République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mohamed Khider – Biskra

N° D'ordre : ……..

Série : ……..

Faculté des Sciences Exactes et Sciences de la Nature et de la Vie
Département d'Informatique

THESE

Présentée pour obtenir le grade de
DOCTORAT DE TROISIEME CYCLE EN INFORMATIQUE
Option : Intelligence Artificielle
Par

Yasser Moussa BERGHOUT

THEME

Probabilistic Model-Based Diagnosis of Distributed Systems

Devant le jury composé de :

Mr. Okba KAZAR	Professeur à l'Université de Biskra	Président
Mr. Hammadi BENNOUI	Maitre de conférences A à l'Université de Biskra	Rapporteur
Mr. Allaoua CHAOUI	Professeur à l'Université de Constantine 2	Examinateur
Mr. Djamel-Eddine SAIDOUNI	Professeur à l'Université de Constantine 2	Examinateur
Mr. Laid KAHLOUL	Maitre de conférences A à l'Université de Biskra	Examinateur

People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
Mohamed Khider University - Biskra

Order Number: ……..

Series : ……..

Faculty of Exact Sciences and Sciences of Nature and Life
Computer Science department

THESIS

Submitted in partial fulfillment of the
requirements for the degree of
DOCTORATE OF THE THIRD CYCLE IN COMPUTER SCIENCE
Option: Artificial Intelligence

By

Yasser Moussa BERGHOUT

TITLE

Probabilistic Model-Based Diagnosis of Distributed Systems

In front of the jury composed of:

Mr. Okba KAZAR	Professor at the University of Biskra	President
Mr. Hammadi BENNOUI	Associate Professor at the University of Biskra	Supervisor
Mr. Allaoua CHAOUI	Professor at the University of Constantine 2	Examiner
Mr. Djamel-Eddine SAIDOUNI	Professor at the University of Constantine 2	Examiner
Mr. Laid KAHLOUL	Associate Professor at the University of Biskra	Examiner

Probabilistic Model-Based Diagnosis of Distributed Systems

by

Yasser Moussa BERGHOUT

Abstract

This thesis addresses the problem of modeling uncertainty in the distributed context. It is situated in the field of diagnosis; more precisely, model-based diagnosis of distributed systems. A special focus is given to modeling uncertainty using probabilistic and possibilistic reasoning. Thus, for its first contribution, this work is based on a probabilistic modeling formalism called: “probability propagation nets" (PPNs), which is designed for centralized systems. Hence, an extension of this model is proposed to suit the distributed context. Distributed probability propagation nets (DPPNs), the proposed extension, were conceived to consider the distributed systems’ particularities. So, the set we consider is a set of interacting subsystems, each of which is modeled by a DPPN. The interaction among the subsystems is modeled through the firing of common transitions belonging to more than one subsystem. Moreover, the diagnostic process is done by exploiting transition-invariants; a diagnostic technique developed for Petri nets.

Furthermore, and as a second contribution, we exploit another theory to model uncertainty; that is the theory of possibility. In fact, another class of Petri nets called “Possibilistic Petri nets" (PoPNs) captures the possibilistic behavior of a process. Possibility measures are attached to each obtained diagnosis as a quantifiable basis regarding its uncertainty. It is possible to use such measures to detect some inconsistencies within the diagnoses.

Thesis Supervisor: Hammadi Bennoui
Title: Associate Professor

Acknowledgments

I have a lot to be thankful for in my life, and this shared few lines are for some of it, especially regarding the people who helped in the accomplishment of this thesis. Special thanks go to my advisor Dr. Hammadi Bennoui, for his help and support. After more than three years of working with him, the first word that comes to mind when describing him is "*cool*." I would also like to thank Pr. Okba Kazar, Pr. Allaoua Chaoui, Pr. Djamel-Eddine Saidouni, and Dr. Laid Kahloul for reviewing and evaluating this thesis.

Pursuing a doctorate would have never been an option without the full support that I got from my parents in particular and my family in general from the very beginning, and if I owe anyone the accomplishments made in my life, it is them. The journey to a doctorate is a long ride, and having my friends along that ride made it more appreciated. So, to all these amazing people who went with me along this journey, I sincerely thank you.

Contents

1 Introduction **15**

1.1 Pillars of the Thesis . . . 15

1.2 Motivation . . . 16

1.3 Problem statement . . . 17

1.4 Thesis Organization . . . 18

2 Model-Based Diagnosis **21**

2.1 Introduction . . . 21

2.2 Overview on Model-based Diagnosis . . . 23

2.2.1 Terminology . . . 24

2.2.2 Diagnosis from First Principles . . . 25

2.3 Causal Models . . . 27

2.4 Petri Nets . . . 29

2.4.1 General view . . . 29

2.4.2 Formal Definition . . . 29

2.4.3 Diagnostic Scheme with Petri Nets . . . 29

2.4.4 Literature Review on Centralized Diagnosis with Petri Nets . . . 30

2.5 Distributed Systems . . . 30

2.5.1 General Perception & Classification . . . 30

2.5.2 Examples of Computer Architectures of Distributed Systems . . . 32

2.5.3 Literature Review on Distributed/Decentralized Diagnosis . . . 33

2.6 Assumptions in Model-based Diagnosis . . . 34

2.7 Conclusion . . . 35

3 Uncertainty & Petri Nets **37**

3.1 Introduction . . . 37

3.2 Reasoning under Uncertainty . . . 38

3.3 Literature Review on Uncertainty in Diagnosis . . . 39

3.4 Bayesian Networks and Petri Nets . . . 40

3.4.1 Bayesian Networks . . . 40

3.4.2 Probability Propagation Nets . . . 41

3.5 Possibility Theory and Petri Nets . . . 47

3.5.1 Possibility Theory . . . 47

3.5.2 Possibilistic Petri Nets . . . 49

3.6 Conclusion . . . 54

4 Distributed Probability Propagation Nets & Diagnosis **55**

4.1 Introduction . . . 55

4.2 System Setting . . . 57

4.2.1 System Description . . . 57

4.2.2 Hierarchical Perception . . . 59

4.3 Distributed Probability Propagation Nets . . . 60

4.4 Diagnostic Reasoning Scheme . . . 63

4.4.1 Centralized diagnosis . . . 65

4.4.2 New evidence & inconsistency . . . 67

4.4.3 Local diagnosis . . . 69

4.4.4 Distributed diagnosis . . . 70

4.5 Discussion . . . 76

4.6 Conclusion . . . 77

5 Distributed Diagnosis with Possibilistic Petri Nets **79**

5.1 Introduction . . . 79

5.2 Centralized Diagnosis (Formalization) . . . 81

5.3 Distributed Diagnosis . . . 86

5.3.1 Motivation . . . 86

5.3.2 System Model 86
5.3.3 The DP Projection on PoPNs 88
5.3.4 Cooperation Protocol 88
5.3.5 Diagnoses Computation 90
5.3.6 Proof of Correctness 95
5.4 Conclusion 96

6 Conclusion **97**

List of Figures

2-1 A full adder. 27
2-2 A causal network model. 28
2-3 A diagnostic process architecture. 31

3-1 Bayesian network. 41
3-2 Probability propagation net. 46
3-3 A simple example of a PoPN. 50
3-4 Possible worlds for possible information. 51
3-5 A semantic tree. 52

4-1 An abstract architecture of a distributed system. 58
4-2 Common component capturing interaction between two subsystems. 58
4-3 Hierarchy of the system's abstraction. 59
4-4 Two interacting subsystems. 64
4-5 A probability propagation net model of a faulty behavior of a car. 68
4-6 Two interacting subsystems with an inter-loop. 72
4-7 Two interacting subsystems. 75

5-1 A simple example of a faulty behavior of a car. 84
5-2 Two agents communicating. 90
5-3 An example of an open PoPN. 91

List of Tables

2.1 Model-based strategies vs experience-based strategies [81]. 24

3.1 Possibility and probability distributions associated with X. 47
3.2 Truth values of possible worlds. 51

4.1 States and their description. 65
4.2 Probabilities associated to transitions for the first subsystem. 65
4.3 Probabilities associated to transitions for the second subsystem. 65
4.4 T-invariants of the first subsystem. 66
4.5 T-invariants of the second subsystem. 66
4.6 Probabilities associated to transitions of the PPN model. 67
4.7 T-invariants of the of the PPN model. 67
4.8 Probabilities associated to transitions for the first subsystem S_1. 74
4.9 Probabilities associated to transitions for the second subsystem S_2. 76
4.10 T-invariants of the first subsystem S_1. 76
4.11 T-invariants of the second subsystem S_2. 76

5.1 States and their faulty values. 83
5.2 Possibilities associated to transitions of Example 5. 85
5.3 States and their description. 92
5.4 Possibilities associated to transitions of Example 6. 92
5.5 Minimal supports P-invariants of S_1. 93
5.6 Minimal supports P-invariants of S_2. 93

Chapter 1

Introduction

Systems, in their general definition, are prone to fail at a certain point of their existence. When that happens, detecting the source leading to the failure could be very crucial to get the system back to its well-functioning state. From here the importance of diagnosis arises. It represents the procedure followed to detect the source of any failure. Model-based diagnosis is an approach developed for a high level of abstraction diagnostic schemes. It pre-assumes the existence of a model describing the "normal" behavior of a system with a possibility to observe some of its outputs. Roughly speaking, it considers the inconsistency between the observations and the normal behavior described by the system model as a sign of a malfunction.

1.1 Pillars of the Thesis

The three big pillars on which this thesis is constructed are:

- Model-based diagnosis: the core of the thesis and its main purpose, the other two pillars are just like constraints on the performed diagnosis. This approach is mostly developed and used by computer scientists (mainly artificial intelligence and formal methods communities). It assumes the relevance of a system model to perform the required task.

- Uncertainty treatment: a more realistic modeling approach to diagnosis (or any other

procedure) should adopt an uncertainty quantification formalism that actually represents the flaws of a non-perfect system. As to our subject matter, diagnosis is known to have its flaws and ambiguity, since multiple faults could share considerably resembling symptoms (if not the exact same ones) which make it quite difficult to distinguish between them. A probabilistic approach to diagnosis would offer a ranking feature among the possible solutions.

- Distribution of the solution: the complexity of some systems nowadays is so immense that having them under a centralized controller is so complicated (if not impossible). To overcome such complexity, it is better to divide them into more controllable units, following the paradigm of "divide and conquer," which inspires the necessity to develop distributed solutions that go with them. Such complexity is even predicted to get greater in the future.

1.2 Motivation

To highlight the use of a distributed approach, let us quote here Su and Wonham [105]: "*It is well known that centralized approaches suffer from high space complexity (i.e., model size), which may be a problem also for those decentralized approaches which rely on an intermediate centralized plant model. For this reason attention has turned increasingly to distributed approaches*." In this view, distributed approaches to diagnosis offer a convenient solution the problem of high space complexity in centralized models, and even decentralized ones.

"*Surprisingly, very little work has been done in the area of distributed fault localization*" is another quote from a 2004 survey on fault localization techniques in computer science [64] highlighting the lack of sufficient work treating such a field. Nevertheless, since then numerous research papers have taken this issue into consideration, but it was not representative of the importance of the subject. Another survey in 2015 still does not have much to mention [40] in this regard, even though the authors have missed some important work that shall be mentioned within the course of this thesis. One of the problems regarding distributed approaches is the complexity of their contexts, which makes it hard to maintain

relevant knowledge about a system's state. One more quote from this last reference [40] shall emphasize more the relevance of this course of research: "*This kind of decentralized or distributed structure has become the mainstream in complex industrial processes owing to its less use of network resources, cost effectiveness, and convenience for expansion*."

The contributions of this thesis treat the mentioned three points. We use initially a probabilistic model based on Petri nets called "probability propagation nets" (PPNs) to capture the underlying uncertainty within the diagnostic model. PPNs, as they are defined, do not well suit the system setting of distributed systems. Thus, to adapt it to the considered setting, we suggest distinguishing the "input" and "output" components (that characterize the distributed setting) as separated entities in the model. To do so, we extend PPNs to what we call "distributed probability propagation nets" that make such distinction. Thus, the system setting we are considering is composed of a set of interacting subsystems, with common transitions to capture their interactions through firing. As a second contribution, we exploit a different formalism to model uncertainty, that is "possibility theory." Always in diagnosis based on Petri net modeling, another class of Petri nets called "Possibilistic Petri nets" (PoPN) is utilized to capture the possibilistic behavior of the system. Possibilistic measures are used to check the consistency of diagnoses, so inconsistent diagnoses are discarded. The use of possibility theory to model uncertainty offers a different perspective on the diagnostic process.

1.3 Problem statement

On the one hand, and with the absence of a distinguished distributed diagnostic scheme that treats uncertainty, an attempt to propose one is envisaged. On the other hand, uncertain diagnostic models and schemes are extensively treated in the centralized context. Thus, this proposal targets already established models for uncertain centralized diagnosis to extend them to the distributed context. These extensions prove to be challenging as it will be seen throughout the thesis. Hence the treated problem could be divided to the following subproblems:

- extending the centralized uncertainty models;

- extending the diagnostic schemes;

- dealing with the consequences of uncertainty in the distributed context.

1.4 Thesis Organization

- **The current chapter** is meant to introduce a reader to the context of the thesis. It shows the bigger picture of its composing elements. Also, it states the reasons that motivated it, alongside some obstacles encountered during its production. Finally, it overviews the rest of the chapters.

- **Chapter 2** outlines a variety of concepts in relation with model-based diagnosis in a general manner. Starting from a view on diagnosis in general, then narrow it to the model-based approach. It discusses causal models and their relation to a diagnostic process. It demystifies Petri nets as an adequate modeling tool with a general reasoning scheme for diagnosis. Also, distributed systems as the subject of diagnosis are discussed. Furthermore, it clarifies some definitions and taxonomy regarding diagnosis, causal models, Petri nets and distributed systems.

- **Chapter 3** focuses on uncertainty and the ways to cope with it. Among the variety of uncertainty models, the center of interest was two Petri-net-based models. The first one, probability propagation nets, captures probabilistic reasoning in Bayesian networks, while the second one captures possibilistic reasoning.

- **Chapter 4** illustrates the first contribution, which is an extension of probability propagation nets that is better suited for distributed diagnosis. Common transitions were proposed to model interaction among subsystems, with a better focus on the modularity of the system. It is also shown how to update the probabilities within the model in the case of new evidence and how that could be problematic in a certain way.

- **Chapter 5** illustrates our second contribution on how possibilistic Petri nets could be utilized for distributed diagnosis, starting from adapting them to a formalized

diagnostic problem for centralized diagnosis, then setting them in a distributed manner with common bordered places as interaction channels to model the distributed system. The diagnostic problem has been distributed to correlate to the distributed setting. Moreover, to verify the consistency of local diagnoses with the global one, a protocol of communication between diagnostic agents has been set. Finally, an evaluation of the correctness of the work has been discussed.

- **Chapter 6** provides some concluding remarks on the thesis. It highlights some difficulties encountered while producing the present work alongside possible perspectives to advance this work even further in the future.

Chapter 2

Model-Based Diagnosis

> The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.
>
> *Weiser, Scientific American, 1991*

2.1 Introduction

"*My computer stopped working, what is wrong with it?*" A situation, supposedly any computer owner can relate to, is somewhat a starting point to the whole field of diagnosis and in particular model-based diagnosis (MBD). As the chapter describing the state of the art related to this thesis, it sets the context on which the contributions would be built. Diagnosis, in its general view, answers an old question that goes like "*something went wrong, why?*" that affects a variety of fields ranging from medicine and biology to engineering and computer science, it may even apply to humanities such as historical studies and sociology.

Model-based diagnosis is an approach to diagnosis that, instead of dealing with the physical system, deals with its model that supposedly captures all its behavioral characteristics required to perform a diagnosis. This kind of approaches offers a high level of abstraction and independence from the physical constraints. Under this view, a more accu-

rate formulation of the problem would be like "*the system is not functioning as it should, what caused this malfunction?*"

It is important to keep in mind that there is more than a single research community working on diagnosis. Notably, the two major communities working on the field are the DX[1] community (derived from the artificial intelligence discipline) and FDI (Fault Detection and Isolation) community (derived from engineering disciplines, i.e. control theory). Moreover, it is worth noting that other communities following other fields such as networks [64] and formal methods [36, 116] have significantly contributed to this field. In general, these communities have multiple intersections and could be related to each other, with some differences in the level of abstraction, terminology, and context. In fact, some researchers have tried to close the gap between the two major communities through comparative studies and joint applications [10, 42, 107].

In general, among the differences between the two approaches [22], in their modeling paradigm, FDI approaches do not make an explicit use of the concept of components, in contrast to DX approaches that give a special concept to the system components. Moreover, the FDI approaches tend to be more off-line and limited regarding the number of faults they deal with [107]. On the other hand, DX approaches are more natural in dealing with multiple faults, and in an on-line fashion.

The remainder of this chapter is organized as follows. We take an overview of model-based diagnosis in the next section (2.2), including some terminology and Reiter's theory of diagnosis. Section 2.3 discusses causal models and their relation to diagnosis. Section 2.4 focuses on Peri nets as the modeling used to model the systems to be diagnosed. Distributed systems, as the subject of application of diagnosis, are highlighted in Section 2.5. We explicitly discuss and outline some assumptions related to model-based diagnosis in Section 2.6. Then, Section 2.7 concludes the chapter.

[1] It takes its name from a series of conferences in artificial intelligence dedicated to diagnosis.

2.2 Overview on Model-based Diagnosis

Model-based diagnosis was proposed in the early eighties to overcome some limitations of expert systems [25] (for instance, acquiring and maintaining the expert knowledge is not a trivial task). So, instead of seeking expert knowledge, researchers went with what was referred to as "*deep knowledge*." In this approach to diagnosis, the reasoning is done on an objective model of the system to be diagnosed. Such a model is supposed to be reusable [17], i.e., it is the same model used for other problem-solving tasks aside from diagnosis (e.g., simulation, reconfiguration, ...etc). Furthermore, it should be the same model used in composition (i.e., integrating the system into a larger system).

Usually, the model of a system is given in terms of its components that are prone to malfunctions. The definition of the models also contains specifications about the correct behavior of the system and its faulty behavior. Such behavior is described as a set of relations. Aside from the component-oriented approaches, process-oriented approaches like [82, 90] focus more on the global behavior of the system and usually define it in a causal manner. They are better suited for complex systems [17].

Following the DX community, MBD is based on the assumption that a model reflects the faulty behavior of the real system to be diagnosed. It is characterized by a higher level of abstraction and a strong theoretical background. One of the landmark references in the field is Reiter's work [97], where he assembled an important amount of work published in the eighties and before in an attempt to form a general theory of diagnosis. His approach is referred to as *consistency-based diagnosis*. In contrast, another approach based on logical abduction referred to as *abductive diagnosis* [18] uses a description of logical formulae to model a faulty behavior.

In contrast, experience-based diagnosis provides a different perspective on the diagnostic process. Table 2.1 illustrates a comparison between experience-based strategies and model-based-strategies [81].

	Experience-based strategies	Model-based strategies
Advantages	• A model is not required • A solution procedure is not required • Computationally faster than model-based strategies	• Can assist in diagnosing unfamiliar faults • Models of system components are plant-independent • Knowledge contained in the model aids fault resolution
Limitations	• Can only diagnose faults that have been previously observed • Patterns of symptoms are plant-specific • Fault resolution is dependent upon the extent of fault propagation	• A model is required • A solution procedure is necessary to evaluate the model • Computationally slower than experience-based strategies

Table 2.1: Model-based strategies vs experience-based strategies [81].

2.2.1 Terminology

Establishing definitions of key terms used in this thesis is mandatory to avoid any confusion regarding further development. We inspire mainly from definitions shown in [20, 64, 97].

malfunction. It corresponds to the gap between what a system should do and what is actually doing. If that gap exists, and a system does not provide what it is supposed to, that is a malfunction.

Fault. The source event to cause a malfunction. It could also be perceived as the first event leading the system to malfunction.

manifestation. symptom or observation, the observable part of the system in which a malfunction manifests. In real life applications, it corresponds to measurements on a system's variable.

diagnosis. solution or explanation, determining the part of the system responsible for causing a malfunction. It corresponds to explaining the malfunction.

□

The projection of such definitions on the frame of causal models, which will be used as a support model[2] for diagnostic reasoning, will be demonstrated in the next section (2.3).

2.2.2 Diagnosis from First Principles

Reiter's article [97] is one of the most influential literature papers there is on the theory of diagnosis from the artificial intelligence point of view. Thus, we use some of the notions introduced in it.

Definition 1. *A system S is a pair $(SD, Components)$ where:*

- *SD is the system description;*
- *$Components$ is a finite set of constants representing the system components.*

Definition 2. *(observations) An observation on a system S is a set of first order sentences. A system S with observations made on it shall be depicted as $(SD, Components, Obs)$ with Obs as observations.*

Example 1. The example illustrated in Fig. 2-1 represent a full adder containing: two and gates (A1 and A2), one or gate (O1) and two *exclusive-or* gates (X1 and X2). Hence, the set of $components = \{A1, A2, O1, X1, X2\}$ and the system description DS is given by means of first-order logic sentences like the following:

$ANDG(x) \wedge \neg AB(x) \Rightarrow out(x) = and(in1(x), in2(x)),$

$XORG(x) \wedge \neg AB(x) \Rightarrow out(x) = xor(in1(x), in2(x)),$

$ORG(x) \wedge \neg AB(x) \Rightarrow out(x) = or(in1(x), in2(x)),$

$ANDG(A1), \quad ANDG(A2),$

$ORG(O1),$

$XORG(X1), \quad XORG(X2),$

$out(X1) = in2(A2)$

$out(X1) = in1(X2)$

$out(A2) = in1(O1)$

[2] By support model, we are implying that it is not the main model used to represent diagnostic reasoning, since the main model will be specific classes of Petri nets. This will become evident later.

$in1(A2) = in2(X2)$

$in1(X1) = in1(A1)$

$in2(X1) = in2(A2)$

$out(A1) = in2(O2)$

Further axioms on the system description specifying the binary nature of the circuit inputs are depicted as:

$in1(X1) = 1 \vee in1(X1) = 0$

$in2(X1) = 1 \vee in2(X1) = 0$

$in1(A1) = 1 \vee in1(A1) = 0$

Let's suppose that after observing the system, we obtained the following results:

$in1(X1) = 1$

$in2(X1) = 0$

$in1(A1) = 1$

$out(X2) = 1$

$out(O1) = 0$

Given these results, the system is clearly faulty since the observed values do not much the expected ones, that is an inconsistency which alarms the presence of a fault. A generalized formalization of this approach could be sketched as:

$$SD \cup \{\neg AB(c_1), \ldots, \neg AB(c_n)\} \cup Obs$$

is consistent, such that: $AB(c)$ is a predicate meaning "abnormal" and $\{c_1, \ldots, c_n\} \in components$.

Abductive diagnosis. A more trivial and straightforward approach to model-based diagnosis is using abduction [23,87]. It utilizes the correlation between an effect and its possible causes without any prior knowledge about the sound behavior of a system. A substantial

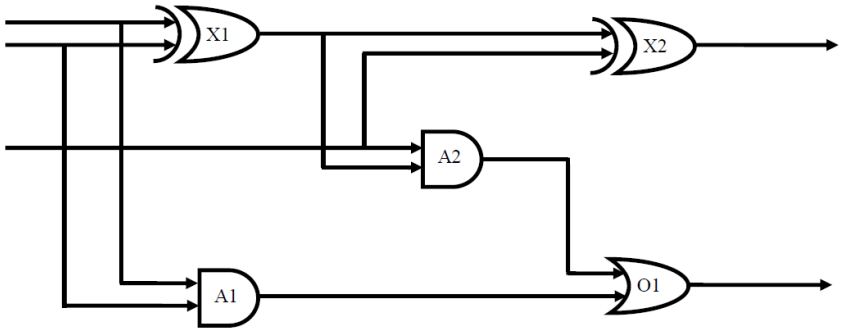

Figure 2-1: A full adder.

difference between this approach and the consistency-based approach is that in this one the expression

$$SD \cup \{\neg AB(c_1), \ldots, \neg AB(c_n)\} \cup Obs$$

is consistent.

2.3 Causal Models

Causality [83] is one of the key concepts associated with a diagnostic process. It describes the *cause→effect* relation among a system components. The basic mathematical model used to describe such a relation is a *directed graph (digraph)*. Composed of a set of nodes with arcs relating them, a digraph captures this relation in its simplest way. Console & Torasso [19] suggest distinguishing at least among three types of nodes:

- *Initial nodes*: the first nodes on a causality chain. They correspond to the initial perturbations leading the system to fail, in case of a faulty model. They have no cause, so no other node leads to them.

- *Internal nodes*: they correspond to the consequences of initial nodes and they have at least one parent and one child node. Since internal nodes can be explained by means of initial nodes, they do not make part of diagnoses.

- *Manifestations*: they correspond to the observable part of the system in which the symptoms of a malfunction are expected to be observed. Since they are the last

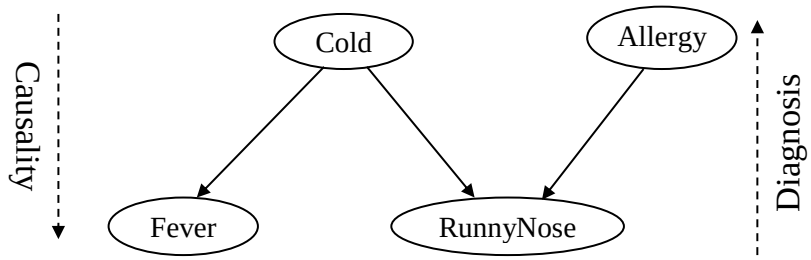

Figure 2-2: A causal network model.

nodes on a causality chain, they lead nowhere.

Following a causal scheme to diagnosis corresponds to explaining a manifestation by means of initial states. Moreover, in the case of Petri nets, the nodes are represented by places and cause-effect relationships are represented by transitions between the corresponding places.

Fig. 2-2 adapted from [52] shows a causal network demonstrating the causal relation between four nodes. For instance, "Cold" causes both "Fever" and "RunnyNose", while "Allergy" causes "RunnyNose". On the other hand, it shows how *diagnosis* works in the other direction of causality. For instance, given that we observe "RunnyNose", a diagnosis shall give us either "Cold" or "Allergy". As one can easily see, both causes are legitimately plausible, and without additional measures it is not possible to exclude any of them. Thus, having a quantifiable basis to distinguish between how likely each of which is the actual cause offers a more realistic representation. That basis is probability. An example of an additional measure is further observing "Fever" reinforce the belief that "Cold" is the actual cause of "RunnyNose".

2.4 Petri Nets

2.4.1 General view

Initially started as a simple graphical way to model industrial processes [86], Petri nets escalated to be a very useful graphical and mathematical tool that is suited to model a variety of processes with their capability to capture aspects like parallelism, concurrency, and synchronism. Some of their more elaborated classes incorporate more delicate aspects such as time and uncertainty. Petri nets now have their own research community and series of conferences and have been extensively used as a modeling tool in engineering and computer science. Petri nets with uncertainty traits are particularly relevant to this thesis, where two classes of such nets will be discussed in detail in the next chapter (3).

2.4.2 Formal Definition

We adopt here the well known definition by Murata [74].

Definition 3. *A petri net is a 5-tuple,* $PN = (P, T, F, W, M_0)$ *where:*

- $P = \{p_1, p_2, \ldots, p_m\}$ *is a finite set of places,*
- $T = \{t_1, t_2, \ldots, t_n\}$ *is a finite set of transitions,*
- $F \subseteq (P \times T) \cup (T \times P)$ *is a set of arcs (flow relations),*
- $W : F \to \{1, 2, 3, \ldots\}$ *is a weight function,*
- $M_0 : P \to \{0, 1, 2, \ldots\}$ *is the initial marking,*
- $P \cap T = \emptyset$ *and* $P \cup T \neq \emptyset$.

A 4-tuple, $N = (P, T, F, W)$ *is a Petri net structure without any specific initial marking* M_0*; and* (N, M_0) *denotes a Petri net with a specific initial marking* M_0.

2.4.3 Diagnostic Scheme with Petri Nets

Fig. 2-3 describes an architecture for the diagnostic process, adapted from [91], to be followed within this thesis. It starts from the expert knowledge about the behavior of a system

to a Petri net model representing the system, passing by a formalism for knowledge representation like first order logic. The architecture then depicts the desired solution of the diagnostic process (diagnoses) as the fruit of exploiting an invariant analysis technique, with some observations as parameters.

2.4.4 Literature Review on Centralized Diagnosis with Petri Nets

Since Petri nets are extensively used in a lot of fields, we focus here solely on its use for diagnosis[3]. We start with Portinale's work [91] due to its particular relevance to the present work, where he exploited *"invariants analysis"* of Petri nets for diagnostic purposes, then he proposed a class of Petri nets called *"behavioral Petri nets"* [92] for the same purposes. Alongside fault trees, Petri nets were used to develop a controller methodology for diagnosis in automated manufacturing systems in [109]. The work in [2, 62, 96, 108] describes a general diagnostic schemes using Petri nets, while [12, 16, 110] provide a more applied schemes for particular cases. Moreover, some other classes of Petri nets are used for diagnosis, like the behavioral Petri nets mentioned earlier; or colored Petri nets [63]; or labeled Petri nets [65] for examples. Also, note that the uncertainty-related Petri nets classes mentioned in the previous subsection are all meant for centralized diagnosis.

2.5 Distributed Systems

2.5.1 General Perception & Classification

Roughly speaking, a distributed system is composed of a set of subsystems interacting with each other. The distribution of a system could be meant in two perspectives [102].

- **Spatially.** In such a view, the system's components are physically distributed (e.g., networked systems).
- **Semantically.** In contrast to spatially distributed systems, the subsystems here may actually be adjacent but divided in terms of perception only. The type of knowl-

[3] It is to be pointed out that a considerable amount of the presented related work has been done under the specifications of *"discrete event systems" (DES)* [14].

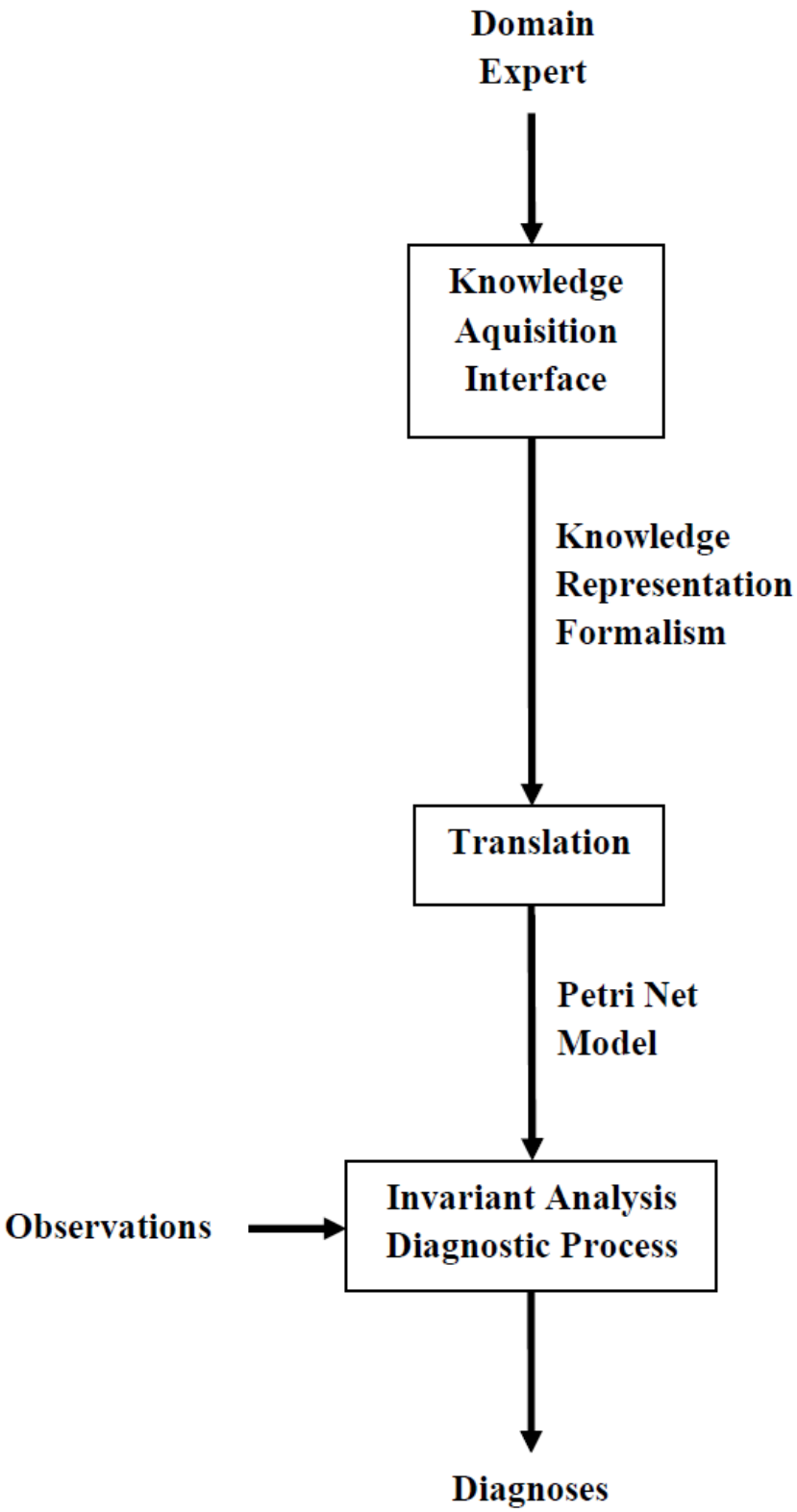

Figure 2-3: A diagnostic process architecture.

edge about the system is the one distributed here, e.g., separate models of a system's hardware and software.

Before going any further within distributed diagnosis, it is helpful to distinguish it from other types of diagnosis in regard to the distribution of their diagnostic solutions. Hence, three types are to be distinguished [5, 79].

- **Centralized diagnosis.** One agent has a global view over the whole system to be diagnosed. It captures all the faults signalizations and provide a global solution. Centralized approaches to diagnosis are known to suffer from high space complexity for large models [105].

- **Decentralized diagnosis.** An agent is associated to each subsystem, in addition to another coordinating agent (supervisor) that provides a global solution once the local diagnoses, computed by each agent, are communicated to it. Such a coordinating agent ensures the global consistency of solutions. Each agent is dedicated to a certain subsystem is only acquainted with its subsystem's knowledge, while a coordinating agent is acquainted with a larger view on a set of subsystems. Decentralized approaches, relying on a centralized coordinator, may also suffer from the problem of high space complexity.

- **Distributed diagnosis.** Differently from decentralized diagnosis, the coordination here is done among agents with the absence of a distinct coordinating agent. When such an agent is absent, a consistency check is usually performed by each agent. Perceived as a solution to the problem of high complexity, distributed approaches seem as a realistic solution towards the diagnosis of complex systems

2.5.2 Examples of Computer Architectures of Distributed Systems

Even though distributed architectures could be found in several application domains, we believe it would be helpful to present some distributed architectures in computer science that one can relate to.

- **Client-Server:** a simple form of distribution, and probably the most known, with two major entities: (1) a client in need of a resource or a service; and (2) a server that can provide the requested resources and services. Usually a client-server architecture contains one server and multiple clients.

- **Remote Procedure Call (RPC):** the possibility to execute a piece of code that belongs to another system.

- **Remote Method Invocation (RMI):** the object-oriented version of RPC.

- **Peer-to-Peer (P2P):** it is based on the concept of peers, which are equally privileged entities in contrast to client-server architecture. Each peer takes a portion of the distributed application's workload and the application goal emerge from their collaboration.

- **Multi-Agent Systems (MAS):** based on multiple intelligent agents interacting with each other to achieve a common goal. This last is usually achieved by the emergence of agents' local achievements.

2.5.3 Literature Review on Distributed/Decentralized Diagnosis

Systems with modular structures have gained more popularity over the past two decades as a way to overcome the high complexity of dealing with a complex system as one. Such development was followed by diagnostic systems conceived in a distributed or a decentralized manner to meet their requirements. Another paper of great relevance to the present one is Bennoui's [6], where he formulated his diagnostic distributed system as a multi-agent system with communicating agents to check the global consistency of local diagnoses. In the same context, Su & wonham [105] provide a study on local and global consistencies in DES. The authors of [1, 11] used labeled Petri nets and partially stochastic Petri nets for their approaches, respectively. As an interaction medium, the authors of [6, 41, 49] used common bordered places as inputs/outputs, while in [7] common transitions were used. Baldan et al. [4] provided a study on the compositional semantics on what he referred to as *"open Petri nets"* using either common places or common transitions. Other work

was more dedicated applications and case studies like [9] with a distributed model for an automotive vehicle; [24] and [101] for robotics applications; [51] for an e-commerce system; [44] for a power system using Bayesian networks and Dempster-Shafer evidence theory. Multi-agent systems have been used as an implementation framework for distributed diagnosis as in [102] by vivid agents and in [99] where the authors suggested a communication protocol between agents.

2.6 Assumptions in Model-based Diagnosis

Underlying assumptions about the process of MBD are inevitable. For instance, the most common assumption is that the model reflects the actual behavior of the real system, which is not usually the case. Real life systems are usually too complex to be tackled without some sort of abstraction. Assumptions are particularly adherent in the context of reasoning under uncertainty since the process of making probabilities and possibilities has its particularities (to be seen further on[4]). Fensel et al. [37] discussed how underlying assumptions can weaken or strengthen the problem-solving method competence, as they argue that there is no such thing as assumption-free reasoning strategies. For instance, the epistemological adequacy of probabilities has been debatable since McCarthy & Hayes's claim of their inadequacy [68], summarized in two points:

1. The amount of data required to assign numerical probabilities is not ordinarily available.[5]

2. The way probabilities are attached to statements containing quantifiers is not clear.

Even though the debate has loosened up since Pearl's book [84], it is still there. Therefore, an assumption is made here about the adequacy of probabilities to overcome this issue. Assumptions are necessary for the sake of abstraction, building reasoning schemes and overcoming computational complexity. The main assumptions made about reasoning along this thesis are:

[4]For instance, Assumption 2 in chapter 4 is an unusual one in MBD.

[5]To calculate the right probability value, one is supposed to know all the possibilities. Whereas some of them are lost in statistical procedures and some are not known at all to begin with.

- The Petri net model corresponds to the actual system.
- The diagnostic agent is considered to be safe.[6]
- All symptoms are observable.
- The reasoning rules are all true.[7]

The ones needed for the formal development of the reasoning scheme will be outlined formally once required. This kind of assumptions motivates actually more the use of reasoning under uncertainty. For more on the subject, an interested reader is referred to [37].

2.7 Conclusion

This chapter was meant to introduce some important concepts related to this thesis proposal. Understanding such concepts is key to comprehending the contributions. It combines a set of the building elements of the proposal, starting from a general view on the concept of diagnosis to situating the work among the different communities and subfields in relation to it. As they are the used modeling tool, Petri nets took a considerable part of this and will take the whole next chapter to discuss their properties, features, techniques and general relevance to capture the desired aspect; that is uncertainty. Causal models provide a scheme to relate an observation to its plausible causes, while distributed systems represent the subject of diagnosis.

[6] In fact, diagnostic agents are also prone to faults, and their faulty behavior could result in wrong diagnoses, while the system to be diagnosed is actually safe. Dealing with such a problem would require a diagnoser on the agent which also is prone to faults and so on. That's why we assume that the diagnostic agent is always safe and doesn't bear any faults.

[7] For instance, in expert systems and rule-based systems in general, this kind of knowledge is obtained from experts. However, they could be wrong, imprecise or misinforming about such knowledge.

Chapter 3

Uncertainty & Petri Nets

Uncertainty is an uncomfortable
position, but certainty is an absurd one.

Voltaire, November 28^{th}*, 1770*

3.1 Introduction

Starting from a philosophical point of view, uncertainty and doubt are among the most experienced intellectual aspects by humans. Varying from unanswered questions (e.g., questions related to the past of the universe and its future) to the daily life questions (e.g., should I take the white or the black shirt), they are always present in the human thinking.

Such an omnipresent aspect, from the daily life decision-making process to the biggest universal questions, has gotten a lot of attention, even since centuries ago. Several formalisms and models have been proposed since then, and probably the most known one among them all is the classical probability theory. Actually, a lot of uncertainty models are based on it or intersect with it somehow. The main interests regarding this thesis are conditional probabilities used in Bayesian networks and a relatively more recent theory called the theory of possibility.

Furthermore, uncertainty is especially present in the diagnostic process, since it is an inherent trait of this last. For instance, if an observable event C could be caused by multiple events, for the sake of simplicity let's say two events A and B. With no additional measures

or observations, there is simply no way to eliminate one of the two possible cause events from being a suspect in causing event C. Thus, a quantifiable measure like probability seems appropriate to provide a more realistic representation of the system.

The remainder of this chapter is organized as follows. Section 3.2 briefly outlines some theories and formalisms to model uncertainty. The main reason behind Section 3.4 is to formally introduce probability propagation nets, but before that, a passage on Bayesian networks, p/t nets and probabilistic Horn abduction is done. Section 3.5 introduces more intrinsically the theory of possibility and then possibilistic Petri nets. Finally, Section 3.6 concludes the chapter.

3.2 Reasoning under Uncertainty

Before introducing and discussing the used uncertainty models and formalisms, an introduction to probabilistic reasoning shall be envisaged. The passages on uncertainty models in this thesis are rather superficial[1]. To start from the beginning, nothing is better than the epistemological definition of abduction as a logical inference. That is, starting from a set of facts and rules to infer premises (or causes). For instance, if A implicates B, and we have B as a fact, that means A is probable to a certain extent.

About uncertainty models, it is worth noting that there is not a standardized classification of them. literature references are diverse on the subject. The process of preparing knowledge in the first place is prone to uncertainty [84, 119]. Whether due to the linguistic inability of accurate expression, abstracting complex ideas, our inability to comprehend exactly what we perceive or simply for the sake of abbreviation some information would be lost. For instance, consider the statement "Birds fly" which is true for most case, but false for few exceptions. So, to not totally falsify the considered statement, it is possible to associate a mathematical measure to quantify the likelihood of the statement being true (e.g., 90% of birds fly). A number of theories and reasoning formalisms have been proposed to deal with such an issue, including the following.

[1] We only focus on what is convenient to the purpose of diagnosis. As a starting point, an interested reader is referred to Pearl's book on probabilistic reasoning in intelligent systems [84].

Probabilistic Reasoning

Derived from the classical probability theory, probabilistic reasoning is essentially about attributing a numerical measure (i.e., a value in the interval $[0, 1]$) to a certain event indicating the likelihood of it happening.

Evidential Reasoning

Dempster-Shafer theory of evidence [103]: could be summarized to its two bounds on confidence (upper and lower bounds), such that: $Bel(P)$ is a measure of the evidence for P; and $Bel(\neg P)$ is a measure of the evidence against P.

Fuzzy Reasoning

It relies on two major concepts [53]. The first is *fuzzy sets*, which responds to the question: "*how well does an object satisfy a vague property?* The second is *fuzzy logic*, which responds to the question: "*how true is a logical statement?*

Rule-based Reasoning

Certainty factors (MYCIN) [104]: deals with uncertainty as a generalized truth value, where the certainty of a formula is defined as a function of the certainties of its subformulas. Roughly speaking, the diagnostic or causal rules undergo a propagation of belief models.

Possibilistic Reasoning

It will be discussed in more detail along this chapter, specifically in Sect. 3.5.

3.3 Literature Review on Uncertainty in Diagnosis

The classical way to model uncertainty is through probability theory, with a function $P(X) \rightarrow [0, 1]$ to indicate the probability of an event X to happen. In a diagnostic framework, it is possible to associate a probability to a malfunction to occur. In the general

view of diagnostic processes, Bayesian networks are extensively used due to their relevance [38, 70, 71, 72, 80, 84], varying from case studies to discussing their properties and inconveniences. In a logical framework, Poole discussed the relation between BNs and probabilistic Horn abduction [89]; and between logic programming, abduction and probability [88]; while Portinale [93] provided a comparative study of Horn models and BNs for diagnostic purposes. The work presented in [39] focuses on detecting inconsistencies in a probabilistic context for model-based diagnosis. For web services, Jia et al. [48] proposed to use probability tables for their diagnosis. Cayrac et al. [15] suggested using possibility theory and fuzzy sets to handle the uncertainty in a satellite fault diagnosis application, while John & Innocent [50] used fuzzy logic for clinical diagnosis.

Furthermore, a variety of Petri nets classes have been incorporated with uncertain reasoning within there model, among which we cite: stochastic Petri nets [43, 61, 100]; fuzzy Petri nets [46, 106, 111, 120]; possibilistic Petri nets [60]; Probability propagation nets [58]. Each of these classes of Petri nets captures a different formalism to model uncertainty.

3.4 Bayesian Networks and Petri Nets

Probably the most used probabilistic model in computerized applications when it comes to modeling uncertainty, Bayesian networks offer a rather intuitive model for such applications. However, their structure proves to be a bit narrow in terms of process representation in comparison to Petri nets. Hence, Probability propagation nets haves been introduced.

3.4.1 Bayesian Networks

Also known as Belief networks [47, 84], a Bayesian network (BN) is a directed acyclic graph where the nodes represent variables of the system. Mostly, the first formalism to think of when it comes probability propagation. Being a graphical model to represent causal dependencies, BNs attribute probabilities to each of their nodes. Hence, they quantify how likely an event related to a node is to happen. Yet, the change of state is not as clearly visible as in Petri nets, which were specially designed and developed to model this change, alongside with the flows of information. The amount of influence a node has over another

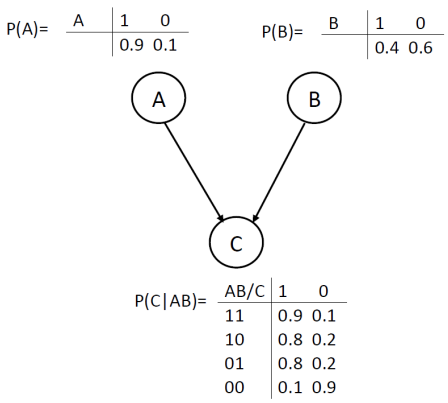

Figure 3-1: Bayesian network.

node is measured by conditional probabilities as a parent-child relationship.

Fig. 3-3 represents a simple Bayesian network with three nodes (representing events) and two dependencies. Both of the events A and B have a probability of happening (*true*) and not happening (*false*), and depending on that, the conditional probability of the event C happening is set. The tables associated to the graph nodes represent each event's probability. Bayesian networks are not the main focus of the paper; they are put as an introductory formalism for probability propagation that could be related to. In fact, BNs are translatable to PPNs, which was treated in [57]. Moreover, it is worth noting that it has been demonstrated by Cooper [21] that the process of updating belief in the probabilistic inference of Bayesian networks is NP-Hard.

3.4.2 Probability Propagation Nets

A formalism introduced by Lautenbach and Pinl [58] where they combined the characteristics and features of Bayesian networks with Petri nets. They exploited some techniques based on transition invariants in Petri nets [91] to calculate diagnoses. By adding probabilistic reasoning in Bayesian networks, PPNs can model uncertainty and quantify it, which gives us a ranking feature among the obtained diagnoses. In addition to probabilistic inference, PPNs also exploit belief update presented by Pearl [84], which deals with any new evidence obtained from observing the system.

One of the questions that should be treated is why not sticking to Bayesian networks? To answer that, we have to point out each one's advantages and disadvantages; Bayesian networks lack the capacity to model behaviors and the change of states. Their main feature is modeling causal dependencies and conditional probabilities associated to them. On the other hand, Petri nets are better suited to manage flows, which is mainly what the propagation is about. Hence, PPNs exploit both formalisms' features.

Formal background on p/t nets

The following formal definitions seem a bit dense, so a beforehand explanation of them sounds appropriate. The formal definition of a PPN is built gradually starting from a basic definition a Petri net (Def. 4), passing by the definitions of some of their properties and extensions, to the definition of a PPN. Def. 7 is of a particular relevance defining transition invariants since the diagnostic technique is based on them. Also, since PPNs are strongly tied to probabilistic Horn abduction and build upon them, it is also relevant to state how they are related. Finally, based on all of that, Def. 11 outlines a probability propagation net. For convenience reasons, we re-adapt the definition of a PN to the one presented in [56].

Definition 4. *(Place/transition nets) A p/t net is a quadruple $N = (S, T, F, W)$ where:*
(a) S is a non empty finite set of places.
(b) T is a non empty finite set of transitions.
(c) $F \subseteq (S \times T) \cup (T \times S)$ is the set of directed arcs.
(d) $W : F \to \mathbb{N}\backslash\{0\}$ is a weight function, assigning a weight to every arc.
(e) $P \cap T = \emptyset$ and $P \cup T \neq \emptyset$.
(f) We use the notation: ${}^\bullet x = \{y : yFx\}$ and $x^\bullet = \{y : xFy\}$.
(g) A node $x \in S \cup T$ is an input (output) node iff ${}^\bullet x = \emptyset (x^\bullet = \emptyset)$.

Definition 5. *Let $N = (S, T, F, W)$ be a p/t net.*

1. *A marking of N is a mapping $M : S \to \mathbb{N}$.*

$M(p)$ *indicates the number of tokens* p *under* M.

$p \in S$ *is marked by* M *iff* $M(p) \geq 1$

$H \subseteq S$ *is marked by* M *iff* $\exists p \in H$, *s.t.* p *is marked by* M.

2. *A transition* $t \in T$ *is enabled by* $M(M[t\rangle)$ *iff* $\forall p \in {}^\bullet t : M(p) \geq W((p,t))$.

3. *The new marking* M' *resulted by the firing of transition* $t(M[t\rangle M')$ *is:*

$$M'(p) := \begin{cases} M(p) - W((p,t)) & \text{if } p \in {}^\bullet t \backslash t^\bullet \\ M(p) + W((t,p)) & \text{if } p \in t^\bullet \backslash {}^\bullet t \\ M(p) - W((p,t)) + W((t,p)) & \text{if } p \in {}^\bullet t \cap t^\bullet \\ M(p) & \text{otherwise} \end{cases} \text{ for all } p \in S.$$

4. $\sigma = t_1, \ldots, t_n$ *is a firing sequence for transitions* $(t_1, \ldots, t_n \in T)$ *iff markings* $M_0, \ldots, M_n$ *exist, such that:* $M_0[t_1\rangle M_1[t_2\rangle \ldots [t_n\rangle M_n$ *holds; this is equivalent to* $M_0[\sigma\rangle M_n$.

Definition 6. *(Place vectors and Transition vectors) Let* $N = (S, T, F, W)$ *be a* p/t *net.*

1. N *is pure iff* $\nexists (x,y) \in (S \times T) \cup (T \times S) : (x,y) \in F \wedge (y,x) \in F$.

2. *A place vector (*$|S|$*-vector) is a column vector* $v : S \to \mathbb{Z}$ *indexed by* S.

3. *A transition vector (*$|T|$*-vector) is a column vector* $w : T \to \mathbb{Z}$ *indexed by* T.

4. *The incidence matrix of* N *is a matrix* $[N] : S \times T \to \mathbb{Z}$ *indexed by* S *and* T, *such that:*

$$[N](p,t) := \begin{cases} -W((p,t)) & \text{if } p \in {}^\bullet t \backslash t^\bullet \\ W((t,p)) & \text{if } p \in t^\bullet \backslash {}^\bullet t \\ -W((p,t)) + W((t,p)) & \text{if } p \in {}^\bullet t \cap t^\bullet \\ 0 & \text{otherwise} \end{cases}$$

Remark 1. *In order to get a one-to-one correspondence between* p/t*-nets and incidence matrices, we assume that all* p/t*-nets are pure.*

Definition 7. *(Transition invariant) Let* i *be a transition vector of* N.

1. i *is a transition invariant (t-invariant) iff* $i \neq 0$ *and* $[N] \cdot i = 0$

2. $||i|| = \{t \in T | i(t) \neq 0\}$ *are the supports of* i.

3. *A t-invariant* i *is minimal iff:*

   - i *is non negative* ($\forall t \in T : i(t) \geq 0$)
   - $\nexists$ *t-invariant* $i' : ||i'|| \subsetneqq ||i||$.
   - *the greatest common divisor of all entries of* i *is 1*

4. *The net representation* $N_i = (S_i, T_i, F_i, W_i)$ *of a t-invariant* i *is defined by:*

   - $T_i := ||i||$
   - $S_i := {}^\bullet T_i \cup T_i^\bullet$
   - $F_i := F \cap ((S_i \times T_i) \cup (T_i \times S_i))$
   - W_i *is the restriction of* W *to* F_i.

The first work, to our knowledge, that used transition invariant (T-invariant) analysis for diagnostic purposes has been introduced by Murata & Yim [73]. However, it was conceived for single fault diagnosis. A more general and relevant work on the subject matter has been done by Portinale [91] where he attempted to partially transform a diagnostic problem solved by symbolic techniques into a problem solved by linear algebraic ones (i.e., t-invariant analysis). The faulty behavior was used to be modeled by means of *definite clauses* (e.g., Horn clauses — to be seen next) to form what is called a *definite logic program*, which is translatable to a Petri net model.

Propositional logic and probabilistic Horn abduction

Basic definitions to construct the reasoning background of the paper. It is actually built upon the work of [58, 88, 89, 93]. We start off with logical definitions of PHA then its canonical net representation followed by defining the PPN.

Definition 8. *Consider propositional logic set of atoms a, b, c, ... and operators* $\neg, \wedge, \vee$ *and the brackets), (. Let* $\tau = \neg a_1 \vee \cdots \vee \neg a_n \vee b_1 \vee \cdots \vee b_m$ *be a clause (disjunction of literals | a literal is an atom or its negation); in set notation:* $\tau = \neg A \vee B$ *for* $\neg A = \{\neg a_1 \vee \cdots \vee \neg a_n\}$ *and* $B = \{b_1 \vee \cdots \vee b_m\}$*;*

- τ *is a fact clause iff* $\neg A = \emptyset$*,*
- τ *is a goal clause iff* $B = \emptyset$*,*
- τ *is a rule clause iff* $\neg A \neq \emptyset \wedge B \neq \emptyset$*,*
- τ *is a Horn clause iff* $|B| \leq 1$*.*

Definition 9. *Let* α *be a conjunctive normal form (CNF) Horn formula and let* $N_\alpha = (S_\alpha, T_\alpha, F_\alpha)$ *be a place/transition-net;* N_α *is the canonical p/t-net representation of* α *iff:* $S_\alpha = \mathbb{A}(\alpha)$ *(set of atoms) and* $T_\alpha = \mathbb{C}(\alpha)$ *(set of clauses); and* $\forall \tau = \neg A \wedge B, F_\alpha$*is determined by:*$^\bullet\tau = \{a_1, \ldots, a_n\}, \tau^\bullet = b$*.*

Definition 10. *For* α *is a Horn formula, let be the following:* $H \subseteq \mathbb{F}(\alpha)$ *a set of assumable hypothesis and* $E \subseteq H$ *be a set of explanations;* $R \subseteq \mathbb{R}(\alpha) \cup \mathbb{F}(\alpha)$ *,* $\gamma \subseteq \mathbb{G}(\alpha)$*, and let* $\varepsilon = \wedge_c | c \in E, \varrho = \wedge_c | c \in R$*, let* $P_\alpha : \mathbb{C}(\alpha) \to [0, 1]$ *be the probability function of* α *such that* $P_\alpha(\varepsilon \wedge \varrho)$ *is the probability of* ε*. let I be a t-invariant of* N_α *of* α*, then the probabilities of* ε *and of* $\neg\gamma$ *equals* $\prod_{t \in \|I\| \setminus \{\gamma\}} P_\alpha(t)$*.*

Remark 2. *The law to calculate the probabilities of explanations provided in Def. 10 is applicable under the assumption that the net is loop-free*[2]*.*

Probability propagation nets

Definition 11. *(Probability propagation net) Let* α *be a Horn formula;* $PN_\alpha = (S_\alpha, T_\alpha, F_\alpha, P_\alpha, L_\alpha)$ *is a probability propagation net (PPN) for* α *iff*

[2]In case of a loopy net, some nodes have a double influence on others, which gives eventually the wrong probability value. To overcome this problem, it possible to use pearl's conditioning approach [84] to cope with loops.

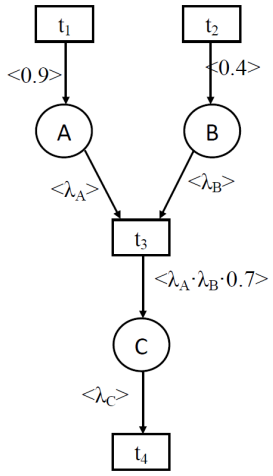

Figure 3-2: Probability propagation net.

- $N_\alpha = (S_\alpha, T_\alpha, F_\alpha)$ *is the canonical net representation of* α*,*

- P_α *is a probability function for* α*,*

- L_α *is an arc label function for* α *where:*
  if $f = (\tau, b) \in F_\alpha \cap (T_\alpha \times S_\alpha)$ *and* $\tau \in \mathbb{F}(\alpha)$ *then* $L_\alpha(f) :=< P_\alpha(\tau) >$*,*
  if $f = (a, \tau) \in F_\alpha \cap (S_\alpha \times T_\alpha)$ *and* $\tau \in \mathbb{R}(\alpha) \cup \mathbb{G}(\alpha)$ *and* λ *ranges over [0, 1] then* $L_\alpha(f) :=< \lambda >$*,*
  if $f = (\tau, b) \in F_\alpha \cup (T_\alpha \times S_\alpha)$ *and* $\tau \in \mathbb{R}(\alpha)$ *then* $L_\alpha(f) :=< P_\alpha(\tau) > \cdot \prod_{a \in {}^\bullet\tau} L_\alpha(a, \tau)$.

Fig. 3-2 shows a simple PPN composed of three places and and four transitions. It represents the Horn formula $\alpha = A \wedge B \wedge (\neg A \vee \neg B \vee C) \wedge \neg C$, and it is also representative of the Bayesian network example shown in Fig. 3-3. The probability function P_α is given as: $P_\alpha(t_1) = 0.9$, $P_\alpha(t_2) = 0.4$, $P_\alpha(t_3) = 0.7$, $P_\alpha(t_4) = 1$. The only t-invariant here is $I = \begin{matrix} t_1 & t_2 & t_3 & t_4 \end{matrix}$
$\begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$, and the probability of ε and $\neg\gamma$ is $\prod_{t \in \|I\| \setminus \{\gamma\}} P_\alpha(t) = 0.252$.

3.5 Possibility Theory and Petri Nets

3.5.1 Possibility Theory

Introductory Example

Let's take the following well known example [77]. In a statement like "Hans ate X eggs for breakfast", where X takes values in $U = \{1, 2, 3, \dots\}$, a *possibility distribution* $\{\pi_X(u)\}_{u=1}^{\infty}$ is associated with X, such that $\pi_X(u)$ is interpreted as the degree of ease with which Hans can eat u eggs for breakfast. Another way to interpret X is by using a *probability distribution* $\{P_X(u)\}_{u=1}^{\infty}$, with $P_X(u)$ as the probability of Hans eating u eggs for breakfast. The assessment of the distributions is shown in table 3.1. This example was meant to set a general idea about possibility.

u	1	2	3	4	5	6	7	8	9	10
$\pi_X(u)$	1	1	1	1	0.8	0.6	0.4	0.2	0.1	0
$P_X(u)$	0.1	0.8	0.1	0	0	0	0	0	0	0

Table 3.1: Possibility and probability distributions associated with X.

History

There is actually some history [26, 35] to the *theory of possibility* before its foundations got established by L. A. Zadeh in 1978, or at least to the concepts used in it. The economist Shackle introduced the concept of *degree of potential surprise* to describe the impossibility of an event to happen. Philosopher D. Lewis introduced the notion of *comparative possibility* in a graded way to relate between the possible worlds. Formally speaking, for events A, B, C:

$$A \geqslant_\pi B \Longrightarrow C \cup A \geqslant_\pi C \cup B, \tag{3.1}$$

where $\geqslant_\pi$ is a comparative possibility relation. In the context of legal reasoning, philosopher L. J. Cohen introduced a degree of provability, which he referred to as *Baconian probability* to highlight the idea that it is difficult to prove someone's guilt based only on statistical arguments. Such concept coincides with necessity measures in the theory of

possibility. Henceforth, after his theory of *fuzzy sets* to capture the uncertainty related to linguistics, L. A. Zadeh came to generalize it to introduce the basics of the theory of possibility, which was used extensively in a variety of fields, but of course not as much as the classical probability theory.

Possibility versus probability

After some reading in this regard, the relation between possibility and probability is not quit definite. For instance, some perceive possibility as a special type of probability [45, 76], while others as relate it logical frameworks (i.e. modal logic) [54]. Thus, unlike probability that has a quantitative definition (through the frequency of occurrence), Possibility is usually tied to a logical definition [94] (i.e. modal logic[3]) with an indeterminate degree of possibility. Then it comes Zadeh's perception on the theory where he tied it to his former theory of fuzzy sets as mentioned earlier. The relationship between uncertainty formalisms has been fairly discussed in the literature [31, 33, 54], but it still needs a lot of emphasis.

Formal background (theoretical setting)

Given a set of possible worlds[4], a proposition r is true in some of them and false in the rest. To model the uncertainty associated with the actual world, we define a possibility distribution over all possible worlds. Such description is used to determine the degree of possibility of the actual world being in a possible world. Formally, Dubois et al. [30] defined the possibility and necessity measures as:

$$\Pi(r) = Sup\{\pi(\omega)|\omega \models r\}, \tag{3.2}$$

$$N(r) = Inf\{1 - \pi(\omega)|\omega \models \neg r\}, \tag{3.3}$$

where:

[3]The theory of possibility has strong ties to modal logic, for which reason it is recommended to have a look on this type of formal logic [94].

[4]Could be referred to as states in certain taxonomies [28]. In a probabilistic logic framework [78], they could be represented as a probability distribution or belief network.

- Π is the possibility measure;
- r is a proposition;
- ω is a possible world;
- N is the necessity measure;
- $\omega \models r$ means that r is true in ω ($\omega \in \Omega$);
- Ω is the set of possible worlds.

3.5.2 Possibilistic Petri Nets

Formal Definition

The idea was firstly introduced by Cardoso et al. [13] then elaborated to suit diagnostic purposes in rule-based reasoning by Lee et al. [60]. However, before formally defining a Possibilistic Petri net (PoPN[5]), a slight difference in from Def. 3 about the nature of tokens should demystified. Fig. 3-3 illustrates a simple example of a PoPN.

Definition 12. *A petri net is a 5-tuple,* $PN = (P, T, F, W, M_0)$ *where:*

- $P = \{p_1, p_2, \ldots, p_m\}$ *is a finite set of places,*
- $T = \{t_1, t_2, \ldots, t_n\}$ *is a finite set of transitions,*
- $F \subseteq (P \times T) \cup (T \times P)$ *is a set of arcs (flow relations),*
- $W : F \to \{1, 2, 3, \ldots\}$ *is a weight function,*
- $M_0 : P \to \{0, 1, 2, \ldots\}$ *is the initial marking,*
- $P \cap T = \emptyset$ *and* $P \cup T \neq \emptyset$.
- *each token is associated with a pair of possibility measures* (N_i, Π_i),
- *we use the notation:* ${}^\bullet x = \{y : yFx\}$ *and* $x^\bullet = \{y : xFy\}$

[5]The original abbreviation of these nets was PPN, but to avoid confusing them with probability propagation nets in this thesis frame, it has been changed to PoPN.

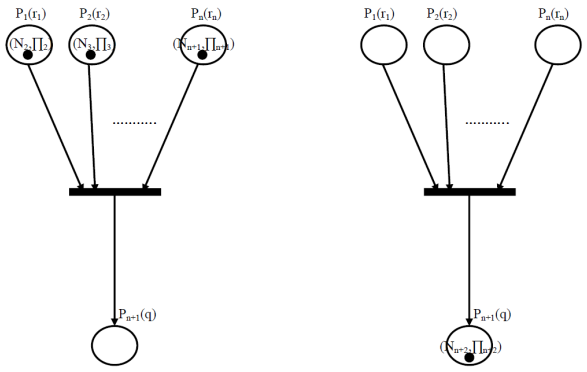

Figure 3-3: A simple example of a PoPN.

Definition 13. *A possibilistic Petri net (PoPN) is 5-tuple,* $PPN = (P, PT, A, W, M_0)$ *where:*

- $P = \{p_1(r_1), p_2(r_2), \ldots, p_m(r_m)\}$ *is a finite set of places (*p_i *represents a classical proposition* r_i*),*
- $PT = \{t_1(N_1, \Pi_1), t_2(N_2, \Pi_2), \ldots, t_n(N_n, \Pi_n)\}$ *is a finite set of possibilistic transitions, with* t_i *representing the connectivity between places,* N_j *denoting the lower bounds of necessity measures and* Π_j *denoting the upper bounds of possibility measures.*
- $F \subseteq (P \times T) \cup (T \times P)$ *is a set of arcs,*
- $W : F \rightarrow \{1, 2, 3, \ldots\}$ *is a weight function,*
- $M_0 : P \rightarrow \{M(P_1), M(P_2), \ldots, M(P_m)\}$ *is the initial marking, with* $M(P_i)$ *standing for the number of tokens in* P_i*.*

Possibilistic Entailment

Inspired by Nilson's work on probabilistic logic [78], more specifically probabilistic entailment, the notion of possibilistic entailment has been outlined in [59] as:

$$\frac{\begin{array}{l} r \rightarrow q, (N_{r \rightarrow q}, \Pi_{r \rightarrow q}) \\ r \qquad\quad , (N_r, \Pi_r) \end{array}}{q, (N_q, \Pi_q)}$$

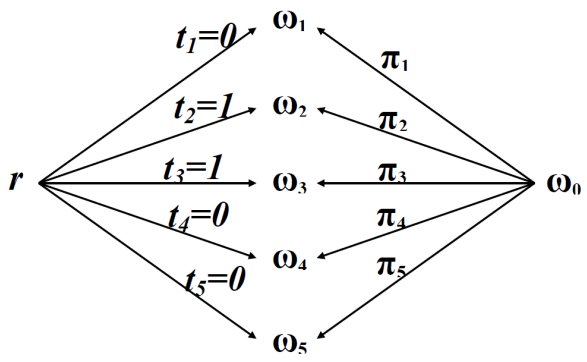

Figure 3-4: Possible worlds for possible information.

The goal of this entailment is to infer a new proposition with its associated necessity and possibility. The possible worlds, in which the actual world might be (see Fig. 3-4), are determined using a semantic tree. Hence, a consistent path in the semantic tree is considered to represent a possible world. Moreover, Table 3.2 shows the truth values of these possible worlds.

	ω_1	ω_2	ω_3	ω_4
r	$true$	$true$	$false$	$false$
$r \rightarrow q$	$true$	$false$	$true$	$true$
q	$true$	$false$	$true$	$false$

Table 3.2: Truth values of possible worlds.

So, given the set of propositions $S = \{r, r \rightarrow q, q\}$, its possible worlds could be deduced using a semantic tree (see Fig. 3-5).

Firing Rules

According to the four distinguishable types of transitions: inference; aggregation; duplication; and aggregation-duplication transitions, the firing rule changes correspondingly. The components of PPNs represent three types of knowledge needed to make an uncertainty reasoning scheme: propositions; uncertain rules; and uncertain facts, represented respectively by: places; possibilistic transitions; and possibilistic tokens. Hence, given the propositions r and q, the firing rules of each type of transitions is formulated as follows:

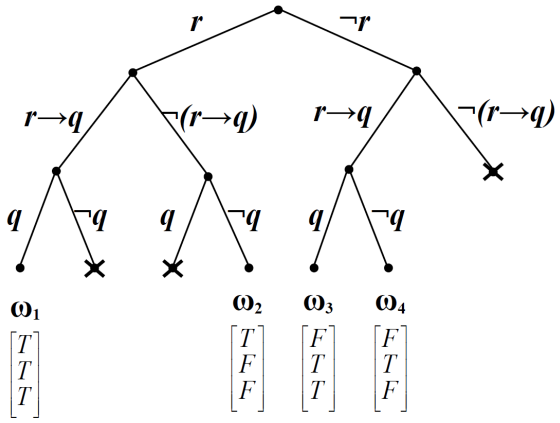

Figure 3-5: A semantic tree.

- *inference transition (t^i)*: represented as a proposition having multiple antecedents:

$$(r_1 \wedge r_2 \wedge \cdots \wedge r_n) \rightarrow q, (N_1, \Pi_1), \tag{3.4}$$

the necessity and possibility measures are calculated using possibilistic entailment [60] with the general formula

$$\begin{aligned} N_q &= min\Big\{max[N_{(r_1 \wedge r_2 \wedge \cdots \wedge r_n) \rightarrow q}, 1 - \Pi_r], \\ &\qquad max[1 - \Pi_{(r_1 \wedge r_2 \wedge \cdots \wedge r_n) \rightarrow q}, N_r]\Big\} \\ \Pi_q &= max\Big\{min[\Pi_{(r_1 \wedge r_2 \wedge \cdots \wedge r_n) \rightarrow q}, \Pi_r], \\ &\qquad min[\Pi_{(r_1 \wedge r_2 \wedge \cdots \wedge r_n) \rightarrow q}, 1 - N_r]\Big\}, \end{aligned} \tag{3.5}$$

that would become

$$\begin{aligned} N_q &= min\{N_{(r_1 \wedge r_2 \wedge \cdots \wedge r_n) \rightarrow q}, N_r\} \\ \Pi_q &= \Pi_{(r_1 \wedge r_2 \wedge \cdots \wedge r_n) \rightarrow q} \end{aligned} \tag{3.6}$$

if the possibility distribution $\hat{\pi}$ is *normalized*[6].

[6]By a normalized possibility distribution we refer to the fact that $\Pi_r < 1$ and $\Pi_{r \rightarrow q} < 1$ do not exist simultaneously, if not then it is partially inconsistent [30].

- *aggregation transition (t^a)*: represented as a proposition having multiple antecedents:

$$\begin{aligned}(r_1 \rightarrow q, (N_1, \Pi_1)), (r_2 \rightarrow q, (N_2, \Pi_2)), \ldots, \\ (r_m \rightarrow q, (N_m, \Pi_m)),\end{aligned} \tag{3.7}$$

to be used for aggregating conclusions in the case where several uncertain rules having the same classical proposition, and to link an antecedent having the same classical proposition. For a proposition of the form:

$$(q, (N_q^1, \Pi_q^1)), \ldots, (q, (N_q^n, \Pi_q^n),$$

it should be aggregated as $(q, (N_q^{n+1}, \Pi_q^{n+1})$ with

$$\begin{aligned}N_q^{n+1} &= max[N_q^1, \ldots, N_q^n] \quad \text{and} \\ \Pi_q^{n+1} &= max[\Pi_q^1, \ldots, \Pi_q^n],\end{aligned} \tag{3.8}$$

also for a normalized distribution.

- *duplication transition (t^d)*: represented as a proposition having one antecedent:

$$\begin{aligned}(r \rightarrow q_1, (N_1, \Pi_1)), (r \rightarrow q_2, (N_2, \Pi_2)), \ldots, \\ (r \rightarrow q_l, (N_l, \Pi_l)),\end{aligned} \tag{3.9}$$

having one antecedent, it duplicates the token with its same previous values.

- *aggregation-duplication transition (t^{ad})*: represented as a proposition having multiple antecedents:

$$\begin{aligned}(r_1 \rightarrow q, (N_1, \Pi_1)), (r_2 \rightarrow q, (N_2, \Pi_2)), \ldots, \\ (r_m \rightarrow q, (N_m, \Pi_m)), (q \rightarrow s_1, (N_{m+1}, \Pi_{m+1})), \\ (q \rightarrow s_2, (N_{m+2}, \Pi_{m+2})), \ldots, \\ (q \rightarrow s_l, (N_{m+l}, \Pi_{m+l})),\end{aligned} \tag{3.10}$$

as a combination of the two previous types.

3.6 Conclusion

This chapter was dedicated to introducing key concepts and formalisms on which the contributions are built. It discusses the concept of uncertainty as the main theme distinguishing this particular work on distributed diagnosis from others. It outlines formally the two classes of Petri net used to capture deferent formalism regarding uncertainty. Probability propagation nets capture a form of classical probability used in graphical models, that is conditional probability, which is mostly known in Bayesian networks. A less known uncertainty formalism is the theory of possibility. It offers a different perception on the uncertain information with its two measures: possibility and necessity. Possibilistic Petri nets extend normal Petri nets to capture uncertainty according to this theory. Some basic properties and characteristics of both classes are demonstrated within this chapter as they will be helpful for further development.

Chapter 4

Distributed Probability Propagation Nets & Diagnosis

> The most important questions of life are indeed, for the most part, really only problems of probability.
>
> *Laplace, Théorie analytique des probabilités , 1812*

4.1 Introduction

Real life systems such as the Internet, industrial manufacturers, and telecommunication networks tend to be more and more distributed. They are headed towards ubiquity and omnipresence, in the pursuit of Weiser's vision [112] (quoted in Chapter 2). This trend comes with a lot of challenges such as: management, security and reliability of complex systems. A special interest is taken into complex systems as they seem to be the future of computer science, more precisely, diagnosing them. The importance of the diagnosis of distributed systems (as a passage to complex systems) arises from the fact that these systems are not perfect, they are expected to fall down at some point. Thus, locating the sources of malfunctions could be critical to the reliability and omnipresence of a system. It is the first step to deal with a malfunction and keep its state at its best. Even in terms of cost,

the diagnostic results could be the line between a cheap fix and an expensive replacement of the whole faulty system.

One of the problems related to the field of diagnosis is the uncertainty of diagnoses. Whereas the result of a diagnostic process is a set of multiple explanations, and if there is no basis to distinguish between them, the only assumption that is taken is that all explanations are equally probable [66]. Therefore, providing a quantifiable basis, to make this distinction, seems an appropriate solution. From here, the importance of probabilistic reasoning comes up to measure and quantify the amount of uncertainty. As concepts, uncertainty and doubt represent a set of the concepts most experienced in human life, especially in the decision-making process. The capacity to operate under uncertainty is argued to be one of the most remarkable human abilities [60]. Dealing with such uncertainty necessitates associating probabilities to events defining how likely they are to happen. Thus, probabilistic reasoning could be used as a ranking and a recommendation tool [85, 115].

The system setting for this contribution is divided into subsystems interacting with each other, pursuing the paradigm of "divide & conquer." Our work is essentially constructed for model-based diagnosis of distributed systems. Consequently, modeling takes the biggest part of it. We want initially to model each of these subsystems by a probability propagation net (PPN) [58] as a probabilistic model. However, the current form of a PPN, as it is defined by Lautenbach and Pinl, is oriented to centralized systems and do not suit the distributed context with its particularities, such as: modularity and encapsulation. Hence, an extension of PPNs is proposed; distributed probability propagation nets (DPPNs) are defined as a PPN in addition to common transitions to model the interaction among the subsystems. Thus we model each subsystem by means of a DPPN, where the interaction is represented by the firing of common transitions. Since PPNs are based on Petri nets, the diagnostic technique to be used is based on transition-invariants. The implications of this extension are shown, along with both logical and graphical representation of the model. We try to build a formal background to the model first, and then we explain its applications graphically on an example.

The rest of the chapter is organized as follows: Section 4.2 outlines a description of systems on which the diagnostic reasoning could be applied. Section 4.3 discusses the formal

building of distributed probability propagation nets starting from defining the concept of common transitions, alongside an important theorem to relate them to a diagnostic solution. Section 4.4 discusses what we refer to as "*new evidence effect*" and it relation to consistency checking. Furthermore, how to perform a local then global diagnoses is explained in the same section. Finally, the chapter is concluded in section 4.6.

4.2 System Setting

4.2.1 System Description

There is a debate actually about which is better in modeling; going for high abstraction or low abstraction. The first tendency does not consider a lot of details about the system to be modeled and keeps it as general as possible. On the other hand, the second tendency entails more details of a real system, and thus it is more applicable to a specific type of systems. Compared to the fault detection and isolation community, the DX community usually goes for a higher abstraction, and following their path, we adopt a general definition of a distributed system composed of n subsystem as

$$DS = \bigcup_{i=1}^{n} SS_i, \tag{4.1}$$

- DS : Distributed System;
- SS : SubSystem.

Each of the components of a distributed system DS interacts with other components. A more detailed definition of a subsystem is required since we work directly on models. In fact, we work under the supposition that the system model is provided at the beginning. This section actually discusses what to expect as a model.

At a certain level of abstraction, a distributed system could be perceived as shown in Fig. 4-1, where the whole system is composed of a set of subsystems. Each of which has its own internal components that may cause a malfunction, while they interact with each other through mediums, represented here by means of arrows. Fig. 4-6 focuses on the

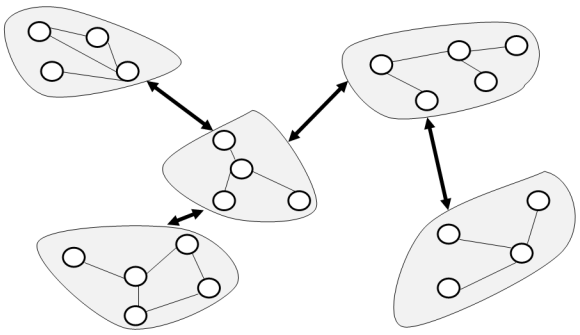

Figure 4-1: An abstract architecture of a distributed system.

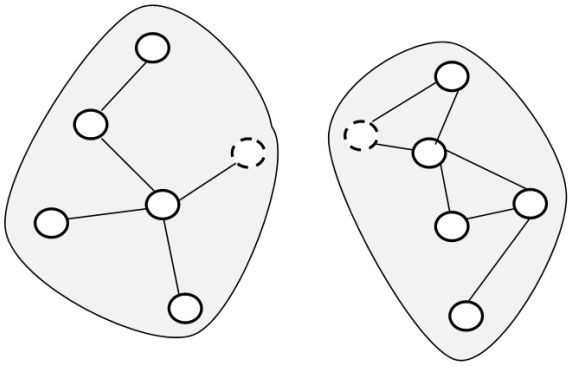

Figure 4-2: Common component capturing interaction between two subsystems.

interaction medium as a common component between two subsystems. It is represented by the circle with the dashed line, where the two circles stand for the same component; their role is to model the interaction between them. In a distributed system, we have the subsystems and the links between them. In real life systems, the interaction medium represents the interconnection tools, such as wires and waves. In the case of distributed systems, considering the concept of modularity can be very helpful to simplify managing the whole system, especially if it is considerably large. Thus, the system is seen as a set of subsystems interacting with each other. Each of those subsystems could be modeled by a PPN.

We seek, in this chapter, to establish a logical basis for a distributed model-based diagnostic approach based on PPNs. Such a basis allows a safe building of the model and a high level of abstraction. Aside from the logical definitions, a graphical representation based on Petri nets is shown. Since probability propagation nets are Petri nets based, every

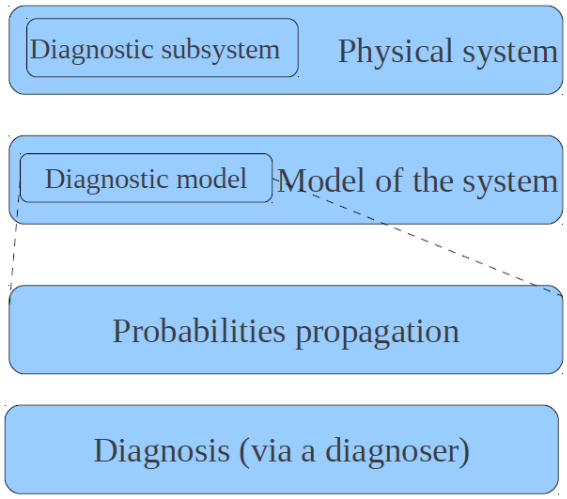

Figure 4-3: Hierarchy of the system's abstraction.

system modeled by Petri nets could be upgraded to a PPN.

It is actually possible to model a distributed system by PPNs as they are, and Petri nets (transitively PPNs) are known for their capability in this matter. However, a condition to be made on that is the total knowledge about its structure and behavior, which is not the case we treat. We consider encapsulation and modularity.

4.2.2 Hierarchical Perception

In order to explain better our perception of the diagnostic system, we suggest the multi-layer model shown in figure 4-3. It describes the process' layers as we see them. The passage from the physical system to its model is a mere abstraction, where we consider only representing the important parts of the system. The diagnostic model focuses on the relation between the susceptible parts (nodes) of being down or to fail and their symptoms. In this case, we associate probabilities to each susceptible node to calculate or to rank their probability of failure. The diagnosis process determines its results based on the rank of failure's possibility of the node.

To defend our choice to model the system with such layers, we state the following facts; a system's raison d'etre is not usually diagnosis, however, a diagnostic subsystem is usually implemented with it. The *Diagnostic subsystem* is meant to determine the part(s) responsi-

ble for the failure and to find a solution to the quest of diagnosis (it is called a subsystem as a part of the physical system and not as a subsystem in the distributed system). Furthermore, for the second layer, it represents an abstraction to the previous layer. For the third layer, probabilities propagation is used to model the uncertainty in the diagnostic process, and the fourth layer is where the diagnoser gives its results based on the information gotten from the previous layers.

4.3 Distributed Probability Propagation Nets

At a lesser level of abstraction, it is possible to model each subsystem by means of a Petri net, then transitively, a PPN which captures their probabilistic behavior. However, the current definition of a PPN requires some refinement to suit the distributed context, basically to represent interaction aspects.In Petri nets, there are two ways of modeling the interaction among subsystems. Whether using common places or common transitions, and each one of them has its significance. The common places indicate the existence of an entity belonging to both subsystems, like a shared memory for example. The common transitions indicate that there is a synchronization and order among the components and operations of the subsystems. In a lot of works in the literature, such as [6,41,49], the Petri net modeling of the interaction is done through common places. In our case, we choose to model it by the common transitions approach [4] as it is more suited for PPNs because the canonical p/t-net representation requires starting and ending up with transitions. The interaction among subsystems is captured through the firing of common transitions.

Formally speaking, we add to every subsystem model some common transitions CTs that relate the subsystem to its neighbors. A common transition belonging to more than one subsystem at a time is seen differently from each subsystem's perspective. For a subsystem where the common transition is the last one to be fired in a sequence, it is considered as an "*out common transition*" and in the other case where the common transition is the first to be fired, it is considered as an "*in common transition*". Of course, the concept of "*in*" and "*out*" common transition is seen from the subsystems' local perspective, but for the whole distributed system they are seen as one common transition belonging to more than

one subsystem. "*Distributed Probability Propagation Nets*" have been introduced in [7] and extended in [8] like the following.

Definition 14. *(Common transitions) For a subsystem S_i, let α_i be a Horn formula; $CT_{\alpha_i} \in \mathbb{C}(\alpha_i)$ is the set of common transitions such that: for $ct_k \in CT_{\alpha_i} \Rightarrow ct_k \in CT_{\alpha_j}|\alpha_j$ is the Horn formula of S_j (a neighboring subsystem of S_i).*
For a subsystem S_i

- *if $ct_k \in CT_{\alpha_i}$ and $ct_k^\bullet = \phi$ then $ct_k \in CT_{\alpha_i}^{out}$ (the subset of "out common transitions"), referred to as: ct_k^{out},*
- *if $ct_k \in CT_{\alpha_i}$ and ${}^\bullet ct_k = \phi$ then $ct_k \in CT_{\alpha_i}^{in}$ (the subset of "in common transitions"), referred to as: ct_k^{in},*

such that $ct_k^{out} \in S_i$ and $ct_k^{in} \in S_j$, with $i \neq j$.

The reason to distinguish between the two types of common transitions that a same common transition ct_k may hold two different values: one associated with a subsystem S_i and the other associated with a subsystems S_j (i.e. $P(ct_k^{in}) \neq P(ct_k^{out})$). Additionally, this distinction provides a clearer perception on the connection elements as they are for *entering* (i.e. ct_k^{in}) or *exiting* (i.e. ct_k^{out}) the model.

Definition 15. *(Distributed probability propagation nets) Let α_i be a Horn formula for a subsystem S_i; $DPN_{\alpha_i} = (S_{\alpha_i}, T_{\alpha_i}, F_{\alpha_i}, P_{\alpha_i}, L_{\alpha_i}, CT_{\alpha_i})$ is the distributed probability propagation net (DPPN) for α_i where:*
$PN_{\alpha_i} = (S_{\alpha_i}, T_{\alpha_i}, F_{\alpha_i}, P_{\alpha_i}, L_{\alpha_i})$ is a probability propagation net (PPN) for α_i, and CT_{α_i} is the set of common transitions such that $CT_{\alpha_i} \in \mathbb{C}(\alpha_i)$. A distributed system DS, constructed of n subsystems, is defined as follows: $DS = \bigcup_{i=1}^{n} DPN\alpha_i$.

Moreover, the projection of this extension of the general definition of a distributed system presented in Eq. 4.1 would relult the following definition.

Definition 16. *A distributed system DS, constructed of n subsystems, is defined as follows: $DS = \bigcup_{i=1}^{n} DPN\alpha_i$, where:*
$DPN\alpha_i$ is a distributed probability propagation net for each subsystem S_i.

Theorem 1. *For a common transition* $ct_k \in CT_{\alpha_i}$

- *if it is a* ct_k^{out} *then* ct_k *is a goal transition,*
- *if it is a* ct_k^{in} *then* ct_k *is a fact transition.*

Proof. By definition (if $ct_k^+ = \emptyset$; then $ct_k \in CT_{\alpha_i}^{out}$), in a subsystem: ct_k^{out} is a last transition on the edge of the subsystem that, in the same subsystem leads nowhere. A transition leading nowhere is logically defined by a conjunctive normal form where all its literals are negative, which is the definition of a goal clause with $B = \emptyset$ representing a goal transition. In the same way we prove the second statement. □

In case PHA representation is not needed, it is possible to not consider α. Thus, the definition of the model becomes like:

Definition 17. *a* $DPN_i = (S_i, T_i, F_i, P_i, L_i, CT_i)$ *is composed of:*

- (S_i, T_i, F_i) *is a place/transition net;*
- P_i *is a probability function;*
- L_i *is an arc label function;*
- $CT_i \in T_i$ *is the set of common transitions.*

The interaction among subsystems is captured through the firing of common transitions. In fact, the usually used components, in the literature, to capture this interaction are common places. However, for the case of PPNs, it is more suitable to model it using transitions. About the common transitions, we distinguish two types of them: "*in common transition*" and "*out common transition*", where the first ones correspond to initial nodes in terms of a causal model, while the second ones correspond to end nodes of the same model.

Assumption 1. The graph G representing interactions between the local models of subsystems is acyclic.

As discussed in Sect.2.6, there is no such thing as assumption-free reasoning strategies, whether due to high complexity issues or to relate the diagnostic system to its environment or on the availability of some priorly necessary data ...etc, thus some assumptions need

to be presumed. Here, Assumption 1 is relaxed to avoid an infinite cycle of blames [98]. Given that A_i the diagnostic agent of S_i blames the neighboring subsystems S_j for observed malfunction, if A_j (the diagnostic agent of S_j) blames S_i for its observed malfunction by its turn, we may obtain a cycle of blames that supports itself. This also implicates not having a cycle of updating probabilities. Furthermore, in the context of logical frameworks, the diagnostic problem becomes NP-hard [98].

Example 2. When we say "*distributed system*" or even "*system*" in general, the first idea to come to mind is a computer system or an electrical system; mostly, engineering-related systems. However, the definition of a system is more general than that, it even applies to humans. So, as an example, let's consider the human social system; it is composed of subsystems (humans) interacting with each other. Each of which has its own states, e.g.: happy, angry, sick, fat ...etc. There is an influence among states over each other, whether on the same subsystem or not. To facilitate understanding, we consider only two subsystems: a *father* and his *daughter*. Fig. 4-4 shows a graphical representation of the system model; including its behavior and its associated probabilities. It models a defined scenario of interaction. So, when the father comes back home, there is a probability that he buys a gift for his daughter. She may like it or not, and based on that the probability of her using it is set. The daughter's happiness influences the father's happiness. Also, getting good grades and behaving in a good manner make the father proud. Nevertheless, we considered only positive states such as "*buy*" and not "*buy not*" for simplicity reasons. Table 4.1 illustrates the meaning of each state shown in Fig. 4-4. Moreover, Tables 4.2 and 4.3 show associated probabilities to transitions of the two subsystems, while Tables 4.4 and 4.5 show their corresponding t-invariants.

4.4 Diagnostic Reasoning Scheme

Let's first note that the difference between probabilities held by the same common transition could be interpreted in two ways:

1. Consider it an inconsistency, which would lead to discarding some solutions based

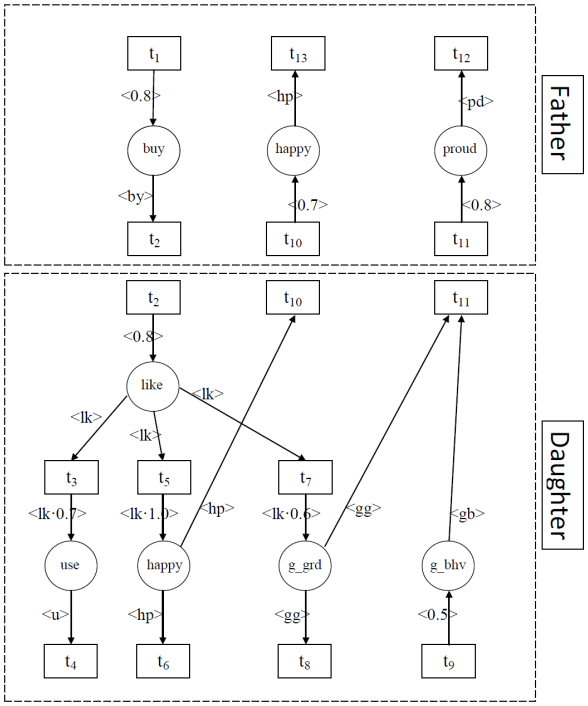

Figure 4-4: Two interacting subsystems.

on it.

2. Consider it as a new evidence and adjust the other model's nodes probabilities.

The first interpretation could set the basis for an inconsistency check in order to discard some inconsistent solutions, while the second one offers an interesting feature to update the model's probabilities according to the development of the system and the new observations made on it. Since dealing with new evidence is one of the key features of PPNs, and due to the influence of McCarthy and Hayes's [68] thoughts on the epistemological inadequacy of probability, we went with keeping the feature of adjusting model's probabilities according to new evidence and not leaning on probability as a basis to claim an inconsistency.

Furthermore, we need to establish two levels of diagnosis: the first one is the result of a local diagnosis that each diagnoser computes independently; the second one is the result of a collaboration between diagnosers. But before that, we need to discuss what we refer to as the "*new evidence effect*." But before that, it is relevant to demystify the t-invariant diagnostic technique on a centralized example first.

state	description
buy	father buys a gift for his daughter
like	daughter likes father's gift
use	daughter uses the gift
happy	daughter is happy
g_grd	daughter gets good grades
g_bhv	daughter behaves in a good way
proud	father is proud
happy	father is happy

Table 4.1: States and their description.

transition	t_1	t_2	t_{10}	t_{11}	t_{12}	t_{13}
probability	0.8	0.8	0.7	0.8	1.0	1.0

Table 4.2: Probabilities associated to transitions for the first subsystem.

4.4.1 Centralized diagnosis

Since local diagnosis is basically a special case of centralized diagnosis, we suggest the following example adapted from [91].

Example 3. Fig. 4-5 shows a PPN model for the faulty behavior of a car adapted from [91] with Table 4.7 for the model t-invariants. We load the transitions of the model with the probabilities illustrated in Table 4.6.

To illustrate the ranking feature offered by PPNs, let's take an observation with multiple possible explanations. For instance, the observation that the acceleration response is irregular ($acc\_resp(irreg)$) corresponds to firing t_{ari}, which belongs to three t-invariants: I_9; I_{10} and I_{11}. In terms of the diagnostic problem, it gives us: $\Psi^+ = \{acc\_resp(irreg)\}$; and $\Psi^- = \{\emptyset\}$. This implicates three possible explanations depending on the firing of fact (initial) transitions:

transition	t_2	t_3	t_4	t_5	t_6	t_7
probability	0.8	0.7	1.0	1.0	1.0	0.6
transition	t_8	t_9	t_{10}	t_{11}		
probability	1.0	0.5	0.7	0.8		

Table 4.3: Probabilities associated to transitions for the second subsystem.

	t_1	t_2	t_{10}	t_{11}	t_{12}	t_{13}
I_1	1	1				
I_2			1			1
I_3				1	1	

Table 4.4: T-invariants of the first subsystem.

	I_1	I_2	I_3	I_4	I_5
t_2	1	1	1	1	1
t_3	1				
t_4	1				
t_5		1	1		
t_6		1			
t_7				1	1
t_8				1	
t_9					1
t_{10}			1		
t_{11}					1

Table 4.5: T-invariants of the second subsystem.

- the firing started from t_{psw} and t_{cti}, that is the *worn piston state* and the *irregular carbur tuning*, thus $\Delta_1 = (t_{psw}, t_{cti})$;
- the firing started from t_{ossw}, t_{gcl} and t_{cti}, that is the *worn oil sump state*, the *low ground clearance* and the *irregular carbur tuning*, thus $\Delta_2 = (t_{ossw}, t_{gcl}, t_{cti})$;
- the firing started from t_{spmh}, that is the *high spark plug mileage*, thus $\Delta_3 = (t_{spmh})$.

More importantly, the probability of each diagnosis is calculated as shown in Def. 10 like:

$P(\Delta_1) = P(t_{psw}) \cdot P(t_{cti}) \cdot P(t_1) \cdot P(t_6) \cdot P(t10) \cdot P(t_{15}) \cdot P(t_{16}) \cdot P(t_{17})$, by going back to Table 4.6, that is:

$P(\Delta_1) = 0.6 \cdot 0.5 \cdot 0.9 \cdot 1.0 \cdot 1.0 \cdot 0.9 \cdot 1.0 \cdot 0.8 = 0.1944$.

In the same manner we obtain: $P(\Delta_2) = 0.127$ and $P(\Delta_3) = 0.336$. Now the ranking feature among diagnoses is more obvious, where Δ_3 is the most probable explanation then Δ_1 then Δ_2 w.r.t. this example.

Remark 3. *Note that the calculated probabilities in Example 1 are not normalized, i.e.*

they do not add up to one. Since the goal here is to compare explanations' probabilities, a normalization will not be necessary.

Remark 4. *The example in Fig. 4-5 does not show any arc labels (discussed in Def. 11) because, once again, they are not needed for our purposes.*

transition	t_{psw}	t_{ossw}	t_{gcl}	t_{spmh}	t_{cti}	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8	t_9
probability	0.6	0.7	0.7	0.6	0.5	0.9	0.8	0.7	0.8	0.7	1.0	0.9	0.9	1.0
transition	t_{10}	t_{11}	t_{12}	t_{13}	t_{14}	t_{15}	t_{16}	t_{17}						
probability	1.0	0.8	0.7	0.9	0.8	0.9	1.0	0.8						

Table 4.6: Probabilities associated to transitions of the PPN model.

I_1	$t_{psw}, t_1, t_5, t_{esb}$
I_2	$t_{psw}, t_1, t_6, t_9, t_{olo}$
I_3	$t_{ossw}, t_{gcl}, t_2, t_7, t_9, t_{olo}$
I_4	$t_{psw}, t_1, t_6, t_{10}, t_{11}, t_{13}, t_{14}, t_{sfey}$
I_5	$t_{ossw}, t_{gcl}, t_2, t_7, t_{10}, t_{11}, t_{13}, t_{14}, t_{sfey}$
I_6	$t_{psw}, t_1, t_6, t_{10}, t_{11}, t_{12}, t_{tir}$
I_7	$t_{ossw}, t_{gcl}, t_2, t_7, t_{10}, t_{11}, t_{12}, t_{tir}$
I_8	$t_{ossw}, t_{gcl}, t_2, t_8, t_{hosy}$
I_9	$t_{psw}, t_{cti}, t_1, t_6, t_{10}, t_{15}, t_{16}, t_{17}, t_{ari}$
I_{10}	$t_{ossw}, t_{gcl}, t_{cti}, t_2, t_7, t_{10}, t_{15}, t_{16}, t_{17}, t_{ari}$
I_{11}	$t_{spmh}, t_3, t_4, t_{ari}$

Table 4.7: T-invariants of the of the PPN model.

4.4.2 New evidence & inconsistency

The capacity to deal with new observations on the system and changing the probabilities associated to the model accordingly is an interesting feature of PPNs. It gives it a certain dynamicity to cope with a changing system. However, it would take away the capacity to measure inconsistency[1], since if the observed value is different from the expected one; then the new one is just considered as a new evidence. To better explain this, let's say that in a

[1]By measuring inconsistency we are referring to the contradiction between "*what we observe*" and "*what we should observe*", and based on that contradiction, some diagnoses may be discarded. For more details, see [97].

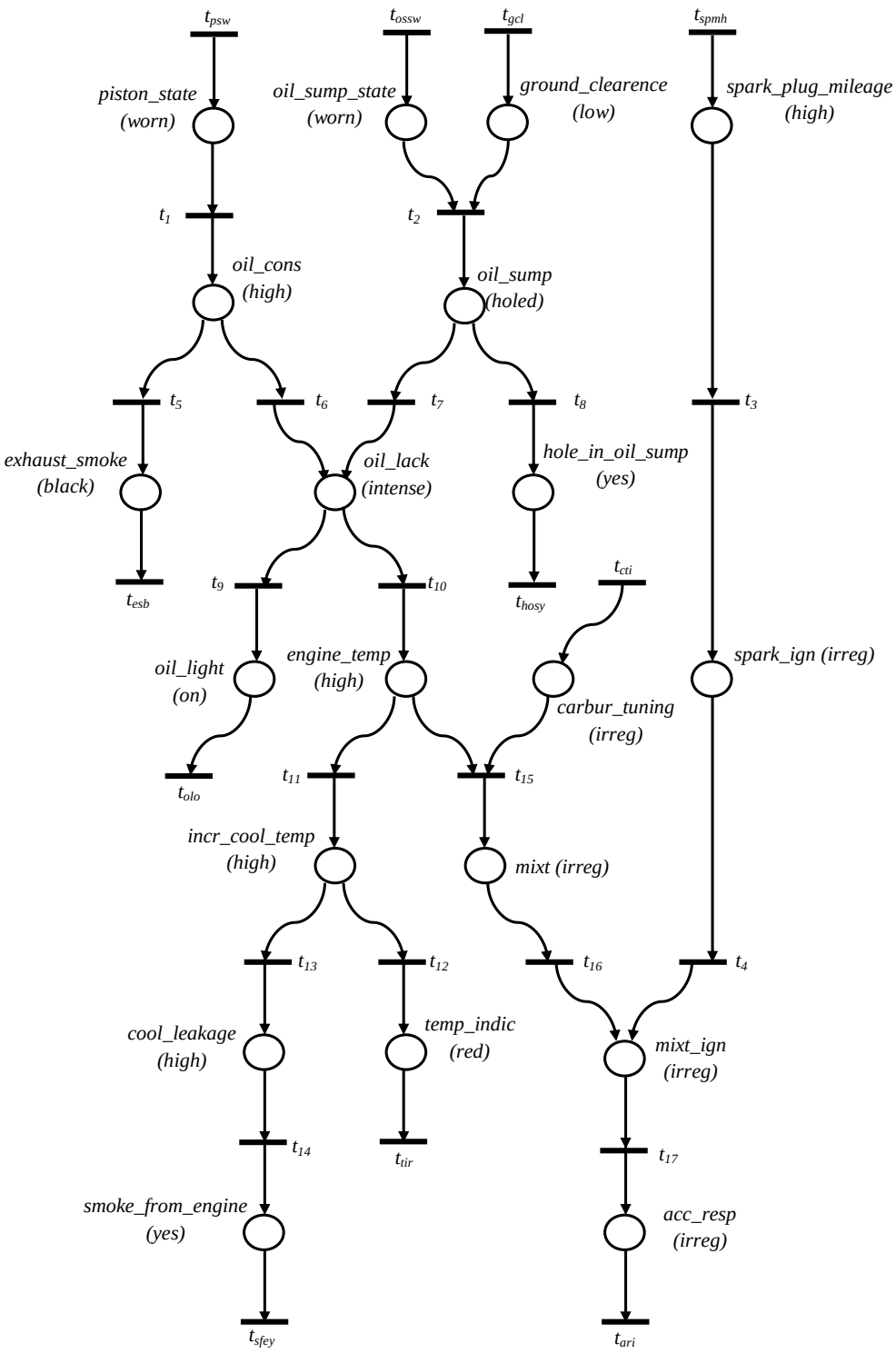

Figure 4-5: A probability propagation net model of a faulty behavior of a car.

distributed system composed of two subsystems to which a diagnosing agent is associated to each one, agent A_1 calculates some diagnoses among which $\Delta_n = (t_2, t_{12}, ct_3^{in})$ with $P(ct_3^{in}) = 0.5$, in such case A_1 requests from its neighboring agent to check this value; if $ct_3^{out} \neq 0.5$ that is supposed to be taken as an inconsistency because it does not fit to the diagnosis obtained locally, but in this case the value of $P(ct_3^{out})$ is just considered as a new evidence that A_1 was not aware of and it is used to update $P(ct_3^{in})$. Furthermore, additional constraints about the termination of new evidence stabilizing the net should be discussed.

It is possible though to give up on this feature (updating the systems probabilities) for the sake of having a basis to measure inconsistency, which is the difference between $P(ct_k^{in})$ and $P(ct_k^{out})$ of a same common transition ct_k.

4.4.3 Local diagnosis

In distributed systems, it is preferable to construct elementary-oriented solutions, where each of the system's components contributes a local solution based on its knowledge. The emergence of local solutions would provide a global one. Following this philosophy, we would first show how a local diagnosis is computed (with a total absence of interaction aspects, externally), then how to use it in the distributed context.

The first step to take in local diagnosis is to compute the t-invariants within the subsystem's model[2]. On each calculated t-invariant, there must be at least one fact transition and one goal transition. Usually, a t-invariant contains: (1) more than one fact transition, (2) several rule transitions and (3) one goal transition.

Definition 18. *(Local diagnosis) Let DPN_i be the model of a subsystem S_i; a diagnosis Δ_k for a t-invariant I_k is given as:*

$$\Delta_k = \|I_k\| \cap \mathbb{F}_k(t),$$

where $\mathbb{F}_k(t)$ is the set of fact transitions of the t-invariant I_k. Hence, a diagnosis Δ_k is

[2]A well-known algorithm by Martinez & Silva [67] could be used to compute the t-invariants of a Petri net model.

given as:

$$\Delta_k = ft_1 \wedge ft_2 \wedge \cdots \wedge ft_n,$$

with n is the number of fact transition.

Starting from the probabilities associated to each transition, the probability of a diagnosis is given as discussed in Sect. 3.4.2. Let's consider the example shown in Fig. 4-4. For the subsystem "*daughter*", we want to calculate the probability of her using a gift: by looking at Table 4.5, we note that t_4 (corresponding to "*use*") belongs only to I_1. A first deduction to be made is that we have only one diagnosis (one t-invariant). Next, we calculate its probability as: $P(\Delta) = P(t_3) \cdot P(t_2) = 0.8 \cdot 0.7 = 0.56$. Informally speaking, this means that: if the daughter uses the gift, there is a 0.56 probability that she likes it. *Notes:*

- In the example in Fig. 4-4, we totally ignore the "*father*" subsystem and consider the "*daughter*" subsystem alone. Such that: t_2 is a fact transition and not a common transition.
- We have used a very simple example, where the goal transition has only one t-invariant. In case of more than one t-invariant, we would have more than one diagnosis. Consequently, the ranking feature would appear clearly among diagnoses.

4.4.4 Distributed diagnosis

Based on the model definition provided in Sect. 4.3, another aspect would be taken into account in diagnosis, which is interaction. Diagnosers should be distributed according to the distribution of the subsystems. Hence, each of which is assigned to a subsystem. Differently from local diagnosis shown above, common transitions (which represent interaction) can hold information that is unknown to the diagnoser. This information may change its perception about the gotten diagnoses. In general, a diagnosis must ensure a global consistency of the system. The following implies implicitly a protocol of collaboration between diagnosers.

An agent A_i (diagnoser) computes the t-invariants in its corresponding subsystem S_i. If a t-invariant doesn't contain any common transitions, then its related diagnosis cannot be

rectified. Otherwise, a probability rectification is possible. Before we proceed any further, here are some remarks to keep in mind about the model:

- The calculation of diagnoses is done through t-invariants.
- All the probabilities in a t-invariant must be known prior to the calculation of diagnoses.
- Diagnoses cannot be discarded due to the "*new evidence effect*", which consists of the possibility to a transition's firing probability from 0 (insignificant) to a significant value.
- A neighboring diagnoser calculates $P(ct_i^{out})$ by considering it as a goal transition, then calculating its probability.
- Diagnoses are ranked based on their corresponding probabilities.

Once a common transition is found, A_i must contact A_j, the corresponding agent to S_j, such that: $ct_l \in S_i \cap S_j$. The reason to contact A_j is to verify the relevance of the common transition's probability. Algorithm 1 illustrate a general reasoning scheme by an agent.

Assumption 2. The graph G representing interactions between the local models of subsystems is inter-loops[3] free.

Assumption 2 is relaxed to overcome the problem of loopy nets that cannot be detected on a distributed scheme. If a part of the loop belongs to S_i and another part of it belongs to S_j, only a diagnoser having knowledge about both subsystems models can detect and resolve the loop. Otherwise, which is our case, such an assumption holds. Fig. 4-6 represent the previous example with a small change in the father's submodel where an arc is added from transition t_{12} to state $happy$. Such change incorporates an inter-loop that starts from the fork on the $like$ state in the daughter's submodel and ends with a join state $happy$ on the father's submodel. On the level probability propagation, it implicates a double influence from the fork node on the join node. Hence, our solution is not applicable to this example. Theorem 2 suggests the absence of an infinite cycle of invocations between agents.

[3]By inter-loop we refer to a loop where its *fork* node belongs to one subsystem and its *join* node belongs to another.

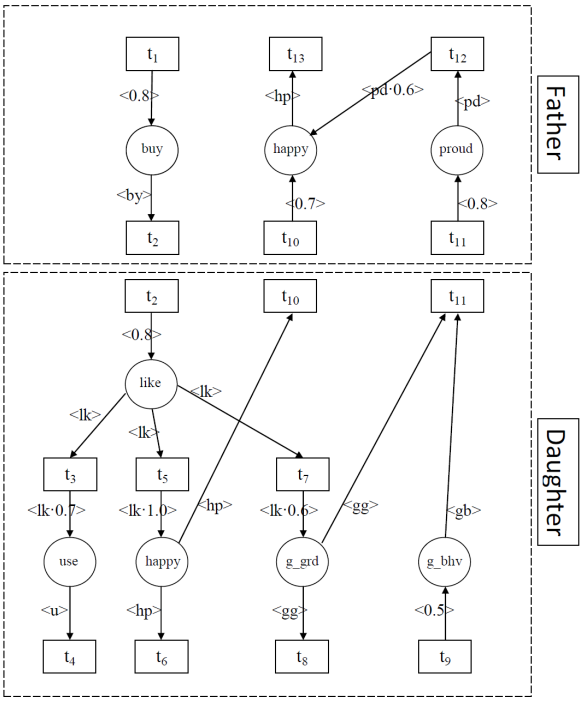

Figure 4-6: Two interacting subsystems with an inter-loop.

Theorem 2. *Let* $DS = \bigcup_{i=1}^{n} DPN_i$ *be a distributed system; for each subsystem* DPN_i*, the updating process terminates after a finite number of invocations.*

Proof. This follows as a consequence of the acyclicity property assumed in Assumption 1. □

Given a common transition ct_l, its two perceptions: ct_l^{out} and ct_l^{in} may hold different probabilities. This different values may be caused due to the mismatch in setting the values on the model the first time. Another reason for difference in the "*in*" and "*out*" probabilities is the "*new evidence effect*", where an observation is made about a subsystem S_j to which ct_l^{out} belongs. This observation changes the probability of a goal transition gt to a certainty, such that $P(gt) = 1$ (gt stands for a goal transition), which leads to a change in all the set probabilities on t-invariants related to gt, including ct_l^{out}. While A_i is unaware of the change, $P(ct_l^{in})$ remains as it is. Thus, A_j is asked to provide $P(ct_l^{out})$ in order to update $P(ct_l^{in})$. To accomplish this task (providing $P(ct_l^{out})$), A_j considers ct_l^{out} as a goal transition and calculates its probability of firing. In case $P(ct_l^{out}) \neq P(ct_l^{in})$, then

Algorithm 1 Diagnoser (subsystem: S_i)

input: subsystem model
output: local diagnosis
Compute T-invariants
for each T-invariant I_k **do**
    if the net is loopy **then** eliminate the loops
    end if
    for each initial transition **do**
        if $t_l \in CT$ **then** Invoke Neighbor (S_j, t_l) such that S_j shares the common transition t_l with S_i
        end if
        if $P(ct_l^{out}) \neq P(ct_l^{in})$ **then** $P(ct_l^{in}) \leftarrow P(ct_l^{out})$
        end if
    end for
    $P(\Delta_k) := \prod_{t \in \|I_k\| \setminus \{\gamma\}} P(t)$
end for

$P(ct_l^{in}) \leftarrow P(ct_l^{out})$, which is done by A_i. This update of value will change the probability of diagnosis $P(\Delta)$ and it is possible to change its rank as well. In the same manners, if the t-invariant containing ct_l^{out} contains also another common transition ct_m, the diagnoser has to address a request to the neighboring diagnoser in order to verify its probability ...etc. Algorithm 1 gives an insight on how an agent operates to calculate diagnoses and their respective probabilities. At some point, it invokes another algorithm called *Neighbor* from the neighboring agent that returns the value of $P(ct_l^{out})$.

By going back again to Example 2, let's calculate the probability of the same diagnosis, just this time we consider the interaction. So, t_2 is a common transition with: $t_2^{out} \in S_1$ (*father*) and $t_2^{in} \in S_2$ (*daughter*). Two agents A_1 and A_2 are assigned as diagnosers to S_1 and S_2 respectively. Hence, A_2 calculates the probability of firing t_4, as calculated in the previous subsection; $P(t_4) = 0.56$. To verify if the gotten result is up to date, A_2 "*asks*" A_1 to provide $P(t_2^{out})$. A_1 calculates immediately $P(t_2^{out}) = 0.8$ and replies to A_2. By its turn, A_2 compares $P(t_2^{out})$ with $P(t_2^{in})$, which are alike; $P(t_2^{out}) = P(t_2^{in}) = 0.8$, so $P(\Delta)$ stays as it is. One little change about the semantic of the diagnosis is that this one implies an outer cause of the gotten diagnosis. To show a case where $P(\Delta)$ changes, let's calculate $P(t_{12})$ that the father is proud. Instantly, we calculate $P(t_{12}) = 0.8$ the probability of firing

t_{11} which leads directly to t_{12}. Since t_{11} is a common transition, A_1 asks A_2 for $P(t_{11}^{out})$, which belongs to I_5; $P(t_{11}^{out}) = 0.8 \cdot 0.6 \cdot 0.5 = 0.24$. So, the probability of firing t_{11}^{in} is updated to $P(t_{11}^{in}) = 0.24$.

Example 4. On a more engineering-related note, let's consider the example depicted in Fig. 4-7, which is a modified version of and example provided in [6], with a bit of restructuring to suit our purposes. The modification consists mainly in using common bordered transition as an interaction medium instead of places. Now, suppose that we have the observation $temp\_ind(red)$, it belongs to two t-invariants: I_4^2 and I_5^2. Hence, $\Delta_1 = (t_{spmh})$ and $\Delta_2 = (t_y)$. The probability of each diagnosis is calculated in the same manner as in the first example, thus $P(\Delta_1) = 0.2592$ and $P(\Delta_2) = 0.504$.

Since t_y is a common transition, such that $t_y^{in} \in S_2$ and $t_y^{out} \in S_1$, a consistency check is performed. Meaning that t_y^{in} and t_y^{out} may hold different probabilities, which needs to be verified. To do so, t_y^{out} is considered to be a goal transition, and on the light of that its probability of firing given that $t_y^{out} \in I_2^1 \cup I_3^1$ is calculated as the following:
$P(t_y^{out}) = [P(t_5) \cdot P(t_4) \cdot P(t_2) \cdot P(t_1) \cdot P(t_{prsw}) \cdot P(t_{psw})] + [P(t_5) \cdot P(t_x)]$.
All these probabilities are known, but since t_x is a common transition, its probability also needs to be checked. Hence, the diagnoser of S_2 is invoked again to provide $P(t_x^{out})$. In the same manner, the probability of firing t_x^{out} is calculated to be $P(t_x^{out}) = 0.8$. Thus,
$P(t_y^{out}) = (0.7 \cdot 0.8 \cdot 0.8 \cdot 0.9 \cdot 0.7 \cdot 0.7) + (0.7 \cdot 0.8) = 0.1975 + 0.56 = 0.7575$.

Then $P(t_y^{in})$ should be updated to 0.7575, and thus $P(\Delta_2)$ becomes 0.5454 instead of 0.504. That is not enough to change the order of diagnoses, but it offers more accurate results, and hence Δ_2 is still the most probable and Δ_1 is the second probable.

transition	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8	t_9	t_{prsw}	t_{psw}	t_{ossi}	t_x
probability	0.9	0.8	0.7	0.8	0.7	1.0	0.9	0.9	1.0	0.7	0.7	0.6	0.5

Table 4.8: Probabilities associated to transitions for the first subsystem S_1.

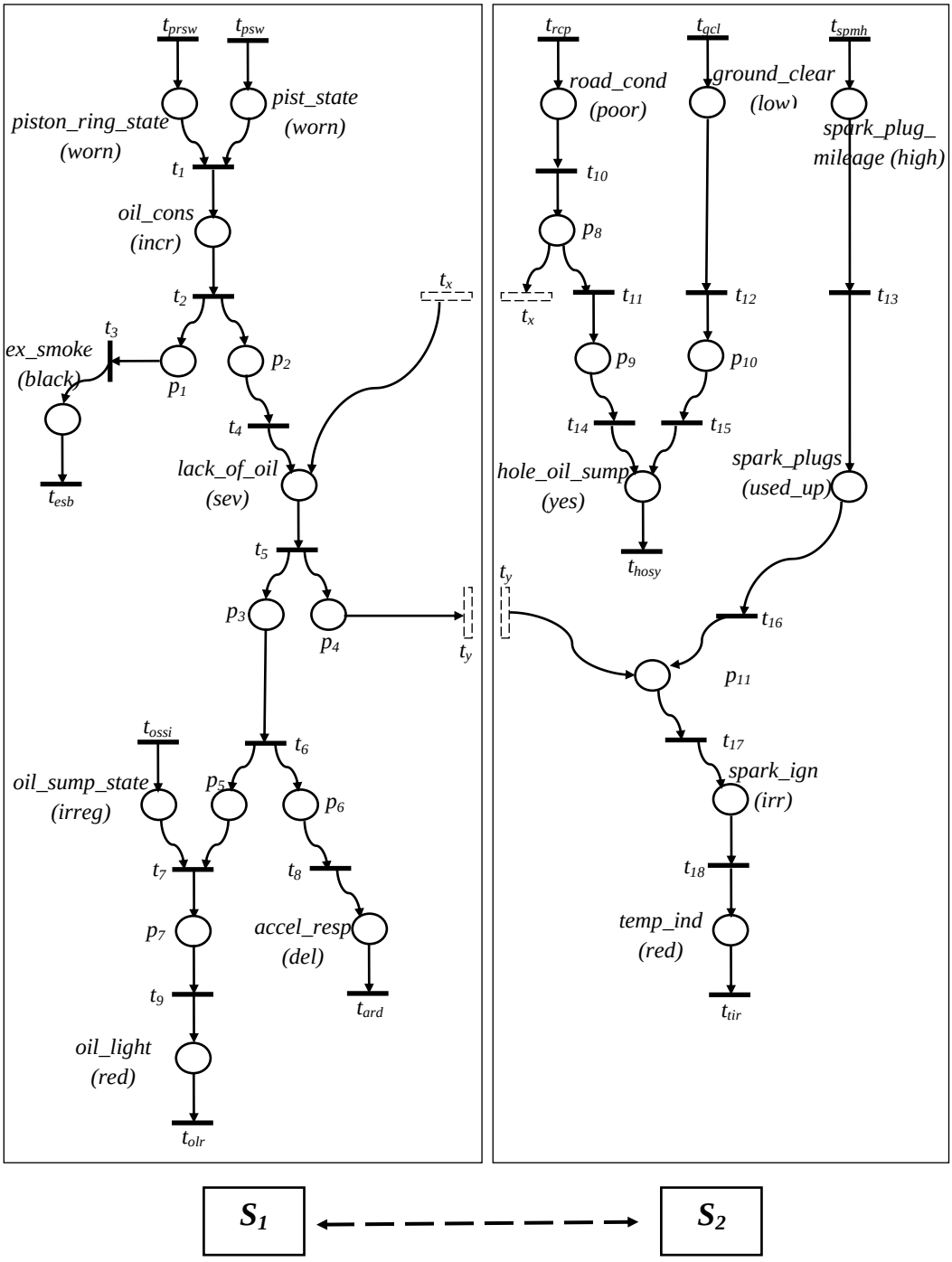

Figure 4-7: Two interacting subsystems.

transition	t_{10}	t_{11}	t_{12}	t_{13}	t_{14}	t_{15}	t_{16}	t_{17}	t_{18}	t_{rcp}	t_{gcl}	t_{spmh}	t_y
probability	1.0	0.8	0.7	0.9	0.8	0.9	1.0	0.8	0.9	0.8	0.7	0.4	0.7

Table 4.9: Probabilities associated to transitions for the second subsystem S_2.

	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8	t_9	t_{prsw}	t_{psw}	t_{ossi}	t_x	t_{esb}	t_{olr}	t_{ard}	t_y
I_1^1	1	1	1							1	1			1			
I_2^1	1	1		1	1					1	1						1
I_3^1					1								1				1
I_4^1	1	1		1	1	1	1		1	1	1	1			1		
I_5^1					1	1	1		1			1	1		1		
I_6^1	1	1		1	1	1		1		1	1					1	
I_7^1					1	1		1					1			1	

Table 4.10: T-invariants of the first subsystem S_1.

4.5 Discussion

It is commonly known withing the distributed and complex systems community, that the passage from centralized approaches to distributed ones comes with the benefit of breaking complexity but with the cost of a nonuniversal solution. That is, in our case, the possibility of losing some explanations that do not belong to the subsystem. For instance, if a malfunction seen in a subsystem S_i is tracked to a common transition, the explanation is said to belong to another subsystem S_j without identifying the exact node responsible for the malfunction because it is unknown to the diagnoser of S_i. Still, breaking the complexity in the system model and the diagnostic process is enough reason to pursue the path of distributed approaches. Furthermore, The formal development of our proposal should be sufficient for validation, since a computerized implementation should give us the same results of a

	t_{10}	t_{11}	t_{12}	t_{13}	t_{14}	t_{15}	t_{16}	t_{17}	t_{18}	t_{rcp}	t_{gcl}	t_{spmh}	t_y	t_{hosy}	t_{tir}	t_x
I_1^2	1									1						1
I_2^2	1	1			1					1				1		
I_3^2			1			1					1			1		
I_4^2				1			1	1	1			1			1	
I_5^2								1	1				1		1	

Table 4.11: T-invariants of the second subsystem S_2.

manually developed computed diagnosis. That includes the calculation of t-invariants, the explanations of a given observation, their probabilities and their ranks.

Admittedly, the assumptions made on the distributed system model are fairly restrictive. In particular, assuming the freedom of the model from inter-loops (Assumption 2) is a new one that comes with probabilistic modeling, but it is what it takes to keep the probability propagation sound. Actually, as in the case of regular loops, a solution could be found to such a problem,[4] but with an unknown cost for the moment, which could involve sacrificing some aspects like modularity. On the other hand, acyclicity (Assumption 1) and other assumptions not explicitly stated within the article, e.g., the soundness of diagnosers and the correctness of the model, are generally known and accepted in model-based diagnosis.

4.6 Conclusion

This chapter was conceived to treat the problem of model-based diagnosis while quantifying uncertainty using probabilistic reasoning. It has distributed and complex systems as a subject, considered as a set of interacting subsystems. Each of which is modeled by a distributed probability propagation net, with bordered common transitions to capture interaction. Thus, based on initial probabilities provided with the system model, along with the ones calculated with the propagation, some transitions (including common transitions) are able to update their probabilities, and thus change the probabilities of diagnoses. In general, the model's probabilities could be changed throughout the lifetime of the system to be diagnosed whether due to new observations or new statistical measures[5]. Therefore, a diagnoser shall expect an inconsistency between a common transition's in and out probabilities at every diagnostic process it executes. The used diagnostic method is an algebraic technique called transition invariants analysis, which has been empirically shown to provide better results in terms of execution time [6] over the more known reachability analysis technique in Petri nets frameworks.

[4]There has been some research about dealing with loopy nets in graph theory that made a considerable advancement, notably [75, 113, 114].

[5]Note that how the probabilities change does not make part of the scope of this work. It could be implemented nonetheless through a different process that should make an idea for a further paper.

Probabilistic reasoning belongs to a larger research field, that is uncertainty modeling. This last offers and exploits other formalisms such as fuzzy sets and systems, possibility theory, probabilistic logic and Markov models. As to future work, such formalisms should offer a different perspective on the uncertainty associated with the diagnostic process in the distributed context, and they are waiting for exploitation.

Chapter 5

Distributed Diagnosis with Possibilistic Petri Nets

> The imprecision that is intrinsic in natural languages is, in the main, possibilistic rather than probabilistic in nature.
>
> *Zadeh, Fuzzy Sets and Systems, 1978*

5.1 Introduction

As a second contribution, we exploit another formalism to model uncertainty; that is *possibility theory*. Integrated in a PN framework, a class of PNs called “possibilistic Petri nets" (PoPNs) is used to capture the possibilistic behavior of a system. Since that the work by Lee et al. [60] did not provide a formalization of the diagnostic problem, the following formalization is suggested.

Reasoning under uncertain circumstances is considered as one of the human intelligence characteristics. One of the goals of artificial intelligence is to deal with such uncertainty; this includes understanding, modeling and simulating such aspect. The most known way to do so is using the classical probability theory, namely some formalisms like Bayesian networks (BNs) [47, 84] and Markov models [95, 118]. Another way to capture

uncertainty reasoning that has been exploited a lot in computer science is the fuzzy sets theory [119]. It is basically used to capture the fuzziness related to linguistic expressions. There are actually some other theories and formalisms that treat this subject but got less attention in terms of application, notably possibility theory [34, 77], the Dempster-Shafer theory of evidence [103], probabilistic logic [78], possibilistic logic [30] ... etc. The focus of this chapter will be on possibility theory and its application to distributed diagnosis.

Following the approaches of artificial intelligence to diagnosis, which includes model-based diagnosis (MDB), expert systems, rule-based diagnosis ... etc, we are more interested in model-based diagnosis. Whereas the diagnostic scheme is built upon a predefined model (usually mathematical) that supposedly captures the needed characteristics of the real system. By its turn, MDB is divided into two main approaches [39]: consistency-based diagnosis [27,97] and abductive diagnosis [18]. The most known work to frame a diagnostic problem in MDB is Reiter's formalization [97], where he describes it as a set of logical clauses with some observations on the system's status. A diagnostic process consists of inferring *explanations* of an *abnormal behavior* given some *observable manifestations*.

As a modeling formalism, Petri nets have been extensively used to model all sorts of processes, including diagnostic ones. Their capability to capture parallelism, synchronization, concurrency ... etc, makes them an adequate modeling tool. For instance, their mathematical representation allows a formal building of its techniques and makes it them easily translatable to computerized languages. A particular class of Petri nets is used in this work, called *"possibilistic Petri nets" (PoPNs)* [13,60], to capture the possibilistic behavior of a diagnostic process. It uses possibilistic tokens loaded with its two measures (*"possibility"* and *"necessity"*) with certain firing rules for transitions to compute any change in those measures. Influenced by Bennoui's work [6], we particularly investigate its extension to distributed systems, after showing how it could be used for centralized diagnosis using Portinale's framework [91].

The setting we take as subject to the diagnostic process is a distributed system composed of a set of interacting subsystems. Each of which is modeled by means of a PoPN with common bordered places to capture the interaction between them. Such interaction is captured through the passage of tokens through these bordered places. Each subsystem

has its own diagnostic system that could be referred to as a *diagnoser* following the terminology of [41] or simply an *agent* as in multi-agent systems due to their relevance to such settings, following the methodology of [6]. In fact, each agent can communicate with its neighboring agents to check the consistency of its local explanations with the others' knowledge. Hence, the inconsistent explanations shall be discarded.

The use of possibility theory instead of the well known probability theory is because, in real life applications when not enough data is collected to set accurate probabilities[1], possibility offers a better alternative [117]. Moreover, possibility is less sensitive to uncertainty measurement errors [32]. In fact, it has already been used in diagnostic approaches as an uncertainty model in both single [29] and multiple [117] fault diagnosis in centralized contexts.

The remainder of this chapter is organized as the following. The application of PoPNs for centralized diagnosis is illustrated in section 5.2. Section 5.3 demonstrates the extension of both diagnostic problem definition and PoPNs for distributed diagnosis. Moreover, a protocol of communication has been defined for diagnostic agents to share their local knowledge with the neighborhood if requested for solutions' consistency check, alongside a discussion about the correctness of the proposal in the same section. Finally, section 5.4 concludes the chapter.

5.2 Centralized Diagnosis (Formalization)

Before passing to distributed diagnosis, it is important to show a diagnostic process in the formalized framework to be used later.[2] When following a causal scheme to diagnosis using a Petri net model, it is important to make the projection of a causal model on a PoPN framework, which would be as following:

- a place corresponds to state of a causal model, hence three types of places could be

[1] Actually, this argument has been outlined by McCarthy and Hayes [68] to claim the inadequacy of probability from an epistemological point of view, here we quote "The information necessary to assign numerical probabilities is not ordinarily available." In contrast, Pearl offers another perspective on the subject matter, hence an interested reader is referred to his book [84].

[2] This section was considered as a part of the contribution because the only known work to use possibilistic Petri nets for diagnosis [60] did not formally define the diagnostic problem and just went with it intuitively.

distinguished accordingly;

- a transition represents the cause-effect relationship;
- a source place corresponds to an initial state;
- a sink place corresponds to either an internal state or a manifestation.

We follow the diagnostic problem definition presented in [20] as $DP = (BM, Ctx, \langle \Psi^+, \Psi^- \rangle)$ where DP stands for the diagnostic problem, BM represent the behavioral model of the system to be diagnosed, Ctx is the set of possible fault hypotheses (the observations have to be explained by means of elements of Ctx), $\langle \Psi^+, \Psi^- \rangle$ represent the made observation such that Ψ^+ is for manifestations to be entailed by a diagnosis and Ψ^- is for manifestations not to be entailed (they are in conflict with the first ones). Such a problem has been reformulated to the context of Petri nets where, following the causal model scheme, a diagnostic solution is given in terms of source places (corresponding to initial nodes) that should have an initial marking μ^{ini} that is consistent with the made observations.

The illustrated definition of a diagnostic problem is considered to be an "*abduction problem with consistency constraints*," in which a diagnosis could be seen logically as a set of assumptions ($\Delta \subseteq Ctx$) about the presence of a fault such that:

$$\begin{aligned} \forall m \in \Psi^+ : BM \cup \Delta \vdash m; \\ \forall n \in \Psi^- : BM \cup \Delta \nvdash n. \end{aligned} \tag{5.1}$$

Assumption 3. The PoPN model we use is safe and irreflexive.

Definition 19. *A marking μ of a PoPN is said to be final if there is no transitions to be fired at μ.*

Theorem 3. *In a marked PoPN there is exactly one final marking.*

Proof. This theorem can be proven in the same manner as theorem IV-B of [92], where the author used the properties: safeness, irreflexitivity and the absence of source transitions to sketch the final marking uniqueness from determinism. □

The assumption that the net model is safe and irreflexive is a common one for diagnostic models. Furthermore, the projection of the diagnostic problem definition on a PoPN framework would result the following definition. A possibilistic Petri net diagnostic problem is defined as $PoPNDP = (N, P^{ini}, \langle P^+, P^- \rangle)$, such that: an initial marking μ^{ini} is a solution to $PoPNDP$ if and only if the final marking μ of N covers P^+ and zero-covers P^- according to the following definition.

Definition 20. *Let $Q \subseteq P$ and let $N = \langle P, T, F \rangle$ be a Petri net, a marking μ of a N is said to cover Q if and only if $\forall p \in Q \rightarrow \mu(p) = 1$; while it is said to zero-cover Q if and only if $\forall p \in Q \rightarrow \mu(p) = 0$.*

To explain the modeling methodology, we suggest the following example of a faulty PoPN model.

	state	Faulty value
Initial states	*piston_state*	*worn*
	ground_clearance	*low*
	oil_sump_state	*worn*
	spark_plague_mileage	*high*
	carbur_tuning	*severe*
Internal states	*oil_consumption*	*high*
	oil_sump	*holed*
	oil_lack	*intense*
	engine_temp	*high*
	incr_cool_temp	*high*
	cool_leakage	*high*
	spark_ign	*irreg*
	mixt	*irreg*
	mixt_ign	*irreg*
Manifestations	*exhaust_smoke*	*black*
	hole_in_oil_sump	*yes*
	oil_light	*on*
	temp_indic	*red*
	smoke_from_ing	*yes*
	acc_resp	*irreg*

Table 5.1: States and their faulty values.

Example 5. As a centralized example, let's re-use the one presented in [91]. We illustrate first how a diagnosis is performed in a general manner, then we demystify how PoPNs

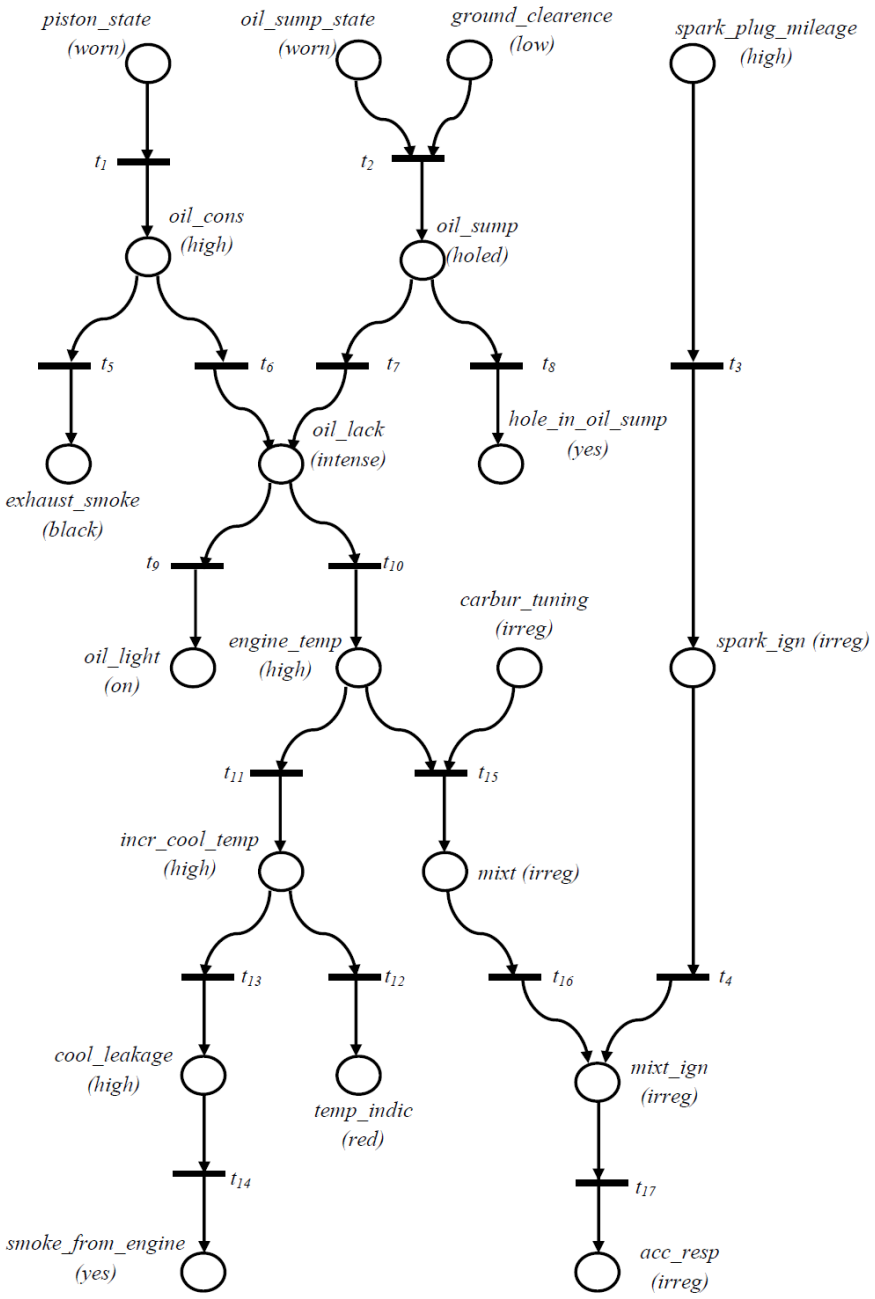

Figure 5-1: A simple example of a faulty behavior of a car.

t	t_1	t_2	t_3	t_4	t_5	t_6
p	(0.9, 1.0)	(0.5, 1.0)	(0.4, 1.0)	(0.5, 1.0)	(0.8, 1.0)	(0.6, 1.0)
t	t_7	t_8	t_9	t_{10}	t_{11}	t_{12}
p	(0.8, 1.0)	(0.9, 1.0)	(0.9, 1.0)	(0.8, 1.0)	(0.9, 1.0)	(0.9, 1.0)
t	t_{13}	t_{14}	t_{15}	t_{16}	t_{17}	
p	(0.9, 1.0)	(0.9, 1.0)	(0.8, 1.0)	(0.7, 1.0)	(0.7, 1.0)	

Table 5.2: Possibilities associated to transitions of Example 5.

could be used in this context to model the uncertainty related to the diagnostic process. The three types of places are distinguishable as in Table 5.1 and the possibility measures associated to each transition are illustrated in Table 5.2. A diagnosis could be performed using a reachability graph [3] or invariant analysis [55, 69], albeit the invariant analysis approach has been empirically shown to provide better results in terms of time needed to accomplish a diagnostic process in both centralized and distributed contexts [6, 91]. It is to be noted that the shown example is originally represented logically in terms of *definite clauses* without recursion[3] of the form

$$piston\_state(worn) \rightarrow oil\_cons(high).$$

In the example, graphically illustrated in Fig.5-1, let's suppose that we have the observation $hole\_in\_oil\_sump(yes)$. Such an observation implicates the presence of a token in the place $hole\_in\_oil\_sump(yes)$ that holds a certain possibility measures, supposedly $N_{hole\_in\_oil\_sump(yes)} = 0.5$ and $\Pi_{hole\_in\_oil\_sump(yes)} = 1.0$. Just intuitively[4] it is possible to track it back to the initial states[5] to obtain

$$\delta_1 =< ground\_clearance(low), oil\_sump\_state(worn) >,$$

[3]This sort of representation could be used in logic-based programming languages.

[4]Even though the construction of a reachability graph or calculating the invariants that hold the $hole\_in\_oil\_sump(yes)$ state is not that much of a task for a simple subnet like this, however the purpose here is just to demonstrate the use of possibilistic reasoning in diagnosis, so a formal building to it is not necessary. In this case, we suppose that the only made observation is $hole\_in\_oil\_sump(yes)$, with an undetermined state of other observations. That means: $\Psi^+ = \{hole\_in\_oil\_sump(yes)\}$ and $\Psi^- = \emptyset$.

[5]A little confusion could be due to general use of the word "*state*" for the net markings in Petri nets frameworks. however, following Portinale's framing [91], a state here represent a partial state, i.e. conditions concerning a part of the model.

whereas its possibility measures are given as $(\delta_1, (0.5, 1.0))$. It is possible to confirm the obtained measures by the application of Eq. (3.6) on δ_1 using the possibility measures illustrated in Table 5.2 corresponding to transitions t_2 and t_8 onto the firing sequence leading to the state $hole\_in\_oil\_sump(yes)$.

5.3 Distributed Diagnosis

5.3.1 Motivation

There are a lot of reasons that motivate the tendency towards distribution rather than keeping up with centralization. The first of them all is the distributed nature of the systems to be diagnosed themselves. For instance, all modular and networked systems like the Internet or industrial plants make good examples for such a nature. Furthermore, to break the complexity of a system following the paradigm of "*divide & conquer.*" For some systems characterized with complexity and considerable dynamicity, it is hard to maintain and accurate view on the system model over time. Another reason is encapsulation; where a global knowledge on the system model is just not desired to keep the privacy of some of its parts.

5.3.2 System Model

Starting from the system description, the distributed diagnostic problem could be formalized as the conjunction of n local diagnostic problem, hence

$$DP = \bigcup_{i=1}^{n} DP_i,$$

with each DP_i corresponds to a subsystem. Nonetheless, a local diagnostic problem couldn't be solved exactly as a centralized problem without considering the interaction mediums, which could be categorized into two subclasses: "*In*" mediums and "*Out*" mediums. Following this perception, the definition of a local diagnostic problem becomes as Def.21.

Definition 21. *For a subsystem S_i, a local diagnostic problem is defined as $DP_i = (BM_i, Ctx_i, In_i, Out_i, \langle \Psi_i^+, \Psi_i^- \rangle)$, where:*

- *BM_i is the behavioral model of S_i;*
- *Ctx_i is the set of local possible fault causes;*
- *In_i and Out_i correspond to interaction mediums as inputs and outputs respectively;*
- *$\langle \Psi_i^+, \Psi_i^- \rangle$ correspond to the local observations that should (respectively shouldn't) be entailed.*

In such a view, a local solution (diagnosis) of a local diagnostic problem DP_i could be seen logically as a set of assumptions $\Delta_i \subseteq Ctx_i$ about the presence of a local fault such that:

$$\begin{aligned} \forall m \in \Psi_i^+ : BM_i \cup In_i \cup \Delta_i \vdash m; \\ \forall n \in \Psi_i^- : BM_i \cup In_i \cup \Delta_i \nvdash n. \end{aligned} \tag{5.2}$$

As it could be observed in Def. 21, the diagnostic problem definition changed to hold i as the index of subsystems, alongside In_i and Out_i as the sets of interaction elements. As it is deducible from their terminology: In_i corresponds to the set of input elements to S_i; while Out_i corresponds to outputs from S_i. Following the causal view, the elements of Out_i fit into the description of a manifestation from an agent A_i perception, as the last element of a causality chain in a subsystem S_i. Hence, it is possible to distinguish accordingly two subsets of Out_i: that is Out_i^+ and Out_i^-. Naturally, Out_i^+ to the deducible values of BM_i and Out_i^- to those contradicting the previous ones. Logically, this could be formalized as:

$$\begin{aligned} \forall a \in Out_i^+ : BM_i \cup In_i \cup \Delta_i \vdash a; \\ \forall b \in Out_i^- : BM_i \cup In_i \cup \Delta_i \nvdash b. \end{aligned} \tag{5.3}$$

By combining Eq. (5.2) and Eq. (5.3), we would obtain a general logical definition of a consistent local diagnosis as:

$$\begin{aligned} \forall m \in \Psi_i^+ \cup Out_i^+ : BM_i \cup In_i \cup \Delta_i \vdash m; \\ \forall n \in \Psi_i^- \cup Out_i^- : BM_i \cup In_i \cup \Delta_i \nvdash n. \end{aligned} \tag{5.4}$$

5.3.3 The DP Projection on PoPNs

In terms of a PoPN model, the PoPN diagnostic problem could be induced from the distributed diagnostic problem as

$$PoPNDP = \bigcup_{i=1}^{n} PoPNDP_i.$$

Furthermore, a projection of Def. 21 on a PoPN framework would result the next definition.

Definition 22. *For a subsystem S_i modeled by a PoPN, a local diagnostic problem is defined as $PoPNDP_i = (N_i, P_i^{In}, P_i^{Out}, \langle P_i^+, P_i^- \rangle)$, where:*

$N_i = (P_i, PT_i, A_i)$ is a PoPN model of S_i;

P_i^{In} and P_i^{Out} are two sets of places denoting elements of In_i and Out_i respectively;

In_i and Out_i correspond to interaction mediums as inputs and outputs respectively;

$\langle P_i^+, P_i^- \rangle$ correspond to places representing local observations that should (respectively shouldn't) be entailed.

Some properties of a global net model composed of a conjunction of local models as $N = \bigcup_{i=1}^{n} N_i$ (s.t. $N = (P, PT, A)$) can be depicted as follows:

- Given that $P = \bigcup_{i=1}^{n} P_i$; and $\forall i \rightarrow \exists j$ s.t. $P_i \cap P_j \triangleq P_{ij} \neq \emptyset, P_{ij} \subseteq P_i^{In} \cup P_i^{Out}$;
- $PT = \bigcup_{i=1}^{n} PT_i$; and $\forall i \neq j \rightarrow PT_i \cap PT_j = \emptyset$;
- $P^{In} = \{p | (p^\bullet \in PT_i) \wedge ({}^\bullet p \notin PT_i)\}$; and $P^{Out} = \{p | (p^\bullet \notin PT_i) \wedge ({}^\bullet p \in PT_i)\}$.

Assumption 4. The net model representing the interaction between subsystems is acyclic[6].

5.3.4 Cooperation Protocol

It is possible for a diagnostic process to generate multiple diagnoses for a same given observation, some of which may simply be wrong or inconsistent with the global model knowledge. Thus, to rectify the obtained diagnoses, establishing a communication protocol

[6]Such an assumption is relaxed to avoid an infinite loop of blames among agents [98].

is necessary for acquiring such knowledge to provide a basis for discarding some of them. The protocol we are proposing is not supervised, meaning that it is agent-oriented without the need of a global supervision. An important part of it was inspired from [6], which seems appropriate for this case due to the resemblance of the systems models.

Since diagnoses are given in terms if initial markings, including the marked places belonging to P_i^{In}, agent A_i requests from its neighboring agent A_j its predicted values of places in P_i^{In}. For A_j, those are values belonging to P_j^{Out}. Fig. 5-2 sketches a general perception on the communication protocol between two agents. Henceforth, it is illustrated in the following steps:

1. at some point, the net model will reach its final marking;

2. each agent starts from its local final marking as local observations;

3. they track back the sources of resulting these observations; that is computing initial markings μ_i^{ini} of each net model i;

4. for an agent A_i obtaining $\mu(P_i^{In}) \neq \emptyset$ (s.t. $\mu(P_i^{In}) \in \mu_i^{ini}$), it sends a message $msg_{i \to j}$ to its neighboring agent A_j (corresponding to the subsystem S_j that shares bordered places with it) requesting its predicted marking of output places ($\mu(P_i^{Out})$ corresponding to P_i^{In};

5. then a comparison is made between $\mu(P_i^{In})$ and $\mu(P_j^{Out})$;

6. if some of (or all) the local diagnoses made by A_i are not supported by $\mu(P_j^{Out})$, then a refinement of diagnoses should be done by discarding inconsistent ones;

7. in case neither of the obtained diagnoses by A_i is supported by $\mu(P_j^{Out})$, a negative response is sent to A_j;

8. otherwise, a positive response should be sent to A_j;

9. the protocol keeps going until it reaches a stable point where all the obtained diagnoses are consistent with each other.

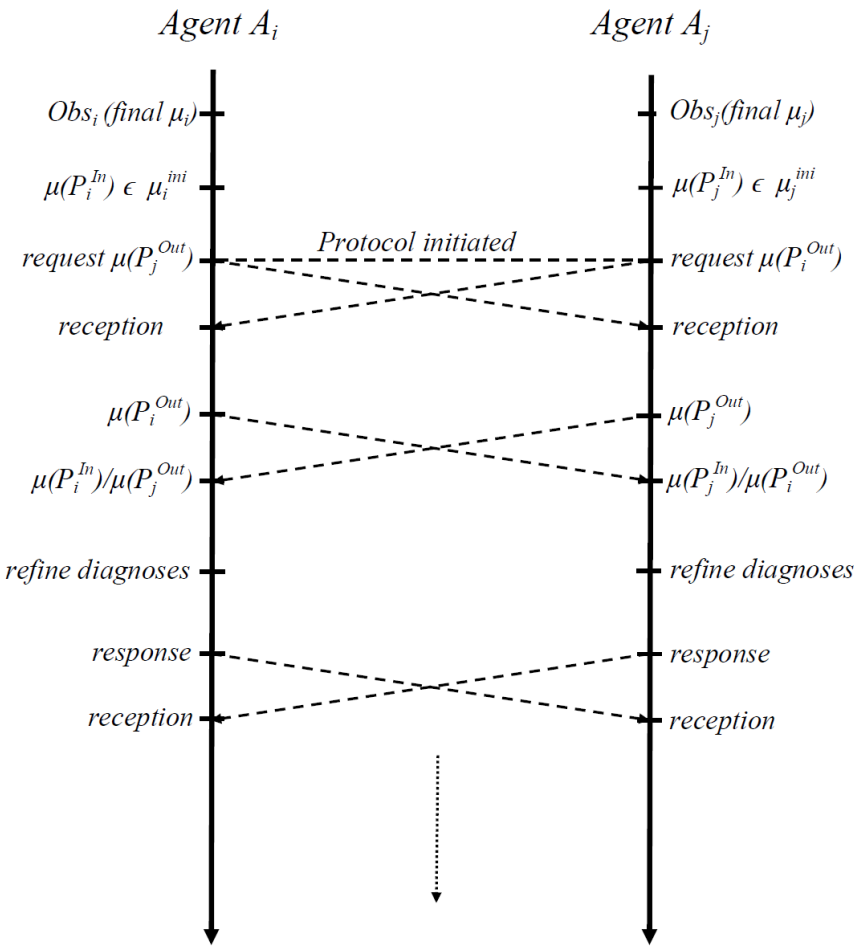

Figure 5-2: Two agents communicating.

Remark 5. *The explained protocol above is from one agent's point of view, so each agent is meant to execute this protocol once they find input places marked alongside an initial marking. Furthermore, the communication between the two agents illustrated in Fig. 5-2 seems synchronized, which is not the case actually (e.g., agents do not necessarily request the markings of Out places of other subsystems simultaneously).*

5.3.5 Diagnoses Computation

Proposition 1. Let $\Delta = \{\delta_1, \ldots, \delta_n\}$ be a set of possible diagnoses; and let σ be the firing sequence leading from the explanation δ_i to its corresponding manifestation.

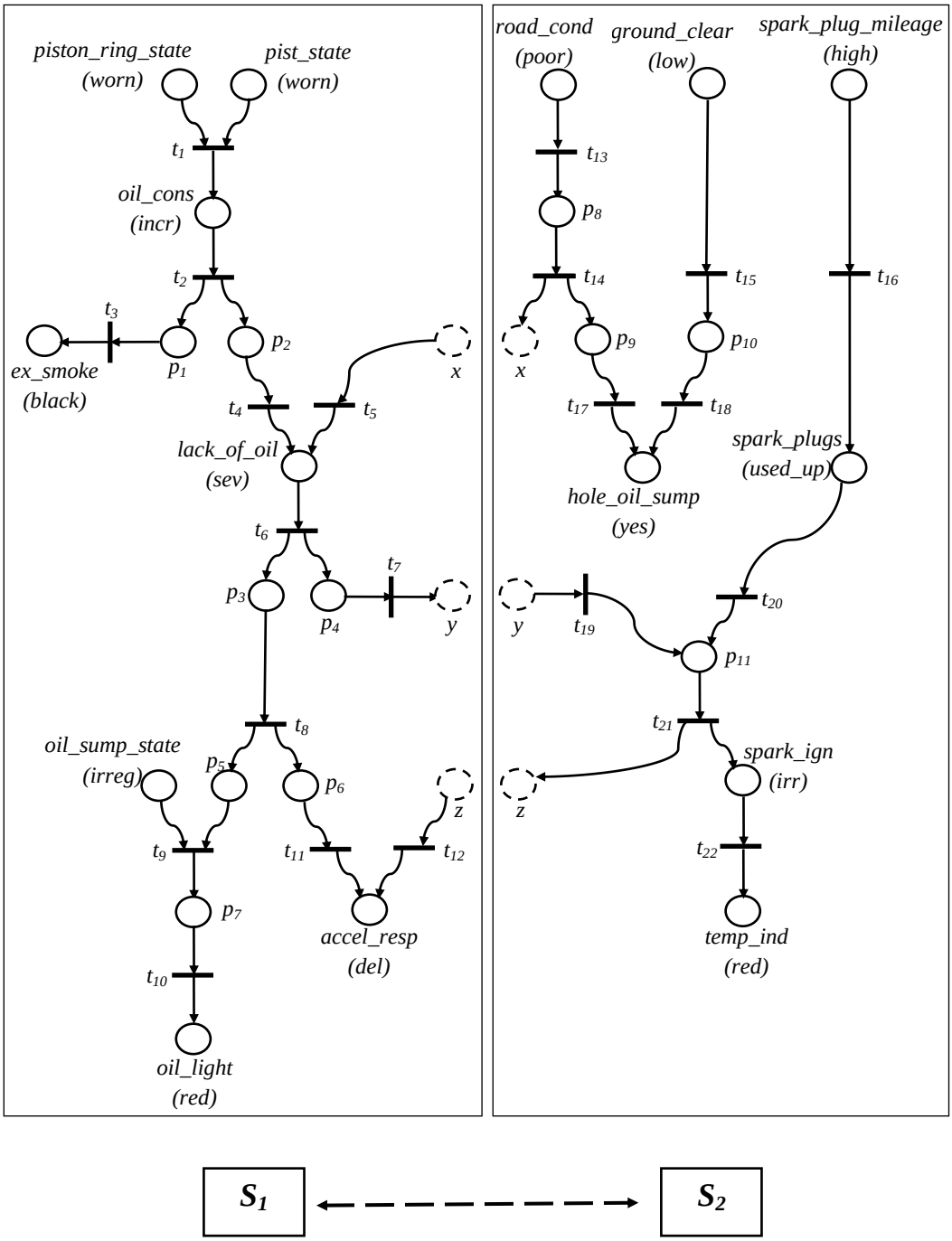

Figure 5-3: An example of an open PoPN.

state	Acronym	Faulty value
piston ring state	*pist_ring_state*	*worn*
piston state	*pist_state*	*worn*
oil consumption	*oil_cons*	*increased*
exhaustive smoke	*ex_smoke*	*black*
lack of oil	*lack_oil*	*severe*
oil sumption state	*oil_sump_state*	*worn*
oil light	*oil_light*	*red*
acceleration response	*accel_resp*	*delayed*
road conditions	*road_cond*	*poor*
ground clearance	*ground_clear*	*low*
spark plug mileage	*spark_plug_mileage*	*high*
spark plugs	*spark_plugs*	*used_up*
hole in oil sumption	*hole_oil_sump*	*yes*
spark ignition	*spark_ign*	*irregular*
temperature indicator	*temp_ind*	*red*

Table 5.3: States and their description.

t	t_1	t_2	t_3	t_4	t_5	t_6
p	(0.4, 1.0)	(0.9, 1.0)	(0.7, 1.0)	(0.6, 1.0)	(0.7, 1.0)	(0.6, 1.0)
t	t_7	t_8	t_9	t_{10}	t_{11}	t_{12}
p	(0.7, 1.0)	(0.8, 1.0)	(0.9, 1.0)	(0.8, 1.0)	(0.8, 1.0)	(0.7, 1.0)
t	t_{13}	t_{14}	t_{15}	t_{16}	t_{17}	t_{18}
p	(0.6, 1.0)	(0.7, 1.0)	(0.8, 1.0)	(0.9, 1.0)	(0.8, 1.0)	(0.7, 1.0)
t	t_{19}	t_{20}	t_{21}	t_{22}		
p	(0.8, 1.0)	(0.9, 1.0)	(0.8, 1.0)	(0.9, 1.0)		

Table 5.4: Possibilities associated to transitions of Example 6.

If $\exists t \in \sigma \cap T^i$ (T^i is the set if inference transitions), such that: $N_t < N_{\delta_i}$ or $\Pi_t > \Pi_{\delta_i}$; then the diagnosis δ_i is inconsistent.

Proof. The proof follows from the definition of the possibility measures where a necessity N is supposed to be the lower bound and a possibility Π is supposed to be the upper bound, and using the PoPNs firing rules (discussed in the preliminaries section), mainly Eq. (3.5). □

After obtaining the first results of the diagnostic process, it is possible to discard some of them that are inconsistent with the neighbors' local knowledge, since they don't belong

$\varsigma_1^1 = \{pist\_ring\_state(worn), oil\_cons(incr), p_1, ex\_smoke(black)\}$;
$\varsigma_1^2 = \{pist\_state(worn), oil\_cons(incr), p_1, ex\_smoke(black)\}$;
$\varsigma_1^3 = \{pist\_ring\_state(worn), oil\_cons(incr), p_2, lack\_of\_oil(sev), p_4, y\}$;
$\varsigma_1^4 = \{pist\_state(worn), oil\_cons(incr), p_2, lack\_of\_oil(sev), p_4, y\}$;
$\varsigma_1^5 = \{pist\_ring\_state(worn), oil\_cons(incr), p_2, lack\_of\_oil(sev), p_3, p_6, accel\_resp(del)\}$;
$\varsigma_1^6 = \{pist\_state(worn), oil\_cons(incr), p_2, lack\_of\_oil(sev), p_3, p_6, accel\_resp(del)\}$;
$\varsigma_1^7 = \{pist\_ring\_state(worn), oil\_cons(incr), p_2, lack\_of\_oil(sev), p_3, p_7, oil\_sump\_state(worn), p_5, oil\_light(red)\}$;
$\varsigma_1^8 = \{pist\_state(worn), oil\_cons(incr), p_2, lack\_of\_oil(sev), p_3, oil\_sump\_state(worn), p_5, p_7, oil\_light(red)\}$;
$\varsigma_1^9 = \{x, lack\_of\_oil(sev), p_4, y\}$;
$\varsigma_1^{10} = \{x, lack\_of\_oil(sev), p_3, p_6, accel\_resp(del)\}$;
$\varsigma_1^{11} = \{x, lack\_of\_oil(sev), p_3, oil\_sump\_state(worn), p_5, p_7, oil\_light(red)\}$;
$\varsigma_1^{12} = \{z, accel\_resp(del)\}$.

Table 5.5: Minimal supports P-invariants of S_1.

to the set of global diagnoses. The following example illustrates this.

Example 6. Let's consider the distributed system shown in Fig. 5-3 which was adapted from [6] with a little restructuring to suit the specifications of a PoPN, whereas Table 5.3 and Table 5.4 present the system's states and the possibility measures of its transitions, respectively. Moreover, Table 5.5 and Table 5.6 present the computed minimal supports of P-invariants of subsystems S_1 and S_2, respectively. Suppose that the observed system reached its final marking with the following:

$\varsigma_2^1 = \{road\_cond(poor), p_8, x\}$;
$\varsigma_2^2 = \{road\_cond(poor), p_8, p_9, hole\_oil\_sump(yes)\}$;
$\varsigma_2^3 = \{ground\_clear(low), p_{10}, hole\_oil\_sump(yes)\}$;
$\varsigma_2^4 = \{spark\_plug\_mileage(high), spark\_plugs(used\_up), p_{11}, spark\_ign(irr), temp\_ind(red)\}$;
$\varsigma_2^5 = \{spark\_plug\_mileage(high), spark\_plugs(used\_up), p_{11}, z\}$;
$\varsigma_2^6 = \{y, p_{11}, spark\_ign(irr), temp\_ind(red)\}$;
$\varsigma_2^7 = \{y, p_{11}, z\}$.

Table 5.6: Minimal supports P-invariants of S_2.

- for the subsystem S_1:
  1. place $ex\_smoke(black)$ is empty;
  2. place $oil\_light(red)$ is empty;
  3. the marking of place $accel\_resp(rel)$ is unknown (it is possible for an agent to not recover all the markings of manifestations);
- for the subsystem S_2:
  1. place $hole\_oil\_sump(yes)$ is empty;
  2. place $temp\_ind(red)$ is marked with a token holding the measures (0.8, 1.0);

Performing a diagnostic process based on P-invariants would proceed as:

- the only known marked place observed by A_2 is $temp\_ind(red)$;
- according to Table 5.6, this place belongs to two P-invariants ($temp\_ind(red) \in \varsigma_2^4$ and $temp\_ind(red) \in \varsigma_2^6$);
- tracking back this manifestation to its source places in both invariants would result two possible diagnoses:
  1. $\delta_1 =< spark\_plug\_mileage(high) >$ (s.t. $(\delta_1, (0.8, 1.0))$);
  2. $\delta_2 =< y >$ (s.t. $(\delta_2, (0.8, 1.0))$);
- among the obtained diagnoses, one is not explained locally which would initiate the communication protocol to get the Out marking of y ($\mu(y^{Out})$ belonging to S_1;
- according to Table 5.5, y belongs to ς_1^3 and ς_1^9
- since no manifestation was observed, all source places of S_1 are assumed to be empty, including those belonging to ς_1^3, while ς_1^9 lead to another bordered place which would invocate its neighboring agent A_2 to provide $\mu(x^{Out})$ belonging to S_2;
- place x belongs to one invariant ς_2^1 that possesses one source place $road\_cond(poor)$ which is assumed to be empty since the other invariant leading to it has an empty manifestation ($hole\_oil\_sump(yes)$);

- A_2 responds to A_1 with a message indicating that $\mu(x^{Out}) = \emptyset$, then A_1 responds to A_2 with a message indicating that $\mu(y^{Out}) = \emptyset$;
- hence, A_2 discards δ_2 since it is inconsistent, and the protocol would terminate.

Remark 6. *In the illustrated example, even in case y could be found marked, its token would hold at least a necessity of 0.7 from the firing of the inference transition $t_7 = {}^\bullet y$ which is less than the observed 0.8 (that is an inconsistency).*

5.3.6 Proof of Correctness

Proposition 2. Let Δ_{global} be the set of global diagnoses of the whole distributed system, with $DP = (N, \langle P^+, P^- \rangle)$ as its diagnostic problem; given that Δ_i is the set of local diagnoses of a subsystem i, with $DP_i = (N_i, P_i^{In}, P_i^{Out}, \langle P_i^+, P_i^- \rangle)$ as its diagnostic problem, such that $DP = \bigcup_{i=1}^{n} DP_i$; then the projection of global diagnoses on the subnet N_i should result the local diagnoses (i.e., $\Pi_{N_i}(\Delta_{global}) = \Delta_i$), when the protocol of communication terminates, $\forall i \in \{1 \dots n\}$.

Proof. Since both global and local diagnoses are obtained using the same computation technique from the same given observations on the same model; the projection of a global diagnosis on a local model should be seen as a local one. □

The above proposition indicates that, given one centralized diagnostic system (a global diagnostic agent) in charge of the distributed system as a whole, its obtained diagnoses for the subnet N_i corresponding to a subsystem S_i should be also obtained by the local diagnostic agent corresponding to S_i. Consequently, all obtained diagnoses by the global agent should also be derived by local ones. In the view of P-invariants, if L is the set of P-invariants of the global PoPN model with L_i a set of local P-invariants of N_i, then L could be derived as the composed union over common bordered places of all sets L_i. Moreover, the proof of the termination of the communication protocol after a finite number of rounds could be derived from the model's properties of safeness (assumed in Assumption 3) and its acyclicity over composed sub-model (assumed in Assumption 4).

5.4 Conclusion

The main issue treated in this chapter was also the quantification of the uncertainty associated with diagnosis, particularly in the distributed context. To do so, this time, a class of high-level Petri nets called Possibilistic Petri nets has been used to capture uncertainty on the ground of possibility theory. In a setting composed of interacting subsystems, the possibility measures observed on tokens could be used to check the consistency of local explanations with exterior knowledge, provided through the communication of agents with each other. Thus, a communication protocol was set to ensure knowledge sharing. Meanwhile, the interaction between subsystems is captured through the passage of possibilistic tokens through common bordered places. The diagnostic problem definition of a centralized system was extended to suit the distributed case and projected on PoPNs to build a correspondence with the distributed model. Furthermore, a discussion about the correctness of the proposal is provided.

Chapter 6

Conclusion

The tendency of systems' design and implementation towards complex systems is inevitable. It is a natural consequence a more and more interconnected world and detailed systems to fulfill certain objectives desired by developers. Keeping up with such tendency requires confronting the difficulties that come with a system's complexity, which pushed for distributed approaches to break it. Diagnostic approaches are no exception to that, whereas the suggested approaches rely on distributing tasks on a set of agents to break complexity.

The context of this thesis is the diagnosis of distributed systems. following artificial intelligence approaches, more specifically model-based ones, the work proceeds on a high level of abstraction. It utilizes models' properties to perform a diagnostic reasoning. The considered system is divided into a set of subsystems interacting with each other. Each of which is modeled substantially by a Petri net. For the first contribution, probability propagation nets were the used net model; and for the second contribution, possibilistic Petri nets were used.

In this thesis, a particular focus was given to modeling uncertainty within a distributed diagnosis framework. Since the chosen basic model for a system here is Petri nets, two extended classes of them were used to capture uncertainty. The first class, probability propagation nets, underwent a process of distribution itself to introduce the class of distributed probability propagation nets, a class in which interaction components are explicitly distinguished and separated into two types according to the diagnostic agent's perception on them. The other class, possibilistic Petri nets, needed to be put under a formal specifica-

tion of a diagnostic problem first in order to set the context. Then, to set the modeling formalism for distributed diagnosis purposes, the definition of a diagnostic problem had to adjusted to consider interaction aspects, which also included the PoPN model by projection. In order check the consistency of obtained local diagnoses, diagnostic agents would need to communicate with each other, which requires setting a protocol for communication to ensure such communication. Finally, an evaluation of the correctness of the approach and the termination of the communication protocol was discussed.

Providing a quantifiable basis of uncertainty related to obtained diagnoses would certainly help distinguish between them, especially in decision-making processes. Whereas the more known probability theory (captured by PPNs) provides a ranking feature to classify diagnoses. On the other hand, the ranking feature would appear less in possibility theory[1] (captured by PoPNs), but the values of its measures could be used in consistency checking.

For those who are interested in building upon, completing or simply working on a similar synthesis to this thesis, pointing out some of the obstacles encountered while realizing it may be quite helpful. Hence, the following points take place.

- The main obstacle in realizing this thesis was dealing with the uncertainty context, such that it takes away a lot of valid properties in the certain context, e.g., the possibility to claim an inconsistency, which is an essential property to reduce the number of possible diagnoses.

- The high level of abstraction of the field (that is supposed to be oriented towards applicative approaches) made it difficult to keep track of real life systems requirements.

- Having multiple research communities working on the field made the state of the art too large, and one can easily get lost in the literature of the "wrong" community.

- Another difficulty found while producing this thesis was the largeness and diversity of the uncertainty field. From merely philosophical points of view about it to its

[1]Comparison between firm numbers is clear and straightforward, unlike comparison between intervals which is not always firm, that is the case of possibility theory.

intuitively simple models in terms of abstraction level, passing by the variety of ways to perceive it and cope with it, having an overall look is not evident.

As to future work and perspectives, a lot is still to be done. For instance, in Petri nets alone, there is a considerable amount of classes manipulating uncertainty that were not exploited in distributed diagnosis (e.g., fuzzy Petri nets). Aside from Petri net models, formalisms dealing with uncertainty keep getting advanced by mathematicians that need to be put into application such as the Dempster-Shafer theory of evidence and probabilistic logic. On a different track for perspectives, such work needs to be more oriented towards real life applications.

Reasoning under uncertainty turned out to be a larger field than expected!

Bibliography

[1] Armen Aghasaryan, Eric Fabre, Albert Benveniste, Renée Boubour, and Claude Jard. Fault detection and diagnosis in distributed systems: an approach by partially stochastic petri nets. *Discrete event dynamic systems*, 8(2):203–231, 1998.

[2] Mildreth Alcaraz-Mejia, Ernesto Lopez-Mellado, Antonio Ramírez-Treviño, and Israel Rivera-Rangel. Petri net based fault diagnosis of discrete event systems. In *Systems, Man and Cybernetics, 2003. IEEE International Conference on*, volume 5, pages 4730–4735. IEEE, 2003.

[3] Cosimo Anglano and Luigi Portinale. Bw analysis: a backward reachability analysis for diagnostic problem solving suitable to parallel implementation. In *International Conference on Application and Theory of Petri Nets*, pages 39–58. Springer, 1994.

[4] Paolo Baldan, Andrea Corradini, Hartmut Ehrig, and Reiko Heckel. Compositional semantics for open petri nets based on deterministic processes. *Mathematical Structures in Computer Science*, 15(01):1–35, 2005.

[5] Hammadi Bennoui. *Distributed Causal Model-based Diagnosis: An Approach by Interacting Petri Nets*. PhD thesis, University of Biskra, 2012.

[6] Hammadi Bennoui. Interacting behavioral petri nets analysis for distributed causal model-based diagnosis. *Autonomous agents and multi-agent systems*, 28(2):155–181, 2014.

[7] Yasser M Berghout and Hammadi Bennoui. Introduction to distributed probability propagation nets. In *Proceedings of the International Conference on Intelligent Information Processing, Security and Advanced Communication*, page 29. ACM, 2015.

[8] Yasser Moussa Berghout and Hammadi Bennoui. Distributed diagnosis based on distributed probability propagation nets. *International Journal of Computational Science and Engineering (In press)*.

[9] Jonas Biteus, Erik Frisk, and Mattias Nyberg. Distributed diagnosis using a condensed representation of diagnoses with application to an automotive vehicle. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 41(6):1262–1267, 2011.

[10] Walid Bouallègue, Salma Bouslama Bouabdallah, and Moncef Tagina. Causal approaches and fuzzy logic in fdi of bond graph uncertain parameters systems. In *Communications, Computing and Control Applications (CCCA), 2011 International Conference on*, pages 1–6. IEEE, 2011.

[11] Maria Paola Cabasino, Alessandro Giua, Andrea Paoli, and Carla Seatzu. Decentralized diagnosis of discrete-event systems using labeled petri nets. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 43(6):1477–1485, 2013.

[12] Vito Calderaro, Christoforos N Hadjicostis, Antonio Piccolo, and Pierluigi Siano. Failure identification in smart grids based on petri net modeling. *IEEE Transactions on Industrial Electronics*, 58(10):4613–4623, 2011.

[13] Janette Cardoso, Robert Valette, and Didier Dubois. Possibilistic petri nets. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 29(5):573–582, 1999.

[14] Christos G Cassandras and Stephane Lafortune. *Introduction to discrete event systems*. Springer Science & Business Media, 2009.

[15] Didier Cayrac, Didier Dubois, and Henri Prade. Handling uncertainty with possibility theory and fuzzy sets in a satellite fault diagnosis application. *IEEE Transactions on fuzzy Systems*, 4(3):251–269, 1996.

[16] Sheng-Luen Chung, Chien-Chung Wu, and MuDer Jeng. Failure diagnosis: a case study on modeling and analysis by petri nets. In *Systems, Man and Cybernetics, 2003. IEEE International Conference on*, volume 3, pages 2727–2732. IEEE, 2003.

[17] Luca Console and Oskar Dressler. Model-based diagnosis in the real world: lessons learned and challenges remaining. In *IJCAI*, volume 99, pages 1393–1400, 1999.

[18] Luca Console, Daniele Theseider Dupré, and Pietro Torasso. On the relationship between abduction and deduction. *Journal of Logic and Computation*, 1(5):661–690, 1991.

[19] Luca Console and Pietro Torasso. Hypothetical reasoning in causal models. *International Journal of Intelligent Systems*, 5(1):83–124, 1990.

[20] Luca Console and Pietro Torasso. A spectrum of logical definitions of model-based diagnosis1. *Computational intelligence*, 7(3):133–141, 1991.

[21] Gregory F Cooper. The computational complexity of probabilistic inference using bayesian belief networks. *Artificial intelligence*, 42(2-3):393–405, 1990.

[22] M-O Cordier, Philippe Dague, François Lévy, Jacky Montmain, Marcel Staroswiecki, and Louise Travé-Massuyès. Conflicts versus analytical redundancy relations: a comparative analysis of the model based diagnosis approach from the artificial intelligence and automatic control perspectives. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 34(5):2163–2177, 2004.

[23] Philip T Cox and Tomasz Pietrzykowski. General diagnosis by abductive inference. In *Symposium on Logic Programming*.

[24] Matthew J Daigle, Xenofon D Koutsoukos, and Gautam Biswas. Distributed diagnosis in formations of mobile robots. *IEEE Transactions on Robotics*, 23(2):353–369, 2007.

[25] Randall Davis and Walter Hamscher. Model-based reasoning: Troubleshooting. *Exploring artificial intelligence*, 8:297–346, 1988.

[26] Gert De Cooman. Possibility theory i: the measure-and integral-theoretic groundwork. *International Journal of General Systems*, 25(4):291–323, 1997.

[27] Johan De Kleer, Alan K Mackworth, and Raymond Reiter. Characterizing diagnoses and systems. *Artificial Intelligence*, 56(2-3):197–222, 1992.

[28] Lorenz Demey, Barteld Kooi, and Joshua Sack. Logic and probability. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, winter 2016 edition, 2016.

[29] Didier Dubois, Michel Grabisch, Olivier De Mouzon, and Henri Prade. A possibilistic framework for single-fault causal diagnosis under uncertainty*. *INTERNATIONAL JOURNAL OF GENERAL SYSTEM*, 30(2):167–192, 2001.

[30] Didier Dubois, Jérôme Lang, and Henri Prade. Possibilistic logic 1. 1994.

[31] Didier Dubois, Hung T Nguyen, and Henri Prade. Possibility theory, probability and fuzzy sets misunderstandings, bridges and gaps. In *Fundamentals of fuzzy sets*, pages 343–438. Springer, 2000.

[32] Didier Dubois and Henri Prade. Epistemic entrenchment and possibilistic logic. *Artificial Intelligence*, 50(2):223–239, 1991.

[33] Didier Dubois and Henri Prade. Possibility theory, probability theory and multiple-valued logics: A clarification. *Annals of mathematics and Artificial Intelligence*, 32(1-4):35–66, 2001.

[34] Didier Dubois and Henri Prade. *Possibility theory: an approach to computerized processing of uncertainty*. Springer Science & Business Media, 2012.

[35] Didier Dubois and Henry Prade. Possibility theory and its applications: Where do we stand? In *Springer Handbook of Computational Intelligence*, pages 31–60. Springer, 2015.

[36] Oliver Faust, U Rajendra Acharya, and Toshiyo Tamura. Formal design methods for reliable computer-aided diagnosis: a review. *IEEE reviews in biomedical engineering*, 5:15–28, 2012.

[37] Dieter Fensel, Richard Benjamins, et al. *Assumptions in model-based diagnosis*. AIFB, Univ., 1997.

[38] Ildikó Flesch, Peter Lucas, and Theo Van Der Weide. Probabilistic properties of model-based diagnostic reasoning in bayesian networks. In *19th Belgium-Netherlands Artificial Intelligence Conference. Netherlands: Kluwer Academic Publishers*, pages 119–126. Citeseer, 2007.

[39] Ildikó Flesch, Peter JF Lucas, and Theo P van der Weide. Conflict-based diagnosis: Adding uncertainty to model-based diagnosis. In *IJCAI*, volume 2007, pages 380–385, 2007.

[40] Zhiwei Gao, Carlo Cecati, and Steven X Ding. A survey of fault diagnosis and fault-tolerant techniques—part i: Fault diagnosis with model-based and signal-based approaches. *IEEE Transactions on Industrial Electronics*, 62(6):3757–3767, 2015.

[41] Sahika Genc and Stéphane Lafortune. Distributed diagnosis of place-bordered petri nets. *Automation Science and Engineering, IEEE Transactions on*, 4(2):206–219, 2007.

[42] Sylviane Gentil, Jacky Montmain, and Christophe Combastel. Combining fdi and ai approaches within causal-model-based diagnosis. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 34(5):2207–2221, 2004.

[43] Pavlos S Georgilakis, John A Katsigiannis, Kimon P Valavanis, and Athanasios T Souflaris. A systematic stochastic petri net based methodology for transformer fault diagnosis and repair actions. *Journal of Intelligent and Robotic Systems*, 45(2):181–201, 2006.

[44] Xiaofei He, Xiaoyang Tong, and Mingwei Sun. Distributed power system fault diagnosis based on bayesian network and dempster-shafer evidence theory. *Dianli Xitong Zidonghua(Automation of Electric Power Systems)*, 35(10):42–47, 2011.

[45] E Hisdal. Possibilities and probabilities. *Ballester, A., Cardus, D. and Trillas, E*, 1982.

[46] Hesuan Hu, Zhiwu Li, and Abdulrahman Al-Ahmari. Reversed fuzzy petri nets and their application for fault diagnosis. *Computers & Industrial Engineering*, 60(4):505–510, 2011.

[47] Finn V Jensen. *An introduction to Bayesian networks*, volume 210. UCL press London, 1996.

[48] Zhichun Jia, Rong Chen, and Xing Xing. probabilistic fault diagnosis method for web services. *Journal of Computational Information Systems*, 9(21):8629–8637, 2013.

[49] George Jiroveanu and René K Boel. Distributed diagnosis for petri nets models with unobservable interactions via common places. In *Proceedings of the 44th IEEE Conference on Decision and Control*, pages 6305–6310. IEEE, 2005.

[50] Robert Ivor John and Peter R Innocent. Modeling uncertainty in clinical diagnosis using fuzzy logic. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 35(6):1340–1350, 2005.

[51] Gunjan Khanna, Ignacio Laguna, Fahad A Arshad, and Saurabh Bagchi. Distributed diagnosis of failures in a three tier e-commerce system. In *Reliable Distributed Systems, 2007. SRDS 2007. 26th IEEE International Symposium on*, pages 185–198. IEEE, 2007.

[52] Uffe B Kjærulff and Anders L Madsen. Probabilistic networks: an introduction to bayesian networks and influence diagrams. *Recuperado em*, 30, 2005.

[53] George Klir and Bo Yuan. *Fuzzy sets and fuzzy logic*, volume 4. Prentice hall New Jersey, 1995.

[54] George J Klir and David Harmanec. On modal logic interpretation of possibility theory. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 2(02):237–245, 1994.

[55] Kurt Lautenbach. Linear algebraic techniques for place/transition nets. In *Petri nets: central models and their properties*, pages 142–167. Springer, 1987.

[56] Kurt Lautenbach. Reproducibility of the empty marking. In *International Conference on Application and Theory of Petri Nets*, pages 237–253. Springer, 2002.

[57] Kurt Lautenbach, Stephan Philippi, and Alexander Pinl. Bayesian networks and petri nets. *Entwurf komplexer Autimatisierungssysteme, EKA*, 9, 2006.

[58] Kurt Lautenbach and Alexander Pinl. Probability propagation in petri nets. *Fachberichte Informatik*, pages 16–2005, 2005.

[59] Jonathan Lee, Kevin FR Liu, and Weiling Chiang. A possibilistic-logic-based approach to integrating imprecise and uncertain information. *Fuzzy Sets and Systems*, 113(2):309–322, 2000.

[60] Jonathan Lee, Kevin FR Liu, and Weiling Chiang. Modeling uncertainty reasoning with possibilistic petri nets. *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, 33(2):214–224, 2003.

[61] Dimitri Lefebvre. Fault diagnosis and prognosis with partially observed stochastic petri nets. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 228(4):382–396, 2014.

[62] Dimitri Lefebvre and Catherine Delherm. Diagnosis of des with petri net models. *IEEE Transactions on Automation Science and Engineering*, 4(1):114–118, 2007.

[63] Adrien Leitold, Miklós Gerzson, Anna I Pózna, and Katalin Hangos. On-line qualitative model-based diagnosis of technological systems using colored petri nets. In *EUROSIS*, 2014.

[64] Ma łgorzata Steinder and Adarshpal S Sethi. A survey of fault localization techniques in computer networks. *Science of computer programming*, 53(2):165–194, 2004.

[65] Baisi Liu, Mohamed Ghazel, and Armand Toguyéni. Model-based diagnosis of multi-track level crossing plants. *IEEE Transactions on Intelligent Transportation Systems*, 17(2):546–556, 2016.

[66] Peter JF Lucas. Bayesian model-based diagnosis. *International Journal of Approximate Reasoning*, 27(2):99–119, 2001.

[67] Javier Martínez and Manuel Silva. A simple and fast algorithm to obtain all invariants of a generalised petri net. In *Application and Theory of Petri nets*, pages 301–310. Springer, 1982.

[68] John McCarthy and Patrick J Hayes. Some philosophical problems from the standpoint of artificial intelligence. *Readings in artificial intelligence*, pages 431–450, 1969.

[69] Gérard Memmi and Gérard Roucairol. Linear algebra in net theory. In *Net Theory and Applications*, pages 213–223. Springer, 1980.

[70] Ole J Mengshoel, Mark Chavira, Keith Cascio, Scott Poll, Adnan Darwiche, and Serdar Uckun. Probabilistic model-based diagnosis: An electrical power system case study. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 40(5):874–885, 2010.

[71] Isabel Milho and Ana Fred. A user-friendly development tool for medical diagnosis based on bayesian networks. In *Enterprise Information Systems II*, pages 113–118. Springer, 2001.

[72] Roy A Gómez Morales, Jose I Garcia Melo, and Paulo E Miyagi. Diagnosis and treatment of faults in productive systems based on bayesian networks and petri net. In *Automation Science and Engineering, 2007. CASE 2007. IEEE International Conference on*, pages 357–362. IEEE, 2007.

[73] T Murata and J Yim. Petri-net deduction methods for propositional-logic rule-based systems. Technical report, Technical Report UIC-EECS-89-15, University of Illinois at Chicago, 1989.

[74] Tadao Murata. Petri nets: Properties, analysis and applications. *Proceedings of the IEEE*, 77(4):541–580, 1989.

[75] Kevin P Murphy, Yair Weiss, and Michael I Jordan. Loopy belief propagation for approximate inference: An empirical study. In *Proceedings of the Fifteenth conference on Uncertainty in artificial intelligence*, pages 467–475. Morgan Kaufmann Publishers Inc., 1999.

[76] B Natvig. Possibility versus probability. *Fuzzy Sets and Systems*, 10(1-3):31–36, 1983.

[77] C Negoita, L Zadeh, and H Zimmermann. Fuzzy sets as a basis for a theory of possibility. *Fuzzy sets and systems*, 1(3-28):61–72, 1978.

[78] Nils J Nilsson. Probabilistic logic. *Artificial intelligence*, 28(1):71–87, 1986.

[79] Diana Borrego Núnez. *Automation of distributed model-based diagnosis using structural analysis*. PhD thesis, University of Sevilla.

[80] Agnieszka Onisko, Marek J Druzdzel, and Hanna Wasyluk. A bayesian network model for diagnosis of liver disorders. In *Proceedings of the Eleventh Conference on Biocybernetics and Biomedical Engineering*, volume 2, pages 842–846. Citeseer, 1999.

[81] Bernard Louis Palowitch. *Fault diagnosis of process plants using causal models*. PhD thesis, Massachusetts Institute of Technology, 1987.

[82] Ramesh S Patil, Peter Szolovits, and William B Schwartz. Causal understanding of patient illness in medical diagnosis. In *IJCAI*, volume 81, pages 893–899, 1981.

[83] Judea Pearl. *Causality*. Cambridge university press, 2009.

[84] Judea Pearl. *Probabilistic reasoning in intelligent systems: networks of plausible inference*. Morgan Kaufmann, 2014.

[85] Hao Peng, Chris Gates, Bhaskar Sarma, Ninghui Li, Yuan Qi, Rahul Potharaju, Cristina Nita-Rotaru, and Ian Molloy. Using probabilistic generative models for ranking risks of android apps. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 241–252. ACM, 2012.

[86] Carl Adam Petri. Kommunikation mit automaten. 1962.

[87] David Poole. Normality and faults in logic-based diagnosis. In *IJCAI*, volume 89, pages 1304–1310, 1989.

[88] David Poole. Logic programming, abduction and probability. *New Generation Computing*, 11(3-4):377–400, 1993.

[89] David Poole. Probabilistic horn abduction and bayesian networks. *Artificial intelligence*, 64(1):81–129, 1993.

[90] Marc Porcheron, Benoit Ricard, J Luc Busquet, and Patrice Parent. Diapo: A case study in applying advanced a1 techniques to the diagnosis of a complex system. In *ECAI*, pages 43–43. PITMAN, 1994.

[91] Luigi Portinale. Exploiting t-invariant analysis in diagnostic reasoning on a petri net model. In *Application and Theory of Petri Nets 1993*, pages 339–356. Springer, 1993.

[92] Luigi Portinale. Behavioral petri nets: a model for diagnostic knowledge representation and reasoning. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 27(2):184–195, 1997.

[93] Luigi Portinale and Pietro Torasso. A comparative analysis of horn models and bayesian networks for diagnosis. In *AI* IA 97: Advances in Artificial Intelligence*, pages 254–265. Springer, 1997.

[94] Arthur N Prior. Formal logic. 1962.

[95] Lawrence Rabiner and B Juang. An introduction to hidden markov models. *ieee assp magazine*, 3(1):4–16, 1986.

[96] Antonio Ramírez-Treviño, Elvia Ruiz-Beltrán, Israel Rivera-Rangel, and Ernesto Lopez-Mellado. Online fault diagnosis of discrete event systems. a petri net-based approach. *IEEE Transactions on Automation Science and Engineering*, 4(1):31–39, 2007.

[97] Raymond Reiter. A theory of diagnosis from first principles. *Artificial intelligence*, 32(1):57–95, 1987.

[98] Nico Roos, Annette ten Teije, André Bos, and Cees Witteveen. Multi-agent diagnosis with spatially distributed knowledge. In *Proceedings of the Belgium-Dutch Conference on Artificial Intelligence (BNAIC-02)*, pages 275–282, 2002.

[99] Nico Roos, Annette Ten Teije, and Cees Witteveen. A protocol for multi-agent diagnosis with spatially distributed knowledge. In *Proceedings of the second international joint conference on Autonomous agents and multiagent systems*, pages 655–661. ACM, 2003.

[100] Yu Ru and Christoforos N Hadjicostis. Fault diagnosis in discrete event systems modeled by partially observed petri nets. *Discrete Event Dynamic Systems*, 19(4):551–575, 2009.

[101] Nargess Sadeghzadeh-Nokhodberiz and Javad Poshtan. Distributed interacting multiple filters for fault diagnosis of navigation sensors in a robotic system. *IEEE Transactions on Systems, Man, and Cybernetics: Systems (In press)*.

[102] Michael Schroeder and Gerd Wagner. Distributed diagnosis by vivid agents. In *Proceedings of the first international conference on Autonomous agents*, pages 268–275. ACM, 1997.

[103] Glenn Shafer et al. *A mathematical theory of evidence*, volume 1. Princeton university press Princeton, 1976.

[104] Edward H Shortliffe. Mycin: Computer-based medical consultations, 1976.

[105] Rong Su and W Murray Wonham. Global and local consistencies in distributed fault diagnosis for discrete-event systems. *IEEE Transactions on Automatic Control*, 50(12):1923–1935, 2005.

[106] Jing Sun, Shi-Yin Qin, and Yong-Hua Song. Fault diagnosis of electric power systems based on fuzzy petri nets. *IEEE Transactions on Power Systems*, 19(4):2053–2059, 2004.

[107] Louise Travé-Massuyès. Bridging control and artificial intelligence theories for diagnosis: A survey. *Engineering Applications of Artificial Intelligence*, 27:1–16, 2014.

[108] Toshimitsu Ushio, Isao Onishi, and Koji Okuda. Fault detection based on petri net models with faulty behaviors. In *Systems, Man, and Cybernetics, 1998. 1998 IEEE International Conference on*, volume 1, pages 113–118. IEEE, 1998.

[109] N Viswanadham and TL Johnson. Fault detection and diagnosis of automated manufacturing systems. In *Decision and Control, 1988., Proceedings of the 27th IEEE Conference on*, pages 2301–2306. IEEE, 1988.

[110] Lei Wang, Qing Chen, Zhanjun Gao, Lin Niu, Yishu Zhao, Zhiguang Ma, and Dejun Wu. Knowledge representation and general petri net models for power grid fault diagnosis. *IET Generation, Transmission & Distribution*, 9(9):866–873, 2015.

[111] Ying N Wang, F Ye Jin, Guo J Xu, Qing M Chen, Hai Y Li, and Xin R Liu. Novel hierarchical fault diagnosis approach for smart power grid with information fusion of multi-data resources based on fuzzy petri net. In *2014 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, pages 1183–1189. IEEE, 2014.

[112] Mark Weiser. The computer for the 21st century. *Scientific american*, 265(3):94–104, 1991.

[113] Yair Weiss. Correctness of local probability propagation in graphical models with loops. *Neural computation*, 12(1):1–41, 2000.

[114] Max Welling and Yee Whye Teh. Belief optimization for binary networks: A stable alternative to loopy belief propagation. In *Proceedings of the Seventeenth conference on Uncertainty in artificial intelligence*, pages 554–561. Morgan Kaufmann Publishers Inc., 2001.

[115] Haitao Wu, Wen-Kuang Chou, Ningbo Hao, Duan Wang, and Jingfu Li. Collaborative filtering recommendation based on conditional probability and weight adjusting. *International Journal of Computational Science and Engineering*, 10(1-2):164–170, 2015.

[116] Jianwen Xiang, Kokichi Futatsugi, and Yanxiang He. Fault tree and formal methods in system safety analysis. In *Computer and Information Technology, 2004. CIT'04. The Fourth International Conference on*, pages 1108–1115. IEEE, 2004.

[117] Koichi Yamada. Diagnosis under compound effects and multiple causes by means of the conditional causal possibility approach. *Fuzzy sets and systems*, 145(2):183–212, 2004.

[118] Shun-Zheng Yu. Hidden semi-markov models. *Artificial Intelligence*, 174(2):215–243, 2010.

[119] Lotfi A Zadeh. Fuzzy sets. *Information and control*, 8(3):338–353, 1965.

[120] Yan Zhang, Yong Zhang, Fushuan Wen, Chi Yung Chung, Chung-Li Tseng, Xiaoyi Zhang, Fei Zeng, and Yubo Yuan. A fuzzy petri net based approach for fault diagnosis in power systems considering temporal constraints. *International Journal of Electrical Power & Energy Systems*, 78:215–224, 2016.

Résumé

Cette thèse traite le problème de la modélisation de l'incertitude dans le contexte distribué. Elle est située dans le domaine de diagnostique; plus précisément, le diagnostique basé modèle des systèmes distribués. On focalise spécialement sur la modélisation de l'incertitude par le raisonnement probabiliste et possibiliste. Ainsi, pour la première contribution, on se base sur un formalisme de modélisation probabiliste appelé : "probability propagation nets" (PPNs), qui est destiné aux systèmes centralisés. Par conséquent, on a proposé une extension à ce formalisme pour l'adapter au contexte distribué. "Distributed probability propagation nets" (DPPNs), l'extension proposée, est conçue pour considérer les particularités des systèmes distribués. Ce dernier est considéré comme un ensemble de sous-systèmes, chaqu'un est modélisé par un DPPN. L'interaction entre les sous-systèmes est capturée par l'affranchissement des transitions communes qui appartiennent à plus d'un sous-système. En plus, le processus de diagnostique est fait par l'exploitation des transitions-invariants; une technique de diagnostique développée pour les réseaux de Petri.

Comme une deuxième contribution, on exploite une autre théorie qui modélise l'incertitude; la théorie des possibilités. En fait, une autre classe des réseaux de Petri appelée "Possibilistic Petri nets" (PoPNs) qui capture le comportement possibiliste est exploitée. Les mesures de possibilité sont attachées à chaque diagnostique obtenu comme une base pour mesurer le degré de son incertitude. Il est possible d'utiliser telles mesures pour détecter les incohérences des diagnostiques.

ملخص

تتناول هذه الأطروحة مشكلة نمذجة «عدم اليقين» في الانظمة الموزعة. تندرج تحديدا ضمن مجال تشخيص الاعطاب، بصفة ادق، التشخيص المبني على نموذج. نولي اهتمام خاص بنمذجة عدم اليقين باستعمال النماذج الاحتمالية و الامكانية. لهذا الغرض نستعمل نموذج احتمالي مبني على نوع خاص من «شبكات بتري» والمستعمل للأنظمة المركزية. نقوم بتمديد هذا النموذج ليتناسب مع الانظمة الموزعة. الانظمة التي نتعامل معها مكونة من عدة انظمة جزئية منمذجة بالنموذج الممدد المقترح، بالاضافة الى هذا فان طريقة التشخيص المستعملة مبنية على ثوابت الانتقالات.

علاوة على ذلك، وكمساهمة ثانية، نستغل نظرية أخرى لنمذجة عدم اليقين، وهي «نظرية الامكانات». في الواقع، هناك فئة أخرى من شبكات بيتري تسمى «شبكات بيتري الامكاناتية»، والتي تلتقط السلوك الامكاني للعمليات. نقوم بوسم كل تشخيص تم الحصول عليه بمقاييس الامكانات ككمية قابلة للقياس فيما يتعلق بعدم اليقين، ومن الممكن استخدام هذه المقاييس في الكشف عن بعض التناقضات في التشخيصات.