Proposition de thèse de doctorat / PhD

Subject

Runtime validation of timed properties

Keywords: timed systems, runtime validation, enforcement, model based testing, test purpose, test generation, timed traces

Terms

Title: Runtime validation for timed properties: expressiveness, efficiency,...
Duration: 36 months
Type: PhD position

Main advisors

Antoine Rollet
LaBRI - University of Bordeaux
(+33)5 40 00 35 34
email: rollet_AT_labri.fr

Ylies Falcone
LIG - Université de Grenoble
(+33)4 76 82 72 14
email: Ylies.Falcone_AT__ujf-grenoble.fr

Official advisor

Mohamed Mosbah
LaBRI - University of Bordeaux
(+33)5 40 00 69 17
email: mosbah_AT__labri.fr

Context

Timed properties are often used to specify the behavior of (safety-critical) systems. Having behavioral specifications that take time into account offers desirable expressiveness but raises new challenges for the validation process.

One "family" of techniques are the so-called dynamic validation techniques where verification occurs at runtime. This family includes techniques such as runtime verification...
[Hav00,HR01,HR02,LKK+99,LS08], runtime enforcement [HMS06,Sch00,Vis00,LBW09,LBW05,Fal09,FFM12]. Common to these techniques is that the full behavioral specification of the system is not required.

- **Runtime verification**: a "monitor" is used to check if an execution trace verifies a property P without modifying the execution of the system. Compared to many testing approaches, this technique does not require a specification of the system, but only the property to check.

- **Runtime enforcement**: may be seen as an extension of the previous approach. The monitor (called now enforcer) can be seen as a kind of "filter" (e.g., a firewall). It is now equipped with a memory and is able to store the events. If it is possible, it releases the actions assuring that the required property P is verified. In this case, the enforcer modifies the general execution of the system. Output sequences of the enforcer have to be "correct" (sequence verifies property P) and "transparent" (correct input sequences are not modified).

On the application perspective it is worth mentioning that some industrial partners such as Microsoft and Google started to use runtime validation frameworks proposed by early research endeavors.

**Subject:**

A first attempt of runtime enforcement using timed automata has been proposed in [PFJMRN12]. In a general way, the objective of this PhD position is to extend runtime verification and enforcement in the context of timed systems and complete the picture of theoretical results.

Some questions still remain open. Which timed properties can be monitored / enforced? How the set of enforeable/monitorable properties evolves according to the architecture and under different enforcement primitives for the monitor? How can we synthesize an enforcement monitors from descriptive specifications. Intuitively, in runtime enforcement, one of the difficulties is that the operations of the enforcer influence the timings constraints of the initial behavior.

The main objective of this work is to provide a complete framework of monitoring / enforcement of timed systems, with several kinds of timed properties (safety, co-safety, and more expressive properties...) described in timed temporal logics and using several transparency rules. The implementability of this approach should also be investigated.

Theoretical results should be supported by a tool in order to demonstrate the effectiveness of the proposed approaches.

**Prerequisites:**

- Master in Computer Science.
- A first experience in the domain of formal methods is a strong asset.
References:


"Run-time enforcement of nonsafety policies".

"Enforcing Non-safety Security Policies with Program Monitors".
In ESORICS, pages 355-373, 2005.

[Fal09] Ylies Falcone
"Etude et mise en œuvre de techniques de validation à l'exécution"
Phd thesis, University of Grenoble 1, France

[JJ05] Claude Jard and Thierry Jeron.
"Tgv : theory, principles and algorithms".

"Off-line Test Selection with Test Purposes for Non-Deterministic Timed Automata".
In Proceedings of the 17th International Conference on Tools and Algorithms for the
Construction and Analysis of Systems (TACAS’11), Saarbrücken, Germany, April 2011. LNCS
6605, pages 96-111. Springer.

[NR11] O. Nguena-Timo and A. Rollet
Test Selection for Data-Flow Reactive Systems based on Observations
In 7th Workshop on Advances in Model Based Testing A-MOST 2011, March 21, 2011, Berlin,
Germany, 8p.

[NMR10] O. Nguena Timo and H. Marchand and A. Rollet
Automatic Test Generation for Data-Flow Reactive Systems with time constraints
In 22nd IFIP International Conference on Testing Software and Systems (ICTSS10), (ex
Testcom/Fates), November 8-12, 2010, Natal, Brazil, 6p. (short paper)

[FFM12] Y. Falcone, J-C. Fernandez, L. Mounier.
What can you Verify and Enforce at Runtime?
In STTT: Software Tools for Technology Transfer - Special issue on Runtime Verification.