Networked Evidence Theory Framework in Critical Infrastructure Modeling

Chiara Foglietta, Andrea Gasparri, Stefano Panzieri
Dipartimento di Informatica e Automazione
Università degli Studi ROMA TRE
{panzieri, fogliett, gasparri}@dia.uniroma3.it
Basic Idea

• The Theory of Evidence is a formalism used for modeling uncertainty, e.g., ignorance, instead of classical probability.

• It allows to combine evidence from different sources and arrive at a degree of belief for a proposition on the basis of the available evidence.

• A belief can be assigned to a set describing all the plausible propositions without supporting any in particular.

• The Transferable Belief Model (TBM) introduces the idea of open world, that is data can be in contradiction.
Classical Evidence Theory approach

Frame of discernment: \( \Omega = \{ \omega_1, \omega_2, ..., \omega_n \} \) with \( |\Omega| = n \)

Power set: \( \Gamma(\Omega) = \{ \gamma_1, \gamma_2, ..., \gamma_{2^{|\Omega|}} \} \) with \( |\Gamma(\Omega)| = 2^{|\Omega|} \)

Basic Belief Assignment function: \( m = \Gamma(\Omega) \rightarrow [0; 1.0] \)

Constraints: \( \sum_{\gamma_a \subseteq \Gamma(\Omega)} m(\gamma_a) = 1 \) with \( m(\emptyset) = 0 \)

- The mass \( m(\gamma_a) \) expresses the proportion of all relevant and available evidence that supports the claim that the actual state belongs to \( \gamma_a \) but to no particular subset of \( \gamma_a \).
- The value of \( m(\gamma_a) \) pertains only to the set \( a \) and makes no additional claims about any subsets of \( \gamma_a \).
Belief

- Let us define a Belief function over $\Omega$ as a function:

$$\text{Bel}: 2^\Omega \rightarrow [0,1]$$

$$\text{Bel}(\gamma_a) = \sum_{\gamma_b \subseteq \gamma_a} m(\gamma_b)$$

- The Belief quantifies the total specific amount of belief supporting the proposition.

- The Belief is often used in the decision making process after data aggregation is performed.
Rules of combination

\[\text{Dempster}\{m_i, m_j\}(\emptyset) = 0,\]

\[\text{Dempster}\{m_i, m_j\}(\gamma_a) = \frac{\sum_{\gamma_b \cap \gamma_c = \gamma_a} m_i(\gamma_b)m_j(\gamma_c)}{1 - \sum_{\gamma_b \cap \gamma_c = \emptyset} m_i(\gamma_b)m_j(\gamma_c)}, \forall \gamma_a \in \Gamma(\Omega)\]

\[\text{Smets}\{m_i, m_j\}(\gamma_a) = m_i(\gamma_a) \otimes m_j(\gamma_a), \quad \forall \gamma_a \in \Gamma(\Omega)\]

Where

\[m(\gamma_a) = \sum_{\gamma_b \cap \gamma_c = \gamma_a} m_i(\gamma_b)m_j(\gamma_c), \quad \forall \gamma_a \in \Gamma(\Omega)\]

Degree of conflict:

\[m(\emptyset) = 1 - \sum_{\gamma_a \in \Gamma, \gamma_a \neq \emptyset} (m_i(\gamma_a) \otimes m_j(\gamma_a))\]
Multi Agent System

- A multi-agent system (MAS) is a system composed of multiple interacting intelligent agents.
- The network topology can be described through a proximity graph $G = (V; E)$.
- Suppose that not all agents can interact among them due to distance constraints or lack of communications or lack of reciprocal trust.
- Suppose also that communications are asynchronous.
Objective

• To realize a local interaction rule to perform distributed data aggregation over a network within the framework of Theory of Evidence
From a centralized scenario...
... to a Distributed Scenario

AGGREGATION

Agent 1

Agent 2

Agent 3

Agent 4

AGGREGATION

AGGREGATION

AGGREGATION
A problem with Smet’s rule of combination
Networked data fusion problem

Consider two hypothesis Ω = \{a, b\} and a networked framework with three nodes. We apply the Smets’ rule of combination at the following steps:
1. Node 1 and Node 2
2. The results and Node 3
3. The results and Node 1

RULES OF COMBINATION CANNOT BE APPLIED IN A DISTRIBUTED FRAMEWORK
Main idea

• The idea is to define an operator which allows to decompose the knowledge (state) of an agent with respect to another one in two parts:
  – **Novelty**: Novel part of the knowledge that an agent carries with respect to another agent.
  – **Common Knowledge**: Remaining part of the knowledge shared by the two agents as the result of a previous aggregation.
Networked data fusion Algorithm

Indirect graph: \( \mathcal{G} = \{V, E\} \)
with \( V = \{v_i, \ i = 1, \ldots, n_v\}, E = \{e_{ij} = (v_i, v_j)\} \)
Spanning-tree: \( \mathcal{T} = \{V, \mathcal{E}\} \) where \( \mathcal{E} \subseteq E \)

Communication between agents is asynchronous and is a gossip algorithm defined as:
- \( S \) the set of local states of each agent
- \( \mathcal{R} \) local interaction rule for every pair of agents, as \( \mathcal{R}: \mathbb{R}^q \times \mathbb{R}^q \rightarrow \mathbb{R}^q \)
- \( e \) process of edges selection at each time step

**GOSSIP ALGORITHM:**

```plaintext
while end_condition do
    Select an edge \( e_{ij} \in E(t) \) according to \( e \);
    Update the states of the selected agents applying the operator \( \mathcal{R} \):
    \( s_i(t + 1) = s_i(t) \otimes s_j(t) \)
    \( s_j(t + 1) = s_j(t) \otimes s_i(t) \)
    Let \( t = t + 1 \)
end
```
Networked data fusion Algorithm

Define now the operator $\mathcal{R}$, local interaction rule for every pair of agents, as $\mathcal{R}: \mathbb{R}^q \times \mathbb{R}^q \rightarrow \mathbb{R}^q$.

Consider two sets of BBA, defined as $m_k = \{m_k(\gamma_a): \forall \gamma_a \in \Gamma(\Omega)\}$ and $m_i = \{m_i(\gamma_a): \forall \gamma_a \in \Gamma(\Omega)\}$, so that $m_k = m_i \otimes m_j$.

The operator $\odot$ as $m_j = m_k \odot m_i \triangleq \tilde{m}_k^i$

A local interaction rule $\mathcal{R}$, denoted by $\oplus$, as

$m_i(t+1) = m_j(t+1) = m_i(t) \oplus m_j(t) = \{(\tilde{m}_i^j(t, \gamma_a) \otimes \tilde{m}_i^j(t, \gamma_a)) \otimes \bar{m}_{i,j}(t, \gamma_a),
\forall \gamma_a \in \Gamma(\Omega)\}$

Where $\tilde{m}_i^j(t, \gamma_a)$ is the innovation of agent I with respect to the agent j, calculated as

$\tilde{m}_i^j(t, \gamma_a) = m_i(t, \gamma_a) \odot \bar{m}_{i,j}(t, \gamma_a)$

And $\bar{m}_{i,j}(t, \gamma_a)$ is the common knowledge between the two agents.
Computing the innovation

\[
\tilde{m}^j_i(t, \gamma_a) = \frac{m_i(t, \gamma_a) - \sum_{\gamma_b \cap \gamma_c = \gamma_a} \tilde{m}^j_i(t, \gamma_b) \overline{m}_{i,j}(t, \gamma_c)}{\sum_{\gamma_a \subseteq \gamma_b} \overline{m}_{i,j}(t, \gamma_b)}
\]
Steady state convergence

- After the first interval of time the related leaves will send only the neutral element, after a certain amount of time the root of $T$ achieve the steady state $s$; Finally the steady state is spread over the whole net.
CASE STUDY 1/4

Five interconnected infrastructures: n= 5
Each infrastructure able to define BBA assignment, due to basic sensor information
Aim is to understand a fault cause
Frame of discernment is $\Omega = a, b, c$
- a is a possible intrusion of cyber type
- b indicates the failure of the isolated single unit
- c is natural disaster

<table>
<thead>
<tr>
<th>time</th>
<th>T=1</th>
<th>T=2</th>
<th>T=3</th>
<th>T=4</th>
<th>T=5</th>
<th>T=6</th>
<th>T=7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge</td>
<td>$e_{12}$</td>
<td>$e_{23}$</td>
<td>$e_{34}$</td>
<td>$e_{45}$</td>
<td>$e_{34}$</td>
<td>$e_{23}$</td>
<td>$e_{12}$</td>
</tr>
</tbody>
</table>
### CASE STUDY 2/4

<table>
<thead>
<tr>
<th>Set</th>
<th>Node 1</th>
<th>Node 2</th>
<th>Node 3</th>
<th>Node 4</th>
<th>Node 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\emptyset$</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>${a}$</td>
<td>0.3</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.2</td>
</tr>
<tr>
<td>${b}$</td>
<td>0.3</td>
<td>0.4</td>
<td>0.1</td>
<td>0.4</td>
<td>0.4</td>
</tr>
<tr>
<td>${c}$</td>
<td>0.0</td>
<td>0.4</td>
<td>0.5</td>
<td>0.4</td>
<td>0.1</td>
</tr>
<tr>
<td>${a, b}$</td>
<td>0.3</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>${a, c}$</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>${b, c}$</td>
<td>0.0</td>
<td>0.0</td>
<td>0.3</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>${a, b, c}$</td>
<td>0.1</td>
<td>0.2</td>
<td>0.1</td>
<td>0.2</td>
<td>0.3</td>
</tr>
</tbody>
</table>

Basic Belief Assignment for each of five nodes/agents
## CASE STUDY 3/4

<table>
<thead>
<tr>
<th>Set</th>
<th>Node 12</th>
<th>Node 123</th>
<th>Node 1234</th>
<th>Node 12345</th>
<th>C-TBM</th>
</tr>
</thead>
<tbody>
<tr>
<td>∅</td>
<td>0.36</td>
<td>0.468</td>
<td>0.5304</td>
<td>0.6334</td>
<td>0.6334</td>
</tr>
<tr>
<td>{a}</td>
<td>0.18</td>
<td>0.108</td>
<td>0.0648</td>
<td>0.0451</td>
<td>0.0451</td>
</tr>
<tr>
<td>{b}</td>
<td>0.34</td>
<td>0.346</td>
<td>0.3676</td>
<td>0.3070</td>
<td>0.3070</td>
</tr>
<tr>
<td>{c}</td>
<td>0.04</td>
<td>0.046</td>
<td>0.0308</td>
<td>0.0125</td>
<td>0.0125</td>
</tr>
<tr>
<td>{a, b}</td>
<td>0.06</td>
<td>0.024</td>
<td>0.0048</td>
<td>0.0014</td>
<td>0.0014</td>
</tr>
<tr>
<td>{a, c}</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>{b, c}</td>
<td>0.0</td>
<td>0.006</td>
<td>0.0012</td>
<td>0.0004</td>
<td>0.0004</td>
</tr>
<tr>
<td>{a, b, c}</td>
<td>0.2</td>
<td>0.002</td>
<td>0.0004</td>
<td>0.0001</td>
<td>0.0001</td>
</tr>
</tbody>
</table>

Output of centralized TBM with incremental aggregations
# CASE STUDY 4/4

<table>
<thead>
<tr>
<th>Set</th>
<th>( s_1 \oplus s_2 )</th>
<th>( s_2 \oplus s_3 )</th>
<th>( s_3 \oplus s_4 )</th>
<th>( s_4 \oplus s_5 )</th>
<th>( s_3 \oplus s_4 )</th>
<th>( s_2 \oplus s_3 )</th>
<th>( s_1 \oplus s_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \emptyset )</td>
<td>0.36</td>
<td>0.468</td>
<td>0.5304</td>
<td>0.6334</td>
<td>0.6334</td>
<td>0.6334</td>
<td>0.6334</td>
</tr>
<tr>
<td>( {a} )</td>
<td>0.18</td>
<td>0.108</td>
<td>0.0648</td>
<td>0.0451</td>
<td>0.0451</td>
<td>0.0451</td>
<td>0.0451</td>
</tr>
<tr>
<td>( {b} )</td>
<td>0.34</td>
<td>0.346</td>
<td>0.3676</td>
<td>0.3070</td>
<td>0.3070</td>
<td>0.3070</td>
<td>0.3070</td>
</tr>
<tr>
<td>( {c} )</td>
<td>0.04</td>
<td>0.046</td>
<td>0.0308</td>
<td>0.0125</td>
<td>0.0125</td>
<td>0.0125</td>
<td>0.0125</td>
</tr>
<tr>
<td>( {a, b} )</td>
<td>0.06</td>
<td>0.024</td>
<td>0.0048</td>
<td>0.0014</td>
<td>0.0014</td>
<td>0.0014</td>
<td>0.0014</td>
</tr>
<tr>
<td>( {a, c} )</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>( {b, c} )</td>
<td>0.0</td>
<td>0.006</td>
<td>0.0012</td>
<td>0.0004</td>
<td>0.0004</td>
<td>0.0004</td>
<td>0.0004</td>
</tr>
<tr>
<td>( {a, b, c} )</td>
<td>0.2</td>
<td>0.002</td>
<td>0.0004</td>
<td>0.0001</td>
<td>0.0001</td>
<td>0.0001</td>
<td>0.0001</td>
</tr>
</tbody>
</table>

Output of distributed approach
CockpitCI: Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures

• Develop and deploy **smart detection agents** to monitor the potential cyber threats according to the types of ICT based networks (SCADA, IP...) and types of devices that belong to such networks;

• **Identify, in real time, the CI functionalities impacted by the cyber attacks and assesses the degradation of CI delivered services**;

• Broadcast an alerting message through an improved **Secure Mediation Gateway** at different security levels (low and high level);

• Manage a strategy of **containment of the possible consequences** of cyber attacks at short, medium and long term.

  – **Smart RTU Reaction System**
    • to block attacks
    • to isolate infected systems
    • to deploy tactical and operational security policies.
Secure Mediation Network

Public Network

Secure Mediation Network

Dynamic PIDS

TLC adaptor

SCADA TLC
(Control Room)

ELE SCADA adaptor

SCADA ELE
(Control Room)

Field

On-line Integrated Risk Prediction

Situation Assessment
Impact Assessment
Risk Prediction
Countermeasures selection

On-line Integrated Risk Prediction

Situation Assessment
Impact Assessment
Risk Prediction
Countermeasures selection

RTU

RTU

RTU

RTU
Global Awareness is build in a distributed environment to determine cause, countermeasures, and any other useful index.
CAUSE DETECTION EXAMPLE WITH TWO SCADA ZONES

Power Grid Zone 1

- RTUs
- Router
- SCADA controller

Power Grid Zone 2

- RTUs
- Router
- SCADA controller

SCADA Zone 1

SCADA Zone 2
CAUSES MATRIX

**CAUSES**

- **NATURAL CAUSE 1**
  - **N1**

- **PHISICAL CAUSE 1**
  - **P1**

- **CYBER ATTACK 1**
  - **C1**

- **CYBER ATTACK 2**
  - **C2**

- **PHISICAL CAUSE 2**
  - **P2**

- **NATURAL CAUSE 2**
  - **N2**

**SENSORS**

- **S1**
  - SCADA 1

- **E1**
  - ELECTRIC FIELD 1

- **TLC IDS**

- **E2**
  - ELECTRIC FIELD 2

- **S2**
  - SCADA 2

- ** Implemented with **
  - a centralized Dampster Shafer
  - A distributed Dampster Shafer
Prof. Stefano Panzieri 26

TOWARDS A DISTRIBUTED SITUATION AWARENESS

Secure Mediation Network

Public Network

DISTRIBUTED GLOBAL AWARENESS

Adaptors

DISTRIBUTED GLOBAL AWARENESS

Adaptors

DISTRIBUTED GLOBAL AWARENESS

Adaptors
Thanks!
Any question?