Situational Awareness Using Distributed Data Fusion with Evidence Discounting

Antonio Pietro, Stefano Panzieri, Andrea Gasparri

Chapter 17

SITUATIONAL AWARENESS USING DISTRIBUTED DATA FUSION WITH EVIDENCE DISCOUNTING

Antonio Di Pietro, Stefano Panzieri and Andrea Gasparri

Abstract Data fusion provides a means for combining pieces of information from various sources and sensors. This chapter presents a data fusion methodology for interdependent critical infrastructures that leverages a distributed algorithm that allows the sharing of the possible causes of faults or threats affecting the infrastructures, thereby enhancing situational awareness. Depending on the degree of coupling, the algorithm modulates the information content provided by each infrastructure using a data fusion technique called evidence discounting. The methodology is applied to a case study involving a group of dependent critical infrastructures. Simulation results demonstrate that the methodology is resilient to temporary faults in the critical infrastructure communications layer.

Keywords: Distributed data fusion, cautious conjunctive rule, evidence discounting

1. Introduction

Combining pieces of information through data fusion techniques can enhance the security of critical infrastructure systems by providing improved situational awareness that supports decision making. Usually, critical infrastructure systems combine the information coming from their sensors individually, without sharing information regarding their operating states with other infrastructures. This is mainly due to the fact that the delivery of sensitive information to external entities poses security issues (see, e.g., [6, 21]). However, in real-time environments, there are numerous scenarios in which allowing full information exchange could be beneficial.

Foglietta et al. [9] have applied an algorithm based on the work of Gasparri et al. [11] to share information among a set of critical infrastructures in order to produce common knowledge and decrease the possibility of producing cascading

effects. In their approach, the infrastructures – implemented as "agents" – constitute a connected network and combine their local information about their operating states using a distributed algorithm. However, the approach requires the network to have a spanning tree topology.

Ducourthial et al. [8] have proposed a distributed algorithm that implements data fusion in unknown topologies. The algorithm computes the confidence of each node by combining all the data received from its neighbors using a "discounted cautious operator" and without relying on a central node for data collection. The algorithm converges for any initial configuration and for any unknown network topology. However, the algorithm requires the network topology to become stable (i.e., nodes and links are fixed and agents do not perform any dynamic observations) in order to reach convergence.

Considerable research has focused on applying data fusion techniques to enhance the security of critical infrastructures. Genge et al. [12] have employed cyber-physical data fusion based on the Dempster-Shafer theory [3, 17] to combine knowledge from the cyber and physical dimensions of critical infrastructures in order to implement an anomaly detection system. The system was validated in a scenario involving distributed denial-of-service attacks on an information network whose disturbances propagated to a simulated power grid. However, the centralized nature of this approach (i.e., all the data must be collected by a single node that performs data aggregation) limits its robustness to single node failures.

Oliva et al. [13] have presented a distributed consensus algorithm based on fuzzy numbers and subsequently applied it to a case study related to crisis management. The algorithm provides consensus on the overall criticality of a situation based on the information provided by human operators regarding the state of critical infrastructures. However, the algorithm is complex and requires the generation of appropriate fuzzy membership functions to model operator opinions. Sousa et al. [20] have proposed a critical infrastructure protection methodology based on distributed algorithms and mechanisms implemented between a set of devices that provide secure gossip-based information diffusion among infrastructures. Although the methodology ensures that the data traffic satisfies security policies for mitigating cyber attacks, it lacks flexibility when dealing with physical threats or uncertain threats.

This chapter presents a data fusion methodology for interdependent critical infrastructures based on the algorithm of Ducourthial et al. [8] to exchange information between critical infrastructures and, thus, increase situational awareness. Simulation results show that each infrastructure converges without relying on a static network topology and despite the presence of link failures (e.g., due to natural disasters or cyber attacks). With respect to distributed consensus, the methodology enables each infrastructure to converge and, thus, capture the particular behavior of an infrastructure that, due to its specific dependencies and/or internal failures, may exhibit a particular state. Moreover, the modeling of failures and threats using the Dempster-Shafer formalism takes into account the imprecision and uncertainty in detecting events without the need

to specify membership functions as required by fuzzy-based approaches. The cautious operator [5] and an evidence discounting function are used to aggregate information provided by the connected infrastructures. This operator ensures network convergence when the network topology and direct confidences are stable [7, 8]. The evidence discounting concept was introduced by Shafer [17] to account for the reliability of source information. Cherfaoui et al. [2] have applied evidence discounting to a network of agents based on the distance and age of received messages before combining them with local knowledge. The proposed methodology uses evidence discounting to decrease the information content provided by a supporting infrastructure that is loosely coupled.

2. Overview of the Methodology

The theoretical framework of Rinaldi et al. [16] defines several dimensions of an infrastructure interdependency: (i) type of interdependency; (ii) infrastructure environment; (iii) coupling characteristics; (iv) type of failure; (v) infrastructure characteristics; and (vi) state of operation. As will be discussed later, the proposed methodology addresses three dimensions: (i) coupling characteristics (e.g., tight or loose according to Perrow [15]); (ii) type of failure (e.g., cascading or common cause or escalating failures); and (iii) state of operation (e.g., normal or stressed).

In order to effectively model and simulate the dynamic behavior of infrastructures, several researchers have engaged the network-based paradigm [14], representing infrastructures as network nodes and physical connections between the infrastructures as links (edges). The nodes and edges in an infrastructure topology deliver/consume services and/or resources to/from other nodes. However, in the proposed methodology, while infrastructures are represented as nodes, the edges correspond to communications channels that allow the exchange of information about the possible cause(s) of faults. The resulting information sharing framework provides higher information content at each infrastructure layer regarding the possible evolution of the state of operation of each infrastructure. This information can be used by decision makers to take immediate countermeasures and, thereby, decrease the possibility of cascading effects.

The proposed methodology involves three steps:

- **Event Detection:** Each infrastructure produces local information (e.g., by using sensors) called "direct confidence" regarding the credibility of possible normal and stressed operating states.

- **Knowledge Aggregation:** The infrastructures aggregate their local information according to the gossip communications paradigm [1] to produce more informative data called "distributed confidence" regarding the credibility of possible normal and stressed operating states.

- **Convergence:** At a certain time, the information has been distributed to such an extent that the distributed confidence of each infrastructure

does not vary (i.e., the agents representing each infrastructure reach convergence).

The Dempster-Shafer formalism [3, 17] is used to deal with the imprecision and uncertainty in detecting events. As explained later, each infrastructure i, when fusing its information with the information received from an infrastructure j, discounts the incoming information according to the degree of coupling between infrastructure i and infrastructure j. In other words, information coming from a loosely coupled infrastructure is considered to be less relevant than information coming from a tightly coupled infrastructure; this expresses the fact that the state of operation of the inputs from the supplying infrastructure would have small or large effects on the receiving infrastructure.

Fusing information from two infrastructures requires knowledge of the degree of coupling of the infrastructures. One approach is to use statistical analysis of historical data about the number of disruptions initiated by one infrastructure that caused cascading failures in a second infrastructure; this provides evidence whether the two infrastructures are tightly or loosely coupled. van Eeten et al. [23] have analyzed public media articles about infrastructure disruptions that occurred in The Netherlands from 2010 to 2014. Their analysis revealed that, depending on the infrastructures where the cascading-initiating failures occurred, certain infrastructures were more frequently affected by cascading failures than other infrastructures. For example, when considering health as the affected sector, 50% of the cascading-initiating failures occurred in the energy sector, 13% in the telecommunications and water sectors, and 24% were the result of internal failures.

With regard to agent (infrastructure) interaction in this work, simulation results demonstrate that the proposed methodology is robust to communications link failures occurring in disaster scenarios. Moreover, a strategy is proposed to update the confidence of each node when a specific communications link is unavailable due to: (i) physical destruction of network infrastructure components; (ii) disruptions in supporting infrastructures; and (iii) disruptions due to congestion [22].

3. Data Fusion

The theory of evidence is a formalism that can be used to model imprecision and uncertainty. The theory, introduced by Dempster [3] and Shafer [17] (also known as the Dempster-Shafer theory), embraces the intuitive idea of associating a number between zero and one to model the degree of confidence of a proposition with partial (e.g., uncertain or imprecise) evidence. Let $\Omega = \{\omega_1, ..., \omega_n\}$ be the set of possible values of a variable ω where the elements ω_i are assumed to be mutually exclusive. Let $\Gamma(\Omega) \triangleq 2^{\Omega} = \{\gamma_1, ..., \gamma_{|\Gamma|}\}$ be the associated power set. In this framework, the set Ω, which is referred to as the "frame of discernment," quantifies the confidence of propositions of the form: "the true value of ω is in γ" with $\gamma \in 2^{\Omega}$.

Definition 1 (Basic Belief Assignment) *A function* $m : 2^{\Omega} \rightarrow [0,1]$ *is called a basic belief assignment (BBA)* m *if* $\sum_{\gamma_a \in 2^{\Omega}} m(\gamma_a) = 1$ *with* $m(\emptyset) = 0$.

Definition 2 (Commonality Function) *A BBA* m *can be equivalently represented by its associated commonality* $q : 2^{\Omega} \rightarrow [0,1]$ *defined as:*

$$q(\gamma_a) = \sum_{\gamma_b \supseteq \gamma_a} m(\gamma_b), \quad \gamma_a \in 2^{\Omega} \tag{1}$$

Thus, for $\gamma_a \in 2^{\Omega}$, $m(\gamma_a)$ is the portion of confidence that supports exactly γ_a (i.e., the fact that the true value of ω is in γ_a) but, due to the lack of further information, does not support any strict subset of γ_a.

The main limitation of the Dempster-Shafer theory is the Dempster combination rule [17], which produces counterintuitive results when strong conflict exists among the sources that are combined [24]. The transferable belief model of Smets [18] also relies on the concept of BBA, but it removes the assumption $m(\emptyset) = 0$. The removal of this assumption applies when the frame of reference is not exhaustive, so it is reasonable to believe that another event, not modeled in the considered frame, will occur. This allows for a refined conjunctive rule that is more robust than the Dempster combination rule in the presence of conflicting evidence [4]. However, this rule and the Dempster combination rule rely on the distinctness assumption with regard to the sources. This limitation can be avoided using an interaction rule called the cautious rule of combination [5], which is associative, commutative and idempotent. The use of the rule is also appropriate when all the sources are considered to be reliable and the assumption of independence is not required.

Definition 3 (Weight Function) *Let* m *be a generic BBA. Then, the relative weight function* $w : 2^{\Omega} \setminus \Omega \rightarrow \mathbb{R}^{+}$ *is defined as:*

$$w(\gamma_a) = \prod_{\gamma_b \supseteq \gamma_a} q(\gamma_b)^{(-1)^{|\gamma_b| - |\gamma_a| + 1}}, \quad \forall \gamma_a \in 2^{\Omega} \setminus \Omega \tag{2}$$

Definition 4 (Cautious Rule of Combination ($\textcircled{\scriptsize \wedge}$)) *Let* m_1 *and* m_2 *be two generic BBAs with weight functions* w_1 *and* w_2*, respectively. Then, their aggregation using the cautious rule of combination is defined by the following weight function:*

$$w_{1 \textcircled{\scriptsize \wedge} 2}(\gamma_a) = min(w_1(\gamma_a), w_2(\gamma_a)), \quad \forall \gamma_a \in 2^{\Omega} \setminus \Omega \tag{3}$$

The data aggregation algorithm works with the weight function $w(\cdot)$, which is obtained using the commonality function $q(\cdot)$ derived from the initial set of BBAs. Table 1 shows the function $w_{1 \textcircled{\scriptsize \wedge} 2}(\cdot)$ obtained by applying the cautious combination rule to the weight functions w_1 and w_2. From now on, $w_{ij}(\cdot)$ will denote the weight function obtained by applying the cautious combination rule to two generic weight functions $w_i(\cdot)$ and $w_j(\cdot)$.

Table 1. Application of the cautious combination rule.

BBA	∅	a	b	Ω
$w_1(\cdot)$	1.0	0.5	0.3	
$w_2(\cdot)$	0.8	0.7	0.2	
$w_{1\textcircled{\scriptsize 0}2}(\cdot)$	0.8	0.5	0.2	

DEFINITION 5 (DISCOUNTING FUNCTION) *Let m be a generic BBA. Then, the relative discounting function $m^\alpha(\gamma_a)$ is defined as follows:*

$$m^\alpha(\gamma_a) = \begin{cases} \alpha\ m(\gamma_a) & \text{for } \gamma_a \subset \Omega \\ 1 - \alpha + \alpha\ m(\gamma_a) & \text{for } \gamma_a = \Omega \end{cases}$$

where $\alpha \in [0, 1]$ is called the discounting factor.

Table 2. BBA $m(\cdot)$ and its relative discounting function $m^\alpha(\cdot)$ ($\alpha = 0.2$).

BBA	∅	a	b	Ω
$m(\cdot)$	–	0.30	0.40	0.30
$w(\cdot)$	1.40	0.50	0.40	
$m^{0.2}(\cdot)$	–	0.06	0.08	0.86
$w^{0.2}(\cdot)$	1.00	0.93	0.91	

Table 2 shows an example of BBA $m(\cdot)$ and its relative discounting function $m^\alpha(\cdot)$ obtained for $\alpha = 0.2$. The table also presents the weight functions associated with the two BBAs.

4. Data Fusion Methodology

The goal is to create a model that represents the interdependencies and the communications channels between critical infrastructures as a graph structure. The model embeds the notion of degree of coupling based on the general model of Rinaldi et al. [16] and the specific assumptions described earlier.

4.1 Motivation

In order to motivate the choice of the model, consider $n = 5$ dependent critical infrastructures that can be affected by failures or threats. Each infrastructure is able to produce one BBA expressed as a weight function $w(\cdot)$ from the physical and cyber events detected by the aggregation agents. The frame of discernment is $\Omega = \{a, b, c\}$ where a denotes a possible physical failure, b a possible cyber intrusion or attack and c a normal functioning level.

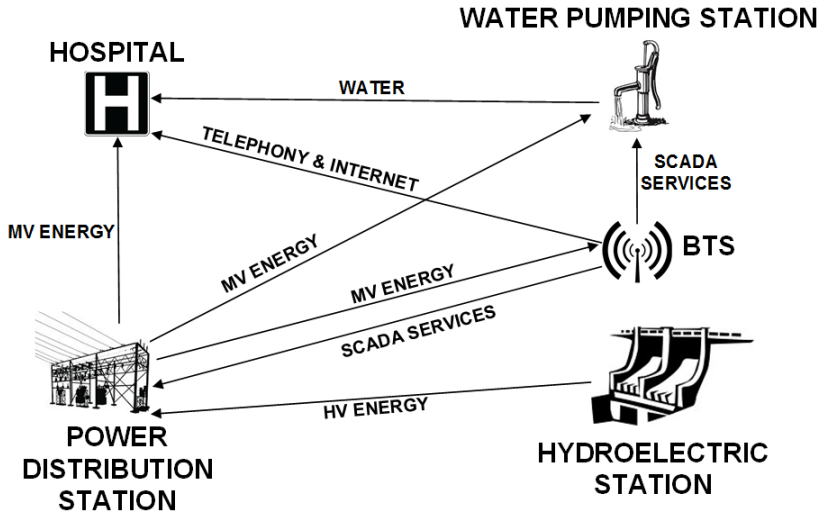

Figure 1. Resources exchanged by the infrastructures.

Assume that the set of systems is geographically distributed and generically corresponds to the infrastructures of a city district. The scenario, derived from [10], incorporates a hydroelectric power station that feeds a power distribution station through a transmission network (not modeled for simplicity). A base transceiver station (BTS) provides telecommunications services required by the SCADA systems of the power distribution station and water pumping station. The base transceiver system receives electricity from the power distribution station. The water pumping station receives electricity from the power distribution station to operate automation devices and water pumps. Failures occurring in the considered infrastructures may produce disruptions at a hospital that receives water from the water pumping station and electricity from the power distribution station. In addition, the hospital may suffer a disruption during a malfunction of the base transceiver system, which provides mobile communications.

Figure 1 shows the dependency layer of the scenario. Assume that the infrastructures can exchange information regarding possible failures or threats. Communications employ virtual private network links between the infrastructures that exhibit non-negligible dependencies.

The model introduced in the following section is able to capture the various couplings between the infrastructures and implement information sharing to enhance situational awareness in the infrastructures.

4.2 Weighted Digraphs

Formally, the model is represented as a weighted digraph $\mathcal{G} = (\mathcal{V}, \mathcal{E}(t), \mathcal{Q})$ where $\mathcal{V} = \{v_1, ..., v_n\}$ with $n > 1$ is the vertex set, $\mathcal{E}(t) = \{e_{ij}\}$ is the edge set

and $\mathcal{Q} = \{q_{ij}\}$ with $q_{ij} \in \mathcal{P} = \{l, m, h\}$ is the set of weight indices associated with each edge e_{ij} in $\mathcal{G}$. It is assumed that $\mathcal{G}$ has no loops. Note that:

- An element v_i of $\mathcal{V}$ represents an agent denoting infrastructure i.
- An element e_{ij} of $\mathcal{E}(t)$ represents the degree of coupling between agents v_i and v_j.
- An element q_{ij} of $\mathcal{Q}$ represents the weight index corresponding to the degree of coupling of agent v_j on agent v_i.

The graph $\mathcal{G}$ represents the dependency layer, where each infrastructure or agent v_j, by combining its direct confidence with the confidences of all the dependent agents v_i, obtains a distributed confidence that expresses the operative level of agent v_j. For the sake of simplicity, technical aspects regarding how communications are realized are abstracted away. More precisely, it is assumed that the graph $\mathcal{G}$ that encodes the network dependence is supported by the communications layer. In other words, communications can always be established between a pair of nodes v_i and v_j with coupling w_{ij} if and only if a non-negligible dependence $e_{ij} \in \mathcal{E}(t)$ exists.

Four assumptions are made regarding the network of agents: (i) graph $\mathcal{G}$ has at least a rooted spanning tree; (ii) every node $v \in \mathcal{V}$ produces a local BBA expressed as a weight function $w(\cdot)$ called the direct confidence; (iii) node communications are asynchronous (i.e., at any time t_k, only a pair of agents (v_i, v_j) interacts); and (iv) each agent can store the current direct confidence, the direct confidences of its ancestors and the distributed confidence that is computed via node aggregation.

4.3 Agent Interactions

In the proposed framework, agent actions are modeled using a gossip algorithm [1], which is defined in terms of the triplet $\{\mathcal{S}, \mathcal{R}, \mathfrak{e}\}$ where:

- $\mathcal{S} = \{s_1, ..., s_n\}$ is the set containing the local states $s_i \in \mathbb{R}^q$ of each agent v_i in the network such that $s_i(t) = (w_i(t, \gamma_1), .., w_i(t, \gamma_q))$ at time t with $q = |2^{\Omega} \setminus \Omega|$.
- $\mathcal{R}$ is the interaction rule based on the cautious operator $\circledcirc$ and the discounting function $r(\cdot)$ where any two agents $v_i, v_j \in \mathcal{V}$ with $e_{ij} \in \mathcal{E}(t)$ yield $\mathcal{R} : \mathbb{R}^q \times \mathbb{R}^q \rightarrow \mathbb{R}^q$ such that:

$$s_j(t) = (w_j(t, \gamma_1) \circledcirc r(w_i(t, \gamma_1)), ..., w_j(t, \gamma_q) \circledcirc r(w_i(t, \gamma_q))) \tag{4}$$

$$r(w_i(t, \gamma_a)) = \begin{cases} r_l(w_i(t, \gamma_a)) = min(1, w_i(t, \gamma_a) + 0.4) & \text{if } q_{ij} = l \\ r_m(w_i(t, \gamma_a)) = min(1, w_i(t, \gamma_a) + 0.25) & \text{if } q_{ij} = m \\ r_h(w_i(t, \gamma_a)) = w_i, (t, \gamma_a) & \text{if } q_{ij} = h \end{cases}$$

Table 3. BBA $m_i^f(0)$ applied to node v_i in case of link failure of e_{ij}.

BBA	**∅**	**a**	**b**	**c**	**ab**	**ac**	**bc**	**Ω**
$m_i^f(0)$	–	0.10	0.10	–	0.40	–	–	0.40

- $\mathfrak{e}$ is the edge selection process that specifies the edges e_{ij} selected at time t.

When updating the generic agent v_j with an incoming agent v_i, a discounting function $r(\cdot)$ is applied to the weight function $w_i(\cdot)$ according to the degree of coupling of v_j on v_i. Note that the choice of the discounting function is generally application-dependent. The function given above is an effective choice for the case study. When the degree of coupling is high ($q_{ij} = h$), the discounting function leaves $w_i(\cdot)$ unchanged. However, when the coupling is medium or low ($q_{ij} = m$ or $q_{ij} = l$, respectively), the discounting function applies a decreasing constant factor to $w_i(\cdot)$. This way, the refined $r(w_i(\cdot))$ approaches the neutral element $w_\perp$ (unit vector consisting only of one values) with respect to the cautious operator to handle low couplings. In order to render the algorithm robust to communications link failures, when the edge selection process $\mathfrak{e}$ extracts one or more links e_{ij} that are unavailable at a certain time t, the algorithm associates the BBA $m_i^f(\cdot)$ to nodes v_i that cannot communicate with node v_j that performs the update. The BBA $m_i^f(\cdot)$ reported in Table 3 implements the worst-case policy that increases the credibility of failures a and b when no information is available about the state of operation of agent v_i.

The proposed methodology is formalized as Algorithm 1, which extends the approach proposed by Ducourthial et al. [8].

4.4 Graph Construction

Based on the model and the example scenario, a graph $\mathcal{G}$ with $n = 5$ agents was constructed where each agent modeled a specific infrastructure and each link modeled the dependency existing between the corresponding infrastructures. The assignment of weights considered the incident data collected by van Eeten et al. [23] and the application of the method based on the occurrence of historical cascading faults described earlier. For each infrastructure i, let $R_j = \frac{N_j}{N_i}$ be the number of historical faults N_j initiated in infrastructure j that produced a fault in infrastructure i calculated over the total number of cascading failures N_i affecting infrastructure i. For each dependency between infrastructures i and j, four cases exist: (i) $q_{ij} = h$ when $R_j \geq 80\%$; (ii) $q_{ij} = m$ when $80\% > R_j \geq 20\%$; (iii) $q_{ij} = l$ when $20\% > R_j \geq 5\%$; and (iv) a negligible dependency (not modeled as an edge) when $R_j < 5\%$. Because there was no mention of cascading failures occurring among the different infrastructures of the energy sector, it was decided to associate a high dependency on

Algorithm 1 : Gossip algorithm.

procedure GossipAlgorithm($s_j(0) \ \ \forall\, j \in 1, ..., N$)
  while stop_condition **do**
    for each edge $e_{ij} \in \mathcal{E}(t)$ according to e **do**
      Update the state of agent j according to R:
      if $q_{ij} = l$ **then**
        $s_j(t+1) = s_j(t) \circledcirc r_l(s_i(t))$
      else
        if $q_{ij} = m$ **then**
          $s_j(t+1) = s_j(t) \circledcirc r_m(s_i(t))$
        else
          $s_j(t+1) = s_j(t) \circledcirc r_h(s_i(t))$
        end if
      end if
    end for
    $t = t + 1$
  end while
  Return $s_j(t_{stop}) \ \ \forall\, i \in 1, ..., N$
end procedure

the power distribution station of the hydroelectric station and to consider it as an autonomous system.

Figure 2 shows the dependency layer graph $\mathcal{G}$ for the example scenario where each edge is labeled with the service provided and the relative degree of coupling. Note that the l, m and h denote low, medium and high degrees of coupling, respectively. The resulting system can be modeled as a multi-agent platform for distributed data aggregation, where each agent produces a BBA expressing the possible critical event(s) and interacts with other agents via a communications channel.

5. Simulation Results

This section presents the simulation results obtained for two situations in the example scenario: (i) the network topology $\mathcal{G}$ is stable (i.e., the set of agents $\mathcal{V}$ and the set of edges $\mathcal{E}$ are both static); and (ii) the network topology $\mathcal{G}$ is dynamic (i.e., the set of agents $\mathcal{V}$ is static and the set of edges $\mathcal{E}$ is dynamic (time-varying)). For each of the two situations, two cases were considered: (i) the direct confidence produced by each agent is static; and (ii) the direct confidence produced by each agent is dynamic (i.e., time-varying). In the situation where the network topology is dynamic, it is assumed that, at each time step, the graph $\mathcal{G}$ is connected and corresponds to a rooted spanning tree. For all four cases, the pignistic transformation [19] was used to transform the convergent normalized BBA $m(\cdot)$ to a probability measure $P_m = Bet(m)$ as follows:

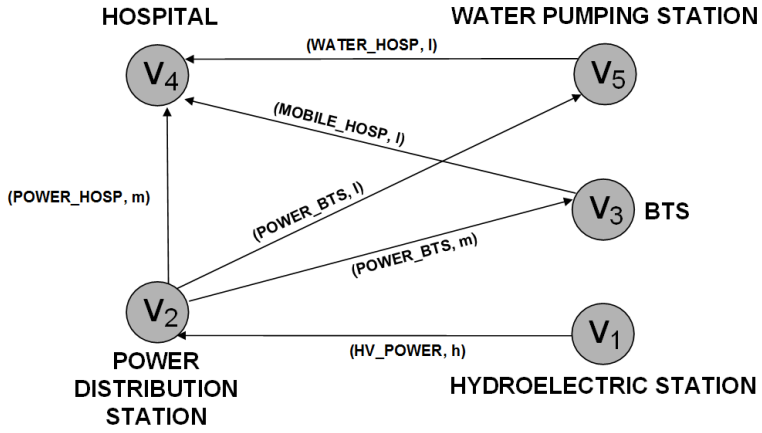

Figure 2. Dependency layer graph $\mathcal{G}$ for the example scenario.

$$P_m(\gamma_a) = \sum_{\emptyset \neq \gamma_b \subseteq \Omega} m(\gamma_b) \frac{|\gamma_a \cap \gamma_b|}{|\gamma_b|}, \qquad \gamma_a \in 2^{\Omega} \tag{5}$$

This measure is useful to decision makers because it quantifies the probability of occurrence of the operational states of an infrastructure.

5.1 Static Network Topology

This section presents the simulation results obtained for the two cases of static and dynamic direct confidence of agents given a static network topology.

Static (Time-Invariant) Confidence. This case considers a stable network topology $\mathcal{G}$ where the set of agents $\mathcal{V}$ and the set of edges $\mathcal{E}$ are both static and the direct confidence of the agents is time-invariant. Table 4 shows the simulation results in terms of the convergent BBAs obtained at time $\overline{t} = 5$ and based on a specific set of BBAs for the system of five agents at time $t = 0$. The results show that agent v_4, which monitors the hospital, starts with a probability of normal functioning $P_{m_4}(t = 0) = 0.55$ and reaches a lower probability of normal functioning $P_{m_4}(t = 5) = 0.38$. This can be explained by the fact that the water pumping station and the power distribution grid maintain stable normal functioning levels over time.

Dynamic (Time-Varying) Confidence. This case considers a stable network topology $\mathcal{G}$ where the set of agents $\mathcal{V}$ and the set of edges $\mathcal{E}$ are both static and the direct confidence of the agents varies over time. Table 5 shows the simulation results in terms of the convergent BBAs obtained at time $\overline{t} = 43$ and based on a specific set of BBAs for the system of five agents through dynamic observations of agents v_2 and v_3 at time $t = 40$. The results show that agent v_4, starts with a probability of normal functioning $P_{m_4}(t = 0) = 0.55$ and reaches

Table 4. Simulation results (static network topology; static agent confidence).

BBA	**∅**	**a**	**b**	**c**	**ab**	**ac**	**bc**	**Ω**
$m_1(0)$	–	–	–	0.70	–	–	–	0.30
$m_2(0)$	–	–	–	0.50	–	–	–	0.50
$m_3(0)$	–	–	0.20	0.20	–	0.10	0.10	0.40
$m_4(0)$	–	–	0.10	0.30	–	0.15	0.15	0.30
$m_5(0)$	–	–	0.20	0.20	–	0.10	0.10	0.40
$\overline{m}_1(\overline{t})$	–	–	–	0.70	–	–	–	0.30
$\overline{m}_2(\overline{t})$	–	–	–	0.50	–	–	–	0.50
$\overline{m}_3(\overline{t})$	0.11	–	0.17	0.20	–	0.09	0.09	0.34
$\overline{m}_4(\overline{t})$	0.09	–	0.09	0.27	–	0.14	0.14	0.27
$\overline{m}_5(\overline{t})$	0.11	–	0.18	0.18	–	0.09	0.09	0.35

Table 5. Simulation results (static network topology; dynamic agent confidence).

BBA	**∅**	**a**	**b**	**c**	**ab**	**ac**	**bc**	**Ω**
$m_1(0)$	–	–	–	0.70	–	–	–	0.30
$m_2(0)$	–	–	–	0.50	–	–	–	0.50
$m_3(0)$	–	–	0.20	0.20	–	0.10	0.10	0.40
$m_4(0)$	–	–	0.10	0.30	–	0.15	0.15	0.30
$m_5(0)$	–	–	0.20	0.20	–	0.10	0.10	0.40
$m_2(40)$	–	0.05	0.30	0.10	0.25	0.05	–	0.25
$m_3(40)$	–	–	0.30	0.20	–	0.20	0.10	0.20
$\overline{m}_1(\overline{t})$	–	–	–	0.70	–	–	–	0.30
$\overline{m}_2(\overline{t})$	–	0.05	0.30	0.10	0.25	0.05	–	0.25
$\overline{m}_3(\overline{t})$	0.12	0.05	0.30	0.13	0.05	0.14	0.07	0.14
$\overline{m}_4(\overline{t})$	0.16	0.03	0.13	0.20	0.07	0.10	0.10	0.20
$\overline{m}_5(\overline{t})$	0.12	0.01	0.19	0.16	0.04	0.08	0.08	0.32

a lower probability of normal functioning $P_{m_4}(t = 43) = 0.29$. This can be explained by the fact that the normal functioning of the power distribution grid has decreased credibility.

Additionally, it was discovered that, if the direct confidences change at time t' with $t' > \overline{t}$ where $\overline{t}$ is the convergence time before the dynamic observations occur, then the edge selection policy does not influence the convergent BBAs. On the other hand, if the direct confidences change at time $t' < \overline{t}$, then the edge selection policy causes the network to reach a different equilibrium point for the convergent BBAs.

Table 6. Simulation results (dynamic network topology; static agent confidence).

BBA	**∅**	**a**	**b**	**c**	**ab**	**ac**	**bc**	**Ω**
$m_1(0)$	–	–	–	0.70	–	–	–	0.30
$m_2(0)$	–	–	–	0.50	–	–	–	0.50
$m_3(0)$	–	–	0.20	0.20	–	0.10	0.10	0.40
$m_4(0)$	–	–	0.10	0.30	–	0.15	0.15	0.30
$m_5(0)$	–	–	0.20	0.20	–	0.10	0.10	0.40
$\overline{m}_1(\overline{t})$	–	–	–	0.70	–	–	–	0.30
$\overline{m}_2(\overline{t})$	0.02	–	0.02	0.48	–	–	–	0.48
$\overline{m}_3(\overline{t})$	0.17	0.02	0.19	0.15	0.09	0.06	0.06	0.26
$\overline{m}_4(\overline{t})$	0.16	0.03	0.13	0.20	0.07	0.10	0.10	0.21
$\overline{m}_5(\overline{t})$	0.13	0.01	0.19	0.16	0.03	0.08	0.08	0.32

5.2 Dynamic Network Topology

This section presents the simulation results obtained for the two cases of static and dynamic direct confidence of agents given a dynamic network topology.

Static (Time-Invariant) Confidence. This case considers a dynamic network topology $\mathcal{G}$ where the set of agents $\mathcal{V}$ is static, the set of edges $\mathcal{E}$ varies over time and the direct confidence of the agents is time-invariant. In the dynamic topology, it is assumed that, at each time step, the set of edges $\mathcal{E}(t)$ may or may not contain some of the edges, e_{23}, e_{24}, e_{25}, e_{34} and e_{54}, so that the graph $\mathcal{G}$ is always connected and exhibits at least a rooted spanning tree. For each link, the probability of failure is assumed to be $P_f = 0.5$.

Table 6 shows the simulation results in terms of the convergent BBAs obtained at time $\overline{t} = 31$. The results show that agent v_4 starts with a probability of normal functioning $P_{m_4}(t = 0) = 0.55$ and reaches a lower probability of normal functioning $P_{m_4}(t = 31) = 0.29$. This can be explained by the occurrence of several link failures that are managed by considering $m_i^f(\cdot)$ as a BBA for a node v_i that cannot communicate with node v_j.

Dynamic (Time-Varying) Confidence. This case considers a dynamic network topology $\mathcal{G}$ where the set of agents $\mathcal{V}$ is static, the set of edges $\mathcal{E}$ varies over time and the direct confidence of the agents varies over time. In the dynamic topology, it is assumed that, at each time step, the set of edges $\mathcal{E}(t)$ may or may not contain some of the edges, e_{23}, e_{24}, e_{25}, e_{34} and e_{54}, so that the graph $\mathcal{G}$ is always connected and exhibits at least a rooted spanning tree. Table 7 shows the simulation results in terms of the convergent BBAs obtained at time $\overline{t} = 50$ and based on a specific set of BBAs for the system of five agents through dynamic observations of agents v_2 and v_3 at time $t = 40$. The

Table 7. Simulation results (dynamic network topology; dynamic agent confidence).

BBA	**∅**	**a**	**b**	**c**	**ab**	**ac**	**bc**	**Ω**
$m_1(0)$	–	–	–	0.70	–	–	–	0.30
$m_2(0)$	–	–	–	0.50	–	–	–	0.50
$m_3(0)$	–	–	0.20	0.20	–	0.10	0.10	0.40
$m_4(0)$	–	–	0.10	0.30	–	0.15	0.15	0.30
$m_5(0)$	–	–	0.20	0.20	–	0.10	0.10	0.40
$m_2(5)$	–	–	0.20	0.20	–	0.10	0.10	0.40
$m_3(5)$	–	–	0.10	0.30	–	0.15	0.15	0.30
$\overline{m}_1(\overline{t})$	–	–	–	0.70	–	–	–	0.30
$\overline{m}_2(\overline{t})$	–	0.05	0.30	0.10	0.25	0.05	–	0.25
$\overline{m}_3(\overline{t})$	0.31	0.04	0.24	0.11	0.04	0.11	0.05	0.11
$\overline{m}_4(\overline{t})$	0.16	0.03	0.13	0.21	0.07	0.10	0.10	0.20
$\overline{m}_5(\overline{t})$	0.12	0.01	0.19	0.16	0.04	0.08	0.08	0.32

simultaneous changes of links and direct confidences of the agents over time causes the network to reach a different equilibrium point.

6. Conclusions

The data fusion methodology described in this chapter enables interdependent critical infrastructures to exchange information about possible threats and failures in order to increase situational awareness. The effectiveness of the methodology was demonstrated using a realistic scenario of critical infrastructures with different degrees of coupling that produce early warnings of possible physical and cyber events. Simulation results reveal that the methodology is robust to communications link failures and converges after the last dynamic observations of the infrastructures. Future work will focus on mathematical proofs of convergence for the static and dynamic network configurations.

References

[1] S. Boyd, A. Ghosh, B. Prabhakar and D. Shah, Randomized gossip algorithms, *IEEE Transactions on Information Theory*, vol. 52(6), pp. 2508–2530, 2006.

[2] V. Cherfaoui, T. Denoeux and Z. Cherfi, Distributed data fusion: Application to confidence management in vehicular networks, *Proceedings of the Eleventh International Conference on Information Fusion*, 2008.

[3] A. Dempster, A generalization of Bayesian inference, *Journal of the Royal Statistical Society, Series B (Methodological)*, vol. 30(2), pp. 205–247, 1968.

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

[5] T. Denoeux, Conjunctive and disjunctive combination of belief functions induced by nondistinct bodies of evidence, *Artificial Intelligence*, vol. 172(2–3), pp. 234–264, 2008.

[6] S. De Porcellinis, G. Oliva, S. Panzieri and R. Setola, A holistic-reductionistic approach for modeling interdependencies, in *Critical Infrastructure Protection III*, C. Palmer and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 215–227, 2009.

[7] B. Ducourthial and S. Tixeuil, Self-stabilization with path algebra, *Theoretical Computer Science*, vol. 293(1), pp. 219–236, 2003.

[8] B. Ducourthial, V. Cherfaoui and T. Denoeux, Self-stabilizing distributed data fusion, in *Stabilization, Safety and Security of Distributed Systems*, A. Richa and C. Scheideler (Eds.), Springer, Berlin, Germany, pp. 148–162, 2012.

[9] C. Foglietta, A. Gasparri and S. Panzieri, A networked evidence theory framework for critical infrastructure modeling, in *Critical Infrastructure Protection VI*, J. Butts and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 205–215, 2012.

[10] V. Formicola, A. Di Pietro, A. Alsubaie, S. D' Antonio and J. Marti, Assessing the impact of cyber attacks on wireless sensor nodes that monitor interdependent physical systems, in *Critical Infrastructure Protection VIII*, J. Butts and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 213–229, 2014.

[11] A. Gasparri, F. Fiorini, M. Di Rocco and S. Panzieri, A networked transferable belief model approach for distributed data aggregation, *IEEE Transactions on Systems, Man and Cybernetics, Part B: Cybernetics*, vol. 42(2), pp. 391–405, 2012.

[12] B. Genge, C. Siaterlis and G. Karopoulos, Data fusion based anomaly detection in networked critical infrastructures, *Proceedings of the Forty-Third IEEE/IFIP International Conference on Dependable Systems and Networks; Workshop on Reliability and Security Data Analysis*, 2013.

[13] G. Oliva, S. Panzieri and R. Setola, Distributed consensus under ambiguous information, *International Journal of Systems of Systems Engineering*, vol. 4(1), pp. 55–78, 2013.

[14] M. Ouyang, Review on modeling and simulation of interdependent critical infrastructure systems, *Reliability Engineering and System Safety*, vol. 121, pp. 43–60, 2014.

[15] C. Perrow, *Normal Accidents: Living with High-Risk Technologies*, Basic Books, New York, 1984.

[16] S. Rinaldi, J. Peerenboom and T. Kelly, Identifying, understanding and analyzing critical infrastructure interdependencies, *IEEE Control Systems*, vol. 21(6), pp. 11–25, 2001.

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

[18] P. Smets, The combination of evidence in the transferable belief model, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 12(5), pp. 447–458, 1990.

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

[20] P. Sousa, A. Bessani, W. Dantas, F. Souto, M. Correia and N. Neves, Intrusion-tolerant self-healing devices for critical infrastructure protection, *Proceedings of the Thirty-Ninth IEEE/IFIP International Conference on Dependable Systems and Networks*, pp. 217–222, 2009.

[21] D. Sutton, J. Harrison, S. Bologna and V. Rosato, The contribution of Neisas to EP3R, in *Critical Information Infrastructure Security*, S. Bologna, B. Hammerli, D. Gritzalis and S. Wolthusen (Eds.), Springer-Verlag, Berlin Heidelberg, Germany, pp. 175–186, 2013.

[22] A. Townsend and M. Moss, Telecommunications Infrastructure in Disasters: Preparing Cities for Crisis Communications, Center for Catastrophe Preparedness and Response and Robert F. Wagner Graduate School of Public Service, New York University, New York (`www.nyu.edu/ccpr/pubs/NYU-DisasterCommunications1-Final.pdf`), 2005.

[23] M. van Eeten, A. Nieuwenhuijs, E. Luiijf, M. Klaver and E. Cruz, The state and the threat of cascading failure across critical infrastructures: The implications of empirical evidence from media incident reports, *Public Administration*, vol. 89(2), pp. 381–400, 2011.

[24] L. Zadeh, On the Validity of Dempster's Rule of Combination of Evidence, Memorandum UCB/ERL-M, Electronics Research Laboratory, University of California, Berkeley, Berkeley, California, 1979.