Aware online interdependency modelling via evidence theory

Giusj Digioia and Chiara Foglietta*

University of 'Roma Tre',
Via della Vasca Navale 79, 00146 Rome, Italy
E-mail: digioia@dia.uniroma3.it
E-mail: fogliett@dia.uniroma3.it

Gabriele Oliva

University Campus BioMedico,
via Alvaro del Portillo 21 00128 Rome, Italy
E-mail: g.oliva@unicampus.it

Stefano Panzieri*

University of 'Roma Tre',
Via della Vasca Navale 79, 00146 Rome, Italy
E-mail: panzieri@uniroma3.it
*Corresponding authors

Abstract: Critical infrastructure interdependency models are typically used in a simulation-based perspective, in order to perform 'what if?' analyses and identify structural vulnerabilities in a dynamic perspective. While in the literature some attempts have been made to use interdependency models at real time, such approaches are flawed by the inability to properly determine the ongoing situation. Such models, typically, receive data from SCADA systems, which are mostly able to assess the effects of failures rather than the causes, while knowing the typology of failure would increase dramatically the predictive-ability of online interdependency models. In this paper, a situation awareness framework is provided with the aim to complement online interdependency models by providing more specific information on the causes of the outages highlighted by sensor data. In order to determine such causes, in this paper a transferable belief model representation is adopted to increase the awareness of interdependency models on fault causes. Moreover in this paper some of the limitations of evidence theory methods are highlighted and discussed, with particular reference to a real time context, providing some insights on how to overcome them, especially the closed-world assumption.

Keywords: critical infrastructures; interdependency modelling; evidence theory; situation awareness; countermeasures.

Reference to this paper should be made as follows: Digioia, G., Foglietta, C., Oliva, G. and Panzieri, S. (2013) 'Aware online interdependency modelling via evidence theory', *Int. J. Critical Infrastructures*, Vol. 9, Nos. 1/2, pp.74–92.

Biographical notes: Biographical notes: Giusj Digioia received her Master in Computer Science and Automation in 2009 and is currently enrolled in a PhD course on Computer Science and Automation, both at University Roma Tre of Rome, Italy. Her research interests include critical infrastructures, situation awareness and evidence theory, and data fusion.

Chiara Foglietta received her Master in Computer Science and Automation in 2009 and is currently enrolled in a PhD course on Computer Science and Automation, both at University Roma Tre of Rome, Italy. Her research interests include critical infrastructures, situation awareness and evidence theory, and smart grids. She is currently involved in several european projects on critical infrastructure protection and smart grids.

Gabriele Oliva received his Master in Computer Science and Automation in 2008 and his PhD in Computer Science and Automation in 2012, both from University Roma Tre of Rome, Italy. His research interests include fuzzy systems, distributed systems and synchronization, critical infrastructures and in general complex systems. He is a member of the European Society for Fuzzy Logic and Technology, the Italian Association of Critical Infrastructures' Experts (www.infrastrutturecritiche.it/aiic) and IEEE Control Systems Society and Robotics and Automation Society. He is involved in several national and European projects on critical infrastructures interdependency modelling and networked control.

Stefano Panzieri received his Laurea in Electronic Engineering in 1989 and his PhD in Systems Engineering in 1994, both from the University of Roma 'La Sapienza'. Since February 1996, he has been with the 'Dipartimento di Informatica e Automazione' (DIA) of the University of 'Roma Tre', where he is currently an Associate Professor. His research interests are in the field of industrial control systems, robotics and sensor fusion. In the field of critical infrastructures protection, he has contributed to the development of a simulation model, the CISIA project. He is also interested in the security-related problems of industrial controllers (SCADA), and more recently, in the application of complex networks theory.

This paper is a revised and expanded version of a paper entitled 'Countermeasures selection via evidence theory' presented at 6th International Conference on Critical Information Infrastructures Security (CRITIS '11), Lucerne, Switzerland, 8–9 September 2011.

1 Introduction

Industrial control systems and critical infrastructures' control centres are able to collect a large amount of data and to elaborate such an information in order to provide the operators with a synoptic view of the ongoing situation. The operator, on the base of such information, is able to understand the ongoing situation and undertake his decisions. Such a paradigm, although effective when infrastructures are relatively decoupled, is becoming less and less adequate derived from the increasing degree of dependency and interoperability among infrastructures. Interdependency arises for many

reasons and, in particular, because of geographical, physical, cyber, or logic relations (Rinaldi, 2004).

Cyber interdependency, in particular, is becoming more and more pervasive, due to the increasingly use of internet-based technologies and public networks to operate critical infrastructures. However, while the internet has been beneficial to both public and private organisations, the increasing reliance on networked systems has augmented the risk of cyber attacks.

Supervisory control and data acquisition (SCADA) systems, first introduced in the 80s and 90s, are still in use. These systems, including those installed until few years ago, did not consider properly the security issues due to the usage of public networks. Such systems were conceived with a monolithic structure, isolated from the outside world and based on proprietary standards for the communication between control centre and field devices.

Over time, due to the rapid growth of the internet and telecommunications networks, SCADA systems have changed, slowly tending to a distributed architecture, with standardised and well documented communication protocols, such as TCP/IP and Modbus. These SCADA systems are usually connected to corporate network. In addition, such systems typically exchange data with no encryption or authentication algorithms.

However, in recent years, there is a growing urge to evaluate the performances of SCADA systems also from the point of view of security. This need arises due the great relevance of these systems for the welfare of citizens and nations. In 2010, the discovery of Stuxnet (Falliere et al., 2011) became a concrete proof that cyber attacks on industrial control systems and SCADA systems are possible. Stuxnet was able to infect Windows computers used to supervise industrial control systems, and to recognise and infect such control systems. In 2010 and in 2011, the amount of SCADA vulnerability disclosures and exploits has exploded. Rios and McCorkle (2011) found 100 SCADA bugs in 100 days, thanks to free software available online.

Impact evaluation of cyber attacks and their consequences are very difficult to perform. The complexity of the problem at hand is indeed non-trivial also due to interdependencies. In fact the domino and cascading effects are sometimes not easy to find, especially with due to the growing importance of telecommunications that may result in unwanted and unnoticed couplings.

For the above reasons, the impact assessment of faults should also encompass cyber attacks, which are becoming a realistic typology of attack for critical infrastructures. The introduction of firewalls, intrusion detection systems (IDS) and degrees of separation between the corporate network and the control system network is a good step toward increasing security, but there is still much to be done.

Another step that may result in an increase of the resilience of facilities is the information exchange among governments and infrastructure owners. The information can be shared using national and international agencies, such as computer emergency response teams (CERTs), or early warning and alerting networks, as European Information Sharing and Alert System (EISAC), US National Cybersecurity and Communications Integration Centre (NCCIC) or Australian Cyber Security Operations Centre (CSOC) (European Commission, 2011).

All the agencies listed above were created with the goal of cooperating with infrastructure operators in the event of a cyber attacks. Each infrastructure, upon suspicion of being under attack, warns its agency or CERT that has the duty to share

information with other agencies and infrastructures that may be involved. In addition, they provide mitigation mechanisms and countermeasures.

Due to the increase of interdependency among infrastructures, in the last years the scientific community has done a huge effort in defining interdependency models able to quantify and predict the dynamics of outages in critical infrastructures considering the loops, domino effects and exacerbation of failures that arise due to the high degree of interdependency (Rinaldi, 2004; Setola et al., 2009; Haimes and Jiang, 2001; Oliva et al., 2011a).

Critical infrastructure interdependency models are typically used in a simulation-based perspective (Haimes and Jiang, 2001; Oliva et al., 2011a), in order to perform 'what if?' analyses and identify structural vulnerabilities in a dynamic perspective. In the literature some tempts have been made to use interdependency models at real time (Gasparri et al., 2009; Oliva et al., 2011b, 2012; Oliva, 2012), in order to quantify interdependency and failures in the near future, based on the sensorial data acquired by the different infrastructures' control rooms. Indeed, such approaches are flawed by the inability to properly determine the ongoing situation.

In this paper a situation awareness (SAW) (Endsley, 1995; Gutwin and Greenberg, 2002) framework is provided with the aim to complement the online interdependency models by providing them more specific information on the causes connected to the outages highlighted by sensor data.

The idea is to set up a framework for the identification of the causes that originated the failures and use such an information in order to evaluate the near-future evolution of the scenario (i.e., the domino effects and the degree of failure of a given infrastructure or subsystem). In fact, while a huge effort has been done to model the effects of specific failures such as fire blasts, terrorist attacks or cyber attacks, when interdependency models are used in a real time prospective (Gasparri et al., 2009; Oliva et al., 2011b, 2012), the only available data is the state of infrastructure components or subsystems which is typically 'working' or 'not working' (eventually a percentage of malfunctioning), without providing insights on the causes. Indeed, as one may expect, if a telecommunication node in a the telecommunication network is down due to a fire blast, the diffusion of failure will have a very different pattern with respect to the spread of a computer virus (i.e., in the case of fire nearby elements will be affected while in the case of computer virus element with the same operating system will be affected). Hence, in order to use such frameworks at real time, the urge for a mechanism able to determine the cause is becoming mandatory.

The paper is organised as follows: in Section 2 the real-time framework is described in order to assess the ongoing situation; in Section 3 the theory of evidence is proposed with a special focus on transferable belief model (TBM); in Section 4 some peculiarities of TBM are reported to evaluate TBM ability in real time contexts, also in the case of incomplete and inaccurate knowledge models; finally, a numerical example is detailed in Section 5 and conclusions are explained in Section 6.

2 Towards an online augmented impact assessment

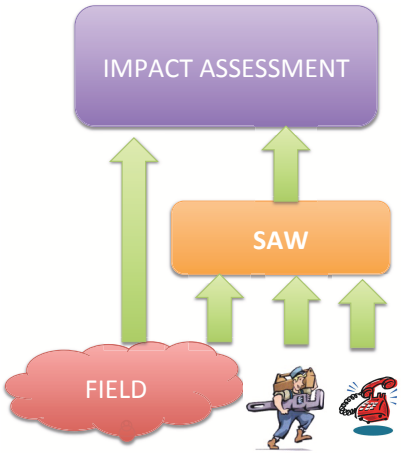
Due to the increasing diffusion of internet-based technology, the infrastructures, once separated and vertically integrated, are becoming more and more tightly interconnected and interdependent. There is then the need to provide a framework able to fuse

the domain specific data at real time, in order to provide predictions with a wider perspective. This has been done in a recent European FP7 Project (FP7 MICIE Project, 2010; Oliva et al., 2011b, 2012) by using data provided by the SCADA systems of the different infrastructures in order to provide a short-term prediction of the expected domino effects. However, although being potentially able to model several classes of failures such as earthquake or fire blast, each with its peculiar diffusion pattern and dynamics, relying on the SCADA system alone allows typically to notice only the effects of outages (e.g., a telecommunication node is down), without giving any insight on the causes.

Hence, a mandatory step is to provide insights on the causes of failure, in order to activate the corresponding dynamics in the interdependency model, which would not be 'excited' otherwise; in fact, as said before, the SCADA system only provides the state of an element (i.e., it is aware of the effects), while in order to perform more refined analyses there is the need to assess the causes, which would influence the interdependency model in a very different way.

To achieve such a result a SAW module should be interposed between the field and the interdependency model, see Figure 1. Such a SAW layer is fed with the fields data, as well as with other information coming from different sources, such as customer or maintenance/recovery teams reports (i.e., unnoticed malfunctioning or blackout) and government or civil protection information (e.g., a tsunami warning). Such a use of SAW leads to an augmented impact assessment in which domino effects can be exploited, with their respective confidence levels. This implies also that the impact assessment should be done with a tool able to manage uncertainty.

Figure 1 The proposed approach for integrating impact assessment via SAW (see online version for colours)



One of the most desirable features of such a SAW modules, given the high degree of cyber interdependency among critical infrastructures, would be the ability to identify cyber-related failures (Barfors et al., 2010; Rieger et al., 2009). For cyber awareness, we refer to the user perception of detecting faults, generated by intrusions and, in general, cyber attacks. In fact, awareness is a process that leads to increased knowledge of the system, of the causes that generated failures and of the quality of services

to customers. Hence, awareness helps to make decisions based on better knowledge of what is happening thanks to the integration of all available data. In the proposed architecture, the cyber awareness can be realised by means of intrusion detection and prevention systems, or by equipment, able to detect anomaly packet flows among SCADA telecommunication networks. These equipment send their outputs to SCADA control centre.

The impact assessment in Figure 1 is a block able to provide the impact evaluation on real equipment and services, after a fault or a failure. This module evaluates the cascading faults and domino effects of faults and failures on all interdependent infrastructures. This model has as inputs the data coming from the field and also outputs of the SAW module. These last data are uncertain, so it is important to consider input with uncertainty. A possible approach is fuzzy theory and especially fuzzy numbers. Among the others, critical infrastructure simulation by interdependent agents (CISIA) (De Porcellinis et al., 2008; Panzieri and Setola, 2008), is an agent-based simulator, using triangular fuzzy numbers, to represent involved quantities. Indeed, this approach can realise the impact assessment module inside this framework.

3 Evidence theory

In this section, the evidence theory framework is described. Such framework can be used for gaining insights on the ongoing situation, thus implementing a SAW schema able to infer the most likely cause of faults.

Evidence theory (Shafer, 1976; Dempster, 2008; Smets, 1990) is a mathematical formalism to handle uncertainty based on some evidences (e.g., sensors providing information). The idea is to evaluate the *belief* and the *plausibility* of a finite set of hypothesis (e.g., the causes that we want to assess).

Let a *frame of discernment* $\Omega = \{\omega_1, \cdots, \omega_n\}$ be a set of mutually exclusive hypotheses, and suppose that the hypotheses in Ω are exhaustive (e.g., we assume that the possible cause of failure for a telecommunication infrastructure are limited).

Consider a set of sensors, each able to raise alarms originated by several causes or hypotheses. The combination of several simultaneous alarms and thus the combination of different hypotheses leads to the definition of measures of belief and plausibility.

Let γ_a be a subset of Ω; evidence theory operates on the *power set* $\Gamma(\Omega)$ that is the set of all possible combination of hypotheses γ_a in Ω:

$$\Gamma(\Omega) = \{\gamma_1, \cdots, \gamma_{2^{|\Omega|}}\} \tag{1}$$

Note that the cardinality of the power set is $|\Gamma(\Omega)| = 2^{|\Omega|}$, since it contains all possible subsets of Ω, including the empty set $\gamma_1 = \emptyset$ and universal set $\gamma_{2^{|\Omega|}} = \Omega$.

Among the other possible approaches, the TBM (Smets, 1990) proved to be very effective. TBM is based on the definition of *basic belief mass* function: $m = \Gamma(\Omega) \rightarrow [0, 1]$. This function is a map that assigns to each element of the power set a value between 0 and 1. The function, also referred to as *basic belief assignment* (BBA), shall respect the following constraint:

$$\sum_{\gamma_a \subseteq \Gamma(\Omega)} m(\gamma_a) = 1 \quad \text{with} \quad m(\emptyset) = 0 \tag{2}$$

The set of elements γ_a in the power set having $m(\gamma_a) \neq 0$ is called the *focal set*.

In this framework, the interest is focused on quantifying the confidence of propositions of the form: 'the true value of ω_i is in γ_a', with $\gamma_a \in \Gamma$. For $\gamma_a \in \Gamma(\Omega)$, $m(\gamma_a)$ is the part of confidence that support exactly γ_a. This means that the true value is in the set γ_a but, due to lack of further information, does not support any strictly subset of γ_a. This is not a probability function, and it does not respect the property of additivity: $m(\gamma_a \cup \gamma_b) \neq m(\gamma_a) + m(\gamma_b)$.

Each BBA is an atomic element within the TBM. In fact, each sensor, agent or node must be able to assign the BBA values by some subjective assumptions, or through appropriate algorithms that automatically determine the assignment.

In the case of different independent information sources, a rule to aggregate the information must be provided.

There are many rules of combination in the literature. Among the others, the most widely used are the Dempster's rule and the Smets' one.

Dempster's (2008) *rule of combination* was the first to be formalised. The Dempster's rule of combination is purely a conjunctive operation. This rule strongly emphasises the agreement between multiple sources and ignores all the conflicting evidence through a normalisation factor, as shown in equation (4). This has the effect to attribute null mass to the empty set. So the rule is formalised as:

$$\text{Dempster}\{m_i, m_j\}(\emptyset) = 0 \tag{3}$$

$$\text{Dempster}\{m_i, m_j\}(\gamma_a) = \frac{\sum\limits_{\gamma_b \cap \gamma_c = \gamma_a} m_i(\gamma_b) m_j(\gamma_c)}{1 - \sum\limits_{\gamma_b \cap \gamma_c = \emptyset} m_i(\gamma_b) m_j(\gamma_c)} \qquad \forall \gamma_a \in \Gamma(\Omega) \tag{4}$$

Smets' (1990) *rule of combination* is another rule that allows to express explicitly the contradiction in the TBM, by letting $m(\emptyset) \neq 0$. This combination rule, compared to the Dempster's one, simply avoids the normalisation while preserving the commutativity and associativity properties. The formalisation is as follows:

$$\text{Smets}\{m_i, m_j\}(\gamma_a) = m_i(\gamma_a) \otimes m_j(\gamma_a) \qquad \forall \gamma_a \in \Gamma(\Omega) \tag{5}$$

where

$$m_i(\gamma_a) \otimes m_j(\gamma_a) = \sum_{\gamma_b \cap \gamma_c = \gamma_a} m_i(\gamma_b) m_j(\gamma_c) \qquad \forall \gamma_a \in \Gamma(\Omega) \tag{6}$$

The fact that $m(\emptyset) > 0$ can be explained in two ways: the open world assumption and the quantified conflict. The closed world assumption, made by Dempster, reflects the idea that the frame of discernment must contain the true value. Necessarily, if the closed world assumption is true, then the set of hypothesis must contains all possibilities. Under this interpretation, being $\emptyset$ the complement of Ω, the mass $m(\emptyset)$ represents the case where the truth is not contained in Ω, and, under the closed world assumption, the value of $m(\emptyset)$ must be zero. On the other hand, if the mass of the $\emptyset$ is not zero, then the meaning is that the true is not included in the considered hypotheses. The second interpretation of $m(\emptyset) > 0$ is that there is some underlying conflict between the sources

that are combined in order to produce the BBA. Hence, the mass assigned to $m(\emptyset)$ represents the degree of conflict. In particular, it can be computed as follows:

$$m_i(\emptyset) \otimes m_j(\emptyset) = 1 - \sum_{\gamma_a \in \Gamma, \gamma_a \neq \emptyset} (m_i(\gamma_a) \otimes m_j(\gamma_a)) \tag{7}$$

The main disadvantage of this approach is its computational complexity, due to compute the power set Ω, that is exponential respect the number of hypotheses. This limit usually discourage researchers to apply evidence theory to real applications. Some methods to reduce the computational complexity are explained in Shafer (1976).

This approach has been also proposed in a distributed framework and applied to critical infrastructure protection field (Foglietta et al., 2012).

4 Real time evidence theory: beyond the closed world assumption

In this section some of the main weaknesses of evidence theory, especially with regard to real-time implementation, are discussed; moreover a methodology aimed at increasing the applicability of such frameworks in an online context is presented.

Evidence theory, as discussed in previous section, heavily relies on the closed-world assumption, that is to say that is particularly ineffective if the set of hypotheses fails to adequately represent the reality of interest.

To overcome such a limitation there is the need to define adequate ways to refine the model of the reality under exam. In literature, model refinement is usually considered an off-line task, because of the necessary involvement of human decisions.

Conversely, it is very hard in general to provide automatic tuning mechanisms, and this is especially true for online frameworks.

In the case of evidence theory, when the model is well-defined and the evidences, detected by the sensors, are enough to discriminate situations, the result is a mass distribution that associates the greatest value to an atomic set (e.g., that the different sensors agree on a single cause).

Conversely, if the mass is mainly accumulated on a non-atomic set, then the evidences are not enough to discriminate the actual cause or the model has too much uncertainty and hence is not able to function properly. Indeed, if a knowledge model is not able to distinguish between situations, the domain knowledge has to be re-analysed.

Another issue is related to the assumption made in Dempster-Shafer framework: the closed world assumption. According to such an hypothesis, the considered situations have to be exhaustive and mutually exclusive.

Smets, with the TBM approach, overcomes this limit including the possibility that empty set may have a non-zero mass; in this way it is possible to determine to which extent the estimation is contradictory. The event of an empty-set with non-zero mass may happen when several combined sources are in conflict, or when the frame of discernment Ω does not contain all possible situations, thus highlighting modelling errors and that the truth is not in Ω.

Hence one of the following situations may lead to an empty set with non-zero mass:

- knowledge model is correct, but there are problems in evidence collecting process or the situation has evolved with time
- knowledge model is incorrect, due to situations not modelled or due to a misidentification of the different situations.

In first case, the problem might be the loss of some evidences due to the process of gathering information. The problem might also be an effect of several situations evolving during time. In a given time period $[t_1, t_2]$ evidences support a situation γ_i, then, when the situation evolves during $[t_2, t_3]$ the result is γ_j; as a result the mass of the empty-set is increased because of new evidences gathered and supporting γ_j, not exactly coherent with those supporting previous situation.

In this case, a solution is to transfer the mass of the empty-set in the universal set Ω, when the empty set mass has exceed a pre-defined threshold. In this way, the system is able to change idea and evaluate the new situation. This method can be applied in real-time context and can be easily implemented.

In the latter case, the problem can not be resolved by simply transferring the mass of the empty set in the universal set. In fact if the model is incorrect, the conflict value will continue to increase. In this case, other approaches are needed. In this paper, we assume that a new hypothesis can be included in the knowledge model.

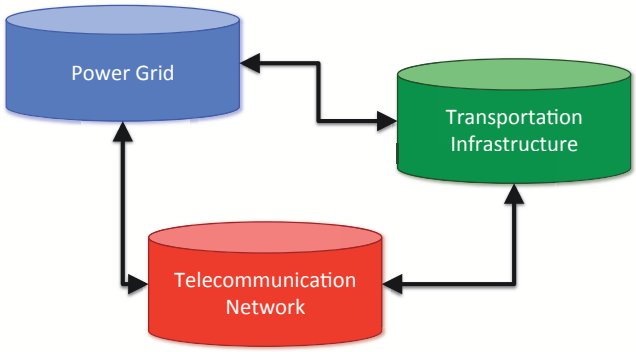
Consider that two sensors have generated alarms simultaneously, producing high contradiction that is not due to a possible change of situation, as even after mass re-distribution the empty set mass keeps on growing; thus highlighting the persistence of contradiction among evidences with regard to the model of situations evaluated. So a new hypothesis can be introduced in the knowledge model, linked to the two specific alarms. In the following numeric example, it has not been verified the possibility that the new hypothesis is mutually exclusive with respect to the other, namely that the new hypothesis is not a subset or partly overlap with those already considered in the knowledge model.

5 Numerical examples

In this section, using a simple case study in the field of critical infrastructure protection, the weaknesses of the evidence theory framework are shown and analysed.

In Figure 2, three infrastructures are depicted: telecommunication network, power grid and a transportation infrastructure as a railway one. The power grid is controlled by a control centre usually far away from the field and so telecommunication network is used to remotely control the power grid from the SCADA control centre. Railways are fed by electricity, especially the electric locomotives, and the railway exchanges are controlled thanks to the telecommunication infrastructures. The coal power plant can work using the coal delivered by the railways.

Figure 2 The case study represents three critical infrastructures: telecommunication network, power grid and transportation infrastructure (see online version for colours)



We assume that three possible anomalies can be detected using three different sensors:

1 (X1) alarms generated by the power SCADA control centre

2 (X2) telecommunication network alarm

3 (X3) power grid anomalies.

The set of evidences is $[X1, X2, X3]$. Evidence theory can help finding the most probable cause generating faults. The frame of discernment is composed of the following four hypotheses:

1 (H1) power grid failure

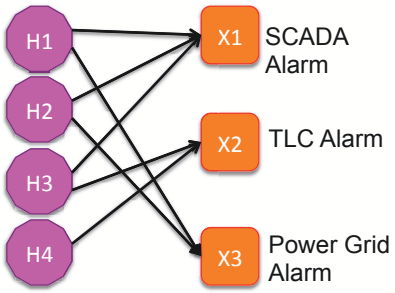
2 (H2) transportation infrastructure failure

3 (H3) cyber attack to telecommunication systems

4 (H4) telecommunication network failure.

For the case study, the frame of discernment is $\Omega = \{H1, H2, H3, H4\}$ and the power set is $2^{\Omega} = \Gamma$. The knowledge model in Figure 3, is represented as a bipartite graph $G = (H, X, E)$ where H and X are the four causes and the three alarms, and E the direct edges in the form $(h_i, x_j) \in E$ with $h_i \in H$ and $x_j \in X$.

Figure 3 The knowledge model for the case study (see online version for colours)



In order to apply the evidence theory framework, a criterion for the assignment of masses to the elements of Γ should be provided. This module is fed with spurious alarms received from the control centres, so the idea is to map each alarm with a subset of possible causes of faults. In SCADA systems, alarm handling is implemented with several reaction strategies. The system is able to monitor several alarm conditions: if the alarm condition is satisfied, an alarm event is occurred and some pre-defined actions are taken. Usually an alarm is depicted in operator interfaces, but also e-mail or messages are send to specific person or alarm indicators are activated.

For each spurious alarm j generated from the field and received by the control centre, we considered the supporting subset Ψ_j, as the sub-set containing all the causes which have an outgoing edge that goes into the j^{th} failure node. At this subset Ψ_j, it has been assigned a mass α equal to the reliability of the sensor generating the alarm; and $1-\alpha$ to the universal set $\{H1, H2, H3, H4\}$, as the set representing the maximum ignorance. In this paper, reliability values are pre-fixed values and never change during simulation. For reliability we means the probability that the alarm is a real alarm and not a false one.

The reliability value for each alarm is, respectively, α for X1, β as reliability value for sensor X2, and γ for sensor X3. The alarm X1 supports the subset $\{H1, H2, H3\}$; X2 alarm supports the subset $\{H3, H4\}$ and X3 supports $\{H1, H2\}$, as depicted in Figure 3.

In this way also a reduction of complexity is available, in fact each time evidence is gathered only a portion of the power set is taken into account as:

$$\Psi = \{\gamma_i \in \Gamma | (h_i, x_j) \in E \quad \text{with} \quad v_j > 0\} \tag{8}$$

where v is the vector containing the value of each sensor, if $v_k = 0$ the sensor has no output, otherwise the reliability value is contained.

5.1 First example: the right behaviour of the model

Suppose that a cyber attack is going to occur. It causes the generation alarms from the SCADA and the telecommunication network. Suppose that after some time, the telecommunication alarm goes down as anomalous traffic that is no further detected and later also the SCADA alarm turn into normality thanks to operator service. The alarm vector at different time steps is the following one:

$$T0 : v = [\alpha, \beta, 0]$$

$$T1 : v = [\alpha, \beta, 0]$$

$$T2 : v = [\alpha, 0, 0]$$

$$T3 : v = [\alpha, 0, 0]$$

where $alpha = 0.6$ and $\beta = 0.9$.

At each time step, evidence theory framework, implementing Smets rule for mass combination, is fed with the displayed alarms at the current time, and with the results of the last evaluation of the module itself. So at time $T1$, we combine the mass assignments of the time steps, due to $v = [\alpha, \beta, 0]$, and the result obtained at $T0$. Consequently, at time $T2$, we combine the mass due to alarm happened at time $T2$, $v = [\alpha, 0, 0]$, and the evaluations obtained at time $T1$.

Table 1 Mass assignment for the first example

	T0	*T1*	*T2*	*T3*
$\{\emptyset\}$	0	0	0	0
$\{H1\}$	0	0	0	0
$\{H2\}$	0	0	0	0
$\{H3\}$	0.54	0.8316	0.9266	0.9647
$\{H4\}$	0	0	0	0
$\{H1, H2\}$	0	0	0	0
$\{H1, H3\}$	0	0	0	0
$\{H1, H4\}$	0	0	0	0
$\{H2, H3\}$	0	0	0	0
$\{H2, H4\}$	0	0	0	0
$\{H3, H4\}$	0.36	0.1584	0.0634	0.0253
$\{H1, H2, H3\}$	0.06	0.0084	0.0094	0.0097
$\{H1, H2, H4\}$	0	0	0	0
$\{H1, H3, H4\}$	0	0	0	0
$\{H2, H3, H4\}$	0	0	0	0
$\{H1, H2, H3, H4\}$	0.04	0.0016	0.0006	0.0003

In Table 1, mass assignment for the power set is shown, at each step time. It is possible to notice that the set $\{H3\}$ is the one containing the higher value respect to the others. In fact, at time T2 and T3 the system increases the trust on $\{H3\}$ as new data are acquired, confirming the evaluation performed by the system at previous time steps. Thus, the belief of the true is in $\{H3\}$ increases, while the belief that it could be in other subsets decreases. the reader can notice that other subsets taken into account by the system at T1 include always $\{H3\}$.

5.2 Second example: the wrong behaviour of the model

In this example, consider at first a cyber attack, arising X1 and X2 alarms as in previous example, then, consider also an attack causing a failure on the power grid, as highlighted by alarm X3. The vector of anomalies is summarised as follows:

- T0: $v = [\alpha, \beta, 0]$
- T1: $v = [\alpha, \beta, 0]$
- T2: $v = [\alpha, 0, 0]$
- T3: $v = [\alpha, 0, 0]$
- T4: $v = [0, 0, \gamma]$
- T5: $v = [0, 0, \gamma]$

where $alpha = 0.6$ and $\beta = 0.9$ and $\gamma = 0.7$.

In Table 2, outputs of the example are shown,with regard to mass assignment. It can be noticed that until time step T3, as in previous example, the system is able to understand the cause of evidences gathered. As soon as the alarm X3 arises, evidence theory algorithm registers high conflict between previous evidences and the new one and assign big part of the mass to the empty set, reducing the mass of all other subsets. After

some iterations, the algorithm is not any more able to identify the subset containing the truth, and it can only state that high contradiction among data has resulted.

Table 2 Mass assignment for the second example

	T0	*T1*	*T2*	*T3*	*T4*	*T5*
$\{\emptyset\}$	0	0	0	0	0.693	0.9009
$\{H1\}$	0	0	0	0	0	0
$\{H2\}$	0	0	0	0	0	0
$\{H3\}$	0.54	0.8316	0.9266	0.9647	0.2894	0.0868
$\{H4\}$	0	0	0	0	0	0
$\{H1, H2\}$	0	0	0	0	0.007	0.0091
$\{H1, H3\}$	0	0	0	0	0	0
$\{H1, H4\}$	0	0	0	0	0	0
$\{H2, H3\}$	0	0	0	0	0	0
$\{H2, H4\}$	0	0	0	0	0	0
$\{H3, H4\}$	0.36	0.1584	0.0634	0.0253	0.0076	0.0023
$\{H1, H2, H3\}$	0.06	0.0084	0.0094	0.0097	0.0029	0.0009
$\{H1, H2, H4\}$	0	0	0	0	0	0
$\{H1, H3, H4\}$	0	0	0	0	0	0
$\{H2, H3, H4\}$	0	0	0	0	0	0
$\{H1, H2, H3, H4\}$	0.04	0.0016	0.0006	0.0003	0.0001	0.0000

Results of this example confirm that evidence theory does not suit dynamic pattern recognition problems.

To overcome this limit, we suggest to re-distribute the mass of the empty-set to the universal one, expressing the maximum ignorance on the true cause. Starting from the universal set, the mass can be spread on all possible subsets of the power set and the system can properly identify both causes, occurred one after the other. With this regard, inputs of the algorithm and mass redistribution at each time step are reported hereafter:

$T0 : v = [\alpha, \beta, 0]$

$T1 : v = [\alpha, \beta, 0]$

$T2 : v = [\alpha, 0, 0]$

$T3 : v = [\alpha, 0, 0]$

$T4 : v = [0, 0, \gamma]$

$T5 : v = [0, 0, \gamma]$

$T6$: mass re-distribution

$T7 : v = [0, 0, \gamma]$

$T8$: mass re-distribution

$T9 : v = [0, 0, \gamma]$

Table 3 Mass assignment for the second example, using the re-distribution approach starting from T5

	T5	*T6*	*T7*	*T8*	*T9*
$\{\emptyset\}$	0.9009	0	0.0624	0	0.0187
$\{H1\}$	0	0	0	0	0
$\{H2\}$	0	0	0	0	0
$\{H3\}$	0.0868	0.0868	0.0260	0.0260	0.0078
$\{H4\}$	0	0	0	0	0
$\{H1, H2\}$	0.0091	0.0091	0.6404	0.6404	0.8734
$\{H1, H3\}$	0	0	0	0	0
$\{H1, H4\}$	0	0	0	0	0
$\{H2, H3\}$	0	0	0	0	0
$\{H2, H4\}$	0	0	0	0	0
$\{H3, H4\}$	0.0023	0.0023	0.0007	0.0007	0.0002
$\{H1, H2, H3\}$	0.0009	0.0009	0.0003	0.0003	0.0001
$\{H1, H2, H4\}$	0	0	0	0	0
$\{H1, H3, H4\}$	0	0	0	0	0
$\{H2, H3, H4\}$	0	0	0	0	0
$\{H1, H2, H3, H4\}$	0.0000	0.9009	0.2703	0.3326	0.0998

Note: Values for previous time steps are in 2.

In Table 3 are shown the outputs of the algorithm from T5 to T9, considering that at time T6 and T8 the system applies mass re-distribution from the empty set to the universal one. The result is that the algorithm approach can also recognise dynamical pattern, as in Table 3. In fact at time T5 the highest value is associated to $\{H3\}$ and at time T9 this value is related to $\{H1, H2\}$. The re-distribution of masses should be applied till the value of the mass of the empty-set is above a pre-defined threshold value.

5.3 Third example: the wrong knowledge model

In this example, we consider an extension of the previous case: after the failure on the power grid, we suppose that another alarm cause X2 arising, while X3 is still persisting. So in these time steps, we have two faults simultaneously: a fault occurred in the power grid and one in the equipment of the telecommunication network. A possible cause for both could be a fire, as it can destroy some branches of the power grid and also equipment that are in proximity to the fire.

The vector of anomalies is the following:

$T0 : v = [\alpha, \beta, 0]$

$T1 : v = [\alpha, \beta, 0]$

$T2 : v = [\alpha, 0, 0]$

$T3 : v = [\alpha, 0, 0]$

$T4 : v = [0, 0, \gamma]$

$T5 : v = [0, 0, \gamma]$

$T6$: mass re-distribution

$T7 : v = [0, 0, \gamma]$

$T8$: mass re-distribution

$T9 : v = [0, 0, \gamma]$

$T10 : v = [0, \beta, \gamma]$

$T11$: mass re-distribution

$T12 : v = [0, \beta, \gamma]$

$T13$: mass re-distribution

$T14 : v = [0, \beta, \gamma]$

Also in this case, we apply the re-distribution algorithm at time step T11 and T13. The re-distribution algorithm can be applied if the value of the empty set is higher than a threshold value. For this reason at time T10, we does not execute the re-distribution algorithm: the value of empty set $\{\emptyset\}$ at T9, as 0.0187 is under the minimum threshold.

Table 4 Mass assignment for the third example, using the re-distribution approach starting from T9

	T9	*T10*	*T11*	*T12*	*T13*	*T14*
$\{\emptyset\}$	0.0187	0.8733	0	0.6575	0	0.6663
$\{H1\}$	0	0	0	0	0	0
$\{H2\}$	0	0	0	0	0	0
$\{H3\}$	0.0078	0.0024	0.0024	0.0007	0.0007	0.0002
$\{H4\}$	0	0	0	0	0	0
$\{H1, H2\}$	0.8734	0.0943	0.0943	0.0708	0.0708	0.0549
$\{H1, H3\}$	0	0	0	0	0	0
$\{H1, H4\}$	0	0	0	0	0	0
$\{H2, H3\}$	0	0	0	0	0	0
$\{H2, H4\}$	0	0	0	0	0	0
$\{H3, H4\}$	0.0002	0.0270	0.0270	0.2447	0.2447	0.2580
$\{H1, H2, H3\}$	0.0001	0.0000	0.0000	0.0000	0.0000	0.0000
$\{H1, H2, H4\}$	0	0	0	0	0	0
$\{H1, H3, H4\}$	0	0	0	0	0	0
$\{H2, H3, H4\}$	0	0	0	0	0	0
$\{H1, H2, H3, H4\}$	0.0098	0.0030	0.8763	0.0263	0.6838	0.0205

Note: Values for previous time steps are in Tables 2 and 3.

In Table 4 we show only last results of the algorithm. In this case the re-distribution of masses does not reduce the contradiction value as evidences gathered will always be in conflict with regard to the knowledge model employed, despite previous example.

In this case, transferring the empty set mass to the ignorance set does not lead to a correct classification of a new situation, but causes again the increasing of $m(\emptyset)$. For what stated before, such a kind of cycles can be regarded as a metric to identify modelling errors and to trigger learning process for real-time model correction.

One possible action to take in this cases is to modify the knowledge model employed as reference. In our example, the problem arises considering together X2 and X3 alarms. In fact the intersection of relative hypotheses of these alarms is the empty set. For

this reason, a possible approach is to increase the frame of discernment, adding a new hypothesis H5. This hypothesis H5 is linked by two edges that go into X2 and X3 alarms. The new knowledge model is depicted in Figure 4. Let now consider the new knowledge model and the following vector of anomalies:

$T0 : v = [\alpha, \beta, 0]$

$T1 : v = [\alpha, \beta, 0]$

$T2 : v = [\alpha, 0, 0]$

$T3 : v = [\alpha, 0, 0]$

$T4 : v = [0, 0, \gamma]$

$T5 : v = [0, 0, \gamma]$

$T6$: mass re-distribution

$T7 : v = [0, 0, \gamma]$

$T8$: mass re-distribution

$T9 : v = [0, 0, \gamma]$

$T10 : v = [0, \beta, \gamma]$

$T11$: mass re-distribution

$T12 : v = [0, \beta, \gamma]$

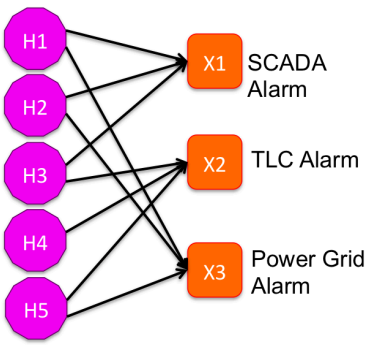
$T13$: mass re-distribution with new hypothesis in the knowledge model

$T14 : v = [0, \beta, \gamma]$

$T15$: mass re-distribution with new hypothesis in the knowledge model

$T16 : v = [0, \beta, \gamma]$

Figure 4 The new knowledge model, considering a frame of discernment of five hypotheses (see online version for colours)



The mass re-allocation process is still necessary to allow the evaluation to evolve. As shown in Table 4 only applying the mass transferring is not enough to model possible causes occurring in the field. As soon as it is noticed that the empty set mass increses

ad decreases with mass-redistribution, at time step T13, the new hypothesis H5 is introduced and, at T14, the higher value of mass is allocated on H5 hypothesis. The empty-set mass is reduced, and this is still true at time T16, after another execution of mass-reallocation and evidence theory. The label associated to H5 can be the fire explosion described in the initial part of the example, but in real-time context and with automatic procedures, identifying the meaning associated to H5 can be very difficult without the help of human operators.

Table 5 Mass assignment for the third example, applying at T13 the new knowledge model

	T9	*T10*	*T11*	*T12*	*T13*	*T14*	*T15*	*T16*
$\{\emptyset\}$	0.0187	0.8733	0	0.6575	0	0.2520	0	0.0650
$\{H1\}$	0	0	0	0	0	0	0	0
$\{H2\}$	0	0	0	0	0	0	0	0
$\{H3\}$	0.0078	0.0024	0.0024	0.0007	0.0007	0.0002	0.0002	0.0001
$\{H4\}$	0	0	0	0	0	0	0	0
$\{H5\}$	-	-	-	-	0	0.4142	0.4142	0.7512
$\{H1, H2\}$	0.8734	0.0943	0.0943	0.0708	0.0708	0.0089	0.0089	0.0009
$\{H1, H3\}$	0	0	0	0	0	0	0	0
$\{H1, H4\}$	0	0	0	0	0	0	0	0
$\{H1, H5\}$	-	-	-	-	0	0	0	0
$\{H2, H3\}$	0	0	0	0	0	0	0	0
$\{H2, H4\}$	0	0	0	0	0	0	0	0
$\{H2, H5\}$	-	-	-	-	0	0	0	0
$\{H3, H4\}$	0.0002	0.0270	0.0270	0.2447	0.2447	0.0805	0.0805	0.0244
$\{H3, H5\}$	-	-	-	-	0	0	0	0
$\{H4, H5\}$	-	-	-	-	0	0	0	0
$\{H1, H2, H3\}$	0.0001	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
$\{H1, H2, H4\}$	0	0	0	0	0	0	0	0
$\{H1, H2, H5\}$	-	-	-	-	0	0.0460	0.0460	0.0236
$\{H1, H3, H4\}$	0	0	0	0	0	0	0	0
$\{H1, H3, H5\}$	-	-	-	-	0	0	0	0
$\{H1, H4, H5\}$	-	-	-	-	0	0	0	0
$\{H2, H3, H4\}$	0	0	0	0	0	0	0	0
$\{H2, H3, H5\}$	-	-	-	-	0	0	0	0
$\{H2, H4, H5\}$	-	-	-	-	0	0	0	0
$\{H3, H4, H5\}$	-	-	-	-	0	0.1775	0.1775	0.1266
$\{H1, H2, H3, H4\}$	0.0998	0.0030	0.8763	0.0263	0.0263	0.0008	0.0008	0.0000
$\{H1, H2, H3, H5\}$	-	-	-	-	0	0	0	0
$\{H1, H2, H4, H5\}$	-	-	-	-	0	0	0	0
$\{H1, H3, H4, H5\}$	-	-	-	-	0	0	0	0
$\{H2, H3, H4, H5\}$	-	-	-	-	0	0	0	0
$\{H1, H2, H3, H4, H5\}$	-	-	-	-	0.6575	0.0197	0.2718	0.0082

Note: Values for previous time steps are in Tables 2 and 3.

6 Conclusions

In this paper an architecture for the situation assessment in the context of critical infrastructure protection is provided. Such an architecture allows to overcome the

limitations of online interdependency models by preprocessing field data by means of evidence theory algorithms, thus providing information on the causes of failure, rather than on the effects (i.e., the simple disruption/disconnection of elements). This framework is specifically designed for real-time context and for distributed situations, see also (Foglietta et al., 2012).

Such a SAW approach has been applied to critical infrastructure interdependency analysis in order to increase the awareness about causes of malfunctioning, such as natural disasters or malicious events. The capability of promptly understanding situations related to critical infrastructures is crucial as it may lead to better decisions and quicker countermeasures to mitigate the effects of potential threats.

To this end, an evidence theory framework has been provided, addressing the issue of wrong/incomplete knowledge model.

Future work will be devoted to refine the assessment procedure and to integrate such a framework with online interdependency models; finally, an important step would be to close the loop by refining the awareness procedure based on the estimations performed by interdependency models.

References

Barford, P., Dacier, M., Dietterich, T.G., Fredrikson, M., Giffin, J., Jajodia, S., Jha, S., Li, J., Liu, P., Ning, P., Ou, X., Song, D., Strater, L., Swarup, V., Tadda, G., Wang, C. and Yen, J. (2010) 'Cyber SA: situational awareness for cyber defense', *Cyber Situational Awareness*, Vol. 46, pp.3–13.

De Porcellinis, S., Setola, R., Panzieri, S. and Ulivi, G. (2008) 'Simulation of heterogeneous and interdependent critical infrastructures', *International Journal of Critical Infrastructures*, Vol. 4, No. 1, pp.110–128.

Dempster, A. (2008) 'Upper and lower probabilities induced by a multivalued mapping', *Classic Works of the Dempster-Shafer Theory of Belief Functions*, Vol. 219, No. 2, pp.57–72.

Dubois, D. and Prade, H. (1995) 'Possibility theory as a basis for qualitative decision theory', *Proceedings of the 14th International Joint Conference on Artificial Intelligence*, Vol. 2, pp.1924–1930.

Endsley, M.R. (1995) 'Toward a theory of situation awareness in dynamic systems', *Proceedings of the Human Factors Society*, Vol. 37, No. 1, pp.32–64.

European Commission (2011) 'Achievements and next steps: towards global cyber-security', Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the Regions on Critical Information Infrastructure Protection.

Falliere, N., O'Murchu, L. and Chien, E. (2011) 'W32. Stuxnet Dossier', White Paper, Symantec Corp., Security Response, Version 1.4.

Foglietta, C., Oliva, G. and Panzieri, S. (2011) 'Online distributed evaluation of interdependent critical infrastructures', *Nonlinear Estimation and Applications to Industrial Systems Control*, Nova Pubblications, To appear.

Foglietta, C., Gasparri, A. and Panzieri, S. (2012) 'Networked evidence theory framework for critical infrastructure modeling', *Proceedings of Sixth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection*.

FP7 MICIE Project (2010) Available at http://www.micie.eu.

Gasparri, A., Oliva, G. and Panzieri, S. (2009) 'On the distributed synchronization of on-line IIM interdependency models', *Proceedings of the 7th IEEE International Conference on Industrial Informatics*, Cardiff (UK), June, pp.795-800.

Gutwin, C. and Greenberg, S. (2002) 'A descriptive framework of workspace awareness for real-time groupware', *Comput. Supported Coop. Work*, Vol. 11, No. 3, pp.411–446, DOI=10.1023/A:1021271517844, available at http://dx.doi.org/10.1023/A:1021271517844.

Haimes, Y. and Jiang, P. (2001) 'Leontief-based model of risk in complex interconnected infrastructures', *Journal of Infrastructure Systems*, No. 1, pp.1–12.

Oliva, G. (2012) 'Stability and level-wise representation of discrete-time fuzzy systems', *International Journal of Fuzzy Systems*, Vol. 14, No. 2, pp.185–192.

Oliva, G., Panzieri, S. and Setola, R. (2011a) 'Fuzzy dynamic input-output inoperability model', *International Journal on Critical Infrastructure Protection*, Vol. 4, Nos. 3–4, pp.165–175.

Oliva, G., Panzieri, S. and Setola, R. (2011b) 'Online distributed interdependency estimation for critical infrastructures', *50th IEEE Conference on Decision and Control*, to appear.

Oliva, G., Panzieri, S. and Setola, R. (2012) 'Distributedsynchronization under uncertainty: a fuzzy approach', *Fuzzy Sets and Systems*, Elsevier, DOI: 10.1016/j.fss.2012.02.003.

Panzieri, S. and Setola, R. (2008) 'Failures propagation in critical interdependent infrastructures', *International Journal of Modelling, Identification and Control*, Vol. 3, No. 1, pp.69–78.

Rieger, C.G., Gertman, D.I. and McQueen, M.A. (2009) 'Resilient control systems: next generation design research', *Conference on Human System Interactions*, pp.632–636.

Rinaldi, S.M. (2004) 'Modeling and simulating critical infrastructures and their interdependencies', *Proceedings of the Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, Vol. 2, No. 1, pp.1–8.

Rios, B. and McCorkle, T. (2011) '100 Bugs in 100 days: an analysis of ICS (SCADA) Software', *DerbyCon 2011*, Session.

Setola, R., De Porcellinis, S. and Sforna, M. (2009) 'Critical infrastructure dependency assessment using input-output inoperability model', *Int. J. Critical Infrastructure Protection (IJCIP)*, Vol. 2, No. 4, pp.170–178.

Shafer, G. (1976) 'A mathematical theory of evidence', *A Mathematical Theory of Evidence*.

Smets, P. (1990) 'The combination of evidence in the transferable belief model', *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 12, No. 5, pp.447–458.