows:

$m_{PIR4}(i) = 0.47$ $m_{PIR4}(s) = 0.43$ $\theta_{PIR4} = 0.1$
$m_{SD1}(i) = 0.3$ $m_{SD1}(s) = 0.6$ $\theta_{SD1} = 0.1$
$m_{PIR1}(s) = 0.58$ $m_{PIR1}(i) = 0.32$ $\theta_{PIR1} = 0.1$

With using formulas number 4 and 5 it can be seen that by DST calculation the system is in the safe mode and by PCR5 is in the attack mode. Therefore, the system realized the intruder at the first minutes of his entrance and alarmed or called the local police station, or even locked the doors or it can done any prevention actions by which it is programmed. The process for calculating the PCR5 mass of intruder and secure is shown below.

$m_{12PCR5}(i) = 0.218 + [(0.13254/1.07) + (0.0387/0.73)] = 0.3949$

$m_{12PCR5}(s) = 0.361 + [(0.05547/0.73) + (0.1692/1.07)] = 0.5951$
$\theta_{12PCR5} = 0.01$
$m_{123PCR5}(i) = 0.5154$
$m_{123PCR5}(s) = 0.4845$
$\theta_{123PCR5} = 0.001$

5. Conclusion

As shown in Fig.2 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 for detection 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 attacked, 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 conflicting masses in PCR5 are transferred to those that contributed in conflicting mass. For future work, "m (intruder ∩ secure) ≠ Ø" could be considered; meanwhile, the other fusion approaches using fuzzy integral operator or neuro-fuzzy method could be applied.

6. References

Blaylock, N. ; and Allen, J. (2004). Statistical Goal Parameter Recognition, *Proceedings of the Fourteenth International Conference on Automated Planning and Scheduling (ICAPS'04),* PP. 297-304, Whistler, British Columbia, June 3-7, 2004, AAAI Press, Whistler

C.Henderson, T.; Grant, E. & Luthy, K. (2005). *Precision Localization in Monte Carlo Sensor Networks*, Proceedings of the ISCA 18th International Conference on Computer Applications in Industry and Engineering PP.26-31, ISBN 1-880843-57-9, Sheraton Moana Surfrider, Honolulu, Hawaii, U.S.A., November 9-11, 2005, ISCA

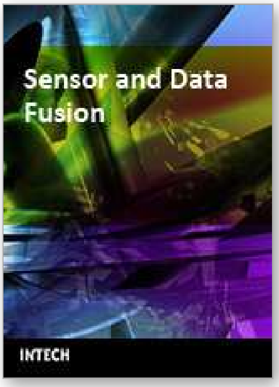
(a) Dezert J.; Smarandache F. (2006). Introduction to the Fusion of Quantitative and Qualitative Beliefs, *Information & Security, an International Journal*, Vol., 20, (June 2006), pp. 9-49

Rowshan, Sh.; Simonetta, R. (2003). *Intrusion Detection for Public Transportation Facilities Handbook*, Transportation Research Board of the National Academies, ISBN 030906760X, Washington D.C., U.S.A.

Sentz, K. ; Ferson, S. (2002). Combination of Evidence in Dempster-Shafer Theory, *Technical Report SAND 2002-0835*, 96 pages, Sandia National Laboratories, Albuquerque, NM

(b) Smarandache F.; Dezert J. (2006). *Advances and applications of DSmT for Information Fusion*, (Collected works), Vol.2, American Research Press, ISBN 1-59973-000-6, Rehoboth, U.S.A.

Wu, H.; Siegel, M.; Stiefelhagen, R. & Yang, J. (2002). Sensor Fusion Using Dempster-Shafer Theory, *Proceedings of 19th IEEE Instrumentation and Measurement Technology Conference* , IMTC '03, Vol. 2, PP. 907-912, , May 20-22, 2002, IEEE, Anchorage



Sensor and Data Fusion

Edited by Nada Milisavljevic

ISBN 978-3-902613-52-3

Hard cover, 436 pages

Publisher I-Tech Education and Publishing

Published online 01, February, 2009

Published in print edition February, 2009

Data fusion is a research area that is growing rapidly due to the fact that it provides means for combining pieces of information coming from different sources/sensors, resulting in ameliorated overall system performance (improved decision making, increased detection capabilities, diminished number of false alarms, improved reliability in various situations at hand) with respect to separate sensors/sources. Different data fusion methods have been developed in order to optimize the overall system output in a variety of applications for which data fusion might be useful: security (humanitarian, military), medical diagnosis, environmental monitoring, remote sensing, robotics, etc.