INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team distribcom

Distributed and Iterative Algorithms in Management and Signal Processing for Telecommunications

Rennes

THEME COM

Activity Report

2004

Table of contents

1. Team

Head of project–team

Albert Benveniste [DR INRIA, part–time]
Claude Jard [PROF. ENS CACHAN]

Administrative assistant

Huguette Béchu [finishing october 2004]
Myriam David [starting october 2004]

Research scientist (inria)

Éric Fabre [CR]
Stefan Haar [CR]
Aline Roumy [CR]
Loic Hélouët [CR]

Faculty member (université de Rennes 1)

Jean–Jacques Fuchs [professor]

Technical staff (inria)

Bruno Marquié [ingénieur expert]

Ph.D. student

Samy Abbes [MENRT grant]
Sébastien Maria [MENRT grant]
Thomas Chatain [Normalien]
Thomas Gazagnaire [Normalien, starting september 2004]
Emmanuel Donin de Rosière [CIFRE grant, FT R&D]

2. Overall Objectives

DistribCom addresses distributed and iterative algorithms for both network & service management and digital communications.

The first and main focus of DistribCom is on *algorithms for distributed management.* Today, research on network and service management focuses mainly on issues of software architecture and infrastructure deployment. However, management involves also algorithmic problems such as fault diagnosis and alarm correlation, provisioning and optimisation, negociation for QoS, and security. DistribCom develops the foundations supporting such algorithms: fundamentals of distributed observation and supervision of systems involving concurrency.

Our algorithms are model-based. For obvious reasons of complexity, such models cannot be built by hand. Therefore we also address the novel topic of *self-modeling,* i.e., the automatic construction of models, both structural and behavioral. For this we use techniques from computer and software engineering (e.g., genericity and reflexive infrastructures) as well as techniques from statistics and control (e.g., Bayesian learning techniques to infer probabilistic parameters from observations).

Some of the iterative techniques we develop are also useful at handling *joint algorithms of signal processing and coding in digital communications.* We develop such studies in the context of Multiple Input Multiple Output (MIMO) or Multi User digital communications. As antennas play a central role in the latter sector, we complement this line of research by investigating estimation, detection, and identification techniques related to antenna processing.

Accordingly, our research topics are structured as follows:

- fundamentals of distributed observation and supervision of concurrent systems;
- self-modeling;

- algorithms for distributed management of telecommunications systems and services;
- joint algorithms of signal processing and coding in digital communications;
- estimation with parsimony in signal processing.

Our main industrial ties are with Alcatel and France-Telecom, on the topic of networks and service management. We participate jointly with them to the SWAN RNRT project on self-management of networks and Web services. On a related topic, we cooperate with France-Telecom on the technology of scenarios.

3. Scientific Foundations

3.1. Models of concurrency: nets, scenarios, event structures, graph grammars, and their variants

Keywords: *Models of concurrency, event structures, graph grammars, nets, scenarios*.

For Finite State Machines (FSM), a large body of theory has been developed to address problems such as: observation (the inference of hidden state trajectories from incomplete observations), control, diagnosis, and learning. These are difficult problems, even for simple models such as FSM's. One of the research tracks of DistribCom consists in extending such theories to distributed systems involving concurrency, i.e., systems in which both time and states are local, not global. For such systems, even very basic concepts such as "trajectories" or "executions" need to be deeply revisited. Computer scientists have for a long time recognized this topic of concurrent and distributed systems as a central one. In this section, we briefly introduce the reader to the models of scenarios, event structures, nets, languages of scenarios, graph grammars, and their variants.

3.1.1. Scenarios.

The simplest concept related to concurrency is that of a finite execution of a distributed machine. The *scenario* shown in Figure 1

is an example. The figure shows the life-time (from top to bottom) of four processes (or instances). The instance can exchange asynchronous messages. In this example, some local variables can be tested and assigned. In this model, events are totally ordered for each instance, but only partially ordered between different instances. Thus, time is local, not global. The natural concept of state is local too (i.e., attached to individual instances). Global states can be defined, they however require nontrivial algorithms for their distributed construction. Finite scenarios introduce the two key concepts of *causality* and *concurrency*. The causality relation is a partial order, we denote it by $\preceq$. In Figure 1, the reception of AU_AIS is causally related to the sending of MS_AIS by the rs_TTP, while it is concurrent with the receipt of MS_AIS by the alarm manager.

Scenarios have been informally used by telecom engineers for a long time. Their formalisation was introduced by the work done in the framework of ITU and OMG on High-level Message Sequence Charts and on UML Sequence Diagrams in the last ten years, see [51][50]. This allowed in particular to formally define infinite scenarios, and to enhance them with variables, guards, etc [63][61][62]. Today, scenarios are routinely offered by UML and related systems and software modeling tools, Figure 1 showed such an example.

3.1.2. Event structures.

The next step is to model sets of finite execution of a distributed machine. *Event structures* were invented by Glynn Winskel and co-authors in 1980 [59][70]. This data structure collects all the executions by superimposing shared prefixes.

Figure 2

shows an example. The top most diagram shows an HMSC. i.e., an automaton whose transitions are labelled by basic scenarios. Regard first the scenarios as abstract labels. The set of all executions of this automaton is

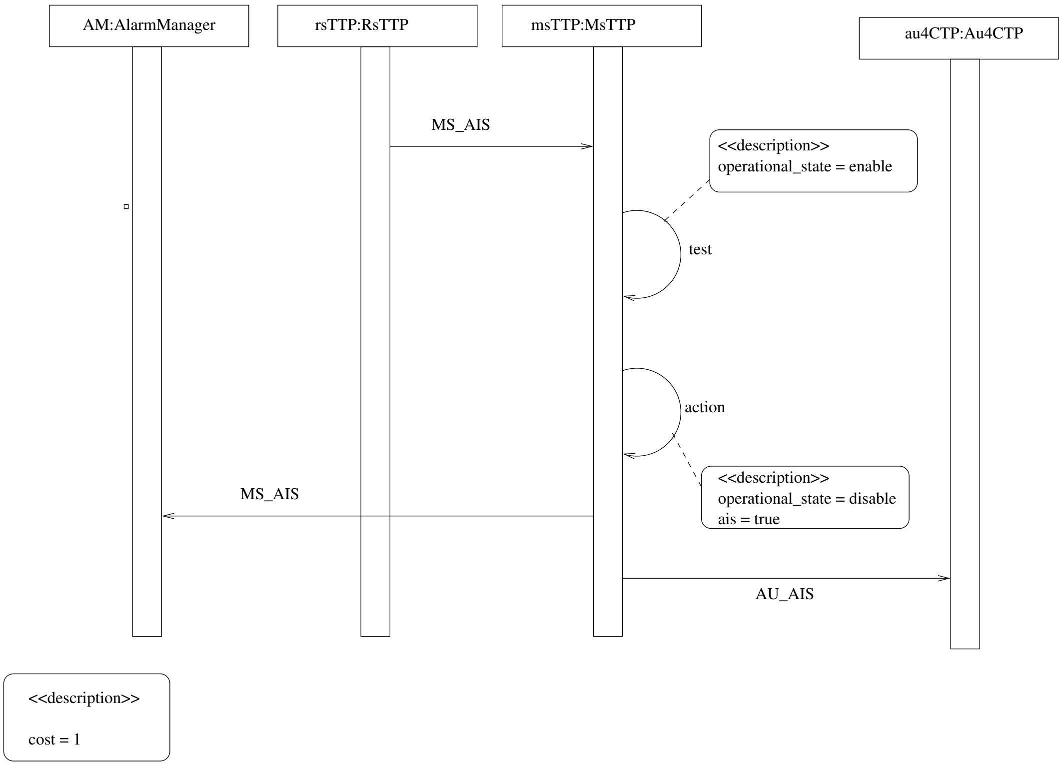

Figure 1. A basic scenario, drawn as a UML sequence diagram.

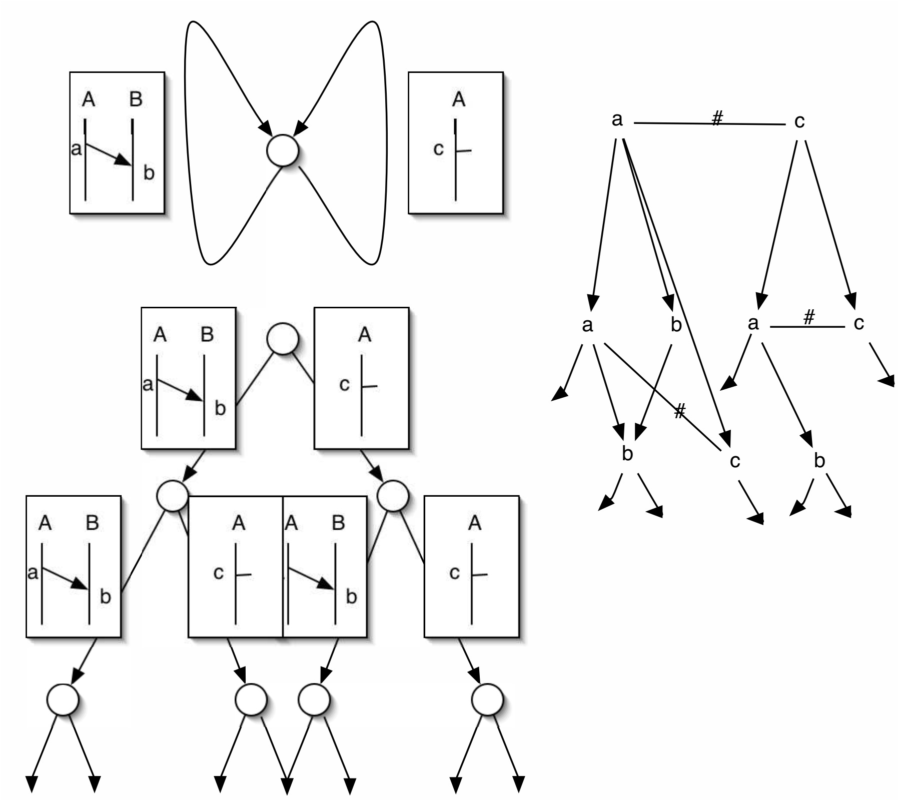

Figure 2. An HMSC (an automaton whose transitions are labeled by scenarios), its execution tree, and its event structure.

then shown on the bottom left diagram, in the form of an execution tree. For sequential machines, executions trees collect all the executions by superimposing shared prefixes.

Now, the right diagram shows the “white box” version of the former, in which the concatenation of the successive basic scenarios has been performed by chaining them instance by instance. The result is a *event structure*, i.e., a branching structure consisting of events related by a *causality* relation (depicted by directed arrows) and a *conflict* relation (depicted by a non directed arc labeled by a symbol). Events that are neither causally related nor in conflict are called *concurrent*. Concurrent processes model the “parallel progress” of components.

Categories of event structures have been defined, with associated morphisms, products, and co-products, see [71]. Products and co-products formalise the concepts of parallel composition and “union” of event structures, respectively. This provides the needed apparatus for composing and projecting (or abstracting) systems. Event structures have been mostly used to give the semantics of various formalisms or languages, such as Petri nets, CCS, CSP, etc [59][70]. We in DistribCom make a nonstandard use of these, e.g., we use them as a structure to compute and express the solutions of observation or diagnosis problems, for concurrent systems.

3.1.3. Nets and languages of scenarios.

The next step is to have finite representations of systems having possibly infinite executions. In DistribCom, we use two such formalisms: *Petri nets* [38][36] and *languages of scenarios* such as High-level Message Sequence Charts (HMSC) [51][62]. Petri nets are wellknown, at least in their basic form, we do not introduce them here. We use so-called *safe* Petri Nets, in which markings are boolean (tokens can be either 0 or 1); and we use also variants, see below. Languages of scenarios are simply obtained as illustrated in Figure 2: 1/ equip basic scenarios with a concatenation operation, 2/ consider an automaton whose transitions are labeled with basic scenarios. Executions of Petri Nets and HMSC can be represented with concurrency in the form of event structures. We have shown this for HMSC’s in Figure 2, and it is obtained in a similar way for Petri nets.

3.1.4. Extensions and variants.

Two extensions of the basic concepts of nets or scenario languages are useful for us:

- Nets or scenario languages enriched with variables, actions, and guards. This is useful to model general concurrent and distributed dynamical systems in which a certain discrete abstraction of the control is represented by means of a net or a scenario language. Manipulating such *symbolic nets* requires using abstraction techniques.
- Probabilistic Nets or event structures. Whereas a huge litterature exists on stochastic Petri nets or stochastic process algebras (in computer science), randomizing *concurrent models*, i.e., with ω’s being concurrent trajectories, not sequential ones, has been addressed only since the 21st century. We have contributed to this new area of research.

3.1.5. Handling dynamic changes in the systems: graph grammars.

The last and perhaps most important issue, for our applications, is the handling of dynamic changes in the systems model. This is motivated by the constant use of dynamic reconfigurations in management systems. Extensions of net models have been proposed to capture this, for example the *dynamic nets* of Vladimiro Sassone [42]; for the moment, such models lack a suitable theory of unfoldings. A relevant alternative is the class of *graph grammars* [37][39]. Graph grammars transform graphs by means of a finite set of rules. Figures 3 and 4

show how graph grammars can encode dynamic nets, i.e., nets in which firing a transition can modify the net structure. Graph grammars have been equipped with a rich theory of unfoldings. Graph grammars have remained mostly in the theoretical arena yet. We at DistribCom use them for distributed management algorithms for systems subject to reconfiguration.

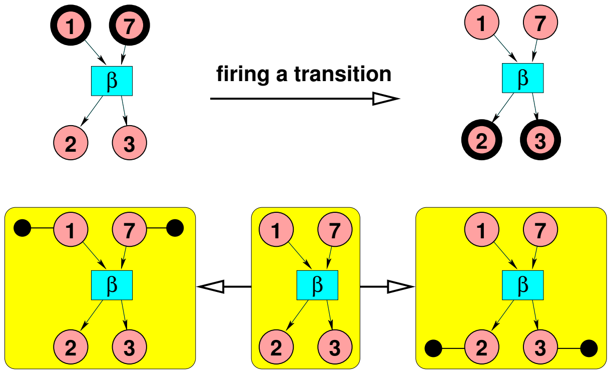

Figure 3. Graph grammars: modeling the movement of tokens.

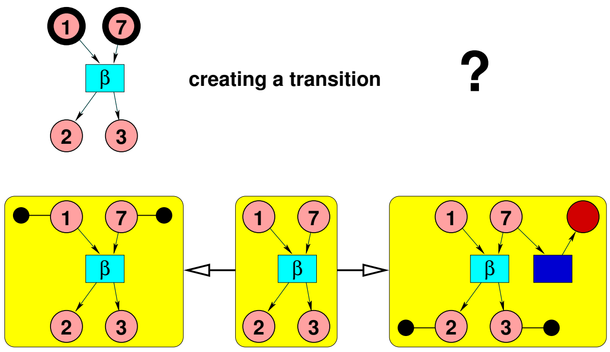

Figure 4. Graph grammars: modeling the change in net structure.

3.2. Joint processing in digital communications

Keywords: *bayesian network*, *channel coding*, *digital communications*, *equalization*, *graphical model*, *turbo–code*.

Due to the ever-growing number of users and the demand for transmission of huge amounts of data (for new services), high rate communication is of great importance today (e.g., for multimedia wireless communications, fixed wireless loops, LAN, and more). However the physical limitations of the wireless channels such as scarce channel capacity and frequency selective fading make high-rate transmission particularly challenging. Facing this challenge and achieving higher data rates therefore require a major research effort.

The past decade has witnessed notable advances to achieve reliable communications and signal processing has become a mature but also very specialized field. To meet future demands in wireless communications, recent trends show that digital communications at the physical layer should evolve from a traditional approach where the different functions of modulation, coding, and equalization, are considered separately, to an integrated systems approach.

Traditionally these problems have been solved separately, mainly for complexity reasons. E.g., equalization to deal with multipath channels, channel coding to better utilize the channel capacity, thus to lower the required signal-to-noise ratios (SNRs), and multiple access to make the users transmit simultaneously. Although this disjoint approach ensures lower complexity, it is sub-optimal since different elements may be optimized in a possibly antagonistic way—most conventional equalizers assume that all possible channel input sequences are equally likely; this however is not true in the presence of channel coding, which is used in most wireless systems.

3.2.1. Iterative receivers and turbo techniques

Rather than considering each problem in isolation, it is therefore more appropriate to consider them jointly. The complexity of the optimal solution (in the sense of the Maximum Likelihood) increases exponentially with the system size. *Turbo* or *iterative* techniques were proposed to address the resulting performance/complexity trade-off. This idea stems from the turbo-codes [41] which aimed at getting the same performance with the code length doubled, whereas the complexity is only doubled and not squared. In [41], Berrou *et al.* showed that turbo-codes can perform within 0.5 dB of the Shannon capacity (at a bit error rate of 10^{-5}). Turbo-techniques can also be successfully applied to other joint problems (equalization and decoding, multiuser detection and decoding, source/channel coding). In that case, the joint design of different functions can be seen as the distributed coordination between different algorithms.

3.2.2. Analysis of iterative receivers

Moreover, [69][60] have shown the connection between the turbo algorithm of Berrou et al. (1993) and Pearl's (1982) belief propagation algorithm, well known in the artificial intelligence community. This allowed [55] to cast all the turbo-iterative schemes in a unified scheme, in which the transmitter is naturally described by graphs (factor graph, or bipartite graph) and the data are estimated at the receiver by the message passing algorithm (the sum-product or the max-product algorithm).

This connection explains the good performance of the turbo-codes only partially. Since a graph in a compound system has many loops, the belief propagation yields only approximate maximum likelihood solutions. It is thus fundamental to create tools to describe such iterative algorithms in order to design the system (transmitter and receiver). One of the most promising approaches for analyzing iterative decoding schemes employs the notion of density evolution [66][65], where the density of the soft messages exchanged is tracked. This approach was performed for a particular type of codes: the Low Density Parity Check codes (LDPC) for which the graph contains variables of dimension 2 only. Instead of the whole density, tenBrink proposed to visualize the mutual information [72], which can therefore be applied to more general graphs. In [11], we have shown that mutual information can also be used to design the transmitter.

3.3. Signal Processing

Traditional statistical modelling has paid a great deal of effort at first identifying the model structure, including the number of its involved parameters. This has lead to the rich body of work around Akaike Information Criterion (AIC) and its many variants BIC, MDL, etc.

Recent studies [45][46][43] have lead to novel alternative approaches in which sparsity in modelling is achieved without the need for a preliminary structure estimation procedure that is always difficult to achieve.

It can be seen as a Bayesian or inverse-problem approach in which the classical maximum likelihood criterion is replaced by a compound criterion that combines fit of the model to the observations with prior information or sparsity requirements.

An interesting approach in this philosophy consists in combining ℓ_2 and ℓ_1 norms in the criterion, where the ℓ_2-part measures the fit of the model to the observations (e.g., the maximum likelihood criterion in the presence of gaussian noise) and the ℓ_1-part ensures parsimony of the representation. In case of linear parameterizations the criterion remains convex and problems with moderate to high number of unknowns are reliably solved with standard programs, such linear or quadratic programming, from well established scientific program libraries. While the algorithmic part is easy, the analysis is in general quite difficult and only preliminary results [49] [9] in quite trivial situations are at hand so far. Even in the most basic identification schemes where the traditional methods require preliminary structure estimation (model order detection or selection of regressors for instance), comparisons of performance seem to be out of reach.

Typical questions amenable to a solution are of the following type: given a matrix A of dimension (n, m) with $m > n$ and a vector $b = A\,x$, find sufficient conditions for b to have a unique sparsest representation as a linear combination of columns of A. Answers to this question are known for arbitrary A with unit Euclidean norm column vectors, for both the true sparseness $\|x\|_0$ where $\|x\|_0$ denotes the number of non–zero components x and the so-called ℓ_1-sparseness i.e.$\min\limits_x \|x\|_1$ where $\|x\|_1 = \sum |x_i|$ denotes the ℓ_1 norm of x. If b or more precisely if $b = Ax_o$ with $\|x_o\|_0$ satisfies this condition then both the solution of the linear program:

$$\min_x \|x\|_1 \qquad \text{subject to} \qquad A\,x = b$$

and the quadratic program:

$$\min_x \frac{1}{2}\|A\,x - b\|_2^2 + h\,\|x\|_1 \qquad \text{with} \qquad h > 0$$

have x_o as unique optimum. Extensions [47] concern the noisy case where $b = Ax_o + e$ with e a vector of perturbations. So far only deterministic analyses where the energy of e, i.e. $\|e\|_2$, is known to be bounded, are available. Corresponding results with e gaussian noise would concern the well investigated selection of variables in multiple linear regression area, where no useable or valuable results are available. Robustness with respect to outliers in the observations and robustness with respect to lack of knowledge of the true underlying model are other issues that need to be introduced in this new setting. Huber M-estimators and Vapnik $\epsilon-$function can indeed be rewritten as compound functions mixing ℓ_∞, ℓ_2 and ℓ_1 norms. Adding redundancy may be a mean to handle poor knowledge or fluctuating models, another mean being to replace the least-squares part of the criterion by a total-least-squares part (error in variable models). While in the least-squares models perturbations are assumed to be present only on the observations in the total-least-squares models potential perturbations are also present on the regressors.

4. Application Domains

4.1. Network and service management in telecommunications

Keywords: *QoS monitoring, failure diagnosis, telecommunication transport network, web service*.

SDH “Synchronous Data Hierarchy,” synchronous transport protocol for high rate transmissions, generally on optical links ; French version of SONet.

WDM "Wavelength Division Multiplex," modulation of several lasers, with different wavelengths, on the same fiber, in order to increase the transmission rate.

GMPLS "(Generalized) Multi Protocol Label Switching," a technique to create dedicated connexions over any type of network/protocol, either connexion oriented (like SDH), or packet oriented (like IP), in order to guarantee a level of quality of service (QoS).

SLA/SLS "Service Level Agreement/Specification," a contract defining the QoS that a service provider has to guarantee to a user. The tendency is to "program" networks at the "business level," by specifying services/policies, and not technical parameters. The latter have to adjust automatically to provide the requested service levels.

Web Service A service/application provided on the web. The trend is to gather elementary services (e.g. weather forecast, plane and hotel reservation, banking,...) into larger services (e.g. travel agency).

Telecommunications have grown up from a basic technology of networks and transport to a much more complex jungle of networks, services, and applications. This motivates a strong research effort towards "autonomic communications": one would like to program networks at the service level (sometimes called the business level, since it directly involves contracts with customers), and let the network adapt itself in order to ensure a given QoS, isolate and repair failures, etc. This tendency appears for exemple in the policy-based management, or in the quest for "self-XX" functionalities (self-configuration, self-monitoring, self-healing, etc.). One of our objectives it to try giving some content to these hidden automatic tasks.

In higher layers, at the level of services, the same search for flexibility motivates the development of tools to rapidly assemble web-services into larger services. Here again, problems are related to the automatic (re)configuration capabilities, to the on-line monitoring of the QoS, the isolation of failures or QoS violations, etc.

These problems have several common features. First of all, they involve concurrent systems, *i.e.* systems where several things can happen at the same time. Secondly, they are built in a modular way, by combining elementary components into large connected structures. Third common point: these systems have a dynamic structure. Reconfigurations, connexions/deconnexions of new components or clients are part of the normal activity, and should not require that monitoring algorithms be reset or modified each time the system is changed. Four, one is partly able to position observation points in the system, and decide what are the relevant phenomena to observe. And finally, the size and heterogeneity of these systems forbids a centralized monitoring architecture. This motivates developing distributed and modular approches.

As an example of distributed monitoring, our first application was related to diagnosis issues in transport networks, i.e. the low-level layers of networks (physical, transport and network layers). We have focused on circuit oriented networks, such as SDH/WDM protocols or GMPLS protocols. These systems assemble hundreds of functions of components, and the failure of one of them generally induces side-effects in many others. This phenomenon is known as "fault propagation;" it results in hundreds of alarms produced by the various components and collected at different locations in the network. Identifying origins of faults from these alarms has now reached a level of complexity that prevents the traditional human analysis of alarms. Due to the size of systems, the automatic diagnosis task cannot be done in a centralized manner, and must be solved by a network of local supervisors that coordinate their work to provide a coherent view of what happened in the network.

5. Software

5.1. SOFAT : a scenario toolbox

Keywords: *partial orders*, *scenarios*.

Participant: Loic Hélouët.

The SOFAT toolbox is a scenario manipulation toolbox. Its aim is to implement all known formal manipulations on scenarios. The toolbox implements several formal models such as partial orders, graph grammars, graphs, and algorithm dedicated to these models (Tarjan, cycle detection for graphs, Caucal's normalization for graph grammars, etc.). The SOFAT toolbox is permanently updated to integrate new algorithms. It is currently used for a research contract with France Telecom, and is freely available form INRIA's website.

6. New Results

6.1. Self-modeling of distributed and concurrent systems

Participant: Claude Jard.

The emerging topic of self-modeling tries to contribute to the automatic self-construction of sophisticated behavioral models from having or discovering its architecture. The fault model has to be constructed from different ingredients. Some aspects of the model could be automated, other require an expert knowledge. At present, it is reasonable to think that the different managed objects (actually their type) could be automatically acquired from the MIBs. Configuration can be also learned by the interrogation of the network. This is particularly important for dynamic systems: object instantiation in the model can be the result of the observation of a change in the network (topology, connections, etc.). The difficult part is the behavioral aspects of network components. Some of them can be generic and described in libraries, others will require a specific modeling.

Our work [12] in that subject relies on generic modeling and has been initiated within the Magda projects and was done with Armen Aghasaryan from Alcatel R&I. The generic model captures the essential structural (generic components and their relations) and behavioral (interactions between the generic components) characteristics of telecommunications network components in the light of their utilization in fault management tools. The structural part of the generic model can also be envisaged to be used in other network application omains, e.g. for service provisioning. The generic model covers both circuit-based and packet-based networks, despite of divergent approaches adopted by the respective standardization bodies. The generic model is described by means of UML notations, namely, class diagrams, sequence diagrams and instance diagrams. These diagrams are intended to be used in: 1/ derivation of the technology-specific models and 2/ generation of rules on generic component instances.

Although the targeted management applications work with the derived specific models, in certain cases they can directly apply the rules defined on generic components. Thus, the effort necessary for deriving a specific model is significantly reduced. For the diagnosis application we have considered, we proved that the generic model can be compiled to obtain generic rules (develoment of the OSCAR tool).

6.2. Event structures for distributed algorithms

Keywords: *Concurrent systems*, *category theory*, *distributed algorithms*, *factorization of unfoldings*, *turbo algorithms*, *unfoldings*.

Participants: Eric Fabre, Albert Benveniste, Stefan Haar.

Several fundamental results have been obtained this year.

In a joint work [8], we have completed a theoretical study of on-line distributed diagnosis. The algorithms we have developed in this work use safe Petri nets and associated event structures to represent the problem and its solution. Local projections of global diagnosis are computed, on-line, by cooperating supervisors. A key step was the use of high-level primitives operating on event structures, to express and formally study these algorithms. These are: net unfoldings, parallel compositions, and projections.

Eric Fabre has proposed an axiomatic theory of iterative distributed algorithms of the kind we use for distributed diagnosis. In these algorithms, agents exchange messages in a chaotic and asynchronous way, in order to ultimately reach a consensus on the solution of a problem—instances include: diagnosis, max-likelihood diagnosis, combinatorial optimization. The so obtained algorithms turn out to be generalizations of the turbo algorithms developed in coding theory. Eric Fabre has proposed a set of high-level definitions and axioms that allow using such algorithms for distributed problems.

Eric Fabre has further investigated the fundamental issues behind the quest for "modular diagnosis". To develop distributed (diagnosis) algorithms, one must be able to handle a system by parts. Consider a large concurrent system obtained by combining many elementary components. Sets of runs of the global system are generally too large, but such sets factorize as a "product" (in a particular sense) of sets of runs for each component, which is a much more compact representation. This year, Eric Fabre has discovered that such factorization properties could be also expressed on unfoldings themselves [44][33]. Surprisingly, this result was already present in a paper by Winskel [71], in a very abstract way, and has apparently not been used by the community developing tools above unfoldings and event structures. Eric Fabre is now recasting distributed diagnosis in the correct setting, namely category theory.

Stefan Haar has pursued his investigation of the concept of *diagnosability* for discrete event concurrent systems modeled by safe Petri nets [18]. Transitions of the net are observed through their labels, seen as "alarms". Diagnosability is the problem of deciding whether a fault can be identified by a finite number of observations collected after the occurrence of that fault. In the case of concurrent systems, runs are partial orders of events, instead of sequences, and in the same way observations are partial orders of "alarms." So the usual notion of diagnosability must be adapted to this new framework.

6.3. Symbolic algorithms for the distributed diagnosis of concurrent systems

Participants: Claude Jard, Thomas Chatain.

The previous work of our group on diagnosis used 1-safe Petri nets with branching processes and unfoldings to define the histories and a distributed algorithm to build them as a collection of consistent local views [8].

In this work [14], we have extended the method to *high-level parameterized Petri nets*, allowing the designer to model data aspects, even on infinite domains, and to parameter the system state. Using this latter feature, one can consider for instance an incomplete model starting in an unknown parameterized initial state. This could be used to start monitoring on a system already in use. This supposes that the possible values for the parameters are symbolically computed and refined during supervision. We think this symbolic approach will be able to deal with more complex distributed systems. At the heart of our scientific contribution is the definition of a symbolic unfolding for high-level Petri nets, which combines the traditional unfolding [53][54] with a kind of α-conversion (λ-calculus) to deal with parameters.

Our parameterized concurrent model is based on the standard high-level Petri net introduced in [52] and augmented with free variables. In order to define the dynamics of such nets, we consider that each place can be fed by a multiset of values taken from a set of types (often called "colors"). These values are tested and forwarded by the transitions. The algorithm for building the possible runs of the net consists in considering all the transitions of the original net, and placing them, one at a time, if they are possible. An event e, instance of a transition t, is placed only if its preset (the input places) is present in the graph and if the following enabling condition is satisfiable. The enabling condition is formed by the conjunction of the local conditions of the events located in the causal past of e (see below the definition of causality) and of its local condition. The local condition is the guard of the transition t (in which the local variables have been renamed by their global names), augmented with the constraint that the variables of the input arcs have the same values that the variables of the output arcs of the input event of the input places, in order to capture the causal relation. To keep track of this condition, we associate a new predicate with the new event.

Two events linked by a path of the graph are *causally* related, since there exists a flow of values between them. Two events are *concurrent* if they are causally related and if they are not in *conflict* (i.e. cannot belong to a same run). There are two causes of conflict. The first one, called *structural conflict* is that they have been separated by a choice in the system, represented in the graph by a branching from an ancestor place of these events. The second possibility is specific to the parameterized model: two events are also in conflict (called *non-structural conflict*) if their predicates are not simultaneously satisfiable. We thus show that the symbolic unfolding is an interesting structure to represent the different runs, in which causality and concurrency are explicitly given. The different runs are superimposed in the graph and separated by the notion of conflict.

6.4. Probabilistic models of concurrent systems

Participants: Samy Abbes, Albert Benveniste, Stefan Haar.

Fault and alarm correlation in concurrent and distributed systems is subject to significant nondeterminism due to ambiguity in the diagnosis. For example, a fault of some component C_1 causing some other component C_2 to fail can yield two possible diagnoses: $\{C_1$: primary fault, causes C_2 to be faulty$\}$, or $\{C_1$: primary fault, C_2 (independent) primary fault$\}$—of course, the second interpretation is less likely to be valid, since it would imply multiple faults. To overcome this, we have enhanced our models with probabilities, thus giving a different likelihood to the above two interpretations.

In year 2000, we have launched a new research programme on probabilistic models of concurrent systems. This is different from stochastic Petri nets in all existing variants, since the latter are ultimately interpreted as Markov chains, a model in which both state and time are global. This is also different from probabilistic automata and process algebras, which are in fact tightly related to Markov Decision Processes. In our case, trajectories ω are partial orders of events with local states, and the Ω space consists of the set of maximal configurations of the unfolding of the considered net. This problem has also been recently and independently considered by Hagen Völzer [68], Daniele Varacca and Glynn Winskel [67].

In his thesis [6][30], Samy Abbes has solved an impressive number of difficult questions:

- When can $(\Omega, \mathcal{F}, \mathbf{P})$ be constructed as a projective limit of finite probabilistic concurrent models? This allows using the elegant Kolmogorov-Prokhorov extension theorem for such a construction.
- Since our models involve concurrency, can we have concurrency tightly reflected by some kind of probabilistic independence?[1] Samy Abbes has introduced the concept of *distributed* probability, and he showed how to construct them.
- Since we do not want to regard our probabilistic models as Markov chains, what is the proper concept of state in our case? *Branching cells* play such a role, they carry the successive and possibly concurrent random choices along executions.
- *Markov property* and the concept of *homogeneity* (such as in Markov chains) can be generalized. Samy Abbes has developed a corresponding *renewal theory*, i.e., the probabilistic study of recurrence. The resulting model is called *Markov net.*
- Last but not least, Samy Abbes has proved very deep *limit theorems.* The *Law of Large Numbers* is a deep and nontrivial generalization of the usual one. What should replace the counter N in the average $1/N \sum_1^N f(X_n)$, since we have no concept of global time? Counting how many branching cells are traversed turns out to be the right solution. Since concurrency is allowed, it is possible that the considered system is made of two non-interacting subsystems; these can obviously run at independent speeds, which raises a difficulty since our average uses a single counter. The law of large numbers has been proved therefore for Markov nets with so-called *integrable concurrent height*, which states that intervals between synchronization of processes must be finite in average.

[1] Note that this never occurs if we adopt previously known approaches.

6.5. Scenarios for distributed systems, application to security

Keywords: *Security*, *covert channels*, *game theory*, *scenarios*.

Participants: Loic Hélouët, Aline Roumy, Eric Fabre.

A covert channel is an unauthorized information flow between corrupted users. These flows are usually created to bypass security or billing mechanisms of a system, and divert systems ressources from their original purpose. Covert channels are information leaks that divert resources of a system from their original purpose. They are a threat for security, and several standardization documents recommend to detect these flows with reproducible and formal methods.

We have proposed a method to detect certain kinds of covert channels in protocols from a scenario model. Previous approaches have been proposed for Bell & La Padulla [40][56] models. A more recent trend in security is to define covert channel presence as a non-interference property violation. A process P is said to interfere with a process Q in a system if the actions of P can influence what Q can do or observe. The first notion of non-interference is due to Goguen and Messeguer [48].

First, covert channels are modeled as a game between a pair of corrupted users (Sender,Receiver), that tries to transfer information and the rest of the system, that tries to prevent information passing. Bits of information are encoded through the behavioral choices of the Sender at given moments, and decoded by the receiver. We have shown [20] with Marc Zeitoun (LIAFA) and Aldric Degorre (ENS) that the existence of a strategy for this game implies the presence of a covert chanel in a protocol.

Once a covert channel is discovered, an important task is computing its bandwidth. This value determines the importance of the information leak, and hence may lead to a modification of the system. We have used an existing $(max, +)$ approach [57] to compute the bandwidth of a covert channel described with scenarios[19]. We have also studied covert chanels bandwidth from another point of view, namely information theory. The main objective is to quantify the bandwidth of a covert channel in terms of mutual information between a sender and a receiver.

However, information leaks is not the only interesting property that can be detected on a scenario model. Covert channel study is a first step towards a more general definition of information flow security properties on scenario languages.

6.6. Deploying distributed diagnosis on Alcatel Management Platform

Participants: Eric Fabre, Stefan Haar.

An important outcome of the RNRT project MAGDA2 is the development of a prototype distributed monitoring software, done jointly with Alcatel. This prototype is connected to a commercialized management platform (Almap) provided by Alcatel, and illustrates the capabilities of our distributed algorithms on a diagnosis problem. Its salient features are :

- the discovery of the underlying network components and connections, and the automatic construction of an internal model for distributed model-based diagnosis (see 6.1),
- the automatic deployment of the *ad hoc* distributed monitoring architecture,
- a distributed alarm correlation procedure, robust to alarm losses and identifying root causes of failures,
- the interaction with Almap for alarm collection, diagnosis display and service impact analysis.

One of our challenges was to prove that the distributed diagnosis procedure could be developed over a rule engine, this technology being the most popular tool for alarm correlation. We have used a commercialized rule engine (JRules, provided by Ilog), and shown that our algorithms boil down to three simple ingredients :

- the structure of the objects handled by the rule engine of each local supervisor ; this structure encodes the network topology and (network elements, functions and connexions),

- a set of generic rules describing the (normal and faulty) behaviors or generic components ; this forms the larger part of the rule set,
- a small overhead of special rules encoding our distributed algorithms : these rules describe operations performed by a local supervisor, and communications between supervisors.

6.7. Active XML and Web services

Keywords: *P2P Systems*, *Web Services*, *XML*.

Participants: Stefan Haar, Albert Benveniste, Eric Fabre, Claude Jard, Loïc Hélouët, Ashwin Limaye.

The language *Active XML* or *AXML* is an extension of XML which allows to enrich documents with *service calls* or sc's for short. These sc's point to web services that, when triggered, access other documents; this materialization of sc's produces in turn AXML code that is included in the calling document. One therefore speaks of dynamic or intensional documents; note in particular that materialization can be *total* (inserting data in XML format) or *partial* (inserting AXML code containing further sc's). AXML has been developped by the GEMO team at INRIA Futurs, headed by Serge Abiteboul. AXML allows to set up P2P systems around repositories of AXML documents (one repository per peer). In the internship of Ashwin Limaye, between May and August 2004 (supervision: Loïc Hélouët and Stefan Haar), a prototype has been created that simulates exploration and discovery of a board (matrix) by a set of "robots" (peers). Robots may

- query the board server about the colour (value) of its square (current position) or of an adjacent square,
- move to an adjacent square,
- communicate with other robots to share knowledge.

A follow-up project with Ecole Louis de Broglie, started in September 2004, aims at extending the implementation with a navigator pilot and graphical interface, to serve as a simulation testbed for behaviours and fault diagnosis of P2P systems.

In another effort, we are connecting with the GEMO team to explore the behavioural semantics of AXML. Current work studies the computation of Petri net unfoldings and diagnosis using an AXML peer system.

6.8. Joint processing in digital communications

Keywords: *bayesian network*, *channel coding*, *digital communications*, *equalization*, *graphical model*, *turbo–code*.

Participants: Aline Roumy, Eric Fabre.

Turbo–code Error correcting codes introduced by Berrou, Glavieux and Thitimajshima [41], joining two convolution codes by means of an interleaver. The name is due to the iterative decoding algorithm, which uses "soft" probabilistic information.

The algorithms we propose for joint processing, arise from the turbo (or iterative) algorithm in digital communications. Our current research on this subject focuses on the analysis of such algorithms in order to propose new designs. In the following we describe, our main focusses.

6.8.1. Coding

In [11], we have shown that mutual information can also be used to design the transmitter. We therefore optimized the random-like ensemble of Irregular Repeat Accumulate (IRA) codes for binary-input symmetric channels in the large blocklength limit. Our optimization technique is based on approximating the Evolution of the Densities of the messages exchanged by the Belief-Propagation message-passing decoder by a one-dimensional dynamical system. In this way, the code ensemble optimization can be solved by linear programming. We propose four such Density Evolution approximation methods, and compare the performance of the obtained code ensembles over the binary symmetric channel and the binary-antipodal input additive white Gaussian channel. Our results clearly identify the best among the proposed methods and show that the IRA codes obtained by these methods are competitive with respect to the best-known irregular Low-Density Parity-Check codes. In view of this and the very simple encoding structure of IRA codes, they emerge as attractive design choices.

6.8.2. Multiple access

A very efficient multiplexing method is the Code Division Multiple Access. This technique has raised a lot of interest in mobile communications due to its large spectral efficiency [64] and is already standardized (IS-95, IMT-2000, UMTS). We propose here two approaches: an LDPC-encoded CDMA system and then an alternative to the CDMA.

For the first one, we investigated in [7] the spectral efficiency achievable by random synchronous CDMA with QPSK modulation and binary error-control codes, in the large system limit where the number of users, the spreading factor and the code block length go to infinity. For given codes, we maximize spectral efficiency assuming an MMSE successive stripping decoder for the cases of equal rate and equal power users. In both cases, the maximization of spectral efficiency can be formulated as a linear program and admits a simple closed-form solution that can be readily interpreted in terms of power and rate control. We provide examples of the proposed optimization methods based on off-the-shelf LDPC codes and we investigate by simulation the performance of practical systems with finite code block length.

Regarding the second approach, we considered codes (and their related iterative decoding algorithms) that are able to get close to the boundary of the capacity region of the Gaussian multiple access channel, without the use of time sharing or rate splitting. The approach is based on density evolution and/or its variant (mean, mutual information). We studied the optimization of LDPC codes for the 2-user Gaussian MAC and have shown that it is possible to design good irregular LDPC codes with very simple techniques, the optimization problem being solved by linear programming [23].

6.8.3. Channel Estimation, and Equalization

We studied the impact of channel estimation and *a priori* information in a maximum a posteriori (MAP) equalizer. More precisely we first considered the case where the MAP equalizer is fed with a priori information on the transmitted data and studied analytically their impact on the MAP equalizer performance [24]. Then we assumed that the channel is not perfectly estimated and show that the use of both the a priori information and the channel estimate is equivalent to a shift in terms of signal-to-noise ratio (SNR) for which we provided an analytical expression [25].

6.8.4. Source-channel coding

Here we propose to adapt standard design tools (e.g. density evolution) to capture *heterogeneous* graphical structures, where correlations between bits are introduced both at the bit level (error correcting code), and at the symbol level (multiple description coding of a source). The target application is related to image coding for transmission over wireless IP, where both packet losses and bit errors may occur [22].

6.9. Sparse representations in redundant dictionaries

Participant: Jean-Jacques Fuchs.

The purpose is to extend previous work on sparse representations of signals in redundant bases developed in the noise-free case [9] to the case of noisy observations.

The type of questions addressed so far is : given a (n,m)-matrix A with $m > n$ and a vector $b = Ax_o$, find a sufficient condition for b to have an unique sparsest representation. The answer is a bound on the number of non-zero entries of say x_o, that guaranties that it is the unique and sparsest solution of $Ax = b$ when $b = Ax_o$.

We now consider the case $b = Ax_o + e$ [47] where x_o satisfies the sparsity conditions requested in the noise-free case and e is a vector of additive noise or modelling errors and seek conditions under which x_o can be recovered from b in a sense to be defined.

The conditions we get, relate the noise energy to the signal level as well as to the hyper-parameter of the quadratic program we use to recover the unknown sparsest representation. When the signal-to-noise ratio is large enough all the components of the signal are still present when the noise is deleted, otherwise the smallest components of the signal are themselves erased in a quite rational and predictable way.

6.10. Selection of variables in multiple linear regression

Participants: Jean–Jacques Fuchs, Sébastien Maria.

Numerous selection procedures have been proposed in the classical multiple linear regression model $y = X\beta + e$. The Backward Elimination Procedure is one of them. It has been developed and is used in the context of Least Squares models where it is assumed that (gaussian) errors e are present in the observation vector y that one wants to explain. This model is not quite general since in many practical situations, the components of some regressors X_j are essentially of the same nature as the components of the observation vector y. There is thus no reason to consider these regressors to be known exactly as is done in the standard Least Squares model. More generally it seems natural, depending upon the type of the regressors to consider that some are subject to noise while others (e.g. those having integer values) are known exactly and to develop selection procedures that allow to take this possibility into account. [58]

The multiple linear regression model where gaussian noise is assumed to be present not only on the observations but also on part of the regressors is known as the Total Least squares (TLS) model. We have developed the Backward Elimination procedure for this type of models. For this we have analyzed the statistical properties of the corresponding Maximum Likelihood parameter vector estimate using results from matrix perturbation analysis and developed a Student test that allows to decide if a component of the estimated β vector should be declared equal to zero.

7. Contracts and Grants with Industry

7.1. Fault diagnosis in telecommunication networks—rnrt project magda2

Participants: Eric Fabre, Albert Benveniste, Stefan Haar, Claude Jard.

Contract INRIA *2 01 C 0694 MPR 01 1, November 2001/January 2004*

The RNRT project is part of a long collaboration with France Télécom R&D, Alcatel (leader of MAGDA2), ILOG, and université de Paris–Nord. Its goal was to demonstrate the usefulness of distributed monitoring algorithms for heterogeneous networks.

We have focused on failure diagnosis issues for networks using a GMPLS communication model, allowing both circuit based networks of SDH or WDM type, or packet switch based networks (e.g. IP). The project has ended with a demo of a prototype displaying the following features :

- automatic discovery of the underlying network components and connections, and deployment of the *ad hoc* distributed monitoring architecture,
- automatic construction of an internal model for distributed model-based diagnosis,
- distributed alarm correlation, built over a commercialized rule engine (JRules, provided by Ilog),
- interaction with a real network management platform (Almap, provided by alcatel), for alarm collection, diagnosis display and service impact analysis.

7.2. rnrt project swan

Participants: Stefan Haar, Albert Benveniste, Eric Fabre, Claude Jard, Thomas Chatain.

Contract INRIA *2 04 A 0082 MC 01 1 — December 2003/June 2006*

The project *"SWAN: Self-Aware Management"* is being funded by the French national network RNRT, Ministry of Research. I started in December 2003 and is scheduled to last 30 months. The Distribcom team cooperates in SWAN with

- the *MADYNE* team of INRIA Lorraine and Paris-Nord University (the latter to be replaced soon by *LABRI* Bordeaux),
- industrial partners Alcatel, France Telecom, and QoSmetrics.

SWAN aims at empowering local autonomous diagnosis and administration functions in networks and services. Compared to the preceding projects *MAGDA* and *MAGDA2*, where *asynchronicity* and *distribution* were already at the heart, the new additional challenge in SWAN is *dynamicity*, namely non-static topologies of interaction. Networks expand or shrink as peers and connections are added or withdrawn at runtime, with the necessary adaptations and negotiations managed locally in the domain directly concerned. Web Services show by nature this dynamical behaviour. Both applications present thus a fundamental challenge to all model-based approaches to diagnosis and supervision more generally: find models that allow for self-modification - compare the discussion in the section on models of concurrency. DistribCom is leader of the SWAN project, and in charge of providing common mathematical models and algorithms for the two fields of applications.

7.3. CO2 : Composition and coherence of scenarios

Participant: Loïc Hélouët.

External research project with France Telecom

Software development often starts with requirement capture, ie collecting a set of representative behaviors of a system. Scenarios collected can be considered as partial views of a system, but may however comport some incoherences. The obective of CO2 is to provide formal definitions of scenario compositions, define notions of coherence for a set of views defined as a collection of scenarios, and provide decision algorithms indicating whether there exists an implementation realizing them.

8. Other Grants and Activities

8.1. Observation et supervision de systèmes complexes, répartis et dynamiques)

Participant: Claude Jard.

Contract CNRS *1 03 C 1559 — July 2003/December 2004*

We co-manage (with JB. Stefani)) a CNRS national prospective action on the supervision and control of large distributed dynamical systems. The other laboratories involved in the action are LIP6 (Paris), LAAS (Toulouse), and LORIA (Nancy). OSSCR has a total budget of 25k Euros for 2004.

8.2. Modèles aléatoires et calcul de performances de systèmes distribués

Participants: Stefan Haar, Samy Abbes.

Contract CNRS *MS08SIGMA2 — July 2003/Octobre 2004*

This prospective action focussing on *Random models and performance evaluation of distributed systems* is managed by L. Truffet (Nantes), comprises a number of teams all over France, and has traced future lines of research in probabilistic distributed systems. DistribCom has contributed on the Probabilistic models of concurrent systems, see the above discussion. The action was frozen for several month for budgetary reasons, and is to close in Oct/November.

8.3. NEWCOM – Network of Excellence in Wireless COMmunication

Participant: Aline Roumy.

Contract CNRS — *March 2004/December 2005.*

The NEWCOM project proposal (Network of Excellence in Wireless COMmunication) addresses the design of systems "beyond 3G". This requires to successfully solve problems such as: the inter-technology mobility management between 3G and ad-hoc wireless LANs, the coexistence of a variety of traffic/services with different and sometimes conflicting Quality of Service (QoS) requirements, new multiple-access techniques in a hostile environment like a channel severely affected by frequency selective fading, the quest for higher data rates also in the overlay cellular system, scaling with those feasible in a wireless LAN environment, permitting seamless handover with the same degree of service to the user, the cross-layer optimisation of physical coding/modulation schemes with the medium access control (MAC) protocols to conform with fully packetised transmission as well as the TCP/IP rules of the core network, and the like. Newcom has a duration of 18 months and we proposed 6 manmonths to be allocated to the DistribCom team.

8.4. PAI-Platon: Iterative turbo-like channel equalization techniques in the frequency domain for DFE performance improvement

Participant: Aline Roumy.

Contract MINISTÈRE DES AFFAIRES ÉTRANGÈRES *January 2003/December 2004.*

This is a collaboration between IRISA, Jacques Palicot, Supélec Rennes and Kostas Berberidis from the Signal Processing and Communications Lab, University of Patras, Greece. The goal of the proposed project is the development of an efficient equalization scheme, suitable for wireless burst communication systems. The basic characteristic of the proposed scheme will be the iterative operation of a channel estimator and a decision feedback equalizer on a data burst, in a way similar to Turbo techniques. This project has a duration of one year and can be extended to one more year. The grant supports travel and living expenses of investigators for short visits to partner institutions abroad.

9. Dissemination

9.1. Scientific animation

As a headline, we are pleased to report that *J.J. Fuchs received the 2003 Best Paper Award from the IEEE Signal Processing Society [46].*

A. Benveniste is associated editor at large (AEAL) for the journal *IEEE Trans. on Automatic Control* and member of the editorial board of the journal and «Proceedings of the IEEE». He has been in 2004 member of the Program Committee of the following conferences: MOVEP, EMSOFT, and has been invited to the for 2005 the Program Committee of HSCC and CONCUR. He has served as en expert for the Strong Research Environment programme of the Swedish Research Council and is member of the Strategic Advisory Council of the Institute for Systems Research, Univ. of Maryland, College Park, USA. He is in charge of managing the INRIA side of the Alcatel external Research Programme (ARP).

J.J. Fuchs is a member of the IEEE-SAM "Sensor Array and Multichannel" technical committee and acted as a co-chair of the Technical Program Committee of the Third IEEE Sensor Array and Multichannel Signal Processing Workshop *(SAM04)* held in Barcelona July 18 - 21, 2004. He is a member of the Program Committee of the French 20th Symposium on Signal and Image Processing GRETSI to be held in Louvain-la-Neuve sept. 6-9, 2005. He served as an expert for the National Science Foundation, USA.

C. Jard has been in 2004 member of the Program Committee of the following conferences: AFADL, MSR, MOVEP, FORTE, WODES, and has been invited for 2005 to the Program Committee of MSR, SAPIR, FORTE. He has served as an expert in the Research Councils of the following labs: CRIM (Canada), LIRMM, Samovar, LIAFA, Ecole Louis de Broglie (France). He was in 2004 member of the Advisory Council of the Information and Communication department of the CNRS, executive member of the national committee of evaluation of scientific research and has served as an expert in several programs of the french ministry of research. He is also member of the editorial board of the *Annales des Télécommunications.*

In 2004, C. Jard was member of the PhD Committees of E. Zinovieva (as supervisor) and B. Gaudin at Rennes, of B. Genest (as rapporteur) in Paris. He also participated to the Habilitation Committees of T. Jeron and Y. Le Traon (as president) at Rennes.

Stefan Haar is member of the working group for evaluation of international activities with the COST committee of INRIA. For the IFAC World congress 2005, he is member of the program subcommittee for discrete event and hybrid systems.

A. Roumy was member of the PHD Committees of Souad GUEMGHAR, Advanced Coding Techniques and Applications to CDMA, January 29th 2004, Télécom Paris, Eric HARDOUIN, égalisation au niveau chip pour la liaison descendante des systèmes de communications mobiles DS-CDMA, May 10th 2004, ENST Bretagne.

9.2. Teaching

J.J. Fuchs is a full-time professor at the Université de Rennes 1 and teaches mainly in the Diplôme d'Ingénieur en Informatique et téléCommunications (DIIC). In the Master-Recherche-STI of this same university he gives a course on Optimization.

É. Fabre and A. Roumy teach information theory and coding theory at Ecole Normale Supérieure de Cachan, Ker Lann campus, in the computer science and telecommunications magistère program.

S. Haar teaches problem sessions for the course on mathematics in computer science and telecommunications of the magistère program at Ecole Normale Supérieure de Cachan, Ker Lann campus, and contributes to the *Master de recherche* course on supervision of large distributed systems.

L. Hélouët teaches the UML notation to the mastere classes at ENST Bretagne.

C. Jard is a full-time professor at the ENS Cachan and teaches mainly at the Master level, in Computer Science and Telecom, and in Maths. He manages the Info-Telecom track of the Master-Recherche-STS of the Rennes 1 university. It is to be noted that one course in this track is on the research subject of DistribCom.

A. Roumy teaches «Modern coding theory» and «Multiuser detection» in the DEA TIS (Traitement des Images et du Signal) at ENSEA, université de Cergy Pontoise.

9.3. Participation in workshops, seminars, lectures, etc.

In May 2004, E. Fabre has visited Alan Willsky's group (LIDS) at MIT, and G. Cybenko's group in Dartmouth, where he gave several seminars (axiomatic derivation of iterative algorithms on graphs, and distributed diagnosis algorithms).

A. Roumy has presented her joint work on the design of LDPC codes for the multiuser access channel at the IEEE international symposium on Information Theory (ISIT) in Chicago in June 2004.

C. Jard has presented a joint work on unfoldings of time Petri nets at the CNRS national action on hybrid systems in Paris in September 2004.

T. Chatain has presented a joint work on symbolic unfoldings at the Forte international symposium on formal techniques at Madrid in September 2004. He has also attended to the summer school in Theoretical Computer Science at Marseille in June 2004, and has presented his PhD subject.

L. Hélouët has presented a joint work on covert channel detection in scenarios at the GDV 2004 workshop (Games in design and Verification) in Boston in July 2004. He has also presented a work on covert channel bandwidth evaluation at the SAM'2004 workshop (SDL and MSC) in Ottawa, in june 2004.

J.J. Fuchs has presented his work [17] on sparse representations at the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2004) in Montreal in May 2004.

9.4. Visits and invitations

Stefan Haar has visited the University of Stuttgart (cooperation with B. Koenig), followed by attendance, upon invitaton, of the Dagstuhl seminar on process algebras and graph grammars in June 2004; following attendance of the ICGT Graph Transformation conference in Rome, he visited Andrea Corradini at University of Pisa and Paolo Baldan at University of Venice / Mestre.

10. Bibliography

Major publications by the team in recent years

[1] S. ABBES. *Probabilistic Models for Distributed and Concurrent Systems. Limit Theorems and Applications to Statistical Parametric Estimation*, University of Rennes I, Ph. D. Thesis, Oct. 2004.

[2] A. BENVENISTE, E. FABRE, C. JARD, S. HAAR. *Diagnosis of asynchronous discrete event systems, a net unfolding approach*, in "IEEE Transactions on Automatic Control", vol. 48, n^o 5, May 2003, p. 714–727.

[3] E. FABRE, A. BENVENISTE, S. HAAR, C. JARD. *Distributed Monitoring of Concurrent and Asynchronous Systems*, in "Journal of Discrete Event Dynamic Systems: Theory and Applications, special issue", to appear.

[4] J. J. FUCHS. *On the application of the global matched filter to DOA estimation with uniform circular arrays*, in "IEEE Trans. on Signal Processing", 2003 Best Paper Award IEEE Trans. on Signal Processing, Apr. 2001, p. 702 - 709.

[5] A. ROUMY, S. GUEMGHAR, G. CAIRE, S. VERDU. *Design Methods for Irregular Repeat-Accumulate Codes*, in "IEEE Trans. on Information Theory", August 2004, p. 1711 - 1727.

Doctoral dissertations and Habilitation theses

[6] S. ABBES. *Probabilistic Models for Distributed and Concurrent Systems. Limit Theorems and Applications to Statistical Parametric Estimation*, University of Rennes I, Committee: J. Mairesse, G. Winskel, A. Benveniste, J-P. Banâtre, J-P. Kaoten, V. Kaimanovitch, S. Haar, Ph. D. Thesis, Oct. 2004.

Articles in referred journals and book chapters

[7] G. CAIRE, S. GUEMGHAR, A. ROUMY, S. VERDU. *Maximizing the spectral efficiency of coded CDMA under successive decoding*, in "IEEE Trans. on Information Theory", Jan. 2004, p. 152 - 164.

[8] E. FABRE, A. BENVENISTE, S. HAAR, C. JARD. *Distributed Monitoring of Concurrent and Asynchronous Systems*, in "Journal of Discrete Event Systems, special issue", to appear.

[9] J. J. FUCHS. *On sparse representations in arbitrary redundant basis*, in "IEEE Trans. on Information Theory", June 2004, p. 1341 - 1344.

[10] C. JARD, T. JÉRON. *TGV: theory, principles and algorithms. A tool for the automatic synthesis of conformance test cases for non-deterministic reactive systems*, in "Software Tools for Technology Transfert", to appear.

[11] A. ROUMY, S. GUEMGHAR, G. CAIRE, S. VERDU. *Design Methods for Irregular Repeat-Accumulate Codes*, in "IEEE Trans. on Information Theory", August 2004, p. 1711 - 1727.

Publications in Conferences and Workshops

[12] A. AGHASARYAN, C. JARD, J. THOMAS. *UML Specification of a Generic Model for Fault Diagnosis of Telecommunication Networks*, in "International Communication Conference (ICT)", August 2004.

[13] A. BENVENISTE, S. HAAR, E. FABRE, C. JARD. *Distributed Unfoldings : a Tool to Address Distributed Discrete Event Systems Diagnosis*, in "42nd IEEE Conference on Decision and Control (CDC), Hawai", IEEE Control Systems Society, December 2003.

[14] T. CHATAIN, J. C.. *Symbolic Diagnosis of Partially Observable Concurrent Systems*, in "24th IFIP WG 6.1 International Conference on Formal Techniques for Networked and Distributed Systems (FORTE 2004)", September 2004.

[15] E. FABRE, A. BENVENISTE, S. HAAR, C. JARD, A. AGHASARYAN. *Algorithms for Distributed Fault Management in Telecommunications Networks*, in "International Communication Conference (ICT)", August 2004.

[16] E. FABRE. *Runs of a Distributed System are a Product of Local Runs*, in "Mathematical Theory of Networks and Systems (MTNS)", July 2004.

[17] J. FUCHS. *Recovery of exact sparse representations in the presence of noise*, in "IEEE ICASSP04", May 2004, p. 533 - 536.

[18] S. HAAR, A. BENVENISTE, E. FABRE, C. JARD. *Partial Order Diagnosability of Discrete Event Systems using Petri Nets Unfoldings*, in "42nd IEEE Conference on Decision and Control (CDC), Hawai", IEEE Control Systems Society, December 2003.

[19] L. HÉLOUËT. *Finding covert channels in protocols with Message Sequence Charts: the case of RMTP2*, in "Proc. of SAM'2004, 4th conference on SDL and MSC", June 2004.

[20] L. HÉLOUËT, M. ZEITOUN, A. DEGORRE. *Scenarios and cover channels: yet another game*, in "Proc. of GDV'04 : 1st workshop on Games In design and Verification", Jul 2004.

[21] J. KLEIN, B. CAILLAUD, L. HÉLOUËT. *Merging Scenarios*, in "Proc. of FMICS'04 (Formal Methods in Industrial and Critical Systems", Sep. 2004.

[22] M. KOCA, E. FABRE, A. ROUMY. *Turbo Decoding of multiple descriptions with quantized frame expansions*, in "International Symposium on Image/Video Communications over fixed and mobile networks, ISIVC'04", Jul 2004.

[23] A. ROUMY, D. DECLERCQ, E. FABRE. *Low Complexity Code Design for the 2-user Gaussian Multiple Access Channel*, in "Proc. of ISIT, IEEE Int. Conference on Information Theory", June 2004.

[24] N. SELLAMI, A. ROUMY, I. FIJALKOW. *On the analysis of the MAP equalizer performance within an iterative receiver*, in "IEEE International Workshop on Signal Processing Advances for Wireless Communications, SPAWC 2004", Jul 2004.

[25] N. SELLAMI, A. ROUMY, I. FIJALKOW. *Performance analysis of the MAP equalizer within an iterative receiver including a channel estimator*, in "IEEE Vehicular Technology Conference, VTC'F04", September 2004.

[26] T. ZIADI, L. HÉLOUËT, JEAN-MARC. JÉZÉQUEL. *Behaviors Generation From Product Lines Requirements*, in "Proc. of UML2004 workshop on Software Architecture Description & UML", Oct. 2004.

[27] T. ZIADI, L. HÉLOUËT, JEAN-MARC. JÉZÉQUEL. *Revisiting Statechart Synthesis with an algebraic approach*, in "Proc. if ISRE'04", may 2004.

Internal Reports

[28] S. ABBES. *A Probabilistic Model for True Concurrency*, Technical report, n° 1591, IRISA, mar. 2004, http://www.irisa.fr/bibli/publi/pi/2004/1591/1591.html.

[29] S. ABBES. *The Projective Formalism for Topological Event Structures, and a Probabilistic Application - Extended Version*, Technical report, n° 1614, IRISA, apr. 2004, http://www.irisa.fr/bibli/publi/pi/2004/1614/1614.html.

[30] S. ABBES, A. BENVENISTE. *Branching Cells as local states for event structures and nets: probabilistic applications*, Technical report, n° 1651, IRISA, oct. 2004, http://www.irisa.fr/bibli/publi/pi/2004/1651/1651.html.

[31] S. ABBES, A. BENVENISTE, S. HAAR. *Distributed Probabilities on Locally Finite Event Structures - Extended Version*, Technical report, n° 1615, IRISA, apr. 2004, http://www.irisa.fr/bibli/publi/pi/2004/1615/1615.html.

[32] A. BENVENISTE, S. HAAR, C. FABRE, C. JARD. *Distributed monitoring of concurrent and asynchronous systems - extended version (update of research report PI-1540)*, Technical report, n° 1636, IRISA, jul. 2004, http://www.irisa.fr/bibli/publi/pi/2004/1636/1636.html.

[33] E. FABRE. *Factorization of Unfoldings for Distributed Tile Systems Part 2: General Case*, Technical report, n° 5186, INRIA, may 2004, http://www.inria.fr/rrrt/rr-5186.html.

[34] J. FUCHS. *Recovery of exact sparse representations in the presence of bounded noise*, Technical report, n° 1618, IRISA, apr. 2004, http://www.irisa.fr/bibli/publi/pi/2004/1618/1618.html.

[35] S. HAAR. *Diagnosability Of Asynchronous Discrete Event Systems in Partial Order Semantics*, Technical report, n° 5248, INRIA, jul. 2004, http://www.inria.fr/rrrt/rr-5248.html.

Bibliography in notes

[36] *Introduction to discrete event systems*, Kluwer Academic Publishers, 1999.

[37] H. EHRIG, H.-J. KREOWSKI, U. MONANARI, G. ROZENBERG (editors). *Handbook of graph grammars*

and computing by graph transformations: vol. 3, concurrency, parallelism, and distribution, World Scientific, 1999.

[38] *Petri nets*, Springer Verlag, 1985.

[39] P. BALDAN, A. CORRADINI, U. MONTANARI. *Unfolding and event structure semantics for graph grammars*, in "Proc. of FOSSACS 1999", LNCS, vol. 1578, Springer Verlag, 1999, p. 73–89.

[40] D. E. BELL, L. J. LAPADULA. *Secure Computer Systems: Mathematical Foundations*, Technical report, n° MTR-2547, Vol. 1, MITRE Corp., Bedford, MA, 1973.

[41] C. BERROU, AL.. *Near Shannon limit error-correcting and decoding: Turbo-codes*, in "Proc. of ICC'93", 1993, p. 1064-1070.

[42] M. BUSCEMI, V. SASSONE. *High-Level Petri Nets as Type Theories in the Join Calculus*, in "FOSSACS'2001", 2001.

[43] D. DONOHO, X. HUO. *Uncertainty principles and ideal atomic decomposition*, in "IEEE Trans. on Information Theory", Nov. 2003, p. 2845 - 2862.

[44] E. FABRE. *Factorization of Unfoldings for Distributed Tile Systems, Part 1 : Limited Interaction Case*, Publication Interne, n° 1529, IRISA, april 2003, ftp://ftp.irisa.fr/techreports/2003/PI-1529.ps.gz.

[45] J. J. FUCHS, B. DELYON. *Minimum L_1-norm reconstruction function for oversampled signals: Application to time-delay estimation*, in "IEEE Trans. on Information Theory", June 2000, p. 1666 - 1673.

[46] J. J. FUCHS. *On the application of the global matched filter to DOA estimation with uniform circular arrays*, in "IEEE Trans. on Signal Processing", Apr. 2001, p. 702 - 709.

[47] J. FUCHS. *Recovery of exact sparse representations in the presence of bounded noise*, Technical report, n° PI n°1618, IRISA, 2004.

[48] J. GOGUEN, J. MESEGUER. *Security Policies and Security Models*, in "IEEE Symposium on Security ans Privacy", apr 1982, p. 11-20.

[49] R. GRIBONVAL, M. NIELSEN. *Sparse representations in unions of bases*, in "IEEE Trans. on Information Theory", Dec. 2003, p. 3320 - 3325.

[50] O. M. GROUP. *Unified Modeling Language Specification version 2.0: Superstructure*, Technical report, n° pct/03-08-02, OMG, 2003.

[51] ITU-TS. *ITU-TS Recommendation Z.120: Message Sequence Chart (MSC)*, ITU-TS, Geneva, September 1999.

[52] K. JENSEN. *Colored Petri nets. Basic concepts, Analysis Methods and Practical Use*, EATCS Monographs on Theoretical Computer Science, Springer Verlag, 1992.

[53] V. KHOMENKO, M. KOUTNY. *Branching Processes to High-Level Petri Nets*, in "Proc. of Intern. Conf. on Tools and Algorithms for the Construction and A nalysis of Systems (TACAS'2003)", H. GARAVEL, J. HATCLIFF (editors)., LNCS, Springer-Verlag, 2003.

[54] V. KOZURA. *Unfolding of Coloured Petri Nets*, Technical report, n° Technical Report 80, A.P. Ershov Institute of Informatics Systems, 2000.

[55] L. H.-A. KSCHISCHANG F.R.. *Factor graphs and the sum-product algorithm*, in "IEEE Trans. on Inf. Th.", vol. 47, n° 2, Feb 2001, p. 498 -519.

[56] L. J. LAPADULA, D. E. BELL. *Secure Computer Systems: A Mathematical Model*, Reprinted in J. of Computer Security, vol. 4, no. 2–3, pp. 239–263, 1996, Technical report, n° MTR-2547, Vol. 2, MITRE Corp., Bedford, MA, 1973.

[57] P. LE MAIGAT, L. HÉLOUËT. *A (max,+) approach for time in Message Sequence Charts*, in "5th Workshop on Discrete Event Systems (WODES 2000)", 2000.

[58] S. MARIA, J. FUCHS. *A new Approach to Variable Selection using the TLS Approach*, in "IEEE ICASSP05", May 2005.

[59] M. NIELSEN, G. PLOTKIN, G. WINSKEL. *Petri nets, event structures and domains, part 1*, in "T.C.S.", 1981.

[60] J.-F. C. R.J. MCELIECE. *Turbo decoding as an instance of Pearl's 'belief propagation' algorithm*, in "IEEE J. on Sel. Areas in Comm.", vol. 16, n° 2, Feb 1998, p. 140-152.

[61] M. RENIERS, S. MAUW. *High-level Message Sequence Charts*, in "SDL97: Time for Testing - SDL, MSC and Trends, Evry, France", A. CAVALLI, A. SARMA (editors)., Proceedings of the Eighth SDL Forum, September 1997, p. 291-306.

[62] M. RENIERS. *Message Sequence Charts: Syntax and Semantics*, Ph. D. Thesis, Eindhoven University of Technology, 1998.

[63] E. RUDOLPH, P. GRAUBMAN, J. GRABOWSKI. *Tutorial On Message Sequence Charts*, in "Computer Networks and ISDN Systems", vol. 28, 1996, p. 1629-1641.

[64] S. S. S. VERDÚ. *Spectral efficiency of CDMA with random spreading*, in "IEEE Trans. on Inf. Th.", vol. 2, March 1999, p. 622-640.

[65] R. U. T.J. RICHARDSON. *The capacity of low-density parity-check codes under message-passing decoding*, in "IEEE Trans. on Inf. Th.", vol. 47, n° 2, Feb 2001, p. 599-618.

[66] R. U. T.J. RICHARDSON. *Design of capacity-approaching irregular low-density parity-check codes*, in "IEEE Trans. on Inf. Th.", vol. 47, n° 2, Feb 2001, p. 619-637.

[67] D. VARACCA, H. VÖLZER, G. WINSKEL. *Probabilistic event structures and domains*, in "Proc. of CONCUR'04", LNCS, 2004.

[68] H. VÖLZER. *Randomized non-sequential processes*, in "Proc. of CONCUR'01", LNCS, vol. 2154, 2001, p. 184–201.

[69] N. WIBERG. *Codes and decoding on general graphs, Ph.D.*, Dept. of Electrical Engineering, University of Sweden, Sweden, 1996.

[70] G. WINSKEL. *Event structures semantics in CCS and related languages*, in "LNCS", vol. 140, Springer Verlag, 1982.

[71] G. WINSKEL. *Categories of models for concurrency*, in "Seminar on Concurrency, Carnegie-Mellon Univ. (July 1984), LNCS 197", 1985, p. 246-267.

[72] S. TEN BRINK. *Convergence behavior of iteratively decoded parallel concatenated codes*, in "IEEE Trans. on Communications", vol. 49, Oct 2001, p. 1727-1737.