ACI Sécurité Informatique CORTOS
« Control and Observation of Real-Time Open Systems »

April 26, 2005

The web site of the project is `http://www.lsv.ens-cachan.fr/aci-cortos/`

1 CORTOS from an Administrative Point of View

Labs involved in the project.

- Institut de Recherche en Communications et en Cybernétique de Nantes (IRCCyN, CNRS UMR 6597 & École des Mines de Nantes & École Centrale de Nantes & Université de Nantes), Group MOVES,
- Laboratoire Spécification et Vérification (LSV, CNRS UMR 8643 & ENS de Cachan),
- VERIMAG (CNRS UMR 5104 & Université Joseph Fourier & Institut National Polytechnique de Grenoble).

Members of the Project. On April 1st, 2005, the members of the project are:

Name	**First name**	**Position**	**Lab**
Cassez	Franck	Chargé de recherche CNRS	IRCCyN
Gardey	Guillaume	Doctorant (BDI CNRS & Région Pays de la Loire)	
Roux	Olivier H.	Maître de conférences IUT de Nantes	
Roux	Olivier	Professeur École Centrale Nantes	
Bel Mokadem	Houda	Doctorant (alloc. ENS de Cachan)	LSV
Bouyer	Patricia	Chargée de recherche CNRS	
Chevalier	Fabrice	Doctorant (AC ENS de Cachan)	
Demri	Stéphane	Chargé de recherche CNRS	
Laroussinie	François	Maître de conférences ENS de Cachan en délégation CNRS	
Markey	Nicolas	Chargé de recherche CNRS	
Reynier	Pierre-Alain	Doctorant (Élève ENS de Cachan)	
Altisen	Karine	Maître de conférence INPG	VERIMAG
Dang	Thao	Chargée de recherche CNRS	
Krichen	Moez	Doctorant (alloc. MENRT)	
Tripakis	Stavros	Chargé de recherche CNRS	

Among the former members some are still involved in the project:

Bérard	Béatrice	Professeur, université Paris Dauphine (since september 2004, formerly at LSV)
Cachat	Thierry	Maître de conférences, université Paris 7 (since september 2004, formerly at LSV)

Other former members are:

Lime	Didier	Post-doc at Aalborg University (Denmark), formerly at IRCCyN
D'Orso	Julien	Post-doc at LIAFA, Paris 7 (France), formerly at IRCCyN

Project Management. Since the project has started in sep. 2003, we have organized five global meetings (dates and programs can be found on our web site). During those meetings, we have invited twice external participants: Jean-François Raskin (Université Libre de Bruxelles, Belgique) and Aymeric Vincent (LaBRI, Bordeaux). One of this meeting has been jointly organized with european project AMETIST. Apart from these global meetings (that all members of the project could attend), several working groups have been organized (to work on more specific subjects and to write papers).

2 Our Results

During our first meetings, we have mostly presented existing works to identify precisely themes on which we wanted to work. We have established a large bibliography (see our internal web site), and we have then focused our interest and invited specialists of domains which were of interest for us. The results we have obtained roughly follow the lines of our initial project statement, and some additional works have been done.

2.1 Observation of Systems

Observation of Real-Time Systems. Observation lies at the heart of many problems, including control. Indeed, although control is a more general problem than observation in terms of decidability and complexity, solving the control problem is most of the times not harder than solving the observation problem.

In the case of real-time systems modeled as timed automata, a crucial assumption made in previous work on controller synthesis is that the controller is state-feedback, that is, can observe the complete state of the system under control, including discrete variables and clocks. In [22] we showed that this assumption can be relaxed, at least in the case of monitoring for purposes of fault detection. We showed that it is possible to synthesize observers using an on-the-fly subset construction technique, consisting in computing the set of all possible states the automaton can be in, given the current observation.

In the course of this project, we have developed the above mentioned ideas further and applied them to monitoring [3] and testing [16, 17, 18]. Testing is very similar to control, in that both can be seen as games. In control, the game is played between the controller and the plant: the controller tries to maintain or achieve a given specification, while the plant "tries" to prevent the controller from doing so. In testing, the game is played between the tester and the system under test (SUT): the tester tries to show that the SUT is non-conforming to the specification, while the SUT tries to prevent the tester from doing so.

We have also extended existing work on the observation problem by synthesizing observers as deterministic timed automata (DTA) [12, 11]. In this setting, the observation problem is modeled as a game between the environment and the observer and we give algorithms for synthesizing observers that are various types of DTA, *e.g.* DTA and event-clock automaton when the observer has bounded resources.

Decentralized Observation Problems. Observation and control is quite well understood for untimed systems in the centralized case, that is, where a unique controller is assumed to control the entire plant. All the work on observation and control for timed systems also assumes a centralized framework.

In this research axis, we study problems of decentralized observation and control, where a number of observers/controllers act in parallel for a given plant. Initially, we focus on observation, which is often a necessary first step in order to understand control. Moreover, in recent work [20, 23] we have shown that some decentralized observation problems are undecidable and can also be used to show undecidability of control problems. In [24] we have extended our study to problems of distributed observation with bounded or unbounded memory and proved several (un)decidability results and proposed algorithms for synthesizing distributed observers.

2.2 Control for Time Petri Nets (TPN)

Scheduling. Hard real-time systems are usually designed as several tasks interacting and sharing one or more processors. Hence, in a system S, tasks have to be scheduled on the processors in such a way that

they respect some properties P imposed by the controlled process. This is usually achieved using either an offline or an online approach.

We consider an extension of TPNs, namely scheduling-TPNs, that allows to take into account the way the real-time tasks of an application distributed over different processors are scheduled. This model allows us to model preemption and resumption of actions in time-dependent systems and is based on the concept of stopwatches. We have proved [4] that the (state) reachability problem is undecidable for a simple class of TPNs extended with stopwatches, even when bounded. This result can be easily generalized to known extensions of TPNs allowing preemption and resumption of transitions [21, 19]. Concerning the analysis of scheduling-TPN, in [19], we tackle the problem of the state space explosion using a fast DBM-based algorithm which overapproximates the set of reachable states but which can then be analyzed using a tool like HyTech.

Safety Control Synthesis on TPNs. Unlike timed automata which have a finite discrete state-space structure (locations), the set of reachable markings of a TPN is generally infinite and this property is undecidable. We study some control synthesis problems on an extension of TPNs that model a plant and its environment. The TPN control model both represents controllable and uncontrollable events, the problem is then to design a function (controller) such that a given property is fulfilled. We focus our analysis on safety properties expressed on the markings of the net and we propose a symbolic method to decide the existence of a controller that ensures this properties. Unlike existing methods on TPNs, that assume the net is bounded, the method is applicable for any TPNs and we prove in particular that existence of a controller which k-bounds the plant is decidable. This work is under submission.

2.3 Timed Modal Logic for Control

In the untimed framework solving a μ-calculus model-checking problem is equivalent to solving the control problem for plants expressed as finite automata. This equivalence is highly used and important. We have then proposed an extension of this reduction to the timed framework [10] and have used the timed modal logic L_ν to express timed control objectives. We have shown that the control problem for a large class of such objectives can be reduced to a model-checking problem for an extension of the logic L_ν with a new modality (which is proved to be necessary to express control problems). We have also proved that model-checking this new logic remains EXPTIME-complete and integrated it in the model-checker CMC (which implements a compositional model-checking method for L_ν).

2.4 Optimal Timed Control

Optimal Reachability Control. One important problem in control is also to optimize the consumption of resources: one wants to control a system but using as few resources as possible. In the case of the reachability control problem and if the resource is time, the aim is to force the environment to reach a particular state q as quickly as possible. The optimal time the controller can guarantee is thus the value t^* s.t. whatever the environment does the controller can guarantee to reach state q within t^* time units, and it cannot guarantee this for any $t < t^*$. The previous problem is known as the "optimal-time reachability control problem" and has been solved in 1999. We have studied a more general version of the problem, namely the cost-optimal control problem, where the resource is more general than time. We have defined the model of priced timed game automata (PTGA) and proved that the computation of the optimal cost for a large class of PTGA is computable [7, 8]. Moreover we have implemented our algorithm [9] with the tool HYTECH.

Optimal Infinite Schedules. In works presented above, control objectives are "reach a given set of states". We have also considered safety control objectives where the aim is to optimize mean cost along schedules of the system, and first restrict to closed systems where all actions are supposed to be controllable. To cover a wide class of optimality criteria we have introduced an extension of the (priced) timed automata model that includes both costs and rewards as separate modelling features. With that model it is

easy to express properties like “find infinite schedules where the cost by time unit is minimal” or “find infinite schedules where the cost by action is minimal”, etc. We have subsequently shown that the derivation of optimal infinite schedules for this model is computable. This is done by a reduction of the problem to the determination of optimal mean-cycles in finite graphs with weighted edges. This reduction is obtained by introducing the so-called corner-point abstraction, a powerful abstraction technique of which we show that it preserves optimal schedules [5, 6]. As further important developments, we aim at solving the problem in the presence of an adversary (*i.e.* when some actions are not controllable).

2.5 Applications of Control Problems

Hybrid Controller Synthesis. In this work, we developed a method for hybrid controller synthesis through the study of an engine control problem, namely, idle speed control. The model of the car engine is a hybrid automaton with both continuous and discrete inputs. One important control objective is to maintain the speed of the car within some desired range (around the reference value). This problem is known to be difficult due to unpredictable external disturbances (for instance, load variations).

The safety controller we want to design is hybrid in the sense that it comprises a continuous law (for the throttle angle), and a mode switching law (the decision between positive and negative sparks). Such controllers can be derived from the maximal invariant set; however, it is hard, both theoretically and practically, to compute this set for a nonlinear hybrid system with both continuous and discrete control inputs. For effective computation purposes, we restrict the continuous laws to be in a class of piecewise constant functions with uncertain interval. Furthermore, using the cascade structure of the system, we apply the compositional assume-guarantee reasoning from model-checking to this controller design process.

In addition, the use of piecewise constant control inputs allows to take into account optimality criteria (such as minimizing gas consumption). We have also studied the problem of quantifying the performance loss due to the use of piecewise constant control in this specific car control problem as well as in a more general context. More details on the results of this work can be found in [13].

Application of Controller Synthesis to Aspect Oriented Programming (AOP). In this work, controller synthesis is used as a conceptual tool to specify and understand aspect oriented programming (AOP) in a formal framework. It aims at providing new facilities to implement or modify existing programs: implementing some new functionality or property in a program P may not be done by adding a new module to the existing structure of P but rather by modifying every module in P. This kind of functionality or property is then called an aspect. AOP provides a way to define aspects separately from the rest of the program and then to introduce or "weave" them automatically into the existing structure.

The goal of this work is to study a notion of aspects for reactive systems. As weaving an aspect into a program P introduces some modifications of the behavior of P, and as we deal with critical systems, our notion of aspect needs to be semantical. Ideally, in a formal framework, when defining an aspect A for a program P, one should be aware of what the weaving of A into P implies on the behavior of the woven program *i.e.* (1) what A changes and what is ensured by the new behaviors; (2) what A does not change w.r.t. P, namely which property of P is preserved when weaving A. (Among these properties, some form of equivalence preservation should of course at least be ensured.) Both (1) and (2) can be interpreted as a controller synthesis problem. We are currently working on that interpretation to better understand the AOP framework [1, 2].

Scheduling of Multi-Threaded Real-Time Programs using Geometry. In this work [15] we examined the behavior of a class of multi-threaded programs, from the point of view of the worst-case response time. We defined a timed version of PV programs and diagrams which can be used to model a large class of multi-threaded programs sharing resources. PV programs and diagrams, introduced by Dijkstra, are models for geometrically describing interactions of concurrent processes and have been used for the analysis of concurrent programs. We also introduced the notion of the worst-case response time of a schedule of a timed PV programs. This framework can be used to compute efficient schedules for multi-threaded programs on a limited number of processors. In particular, to tackle the complexity problem, we defined an abstraction of the optimal schedules and developed a method to construct this abstraction

in order to compute efficient schedules as well as an optimal one. This method is based on a geometric realization (or geometrization) of the timed PV program and a spatial decomposition of the geometrization. An experimental implementation allowed us to validate the method and provided encouraging results.

We are currently working on a new method for computing an optimal schedule, which exploits further the geometry of the timed PV programs. We show a relation between continuous properties of the geometrization and the abstraction of the optimal schedules. This relation can be used to solve the scheduling problem more efficiently.

3 CORTOS in France and Further

The project CORTOS is committed in several national and international activities:

- an invited session of french conference MSR'05 will be devoted to the control of timed systems, and talks will be given by members of the project;
- a tutorial on timed control at a meeting of the AS 155 du RTP 24 "Approches formelles pour l'analyse et la synthèse sûre de contrôle des systèmes dynamiques hybrides" has been given in september 2004 by Franck Cassez;
- a course on the control of timed systems has been given by Patricia Bouyer at the Spring School on Infinite Games (organized by the european network GAMES);

We still plan to organize a workshop on the control of timed systems, possibly as a satellite event of CONCUR'06 (which takes place in Bonn).

References

[1] K. Altisen, F. Maraninchi, and D. Stauch. Exploring aspects in the context of reactive systems. In *Proc. Workshop Foundations of Aspect-Oriented Languages (FOAL'04)*, pp. 45–51, 2004.

[2] K. Altisen, F. Maraninchi, and D. Stauch. Aspect-oriented programming for reactive systems: a proposal in the synchronous framework, 2005. Submitted to Science of Computer Programming, (Special Issue on Foundations of Aspect-Oriented Programming).

[3] S. Bensalem, M. Bozga, M. Krichen and S. Tripakis. Testing conformance of real-time applications by automatic generation of observers. In *Proc. 4th Int. Workshop Runtime Verification (RV'04)*, ENTCS. Elsevier, 2004. To appear.

[4] B. Berthomieu, D. Lime, O. H. Roux, and F. Vernadat. Reachability problems and abstract state spaces for time Petri nets with stopwatches. Technical Report 04483, LAAS, 2004.

[5] P. Bouyer, E. Brinksma, and K. G. Larsen. Staying alive as cheaply as possible. In *Proc. 7th Int. Workshop on Hybrid Systems: Computation and Control (HSCC'04)*, vol. 2993 of *LNCS*, pp. 203–218. Springer, 2004.

[6] P. Bouyer, E. Brinksma, and K. G. Larsen. Optimal infinite scheduling for multi-priced timed automata. *Formal Methods in System Design*, 2005. To appear.

[7] P. Bouyer, F. Cassez, E. Fleury, and K. G. Larsen. Optimal strategies in priced timed game automata. Research Report BRICS RS-04-4, Basic Research in Computer Science, Denmark, 2004. Available on `http://www.brics.dk/RS/04/4/`.

[8] P. Bouyer, F. Cassez, E. Fleury, and K. G. Larsen. Optimal strategies in priced timed game automata. In *Proc. 24th Conf. on Foundations of Software Technology and Theoretical Computer Science (FST&TCS'2004)*, vol. 3328 of *LNCS*, pp. 148–160. Springer, 2004.

[9] P. Bouyer, F. Cassez, E. Fleury, and K. G. Larsen. Synthesis of optimal strategies using HyTech. In *Proc. Workshop on Games in Design and Verification (GDV'04)*, vol. 119(1) of *ENTCS*, pp. 11–31. Elsevier Science Publishers, 2005.

[10] P. Bouyer, F. Cassez, and F. Laroussinie. Modal logics for timed control. Research Report RI-2005-3, IRCCyN/CNRS, Nantes, France, 2005. Submitted to CONCUR'05.

[11] P. Bouyer, F. Chevalier, and D. D'Souza. Fault diagnosis using timed automata. In *Proc. 8th Int. Conf. on Foundations of Software Science and Computation Structures (FOSSACS'2005)*, vol. 3441 of *LNCS*, pp. 219–233. Springer, 2005.

[12] F. Chevalier. Détection d'erreurs dans les systèmes temporisés. Master's thesis, DEA Algorithmique, Paris, 2004.

[13] T. Dang. Application of reachability analysis to idle speed control synthesis. *Int. Journal of Software Engineering & Knowledge Engineering (IJSEKE)*, 2005. Special issue of selected papers from the Int. Embedded and Hybrid Systems Conf. (IEHSC'05), to appear.

[14] S. Demri, R. Lazić, and D. Nowak. On the freeze quantifier in constraint LTL: Decidability and complexity. In *Proc. 12th Int. Symp. on Temporal Representation and Reasoning (TIME'05)*. IEEE Computer Society Press, 2005. To appear.

[15] P. Gerner and T. Dang. Computing schedules for multithreaded real-time programs using geometry. In *Proc. Joint Conf. on Formal Modelling and Analysis of Timed Systems and Formal Techniques in Real-Time and Fault Tolerant System (FORMATS+FTRTFT'04)*, vol. 3253 of *LNCS*, pp. 325–342. Springer, 2004.

[16] M. Krichen and S. Tripakis. Black-box conformance testing for real-time systems. In *Proc. 11th Int. SPIN Workshop (SPIN'04)*, vol. 2989 of *LNCS*, pp. 109–126. Springer, 2004.

[17] M. Krichen and S. Tripakis. Real-time testing with timed automata testers and coverage criteria. In *Proc. Joint Conf. on Formal Modelling and Analysis of Timed Systems and Formal Techniques in Real-Time and Fault Tolerant System (FORMATS+FTRTFT'04)*, vol. 3253 of *LNCS*, pp. 134–151. Springer, 2004.

[18] M. Krichen and S. Tripakis. An expressive and implementable formal framework for testing real-time systems. In *Proc. 17th IFIP Int. Conf. on Testing of Communicating Systems (TESTCOM'05)*, LNCS. Springer, 2005. To appear.

[19] D. Lime and O. H. Roux. A translation based method for the timed analysis of scheduling extended time Petri nets. In *Proc. 25th IEEE Real-Time Systems Symp. (RTSS'04)*, pp. 187–196. IEEE Computer Society Press, 2004.

[20] A. Puri, S. Tripakis, and P. Varaiya. *Synthesis and Control of Discrete Event Systems*, chapter Problems and Examples of Decentralized Observation and Control for Discrete Event Systems, pp. 37–56. Kluwer Academic Publishers, 2002. First published in Proc. Symp. Sypervisory Control for Discrete Event Systems (SCODES'01).

[21] O. H. Roux and D. Lime. Time Petri nets with inhibitor hyperarcs. Formal semantics and state space computation. In *Proc. 25th Int. Conf. Application and Theory of Petri Nets (ICATPN'04)*, vol. 3099 of *LNCS*, pp. 371–390. Springer, 2004.

[22] S. Tripakis. Fault diagnosis for timed automata. In *Proc. 7th Int. Symp. on Formal Techniques in Real-Time and Fault Tolerant Systems (FTRTFT'02)*, vol. 2469 of *LNCS*, pp. 205–224. Springer, 2002.

[23] S. Tripakis. Undecidable problems of decentralized observation and control on regular languages. *Information Processing Letters (IPL)*, 90(1):21–28, 2004.

[24] S. Tripakis. Two-phase distributed observation problems. In *Proc. 5th Int. Conf. on Application of Concurrency to System Design (ACSD'05)*. IEEE Computer Society Press, 2005. To appear.