Doctorate in Computer Science and Automation

Department of Engineering

XXIX Ph.D Cycle

Models, Security and Control of Cyber-Physical Systems

Ph.D Student Riccardo Santini

....

Supervisor Prof. Stefano Panzieri

....

Ph.D Coordinator Prof. Stefano Panzieri

....

Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. This dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and Acknowledgements. This dissertation contains fewer than 65,000 words including appendices, bibliography, footnotes, tables and equations and has fewer than 150 figures.

Riccardo Santini

May 2017

Abstract

Modern control systems integrate physical processes with communication capabilities and computational resources. In general, the integration of the aforementioned capabilities improves system efficiency and operational performance, but at the same time introduces security concerns related to the intrusion of adversaries in the system. Moreover, the increasing amount of available sensor data poses new challenges in the task of monitoring malicious attacks against the system. During the last years, these motivations have led to the study of a particular class of control systems: the Cyber-Physical Systems (CPSs). Cyber-Physical Systems combine physical processes with computational resources in an interconnected framework, but expose control systems to new vulnerabilities and threats due to the inter-dependencies and links between cyber and physical layers.

Examples of Cyber-Physical Systems include Supervisory Control And Data Acquisition (SCADA) systems, Power and Smart grids, where data fusion methodologies are useful for analyzing threats and faults. Within the cyber-physical security framework, Evidence Theory can be a powerful tool to help the control centers to make and plan decisions and/or countermeasures.

In particular, in this thesis we develop a new approach for the diagnosis of faults and threats when cyber-attacks compromise physical operations in Power Grids (cyber-physical attacks). To handle the complexity of the fusion process and to minimize the computational overhead, we also propose a new way to model Cyber-Physical Systems in Evidence Theory framework.

Moreover, through Graph Theory, risk assessment for Cyber-Physical Systems is rediscovered as an application field for Evidence Theory. We provide theoretical findings, supported by simulations results, able to manage risks arising from cyber-physical attacks.

It is worth noticing that, CPSs act in dynamically changing environments and, despite significant advances in relevant areas, several challenges still hinder the development of high-assurance, robust and reconfigurable Cyber-Physical networks. Hence, in this thesis, we also address the problem of characterizing the robustness of Cyber-Physical Systems, viewed as interconnected network systems, with respect to the interconnection structure. Specifically, we adopt the $\mathcal{H}_2$ norm, to measure the robustness of a CPS network against external disturbances. For networks arising from the composition of atomic structures, we provide a closed-form expression of the robustness, and we identify optimal composition rules. Furthermore, we also generalize the proposed model, using the class of M - matrices and their inverses. The problem of finding the optimal robust network structure has been analyzed as an optimization problem: we found several properties of the objective function and we also characterized the expression of the optimal solution.

Table of contents

List of figures

List of tables

Introduction

Modern control systems integrate physical processes with communication capabilities and computational resources. Moreover, embedded and complex systems are becoming pervasive in our daily life, where health, services, safety and security increasingly depend on the interdependencies among these systems.

During the last years, in combination and in close interaction with the unpredictable real world environment and humans, modern control systems have been considered in a more complex class, the "Cyber-Physical Systems" [1].

Cardenas, *et al.* [2] define a Cyber-Physical System (CPS) as integrating computing, communications and storage capabilities with monitoring and/or control of entities in the physical world, which is done in a dependable, safe, secure and efficient manner under real-time constraints. Poovendran [3] notes that the concept of a cyber-physical system changes the notion of a physical system to include humans, the infrastructure and the software platform in which the overall system is highly networked. Even though several definitions for Cyber-Physical Systems and for their functionalities have been given (see [4] and the references therein), we can say that a CPS acts independently, co-operatively or as "systems of systems". Some of these systems may be older legacy plants or interconnected autonomous systems, originally developed to fulfill dedicated tasks. Examples of Cyber-Physical Systems include SCADA systems, transportation networks, power generation and distribution networks, water and gas distribution networks, and advanced communication systems.

From a practical control-systems prospective, the behaviour of CPS is characterized by the nonlinear interaction between discrete (computing device) and continuous phenomena in order to produce global and desired results. Hence, several techniques are indispensable to capture and analyze both the behaviour on the low level (discrete control logic, communication, effects of distributed computing) and global effects [5]. In more general terms, due to complex interactions among systems' components, Cyber-Physical Systems combine physical processes with computational resources in an interconnected framework, but also expose control systems to new vulnerabilities and threats due to the inter-dependencies and links between cyber and physical layers.

Even though the integration of the aforementioned capabilities improves system efficiency and operational performance, at the same time introduces security concerns related to the intrusion of adversaries in the system. Moreover, the increasing amount of available sensor data, poses new challenges in the task of monitoring malicious attacks against the system.

Concerns about security of control systems are not new, as the high number of manuscripts on fault and/or attack detection, isolation and recovery testify. Cyber-Physical Systems, however, suffer from specific vulnerabilities which do not affect classical control systems, and for which appropriate detection and identification techniques need to be developed. Despite significant advances in relevant areas, several challenges still hinder the development of high-assurance and reconfigurable Cyber-Physical Systems. These include limitations in processing real-time input data, which may vary significantly in its volume, complexity and variety, together with limited sensing/actuation accuracy and computing capabilities.

In the last years, the analysis of cyber-physical vulnerabilities has received increasing attention. Starting with approaches based on geometric control theory, such as distributed estimation and false data detection or secure consensus computation, to end with data aggregation methods, a lot of work in the research field has been done to ensure a correct and reliable functionality in the face of failures and attacks for CPS [6] [7] [8] [9].

Is now clear that Cyber-physical systems cannot be designed and managed using theories and tools from only one domain and they will transform how we interact with the physical world just as the Internet transformed how we interact with one another.

In this work, several techniques will be presented in order to model the complex interactions of a CPS and to introduce new mathematical tools for robust, reconfigurable and high-assurance Cyber-Physical networks.

Contribution Within the cyber-physical security framework, Evidence Theory can be a powerful tool to help the control centers to take and planning decisions and/or countermeasures. In particular, in **Chapter 3** we develop a new approach for the diagnosis of faults and threats when cyber-attacks compromise physical operations in Power Grids (cyber-physical attacks). To handle the complexity of the fusion process and to minimize the computational overhead, we also propose a new way to model Cyber-Physical Systems in Evidence Theory framework.

Moreover, through Graph Theory, in **Chapter 4** risk assessment for Cyber-Physical Systems is re-discovered as an application field for Evidence Theory. We provide theoretical findings, supported by simulations results, able to manage risks arising from cyber-physical attacks.

With the aim to model robust and reconfigurable Cyber-Physical networks, we also investigate how the topology of a dynamical network affects its robustness against exogenous disturbances. Hence, in **Chapter 5**, we also address the problem of characterizing the robustness of Cyber-Physical Systems, viewed as interconnected network systems, with respect to the interconnection structure. Specifically, we adopt the $\mathcal{H}_2$ norm, to measure the robustness of a CPS network against external disturbances. For networks arising from the composition of atomic structures, we provide a closed-form expression of the robustness, and we identify optimal composition rules. Furthermore, we also generalize the proposed model, using the class of M - matrices and their inverses. The problem of finding the optimal robust network structure has been analyzed as an optimization problem: we found several properties of the objective function and we also characterized the expression of the optimal solution.

Chapter 1

Graph Theory

The basic concepts of Graph Theory are extraordinarily simple and can be used to express problems from many different subjects such as biological systems, robotics, power grids, telecommunications and multi-agent networks. Graphs also pervade computer science, where hundreds of interesting computational problems are couched in terms of graphs. In general, many applications in real-world systems can be treated through graphs representation. Hence, providing a formal mathematical model has been of interest since 1736 when Leonard Euler published his paper on the "Seven Bridge of Konigsberg".

In this chapter we introduce elements of graph theory, giving basic definitions and operations on graphs, with particular emphasis on the Algebraic Graph Theory [10] [11].

1.1 Basic notions

In its simplest form, a graph is a collection of vertices (nodes) that can be connected to each other by means of edges. In particular, each edge of graph joins exactly two vertices. We refer to the collection of vertices as *vertex set* and denote it by $\mathcal{V}$. In particular, when this set has n elements, we represent it as

$$\mathcal{V} = \{v_1, v_2, \cdots, v_n\} .$$

Let us consider the set of two elements subsets of $\mathcal{V}$ denoted by $\|\mathcal{V}\|^2$. Each element of this set can be represented in the form $\{v_i, v_j\}$ such that $i, j = 1, 2, \cdots, n$ with $i \neq j$. Starting from $\|\mathcal{V}\|^2$ we can formally introduce the set of edges of a graph as

$$\mathcal{E} = \Big\{ \{e_1, e_2, \cdots, e_n\} \subset \|V\|^2 \mid e_i = \{v_i, v_j\} , \quad i, j = 1, 2, \cdots, n, \quad i \neq j \Big\} .$$

At this point, using a formal notation, a graph can be defined as follows

Definition 1.1. ***(Finite Graph)*** *A finite graph $\mathcal{G}$ consists of a finite collection of vertices $\mathcal{V}$ and edges $\mathcal{E}$ for which we can write $\mathcal{G} = (\mathcal{V}, \mathcal{E})$.*

A graph $\mathcal{G}$ is said *undirected*, when the relations between each pair of vertices are symmetric, that is, nodes on edges form unordered pairs. On the contrary, when nodes on edges form ordered pairs, the graph is called *directed* (or *di-graph*). We indicate a *di-graph* with $\mathcal{D}(\mathcal{V}, \mathcal{E})$.

For each node $v_i \in \mathcal{V}$, if the edge $e_i = (v_i, v_j)$ exists, then we call v_i and v_j *adjacent* and e_i *incident* to v_i and v_j.

Another important property for the nodes in a graph, is the concept of *neighborhood*. To be more precise, we formally have

Definition 1.2. ***(Neighborhood)*** *For any graph $\mathcal{G}$ and vertex $v_i \in \mathcal{V}$, the neighborhood set $\mathcal{N}(v_i)$ of v_i is the set of all vertices adjacent to v_i. Specifically*

$$\mathcal{N}(v_i) = \{v_j \in \mathcal{V} \mid (v_i, v_j) \in \mathcal{E}\} .$$

In a *undirected* graph, if $v_j \in \mathcal{N}(v_i)$ it follows that $v_i \in \mathcal{N}(v_j)$, since the edge set consist of unordered vertex pairs.

Starting from the notion of adjacency, we can introduce the concept of *path.*

Definition 1.3. ***(Path of length k in $\mathcal{G}$)*** *A path of length k in $\mathcal{G}$, is a sequence of vertices $(v_1, \cdots, v_k)$, such that $v_i \neq v_j, \quad \forall i \neq j$.*

A graph $\mathcal{G}$ is said *connected* if, for every pair of vertices in $\mathcal{V}$, there exists a *path* that has them as its end vertices. A graph is *strongly connected* if there is a path between every pair of vertices. We will call a graph *disconnected* if there exist at least two vertices v_i and v_j, such that there is no path from v_i to v_j.

1.2 Subgraphs

Another important concept in graph theory, is the notion of sub-graph. If we consider a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ and, respectively, a subset of vertices and edges $\mathcal{V}' \subseteq \mathcal{V}$ and $\mathcal{E}' \subseteq \mathcal{E}$ we have

Definition 1.4. ***(Sub-graph of $\mathcal{G}$)*** *A graph $\mathcal{G}'$ is called sub-graph of $\mathcal{G}$ if, for $\mathcal{V}' \subseteq \mathcal{V}$ and $\mathcal{E}' \subseteq \mathcal{E}$ such that $\forall \quad e'_i = \left\{v'_i, v'_j\right\} \in \mathcal{E}'$, we have $v'_i, v'_j \in \mathcal{V}'$.*

In particular, if $\mathcal{G}'$ is constructed by taking a subset $\mathcal{V}^\star$ of vertices and all the original edges from $\mathcal{G}$, then $\mathcal{G}'$ is called *induced* sub-graph. Moreover, all the operations that can be performed on a graph (such as union, intersection, boundaries and closure) are preserved also in the case of sub-graphs.

1.3 Matrix Representation

When algebraic methods are applied to problems about graphs, Algebraic Graph Theory is a powerful tool for analyzing several properties. In particular, we can use the matrix representation of a graph to better understand the connection with Linear Algebra. In what follows some of these matrices will be introduced.

1.3.1 Degree Matrix

Consider a graph with n vertices and m edges. The degree matrix is a diagonal matrix which contains information about the degree of each vertex, that is, the number of edges attached to each vertex. In a directed graph, the term degree may refer either to in-degree (the number of incoming edges at each vertex) or out-degree (the number of outgoing edges at each vertex). For an undirected graph $\mathcal{G}$, we indicate with $d(v_i)$ the degree of a given vertex. Using the concept of *neighborhood set*, we can say that the degree $d(v_i)$ represents the cardinality of $\mathcal{N}(v_i)$ (Section 1.1). The degree matrix of $\mathcal{G}$ is a $n \times n$ diagonal matrix, containing as diagonal entries, the vertex degrees of $\mathcal{G}$, that is,

$$\Delta(\mathcal{G}) = \begin{bmatrix} d(v_1) & 0 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & d(v_n) \end{bmatrix}$$

1.3.2 Adjacency and Incidence Matrices

Consider a graph with n vertices and m edges. The *adjacency matrix* $A(\mathcal{G})$ is a symmetric $n \times n$ matrix, where each entry denotes the existence of a vertex between v_i and v_j. We can formally define the *adjacency matrix* as follows

$$A(\mathcal{G})_{ij} = \begin{cases} 1 & \text{if } v_i v_j \in \mathcal{E} \\ 0 & \text{otherwise} \end{cases}$$

Where $A(\mathcal{G})_{ij}$ denotes the i, j entry of $A(\mathcal{G})$.

For the adjacency matrix, the sum of values in row i is equal to the degree of vertex v_i, that is, $d\left(v_i\right) = \sum_{j=1}^{n} A(\mathcal{G})_{ij}$. We call a graph $\mathcal{G}$ simple, if and only if for all i, j holds

- $A(\mathcal{G})_{ij} \leq 1$;
- $A(\mathcal{G})_{ii} = 0$.

As an alternative, we can use an *incidence matrix* of a graph as its representation. The *incidence matrix* $M\left(\mathcal{G}\right)$ is a $n \times m$ matrix , where each entry counts the number of times that edge e_j is incident with vertex v_i. Under the assumption that labels have been associated with the edges in a graph whose edges have been arbitrarily oriented, we can formally define the *incidence matrix* as follows

$$M(\mathcal{G})_{ij} = \begin{cases} -1 & \text{if } v_i \text{ is the tail of } e_j \\ 1 & \text{if } v_i \text{ is the head of } e_j \\ 0 & \text{otherwise} \end{cases}$$

Where $M(\mathcal{G})_{ij}$ denotes the i, j entry of $M(\mathcal{G})$.

An important property of the *incidence matrix*, is the fact that the column sum always equal zero, since every edge has exactly one tail and one head.

1.3.3 Graph Laplacian

Another important matrix representation for $\mathcal{G}$ is the *graph Laplacian* matrix, usually indicated with $L\left(\mathcal{G}\right)$. If we consider an undirected graph, the formal definition of the *Graph Laplacian* is

$$L\left(\mathcal{G}\right) = \Delta\left(\mathcal{G}\right) - A\left(\mathcal{G}\right),$$

where $\Delta(\mathcal{G})$ and $A(\mathcal{G})$ are, respectively, the *degree* and *adjacency* matrices. It should be noted that, for all graphs, the row sum of the *graph Laplacian* is equal to zero. For a *di-graph* $\mathcal{D}$, the *graph Laplacian* can be defined as

$$L(\mathcal{D}) = M(\mathcal{D})\, M(\mathcal{D})^{\mathsf{T}},$$

where $M(\mathcal{D})$ represent the incidence matrix of the oriented graph.

An important property of the *Graph Laplacian*, is that $L(\mathcal{G})$ is a symmetric and positive semi-definite matrix.

1.4 Spectral Graph Theory

Is now clear how to represent a generic graph through matrices, in connection with Linear Algebra . All the graphs structural properties (i.e. connectivity, Section 1.1), can be then studied in relationship to *characteristic polynomial*, *eigevalues* and *eigenvectors* of matrices associated with the graph.

Consider a graph with n vertices and m edges and (as an example) the corresponding *Laplacian* matrix. As we said before, this matrix is known to be symmetric and positive semi-definite. If we compute the *eigenvalues* of $L(\mathcal{G})$ we can order them as

$$0 = \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n.$$

Looking at the second smallest *Laplacian* eigenvalue, we have the following

Theorem 1.1. ***(Algebraic Connectivity)*** *The graph $\mathcal{G}$ is connected, if and only if $\lambda_2 > 0$.*

The second smallest *Laplacian* eigenvalue λ_2, is called *algebraic connectivity* [12][13]. Another important result in the *Spectral Graph Theory*, is the so-called *Matrix-Tree Theorem.* Let L_i be the matrix obtained after removing the $i-th$ row and column of $L\left(\mathcal{G}\right)$ (principal sub-matrix of L [1]), then we have the following

Theorem 1.2. ***(Matrix-Tree Theorem)*** *Let $t\left(\mathcal{G}\right)$ be the number of spanning trees in $\mathcal{G}$. Then*

$$t\left(\mathcal{G}\right) = det\left(L_i\right),$$

where $det(L_i)$ is the determinant of the reduced *Laplacian.*

Another theorem of major importance in the study of graph eigenvalues, is the *Cauchy's Interlacing Theorem.*

Theorem 1.3. ***(Interlacing Theorem)*** *Let A be a real symmetric $n \times n$ matrix with eigenvalues $\gamma_1 \leq \gamma_2 \cdots \leq \gamma_n$ and let $\mu_1 \leq \mu_2 \leq \cdots \leq \mu_{n-1}$ be the eigenvalues of a principal sub-matrix of A. Then $\gamma_i \leq \mu_i \leq \gamma_{i+1}$, for $i = 1, 2, \cdots, n-1$.*

It should be noted that a principal sub-matrix corresponds to an induced subgraph (see Section 1.2) with one fewer vertex.

[1] A principal sub-matrix of matrix A, is obtained by deleting the $i-th$ row and column of A.

Chapter 2

Evidence Theory

Evidence Theory appears for the first time thanks to Shafer [14], who reinvented Dempster's previous work [15] and embraces the familiar idea of using a number between zero and one to indicate the degree of confidence for a particular proposition, on the basis of the available evidence. In particular, Evidence Theory represents an interesting alternative to the Bayesian framework: the main difference concerns the way in which the ignorance is handled. To be more specific, the uncertainty, in the probabilistic framework, is treated by splitting the amount of credibility among plausible events, whereas in the Evidence Theory framework a belief is assigned to the set describing all the plausible hypotheses. In [16], the Transferable Belief Model is presented. In this case, the proposed approach to Evidence Theory is axiomatic and based on the definition of a particular function, known as Basic Probability Assignment (BPA).

Thanks to its flexibility, Evidence theory is often considered when dealing with Data Fusion problems, that is combining information and data generated from heterogeneous sources/sensors to devise an estimate of the ongoing events [17].

Two are the main limitations of Evidence Theory: the computational complexity, which grows exponentially with respect the number of hypotheses, and the unacceptable behavior of certain combination rules in presence of high conflict among sources.

This chapter presents an overview on Evidence Theory, introducing the basic notions and the principal combination rules. Moreover, an extension of the classical theory to overcome the inherent limitations is described.

2.1 Basic Notions

Evidence Theory (*ET*) is a mathematical formalism for handling uncertainty by combining evidence from different sources to converge to an accepted belief [14] [15]. In particular, this framework has been derived from an extension of Bayesian inference. The basic concept in *ET*, is to reduce uncertainty in order to identify the set that contains the correct answer to a question. In what follows, we will introduce the basic concept related to this theory.

Definition 2.1. (***Frame Of Discernment***) *Let $\Omega = \{\omega_1, \ldots, \omega_n\}$, be the set of exclusive elementary hypotheses that represents a possible value of the variable ω.*

In classical Evidence Theory, the hypotheses are also assumed to be mutually exclusive, that is, the intersections among ω_i are always empty [14] [15].

Given the *frame of discernment* Ω, it is possible to define the *powerset* as follows

Definition 2.2. (***Power Set***) *Let $\Gamma(\Omega) = \{\gamma_1, \ldots, \gamma_{2^{|\Omega|}}\}$ be a set originated by the frame of discernment Ω. This set has cardinality $|\Gamma(\Omega)| = 2^{|\Omega|}$, and contains all possible subsets $\gamma_i \subseteq \Omega$ built from Ω with $\cup$ operator .*

Therefore by convention, we write $\Gamma(\Omega) = (\Omega, \cup)$. The cornerstones of the ET rely on the following assumptions:

Assumption 2.1. (***Shafer's model***) *All the hypotheses in* Ω *are assumed to be exhaustive and mutually exclusive.*

Assumption 2.2. (***Third middle excluded principle***) *There exists the complement for any elements/ proposition belonging to the power set of* Ω*.*

Shafer's model [14] relies on the so-called *Basic Probability Assignment* (BPA). The BPA function $m\,(.)$ can be defined as

Definition 2.3. (***BPA function***) *Let* $\Gamma(\Omega)$ *be the power set and* $m\,(.)$ *be a function that assigns to each element of* $\Gamma(\Omega)$*, a value in the* $[0, 1]$ *interval. Then we have*

$$m\,(.) = \Gamma(\Omega) \rightarrow [0, 1].$$

This function shall respect the following constraints:

$$\begin{aligned} m(\emptyset) &= 0 \\ m(\gamma_i) &\geq 0, \forall \gamma_i \subseteq \Gamma(\Omega) \\ \sum_{\gamma_i \subseteq \Gamma(\Omega)} m(\gamma_i) &= 1. \end{aligned}$$

Considering a BPA assignment, the elements of the *Power Set* with values greater than zero are called *focal set.* It should be noted that $m\,(.)$ is not a probability function, and it does not respect the additivity property: $m(\gamma_a \cup \gamma_b) \neq m(\gamma_a) + m(\gamma_b)$.

2.2 Combination Rules

In the case of independent information sources, a rule that aggregates the data is required. Several combination rules, with different features and different application fields, have been proposed in the literature. Among the other rules, the most widely used are Dempster's and Smets' one. In what follows, several rules will be presented just to underline the differences among the aggregations. For further analysis on the properties and the mathematical expression of the rules, we refer the reader to [18].

Dempster's Rule.

Dempster's rule of combination [15] was the first to be formalized. This rule uses a conjunctive operation, and strongly emphasizes the agreement between multiple sources. On the contrary, the conflicting evidence among the information sources, is neglected through a normalization factor. So the rule is formalized as, $\forall \gamma_a \in \Gamma(\Omega)$:

$$\begin{aligned} \text{Dempster}\{m_i, m_j\}(\emptyset) &= 0 \\ \text{Dempster}\{m_i, m_j\}(\gamma_a) &= \frac{\sum\limits_{\gamma_b \cap \gamma_c = \gamma_a} m_i(\gamma_b) m_j(\gamma_c)}{1 - \sum\limits_{\gamma_b \cap \gamma_c = \emptyset} m_i(\gamma_b) m_j(\gamma_c)}. \end{aligned} \tag{2.1}$$

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

Smet's Rule.

Smets and Kennes in [16] proposed a new rule of combination that allows to express explicitly the contradiction in the DS framework, based on the *Transferable Belief Model* (TBM), by letting $m(\emptyset) > 0$. This combination rule, compared to Dempster's one, simply avoids the normalization while preserving the commutativity and associativity properties. The formalization is as follows, $\forall \gamma_a \in \Gamma(\Omega)$:

$$\text{Smets}\{m_i, m_j\}(\gamma_a) = m_i(\gamma_a) \otimes m_j(\gamma_a) \qquad \forall \gamma_a \in \Gamma(\Omega), \tag{2.2}$$

where

$$m_i(\gamma_a) \otimes m_j(\gamma_a) = \sum_{\gamma_b \cap \gamma_c = \gamma_a} m_i(\gamma_b) m_j(\gamma_c).$$

The inequality $m(\emptyset) > 0$ can be explained in two ways. The first is the open world assumption of Dempster [15], which expresses the idea that the *frame of discernment* must contain the true value. Necessarily, if the open world assumption is true, then the set of hypotheses must contain all the possibilities. Under this interpretation, if $\emptyset$ is the complement of Ω, then mass $m(\emptyset) > 0$ represents the case where the truth is not contained in Ω. The second interpretation of $m(\emptyset) > 0$ is that there is some underlying conflict between sources. Hence, the mass $m(\emptyset)$ represents the degree of conflict. In particular, the mass $m(\emptyset)$ can be computed as:

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

Conjunctive Rule.

The conjunctive rule simply uses the intersection operator, for combining evidences from $s \geq 2$ independent sources. Starting from the *frame of discernment* Ω, we can formally define the conjunctive rule as

$$m_{\cap}(\gamma_a) = \sum_{\gamma_1 \cap \cdots \cap \gamma_s = \gamma_a} \prod_{i=1}^{s} m_i(\gamma_i) \qquad \forall \gamma_a \in \Gamma\left(\Omega\right).$$

Disjunctive Rule.

The disjunctive rule of combination [19] [20] is a commutative and associative rule proposed by Dubois and Prade in 1986. Starting from the *frame of discernment* Ω, we can formally define the disjunctive rule as

$$m_{\cup}\{m_i, m_j\}(\emptyset) = 0$$

$$m_{\cup}\{m_i, m_j\}(\gamma_a) = \sum_{\gamma_b \cup \gamma_c = \gamma_a} m_i(\gamma_b) m_j(\gamma_c) \qquad \forall(\gamma_a \neq \emptyset) \in \Gamma\left(\Omega\right).$$

This rule is usually preferred when one knows that one or some of the sources, could be mistaken but without knowing which one.

Yager's Rule.

Yager's rule of combination states that, in case of high conflict among information sources, the result is not reliable. This rule is commutative but not associative [21]. Starting from the *frame of discernment* Ω, we can formally define Yager's rule as $\forall(\gamma_a \neq \emptyset) \in \Gamma\left(\Omega\right)$

$$m_Y\{m_i, m_j\}(\emptyset) = 0$$

$$m_Y\{m_i, m_j\}(\gamma_a) = \begin{cases} \sum\limits_{\gamma_b \cap \gamma_c = \gamma_a} m_i(\gamma_b) m_j(\gamma_c) & \text{if } \gamma_a \neq \Omega \\ m_i(\Omega) m_j(\Omega) + \sum\limits_{\gamma_b \cup \gamma_c = \emptyset} m_i(\gamma_b) m_j(\gamma_c) & \text{if } \gamma_a = \Omega \end{cases}$$

where $\gamma_a = \Omega$ represents the full ignorance according to [14].

Dubois and Prade's Rule.

Dubois and Prade's rule of combination [20] is a commutative but not associative rule. The main principle on which this rule poses its foundations admits that the two sources are reliable when they are not in conflict, but one of them is right when a conflict occurs. As long as $\gamma_b \cap \gamma_c \neq \emptyset$, then the truth lies in $\gamma_b \cap \gamma_c$ otherwise the true value lies in $\gamma_b \cup \gamma_c$. We can formally define this rule as $\forall(\gamma_a \neq \emptyset) \in \Gamma(\Omega)$

$$m_{DP}\{m_i, m_j\}(\emptyset) = 0$$

$$m_{DP}\{m_i, m_j\}(\gamma_a) = \sum_{\substack{\gamma_b \cap \gamma_c = \gamma_a \\ \gamma_b \cap \gamma_c \neq \emptyset}} m_i(\gamma_b) m_j(\gamma_c) + \sum_{\substack{\gamma_b \cup \gamma_c = \gamma_a \\ \gamma_b \cap \gamma_c = \emptyset}} m_i(\gamma_b) m_j(\gamma_c).$$

Has been shown [20] that this rule is a reasonable trade-off between precision and reliability.

2.3 Evidence Theory Extension: DSmT

As previously described, Evidence Theory is an attractive framework in the Information Fusion field, because it gives a nice mathematical model for the representation of uncertainty and it includes Bayesian theory as a special case. Although very appealing, the ET presents some weaknesses and limitations. In particular, when the hypotheses are vague and imprecise, or when conflicts between sources become large, then combining evidence become quite difficult within the classical Evidence Theory framework. Hence, from the necessity to overcome the inherent limitations of ET, Dezert and Smarandache proposed in [22] [18] a new mathematical framework, called Dezert-Smarandache Theory (DSmT). This theory refuses Assumption 2.1 and Assumption 2.2 introduced in Section 2.1 of the classical ET, but maintains the concept of the BPA function. To be more precise, DSmT allows to formally combine any types of independent sources of information solving complex static or dynamic fusion problems, when conflicts between sources become large.

2.3.1 Hyper Power Set

Instead the classical power set, DSmT makes use of a particular set, called hyper-power set. Let $\Theta = \{\theta_1, \cdots, \theta_n\}$ be a finite set of n exhaustive elements, we define

Definition 2.4. (***Hyper-power set***) *Let D^Θ be a set originated of all composite subset built from Θ with $\cup$ and $\cap$ operators such that:*

1. *$\emptyset, \theta_1, \cdots, \theta_n \in D^\Theta$;*
2. *if $\theta_1, \theta_2 \in D^\Theta$, then $\theta_1 \cap \theta_2 \in D^\Theta$ and $\theta_1 \cup \theta_2 \in D^\Theta$;*
3. *No other elements belong to D^Θ, except those obtained by using* 1 *and* 2*.*

Therefore by convention, we write $D^\theta = (\Theta, \cup, \cap)$. It should be noted that the cardinality of D is majored by 2^{2^n} when $|\Theta| = n$ and, due to the intersection operator, follows Dedekind's number sequence: $1, 2, 5, 19, 167, 7580, 7828353, 56130437228687557907787$. Nowadays only cases up to $n < 7$ are tractable with current computing technology [23].

2.3.2 PCR combination rules

An alternative way for data aggregation, respect to the classical Evidence Theory, is proposed in DSmT introducing a new class of rules. The idea behind the Proportional Conflict Redistribution (PCR) rules is to transfer the total or partial conflicting masses to non empty set involved in the conflicts, proportionally with respect to the masses assigned to them by sources as follows:

- Use the conjunctive rule to compute the belief masses of sources;

- Compute the total or partial conflicting masses;
- Redistribute the total or partial conflicting masses to the non-empty masses in the conflicts, proportionally with respect to their masses assigned by the sources.

The way the conflicting mass is redistributed yields actually several versions of PCR rules. These PCR fusion rules work for any degree of conflict, for any models (Shafer's model, DSmT model) and both in Evidence Theory and DSmT frameworks for static or dynamical fusion situations. Among the others, the best version of the PCR rules is the PCR-6 which has been proposed in [18] for combining BPAs..

PCR-6 Rule.

This version of the PCR rule is quasi-associative and the obtained solutions, after the combination process, are better in terms of quality-conflict ratio [18] [24]. For $s > 2$ sources the rule has the following expression $\gamma_a \in D^\Theta \setminus \emptyset$

$$\begin{aligned}
&\mathrm{PCR}_6(\emptyset) = 0\\
&\mathrm{PCR}_6(\gamma_a) = m_{\cap}(\gamma_a) + \\
&+ \sum_{i=1}^{s} m_i\left(\gamma_a\right)^2 \sum_{\substack{\cup_{k=1}^{s-1} Y_{\sigma_i(k)} \cup \gamma_a \equiv \emptyset \\ (Y_{\sigma_i(1)}, \cdots, Y_{\sigma_i(s-1)}) \in \left(D^\theta\right)^{s-1}}} \left(\frac{\prod_{j=1}^{s-1} m_{\sigma_i(j)}\left(Y_{\sigma_i(j)}\right)}{m_i(\gamma_a) + \sum_{j=1}^{s-1} m_{\sigma_i(j)}\left(Y_{\sigma_i(j)}\right)} \right).
\end{aligned} \tag{2.3}$$

In the special case of $s = 2$ we obtain $\forall \gamma_a \in D^\Theta \setminus \emptyset$

$$\begin{aligned}
&\mathrm{PCR}_6(\emptyset) = 0 \\
&\mathrm{PCR}_6\{m_i, m_j\}(\gamma_a) = m_\cap\{m_i, m_j\}(\gamma_a) + \\
&+ \sum_{\substack{\gamma_b \in D^\Theta \setminus \gamma_a, \\ \gamma_a \cap \gamma_b = \emptyset}} \left[\frac{m_i^2(\gamma_a) m_j(\gamma_b)}{m_i(\gamma_a) + m_j(\gamma_b)} + \frac{m_j^2(\gamma_a) m_i(\gamma_b)}{m_j(\gamma_a) + m_i(\gamma_b)} \right].
\end{aligned}$$

Chapter 3

Evidence Theory for Cyber-Physical Systems

The cyber and the physical worlds are no more distinct domains and, nowadays, the need for proper methodologies and technologies able to deal with both fields is urgently needed. In particular, telecommunications networks have exposed physical systems to new vulnerabilities and threats due to interdependencies and links between the cyber and physical layers: Cyber-Physical Systems are the class of control systems that include these weaknesses. Examples of cyber-physical systems include Supervisory Control And Data Acquisition (SCADA) systems that monitor and control electric power grids, oil and gas pipelines, water supply networks and waste-water treatment systems [25]. Research activities related to these systems usually focus on reliability and resilience.

Also Smart and Power grids have been recently introduced under the concept of cyber-physical systems. In particular, in [26], the authors studied the effects of synchronized cyber attacks on the IEEE 9 bus-bar test system.

In the context of detection and characterization of Cyber-Physical attacks, in [27] [28] [29], the authors proposed strong mathematical models based on fault detection techniques and graph theory for power networks.

Krishna and Koren [30] have proposed an adaptive control methodology for cyber-physical systems to handle failures of cyber and physical components. Cardenas, *et al.* [2] have studied integrity, confidentiality and denial-of-service attacks on cyber-physical systems.

Within the cyber-physical security framework, data fusion methodologies such as Evidence Theory are useful for analyzing threats and faults.

Evidence theory has been applied in multi-sensor fusion problems such as diagnosis [31]. Fan and Zuo [32], improving Dempster-Shafer framework by means of fuzzy membership functions, applied multi-source Evidence Theory and decision-making algorithms for fault diagnosis. Siaterlis and Genge [33] have proposed an evidence theory framework for anomaly detection. The authors apply Evidence Theory and provide a simple guideline to define Basic Probability Assignments, without considering possible weaknesses due to the chosen rule and due to the assumptions for the frame of discernment.

Unfortunately, the simple analysis of threats and faults can lead to contradictory situations that cannot be resolved by classical models. Classical evidence theory extensions, such as the Dezert-Smarandache framework [22], are not well suited to large numbers of hypotheses due to their computational overhead. Therefore, a new approach is required to handle the complexity while minimizing the computational load.

Contribution In what follows, starting from the classical theory proposed by Dempster and Shafer, we first propose a diagnostic metric for cyber-physical anomalies in Smart Grids, and we then develop a hybrid knowledge model to handle the limitation of the Evidence Theory methodology. A hybrid frame of discernment is presented using a notional smart grid architecture that transforms the basic probability assignment values from the classical framework. In particular, by noticing that an intersection among the hypotheses exists, we will show how to use the new approach to handle model complexity while reducing the computational overhead. Several analyses and simulations are conducted, with the goal of properly identifying the causes of faults and threats when a cyber attack compromises power grid operations, in order to decrease conflict values between two independent sources during the fusion process. A comparative analysis is performed using different frames of discernment and rules in order to identify the best knowledge model. Additionally, a computational time analysis is conducted

3.1 Architecture for Smart Grid Diagnostic

A smart grid is an excellent example of a cyber-physical system – it comprises the physical electrical grid and an integrated telecommunications network that monitors and controls the energy flow. Figure 3.1 shows a simplified cyber-physical representation of a smart grid. Note that the Energy Management System (EMS) /Dealer Management System (DMS) control system uses a telecommunications network to send and receive information from substations in the power grid.

Two assumptions are made about the smart grid architecture. The first assumption concerns the information exchanged by the equipment:

Assumption 3.1. ***(Packet Types)*** *Under normal conditions, the cyber information can be represented by the timing and volume of four packet types (Command, Ack-Receive, Reply and Ack-Response).*

The second assumption concerns the sensors used for smart grid management:

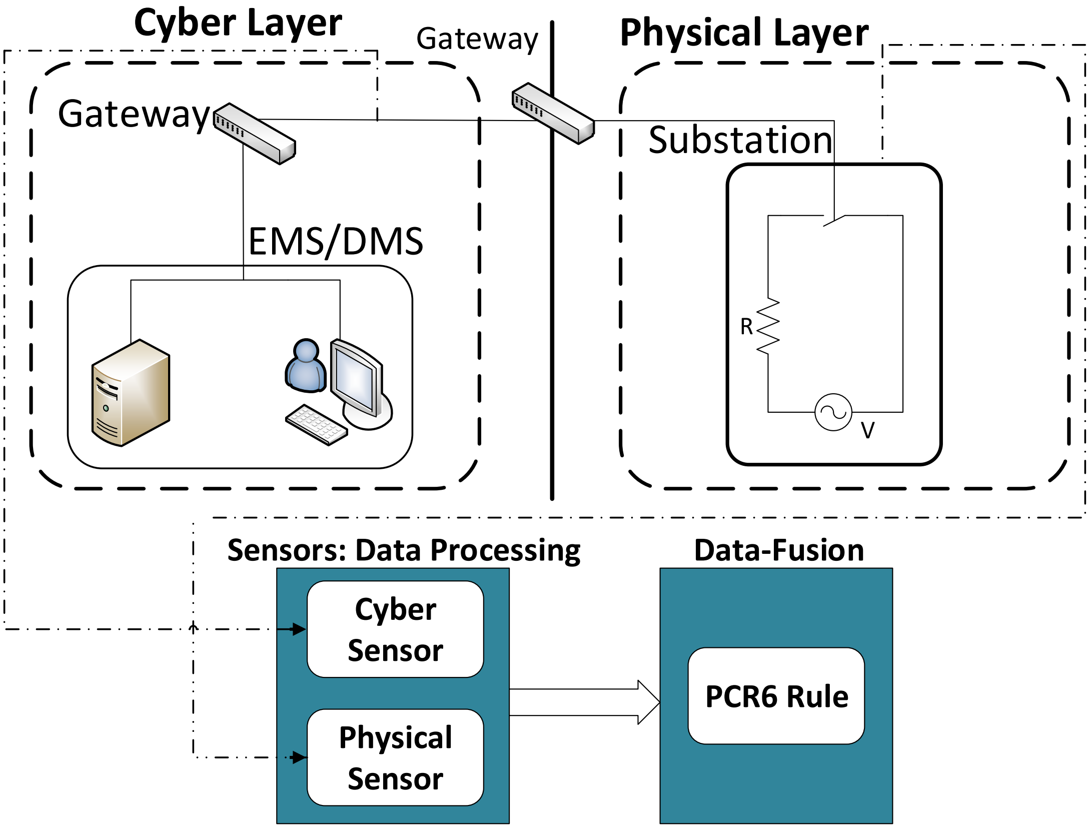


Figure 3.1 The proposed architecture for a power grid

Assumption 3.2. ***(Sensor Types)*** *A packet-sniffing sensor is used in the cyber layer to detect the number of packets in the network and a physical layer sensor is used to indicate whether a piece of equipment (e.g., circuit breaker) is working or not.*

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

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

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

- **Situation 2 (28 to 35 seconds):** The cyber sensor detects an increasing number of packets in the network (due to the attacker's intrusion), but the circuit breaker is still working.

- **Situation 3 (36 to 95 seconds):** The cyber sensor and the physical sensor both detect anomalous behavior. The packet-sniffing sensor detects a high number of packets and the circuit breaker does not respond to commands.

- **Situation 4 (96 to 100 seconds):** The smart grid is back to normal after the cyber-physical attack because the countermeasures were successful.

Table 3.1 Events happening during the simulation and the arising alarms.

Time (Sec)	**Events**	**Detecting Sensor**
0 - 27	Normal State	-
28 - 35	Cyber Anomaly	Cyber Sensor
36 - 95	Cyber Anomaly + Physical Fault	Cyber + Physical Sensor
96 - 100	Normal State	-

Table 1 summarizes the simulation events, with a focus on the time and information sources. The goal is to fuse all the data provided by the sensors during a simulation in order to detect a cyber-physical attack.

3.1.1 Frame of Discernment and BPA assignment

In order to fuse all the data provided by the sensors, we modeled the frame of discernment Ω, according to the classical evidence theory as:

$$\Omega = \{C, P, N\} \tag{3.1}$$

As shown in Figure 3.2, in the classical evidence theory framework, the hypotheses are mutually exclusive with empty intersections.

Starting with Ω, the power set is:

$$\Gamma(\Omega) = \{\emptyset, C, P, N, C \cup P, C \cup N, P \cup N, C \cup P \cup N\} \tag{3.2}$$

Each sensor has to distribute a unitary mass over specific focal sets during a simulation. Using a combination rule, a fusion result can then be obtained. Specifically, the focal sets for the cyber sensor are $\{C, N, P \cup N, \Omega\}$. Note that a cyber security

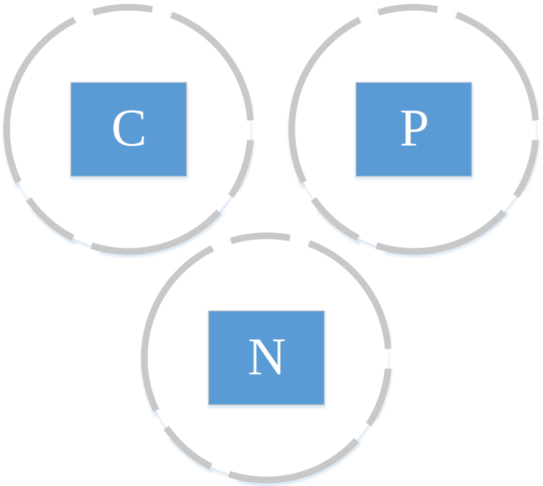


Figure 3.2 Representation of the frame of discernment

expert could identify a cyber anomaly, but is unlikely to discern a physical anomaly. Similarly, the focal sets for the physical sensor are $\{P, N, C \cup N, \Omega\}$. A cyber-physical fault is detected in the presence of mutually exclusive hypotheses by noticing the existence of non-zero similar masses in the cyber cause set and the physical cause set. Such problems are primarily related to the BPA assignments for the sources, which are application dependent. Furthermore, in literature the best way to assign BPA (Basic Probability Assignment) from each sensor does not exist, and usually the assignment procedure is a non-trivial question and it needs several trials. In our case study, we notice that the sources need to assign to each focal set values proportional to specific conditions:

- For the cyber sensor the BPA values must be proportional to the number of packets observed during the simulation: very low in normal condition and quickly increase up to one during the cyber-physical attack;

- For the physical sensor the BPA values must be proportional to the boolean data belonging to the states of the circuit breaker: very low in normal condition and quickly increase up to one for the persistence of the fault during the cyber-physical attack.

Following the previous considerations, we performed several trials on our simulated environment in order to obtain the best BPA assignment for our application. In particular, different mathematical functions have been tested and the following exponential function represents our choice for modeling the system behavior:

$$e^{\dfrac{-a \cdot p}{x}}, \tag{3.3}$$

where a and p are positive tuning parameters and x represents the number of captured packets to set the mass of $\{C\}$, or the persistence of the fault to express the mass of $\{P\}$ (see Figure 3.3).

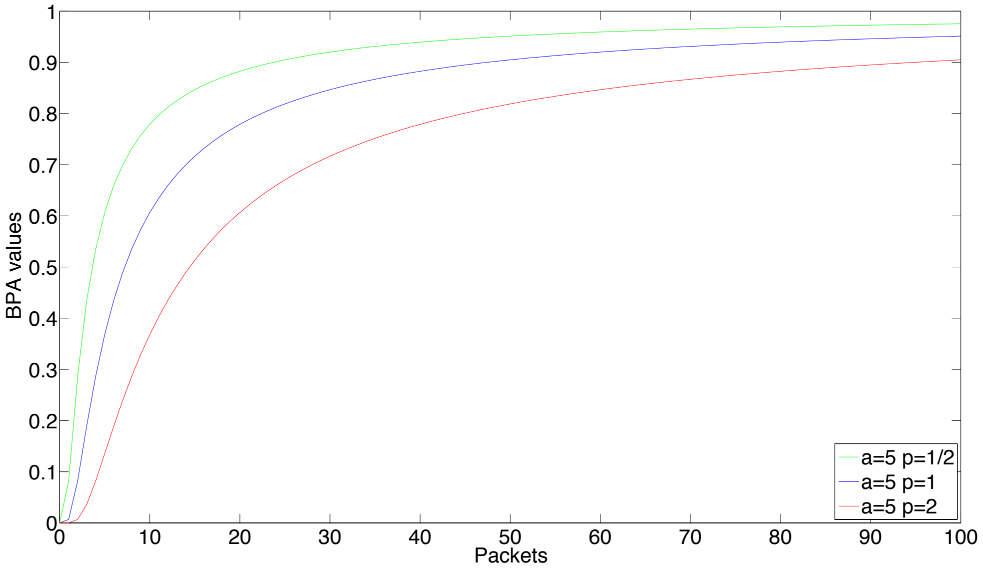


Figure 3.3 Tuning the BPA assignment from packet sniffing sensor, respect to a and p parameters.

3.2 Classic Power Set: Simulations and Results

In this section we report the simulations and results obtained with the power set defined in Equation 3.2. Tables 3.2 and 3.3 summarize the experimental values for the BPA assignment used in the simulations.

Table 3.2 BPA assignment for the Cyber sensor. BPA function parameters: $a = 5$ and $p = 2$.

	Percentage	**Packet number**
$\mathbf{m}(C)$	$m(\alpha)$	$e^{\frac{-a \cdot p}{x}}$
$\mathbf{m}(N)$	$55\%(1 - m(\alpha))$	$0.55 \cdot (1 - e^{\frac{-a \cdot p}{x}})$
$\mathbf{m}(P \cup N)$	$31.5\%(1 - m(\alpha))$	$0.315 \cdot (1 - e^{\frac{-a \cdot p}{x}})$
$\mathbf{m}(\Omega)$	$13.5\%(1 - m(\alpha))$	$0.135 \cdot (1 - e^{\frac{-a \cdot p}{x}})$

Table 3.3 BPA assignment for the Physical sensor. BPA function parameter $a = 5$ and $p = 2$.

	Percentage	**Fault**	**No Fault**
$\mathbf{m}(P)$	$m(\beta)$	$e^{\frac{-a \cdot p}{t}}$	0.1
$\mathbf{m}(N)$	$55\%(1 - m(\beta))$	$0.55 \cdot (1 - e^{\frac{-a \cdot p}{t}})$	0.495
$\mathbf{m}(C \cup N)$	31.5%(1-m(β))	$0.315 \cdot (1 - e^{\frac{-a \cdot p}{t}})$	0.2835
$\mathbf{m}(\Omega)$	13.5%(1-m(β))	$0.135 \cdot (1 - e^{\frac{-a \cdot p}{t}})$	0.1215

During the simulations, at each time step, we evaluated the conflict between the sources and the result is reported in Figure 3.4.

As we can see from Figure 3.4, the conflict value is very high and, to redistribute the conflict among the elements of the power set, we decide to test as fusion rule Dempster's rule of combination (see Equation 2.1). The results of the fusion process are reported in Figure 3.5

When two information sources that have high conflict exist in the cyber and physical realms, the rough values obtained after fusion using Dempster's rule are unsuitable: as we can see in Figure 3.5, the value associated to the cyber-physical anomaly became too small for the anomaly detection.

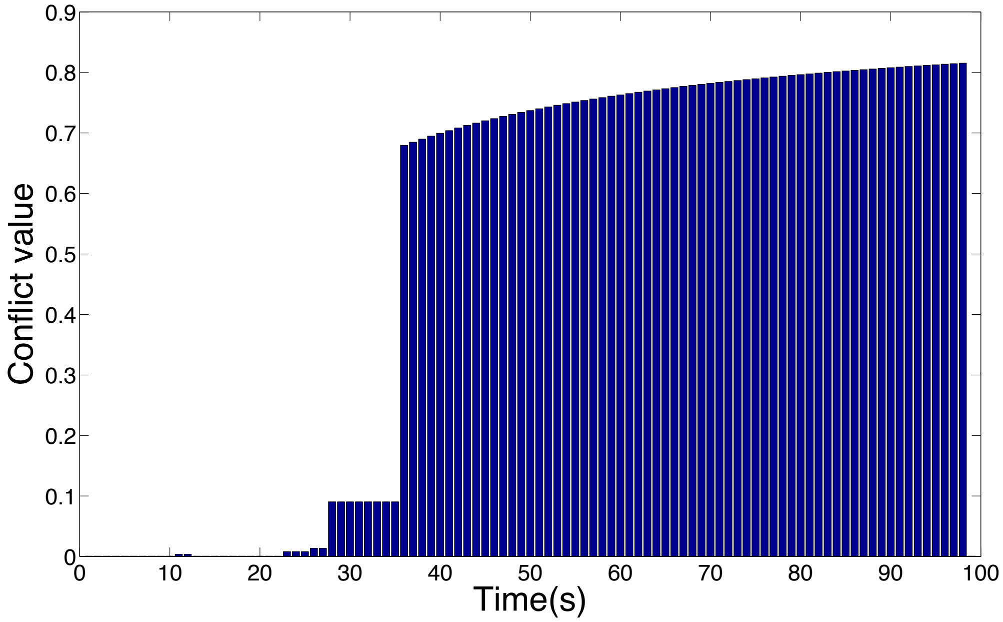


Figure 3.4 Conflict value between sources.

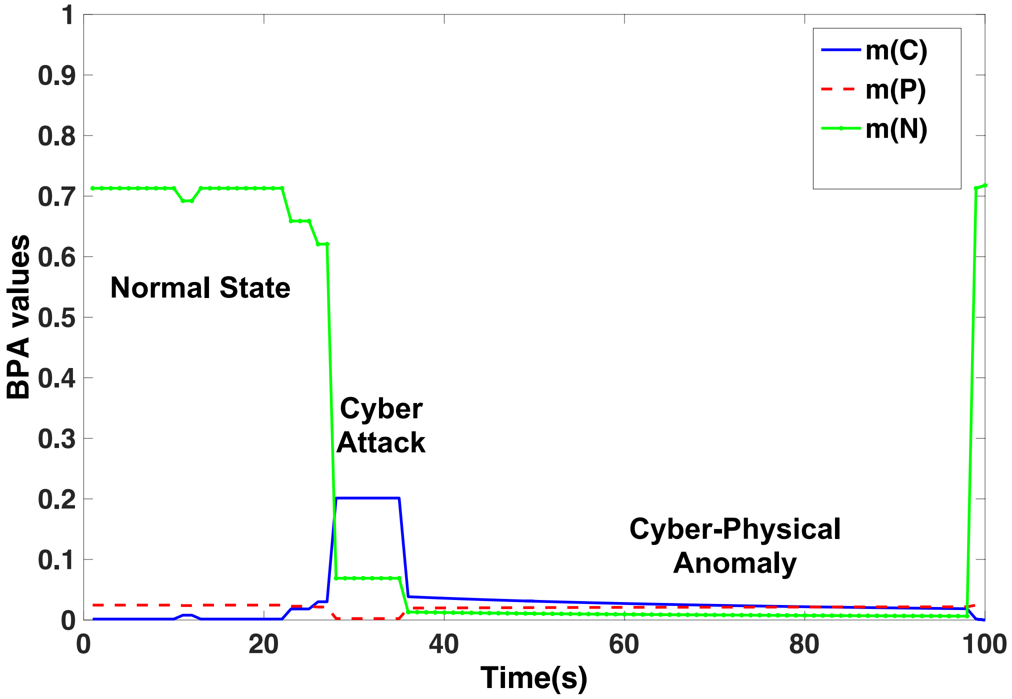


Figure 3.5 Fusion Results with Dempster's rule.

To overcome this issue, we decided to test as fusion rule the PCR-6 rule of combination, introduced in DSmT for solving fusion problems when conflicts between sources become large (see Section 2.3). In particular, this rule, is able to redistribute the conflict between the pair of elements involved in the conflict itself (Equation 2.3). The results of the fusion process are reported in Figure 3.6.

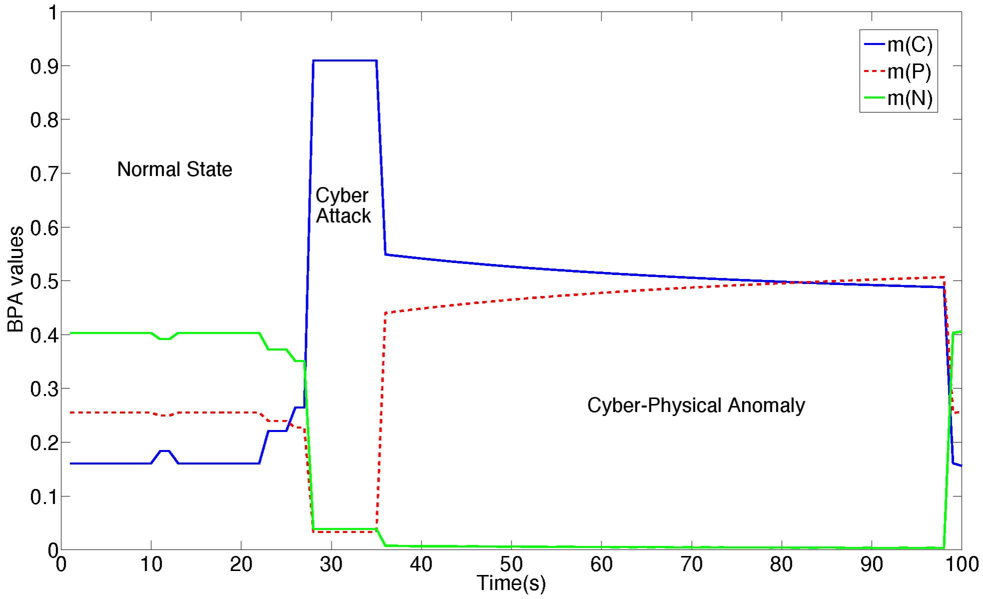


Figure 3.6 Results using PCR-6 rule for the singletons

As shown in Figure 3.6, the results are quite interesting. During the simulation, $m(\{C\})$ and $m(\{P\})$ converge to the same value even though they belong to two exclusive sets as the classical evidence theory assumes. The possible interpretation is that the assumption of exclusivity of the hypotheses is not valid. So an intersection among the hypothesis exists and it is different from $\emptyset$: the cause could be both cyber and physical; in particular the physical damage could be a consequence of the cyber attack.

Upon analyzing the results, we propose a cyber-physical diagnostic metric based on the PCR-6 rule. To be more specific, using Smet's rule (Equation 2.2) to evaluate the conflict value of the mass distribution over Ω, and compare it with the sum of the two masses in $\{C\}$ and $\{P\}$ obtained with PCR-6, a cyber-physical alarm triggering equation is given by:

$$\begin{cases} \max\{m_{\mathrm{PCR-6}}(\gamma_a)\}\,\forall\gamma_a \in \Omega, & \text{if } m_{\mathrm{Smets}}(\{\emptyset\}) \leq \rho \\ m_{\mathrm{PCR-6}}(\{C\}) + m_{\mathrm{PCR-6}}(\{P\}) \geq m_{\mathrm{Smets}}(\{\emptyset\}), & \text{if } m_{\mathrm{Smets}}(\{\emptyset\}) \geq \rho \end{cases} \tag{3.4}$$

where $\rho = 0.7$ is a pre-defined threshold for an admissible conflict value.

Using Equation 3.4, it is possible to transmit to the control center the current state of the system, underlying the occurrence of the cyber-physical attack.

As we said before, analyzing the results it is possible to confirm that an intersection exists among the sets in the frame of discernment. Smarandache and Dezert [18] have proposed an extended version of evidence theory (Section 2.3). The extended theory eliminates the constraint on the exclusivity of hypotheses and explicitly considers intersections among the elements of the power set. Although the theory appears to be useful in our case study, the main problem is the intersection operator. In fact, after defining the frame of discernment Ω, it is necessary to define a special power set called the hyper power set D^{Ω}. The cardinality of D^{Ω} is usually very high due to the intersection operator, and only cases up to $n < 7$ are tractable with current computing technology (see Section 2.3.1). In the following sections, we show how to solve this problem by using a hybrid knowledge model based on classical evidence theory and Dezert-Smarandache theory.

3.3 Exploring the Frame of Discernment

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

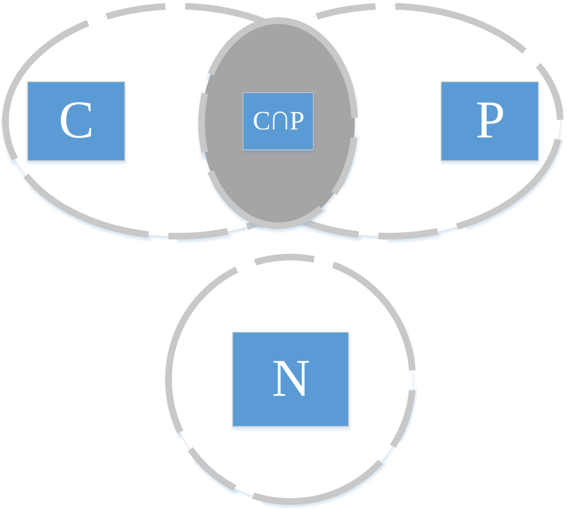


Figure 3.7 Representation of the new frame of discernment

The new frame of discernment, which is shown in Figure 3.7, is given by:

$$\Omega' = \{C', P', N, C \cap P\} \tag{3.5}$$

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

The new power set is given by:

$$\begin{aligned}\Gamma(\Omega') = \{&\emptyset, C', P', N, C \cap P, C' \cup P',\\ &C' \cup N, C' \cup (C \cap P), P' \cup N, P' \cup (C \cap P),\\ &N \cup (C \cap P), C' \cup P' \cup N, C' \cup P' \cup (C \cap P),\\ &C' \cup N \cup (C \cap P), P' \cup N \cup (C \cap P), \Omega'\}\end{aligned} \tag{3.6}$$

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

Table 3.4 BPA assignment for the Cyber sensor considering the new frame, where $a = 5$ and $p = 2$.

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

Table 3.5 BPA assignment for the Physical sensor considering the new frame, where $a = 5$ and $p = 2$.

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

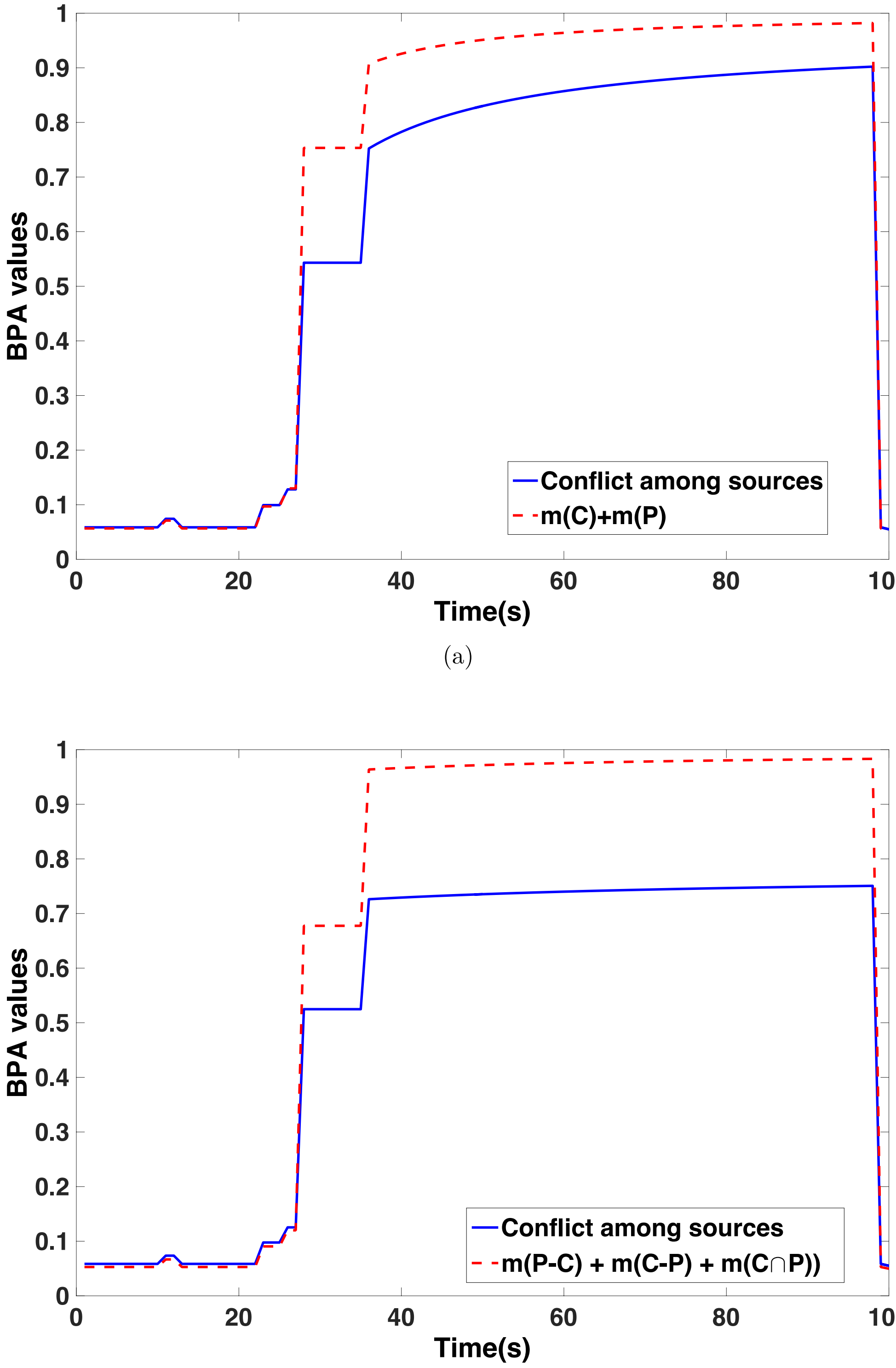
Considering the results obtained in the case study above and the results obtained using the approach presented in Section 3.2, we selected the function defined in Equation 3.3 for the BPA assignment. The BPA values for the cyber sensor and physical sensor are summarized in Tables 3.4 and 3.5, respectively. Note that the only difference is related to the BPA assignment of the focal sets:

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

As discussed above, the BPA assignment is still an open question in the context of evidence theory. Indeed, there is no consensus on how to assign the BPA values. Thus, the BPA functions are selected based on the application. Note that the values reported in Tables 3.4 and 3.5 were obtained after exhaustive tests on the system.

3.4 Hybrid Power Set: Simulations and Results

The hybrid power set was tested by fusing the information using the Dempster and PCR-6 rules. Figure 3.8a and Figure 3.8b show comparisons of the evaluations of the conflict between the information sources. Note that the conflict value in Ω' is smaller than Ω and is reduced by approximately 11% during the simulation compared with the original case.



(a)

(b)

Figure 3.8 Figure 3.8-a) Conflict and sum of $m(C)$ and $m(P)$ in Ω.Figure 3.8-b) Conflict and sum of $m(P-C)$, $m(C-P)$ and the intersection $m(C \cap P)$ in Ω'.

When Dempster's rule is used, the values are low and demonstrate contradictory behavior. Note that the set $P - C$is set P' in Ω' and $C - P$ is C' in Ω'.

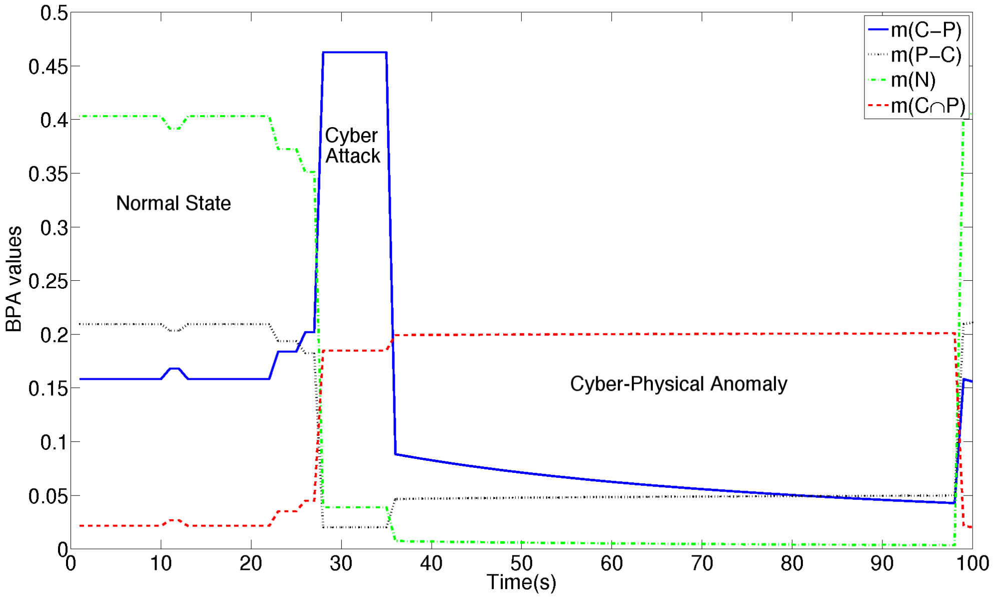


Figure 3.9 Results using Dempster's rule for the new frame of discernment Ω'. The set $P - C$ is set P' in Ω' and $C - P$ is C' in Ω'

As shown in Figure 3.9, during the cyber-physical anomaly, the values of $m(C)$ and $m(P)$ are approximately the same ($\simeq 0.05$). Note that $m(C \cap P)$ has a higher value ($\simeq 0.2$), but this is not relevant because the conflict value is high. Figure 3.10 shows the values of the singletons after fusion using the PCR-6 rule. Note that the set $P - C$ is set P' in Ω' and $C - P$ is C' in Ω'. In this case, the dashed line (i.e., $m(C \cap P)$) is greater than the others during the cyber-physical anomaly. Upon examining Figure 3.9, it is seen that the values of $m(C \cap P)$ are comparable with $m(C)$ or $m(P)$ using Ω instead of Ω' as the frame of discernment.

Therefore, with the hybrid power set, it is possible to manage the intersection between hypotheses to obtain good results. Using the new frame of discernment and the PCR-6 rule, an operator is able to recognize, with the help of the fusion algorithm, a cyber-physical anomaly represented by $C \cap P$. With the hybrid frame of discernment,

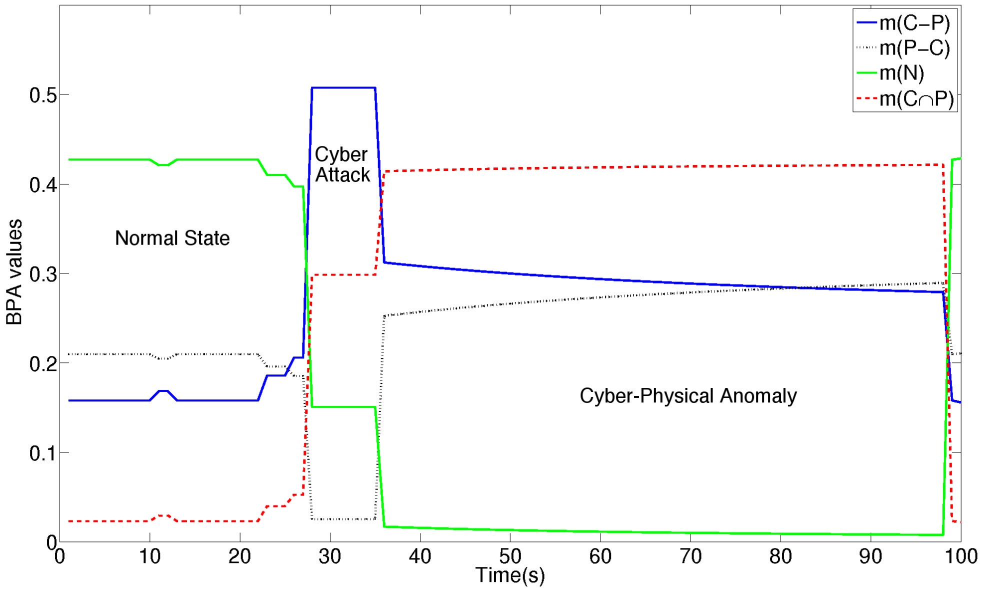


Figure 3.10 Results using PCR-6 rule for the frame of discernment Ω'. The set $P - C$ is set P' in Ω' and $C - P$ is C' in Ω'

the results can be analyzed using a classical metric (i.e. the highest BPA value). Note that throughout the simulation there is one element of the power set with the highest value. As such, an operator does not need any other metrics to trigger a particular event (i.e., cyber-physical anomaly, see Equation 3.4).

For the other elements of the power set $\Gamma(\Omega')$, the sets represented in Figure 3.11 are the only ones with non-zero masses. The values $m(C' \cup N \cup (C \cap P))$ (triangle-marked line) and $m(P' \cup N \cup (C \cap P))$ (dotted line) are the same.

Table 3.6 Comparing the computational time of simulations for the two power sets $\Gamma(\Omega)$ and $\Gamma(\Omega')$

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

Table 3.6 shows the computational times of the fusion script for the two frames of discernment Ω and Ω'. The script, which was written in Matlab [34] tested on a

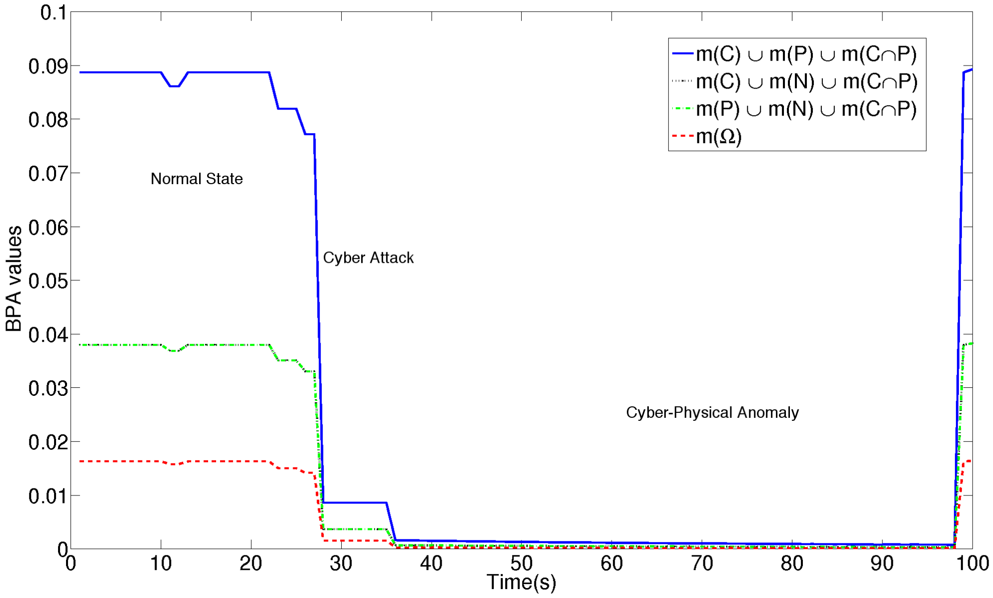


Figure 3.11 Results using PCR-6 rule for the remaining meaningful elements of the frame of discernment Ω'

laptop with a 2.6 GHz quad-core Intel Core i7 processor and 8 GB RAM. The script was executed 100 times. Table 3.6 reports the means the variances. The frame of discernment with fewer elements (i.e., Ω) requires less time on the average than Ω', but it the time required has greater variance. Note that the performances would improve if a non-interpreted programming language such as Java or C++ were to be used. Nevertheless, the results are encouraging with regard to the application of evidence theory in real-time environments.

Chapter 4

Graph-Based Evidence Theory for Assessing Risk

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

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

In this chapter, risk assessment of interconnected systems is re-discovered as an application field for Evidence Theory. Evidence Theory (ET) is a mathematical formalism born in the context of Data Fusion, in order to merge data and information coming from several and heterogeneous sensors. This theory has been already applied in electric grid for diagnostic problems. In [33], an architecture on how to apply Evidence Theory in Smart Grids has been proposed with the aim to identify the real causes of faults. In Chapter 3 we showed how to use ET and relative extensions during the so-called “Cyber-Physical threats”, i.e. cyber threats aiming to disrupt the proper operations of physical equipment.

In the general circumstances, Evidence Theory is used to deal with epistemic uncertainty due to a lack of knowledge of quantities, system process or environment. Epistemic uncertainty, also known as systematic uncertainty, is a source of a non-deterministic behavior deriving from the lack of knowledge (incomplete information or incomplete knowledge) of some characteristics of the system or the environment. Examples of sources of epistemic uncertainty are: little or no experimental data for a fixed (but unknown) physical parameter, a range of possible values of a physical quantity provided by expert opinion, limited understanding of complex physical processes, and the existence of fault sequences or environmental conditions not identified for inclusion in the analysis of a system. Epistemic uncertainty often becomes an issue when expert opinion is required to solve a problem.

Usually epistemic uncertainty is not considered apart from the aleatory one [35] and, therefore, uniform probability distribution is used to represent both. The main drawback is the possibility to underestimate uncertainty in system responses, see [36].

The classical probability approach is not enough when someone needs to merge heterogeneous information as physical and cyber data, because epistemic uncertainty arises. Hence, different mathematical frameworks can be used, such as Fuzzy Sets, Possibility Theory or Evidence Theory. In [37] and [38], the definition of epistemic and aleatory uncertainty within the context of risk analysis is discussed.

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

In [39], the authors used the Dempster-Shafer framework for evaluating risk due to network security. They proposed a long process based on an improved Dempster's rule of combination in order to combine the masses of network security risk factors. Finally, the belief value of network security risk is obtained. The security properties of the network are divided into communication and operation, access control and asset.

Usually, Evidence Theory is applied in risk assessment tied with other methodologies. The work of Miao and Liu, [40], presents a risk assessment model combining grey relational analysis and Dempster-Shafer theory. The grey relational grades for each risk rating were used to determine the basic probability assignment functions in Dempster-Shafer theory.

A new combination rule is proposed by Liu, Chen, Gao and Jiang in [41]. This combination rule is called Risk Integrated Basic Strength Assignment and is generated from the Dempster one in order to allow experts to evaluate risk event completely on their own professional experiences and knowledge independently.

When only weak information is available, Demotier, Schon and Denœux presented a framework based on Evidence Theory for risk assessment [42]. An approach to handle such problems is proposed, based on the belief functions of Dempster-Shafer. Belief functions are used to describe expert knowledge of treatment process efficiency, failure rates, and latency times, as well as statistical data regarding input water quality. Evidential reasoning provides mechanisms to combine this information and assess the plausibility of various non-compliance scenarios. The work of Demotier, Schon and Denœux exploits the knowledge on the water treatment plant in order to define mass functions, in a situation where epistemic uncertainty is obvious.

Yi and Xie, [43], assess the vulnerability analysis of natural hazard in a given geographic area. Dempster-Shafer theory is used as the mathematical foundation of the vulnerability analysis. Based on the frame of discernment of vulnerability variables and criteria of human perception, the mass functions of evidence theory are designed.

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

It should be noted that, in all the methods reported in literature, the straightforward application of Evidence Theory to risk assessment is not possible due to the existence of some elements of the power set that, structurally, contain a clear contradiction (e.g. a risk value that is both low and high at the same time).

Contribution In this chapter, the main structure of the Evidence Theory is still valid. The novelty is to combine the Dempster-Shafer framework with graph theory and Cyber-Physical Systems, with a view to define a proper power set in order to avoid all the cases where the power set elements are in a clear contradiction, such as sets where both low and high risk values are considered. In particular, we propose a graph representation of the frame of discernment able to generate a smaller power set (called Reduced Power Set) that is minimum with respect to the case study, i.e. analysis of risk. Using the Reduced Power Set has the same accuracy of the power set if the constraint on the frame of discernment is respected. This property will be demonstrated asserting that the Reduced Power Set is closed under the intersection operator, and therefore it can be applied with each combination rule based on the intersection operator, such as Dempster's, Smets or PCR-6 rule. Some experimental results are also explained in order to understand the benefit of a smaller power set in terms of computational time, and a Cyber-Physical System (a notional power grid architecture) is taken as case study.

4.1 Analysis on Frame of Discernment: the Reduced Power Set

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

$$\Omega = \{A, B, C, D, E\} \tag{4.1}$$

The values in (Equation 4.1) constitute a risk scale from low (A) to high (E), represented as a discrete set of five elements. Starting from Ω, as the Evidence Theory assumes, the definition of the power set $\Gamma(\Omega)$ is the following one:

$$\begin{aligned}\Gamma(\Omega) = \{&\emptyset, A, B, A \cup B, C, A \cup C, B \cup C, A \cup B \cup C,\\ &D, A \cup D, B \cup D, A \cup B \cup D, C \cup D, A \cup C \cup D,\\ &B \cup C \cup D, A \cup B \cup C \cup D, E, A \cup E, B \cup E,\\ &A \cup B \cup E, C \cup E, A \cup C \cup E, B \cup C \cup E,\\ &A \cup B \cup C \cup E, D \cup E, A \cup D \cup E, B \cup D \cup E,\\ &A \cup B \cup D \cup E, C \cup D \cup E, A \cup C \cup D \cup E,\\ &B \cup C \cup D \cup E, A \cup B \cup C \cup D \cup E\}\end{aligned} \tag{4.2}$$

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

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

In risk assessment, Ω can be represented as an undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \{\omega_1, \ldots, \omega_n\}$ is the set of vertices (representing singletons of Ω) and $\mathcal{E} = \{e_{ij} = (\omega_i, \omega_{i+1}), i = 1, \ldots, n-1\}$ is the set of edges connecting vertices, as depicted in Figure 4.1. Therefore, the only reasonable subsets of the power set are the ones where the elements respect the following definition.

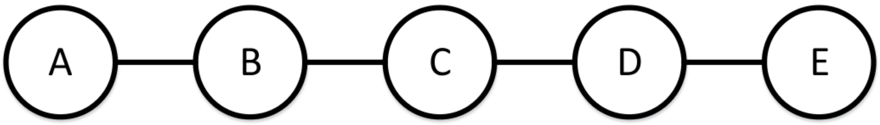


Figure 4.1 A graph representation of the considered frame of discernment.

Definition 4.1. ***(Induced Sub-graph of*** Γ***)*** *Each element of the power set* $\gamma_i \in \Gamma(\Omega)$ *defines a sub-graph* $\mathcal{G}'$ *of* $\mathcal{G}$ *induced by* $\mathcal{V}' = \gamma_i$*. The induced sub-graph* $\mathcal{G}' = (\mathcal{V}', \mathcal{E}')$ *contains all the edges of* $\mathcal{G}$ *that connect elements of the given subset of the vertex set* $\mathcal{V}'$ *of* $\mathcal{G}$*, and only those edges. Formally,*

$$\mathcal{V}' = \gamma_i \subseteq \mathcal{V} \tag{4.3}$$

$$\forall \omega_j, \omega_k \in \mathcal{V}', e = (\omega_j, \omega_k) \in \mathcal{E} \qquad \Rightarrow \qquad e \in \mathcal{E}' \tag{4.4}$$

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

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

Let us provide a brief example, in which the previous definition (4.1) is applied. Let $\gamma_i = \{B \cup C \cup D\}$ as a candidate of the focal set. The induced sub-graph $\mathcal{G}' = (\mathcal{V}', \mathcal{E}')$ is made of $V' = \{B, C, D\}$ and $E' = \{(B, C), (C, D)\}$. For each couple of elements we need to find a path among them over $\mathcal{G}'$:

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

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

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

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

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

Following 4.1, the Reduced Power Set consists of all subsets whose induced sub-graph satisfies connectivity condition. Throughout the paper, we will refer to the Reduced Power Set as $\Gamma'(\Omega)$.

Referring to the previous considerations and remembering that the empty-set must be a part of $\Gamma'(\Omega)$, the Reduced Power Set from $\mathcal{G}$ in Figure 4.1 is:

$$\begin{aligned}\Gamma'(\Omega) = \{&\emptyset, A, B, A \cup B, C, B \cup C,\\ &A \cup B \cup C, D, C \cup D,\\ &B \cup C \cup D, A \cup B \cup C \cup D,\\ &E, D \cup E, C \cup D \cup E\\ &B \cup C \cup D \cup E, A \cup B \cup C \cup D \cup E\}\end{aligned} \tag{4.5}$$

Definition 4.2. ***(Cardinality of the Reduced Power Set)*** *The cardinality of* $\Gamma'(\Omega)$ *is*

$$|\Gamma'(\Omega)| = \left(\sum_{i=1}^{n} i\right) + 1 \tag{4.6}$$

where n *is the number of elements in* Ω*.*

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

In order to use the Reduced Power Set in the Evidence Theory framework, it is mandatory to demonstrate that the result of the combination rules is still a mapping function that gives not-zeros values to the elements of the Reduced Power Set, i.e., $m : \Gamma'(\Omega) \rightarrow [0, 1]$. Most of the combination rules, (see Table 4.1), exploit the intersection operator to obtain the result of the mapping function m.

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

Proposition 4.1. ***(Closeness of*** $\Gamma'(\Omega)$***)*** $\Gamma'(\Omega)$ *is closed under the intersection operator.*

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

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

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

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

$$\mathcal{V}'_z \subseteq \mathcal{V}'_i, \qquad \text{and} \qquad \mathcal{V}'_z \subseteq \mathcal{V}'_j \tag{4.7}$$

$$\mathcal{E}'_z \subseteq \mathcal{E}'_i, \qquad \text{and} \qquad \mathcal{E}'_z \subseteq \mathcal{E}'_j \tag{4.8}$$

The induced sub-graphs $\mathcal{G}'_i$ and $\mathcal{G}'_j$ are connected and so they must also contain a subset of $\mathcal{G}'$, in Figure 4.1, not included in $\mathcal{G}'_z$. This specific sub-graph is denoted $\mathcal{G}'_c$ and considering the graph $\mathcal{G}$, $\mathcal{G}'_c$ is unique. Therefore, this sub-graph $\mathcal{G}'_c$ is included in $\mathcal{G}'_i$ and in $\mathcal{G}'_j$ because they must be connected for definition, but in this way, also $\mathcal{G}'_c \subseteq \mathcal{G}'_z$. Hence, $\mathcal{G}'_z$ is connected. □

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

It is worth noticing that the principal combination rules (such as Equation 2.1, Equation 2.2 and Equation 2.3), exploit the intersection operator among sets to obtain the final fusion results. In Table 4.1, the principal combination rules are listed with their use of two operators: ∪ and ∩. For further analysis on the properties and the mathematical expression of the rules reported in Table 4.1, see also [18].

Table 4.1 Operators ∪ and ∩ in the principal rules of combination.

	Dempster	Smets	PCR	Yager	Dubois-Prade	Conj	Disj
∪					x		x
∩	x	x	x	x	x	x	

Table 4.2 Results of the example using different combination rules, such as Dempster, Smets and PCR-6 rules.

	m1	m2	Dempster	Smets	PCR
$\emptyset$	0.0	0.0	0.0	0.31	0.0
A	0.1	0.0	0.06	0.02	0.029
B	0.1	0.0	0.09	0.06	0.087
C	0.1	0.1	0.21	0.18	0.2609
D	0.0	0.1	0.09	0.06	0.087
E	0.0	0.1	0.06	0.02	0.029
AB	0.1	0.0	0.05	0.02	0.029
AC	0.0	0.0	0.0	0.0	0.0
AD	0.0	0.0	0.0	0.0	0.0
AE	0.0	0.0	0.0	0.0	0.0
BC	0.1	0.0	0.085	0.07	0.1014
BD	0.0	0.0	0.0	0.0	0.0
BE	0.0	0.0	0.0	0.0	0.0
CD	0.0	0.1	0.085	0.07	0.1014
CE	0.0	0.0	0.0	0.0	0.0
DE	0.0	0.1	0.05	0.02	0.029
ABC	0.1	0.1	0.055	0.04	0.058
ABD	0.0	0.0	0.0	0.0	0.0
ABE	0.0	0.0	0.0	0.0	0.0
ACD	0.0	0.0	0.0	0.0	0.0
ACE	0.0	0.0	0.0	0.0	0.0
ADE	0.0	0.0	0.0	0.0	0.0
BCD	0.1	0.1	0.07	0.06	0.087
BCE	0.0	0.0	0.0	0.0	0.0
BDE	0.0	0.0	0.0	0.0	0.0
CDE	0.1	0.0	0.055	0.04	0.058
$ABCD$	0.1	0.1	0.015	0.01	0.0145
$ABCE$	0.0	0.0	0.0	0.0	0.0
$ABDE$	0.0	0.0	0.0	0.0	0.0
$ACDE$	0.0	0.0	0.0	0.0	0.0
$BCDE$	0.0	0.1	0.015	0.01	0.0145
Ω	0.1	0.1	0.01	0.01	0.0145

In the following, an example is reported in order to show that, choosing as focal sets of $\Gamma(\Omega)$ only elements that respect 4.1 and applying combination rules that exploit the intersection operator, the fusion results are contained in the Reduced Power Set $\Gamma'(\Omega)$, see Table 4.2. As BPA values (m_1 and m_2), a random function assigns values between 0 and 1 to the focal sets. As combination rules, the authors choose Dempster's (Equation 2.1), Smets' (Equation 2.2) and PCR-6 (Equation 2.3) rules.

In conclusion, the Reduced Power Set $\Gamma'(\Omega)$ can be used in risk assessment, to achieve high accuracy and small computational time, during the fusion process.

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

4.2 Power Grid as an Application for Risk Assessment

In this paragraph, a Medium Voltage power grid controlled by a Supervisory Control And Data Acquisition (SCADA) system, connected to a ethernet-based telecommunication network [44], is considered as an application scenario.

The power grid is composed of two main lines, fed by the two substations in Figure 4.2. Different current branches (with physical redundancy) provide power to the loads connected to the grid. In normal conditions, the two main lines are usually disconnected thanks to breaker no. 7 and breaker no. 8 that are normally open. To maintain a radial topology, breaker no. 3 and breaker no. 5 are also open.

The SCADA system in Figure 4.3 is able to monitor the actual state of the power grid and eventually reconfigure the topology by the adoption of the Fault Isolation and System Restoration (FISR) procedure, also called power load shedding. In general if a permanent fault happens, the operator restores the power in the grid by opening and

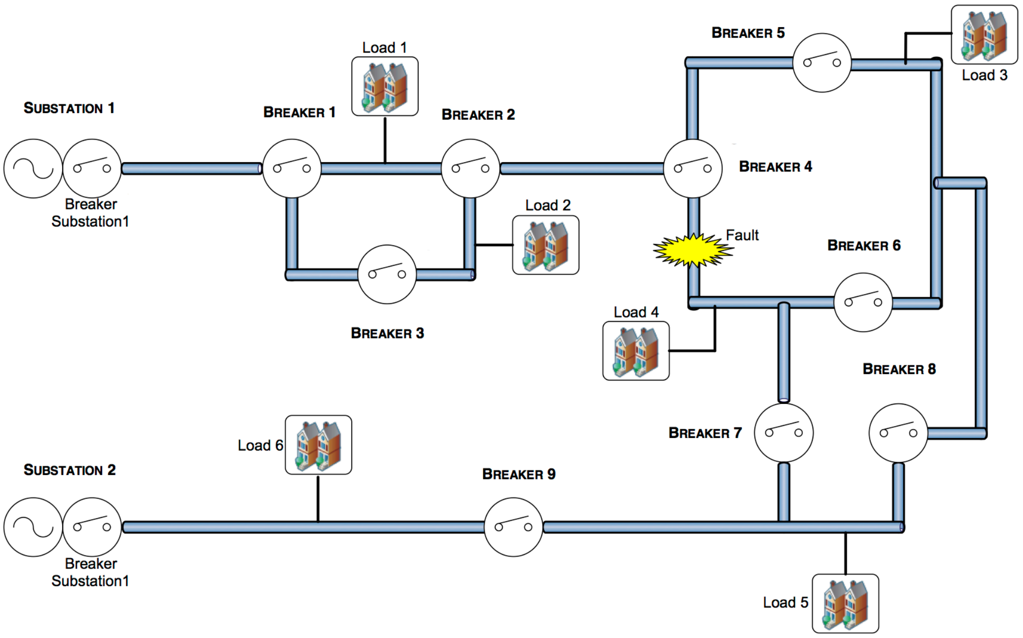


Figure 4.2 An example of Medium Voltage (MV) power grid

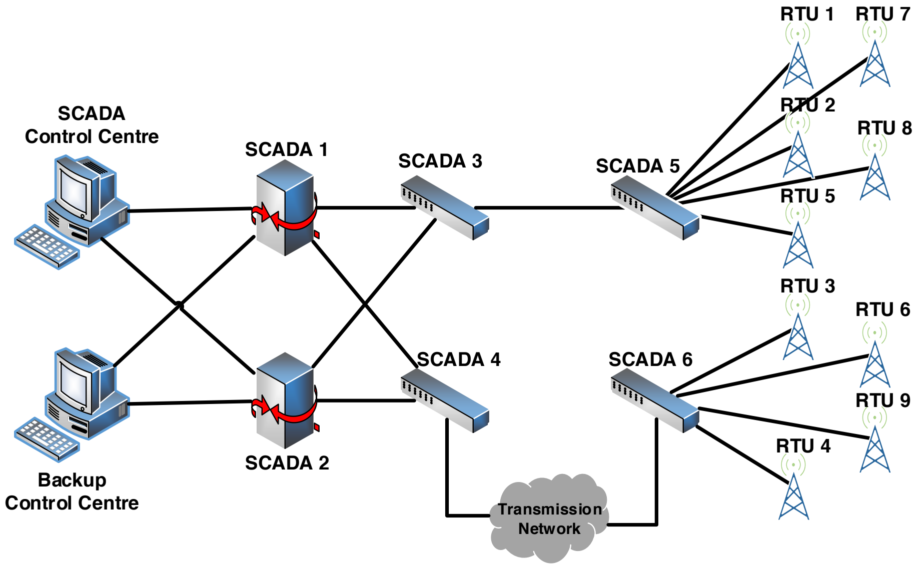


Figure 4.3 The SCADA telecommunication network

closing the breakers. Such procedure is grid-dependent, because different power grids have different FISR procedures, derived by the topology. A complete description of FISR algorithms is outside the scope of this thesis, see [45] for further explanations.

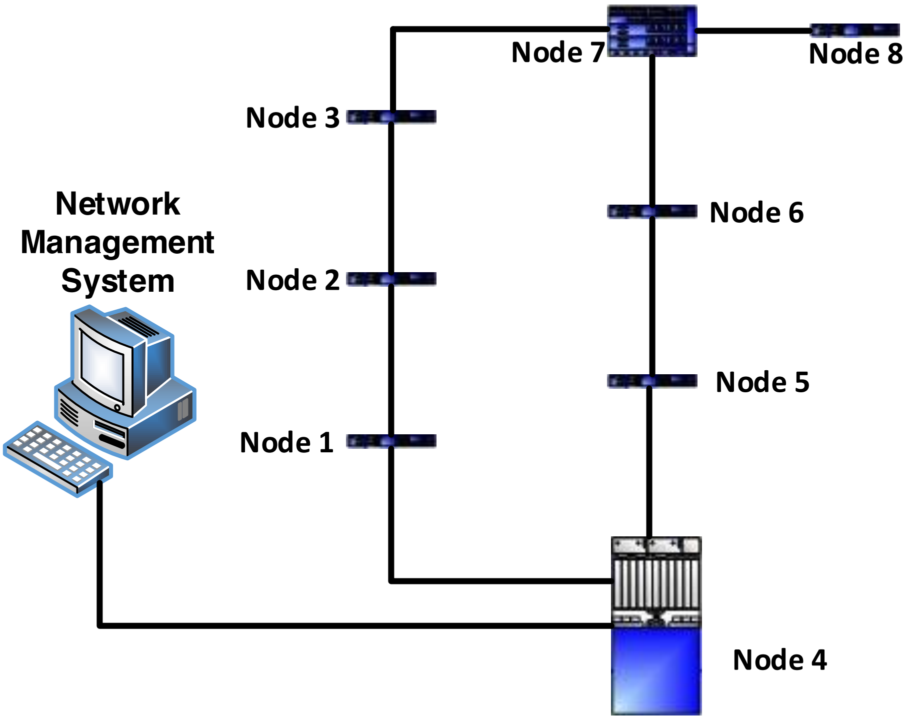


Figure 4.4 A general-purpose telecommunication network

In Figure 4.4, the general-purpose telecommunication network is needed to transmit information from the SCADA control center towards the power grid breakers. This network has mainly a ring topology: in the event of a link failure, packets are sent back to the source node in order to change the routing protocol. In Figure 4.4, node n. 8 and node n. 4 are the links between this network and the SCADA layer.

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

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

In the event of mechanical fault or cyber attack, it is important to evaluate the risk on the overall system. As already done in [33] and as we showed in Chapter 3, this kind of scenario has been used to individuate the cause of cyber-physical faults, fusing information coming from specific domain sensors (tied to Cyber and Physical layers), when an attacker wants to compromise the regular operations within the power grid through telecommunication vulnerabilities. In what follows we will show that it is possible not only to find the most plausible cause of faults, but also to estimate a comprehensive risk belonging to the two layers, cyber and physical, of the power grid.

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

Two subsequent situations are evaluated in the following:

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

As already done by Gao *et al.* in [39] for risk evaluation in network security, we merged several sources and risk factors in order to find the overall risk index. The sources of information from the three infrastructures are:

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

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

Simulations over the real system were carried out with CISIApro, an agent-based simulator for Critical Infrastructures [46]. An Evidence Theory module was added to the simulator with the aim to apply and test the framework introduced in Section 4.1.

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

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

In particular, we consider as Frame of Discernment Ω a risk scale from low (A) to high (E) and $\Gamma'(\Omega)$ as power set. The PCR-6 rule (Equation 2.3) is used to combine sources with the aim of obtaining good solutions in terms of quality-conflict ratio, as explained in Section 2.3.2.

4.2.1 Man In The Middle Attack: Simulations and Results

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

In Table 4.3, BPA values are summarized. In the first column, the focal sets are listed: AB means the element of the power set usually indicated as $\{A \cup B\}$, and so on. The physical sensor m_1 of the power grid detects a lower risk; the SCADA-specific IDS m_2 assigns must of the BPA to B set; and the IT IDS has confidence that the risk of a MITM attack is middle, i.e. $m_3(C) = 0.6$.

Table 4.3 BPA assignments for the Man in the Middle attack.

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

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

In Figure 4.5, only the not-zero sets of $\Gamma'(\Omega)$, after the PCR-6 fusion, are displayed. The blue bars represent the fusion of m_1 and m_2 (getting m_{12}); the red ones, instead, are the results obtained combining m_{12} and m_3.

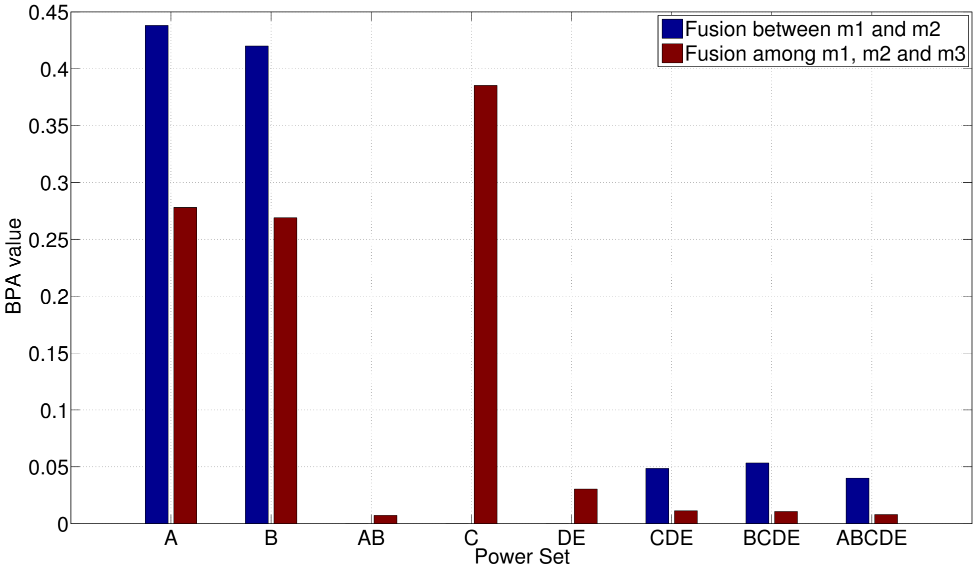


Figure 4.5 Results using PCR-6 rule for combining three information sources

As demonstrated in Section 4.2, no evidences are assigned to the elements of $\Gamma(\Omega) \setminus \Gamma'(\Omega)$: the combination results and the initial focal sets are contained within $\Gamma'(\Omega)$. The overall risk is medium, because the value of the C is the greatest one.

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

4.2.2 Infection Attack: Simulations and Results

In this case, a different situation is considered: an infection is spreading from the telecommunication network towards the power grid in order to cause malfunctioning in the physical layer. In Table 4.4, the BPA values are listed:

m_1 Represents the assignment from the physical sensor in the power grid. A medium risk value is allocate through the sets;

- m_2 Contains the values of the SCADA-specific IDS. A high risk value is assigned to $m(D)$;

- m_3 Corresponds to the telecommunication IDS assignment, after the detection of the infection attack.

Table 4.4 BPA assignments for the Infection attack.

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

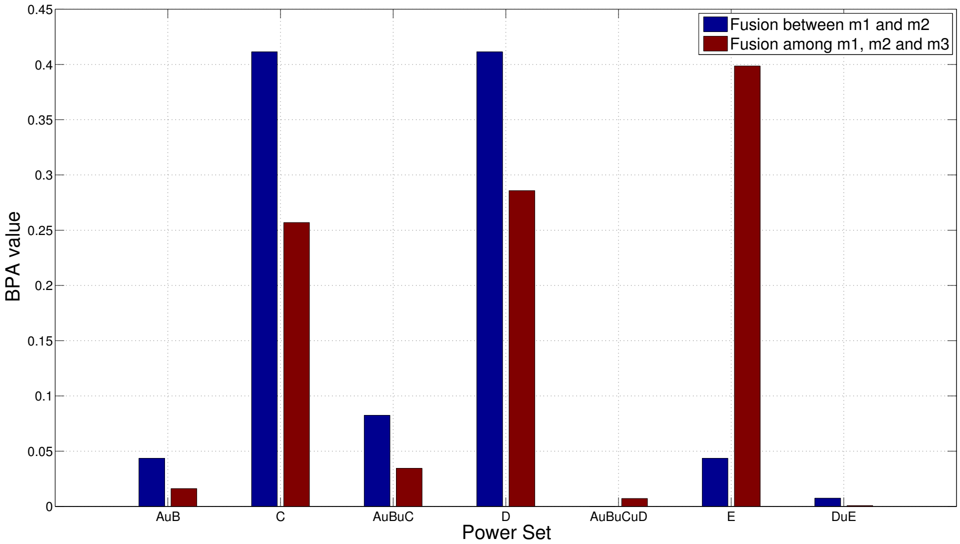


Figure 4.6 Results using PCR-6 rule for combining four information sources

The output of the combination rule, using PCR-6, is depicted in Figure 4.6. The result demonstrates how, if an infection attack is carried out, the risk of possible electrical blackout is very high ($m(E) = 0.4$).

To perform computational time analysis between the classical Evidence Theory framework and the proposed framework, the data obtained from CISIApro simulator [46] were evaluated with Matlab [34]. A simulation script shown, after 1,000,000 trials, that the mean time for fusion process using PCR-6 rule over $\Gamma(\Omega)$ is 2.52 seconds, instead of 1.47 seconds for $\Gamma'(\Omega)$. In this case, the improvement is not remarkable but it increases with the cardinality of the frame of discernment as asserted in Definition 4.2. For example, if the cardinality of the frame of discernment is $n = 10$, the power set contains $2^n = 1024$ instead the Reduced Power Set has only 56, reducing the computational time of around 20 times.

So, as introduced in Section 4.1, the Reduced Power Set is better than $\Gamma(\Omega)$ in terms of computational time.

A final remark on the fusion process must be made: as explained before, the BPAs were fused in a sequential way and, because the PCR-6 rule is non associative, the sequential fusion process is known to be sub-optimal [18]. To get optimal results the BPAs must be combined all together using a generalized PCR-6 rule. Although, this remark does not affect the obtained results because the rule is still based on the intersection operator and so our case study demonstrates the effectiveness of the proposed framework.

Chapter 5

Network Composition for Optimal Disturbance Rejection

Network systems are ubiquitous in engineering, social, and natural domains, where they enable complex functionalities by interconnecting diverse components. An important property of such systems is their robustness to external disturbances altering individual node or interconnection dynamics: the failure of a single network component may cascade into the failure of all interconnected parts [47]. Cyber-Physical Systems are, nowadays, an important class of network systems: they combine physical processes with computational resources in an interconnected framework. These systems act in dynamically changing environments, collect multimodal sensor data, process data at runtime, and communicate with control centers responsible of taking control and planning decisions accordingly. Despite significant advances in relevant areas, several challenges still hinder the development of high-assurance and reconfigurable networks of cyber-physical systems. Increasing robustness of these systems is a very important task for a control system engineer.

Robustness of interconnected networks depends on both the robustness of the isolated sub-networks, as well as on the topological properties of the connections among different networks.

The majority of the existing research on the robustness of dynamical systems and networks focuses on single or isolated components. Classic work in the controls literature defines different measures of the robustness of a dynamical system to disturbances; e.g., see [48]. In the context of network systems, network re-wiring and re-weighting schemes are proposed in [49, 50] to improve the robustness of a single network to environmental disturbances. In the more recent literature on network of networks, different metrics have been used to analyze the robustness of interconnected systems. In [51], cascading failures through interconnected networks are studied via percolation theory. In [52], robustness against random failures or intentional attacks is considered, and a block-based model is proposed to incorporate information of both connectivity and correlations among blocks and links, and infer upon the structure of robust networks. Multi-layer networks, their dynamical properties, and their robustness to random failures are studied, for instance, in [53, 54]. Finally, the importance of the interconnection topology and its structural properties to mitigate failures across networks is highlighted in [55].

We depart from these works by considering a different measure of network robustness and network dynamics, by providing a control-theoretic characterization of the robustness of interconnected networks, and by providing an algorithm for the design of optimally robust networks of networks. Our results are in accordance and provide a quantitative study of recent findings; e.g., see [47].

Contribution The contributions of this chapter are threefold. First, we construct a mathematical framework to analyze the robustness of Cyber-Physical Systems, viewed as interconnected network systems, where the dynamics evolve according to modified Laplacian matrix. We adopt the $\mathcal{H}_2$ system norm to quantify the robustness of a network system to external disturbances. For the case of two interconnected networks, we provide a closed-form expression of the $\mathcal{H}_2$ system norm with respect to the individual components. We show, and quantify, that the $\mathcal{H}_2$ system norm always increases upon interconnection of multiple blocks, so that interconnected networks are less robust than the isolated parts. Second, we prove that interconnections among nodes of the atomic networks with highest degree yield maximum robustness of the interconnected system. In other words, we provide a network interconnection rule that maximizes robustness to disturbances. In addition, we describe an interconnection algorithm for the case of multiple sub-networks, and we provide bounds on the robustness of the composite network. Third and finally, we also generalize the proposed model, making a step further in the problem of finding the optimal robust topology for network systems and, in particular, for Cyber-Physical Systems.

5.1 Problem Setup and Preliminary Notions

In this chapter we study the robustness properties of a dynamical network arising from the interconnections of multiple isolated components, with respect to the interconnection topology. To this aim, let $\mathcal{S} = \{s_1, \dots, s_n\}$ be a set of n *atomic* dynamical networks. Every network is described by the connected and undirected graph $\mathcal{G}_i = (\mathcal{V}_i, \mathcal{E}_i)$ with $|\mathcal{V}_i| = n_i$. Let the dynamics of the network s_i be described by

$$\dot{x}_i = -Q_i \, x_i,$$

where $x_i : \mathbb{R}_{\geq 0} \to \mathbb{R}^{n_i}$ is the map containing the state of the i-th network. For each network s_i, the network matrix is defined as

$$Q_i = \alpha\, I_i + L_i, \tag{5.1}$$

with L_i the Laplacian matrix associated with $\mathcal{G}_i$ [56], and $\alpha \in \mathbb{N}_{>1}$. The network dynamics (5.1) can be thought as the composition of two parts: the *nominal* dynamics, i.e., $I + L$, and the network *interconnection* dynamics, i.e., $(\alpha - 1)\, I$. The parameter $\alpha > 1$ represents an upper bound on the number of interconnections that can be performed through each node of the network. Notice that, by construction, Q_i is positive definite and strictly diagonally dominant, hence invertible [57].

We adopt the open loop $\mathcal{H}_2$ system norm to measure the ability of a network to reject disturbances [49]. As we are interested in quantifying the effect on the whole state of a disturbance affecting all network nodes, the $\mathcal{H}_2$ of the network s_i is defined as

$$\mathcal{H}_2(s_i) = \text{Trace}\left(\int_0^{\infty} e^{-2Q_i t}\, dt\right) = \frac{1}{2}\text{Trace}(Q_i^{-1}). \tag{5.2}$$

In order to interconnect the networks s_i and s_j, we select two nodes $h \in \mathcal{V}_i$ and $k \in \mathcal{V}_j$ for which the constraint α on the maximum number of interconnection is satisfied[1], and define the composite network s_{ij} with $\mathcal{G}_{ij} = (\mathcal{V}_{ij}, \mathcal{E}_{ij})$, where $\mathcal{V}_{ij} = \mathcal{V}_i \cup \mathcal{V}_j$ and $\mathcal{E}_{ij} = \mathcal{E}_i \cup \mathcal{E}_j \cup (h, k)$, and dynamics

$$\dot{x}_{ij} = -Q_{ij}\, x_{ij},$$

[1] Given a matrix Q_i and a node h, to check whether an interconnection can be established through node h we simply check that the $h - th$ row-sum is greater than one, that is $\sum_j^{n_i} Q_i(h, j) > 1$.

where $x_{ij} = [x_i^\mathsf{T}\ x_j^\mathsf{T}]^\mathsf{T}$ and, being e_i the i-th canonical vector of appropriate dimension,

$$Q_{ij} = \begin{bmatrix} Q_i & -e_h e_k^\mathsf{T} \\ -e_k e_h^\mathsf{T} & Q_j \end{bmatrix}. \tag{5.3}$$

Clearly, $\mathcal{H}_2(s_{ij}) = \text{Trace}(Q_{ij}^{-1})/2$. Observe that, by constraining each network to perform at most $\alpha - 1$ interconnections through each of its nodes, we ensure the Q_{ij} matrix to remain positive definite and strictly diagonally dominant, and hence invertible.

In the sequel we assume that the constraint on the maximum number of interconnections (dictated by α) is satisfied when selecting a pair of nodes to perform an interconnection between two networks.

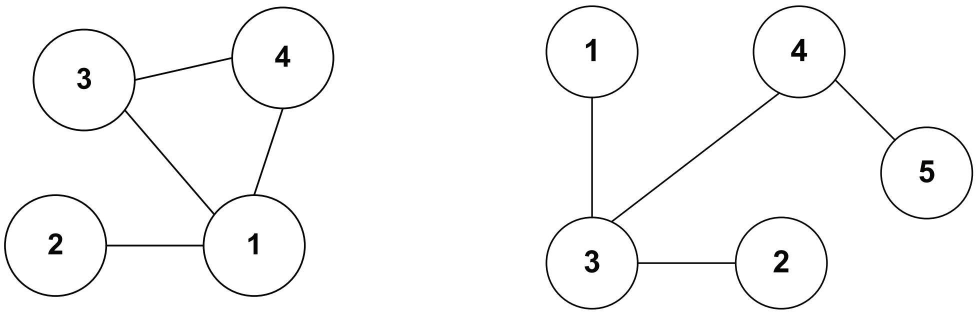
5.1.1 An Illustrative Example

Consider two networks s_1 and s_2 composed, respectively, of $n_1 = 4$ and $n_2 = 5$ nodes as in Figure 5.1, with $\alpha = 2$. The $\mathcal{H}_2$ norm of the two isolated networks is $\mathcal{H}_2(s_1) = 0.600$ and $\mathcal{H}_2(s_2) = 0.8121$. We now compute the robustness of the composite network after interconnecting different pairs of nodes.

Table 5.1 Composite network $\mathcal{H}_2$ normalized ratio.

$s_1 \backslash s_2$	1	2	3	4	5
1	1.0251	1.0251	1.0152	1.0188	1.0259
2	1.0407	1.0407	1.0244	1.0302	1.0419
3	1.0309	1.0309	1.0186	1.0230	1.0318
4	1.0309	1.0309	1.0186	1.0230	1.0318

Table 5.1 shows the normalized ratio computed as the $\mathcal{H}_2$ norm of the composite network obtained interconnecting the pair of nodes (h, k), with $h \in \mathcal{V}_1$ and $k \in \mathcal{V}_2$, divided by the sum of the $\mathcal{H}_2$ norm of the two isolated networks. Clearly, the lower the value of this ratio, the better the performance of the interconnection pair (h, k).

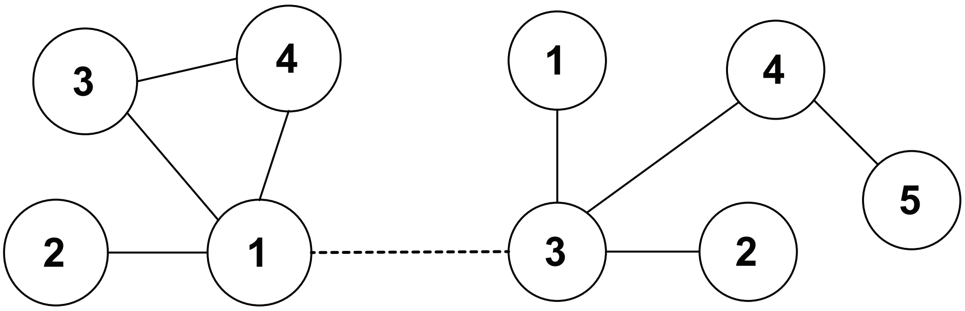


$$Q_1 = \begin{pmatrix} 3+\alpha & -1 & -1 & -1 \\ -1 & 1+\alpha & 0 & 0 \\ -1 & 0 & 2+\alpha & -1 \\ -1 & 0 & -1 & 2+\alpha \end{pmatrix}$$

(a)

$$Q_2 = \begin{pmatrix} 1+\alpha & 0 & -1 & 0 & 0 \\ 0 & 1+\alpha & -1 & 0 & 0 \\ -1 & -1 & 3+\alpha & -1 & 0 \\ 0 & 0 & -1 & 2+\alpha & -1 \\ 0 & 0 & 0 & -1 & 1+\alpha \end{pmatrix}$$

(b)



$$Q_{12} = \left(\begin{array}{cccc|ccccc} 3+\alpha & -1 & -1 & -1 & 0 & 0 & -1 & 0 & 0 \\ -1 & 1+\alpha & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 2+\alpha & -1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & -1 & 2+\alpha & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1+\alpha & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1+\alpha & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 & -1 & -1 & 3+\alpha & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2+\alpha & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1+\alpha \end{array}\right)$$

(c)

Figure 5.1 Example of network composition. In particular, Figure 5.1-a) and Figure 5.1-b) show two dynamical networks $\mathcal{G}_1$ and $\mathcal{G}_2$ along with their network matrices $\mathcal{Q}_1$ and $\mathcal{Q}_2$, respectively. Figure 5.1-c) shows the graph $\mathcal{G}_{12}$ resulting from the interconnection (dashed edge) of two nodes (hubs), and the related network matrix $\mathcal{Q}_{12}$.

According to the numerical results, the best performance is obtained with the pair $(1, 3)$, while the worst performance with $(2, 5)$. From this numerical evaluation two interesting observations can be made: first, the robustness of the composite network seems to be always less than the robustness of the (sum of the) isolated components and, second, interconnections carried out through different pairs of nodes (h, k) lead to composite networks s_{12} with different robustness levels.

Next, we investigate how different interconnection nodes perform when the cardinality of the networks increases. We consider a sequence of n networks of size n_i, and compute the two interconnection sequences with best and worst performance. Due to the dimensionality of the problem, we let $n_i = 4$ and n vary from 2 to 6, and report our result in Figure 5.2. This numerical study shows that the difference between the best and worst interconnection sequence is bound to diverge to as the number of networks increases, thus confirming the importance of the problem of designing efficient algorithm to select optimal interconnection patterns.

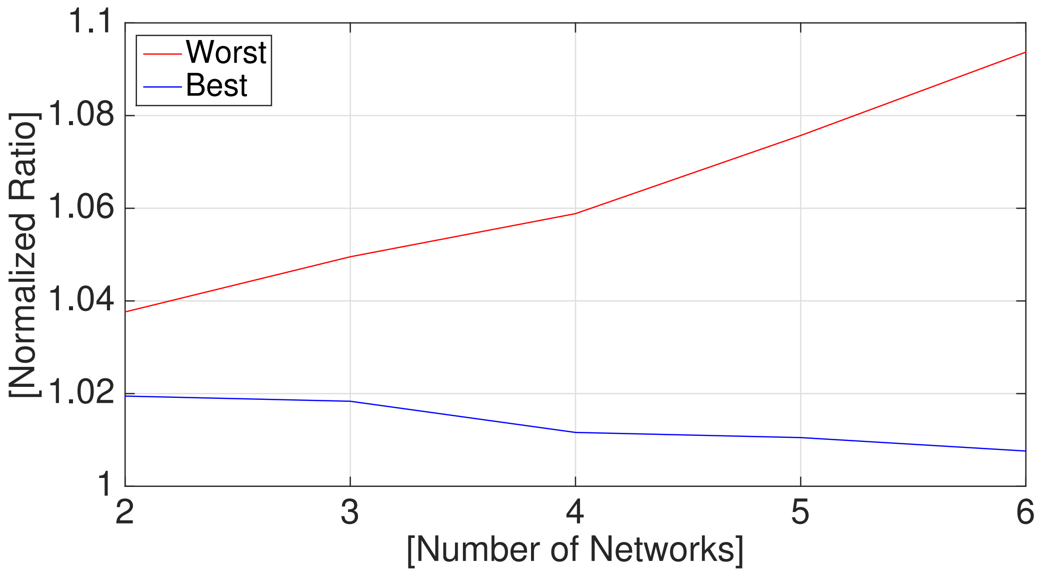


Figure 5.2 Numerical example with n networks ranging from 2 to 6. Each network was with fixed size $n_i = 4$. For each fixed number of networks n, all possible combinations of pair of nodes were computed for the interconnection.

5.2 Optimal Interconnection of Networks

In this section we characterize how the $\mathcal{H}_2$ norm changes when multiple networks are interconnected. We start with the case of two networks, and then we generalize our results to the case of multiple networks.

5.2.1 Interconnection of Two Networks

Let us consider two atomic networks Q_i and Q_j. We first provide a closed-form expression for the $\mathcal{H}_2$ norm of the interconnected network Q_{ij}. To this aim, let $Q(h,k)$ and $Q^{-1}(h,k)$ denote the entry in the h-th row and k-th column for the matrix Q and the inverse matrix Q^{-1}, respectively. In addition, let $Q^{-1}(:,h)$ and $Q^{-1}(:,k)$ denote the h-th row and the k-th column of the matrix Q^{-1}, respectively.

Theorem 5.1. ***($\mathcal{H}_2$ norm of two interconnected networks)*** *Let $\mathcal{Q}_{ij}$ be as in* (5.3). *Then,*

$$Trace(Q_{ij}^{-1}) = Trace(Q_i^{-1}) + Trace(Q_j^{-1}) + \lambda_{ij}^{hk} + \lambda_{ij}^{kh},$$

where

$$\lambda_{ij}^{hk} = \frac{\|Q_i^{-1}(:,h)\|^2}{1/Q_j^{-1}(k,k) - Q_i^{-1}(h,h)} > 0,$$

$$\lambda_{ij}^{kh} = \frac{\|Q_j^{-1}(:,k)\|^2}{1/Q_i^{-1}(h,h) - Q_j^{-1}(k,k)} > 0.$$

Proof. In order to prove the Theorem, we first derive a closed form for the main diagonal of the inverse of the block matrix Q_{ij} defined as in (5.3), and then we compute its trace as a function of the two matrices Q_i and Q_j and of the interconnections through the nodes $h \in \mathcal{V}_i$ and $k \in \mathcal{V}_j$. In particular, the following closed-form expression for

Q_{ij}^{-1} holds

$$Q_{ij}^{-1} = \begin{bmatrix} \left(Q_i - e_h e_k^{\mathsf{T}} Q_j^{-1} e_k e_h^{\mathsf{T}}\right)^{-1} & \star \\ \star & \left(Q_j - e_k e_h^{\mathsf{T}} Q_i^{-1} e_h e_k^{\mathsf{T}}\right)^{-1} \end{bmatrix}, \tag{5.4}$$

where the block off-diagonal can be neglected as they do not affect the computation of the Trace.

Let us now consider the first block on the main diagonal of the inverse matrix Q_{ij}^{-1}. In particular, let us recall that the interconnection is obtained by connecting the h-th node of the system s_1 with the k-th node of the system s_2. Then the following holds

$$\begin{aligned} &\left(Q_i - e_h e_k^{\mathsf{T}} Q_j^{-1} e_k e_h^{\mathsf{T}}\right)^{-1} = \left(Q_i - Q_j^{-1}(k,k) e_h \, e_h^{T}\right)^{-1} \\ &= Q_i^{-1} + \frac{Q_i^{-1}(:,h) Q_i^{-1}(h,:)}{1/Q_j^{-1}(k,k) - Q_i^{-1}(h,h)} = Q_i^{-1} + P_{ij}^{hk}, \end{aligned}$$

where Lemma A.5 has been used to obtain the second equality.

By following a similar reasoning for the second block on the main diagonal of the inverse matrix Q_{ij}^{-1} we obtain

$$\begin{aligned} &\left(Q_j - e_k e_h^{\mathsf{T}} Q_i^{-1} e_h e_k^{\mathsf{T}}\right)^{-1} = \left(Q_j - Q_i^{-1}(h,h) e_k \, e_k^{T}\right)^{-1} \\ &= Q_j^{-1} + \frac{Q_j^{-1}(:,k) Q_j^{-1}(k,:)}{1/Q_i^{-1}(h,h) - Q_j^{-1}(k,k)} = Q_j^{-1} + P_{ij}^{kh}, \end{aligned}$$

Since the objective is to compute the trace of the block-diagonal matrix Q_{ij}^{-1} given in (5.4), let us now investigate the structure of the eigenvalues of the two perturbations P_{ij}^{hk} and P_{ij}^{kh}. In particular, by noticing that these perturbations are by construction rank-1 matrices the following holds

$$\begin{aligned} \operatorname{spec}(P_{ij}^{hk}) &= \{\lambda_{ij}^{hk}, 0, \ldots, 0\}, \\ \operatorname{spec}(P_{ij}^{kh}) &= \{\lambda_{ij}^{kh}, 0, \ldots, 0\}, \end{aligned}$$

where the eigenvalues λ_{ij}^{hk} and λ_{ij}^{kh} are by construction defined as

$$\begin{aligned} \lambda_{ij}^{hk} &= \frac{\left\|Q_i^{-1}(:,h)\right\|^2}{1/Q_j^{-1}(k,k) - Q_i^{-1}(h,h)}, \\ \lambda_{ij}^{kh} &= \frac{\left\|Q_j^{-1}(:,k)\right\|^2}{1/Q_i^{-1}(h,h) - Q_j^{-1}(k,k)}. \end{aligned}$$

Therefore, from the linearity of the Trace operator it follows

$$\text{Trace}(Q_{ij}^{-1}) = \text{Trace}(Q_i^{-1}) + \text{Trace}(Q_j^{-1}) + \lambda_{ij}^{kh} + \lambda_{ij}^{hk}.$$

At this point in order to prove that $\lambda_{ij}^{hk} > 0$ and $\lambda_{ij}^{hk} > 0$ it is sufficient to show that by construction

$$\begin{aligned} 1/Q_j^{-1}(k,k) - Q_i^{-1}(h,h) > 0, \\ 1/Q_i^{-1}(h,h) - Q_j^{-1}(k,k) > 0. \end{aligned} .$$

In this regard, note that Q_i and Q_j are symmetric strictly diagonally dominant M-matrices which, by construction, are irreducible being the graphs $\mathcal{G}_1$ and $\mathcal{G}_2$ associated to them (strongly) connected by definition. Then from Lemma A.3 it follows that Q_i^{-1} and Q_j^{-1} are symmetric entrywise positive matrix. Furthermore, by construction we also know that

$$\Big(Q_r(i,i) - \sum |Q_r(i,j)|\Big) > 1, \; \forall\, i\, \in 1, \, \ldots, \, n_r,$$

with $r \in \{i, j\}$. Thus from [58] it follows that

$$\sum_{j=1}^{n_r} Q_r^{-1}(i,j) \leq 1, \; \forall\, i\, \in 1, \, \ldots, \, n,$$

with $r \in \{i, j\}$, which in turn implies

$$Q_i^{-1}(h,h) < 1, \quad \forall\, h \,\in\, \mathcal{V}_1,$$
$$Q_j^{-1}(k,k) < 1, \quad \forall\, k \,\in\, \mathcal{V}_2,$$

thus the result follows.

□

Theorem 5.1 provides a general closed-form expression for the $\mathcal{H}_2$ norm of a composite network. It should be noticed that the relation in Theorem 5.1 depends on the interconnection parameter α, and that this dependency is implicit in the matrices Q_i and Q_j. Theorem 5.1 implies that networks arising from the interconnection of two isolated atomic networks are less robust than the isolated components. In fact,

$$\text{Trace}(Q_{ij}^{-1}) > \text{Trace}(Q_i^{-1}) + \text{Trace}(Q_j^{-1}).$$

Moreover, it follows from Theorem 5.1 that the minimum $\mathcal{H}_2$ performance of the composite network is achieved when the interconnections nodes h and k are selected to minimize the perturbation $\lambda_{ij}^{kh} + \lambda_{ij}^{hk}$. Let $\deg(i)$ denote the degree of node i, and recall that a node of a network is a *hub* if it has the highest degree [56]. We next show that the $\mathcal{H}_2$ norm of a composite network is minimized when the nodes h and k are two hubs of the atomic networks $\mathcal{G}_1$ and $\mathcal{G}_2$, respectively.

Theorem 5.2. ***(Connections via hubs)*** *Let Q_{ij} be as in* (5.3), *and let h^* and k^* satisfy*

$$\lambda_{ij}^{h^*k^*} + \lambda_{ij}^{k^*h^*} = \min_{h \in \mathcal{V}_i, k \in \mathcal{V}_j} \lambda_{ij}^{kh} + \lambda_{ij}^{hk},$$

where λ_{ij}^{kh} *and* λ_{ij}^{hk} *are defined as in* (5.1)*. Then,*

$$deg(h^*) = \max_{h \in \mathcal{V}_i} deg(h), \ \textit{and } deg(k^*) = \max_{k \in \mathcal{V}_j} deg(k).$$

Proof. n order to prove the Theorem it is sufficient to show that

$$\lambda_{ij}^{kh} + \lambda_{ij}^{hk} > \lambda_{ij}^{k^*h^*} + \lambda_{ij}^{h^*k^*},$$

for all $h \in \mathcal{V}_1$ and $k \in \mathcal{V}_2$ such that

$$\deg(h) < \deg(h^*), \text{ and } \deg(k) < \deg(k^*),$$

where

$$\deg(h^*) = \max_{h \in \mathcal{V}_i} \deg(h), \text{ and } \deg(k^*) = \max_{k \in \mathcal{V}_j} \deg(k).$$

In particular, it should be noticed that by construction the quantity $\lambda_{ij}^{kh} + \lambda_{ij}^{hk}$ is minimized when the terms $Q_i^{-1}(h,h)$ and $Q_j^{-1}(k,k)$ are *minimized* at the denominator and the terms $\|Q_i^{-1}(:,h)\|^2$ and $\|Q_j^{-1}(:,k)\|^2$ are *minimized* at the numerator. Therefore, the problem can be equivalently stated as proving that for all $h \in \mathcal{V}_1$ and $k \in \mathcal{V}_2$ such that

$$\deg(h) < \deg(h^*), \text{ and } \deg(k) < \deg(k^*),$$

then for the system s_i we have:

$$Q_i^{-1}(h,h) > Q_i^{-1}(h^*,h^*), \text{and } \|Q_i^{-1}(:,h)\|^2 > \|Q_i^{-1}(:,h^*)\|^2,$$

and for the system s_j we have:

$$Q_j^{-1}(k,k) > Q_j^{-1}(k^*,k^*), \text{and } \|Q_j^{-1}(:,k)\|^2 > \|Q_j^{-1}(:,k^*)\|^2,$$

In this regard, let us now focus on the first inequality for the system s_i as a similar reasoning will hold for the system s_j. In particular, by recalling that $Q_i\, Q_i^{-1} = I$, for any two vertices h and h^* we have

$$\begin{aligned} \sum_{r=1}^{n_i} Q_i(h^*,r)Q_i^{-1}(r,h^*) &= 1, \\ \sum_{r=1}^{n_i} Q_i(h,r)Q_i^{-1}(r,h) &= 1, \end{aligned} \tag{5.5}$$

from which by equating we obtain

$$\sum_{r=1}^{n_i} Q_i(h^*,r)Q_i^{-1}(r,h^*) = \sum_{r=1}^{n_i} Q_i(h,r)Q_i^{-1}(r,h).$$

At this point, by recalling that $Q_i(h,h) < Q_i(h^*,h^*)$ we have that

$$\begin{aligned} Q_i^{-1}(h^*,h^*) &= \frac{Q_i(h,h)}{Q_i(h^*,h^*)} Q_i^{-1}(h,h) \\ &+ \sum_{r=2}^{n_1} \frac{Q_i(h^*,r)}{Q_i(h^*,h^*)} Q_i^{-1}(r,h^*) - \sum_{r=2}^{n_1} \frac{Q_i(h,r)}{Q_i(h^*,h^*)} Q_i^{-1}(r,h), \end{aligned}$$

Therefore it follows that $Q_i^{-1}(h^*,h^*) < Q_i^{-1}(h,h)$ if and only if

$$\begin{aligned} \sum_{r=2}^{n_1} \frac{Q_i(h^*,r)}{Q_i(h^*,h^*)} Q_i^{-1}(r,h^*) - \sum_{r=2}^{n_1} \frac{Q_i(h,r)}{Q_i(h^*,h^*)} Q_i^{-1}(r,h) \\ < \left(1 - \frac{Q_i(h,h)}{Q_i(h^*,h^*)}\right) Q_i^{-1}(h,h), \end{aligned}$$

which can be equivalently expressed as

$$\sum_{r=2}^{n_1} Q_i(h^*,r)Q_i^{-1}(r,h^*) - \sum_{r=2}^{n_1} Q_i(h,r)Q_i^{-1}(r,h)$$
$$< \left(Q_i(h^*,h^*) - Q_i(h,h)\right) Q_i^{-1}(h,h),$$

At this point, by recalling that the equalities (5.5) hold, the previous equation can be expressed solely in terms of the elements $Q_i(h,h)$, $Q_i^{-1}(h,h)$ and $Q_i(h^*,h^*)$, $Q_i^{-1}(h^*,h^*)$ as follows

$$\Big(1 - Q_i(h,h)\, Q_i^{-1}(h,h)\Big) - \Big(1 - Q_i(h^*,h^*)\, Q_i^{-1}(h^*,h^*)\Big)$$
$$< \left(Q_i(h^*,h^*) - Q_i(h,h)\right) Q_i^{-1}(h,h),$$

from which we obtain

$$Q_i(h^*,h^*)\, Q_i^{-1}(h^*,h^*) - Q_i(h,h)\, Q_i^{-1}(h,h)$$
$$< \left(Q_i(h^*,h^*) - Q_i(h,h)\right) Q_i^{-1}(h,h),$$

by further simplifying we have

$$Q_i(h^*,h^*)\, Q_i^{-1}(h^*,h^*) < Q_i(h^*,h^*)\, Q_i^{-1}(h,h),$$

that is

$$Q_i^{-1}(h^*,h^*) < Q_i^{-1}(h,h).$$

and thus the first inequality for the system s_i follows.

Let us now focus on the second inequality for the system s_i as again a similar reasoning will hold for the system s_j. In this regard, it should be notice that $\|Q_i^{-1}(:,h)\|^2$ represents the entry (h,h) of the matrix $\left(Q_i^{-1}\right)^2$. Therefore, the result we are seeking can be obtained by following the same reasoning as before if the following two properties hold

$$Q_i^2\left(Q_i^{-1}\right)^2 = I,$$

and for all $h \in \mathcal{V}_1$ such that $\deg(h) < \deg(h^*)$ we have

$$Q_i^2(h,h) < Q_i^2(h^*,h^*) \Longleftrightarrow Q_i(h,h) < Q_i(h^*,h^*).$$

The first property follows directly from the fact that $Q_1\, Q_1^{-1} = I$; while the second property can be shown noticing that by construction the (i,i) entry of the matrix Q_1^2 is defined as

$$Q_1^2(h,h) = \sum_{r=1}^{n_1} Q_1(h,r)\; Q_1(r,h) = \left\|Q_i(:,h)\right\|^2,$$

where the last equality follows because Q_i is symmetric. □

Theorem 5.2 implies that, in order to minimize the $\mathcal{H}_2$ norm of the interconnected system, two atomic networks should be connected by creating links between nodes with highest degree. Note that the isolated atomic networks may have multiple hubs, and the choice of an hub remains, at this stage, a combinatorial problem.

5.2.2 Interconnection of Multiple Networks

We now study the robustness of networks arising from the composition of multiple components. In this context the pairwise interconnection previously introduced for two dynamical networks is now generalized to the case of networks which themselves may already represent composite networks. In particular, we assume that at each iteration only a pairwise interconnection between two (composite) dynamical networks may be carried out.

We now introduce the following preliminary result.

Lemma 5.1. ***(Trace decomposition)*** *Let $A_i = D_i + L_i$ and $A_j = D_j + L_j$ be symmetric positive definite and diagonally dominant with D_i and D_j diagonal entrywise positive (integer) matrix and let A be*

$$A_{ij} = \begin{bmatrix} A_i & -e_h e_k^\mathsf{T} \\ -e_k e_h^\mathsf{T} & A_j \end{bmatrix}, \tag{5.6}$$

for some canonical vectors e_h and e_k such that

$$h = \operatorname{argmax}_r A_i(r,r), \ \textit{and}\ k = \operatorname{argmax}_r A_j(r,r),$$

Then, $A_{ij} = D_{ij} + L_{ij}$ is symmetric positive definite and diagonally dominant, and

$$\operatorname{Trace}(A_{ij}^{-1}) \leq \operatorname{Trace}(A_i^{-1}) + \operatorname{Trace}(A_j^{-1}) + \Delta_{ij} + \Delta_{ji},$$

where

$$\begin{aligned} \Delta_{ij} &= \frac{(1+\gamma_i^2)^2(1+\gamma_j)^2 A_i^{max}}{\gamma_i A_i^{2^{max}}\left(16\gamma_i\gamma_j A_i^{max} A_j^{max} - (1+\gamma_i)^2(1+\gamma_j)^2\right)}, \\ \Delta_{ji} &= \frac{(1+\gamma_i)^2(1+\gamma_j^2)^2 A_j^{max}}{\gamma_j A_j^{2^{max}}\left(16\gamma_i\gamma_j A_i^{max} A_j^{max} - (1+\gamma_i)^2(1+\gamma_j)^2\right)}, \end{aligned} \tag{5.7}$$

with $\gamma_k = \lambda_{max}(A_k)/\lambda_{min}(A_k)$ and

$$A_k^{max} = \max_r A_k(r,r), \ \textit{and}\ A_k^{2^{max}} = \max_r A_k^2(r,r).$$

Proof. As for the proof of Theorem 5.1, by using to the closed-form for the inverse of a two-block matrix and by exploiting Lemma A.5, it can be shown that the following holds for the matrix A_{ij} defined as in (5.6):

$$\operatorname{Trace}(A_{ij}^{-1}) = \operatorname{Trace}(A_i^{-1}) + \operatorname{Trace}(A_j^{-1}) + \lambda_{ij}^{hk} + \lambda_{ij}^{kh},$$

with λ_{ij}^{kh} and λ_{ij}^{hk} defined as

$$\lambda_{ij}^{hk} = \frac{\|A_i^{-1}(:,h)\|^2}{1/A_j^{-1}(k,k) - A_i^{-1}(h,h)} > 0,$$

$$\lambda_{ij}^{kh} = \frac{\|A_j^{-1}(:,k)\|^2}{1/A_i^{-1}(h,h) - A_j^{-1}(k,k)} > 0.$$

Therefore in order to prove the Lemma we must characterize an upper bound for these two terms λ_{ij}^{kh} and λ_{ij}^{hk}. In particular, it should be noticed that this problem can be equivalently expressed in terms of characterizing an upper bound for the terms $A_i^{-1}(h,h)$, $\|A_i^{-1}(:,h)\|^2$, $A_j^{-1}(k,k)$, and $\|A_j^{-1}(:,k)\|^2$.

Let us now focus on the two terms $A_i^{-1}(h,h)$ and $\|A_i^{-1}(h,:)\|^2$ as a similar reasoning will hold for the other two terms. In particular, from Lemma A.1 we know that the following holds

$$A_i^{-1}(h,h) \leq \frac{\left(\gamma_i^{1/2} + \gamma_i^{-1/2}\right)^2}{4\,A_i^{\max}}.$$

where $\gamma_i = \lambda_{\max}(A_i)/\lambda_{\min}(A_i)$ and since $h = \operatorname{argmax}_r A_i(r,r)$ then $A_i^{\max} = A_i(h,h)$.

At this point, by recalling that by construction $\|A_i^{-1}(:,h)\|^2$ represents the entry (h,h) of the matrix $\left(A_i^{-1}\right)^2$, and the eigenvalues of a squared matrix are the squared eigenvalues of the matrix itself, the following upper bound is obtained

$$\left\|A_i^{-1}(:,h)\right\|^2 \leq \frac{\left(\gamma_i + \gamma_i^{-1}\right)^2}{4\,A_i^{2\max}},$$

where $A_i^{2\max} = \max_r A_i^2(r,r)$ and similarly to the previous case since $h = \operatorname{argmax}_r A_i(r,r)$ then by definition it follows that $A_i^{2\max} = A_i^2(h,h)$.

At this point, by following the same reasoning, similar bounds can be found for the two terms $A_j^{-1}(k,k)$ and $\|A_j^{-1}(:,k)\|^2$.

Finally, by substituting these bounds in the definition of the two terms λ_{ij}^{kh} and λ_{ij}^{hk} and by doing simply algebraic manipulations the bounds Δ_{ij} and Δ_{ji} given in (5.7) follow. □

Note that, both the the dynamical matrix of the isolated components Q_i as in (5.1) and of the composite network Q_{ij} as in (5.3) fit the structure of a matrix A_i given in Lemma 5.1. We now provide a useful result for a composite network which relates the computation of the parameters showing up in (5.7) to the isolated part of which it is composed of. Intuitively, this will enable the (recursive) application of Lemma 5.1 for the derivation of robustness bounds to che case of composite networks arising from the interconnection of multiple components.

Lemma 5.2. ***(Bounds on composite networks)*** *Let Q_i and Q_j be as in* (5.1) *or* (5.3) *and let their interconnection Q_{ij} via hubs be as in* (5.6)*. Then,*

$$\begin{aligned} \gamma_{ij} &< 2\ \max\{Q_i^{max}, Q_j^{max}\}, \\ Q_{ij}^{max} &= \max\left\{Q_i^{max},\, Q_j^{max}\right\}, \\ Q_{ij}^{2\ max} &> \max\left\{Q_i^{2\,max},\, Q_j^{2\,max}\right\}. \end{aligned}$$

Proof. In order to prove the lemma, we notice that from the Gershgorin circle theorem by construction the matrix Q_{ij} has the following spectrum

$$\operatorname{spec}(Q_{ij}) \subseteq \left[1,\ \alpha + 2 \max_{h\in\mathcal{V}_i, k\in\mathcal{V}_j}\{\deg(h), \deg(k)\} + 1\right].$$

In particular, by noticing that

$$\alpha + \max_{h\in\mathcal{V}_i, k\in\mathcal{V}_j}\{\deg(h), \deg(k)\} > \max_{h\in\mathcal{V}_i, k\in\mathcal{V}_j}\{\deg(h), \deg(k)\} + 1,$$

and by recalling that by definition

$$Q_r^{\max} = \alpha + \max_{p \in \mathcal{V}_r}\{\deg(p)\},\ r \in \{i,j\},$$

the spectrum of the matrix Q_{ij} can be also written as

$$\operatorname{spec}(Q_{ij}) \subseteq \left[1,\ 2\max\{Q_i^{\max}, Q_j^{\max}\}\right],$$

thus by recalling that $\gamma_{ij} = \lambda_{\max}(Q_{ij})/\lambda_{\min}(Q_{ij})$, it follows that

$$\gamma_{ij} < 2\max\{Q_i^{\max}, Q_j^{\max}\}.$$

Furthermore, since the matrix Q_{ij} as in (5.3) is a block matrix by construction we have

$$Q_{ij}^{\max} = \max\left\{Q_i^{\max},\, Q_j^{\max}\right\},$$

and the following holds for Q_{ij}^2

$$Q_{ij}^{2\ \max} = \max\left\{Q_i^{2\max},\, Q_j^{2\max}\right\} + 1,$$

as the block matrices on the main diagonal of Q_{ij}^2 are given exactly by $Q_i^2 + \operatorname{diag}(e_h)$ and $Q_j^2 + \operatorname{diag}(e_k)$ with $\operatorname{diag}(e_k)$ a diagonal matrix with all zeros but the entry in the k-row and k-th column which is equal to 1. This follows directly from the fact that when computing Q_{ij}^2 by construction we have $(e_h e_k^\mathsf{T})(e_k e_h^\mathsf{T}) = \operatorname{diag}(e_h)$ and $(e_k e_h^\mathsf{T})(e_h e_k^\mathsf{T}) = \operatorname{diag}(e_k)$. □

As far as the network composition in the context of multiple networks is concerned, we recall that interconnections are assumed to be performed pairwise, thus yielding to the same block-matrix structure as in (5.3). We remark that the major difference compared to the case of a two-networks interconnection relies on the fact that in this case, at a given step, the isolated parts appearing on the main diagonal of such a block matrix may themselves represent composite networks. Notably, this properties is already captured by the more general block matrix form given in (5.6).

We are now ready to state our main result which provides an upper and lower bound on the $\mathcal{H}_2$ norm of a composite dynamical network.

Theorem 5.3. ***($\mathcal{H}_2$ of composite networks)*** *Let Q be a matrix resulting from a pairwise interconnection of $Q_1, \ldots, Q_n$. Then, Q is positive definite and diagonally dominant and*

$$\begin{aligned}\mathrm{Trace}(Q^{-1}) &\leq \sum_{i=1}^{n} \mathrm{Trace}(Q_i^{-1}) + (n-1)\bar{\Delta}^{\max},\\ \mathrm{Trace}(Q^{-1}) &\geq \sum_{i=1}^{n} \mathrm{Trace}(Q_i^{-1}),\end{aligned}$$

where $\bar{\Delta}^{\max}$ is defined as

$$\bar{\Delta}^{\max} = \max_{i,j=\{1,\ldots,n\}} \{\bar{\Delta}_{ij} + \bar{\Delta}_{ji}\}$$

with $\bar{\Delta}_{ij}$ defined as

$$\bar{\Delta}_{ij} = \frac{\left(1+(Q_i^{max})^2\right)^2 (1+Q_j^{max})^2 Q_i^{max}}{\gamma_i Q_i^{2max}\left(16\,(Q_i^{max})^2\left(Q_j^{max}\right)^2 - (1+Q_i^{max})^2\,(1+Q_j^{max})^2\right)} \tag{5.8}$$

Proof. In order to prove the first inequality of the Theorem, let us consider for the sake of clarity a set $\mathcal{S} = \{1,\, 2,\, 3\}$ of 3 dynamical networks and assume with no lack of generality that interconnections are performed sequentially, that is first the matrix Q_1 is interconnected with the matrix Q_2 and then the resulting network matrix Q_{12} is connected with the matrix Q_3.

At this point, by recursively applying Lemma 5.1, the following holds for the trace of the composite network Q_{123}

$$\begin{aligned}\mathrm{Trace}(Q_{123}^{-1}) &\leq \mathrm{Trace}(Q_{12}^{-1}) + \mathrm{Trace}(Q_3^{-1}) + \Delta_{12,3} + \Delta_{3,12} \\ &\leq \mathrm{Trace}(Q_1^{-1}) + \mathrm{Trace}(Q_2^{-1}) + \Delta_{1,2} + \Delta_{2,1} \\ &+ \mathrm{Trace}(Q_3^{-1}) + \Delta_{12,3} + \Delta_{3,12}\end{aligned}$$

In particular, by recalling the definition of the terms Δ_{ij} and Δ_{ji} as in (5.7) and by exploiting Lemma 5.2, the following bound for the terms $\Delta_{12,3} + \Delta_{3,12}$ is obtained with respect to the atomic parts, namely Q_1, Q_2 and Q_3

$$\Delta_{12,3} + \Delta_{3,12} \leq \max\{(\bar{\Delta}_{1,3} + \bar{\Delta}_{3,1}), (\bar{\Delta}_{2,3} + \bar{\Delta}_{3,2})\},$$

where $\bar{\Delta}_{i,j}$ given in (5.8) differs from $\Delta_{i,j}$ as the γ_i and γ_j are replaced with their upper bound $2Q_i^{\max}$ and $2Q_j^{\max}$, respectively. Note that by using $Q_i^{\max}$ and $Q_{ij}^{2\ \max}$ in $\bar{\Delta}_{i,j}$, we intrinsically exploit the equality and the lower bound given in the second and third equations of Lemma (5.2), respectively. Therefore we obtain

$$\begin{aligned}\mathrm{Trace}(Q_{123}^{-1}) &\leq \mathrm{Trace}(Q_1^{-1}) + \mathrm{Trace}(Q_2^{-1}) + \mathrm{Trace}(Q_3^{-1}) \\ &+ (\Delta_{1,2} + \Delta_{2,1}) \\ &+ \max\{(\bar{\Delta}_{1,3} + \bar{\Delta}_{3,1}), (\bar{\Delta}_{2,3} + \bar{\Delta}_{3,2})\}\end{aligned}$$

At this point, by iterating the same reasoning for a given set $\mathcal{S} = \{s_1, s_2, \ldots, s_n\}$ of n dynamical networks and by still assuming interconnections to be performed sequentially, the following bound on the trace of the composite system holds

$$\begin{aligned}\mathrm{Trace}(Q^{-1}) \leq & \sum_{i=1}^{n}\left(\mathrm{Trace}(Q_i^{-1}) + \max_{j=1,\ldots,i-1}\{\bar{\Delta}_{ij} + \bar{\Delta}_{ji}\}\right)\\ \leq & \sum_{i=1}^{n}\mathrm{Trace}(Q_i^{-1}) + (n-1)\,\bar{\Delta}^{\max}\end{aligned}$$

where the second inequality follows from the fact that

$$\bar{\Delta}^{\max} = \max_{i,j=\{1,\ldots,n\}}\{\bar{\Delta}_{ij} + \bar{\Delta}_{ji}\}.$$

with $\bar{\Delta}_{ij} \geq \Delta_{ij}$ for all $i, j \in \{1, \ldots, n\}$ by construction.

Note that, by construction the same upper bound holds regardless of the particular sequence of interconnections and ordering of the dynamical networks. Intuitively, this can be explained by the fact that, by exploiting both the decomposition properties of Lemma 5.1 and the structure of the bounds given in Lemma 5.2, the perturbation introduced by the interconnection of any pair of (intermediate) composite networks can always be bounded from above by the max of a set of “elementary” upper bounds of the perturbation arising from network compositions involving only atomic dynamical networks, i.e., $\bar{\Delta}_{ij}$ with $i, j \in \{1, \ldots, n\}$, and for which the inequality stated above still holds true.

In order to prove the second inequality of the Theorem, it is sufficient to notice that by construction the perturbation terms introduced by the interconnections contribute with a positive term to the computation of the $\mathcal{H}_2$ norm of the composite network. Therefore, a straightforward lower bound is given solely by the sum of the trace of the atomic parts. □

5.2.3 Numerical Results

In this section, we provide numerical results to validate our theoretical findings. In particular, motivated by the fact that the optimal interconnection between two dynamical networks is always achieved via nodes with the highest degree, we propose an algorithm that, at each iteration, minimizes the perturbation terms arising from any possible interconnection of hubs. We remark that the definition of a hub is given with respect to an atomic network as detailed in Theorem 5.1. Thus, even for a composite network nodes are labeled as hubs according to their role in the atomic network they originally belong to.

To evaluate the effectiveness of our algorithm, we provide a comparison against a randomized algorithm that, at each iteration, interconnects two randomly selected networks through a pair of randomly selected nodes as well.

Due to the dimensionality of the problem, we first consider consider a (smaller) set $\mathcal{S} = \{s_1, \dots, s_n\}$ of n atomic dynamical networks ranging from $n = 2$ to $n = 7$, with $n_i \in [10, 20]$ and $\alpha = 3$, for which we compare our algorithm against the randomized one, and against the optimal solution as well computed through a brute force approach. Then, we consider a (larger) set $\mathcal{S} = \{s_1, \dots, s_n\}$ of n atomic dynamical networks ranging from $n = 10$ to $n = 50$, with a granularity of 10, for which we compare our algorithm against the randomized one only. In both cases, for each n, we generate 100 set of $\mathcal{S}$ networks.

Figure 5.3 shows the outcome for the first set of simulations, where the x-axis represents the number of networks involved and the y-axis represents the normalized ratio between the $\mathcal{H}_2$ norm of the composite network and the $\mathcal{H}_2$ norm of the optimal solution, i.e., $\mathcal{H}_2^{\text{opt}}$. In particular, both the mean value and the standard deviation over the 100 run were computed for both our algorithm and the randomized one. According

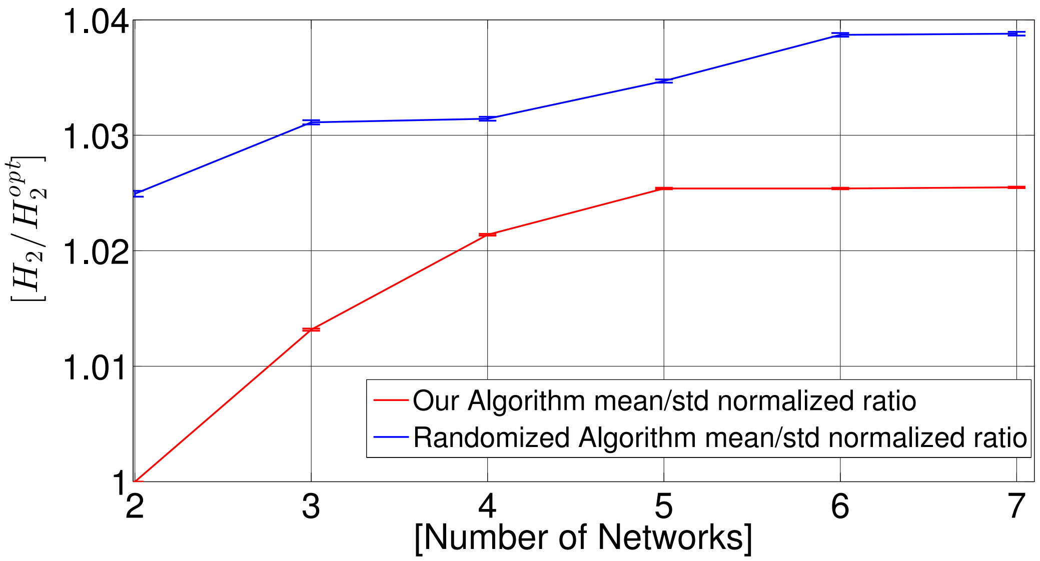


Figure 5.3 Simulation results for the first set (mean and standard deviation) over 100 run. The red lines represent the proposed algorithm, the randomized one is depicted in blue.

to the numerical results, our algorithm always provides a smaller gap with respected to the the optimal solution compared to the randomized one.

Figure 5.4 shows the outcome for the second set of simulations, where the x-axis represents again the number of networks involved whereas the y-axis represents in this case the normalized ratio between the $\mathcal{H}_2$ norm of the composite network and the $\mathcal{H}_2$ norm of the lower bound computed according to Theorem 5.3, i.e., $\mathcal{H}_2^{\mathcal{LB}}$. Also for this numerical evaluation, both the mean value and the standard deviation over the 100 run were computed for both our algorithm and the randomized one. According to the numerical results, also in this case our algorithm always provides a smaller gap with respected to the lower bound compared to the randomized one.

For the second set of simulations, Table 5.2 also provides the value of the upper bound computed according to Theorem 5.3. It can be noticed that the upper bound $\mathcal{UB}$ is not tight. This can be explained by the looseness of the bound given in Lemma 5.2 for the terms γ_{ij}.

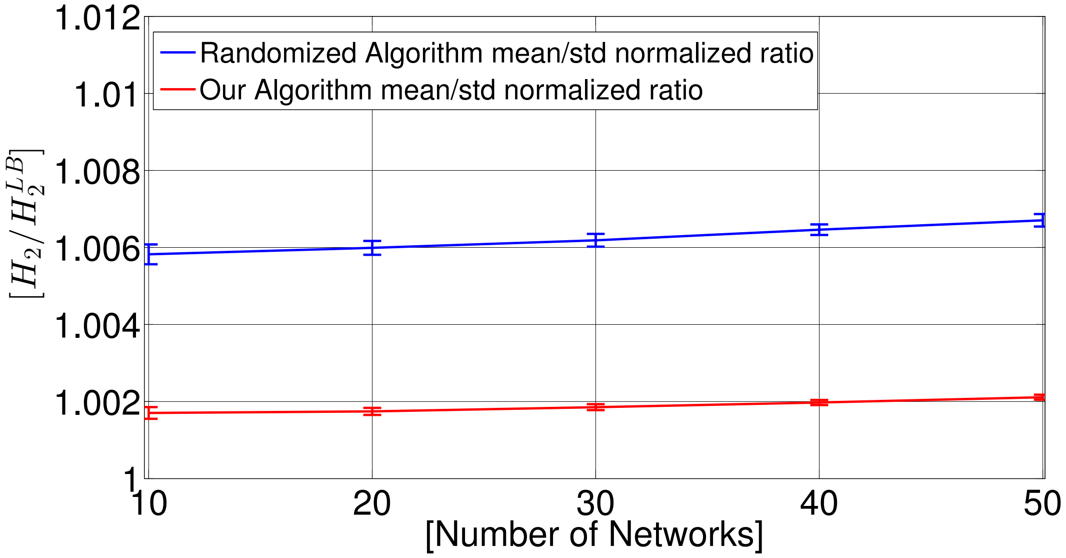


Figure 5.4 Simulation results for the second set (mean and standard deviation) over 100 set of $\mathcal{S}$ networks. The red lines represent the proposed algorithm, the randomized one is depicted in blue.

Table 5.2 Upper Bound for the second set of simulations.

Networks	10	20	30	40	50
Upp. Bound	1.464	1.492	1.498	1.506	1.509
Random	1.0058	1.0060	1.0062	1.0065	1.0067
Our	1.0017	1.0017	1.0019	1.0020	1.0021

5.3 Generalized Dynamical Model

As we said before, in this chapter we study the robustness properties of a dynamical network (i.e. a cyber-physical system) arising from the interconnections of multiple isolated components, with respect to the interconnection topology. In what follows, our aim is to generalize the model presented in Section 5.1.

To this aim, let $\mathcal{S} = \{s_1, \ldots, s_n\}$ be a set of n *atomic* dynamical networks, where the network s_i is identified by the *strongly connected* graph $\mathcal{G}_i = (\mathcal{V}_i, \mathcal{E}_i)$, with $|\mathcal{V}_i| = n_i$, and the weighted adjacency matrix A_i. Let $N = \sum_{i=1}^{n} n_i$. Notice that, because G_i is strongly connected, the matrix A_i is irreducible.

We assume that edges can be created within isolated networks, and across different network. In particular, due to the addition of edges, the weighted adjacency matrix of the *composite* network, that is, the network arising from the interconnection of the isolated components, read as

$$A = \underbrace{\begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & A_n \end{bmatrix}}_{A_D} + \underbrace{\begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & \ddots & & \vdots \\ \vdots & & \ddots & A_{n-1,n} \\ A_{n1} & \cdots & A_{n,n-1} & A_{nn} \end{bmatrix}}_{A_C}, \tag{5.9}$$

where A_D represents the local isolated dynamics, while A_C denotes the interconnection parameters. Let e_i denotes the i-th canonical vector of appropriate dimension. We make the following assumptions on the network matrix A:

Assumption 5.1. ***(Invertible network matrix)*** *The network matrix $A = [a_{ij}] \in \mathbb{R}^{n\times n}$ in* (5.9) *is a symmetric, irreducible and strictly diagonally dominant matrix. That is, $a_{ij} \leq 0 \ \forall i \neq j, 1 \leq i,j \leq N$ and $a_{ii} > 1 + \sum_{j=1}^{N} |a_{ij}|$.*

Assumption 5.1 implies that the network matrix A is an invertible M-matrix. Moreover, each diagonal network matrix A_i is also an invertible M-matrix. We say that the atomic networks s_i and s_j are interconnected if $|A_{ij}| = |A_{ji}| \neq 0$. We restrict our analysis to interconnection matrices satisfying the following assumption:

Assumption 5.2. ***(Interconnection matrix)*** *The weighted interconnection matrix A_C can be written as $A_C = U\Lambda V$, where UV can be expressed as*

$$\begin{aligned} U &= \begin{bmatrix} U_1 \cdots U_k \cdots U_m \end{bmatrix}, U_k = [e_{i_k} \quad e_{j_k}] \\ V &= -\begin{bmatrix} V_1 \cdots V_k \cdots V_m \end{bmatrix}^{\mathsf{T}}, V_k = [e_{j_k} \quad e_{i_k}]^{\mathsf{T}} \end{aligned} \tag{5.10}$$

for some indices $i_1, \dots, i_m, j_1, \dots, j_m \in \{1, \dots, N\}$*, with* $i_k \neq j_k$ *for all* $k \in \{1, \dots, m\}$ *where* e_{i_k}, e_{j_k} *are canonical vectors of appropriate dimension, and* $(i_k, j_k) \neq (i_\ell, j_\ell)$ *for all* $k, \ell \in \{1, \dots, m\}$*.*

Moreover, we can write Λ *as block-diagonal matrix, that is*

$$\Lambda = blkdiag(\Lambda_1 \cdots \Lambda_k \cdots \Lambda_m) \in \mathbb{R}^{m \times m} \tag{5.11}$$

Where each diagonal block read as

$$\Lambda_k = \varepsilon_k I_k, \quad \varepsilon_k \in (0, 1] \tag{5.12}$$

With I_k *identity matrix of appropriate dimension.*

It should be observed that Assumption 5.1 and Assumption 5.2 imply that the number of edges that can be added to any node is bounded. In particular, each node is allowed to create at most $\lceil a_{ii} \rceil - 1$ new connections.

In this chapter we study the robustness of the composite network with network matrix A, with respect to the interconnections A_C. In particular, we adopt the $\mathcal{H}_2$ system norm to quantify the robustness of a network system to external disturbances. Also with this general model, our analysis is restricted to the case where the disturbance affects each network node equally, and measurements are taken at every node. Thus, from Equation (5.2) the robustness of the composite network, considering the matrix A, is defined as

$$\mathcal{H}_2(A) = \text{Trace} \int_0^\infty e^{-2At} \, dt = \frac{1}{2} \text{Trace} \left(A^{-1} \right).$$

To design optimally robust composite, and connected, networks, we study the following minimization problem under Assumptions 5.1 and 5.2:

$$\begin{aligned} \min_{A_C} \quad & \operatorname{Trace}\left((A_D + A_C)^{-1}\right) \\ \text{s.t} \quad & A_D + A_C \text{ is irreducible.} \end{aligned} \tag{5.13}$$

5.3.1 Solution approach

Problem 5.13 can be solved by brute force approaches by enumerating all possible solutions. This kind of approaches result quite expensive in terms of computational load, due to the fact that the number of possible edge in the composite graph $\mathcal{G}(\mathcal{V}, \mathcal{E})$ scales quadratically with the number of nodes in $\mathcal{V}$. To overcome this fact, our study has been focused in finding several properties of the objective function, so that different solution approaches for Problem 5.13 can be proposed. In particular, exploiting the properties of the network matrix A (see Equation 5.9) several theoretical findings will be discussed.

The following lemma provides a formalization of the fact that $\operatorname{Trace}(A^{-1})$ is a monotonic increasing function of the interconnections U, V of A_C.

Lemma 5.3. ***(Trace Monotonicity)***

Let $A \in \mathbb{R}^{n \times n}$ be a symmetric, irreducible and strictly diagonally dominant matrix, with $a_{ij} \le 0 \; \forall i \ne j, 1 \le i, j \le N$ and $a_{ii} > 1 + \sum_{j=1}^{N} |a_{ij}|$. Let $U = [e_i \quad e_j]$ and $V = -[e_j \quad e_i]^T$ with $i \ne j$ and e_i, e_j canonical vectors of appropriate dimensions. Moreover, let $\Lambda = \varepsilon I \in \mathbb{R}^{2\times 2}$ with $\varepsilon \in (0, 1]$, then $\operatorname{Trace} A^{-1} < \operatorname{Trace}((A + U\Lambda V)^{-1})$.

Proof. Exploiting Lemma A.6 it is possible to express the argument of Trace $((A + U\Lambda V)^{-1})$ as

$$\begin{aligned} & A^{-1} - A^{-1}U\left(\Lambda^{-1} + VA^{-1}U\right)^{-1} VA^{-1} = \\ & = A^{-1} - A^{-1}U\left(\frac{I}{\varepsilon} + VA^{-1}U\right)^{-1} VA^{-1}. \end{aligned} \tag{5.14}$$

Where $\Lambda^{-1} = \frac{I}{\varepsilon}$. Expanding the product $(VA^{-1}U)$, due to the form of U, V we have:

$$\left(VA^{-1}U\right) = \begin{bmatrix} -a_{ji}^{-1} & -a_{jj}^{-1} \\ -a_{ii}^{-1} & -a_{ij}^{-1} \end{bmatrix}. \tag{5.15}$$

Notice that, being A a symmetric, irreducible and strictly diagonally dominant M-matrix thus from Lemma A.3 we know that the entries of (5.15) are negative. Moreover, by applying Theorem A.2, with $\frac{1}{\alpha} < 1$ due to $a_{ii} > 1 + \sum_{j=1}^{N} |a_{ij}|$ in A, and by noticing that $\|V\|_\infty = \|U\|_\infty = 1$, we have

$$\|VA^{-1}U\|_\infty \leq \|V\|_\infty \|A^{-1}\|_\infty \|U\|_\infty < 1 \tag{5.16}$$

Furthermore, remembering that $\Lambda = \varepsilon I$ we have by construction that

$$\|\Lambda^{-1}\|_\infty \geq 1. \tag{5.17}$$

Now, computing the sum $\left(\frac{I}{\varepsilon} + VA^{-1}U\right)$ we obtain:

$$\left(\frac{I}{\varepsilon} + VA^{-1}U\right) = \begin{bmatrix} \frac{1}{\varepsilon} - a_{ji}^{-1} & -a_{jj}^{-1} \\ -a_{ii}^{-1} & \frac{1}{\varepsilon} - a_{ij}^{-1} \end{bmatrix}. \tag{5.18}$$

It should be noticed that the matrix in (5.18) is irreducible and strictly diagonally dominant, and due to (5.16) and (5.17) also non singular. In particular, applying the Gershgorin circle theorem, we know that (5.18) is a non singular M-matrix and, exploiting Theorem A.4, we also know that its inverse has only positive entries. At this stage, applying the properties of the trace operator, we can write (5.14) as:

$$\begin{gathered}\operatorname{Trace}\left((A+U\Lambda V)^{-1}\right)=\operatorname{Trace}\left(A^{-1}\right)+\\ -\operatorname{Trace}\left(A^{-1}U\left(\frac{I}{\varepsilon}+VA^{-1}U\right)^{-1}VA^{-1}\right)\end{gathered}$$

Recalling that $V=-[e_j \quad e_i]^\mathsf{T}$ and by noticing that the terms $A^{-1}U$ and VA^{-1} do not change the sign of (5.18), it follows that:

$$-\operatorname{Trace}\left(A^{-1}U\left(\frac{I}{\varepsilon}+VA^{-1}U\right)^{-1}VA^{-1}\right)>0$$

Which in turn implies

$$\operatorname{Trace}\left(A^{-1}\right)<\operatorname{Trace}\left((A+U\Lambda V)^{-1}\right)$$

This concludes the proof. □

Note that, in our model, each individual weight of the interconnection described by $U=[e_i \quad e_j]$ and $V=[e_j \quad e_i]^T$ can be arbitrarily modified considering a different Λ matrix. We now provide a useful result for the objective function of Problem 5.13 which relates the monotonicity of $\operatorname{Trace}(A^{-1})$ respect a weight $w'>w$ for the same interconnection set.

Lemma 5.4. *Let $A\in\mathbb{R}^{n\times n}$ be a symmetric, irreducible and strictly diagonally dominant matrix, with $a_{ij}\le 0\ \forall i\neq j, 1\le i,j\le N$ and $a_{ii}>1+\sum_{j=1}^{N}|a_{ij}|$. Let $U=[e_i \quad e_j]$ and $V=-[e_j \quad e_i]^T$ with $i\neq j$ and e_i,e_j canonical vectors of appropriate dimensions. Moreover, let $\Lambda=\varepsilon I$ and $\Lambda'=\varepsilon' I\in\mathbb{R}^{2\times 2}$ with $\varepsilon,\varepsilon'\in(0,1]$, then* $\operatorname{Trace}((A+U\Lambda V)^{-1})>\operatorname{Trace}((A+U\Lambda' V)^{-1})$ *iff $\varepsilon>\varepsilon'$.*

Proof. We prove the Lemma by contradiction. Let us assume $\text{Trace}\left((A+U\Lambda V)^{-1}\right) < \text{Trace}\left((A+U\Lambda' V)^{-1}\right)$ and $\varepsilon > \varepsilon'$. Since $\varepsilon > \varepsilon'$ we can write $\varepsilon = \varepsilon' + \delta$, with $\delta \in (0,1]$ so that

$$\begin{aligned}\Lambda &= \varepsilon I\\ &= (\varepsilon' + \delta)I\\ &= \Lambda' I + \Lambda'' I.\end{aligned} \tag{5.19}$$

Now, substituting (5.19) in $\text{Trace}\left((A+U\Lambda V)^{-1}\right)$, we have

$$\begin{aligned}\text{Trace}\left((A+U\Lambda V)^{-1}\right) &= \text{Trace}\left((A+U(\Lambda'+\Lambda'')V)^{-1}\right)\\ &= \text{Trace}\left((A+U\Lambda' V+U\Lambda'' V)^{-1}\right)\\ &= \text{Trace}\left((A'+U\Lambda'' V)^{-1}\right).\end{aligned}$$

Where $A' = A + U\Lambda' V$.

At this stage, remembering that $\text{Trace}\left((A+U\Lambda V)^{-1}\right) < \text{Trace}\left((A+U\Lambda' V)^{-1}\right)$ we have

$$\text{Trace}\left((A'+U\Lambda'' V)^{-1}\right) < \text{Trace}\left(A'^{-1}\right). \tag{5.20}$$

However, exploiting Lemma 5.3 we know that (5.20) contradicts the hypothesis that $\text{Trace}\left((A+U\Lambda V)^{-1}\right) < \text{Trace}\left((A+U\Lambda' V)^{-1}\right)$. This concludes the proof. □

In addition to previous results, we also characterize the infimum of the optimization problem 5.13 in terms of the diagonal matrix A_D. In particular, analyzing the structure of the block diagonal matrix Λ, we have the following

Lemma 5.5. *Let Λ be a block-diagonal matrix such that $\Lambda = blkdiag(\Lambda_1, \cdots, \Lambda_k, \cdots, \Lambda_m)$, where $\Lambda_k = \varepsilon_k I_k$ with $\varepsilon_k \in (0, 1]$ and I_k identity matrix of appropriate dimensions, then* $\lim_{\varepsilon_i \to 0} \Lambda_i = 0 \quad \forall i = 1, \cdots, m$.

Proof. From Lemma 5.4 we know that a continuity among all the possible ε_i in each block Λ_i exists so, proceeding with the limit operation on a single block, we have

$$\lim_{\varepsilon_i \to 0} \Lambda_i = 0 \tag{5.21}$$

At this stage, applying iteratively (5.21) on each block, we obtain

$$\lim_{\varepsilon_i \to 0} \Lambda_i = 0, \forall i = 1, \cdots, m.$$

This concludes the proof. □

We are now ready to state the following theorem, which provide the expression of the infimum of Problem 5.13.

Theorem 5.4. ***(Infimum of Problem 5.13)***

Let $\mathrm{Trace}\left((A_D + A_C)^{-1}\right)$ *be the objective function of the minimization problem (5.13) and let $A_C = U\Lambda V$ as in Assumption 2, then* $\mathrm{Trace}\left(A_D^{-1}\right)$ *is the infimum of the problem.*

Proof. From Assumption 2 we have $A_C = U\Lambda V$, with $U, V \neq 0$ and $\Lambda = blkdiag(\Lambda_1, \cdots, \Lambda_k, \cdots, \Lambda_m)$.Exploiting Lemma 5.5 on Λ in A_C, the results follows. □

For a network topology design problem, characterizing the expression of the optimal solution, in terms of the number of links among the nodes of the overall interconnected system, is a quite challenging task. Thanks to the properties of the objective function we formalized before, we are now ready to state the following theorem, which relates the optimal solution to a specific topology of the composite system.

Theorem 5.5. ***(Optimal interconnection)*** *Let $A_C^* = U^*\Lambda^*V^* \in \mathbb{R}^{n\times n}$ be a solution of the minimization problem* (5.13)*. Let $U^* = [U_1 \cdots U_m]$, $V^* = -[V_1 \cdots V_m]$ and $\Lambda^* = blkdiag(\Lambda_1 \cdots \Lambda_k \cdots \Lambda_m) \in \mathbb{R}^{m\times m}$ as defined in Assumption 5.2, then $m = n-1$.*

Proof. We prove the theorem by contradiction. Let $A = A_D + U^*\Lambda^*V^* \in \mathbb{R}^{n\times n}$ with $U^* = [U_1 \cdots U_m]$, $V^* = -[V_1 \cdots V_m]$ and $\Lambda^* = blkdiag(\Lambda_1 \cdots \Lambda_k \cdots \Lambda_m) \in \mathbb{R}^{m\times m}$. By noticing that A_D is composed by n distinct block, we need $m \geq n-1$ in U^*, V^* and Λ^* to ensure that A is irreducible. So, let $m = n-1+k$, with $k \in \mathcal{Z}_{>0}$. At this point, by construction it is always possible to find two subsets $U' \subset U^*$ and $V' \subset V^*$ where $U' = [U_1 \cdots U_{m'}]$, $V' = -[V_1 \cdots V_{m'}]$ with $\Lambda' = blkdiag(\Lambda_1 \cdots \Lambda_k \cdots \Lambda_{m'}) \in \mathbb{R}^{m'\times m'}$ and $m' = n-1$, such that the matrix $A' = A_D + U'\Lambda'V'$ is irreducible. Therefore, from Lemma 5.3 it follows that

$$\text{Trace}\left(A'^{-1}\right) < \text{Trace}\left(A^{-1}\right),$$

which contradicts the fact that A is the optimal solution of the minimization problem (5.13). It follows that it must be $m = m' = n-1$. This concludes the proof.

□

Given a node set $\mathcal{V} = \{1, \cdots, n\}$ and weights $w_e \geq 0$ associated with each edge $e \in \mathcal{V}\times\mathcal{V}$, our goal is to find an edge set $\mathcal{E}_c$ such that the undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}_c)$ is a connected tree with minimum Trace $\left(A_{\mathcal{E}_c}^{-1}\right)$. It is worth noticing that, each $v_i \in \mathcal{V}$ could be a simple node or a more complex virtual node (i.e. a dynamical network itself). Hence, thanks to previous results we can restate the optimization problem 5.13 as

$$\begin{aligned} \min_{\mathcal{E}_c} \quad & \text{Trace}\left(A_{\mathcal{E}_c}^{-1}\right), \\ \text{s.t} \quad & \mid \mathcal{E}_c \mid = n-1, \\ & A_{\mathcal{E}_c} \text{ is irreducible.} \end{aligned} \tag{5.22}$$

The following Greedy algorithm can be used as a heuristic to solve problem 5.22

Algorithm 1: Greedy Tree

```
Input  : $[\mathcal{V}, w_e \forall e \in \mathcal{V}\times\mathcal{V}]$
Output : $\mathcal{T}$ Tree with small trace
$\mathcal{E} \leftarrow \{argmax_{e\in\mathcal{V}\times\mathcal{V}} \quad w_e\}$;
$\bar{\mathcal{V}} \leftarrow \{i, j \mid (i,j) \in \mathcal{E}\}$;
while $\mid \mathcal{E} \mid \leq n-1$ do
    $\bar{\mathcal{E}} =\leftarrow \Big\{(i,j) \mid (i,j) \in \mathcal{V}\times\mathcal{V}\setminus\mathcal{E}, (i,j)\cap\bar{\mathcal{V}} \neq \emptyset\Big\}$;
    $e = argmin_{e\in\bar{\mathcal{E}}}\, \text{Trace}\Big((A_{\mathcal{E}\cup e})^{-1}\Big)$;
    if $A_{\mathcal{E}\cup e}$ is strictly diagonally dominant then
        $\mathcal{E} \leftarrow \mathcal{E} \cup e$;
        $\bar{\mathcal{V}} \leftarrow \bar{\mathcal{V}} \cup \{i, j \mid e = (i,j)\}$;
    end
end
```

Conclusion and Future Work

One fundamental challenge for modern Cyber-Physical Systems is to ensure correct and reliable functionality in the face of failures and attacks. This thesis concerns on (i) proposing a new approach for the diagnosis of faults and threats in Cyber-Physical Systems through Evidence Theory, (ii) presenting an innovative framework for managing and evaluating risk in complex systems after cyber-physical attacks, (iii) characterizing the robustness of a Cyber-Physical Systems, viewed as interconnected network systems, with respect the interconnection topology.

Summary

In **Chapter 1** and in **Chapter 2** we introduced the basic concepts and the notation related, respectively, to Graph Theory and to Evidence Theory.

In **Chapter 3** we applied Evidence Theory to diagnose faults in a Cyber-Physical Systems. In particular, we considered as case study a Smart Grid. We showed that classical approaches, based on Dempster-Shafer model, are somewhat restrictive and a better way to represent the knowledge model is mandatory. Moreover, redefine the frame of discernment explicitly considering Dezert-Smarandache model, brings high computational overhead in the fusion process due to the cardinality of the hyper power set. As a solution, we proposed a hybrid knowledge model based on a specific frame of discernment and a diagnosis metric is presented, with the aim of improving the detection of the cyber-physical attacks in Smart Grids.

In **Chapter 4** we presented an innovative framework for managing and evaluating risk in complex systems. For those systems, the tight interconnection between cyber and physical layers leads to an integrate analysis of risk, considering information and data coming from both fields. Also in this case Evidence Theory, tied with Graph Theory, turned out to be a powerful tool. In particular, we provided theoretical findings for both the evaluation of risk over the frame of discernment and for the definition of BPA functions over the power set. We applied our framework on a complex Cyber-Physical System composed of a Medium Voltage Power Grid controlled by a Supervisory Control And Data Acquisition system. Through the proposed framework, it is possible to drastically decrease the high computational load of Evidence Theory algorithms, that was until now one of its major drawback.

In **Chapter 5** we characterized the robustness of a Cyber-Physical System, viewed as an interconnected network system, as a function of the interconnection topology. Taking into account networks with Laplacian-based dynamics, we gather that interconnected networks are always less robust than the isolated components. Further, we showed that interconnections among nodes of the atomic components with highest degree yield maximum robustness. Then, we proposed an interconnection rule for the design of robust composite networks, and validated its effectiveness through simulations. Finally we generalized the proposed model, using the class of M- matrices and their inverses. The problem of finding the optimal robust network structure was analyzed as an optimization problem: we found several properties of the objective function and we also characterized the expression of the optimal solution.

Future Work

In this thesis, we have studied various approaches for model, protect and control Cyber-Physical Systems (CPSs). Based on our methods, we have proposed a new way to detect threats for Cyber-Physical systems through Evidence Theory, managing risk after cyber physical attacks and characterize the robustness of networked CPSs. However, while this research has solved many security problems for Cyber-Physical Systems, it has raised new questions. We next discuss some aspects requiring future investigation.

Regarding the application of the Evidence Theory with the hybrid power set in Cyber-Physical Systems, our research is currently focusing on generalizing the BPA assignment for different cyber-attacks seek to inflict physical damage. An interesting direction, is to study the theoretical properties of the hybrid power set, in order to integrate both the properties of the classical framework and of the Dezert-Smarandache approach.

For the case of risk assessment, we assumed that the risk scale can be represented as a path graph. The obtained results, based on the graph theoretic approach, encourage the authors to study hierarchical aggregation methods in order to generalize the analysis to different graph topologies and to heterogeneous case studies.

Finally, on the robustness of networked Cyber-Physical Systems, several directions are left for future work. Among the others, extending the approach to general network dynamics with different nodes feature and different interconnection capabilities is a quite interesting topic. Moreover, by considering the attacks in the resulting networks, it would be interesting to understand possible limitation in the proposed mathematical model.

Bibliography

[1] E. A. Lee, "Cyber physical systems: Design challenges," in *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, May 2008, pp. 363–369.

[2] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," *System*, vol. 1, no. a2, p. a3, 2008.

[3] R. Poovendran, "Cyber–physical systems: Close encounters between two parallel worlds [point of view]," *Proceedings of the IEEE*, vol. 98, no. 8, pp. 1363–1366, 2010.

[4] L. Miclea and T. Sanislav, "About dependability in cyber-physical systems," in *2011 9th East-West Design Test Symposium (EWDTS)*, Sept 2011, pp. 17–21.

[5] E. Bartocci, O. Hoeftberger, and R. Grosu, "Cyber-physical systems: theoretical and practical challenges," *ERCIM News*, vol. 2014, no. 97, 2014.

[6] F. Pasqualetti, R. Carli, A. Bicchi, and F. Bullo, "Identifying cyber attacks via local model information," in *Decision and Control (CDC), 2010 49th IEEE Conference on.* IEEE, 2010, pp. 5961–5966.

[7] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[8] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," *IEEE Control Systems*, vol. 35, no. 1, pp. 110–127, 2015.

[9] F. Pasqualetti and Q. Zhu, "Design and operation of secure cyber-physical systems," *IEEE Embedded Systems Letters*, vol. 7, no. 1, pp. 3–6, 2015.

[10] B. Bollobás, *Modern graph theory.* Springer Science & Business Media, 2013, vol. 184.

[11] M. Mesbahi and M. Egerstedt, *Graph theoretic methods in multiagent networks.* Princeton University Press, 2010.

[12] M. Fiedler, "Algebraic connectivity of graphs," *Czechoslovak mathematical journal*, vol. 23, no. 2, pp. 298–305, 1973.

[13] ——, “Laplacian of graphs and algebraic connectivity,” *Banach Center Publications*, vol. 25, no. 1, pp. 57–70, 1989.

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

[15] A. P. Dempster, “Upper and lower probabilities induced by a multivalued mapping,” *The annals of mathematical statistics*, pp. 325–339, 1967.

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

[17] S. K. Das, *High-level data fusion.* Norwood, MA, USA: Artech House Publishers, 2008.

[18] F. Smarandache and J. Dezert, *Advances and Applications of DSmT for Information Fusion (Collected works), second volume: Collected Works.* Infinite Study, 2006, vol. 2.

[19] D. Dubois and H. Prade, “A set-theoretic view of belief functions,” in *Classic Works of the Dempster-Shafer Theory of Belief Functions.* Springer, 2008, pp. 375–410.

[20] ——, “Representation and combination of uncertainty with belief functions and possibility measures,” *Computational Intelligence*, vol. 4, no. 3, pp. 244–264, 1988.

[21] R. R. Yager, “On the dempster-shafer framework and new combination rules,” *Information sciences*, vol. 41, no. 2, pp. 93–137, 1987.

[22] J. Dezert and F. Smarandache, “Dsmt: A new paradigm shift for information fusion,” *arXiv preprint cs/0610175*, 2006.

[23] D. Wiedemann, “A computation of the eighth dedekind number,” *Order*, vol. 8, no. 1, pp. 5–6, 1991.

[24] F. Smarandache and J. Dezert, “Advances and applications of dsmt for information fusion-collected works-volume 3,” 2009.

[25] M. Burmester, E. Magkos, and V. Chrissikopoulos, “Modeling security in cyber–physical systems,” *International Journal of Critical Infrastructure Protection*, vol. 5, no. 3, pp. 118–126, 2012.

[26] B. Genge and C. Siaterlis, “Developing cyber-physical experimental capabilities for the security analysis of the future smart grid,” in *Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on.* IEEE, 2011, pp. 1–7.

[27] F. Pasqualetti, F. Dörfler, and F. Bullo, “Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design,” in *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on.* IEEE, 2011, pp. 2195–2201.

[28] F. Pasqualetti, A. Bicchi, and F. Bullo, "A graph-theoretical characterization of power network vulnerabilities," in *American Control Conference (ACC), 2011*. IEEE, 2011, pp. 3918–3923.

[29] F. Dörfler, F. Pasqualetti, and F. Bullo, "Distributed detection of cyber-physical attacks in power networks: A waveform relaxation approach," in *Communication, Control, and Computing (Allerton), 2011 49th Annual Allerton Conference on*. IEEE, 2011, pp. 1486–1491.

[30] C. M. Krishna and I. Koren, "Adaptive fault-tolerance fault-tolerance for cyber-physical systems," in *Computing, Networking and Communications (ICNC), 2013 International Conference on*. IEEE, 2013, pp. 310–314.

[31] O. Basir and X. Yuan, "Engine fault diagnosis based on multi-sensor information fusion using dempster–shafer evidence theory," *Information Fusion*, vol. 8, no. 4, pp. 379–386, 2007.

[32] X. Fan and M. J. Zuo, "Fault diagnosis using multi-source information fusion," in *2006 9th International Conference on Information Fusion*. IEEE, 2006, pp. 1–6.

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

[34] T. M. Inc., "Matlab version 8.0.0." *Natick*, 2014.

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

[36] J. Helton, J. Johnson, and W. Oberkampf, "An exploration of alternative approaches to the representation of uncertainty in model predictions," *Reliability Engineering & System Safety*, vol. 85, no. 1–3, pp. 39 – 71, 2004. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0951832004000511

[37] G. W. Parry, "The characterization of uncertainty in probabilistic risk assessments of complex systems," *Reliability Engineering & System Safety*, vol. 54, no. 2–3, pp. 119 – 126, 1996, treatment of Aleatory and Epistemic Uncertainty. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0951832096000695

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

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

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

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

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

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

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

[45] D. Ehrenreich, "Automatic fault isolation and system restoration in mv networks," Motorola Inc., Tech. Rep.

[46] "Cisiapro agent-based critical insfrastructure simulator," http://cisiapro.dia.uniroma3.it/.

[47] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.

[48] S. Skogestad and I. Postlethwaite, *Multivariable Feedback Control Analysis and Design*, 2nd ed. John Wiley & Sons, 2005.

[49] A. Chapman, E. Schoof, and M. Mesbahi, "Distributed online topology design for network-level disturbance rejection," in *Decision and Control (CDC), 2013 IEEE 52nd Annual Conference on*.

[50] A. Chapman and M. Mesbahi, "Semi-autonomous consensus: network measures and adaptive trees," *IEEE Transactions on Automatic Control*, vol. 58, no. 1, pp. 19–31, 2013.

[51] J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Robustness of a network of networks," *Phys. Rev. Lett.*, vol. 107, no. 19, 2011.

[52] T. Peixoto and S. Bornholdt, "Evolution of robust network topologies: Emergence of central backbones," *Phys. Rev. Lett.*, vol. 109, no. 11, 2012.

[53] S. Gomez, A. Diaz-Guilera, J. Gomez-Gardeñes, C. J. Perez-Vicente, Y. Moreno, and A. Arenas, "Diffusion dynamics on multiplex networks," *Phys. Rev. Lett.*, vol. 110, no. 2, 2013.

[54] M. De Domenico, A. Solé-Ribalta, E. Cozzo, M. Kivelä, Y. Moreno, M. Porter, S. Gómez, and A. Arenas, "Mathematical formulation of multilayer networks," *Phys. Rev. X*, vol. 3, no. 4, 2014.

[55] A. Gutfraind, "Optimizing network topology for cascade resilience," in *Handbook of Optimization in Complex Networks.* Springer, 2012.

[56] C. D. Godsil and G. F. Royle, *Algebraic Graph Theory*, ser. Graduate Texts in Mathematics. Springer, 2001, vol. 207.

[57] C. D. Meyer, *Matrix Analysis and Applied Linear Algebra.* SIAM, 2001.

[58] J. Varah, "A lower bound for the smallest singular value of a matrix," *Linear Algebra and its Applications*, vol. 11, no. 1, pp. 3 – 5, 1975.

[59] R. A. Horn, *Topics in Matrix Analysis.* New York, NY, USA: Cambridge University Press, 1986.

[60] A. Berman and R. J. Plemmons, *Nonnegative Matrices in the Mathematical Sciences (Classics in Applied Mathematics).* Society for Industrial Mathematics, Jan. 1987.

[61] M. A. Woodbury, *Inverting Modified Matrices*, ser. Statistical Research Group Memorandum Reports. Princeton, NJ: Princeton University, 1950, no. 42.

Publications

[1] R. Santini, C. Foglietta, and S. Panzieri, "Evidence theory for smart grid diagnostics," in *IEEE PES ISGT Europe 2013.* IEEE, 2013, pp. 1–5.

[2] ——, "Evidence theory for cyber-physical systems," in *International Conference on Critical Infrastructure Protection.* Springer, 2014, pp. 95–109.

[3] ——, "A graph-based evidence theory for assessing risk," in *Information Fusion (Fusion), 2015 18th International Conference on.* IEEE, 2015, pp. 1467–1474.

[4] C. Foglietta, C. Palazzo, R. Santini, and S. Panzieri, "Assessing cyber risk using the cisiapro simulator," in *International Conference on Critical Infrastructure Protection.* Springer, 2015, pp. 315–331.

[5] R. Santini, A. Gasparri, F. Pasqualetti, and S. Panzieri, "Network composition for optimal disturbance rejection," in *2016 American Control Conference (ACC)*, July 2016, pp. 3764–3769.

[6] R. Fratini, R. Santini, J. Serafini, M. Gennaretti, and S. Panzieri, "A spatial repetitive controller applied to an aeroelastic model for wind turbines," *World Academy of Science, Engineering and Technology, International Journal of Mechanical, Aerospace, Industrial, Mechatronic and Manufacturing Engineering*, vol. 10, no. 9, pp. 1615–1623, 2016.

[7] R. Santini, A. Gasparri, F. Pasqualetti, and S. Panzieri, "From graphs to trees: Optimal topology design for network robustness," *Automatica (submitted).*

[8] C. Foglietta, C. Palazzo, R. Santini, T. Cruz, L. Lev, and S. Panzieri, "From detecting cyber attacks to mitigating risk within a hybrid environment," *Special Issue of Journal of Computer and System Sciences (submitted).*

Appendix A

Basic Linear Algebra Results

In this section some basic results from Linear Algebra, required for the development of the proofs, are given.

Linear Algebra

Lemma A.1. ***(Positive definite matrices)*** *Let $A \in \mathbb{R}^{n\times n}$ be a positive definite matrix and let A^{-1} be its inverse. Then*

$$A(i,i)\, A^{-1}(i,i) \geq 1, \quad \forall\, i \in \mathcal{V}$$

Furthermore, let λ_1 be the least, λ_n the largest eigenvalue of A, $\gamma = \lambda_n/\lambda_1$. Then

$$\gamma^{1/2} + \gamma^{-1/2} \geq 2 \max_{i=1,\dots,n} \Big(A(i,i)A^{-1}(i,i)\Big)^{1/2}.$$

Lemma A.2. ***(Varah's Bound)*** *If A is a strictly diagonally dominant matrix and set $\alpha = \min_i\{a_{ii} - \sum_{i\neq j}|a_{ij}|\}$, then*

$$\|A^{-1}\|_\infty \leq \frac{1}{\alpha}.$$

In addition, the following results on M-matrix hold [59] and [60]:

Lemma A.3. ***(Element-wise dominance Inverse of M-Matrix)*** *Let A be an irreducible, symmetric, and strictly diagonally dominant M-matrix, then A^{-1} is a symmetric entrywise positive matrix and*

$$A^{-1}(i,i) > A^{-1}(i,j),\ \forall\, i,j \in \mathcal{V}\ :\ i \neq j.$$

Lemma A.4. ***(Inverse of M-Matrix properties)*** *If A is a non singular $M-$ matrix, then $A^{-1} \succeq 0$. Moreover, if A is irreducible, then $A^{-1} \succ 0$.*

The following result concerns the inversion of the sum of two matrices holds:

Lemma A.5. ***(Sherman–Morrison formula)*** *Suppose A is an invertible square matrix and u, v are vectors. Suppose furthermore that $1 + v^T A^{-1} u \neq 0$. Then*

$$(A + uv^T)^{-1} = A^{-1} - \frac{A^{-1}uv^T A^{-1}}{1 + v^T A^{-1} u},$$

where uv^T is the outer product of two vectors u and v.

Finally, the following result concerning a rank-k correction of some matrix holds [61]:

Lemma A.6. ***(Woodbury Formula)*** *Suppose A is an invertible square matrix and U, V and C be any (dimensionally compatible) matrices, then*

$$(A + UCV)^{-1} = A^{-1} - A^{-1}U\left(C^{-1} + VA^{-1}U\right)^{-1} VA^{-1}. \tag{A.1}$$

In the special case where $C = I$ (A.1) read as

$$(A + UV)^{-1} = A^{-1} - A^{-1}U\left(I + VA^{-1}U\right)^{-1} VA^{-1}. \tag{A.2}$$