18th International Conference on Information Fusion
Washington, DC - July 6-9, 2015

A Graph-Based Evidence Theory for Assessing Risk

Riccardo Santini
Engineering Department
University of "Roma TRE"
Via della Vasca Navale 79,
00146 Rome Italy
Email: riccardo.santini@uniroma3.it

Chiara Foglietta
Engineering Department
University of "Roma TRE"
Via della Vasca Navale 79,
00146 Rome Italy
Email: chiara.foglietta@uniroma3.it

Stefano Panzieri
Engineering Department
University of "Roma TRE"
Via della Vasca Navale 79,
00146 Rome Italy
Email: stefano.panzieri@uniroma3.it

Abstract—**The increasing exploitation of the internet leads to new uncertainties, due to interdependencies and links between cyber and physical layers. As an example, the integration between telecommunication and physical processes, that happens when the power grid is managed and controlled, yields to epistemic uncertainty. Managing this uncertainty is possible using specific frameworks, usually coming from fuzzy theory such as Evidence Theory. This approach is attractive due to its flexibility in managing uncertainty by means of simple rule-based systems with data coming from heterogeneous sources. In this paper, Evidence Theory is applied in order to evaluate risk. Therefore, the authors propose a frame of discernment with a specific property among the elements based on a graph representation. This relationship leads to a smaller power set (called Reduced Power Set) that can be used as the classical power set, when the most common combination rules, such as Dempster or Smets, are applied. The paper demonstrates how the use of the Reduced Power Set yields to more efficient algorithms for combining evidences and to application of Evidence Theory for assessing risk.**

I. Introduction

The interconnection between physical equipment and telecommunication networks is growing thanks to the large scale development of internet economy and covering all sectors of our society. Several examples can be found in everyday life: critical infrastructures and their control centres are linked by means of a telecommunication network that could be proprietary or, eventually, general purpose (i.e., Internet). Power grids are an ideal case study for analyses related to both physical and cyber aspects.

Risk is traditionally tied to the loss of productivity, the financial impact or the time spent to restore the system, in order to provide a pre-defined quality of services towards customers. In power grids and in critical infrastructures, the risk is also related to the consequences of an adverse event, such as catastrophic event, system failure or malicious attacks.

In this paper, risk assessment of interconnected systems is re-discovered as an application field for Evidence Theory. Evidence Theory is a mathematical formalism born in the context of Data Fusion, in order to merge data and information coming from several and heterogeneous sensors. Evidence Theory has been already applied in electric grid for diagnostic problems. In [1], an architecture on how to apply Evidence Theory in Smart Grids has been proposed with the aim to identify the real causes of faults. In [2] and [3], the approach has been studied during the so-called "Cyber-Physical threats", i.e. cyber threats aiming to disrupt the proper operations of physical equipment.

In this work, the authors want to apply the same methodology for assessing risk from different and heterogeneous causes. In the general circumstances, Evidence Theory is used to deal with epistemic uncertainty due to a lack of knowledge of quantities, system process or environment. Usually epistemic uncertainty [4] is not considered apart from the aleatory one and, therefore, uniform probability distribution is used to represent both. The main drawback is the possibility to underestimate uncertainty in system responses, see [5].

The classical probability approach is not enough when someone needs to merge heterogeneous information as physical and cyber data, because epistemic uncertainty arises. Hence, different mathematical frameworks can be used, such as Fuzzy Sets, Possibility Theory or Evidence Theory. In [6] and [7], the definition of epistemic and aleatory uncertainty within the context of risk analysis is discussed.

The straightforward application of Evidence Theory to risk assessment is not possible due to the existence of some elements of the power set that do not have meaning as results. So the authors find a graph representation of the frame of discernment able to generate a smaller power set (called Reduced Power Set) that is minimum with respect to the case study, i.e. analysis of risk.

Using the Reduced Power Set has the same accuracy of the power set if the constraint on the frame of discernment is respected. This property will be demonstrated asserting that the Reduced Power Set is closed under the intersection operator, and therefore it can be applied with each combination rule based on the intersection operator, such as Dempster's, Smets or PCR-6 rule. Some experimental results are also explained in order to understand the benefit of a smaller power set in terms of computational time.

Contributions: In this paper, the authors apply the Evidence Theory in the risk assessment process. The contribution of this paper is two-fold:

1) The authors provide a graph-theoretic framework for Evidence Theory. This framework encompasses the definition of a proper frame of discernment and of a Reduced Power Set for risk assessment applications;

978-0-9964527-1-7©2015 ISIF

2) The computational load of Evidence Theory is reduced, without loss of accuracy during the fusion process.

Organization: The paper is structured as follows: related work are presented in Section II; the classical framework of Evidence Theory is introduced in Section III; in Section IV the definition of the Reduced Power Set and its properties are presented; then Section V describes the case study with some results; finally, some conclusions are in Section VI.

II. Related Works

Traditional methods based on probability, such as Bayesian nets, have numerous lacks due to deficiency of data and subjectivity of experts. To overcome those issues, Evidence Theory (or Dempster-Shafer framework) can be applied to evaluate risk.

In [8], the authors used the Dempster-Shafer framework for evaluating risk due to network security. They proposed a long process based on an improved Dempster's rule of combination in order to combine the masses of network security risk factors. Finally, the belief value of network security risk is obtained. The security properties of the network are divided into communication and operation, access control and asset.

Usually, Evidence Theory is applied in risk assessment tied with other methodologies. The work of Miao and Liu, [9], presents a risk assessment model combining grey relational analysis and Dempster-Shafer theory. The grey relational grades for each risk rating were used to determine the basic probability assignment functions in Dempster-Shafer theory.

A new combination rule is proposed by Liu, Chen, Gao and Jiang in [10]. This combination rule is called Risk Integrated Basic Strength Assignment and is generated from the Dempster one in order to allow experts to evaluate risk event completely on their own professional experiences and knowledge independently.

When only weak information is available, Demotier, Schon and Denœux presented a framework based on Evidence Theory for risk assessment [11]. An approach to handle such problems is proposed, based on the belief functions of Dempster-Shafer. Belief functions are used to describe expert knowledge of treatment process efficiency, failure rates, and latency times, as well as statistical data regarding input water quality. Evidential reasoning provides mechanisms to combine this information and assess the plausibility of various non-compliance scenarios. The work of Demotier, Schon and Denœux exploits the knowledge on the water treatment plant in order to define mass functions, in a situation where epistemic uncertainty is obvious.

Yi and Xie, [12], assess the vulnerability analysis of natural hazard in a given geographic area. Dempster-Shafer theory is used as the mathematical foundation of the vulnerability analysis. Based on the frame of discernment of vulnerability variables and criteria of human perception, the mass functions of evidence theory are designed.

Applying the Dempster-Shafer framework to risk assessment has led to analyse how Basic Probability Assignment must be defined starting from the input of experts, or how to change combination rules in order to get meaningful results.

In this paper, the main structure of the Evidence Theory is still valid. The novelty is to combine the Dempster-Shafer framework with graph theory, with a view to define a proper power set in order to avoid all the cases where the power set elements are in a clear contradiction, such as sets where both low and high risk values are considered.

In the next section some details on the mathematical formalism for Evidence Theory are proposed.

III. Evidence Theory

Evidence Theory appears for the first time thanks to Shafer [13], who reinvented Dempster's previous work [14] and represents an interesting alternative to the Bayesian framework. The main difference concerns the way in which the ignorance is handled: the uncertainty, in the probabilistic framework, is treated by splitting the amount of credibility among plausible events, while in the Evidence Theory framework a belief is assigned to the set describing all the plausible hypotheses.

In [15], the Transferable Belief Model is presented. In this case, the proposed approach to Evidence Theory is axiomatic and based on the definition of the mass function, as basic probability assignment (BPA). It introduces the idea of open world assumption in the Dempster-Shafer framework. Two are the main limitations of Evidence Theory: the computational complexity, which grows exponentially with respect the number of hypotheses, see Section III-A, and the unacceptable behaviour of the Dempster's rule of combination, which causes the development of other rules, see Section III-B.

A. Representing the Knowledge Model

Evidence Theory embraces the familiar idea of using a number between zero and one to indicate the degree of confidence for a particular proposition, on the basis of the available evidence.

Definition 1 (Frame of Discernment):
Let $\Omega = \{\omega_1, \cdots, \omega_n\}$ be a finite set of possible values of a variable ω, where the elements ω_i are assumed to be mutually exclusive and exhaustive. The set Ω, so defined, is referred to as frame of discernment and ω_i is hypothesis or a proposition.

Definition 2 (Power Set): Let $\Gamma(\Omega)$ be the power set originated by the frame of discernment Ω. The Power Set is defined as $\Gamma = \{\gamma_1 \cdots \gamma_{|\Gamma|}\}$, and contains every subset $\gamma_i \subseteq \Omega$. The cardinality of the Power Set is $2^{|\Omega|}$.

Definition 3 (Basic Probability Assignment - BPA): A Basic Probability Assignment is represented by a function $m : \Gamma(\Omega) = 2^{\Omega} \rightarrow [0, 1]$. Hence, the symbol m, defines a mapping from the power set $\Gamma(\Omega)$ to the interval between 0 and 1. Two constraints are mandatory:

$$m(\emptyset) = 0 \tag{1}$$

$$\sum_{\gamma_a \in \Gamma(\Omega)} m(\gamma_a) = 1 \tag{2}$$

In this framework, the focus is on quantifying the belief of propositions of the form: *the truth value ω is contained in γ_a*. The value of the BPA for the set γ_a, represented by $m(\gamma_a)$, expresses the quantity of evidence that supports the claim that the true value belongs to the set γ_a, but to no particular subset of γ_a.

Considering a BPA assignment, the elements of the Power Set with values greater than zero are called *focal sets*.

B. Combination Rules

Several rules have been proposed during the years, with different features and different application fields.

Dempster's was the first to be proposed in [14]. This rule of combination is purely a conjunctive operation and it strongly emphasizes the agreement between multiple sources and ignores all the conflicting evidence through a normalization factor. This has the effect to attribute null mass to the empty set. So the rule is formalized as, $\forall \gamma_a \in \Gamma(\Omega)$:

$$\text{Dempster}\{m_i, m_j\}(\gamma_a) = \frac{\displaystyle\sum_{\gamma_b \cap \gamma_c = \gamma_a} m_i(\gamma_b) m_j(\gamma_c)}{1 - \displaystyle\sum_{\gamma_b \cap \gamma_c = \emptyset} m_i(\gamma_b) m_j(\gamma_c)} \tag{3}$$

Smets in [15] proposed his own rule of combination that allows to express explicitly the contradiction in the Dempster-Shafer framework by letting $m(\emptyset) \geq 0$. This combination rule, compared to Dempster's, simply avoids the normalization while preserving the commutativity and associativity properties. The formalization is as follows, $\forall \gamma_a \in \Gamma(\Omega)$:

$$\text{Smets}\{m_i, m_j\}(\gamma_a) = \sum_{\gamma_b \cap \gamma_c = \gamma_a} m_i(\gamma_b) m_j(\gamma_c) \tag{4}$$

In this paper, a non-Bayesian rule for fusing the information is also considered. This rule, denoted *PCR-6*, is the Proportional Conflict Redistribution (PCR) rule no. 6 which has been proposed in [16] for combining BPAs.

In this case, the rule is for two sources of information and it is evaluating as $\text{PCR}_6(\emptyset) = 0$. For $\forall \gamma_a \in \Gamma(\Omega) \setminus \emptyset$ is the following one:

$$\begin{aligned} &\text{PCR}_6\{m_i, m_j\}(\gamma_a) = \text{Smets}\{m_i, m_j\}(\gamma_a) + \qquad (5) \\ &\sum_{\substack{\gamma_b \in \Gamma(\Omega) \setminus \gamma_a, \\ \gamma_a \cap \gamma_b = \emptyset}} \left[\frac{m_i^2(\gamma_a) m_j(\gamma_b)}{m_i(\gamma_a) + m_j(\gamma_b)} + \frac{m_j^2(\gamma_a) m_i(\gamma_b)}{m_j(\gamma_a) + m_i(\gamma_b)} \right] \end{aligned}$$

This rule, in case of high-conflict sources, redistributes the conflict in a different way with respect to the other rules reported in literature: only the focal sets that generate the conflict are involved in the redistribution of this value and the obtained solutions, after the combination process, are better in terms of quality-conflict ratio, see [16]. Risk assessment is a perfect case study for high-conflict sources.

In TABLE I, the principal combination rules are listed with their use of two operators: $\cup$ and $\cap$. Usually, the combination rules, Eq. 3, Eq. 4 and Eq. 5, exploit the intersection among sets for their results. For further analysis on the properties and the mathematical expression of the rules reported in TABLE I, see also [17].

TABLE I. OPERATORS $\cup$ AND $\cap$ IN THE PRINCIPAL RULES OF COMBINATION

	Dempster	Smets	PCR	Yager	Dubois & Prade	Conj	Disj
$\cup$					x		x
$\cap$	x	x	x	x	x	x	

IV. ANALYSIS ON FRAME OF DISCERNMENT: THE REDUCED POWER SET

Usually, risk is represented by scalar numbers or percentages or, in case of quantitative analysis, as a rank number in an interval. Making use of Evidence Theory, in this work, the authors define a particular frame of discernment:

$$\Omega = \{A, B, C, D, E\} \tag{6}$$

The values in (Eq. 6) constitute a risk scale from low (A) to high (E), represented as a discrete set of five elements. Starting from Ω, as the Evidence Theory assumes, the definition of the power set $\Gamma(\Omega)$ is the following one:

$$\begin{aligned} \Gamma(\Omega) \quad = \{&\emptyset, A, B, A \cup B, C, A \cup C, B \cup C, A \cup B \cup C, \\ &D, A \cup D, B \cup D, A \cup B \cup D, C \cup D, A \cup C \cup D, \\ &B \cup C \cup D, A \cup B \cup C \cup D, E, A \cup E, B \cup E, \\ &A \cup B \cup E, C \cup E, A \cup C \cup E, B \cup C \cup E, \\ &A \cup B \cup C \cup E, D \cup E, A \cup D \cup E, B \cup D \cup E, \\ &A \cup B \cup D \cup E, C \cup D \cup E, A \cup C \cup D \cup E, \\ &B \cup C \cup D \cup E, A \cup B \cup C \cup D \cup E\} \end{aligned} \tag{7}$$

The cardinality of $\Gamma(\Omega)$ is equal to $2^{|\Omega|} = 2^5 = 32$ and it is made of all possible subsets of Ω. Among the subsets of the power set, some elements must be considered for the Evidence Theory (i.e., during the fusion process), but have no meaning in risk assessment. For example, the set $\{A \cup E\}$ means that the risk is contained in A or in E, but it is not possible to distinguish between one of the elements of the subset.

To overcome this issue, the authors in this work use a different representation of frame of discernment and Power Set, using graph theory.

In risk assessment, Ω can be represented as an undirected graph $\mathcal{G} = (V, E)$, where $V = \{\omega_1, \ldots, \omega_n\}$ is the set of

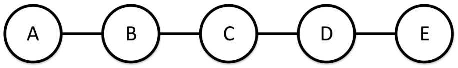

Fig. 1. A graph representation of the considered frame of discernment.

vertices (representing singletons of Ω) and $E = \{e_{ij} = (\omega_i, \omega_{i+1}), i = 1, \dots, n-1\}$ is the set of edges connecting vertices, as depicted in Fig. 1. Therefore, the only reasonable subsets of the power set are the ones where the elements respect the following definition.

Definition 4 (Induced Sub-graph): Each element of the power set $\gamma_i \in \Gamma(\Omega)$ defines a sub-graph $\mathcal{G}'$ of $\mathcal{G}$ induced by $V' = \gamma_i$. The induced sub-graph $\mathcal{G}' = (V', E')$ contains all the edges of $\mathcal{G}$ that connect elements of the given subset of the vertex set V' of $\mathcal{G}$, and only those edges. Formally,

$$V' = \gamma_i \subseteq V \tag{8}$$

$$\forall \omega_j, \omega_k \in V', e = (\omega_j, \omega_k) \in E \qquad \Rightarrow \qquad e \in E' \tag{9}$$

The induced sub-graph $\mathcal{G}'$ is connected **iff** for each pair of vertices $(\omega_j, \omega_z) \in \mathcal{G}'$ either

- $\omega_j = \omega_z$
- $\omega_j \neq \omega_z$, and a path between them on $\mathcal{G}'$ must exist

Let us provide a brief example, in which the previous definition (Definition 4) is applied. Let $\gamma_i = \{B \cup C \cup D\}$ as a candidate of the focal set. The induced sub-graph $\mathcal{G}' = (V', E')$ is made of $V' = \{B, C, D\}$ and $E' = \{(B, C), (C, D)\}$. For each couple of elements we need to find a path among them over $\mathcal{G}'$:

- The path between B and C is direct due to the existence of the edge (B, C);
- The edge (C, D) justifies the existence of a path between C and D;
- The path between B and D is a walk through the vertex C.

So $\{B \cup C \cup D\}$ can be considered as a feasible set, because the induced sub-graph is connected.

Let $\gamma_i = \{A \cup B \cup D \cup E\}$ as a candidate of the focal set. In this case the induced sub-graph $\mathcal{G}' = (V', E')$, where

- $V' = \{A, B, D, E\}$
- $E' = \{(A, B), (D, E)\}$, because those edges are the only ones between the vertices V' in $\mathcal{G}$

This induced sub-graph $\mathcal{G}'$ is not connected because between the vertices B and D there is no path in $\mathcal{G}'$. Therefore, the set $\{A \cup B \cup D \cup E\}$ is not a feasible set for the Reduced Power Set.

Following Definition 4, the Reduced Power Set consists of all subsets whose induced sub-graph satisfies connectivity condition. Throughout the paper, we will refer to the Reduced Power Set as $\Gamma'(\Omega)$.

Referring to the previous considerations and remembering that the empty-set must be a part of $\Gamma'(\Omega)$, the Reduced Power Set from $\mathcal{G}$ in Fig. 1 is:

$$\begin{aligned} \Gamma'(\Omega) = \qquad & \{\emptyset, A, B, A \cup B, C, B \cup C, \\ & A \cup B \cup C, D, C \cup D, \\ & B \cup C \cup D, A \cup B \cup C \cup D, \\ & E, D \cup E, C \cup D \cup E \\ & B \cup C \cup D \cup E, A \cup B \cup C \cup D \cup E\} \end{aligned} \tag{10}$$

Definition 5 (Cardinality of the Reduced Power Set): The cardinality of $\Gamma'(\Omega)$ is

$$|\Gamma'(\Omega)| = \left(\sum_{i=1}^{n} i \right) + 1 \tag{11}$$

where n is the number of elements in Ω. Therefore, the Reduced Power Set has always less elements than the classical Power Set $\Gamma(\Omega)$. In the proposed example, $|\Gamma'(\Omega)| = 16 < |\Gamma(\Omega)| = 32$.

In order to use the Reduced Power Set in the Evidence Theory framework, it is mandatory to demonstrate that the result of the combination rules is still a mapping function that gives not-zeros values to the elements of the Reduced Power Set, i.e., $m : \Gamma'(\Omega) \to [0, 1]$. Most of the combination rules, (see TABLE I), exploit the intersection operator to obtain the result of the mapping function m.

In the following, a property of the Reduced Power Set $\Gamma'(\Omega)$ is introduced in order to apply it within the framework.

Proposition 1: $\Gamma'(\Omega)$ is closed under the intersection operator.

Proof: In order to prove the proposition, it is necessary to define the intersection operator $\cap$ on a graph. In this case study, the result of the intersection between two elements of the power set $\gamma_i \cap \gamma_j = \gamma_z$ is an induced sub-graph $\mathcal{G}'_z = (V'_z, E'_z)$. Notice that this set belongs to $\Gamma'(\Omega)$. Therefore the corresponding induced sub-graph must be connected. Using the same notation, the induced sub-graph for γ_i is denoted as $\mathcal{G}'_i$ and for γ_j is used $\mathcal{G}'_j$.

The induced sub-graph $\mathcal{G}'_z$ considers the vertices that are common to two subsets, so $V'_z = V'_i \cap V'_j$ and the same is for the edges $E'_z = E'_i \cap E'_j$.

Let us prove it by contradiction. We assume that if the induced sub-graph $\mathcal{G}'_z$ is not connected, when both $\mathcal{G}'_i$ and $\mathcal{G}'_j$ are connected induced sub-graphs, a logical contradiction occurs hence $\mathcal{G}'_z$ is connected.

TABLE II. RESULTS OF THE EXAMPLE USING DIFFERENT COMBINATION RULES, SUCH AS DEMPSTER, SMETS AND PCR-6 RULES

	m_1	m_2	$Dempster$	$Smets$	PCR_6
$\emptyset$	0.0	0.0	0.0	0.31	0.0
A	0.1	0.0	0.06	0.02	0.029
B	0.1	0.0	0.09	0.06	0.087
C	0.1	0.1	0.21	0.18	0.2609
D	0.0	0.1	0.09	0.06	0.087
E	0.0	0.1	0.06	0.02	0.029
AB	0.1	0.0	0.05	0.02	0.029
AC	0.0	0.0	0.0	0.0	0.0
AD	0.0	0.0	0.0	0.0	0.0
AE	0.0	0.0	0.0	0.0	0.0
BC	0.1	0.0	0.085	0.07	0.1014
BD	0.0	0.0	0.0	0.0	0.0
BE	0.0	0.0	0.0	0.0	0.0
CD	0.0	0.1	0.085	0.07	0.1014
CE	0.0	0.0	0.0	0.0	0.0
DE	0.0	0.1	0.05	0.02	0.029
ABC	0.1	0.1	0.055	0.04	0.058
ABD	0.0	0.0	0.0	0.0	0.0
ABE	0.0	0.0	0.0	0.0	0.0
ACD	0.0	0.0	0.0	0.0	0.0
ACE	0.0	0.0	0.0	0.0	0.0
ADE	0.0	0.0	0.0	0.0	0.0
BCD	0.1	0.1	0.07	0.06	0.087
BCE	0.0	0.0	0.0	0.0	0.0
BDE	0.0	0.0	0.0	0.0	0.0
CDE	0.1	0.0	0.055	0.04	0.058
$ABCD$	0.1	0.1	0.015	0.01	0.0145
$ABCE$	0.0	0.0	0.0	0.0	0.0
$ABDE$	0.0	0.0	0.0	0.0	0.0
$ACDE$	0.0	0.0	0.0	0.0	0.0
$BCDE$	0.0	0.1	0.015	0.01	0.0145
Ω	0.1	0.1	0.01	0.01	0.0145

If the induced sub-graph $\mathcal{G}'_z$ is not connected, it is still the results of the intersection operator, as defined before, and so:

$$V'_z \subseteq V'_i, \qquad \text{and} \qquad V'_z \subseteq V'_j \tag{12}$$

$$E'_z \subseteq E'_i, \qquad \text{and} \qquad E'_z \subseteq E'_j \tag{13}$$

The induced sub-graphs $\mathcal{G}'_i$ and $\mathcal{G}'_j$ are connected and so they must also contain a subset of $\mathcal{G}'$, in Fig. 1, not included in $\mathcal{G}'_z$. This specific sub-graph is denoted $\mathcal{G}'_c$ and considering the graph $\mathcal{G}$, $\mathcal{G}'_c$ is unique. Therefore, this sub-graph $\mathcal{G}'_c$ is included in $\mathcal{G}'_i$ and in $\mathcal{G}'_j$ because they must be connected for definition, but in this way, also $\mathcal{G}'_c \subseteq \mathcal{G}'_z$. Hence, $\mathcal{G}'_z$ is connected. ■

This proposition shows that, applying an intersection-based combination rule, the result is still a subset of the Reduced Power Set.

In the following, an example is reported in order to show that, choosing as focal sets of $\Gamma(\Omega)$ only elements that respect Definition 4 and applying combination rules that exploit the intersection operator, the fusion results are contained in the Reduced Power Set $\Gamma'(\Omega)$, see TABLE II. As BPA values (m_1 and m_2), a random function assigns values between 0 and 1 to the focal sets. As combination rules, the authors choose Dempster's (Eq. 3), Smets' (Eq. 4) and PCR-6 (Eq. 5) rules. Without loss of accuracy, in risk assessment the power set $\Gamma(\Omega)$ can be substitute with the Reduced Power Set $\Gamma'(\Omega)$ reducing the computational time.

In the next Section, the results of the combination using the PCR-6 rule will be shown.

V. POWER GRID AS AN APPLICATION FOR RISK ASSESSMENT

Evidence Theory could be applied in order to assess risk, merging data and information coming from heterogeneous sources, such as physical data or cyber information.

With a view to provide an appealing case study, a real infrastructure is considered: a Medium Voltage power grid controlled by a Supervisory Control And Data Acquisition (SCADA) system, connected to a general-purpose telecommunication network [18].

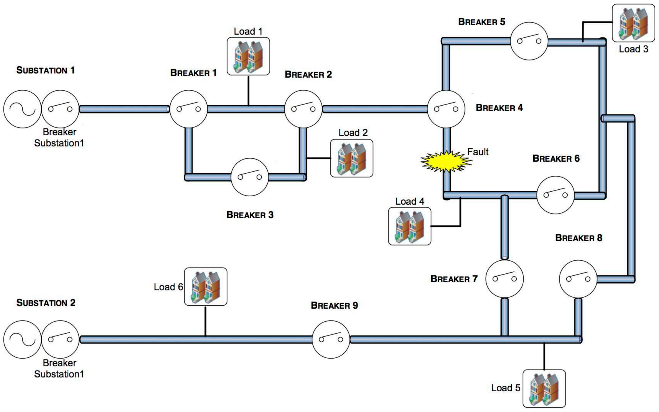

Fig. 2. An example of Medium Voltage (MV) power grid

The power grid is composed of two main lines, fed by the two substations in Fig. 2. Different current branches (with physical redundancy) provide power to the loads connected to the grid. In normal conditions, the two main lines are usually disconnected thanks to breaker no. 7 and breaker no. 8 that are normally open. To maintain a radial topology, breaker no. 3 and breaker no. 5 are also open.

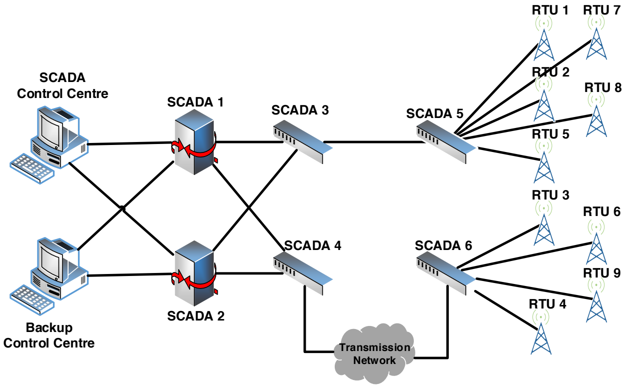

Fig. 3. The SCADA telecommunication network

The SCADA system in Fig. 3 is able to monitor the actual state of the power grid and eventually reconfigure the topology by the adoption of the Fault Isolation and System Restoration (FISR) procedure, also called power load shedding. In general if a permanent fault happens, the operator restores the power in the grid by opening and closing the breakers. Such procedure is grid-dependent, because different power grids have different FISR procedures, derived by the topology. A complete description of FISR algorithms is outside the scope of this paper, see [19] for further explanations.

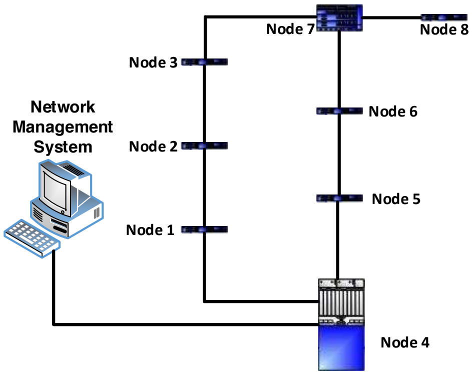

Fig. 4. A general-purpose telecommunication network

In Fig. 4, the general-purpose telecommunication network is needed to transmit information from the SCADA control center towards the power grid breakers. This network has mainly a ring topology: in the event of a link failure, packets are sent back to the source node in order to change the routing protocol. In Fig. 4, node n. 8 and node n. 4 are the links between this network and the SCADA layer.

In the following the information flow among SCADA control center, the power grid and the telecommunication network is described:

- Every circuit breaker is telecontrolled from the SCADA system by means of Remote Terminal Unit (RTU) and/or Programmable Logical Controller (PLC) that use compatible TCP/IP protocol;
- RTUs and PLCs send and receive SCADA packets (containing opening and closing commands) through telecommunication network.

In the event of mechanical fault or cyber attack, it is important to evaluate the risk on the overall system. As already done in [1] and [2], this kind of scenario has been used to individuate the cause of cyber-physical faults, fusing information coming from specific domain sensors (tied to Cyber and Physical layers), when an attacker wants to compromise the regular operations within the power grid through telecommunication vulnerabilities. In this paper, a step further is explained: it is possible not only to find the most plausible cause of faults, but also to estimate a comprehensive risk belonging to the two layers, cyber and physical, of the power grid.

The Quality of Service toward electrical customers is highly dependent on the operability of the power grids and the interconnected infrastructures: in the case study, they are the SCADA network and the telecommunication network. The risk towards customers of the power grid is influenced by the three infrastructures, and their information must be fused for assessing the overall risk.

Two subsequent situations are evaluated in the following:

1) A Man-In-The-Middle (MITM) attack, where a malicious attacker enters into the telecommunication network in order to capture information flows between RTUs and control center;
2) An infection attack, where the malicious intruder wants to modify the behaviour of a specific set of RTUs. In this case the risk of blackouts is greater than in the previous situation, due to active changes in the power grids.

As already done by Gao *et al.* in [8] for risk evaluation in network security, we merged several sources and risk factors in order to find the overall risk index. The sources of information from the three infrastructures are:

- A physical sensor on the substation of the power grid, able to transmit information related to the actual current;
- An Intrusion Detection System (IDS) in the telecommunication network, able to recognize a malicious attacker on the general-purpose network;
- An IDS on the SCADA network. A SCADA system is different from the conventional IT system: it is a hard real-time system; its terminal devices have limited computing and memory capabilities; and the logic execution occurred within SCADA has a direct impact on the physical world dictates safety as the paramount. Hence, a SCADA-specific IDS is needed to detect attackers.

In this context it is essential to define a suitable knowledge model so that different experts (cyber or physical) or sensors can support risk of distinct realms.

Simulations over the real system were carried out with CISIApro, an agent-based simulator for Critical Infrastructures [20]. An Evidence Theory module was added to the simulator with the aim to apply and test the framework introduced in Section IV.

The choice of the BPA assignment is an open question without a unique answer. This assignment is strongly tied to the case study and to the ability of the researcher of properly assigning BPA values. After exhaustive tests over the system, also taking in consideration the behaviours of the MITM and Infection attacks, a proper mass function was assigned to CISIApro simulator. As previously mentioned, the main goal of this paper is the identification of which elements of the power set are meaningful in risk assessment, hence all the questions about how and why a mass function is better than another one are outside the scope of this work.

In the following two examples are proposed with different conflicting values among sources.

The authors consider as Frame of Discernment Ω a risk scale from low (A) to high (E) and $\Gamma'(\Omega)$ as power set. The

PCR-6 rule (Eq. 5) is used to combine sources with the aim of obtaining good solutions in terms of quality-conflict ratio, as explained in Section III. For sake of brevity, the authors omit the results obtained with other combination rules.

A. *First Situation - Man In The Middle Attack*

For Evidence Theory each data coming from the sensors is an independent source of information and must be translated into a BPA assignment (i.e. $m_i, i = 1, 2, 3$).

In TABLE III, BPA values are summarized. In the first column, the focal sets are listed: AB means the element of the power set usually indicated as $\{A \cup B\}$, and so on. The physical sensor m_1 of the power grid detects a lower risk; the SCADA-specific IDS m_2 assigns must of the BPA to B set; and the IT IDS has confidence that the risk of a MITM attack is middle, i.e. $m_3(C) = 0.6$.

TABLE III. EXAMPLE OF BPA ASSIGNMENTS FOR THE FIRST EXAMPLE.

	A	B	C	AB	DE	CDE	$BCDE$	Ω
m_1	0.6	0.0	0.0	0.0	0.0	0.0	0.2	0.2
m_2	0.1	0.6	0.0	0.0	0.0	0.1	0.0	0.2
m_3	0.0	0.0	0.6	0.1	0.1	0.0	0.0	0.2

A value assigned to the subset $\Omega = \{A \cup B \cup C \cup D \cup E\}$ represents the total ignorance of the source and so the inability to discern among the single elements of this set.

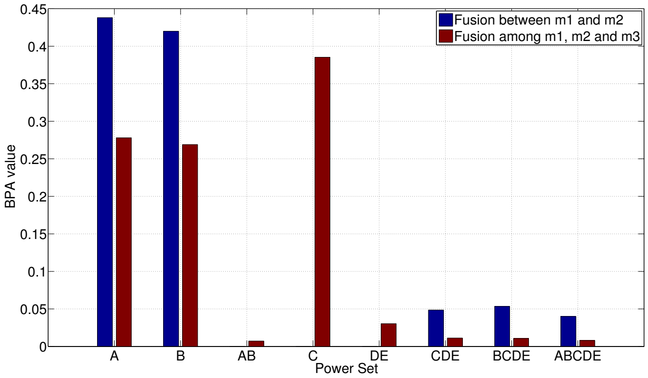

Fig. 5. Results using PCR-6 rule for combining three information sources

In Fig. 5, only the not-zero sets of $\Gamma'(\Omega)$, after the PCR-6 fusion, are displayed. The blue bars represent the fusion of m_1 and m_2 (getting m_{12}); the red ones, instead, are the results obtained combining m_{12} and m_3.

As demonstrated in Section V, no evidences are assigned to the elements of $\Gamma(\Omega) \setminus \Gamma'(\Omega)$: the combination results and the initial focal sets are contained within $\Gamma'(\Omega)$. The overall risk is medium, because the value of the C is the greatest one.

A relevant observation must be done: even if the conflict value raises, due to different sources belonging to heterogeneous domains, the total lack of knowledge denoted as $\{A, B, C, D, E\} = \Omega$ decreases and a common value of risk is reached ($\{C\}$ that means a medium value).

B. *Second Situation - Infection Attack*

In this case, a different situation is considered: an infection is spreading from the telecommunication network towards the power grid in order to cause malfunctioning in the physical layer. In TABLE IV, the BPA values are listed:

- m_1 Represents the assignment from the physical sensor in the power grid. A medium risk value is allocate through the sets;
- m_2 Contains the values of the SCADA-specific IDS. A high risk value is assigned to $m(D)$;
- m_3 Corresponds to the telecommunication IDS assignment, after the detection of the infection attack.

TABLE IV. EXAMPLE OF BPA ASSIGNMENTS FOR SECOND SITUATION.

	C	D	E	AB	DE	ABC	$ABCD$	Ω
m_1	0.6	0.0	0.0	0.1	0.1	0.0	0.2	0.2
m_2	0.0	0.6	0.1	0.0	0.0	0.3	0.0	0.0
m_3	0.0	0.1	0.6	0.0	0.0	0.0	0.2	0.1

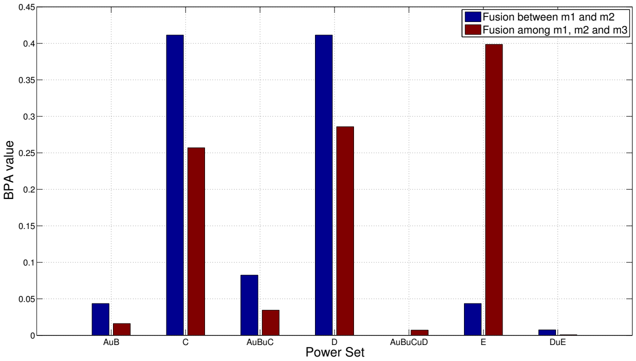

Fig. 6. Results using PCR-6 rule for combining four information sources

The output of the combination rule, using PCR-6, is depicted in Fig. 6. The result demonstrates how, if an infection attack is happened, the risk of possible electrical blackout is very high ($m(E) = 0.4$).

To perform computational time analysis between the classical Evidence Theory framework and the proposed framework, the data obtained from CISIApro simulator [20] were evaluated with Matlab [21]. A simulation script shown, after 1,000,000 trials, that the mean time for fusion process using PCR-6 rule over $\Gamma(\Omega)$ is 2.52 seconds, instead of 1.47 seconds for $\Gamma'(\Omega)$. In this case, the improvement is not remarkable but it increases with the cardinality of the frame of discernment as asserted in Definition 5. For example, if the cardinality of the frame of discernment is $n = 10$, the power set contains $2^n = 1024$ instead the Reduced Power Set has only 56, reducing the computational time of around 20 times.

So, as introduced in Section IV, the Reduced Power Set is better than $\Gamma(\Omega)$ in terms of computational time.

A final remark on the fusion process used in this paper must be made: as explained before, the BPAs were fused in a sequential way and, because the PCR-6 rule is non associative, the sequential fusion process is known to be sub-optimal [16]. To get optimal results the BPAs must be combined all together using a generalized PCR-6 rule. Although, this remark does not affect the obtained results because the rule is still based on the intersection operator and so our case study demonstrates the effectiveness of the proposed framework.

VI. Conclusion

This paper presents an innovative framework for managing and evaluating risk in complex systems. For those systems, the tight interconnection between cyber and physical layers leads to an integrate analysis of risk, considering information and data coming from both fields.

Evidence Theory is a general framework used to manage uncertainty related to knowledge models and to expert opinions. This methodology is able to fuse information coming from heterogeneous source into a common knowledge model, but it is too general to be perfectly applied in the field of risk assessment.

In this paper, the concept of connected sub-graph induced from the frame of discernment is introduced obtaining the Reduced Power Set: a subset of the classical power set with the only elements that are meaningful for evaluating risk.

This Reduced Power Set has another important feature: the combination of focal sets respecting the connected sub-graph definition, leads to another BPA function that respects the same property of m over $\Gamma(\Omega)$. Obviously, this is valid for each combination rule based on the intersection operator, such as Dempster's, Smets' and PCR-6 rules.

The notion of Reduced Power Set drastically decreases the high computational load of Evidence Theory, that was until now one of its major drawback. The obtained results encourage the authors to generalize the presented approach to heterogeneous case studies.

Acknowledgment

The research paper is partially supported by the DG Home Affairs under Prevention Preparedness and Consequence Management of Terrorism and other Security related Risks CIPS Grant Action 2013 (HOME/ 2013/CIPS/AG 2013)(URANIUM - Unified Risk Assessment Negotiation via Interoperability Using Multi-sensor data, ***uranium.theorematica.it****).*

References

[1] C. Siaterlis and B. Genge, “Theory of evidence-based automated decision making in cyber-physical systems,” in *Smart Measurements for Future Grids (SMFG), 2011 IEEE International Conference on*, Nov 2011, pp. 107–112.

[2] R. Santini, C. Foglietta, and S. Panzieri, “Evidence theory for smart grid diagnostics,” in *Innovative Smart Grid Technologies Europe (ISGT EUROPE), 2013 4th IEEE/PES*, Oct 2013, pp. 1–5.

[3] ——, “Evidence theory for cyber-physical systems,” in *IFIP Advances in Information and Communication Technology*, vol. 441, 2014, pp. 95–109.

[4] A. D. Kiureghian and O. Ditlevsen, “Aleatory or epistemic? does it matter?” *Structural Safety*, vol. 31, no. 2, pp. 105 – 112, 2009. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167473008000556

[5] J. Helton, J. Johnson, and W. Oberkampf, “An exploration of alternative approaches to the representation of uncertainty in model predictions,” *Reliability Engineering & System Safety*, vol. 85, no. 13, pp. 39 – 71, 2004. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0951832004000511

[6] G. W. Parry, “The characterization of uncertainty in probabilistic risk assessments of complex systems,” *Reliability Engineering & System Safety*, vol. 54, no. 23, pp. 119 – 126, 1996, treatment of Aleatory and Epistemic Uncertainty. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0951832096000695

[7] T. Nilsen and T. Aven, “Models and model uncertainty in the context of risk analysis,” *Reliability Engineering & System Safety*, vol. 79, no. 3, pp. 309 – 317, 2003. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0951832002002399

[8] H. Gao, J. Zhu, and C. Li, “The analysis of uncertainty of network security risk assessment using dempster-shafer theory,” in *Computer Supported Cooperative Work in Design, 2008. CSCWD 2008. 12th International Conference on*, 2008, pp. 754–759.

[9] W. Miao and Y. Liu, “Information system security risk assessment based on grey relational analysis and dempster-shafer theory,” in *Mechatronic Science, Electric Engineering and Computer (MEC), 2011 International Conference on*, 2011, pp. 853–856.

[10] Y.-Q. Liu, Y.-W. Chen, F. Gao, and G.-P. Jiang, “Risk evaluation using evidence reasoning theory,” in *Machine Learning and Cybernetics, 2005. Proceedings of 2005 International Conference on*, vol. 5, 2005, pp. 2855–2860 Vol. 5.

[11] S. Demotier, W. Schon, and T. Denœux, “Risk assessment based on weak information using belief functions: a case study in water treatment,” *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 36, no. 3, pp. 382–396, 2006.

[12] S. Yi and Y. Xie, “Vulnerability analysis of disaster risk based on geographic information and dempster-shafer theory,” in *Geoinformatics, 2010 18th International Conference on*, 2010, pp. 1–6.

[13] G. Shafer, *A mathematical theory of evidence*. Princeton university press Princeton, 1976, vol. 1.

[14] A. P. Dempster, “Upper and lower probabilities induced by a multivalued mapping,” *The annals of mathematical statistics*, vol. 38, no. 2, pp. 325–339, 1967.

[15] P. Smets and R. Kennes, “The transferable belief model,” *Artificial intelligence*, vol. 66, no. 2, pp. 191–234, 1994.

[16] F. Smarandache and J. Dezert, *Advances and Applications of DSmT for Information Fusion: Collected Works*, ser. Advances and Applications of DSmT for Information Fusion: Collected Works. American Research Press, 2006 - 2009, no. vol. 2 & 3. [Online]. Available: http://fs.gallup.unm.edu/DSmT.htm

[17] ——, *Advances and Applications of DSmT for Information Fusion: Collected Works*, ser. Advances and Applications of DSmT for Information Fusion: Collected Works. American Research Press, 2004, no. vol. 1. [Online]. Available: http://fs.gallup.unm.edu/DSmT.htm

[18] E. Ciancamerla, C. Foglietta, D. Lefevre, M. Minichino, L. Lev, and Y. Shneck, “Discrete event simulation of qos of a scada system interconnecting a power grid and a telco network,” in *What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience*, ser. IFIP Advances in Information and Communication Technology, J. Berleur, M. Hercheui, and L. Hilty, Eds. Springer Berlin Heidelberg, 2010, vol. 328, pp. 350–362. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-15479-9-33

[19] D. Ehrenreich, “Automatic fault isolation and system restoration in mv networks,” Motorola Inc., Tech. Rep.

[20] “Cisiapro agent-based critical insfrastructure simulator,” http://cisiapro.dia.uniroma3.it/.

[21] MATLAB Release 2013a, The MathWorks, Inc., Natick, Massachusetts, United States.