HAL open science

Evidence Theory for Cyber-Physical Systems

Riccardo Santini, Chiara Foglietta, Stefano Panzieri

To cite this version:

Riccardo Santini, Chiara Foglietta, Stefano Panzieri. Evidence Theory for Cyber-Physical Systems. 8th International Conference on Critical Infrastructure Protection (ICCIP), Mar 2014, Arlington, United States. pp.95-109, 10.1007/978-3-662-45355-1_7 . hal-01386757

HAL Id: hal-01386757

https://inria.hal.science/hal-01386757v1

Submitted on 24 Oct 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Chapter 7

EVIDENCE THEORY FOR CYBER-PHYSICAL SYSTEMS

Riccardo Santini, Chiara Foglietta and Stefano Panzieri

Abstract Telecommunications networks are exposed to new vulnerabilities and threats due to interdependencies and links between the cyber and physical layers. Within the cyber-physical framework, data fusion methodologies such as evidence theory are useful for analyzing threats and faults. Unfortunately, the simple analysis of threats and faults can lead to contradictory situations that cannot be resolved by classical models.

Classical evidence theory extensions, such as the Dezert-Smarandache framework, are not well suited to large numbers of hypotheses due to their computational overhead. Therefore, a new approach is required to handle the complexity while minimizing the computational overhead. This paper proposes a hybrid knowledge model for evaluating the intersections among hypotheses. A hybrid frame of discernment is presented using a notional smart grid architecture that transforms the basic probability assignment values from the classical framework. Several analyses and simulations are conducted, with the goal of decreasing conflicts between two independent sources. A comparative analysis is performed using different frames of discernment and rules in order to identify the best knowledge model. Additionally, a computational time analysis is conducted.

Keywords: Cyber-physical systems, Dempster-Shafer evidence theory

1. Introduction

The pervasive growth of network technology has led to the integration of telecommunications technologies and physical processes to create cyber-physical systems. Cardenas, *et al.* [3] define a cyber-physical system as integrating computing, communications and storage capabilities with monitoring and/or control of entities in the physical world, which is done in a dependable, safe, secure and efficient manner under real-time constraints. A cyber-physical system is characterized by the tight connection and coordination between cyber and

physical resources. Poovendran [7] notes that the concept of a cyber-physical system changes the notion of a physical system to include humans, the infrastructure and the software platform in which the overall system is highly networked.

Examples of cyber-physical systems include supervisory control and data acquisition (SCADA) systems that monitor and control electric power grids, oil and gas pipelines, water supply networks and wastewater treatment systems [2]. Research activities related to these systems usually focus on reliability and resilience. Krishna and Koren [5] have proposed an adaptive control methodology for cyber-physical systems to handle failures of cyber and physical components. Cardenas, *et al.* [3] have studied integrity, confidentiality and denial-of-service attacks on cyber-physical systems. This paper considers cyber-physical systems in the context of evidence theory, with the goal of properly identifying the causes of faults and threats when a cyber attack compromises power grid operations. Evidence theory has been applied in multi-sensor fusion problems such as diagnosis [1]. Siaterlis and Genge [10] have proposed an evidence theory framework for anomaly detection. In contrast, this paper proposes a hybrid knowledge model for evaluating the intersections among hypotheses. The new approach handles complexity while reducing the computational overhead.

2. Evidence Theory

Evidence theory is a mathematical formalism for handling uncertainty by combining evidence from different sources to converge to an accepted belief [9]. The basic concept is to reduce uncertainty in order to identify the set that contains the correct answer to a question.

2.1 Frame of Discernment

Let $\Omega = \{\omega_1, \cdots, \omega_n\}$ be the frame of discernment – the set of hypotheses that represents a possible value of the variable ω. In classical evidence theory, the hypotheses are assumed to be mutually exclusive [4, 9].

Given a frame of discernment Ω, it is possible to define the power set $\Gamma(\Omega) = \{\gamma_1, \cdots, \gamma_{2^{|\Omega|}}\}$ with cardinality $|\Gamma(\Omega)| = 2^{|\Omega|}$. This set contains all possible subsets of Ω, including the empty set $\gamma_1 = \emptyset$ and the universal set (frame of discernment) $\gamma_{2^{|\Omega|}} = \Omega$.

2.2 Basic Probability Assignment

Smets and Kennes [12] have defined a model for evidence theory called the transferable belief model. The model relies on a basic probability assignment (BPA) function: $m : \Gamma(\Omega) \rightarrow [0, 1]$. The BPA function assigns a value between 0 and 1 to each element of the power set subject to the constraint:

$$\sum_{\gamma_a \subseteq \Gamma(\Omega)} m(\gamma_a) = 1 \quad \text{with} \quad m(\emptyset) = 0. \tag{1}$$

Each element γ_a with $m(\gamma_a) \neq 0$ is called a focal set.

One of the key goals is to quantify the confidence of propositions of the form: "the true value of ω_i is in γ_a" where $\gamma_a \in \Gamma(\Omega)$. For $\gamma_a \in \Gamma(\Omega)$, $m(\gamma_a)$ is the portion of confidence that supports exactly γ_a. This means that the true value is in the set γ_a; however, due to the absence of additional information, it is not possible to better support any strict subset of γ_a. Note that this does not correspond to a probability function and it does not respect the property of additivity, i.e., $m(\gamma_a \cup \gamma_b) \neq m(\gamma_a) + m(\gamma_b)$.

Each BPA is an atomic element in the transferable belief model. In fact, each sensor, agent and node must be able to assign BPA values based on subjective assumptions or using algorithms that automatically determine the assignments.

2.3 Combination Rules

In the case of independent information sources, a rule that aggregates the data is required. Several combination rules have been proposed in the literature. The most commonly rules are Dempster's rule [4] and Smets' rule [12]. This paper considers an additional rule, called proportional conflict redistribution no. 6 (PCR-6), in order to obtain sufficient solutions in terms of a quality-conflict ratio.

Dempster's Rule. Dempster's rule of combination [4], which was the first to be formalized, is a purely conjunctive operation. This rule strongly emphasizes the agreement between multiple sources and ignores conflicting evidence through a normalization factor:

$$\text{Dempster}\{m_i, m_j\}(\emptyset) = 0 \tag{2}$$

$$\text{Dempster}\{m_i, m_j\}(\gamma_a) = \frac{\sum_{\gamma_b \cap \gamma_c = \gamma_a} m_i(\gamma_b) m_j(\gamma_c)}{1 - \sum_{\gamma_b \cap \gamma_c = \emptyset} m_i(\gamma_b) m_j(\gamma_c)} \qquad \forall \gamma_a \in \Gamma(\Omega). \tag{3}$$

Note that Dempster's rule assigns a null mass to the empty set, which has certain limitations when the conflict value is very high.

Smets' Rule. Smets' rule of combination [12] provides the ability to explicitly express contradictions in the transferable belief model by letting $m(\emptyset) \neq 0$. Smet's rule, unlike Dempster's rule, avoids normalization while preserving commutativity and associativity. The rule is formalized as follows:

$$\text{Smets}\{m_i, m_j\}(\gamma_a) = m_i(\gamma_a) \otimes m_j(\gamma_a) \qquad \forall \gamma_a \in \Gamma(\Omega) \tag{4}$$

where

$$m_i(\gamma_a) \otimes m_j(\gamma_a) = \sum_{\gamma_b \cap \gamma_c = \gamma_a} m_i(\gamma_b) m_j(\gamma_c) \qquad \forall \gamma_a \in \Gamma(\Omega). \tag{5}$$

The inequality $m(\emptyset) > 0$ can be explained in two ways. The first is the open world assumption of Dempster [4], which expresses the idea that the frame of discernment must contain the true value. Necessarily, if the open world assumption is true, then the set of hypotheses must contain all the possibilities. Under this interpretation, if $\emptyset$ is the complement of Ω, then mass $m(\emptyset) > 0$ represents the case where the truth is not contained in Ω.

The second interpretation of $m(\emptyset) > 0$ is that there is some underlying conflict between sources. Hence, the mass $m(\emptyset)$ represents the degree of conflict. In particular, the mass $m(\emptyset)$ is computed as:

$$m_i(\emptyset) \otimes m_j(\emptyset) = 1 - \sum_{\gamma_b \cap \gamma_c = \emptyset} \left(m_i(\gamma_b) \otimes m_j(\gamma_c) \right). \tag{6}$$

PCR-6 Rule. The proportional conflict redistribution rule no. 6 (PCR-6) [11] is a non-Bayesian rule for combining BPAs. PCR-6 considers two sources of information evaluated as $\mathrm{PCR}_6(\emptyset) = 0$ and $\forall \gamma_a \in \Gamma(\Omega) \setminus \emptyset$ according to the following equation:

$$\mathrm{PCR}_6\{m_i, m_j\}(\gamma_a) = \mathrm{Smets}\{m_i, m_j\}(\gamma_a) + \sum_{\substack{\gamma_b \in \Gamma(\Omega) \setminus \gamma_a, \\ \gamma_a \cap \gamma_b = \emptyset}} \left[\frac{m_i^2(\gamma_a) m_j(\gamma_b)}{m_i(\gamma_a) + m_j(\gamma_b)} + \frac{m_j^2(\gamma_a) m_i(\gamma_b)}{m_j(\gamma_a) + m_i(\gamma_b)} \right]. \tag{7}$$

The conflict is redistributed between the elements of the power set. In the case of high-conflict sources, only the focal sets that generate the conflict are involved in the redistribution (see the normalization factor in Equation (7)). Therefore, the solutions obtained after the combination are better in terms of the quality-conflict ratio.

3. Architecture for Smart Grid Diagnostics

A smart grid is an excellent example of a cyber-physical system – it comprises the physical electrical grid and an integrated telecommunications network that monitors and controls the energy flow. Figure 1 shows a simplified cyber-physical representation of a smart grid. Note that the EMS/DMS control system uses a telecommunications network to send and receive information from substations in the power grid.

Two assumptions are made about the smart grid architecture. The first assumption concerns the information exchanged by the equipment: under normal conditions, the cyber information can be represented by the timing and volume of four packet types (Command, Ack-Receive, Reply and Ack-Response). The second assumption concerns the sensors used for smart grid management: a packet-sniffing sensor is used in the cyber layer to detect the number of packets

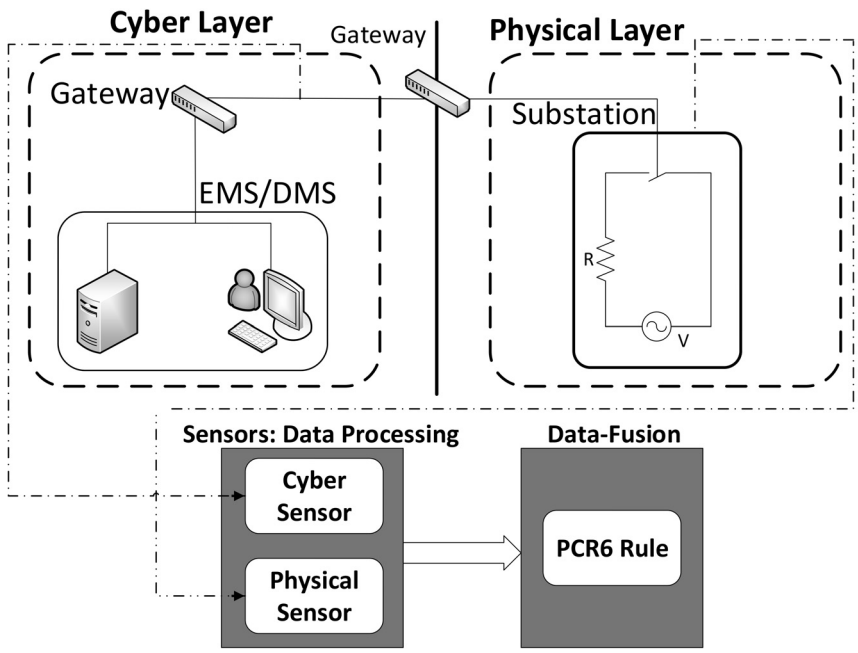


Figure 1. Cyber-physical representation of a smart grid.

in the network and a physical layer sensor is used to indicate whether a piece of equipment (e.g., circuit breaker) is working or not.

In order to apply evidence theory to determine the cause of a malfunction, it is necessary to define the appropriate frame of discernment Ω. In the the example under consideration, there are three hypotheses: normal behavior (N), physical fault (P) and cyber threat (C). The system has normal behavior when the breaker is working and the network packets conform to the operational timing and volume constraints. A physical fault exists when the sensors detect a breaker fault. A cyber threat exists when there is excess or low packet volume. As shown in Figure 2, in the classical evidence theory framework, the hypotheses are mutually exclusive with empty intersections.

A plausible scenario is simulated using the specified architecture and parameters. The scenario involves an attacker who compromises the operation of a piece of equipment (circuit breaker) via a telecommunication attacks (distributed denial-of-service attack). A simulation, which has a duration of 100 seconds, is divided into four different situations:

- **Situation 1 (0 to 27 seconds):** The smart grid behaves normally and no alarms are detected. The breaker is working and the number of network packets in the specified time window is normal.

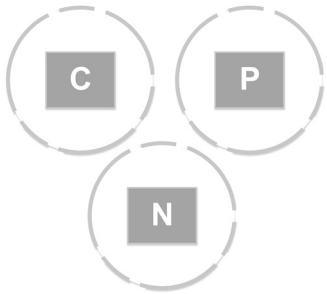


Figure 2. Representation of the frame of discernment.

- **Situation 2 (28 to 35 seconds):** The cyber sensor detects an increasing number of packets in the network (due to the attacker's intrusion), but the breaker is still working.
- **Situation 3 (36 to 95 seconds):** The cyber sensor and the physical sensor both detect anomalous behavior. The packet-sniffing sensor detects a high number of packets and the breaker does not respond to commands.
- **Situation 4 (96 to 100 seconds):** The smart grid is back to normal after the cyber-physical attack because the countermeasures were successful.

Table 1. Events during the simulation and the associated alarms.

Time (sec)	Events	Detecting Sensor
0 – 27	Normal State	–
28 – 35	Cyber Anomaly	Cyber Sensor
36 – 95	Cyber Anomaly + Physical Fault	Cyber + Physical Sensors
96 – 100	Normal State	–

Table 1 summarizes the simulation events, with a focus on the time and information sources.

The goal is to fuse all the data provided by the sensors during a simulation in order to detect a cyber-physical attack. As such, the relative frame of discernment Ω according to the classical evidence theory is:

$$\Omega = \{C, P, N\}\,. \tag{8}$$

Starting with Ω, the power set is:

$$\Gamma(\Omega) = \{\emptyset, C, P, N, C \cup P, C \cup N, P \cup N, C \cup P \cup N\}\,. \tag{9}$$

Each sensor has to distribute a unitary mass over specific focal sets during a simulation. Using a combination rule, a fusion result can then be obtained.

Specifically, the focal sets for the cyber sensor are $\{C, N, P \cup N, \Omega\}$. Note that a cyber security expert could identify a cyber anomaly, but is unlikely to discern a physical anomaly. Similarly, the focal sets for the physical sensor are $\{P, N, C \cup N, \Omega\}$.

Santini, *et al.* [8] have used the PCR-6 rule to develop metrics for identifying the effects of cyber attacks that are designed to inflict physical damage. A cyber-physical fault is detected in the presence of mutually exclusive hypotheses by noticing the existence of non-zero similar masses in the cyber cause set and the physical cause set. Such problems are primarily related to the BPA assignments for the sources, which are application dependent. Another problem relates to the interpretation of conflict values that is done in an *ad hoc* manner. The following exponential function (depending on the number of captured packets) is used as the BPA assignment to set the mass of $\{C\}$:

$$e^{-(a \cdot p)/x} \tag{10}$$

where a and p are positive tuning parameters and x is the number of packets. Equation (10) is used in the same manner to express the mass of $\{P\}$ after a physical fault, where x is the persistence of the fault.

When two information sources that have high conflict exist in the cyber and physical realms, the rough values obtained after fusion using the PCR-6 rule are unsuitable. The solution proposed in [8] is to evaluate at each fusion step the conflict value of the mass distribution over Ω using Smet's rule and compare it with the sum of the two masses in $\{C\}$ and $\{P\}$. The cyber-physical alarm triggering equation is given by:

$$\begin{cases} \max\{m_{\mathrm{PCR-6}}(\gamma_a)\}\, \forall \gamma_a \in \Omega, & \text{if } m_{\mathrm{Smets}}(\{\emptyset\}) \leq \rho \\ m_{\mathrm{PCR-6}}(\{C\}) + m_{\mathrm{PCR-6}}(\{P\}) \geq m_{\mathrm{Smets}}(\{\emptyset\}), & \text{if } m_{\mathrm{Smets}}(\{\emptyset\}) \geq \rho \end{cases} \tag{11}$$

where $\rho = 0.7$ is a pre-defined threshold for an admissible conflict value. Typically, the decision-making rule in evidence theory is set with the highest BPA value after combining the information from all the sources.

In the smart grid case study, Equation (11) is not always valid throughout the simulation: during the cyber-physical anomaly, the decision rule yields different sets for the same events (i.e., initially $\{C\}$ and then $\{P\}$).

As shown in Figure 3, the results are quite interesting. During the simulation, $m(\{C\})$ and $m(\{P\})$ converge to the same value even if they belong to two exclusive sets as the classical evidence theory assumes.

Using Equation (11), it is possible to transmit to the control center the current state of the system, underlying the occurrence of the cyber-physical attack. Upon analyzing the results, it is possible to confirm that an intersection exists among the sets in the frame of discernment.

Smarandache and Dezert [11] have proposed an extended version of evidence theory. The extended theory eliminates the constraint on the exclusivity of hypotheses and explicitly considers intersections among the elements of the power set. Although the theory appears to be useful in our case study,

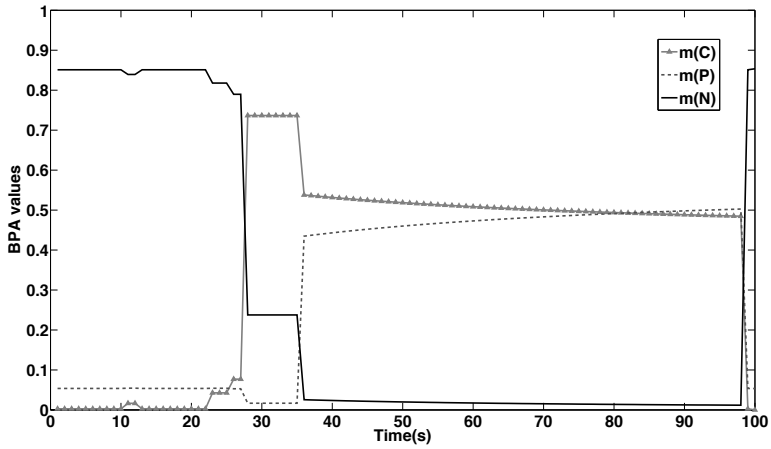


Figure 3. Results using the PCR-6 rule for singletons.

the main problem is the intersection operator. In fact, after defining the frame of discernment Ω, it is necessary to define a special power set called the hyper power set D^{Ω}. The cardinality of D^{Ω} due to the intersection operator follows the Dedekind number sequence: 1, 2, 5, 19, 167, 7580, 7828353, 56130437228687557907787... [11, 13]. Note that only cases up to $n < 7$ are tractable with current computing technology. This paper resolves the problem by using a hybrid knowledge model based on classical evidence theory and Dezert-Smarandache theory, which is described in the following section.

4. Exploring the Frame of Discernment

The computational overhead when using the Dezert-Smarandache theory is extremely high. To address this problem, the initial frame of discernment is modified by considering a hybrid knowledge model between classical evidence theory and Dezert-Smarandache theory. In particular, the intersection of $\{C\}$ and $\{P\}$ is explicitly evaluated as in the case of Dezert-Smarandache theory, but in the context of classical evidence theory.

The new frame of discernment, which is shown in Figure 4, is given by:

$$\Omega' = \{C', P', N, C \cap P\} \tag{12}$$

where $\{C'\} \in \Omega'$ is equal to $\{C\} \setminus \{P\}$ in the initial frame of discernment Ω, and $\{P'\} \in \Omega'$ is $\{P\} \setminus \{C\} \in \Omega$. The intersection $\{C \cap P\}$ is added to the frame of discernment because most of the conflict is between the sets $\{C\}$ and $\{P\}$.

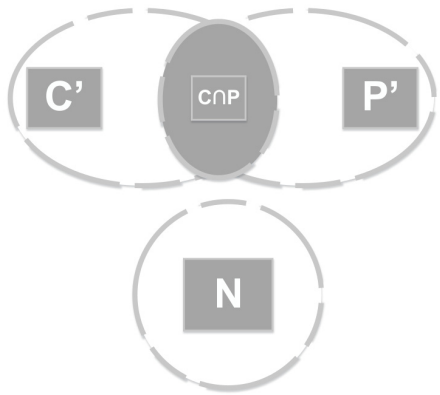


Figure 4. Representation of the new frame of discernment.

The new power set is given by:

$$\begin{aligned}\Gamma(\Omega') = \{&\emptyset, C', P', N, C \cap P, C' \cup P',\\ &C' \cup N, C' \cup (C \cap P), P' \cup N, P' \cup (C \cap P),\\ &N \cup (C \cap P), C' \cup P' \cup N, C' \cup P' \cup (C \cap P),\\ &C' \cup N \cup (C \cap P), P' \cup N \cup (C \cap P), \Omega'\}\end{aligned} \tag{13}$$

In the new approach, when the intersection $C \cap P$ is embedded as another hypothesis in Ω', the cardinality of $\Gamma(\Omega')$ is 16. In contrast, using the Dezert-Smarandache approach and the Dedekind sequence, the cardinality of $|\Gamma(\Omega')|$ is 19. Of course, it is possible to apply the new approach for a number of elements $n \geq 4$ to obtain a hybrid power set with cardinality $< D^{\Omega}$.

Table 2. BPA assignment for cyber sensor with the new frame ($a = 5$, $p = 2$).

	Percentage	**Number of Packets**
$\mathbf{m}(C')$	55% m(α)	$0.55 \cdot e^{-(a \cdot p)/x}$
$\mathbf{m}(C \cap P)$	45% m(α)	$0.45 \cdot e^{-(a \cdot p)/x}$
$\mathbf{m}(N)$	55% (1 – m(α))	$0.55 \cdot (1 - e^{-(a \cdot p)/x})$
$\mathbf{m}(P' \cup N \cup (C \cap P))$	31.5% (1 – m(α))	$0.315 \cdot (1 - e^{-(a \cdot p)/x})$
$\mathbf{m}(\Omega')$	13.5% (1 – m(α))	$0.135 \cdot (1 - e^{-(a \cdot p)/x})$

Considering the results obtained in the case study above and the results obtained using the approach presented in [8], we selected the function defined in Equation (10) for the BPA assignment. The BPA values for the cyber sensor and physical sensor are summarized in Tables 2 and 3, respectively. Note that the only difference is related to the BPA assignment of the focal sets:

Table 3. BPA assignment for physical sensor with the new frame ($a = 5$, $p = 2$).

	Percentage	**Fault**	**No Fault**
$\mathbf{m}(P')$	55% m(β)	$0.55 \cdot e^{-(a \cdot p)/t}$	0.055
$\mathbf{m}(C \cap P)$	45%i m(β)	$0.45 \cdot e^{-(a \cdot p)/t}$	0.045
$\mathbf{m}(N)$	55% (1 – m(β))	$0.55 \cdot (1 - e^{-(a \cdot p)/t})$	0.495
$\mathbf{m}(C' \cup N \cup (C \cap P))$	31.5% (1 – m(β))	$0.315 \cdot (1 - e^{-(a \cdot p)/t})$	0.2835
$\mathbf{m}(\Omega')$	13.5% (1 – m(β))	$0.135 \cdot (1 - e^{-(a \cdot p)/t})$	0.1215

- $m(N)$ has the same value because its intersection with the new set is empty and $\{N\} \cap \{C \cap P\} = \emptyset$.
- $m(C)$ is divided into the sets $\{C'\}$ and $\{C \cap P\}$ belonging to Ω', as reported in Table 2.
- $m(P)$ is divided between $m(\{P'\})$ and to $m(\{C \cap P\})$ of Ω', as reported in Table 3.
- $m(\{P \cup N\})$ is now assigned to $m(\{P' \cup N \cup (C \cap P)\})$ and $m(\{C' \cup N\})$ to $m(\{C' \cup N \cup (C \cap P)\})$, as reported in Tables 2 and 3.

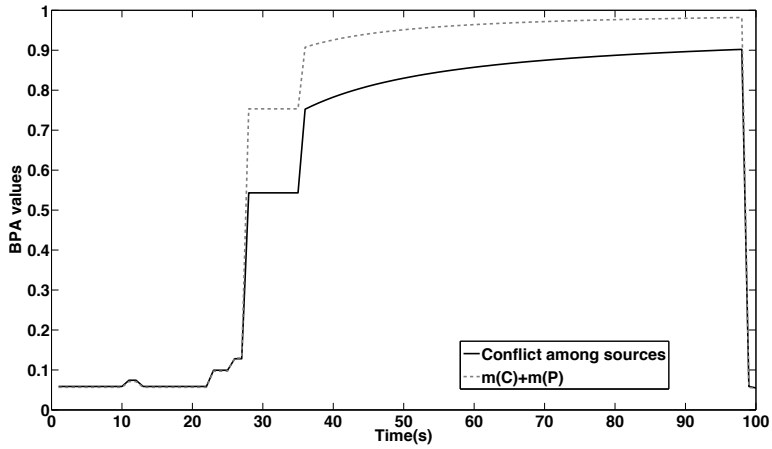
As discussed above, the BPA assignment is still an open question in the context of evidence theory. Indeed, there is no consensus on how to assign the BPA values. Thus, the BPA functions are selected based on the application. Note that the values reported in Tables 2 and 3 were obtained after exhaustive tests on the system.

5. Hybrid Power Set: Simulations and Results

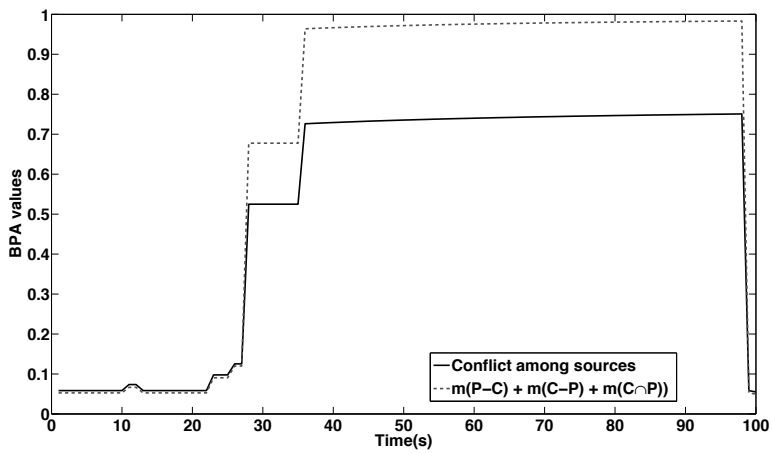
The hybrid power set was tested by fusing the information using the Dempster and PCR-6 rules. Figures 5(a) and 5(b) show comparisons of the evaluations of the conflict between the information sources. Note that the conflict value in Ω' is smaller than Ω and is reduced by approximately 11% during the simulation compared with the original case.

When Dempster's rule is used, the values are low and demonstrate contradictory behavior. Note that the set $P - C$ is set P' in Ω' and $C - P$ is C' in Ω'. As shown in Figure 6, during the cyber-physical anomaly, the values of $m(C)$ and $m(P)$ are approximately the same ($\simeq 0.05$). Note that $m(C \cap P)$ has a higher value ($\simeq 0.2$), but this is not relevant because the conflict value is high.

Figure 7 shows the values of the singletons after fusion using the PCR-6 rule. Note that the set $P - C$ is set P' in Ω' and $C - P$ is C' in Ω'. In this case, the dashed line (i.e., $m(C \cap P)$) is greater than the others during the cyber-physical anomaly. Upon examining Figure 6, it is seen that the values of $m(C \cap P)$ are comparable with $m(C)$ or $m(P)$ using Ω instead of Ω' as the frame of discernment. Therefore, with the hybrid power set, it is possible to manage the intersection between hypotheses to obtain good results.



(a) Conflict and sum of $m(C)$ and $m(P)$ in Ω.



(b) Conflict and sum of $m(P - C)$, $m(C - P)$ and the intersection $m(C \cap P)$ in Ω'.

Figure 5. BPA trends in the power set Ω and hybrid power set Ω'.

Using the new frame of discernment and the PCR-6 rule, an operator is able to recognize, with the help of the fusion algorithm, a cyber-physical anomaly represented by $C \cap P$. With the hybrid frame of discernment, the results can be analyzed using a classical metric (see Equation (11)). Note that throughout the simulation there is one element of the power set with the highest value. As such, an operator does not need any other metrics to trigger a particular event (i.e., cyber-physical anomaly).

For the other elements of the power set $\Gamma(\Omega')$, the sets represented in Figure 8 are the only ones with non-zero masses. The values $m(C' \cup N \cup (C \cap P))$ (triangle-marked line) and $m(P' \cup N \cup (C \cap P))$ (dotted line) are the same.

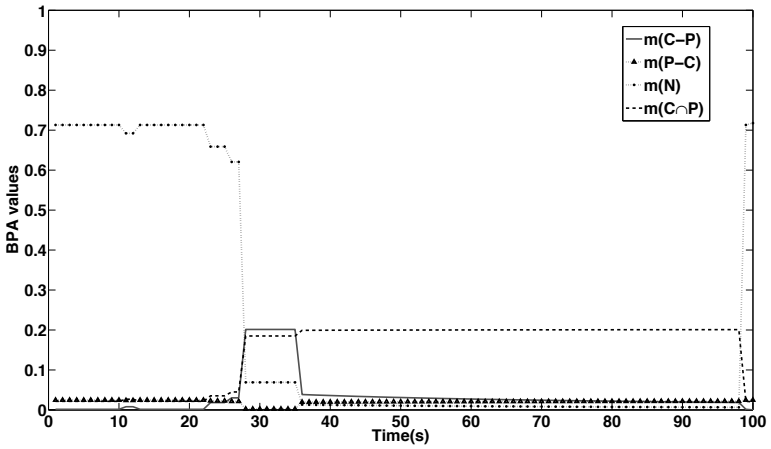


Figure 6. Results using Dempster's rule for the new frame of discernment Ω'.

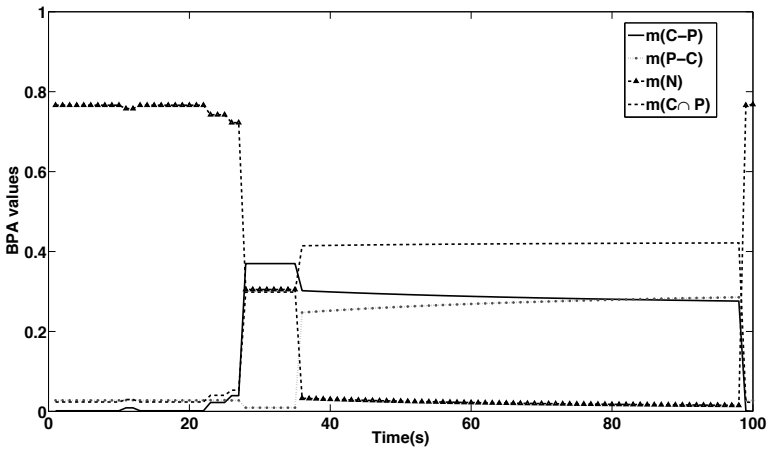


Figure 7. Results using the PCR-6 rule for the frame of discernment Ω'.

Table 4. Computational times for the power sets $\Gamma(\Omega)$ and $\Gamma(\Omega')$.

	Mean Time	**Variance**
$\Gamma(\Omega)$	4.1290 sec	0.1604
$\Gamma(\Omega')$	20.6636 sec	0.0373

Table 4 shows the computational times of the fusion script for the two frames of discernment Ω and Ω'. The script, which was written in Matlab [6], was tested on a laptop with a 2.6 GHz quad-core Intel Core i7 processor and 8 GB

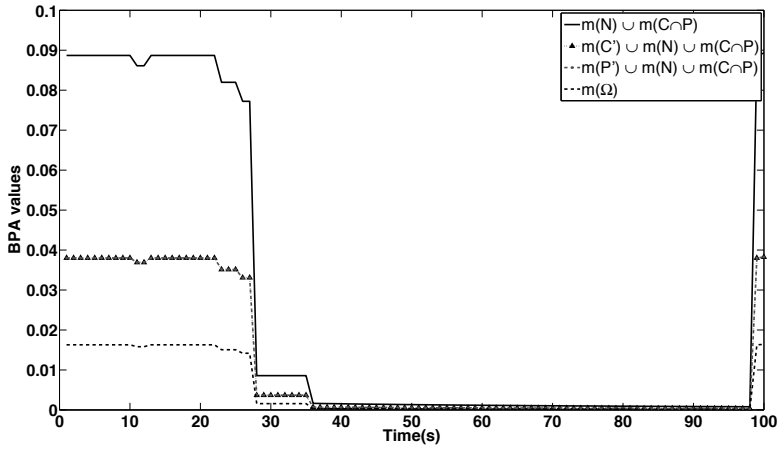


Figure 8. Results using the PCR-6 rule for the remaining meaningful elements of Ω'.

RAM. The script was executed 100 times. Table 4 reports the means and the variances. The frame of discernment with fewer elements (i.e., Ω) requires less time on the average than Ω', but the time required has greater variance. Note that the performance would improve if a non-interpreted programming language such as Java or C++ were to be used. Nevertheless, the results are encouraging with regard to the application of evidence theory in real-time environments.

6. Conclusions

The application of evidence theory to diagnose faults in a cyber-physical system is an important topic in critical infrastructure protection. In certain situations, such as when cyber and physical faults are both present, the classical Dempster-Shafer evidence theory is somewhat restrictive. Therefore, it is necessary to redefine the frame of discernment to better represent the knowledge model due to non-empty intersections between hypotheses. The Dezert-Smarandache model explicitly considers the intersection, but it has a high computational overhead due to the cardinality of the hyper power set. The solution, as presented in this paper, is to use a hybrid knowledge model where the intersection is included in the frame of discernment. The results obtained are encouraging. The conflict value is lower and the situation is described by the singleton set $\{C \cap P\}$ as having the highest value among the elements of the hybrid power set during a cyber-physical anomaly.

Our research is currently focusing on generalizing evidence theory using different BPA values. An issue requiring further research is defining BPAs for different cyber attacks that seek to inflict physical damage. Another problem is to manage conflicts and understand the source of inconsistent results. Addi-

tionally, it is necessary to study of theoretical properties of the hybrid power set.

Acknowledgement

This research was partially supported by the 7th Framework Programme of the European Union STREP Project under Grant Agreement 285647 (COCKPITCI – Cybersecurity of SCADA: Risk Prediction, Analysis and Reaction Tools for Critical Infrastructures (`www.cockpitci.eu`).

References

[1] O. Basir and X. Yuan, Engine fault diagnosis based on multi-sensor information fusion using Dempster-Shafer evidence theory, *Information Fusion*, vol. 8(4), pp. 379–386, 2007.

[2] M. Burmester, E. Magkos and V. Chrissikopoulos, Modeling security in cyber-physical systems, *International Journal of Critical Infrastructure Protection*, vol. 5(3-4), pp. 118–126, 2012.

[3] A. Cardenas, S. Amin and S. Sastry, Secure control: Towards survivable cyber-physical systems, *Proceedings of the Twenty-Eighth International Conference on Distributed Computing Systems Workshops*, pp. 495–500, 2008.

[4] A. Dempster, Upper and lower probabilities induced by a multivalued mapping, in *Classic Works of the Dempster-Shafer Theory of Belief Functions*, R. Yager and L. Liu (Eds.), Springer, Berlin-Heidelberg, Germany, pp. 57–72, 2008.

[5] C. Krishna and I. Koren, Adaptive fault-tolerance for cyber-physical systems, *Proceedings of the International Conference on Computing, Networking and Communications*, pp. 310–314, 2013.

[6] MathWorks, MATLAB version 8.0.0, Natick, Massachusetts (`www.mathworks.com/products/matlab`), 2014.

[7] R. Poovendran, Cyber-physical systems: Close encounters between two parallel worlds, *Proceedings of the IEEE*, vol. 98(8), pp. 1363–1366, 2010.

[8] R. Santini, C. Foglietta and S. Panzieri, Evidence theory for smart grid diagnostics, *Proceedings of the Fourth IEEE/PES Conference on Innovative Smart Grid Technologies Europe*, 2013.

[9] G. Shafer, *A Mathematical Theory of Evidence*, Princeton University Press, Princeton, New Jersey, 1976.

[10] C. Siaterlis and B. Genge, Theory of evidence-based automated decision making in cyber-physical systems, *Proceedings of the IEEE International Conference on Smart Measurements for Future Grids*, pp. 107–112, 2011.

[11] F. Smarandache and J. Dezert (Eds.), *Advances and Applications of DSmT for Information Fusion (Collected Works)*, American Research Press, Rehoboth, New Mexico, 2004.

[12] P. Smets and R. Kennes, The transferable belief model, *Artificial Intelligence*, vol. 66(2), pp. 191–234, 1994.

[13] D. Wiedemann, A computation of the eighth Dedekin number, *Order*, vol. 8(1), pp. 5–6, 1991.