PhD Proposal:
Verification of Large Scale Stochastic Systems, Application to Diagnosis and Opacity

Location : INRIA, Rennes (35), SUMO team

Topic : Information Technologies have provided us with amazing new services, that give us permanent access to all kinds of distant information and applications. Such systems are good examples of the new paradigms of systems that must be considered by computer scientists today: large collections of interconnected softwares, systems and devices, that interact to jointly deliver the expected services. This raises considerable issues both for engineers (design, control, maintenance, verification, security proof, protection, etc.) and for theoreticians, that must find new ways to deal with modularity and scalability issues. The general objective of this thesis is to contribute to the emergence of new formal models for such large systems, and to new algorithms to analyse and control them.

Several research directions are envisioned, taking for example the diagnosis problem as the guideline. The diagnosis problem can be simply stated as follows: some (known) system runs and produces a sequence of observations about its actions. An external observer must then determine whether some specific (fault) event occured or not in the system given the model of this system and the collected observations. Numerous variants of this simple question have been explored, and it can be considered as a basic step towards more elaborate inference problems. Recently, probabilistic settings have been examined, where the system performs random transitions, and the observer would like its detection probability to converge to one, when the fault actually occurred. The thesis will explore the definition of diagnosability degrees for such probabilistic systems.

The distributed or multi-agents aspects of the question will also be examined. When several components are interconnected, one would like to quantify the amount of constraints that each of then imposes to the free behaviors of the other. The question immediately translates into how much the diagnosability degree of a component is altered when this component is inserted into a larger system. Conversely, for input/output systems, one may consider quantifying the amount of information that can be extracted, or that leaks out of a specific component. This has natural connections with security aspects of system compositions. The relations of these problems with information theory will be explored.

A third research direction will explore abstraction techniques for large weighted/probabilistic automata. The objective there is to approximate a possibly large system by a smaller one. One should however lose few information, for example in term of language, or in term of property of interest. Different distances will be examined (again information theory could help). A possible usage could be to perform the diagnosis of a complex system on the basis of a simple approximation of this system, without losing too much in tems of accuracy of the diagnosis. The distributed/multi-agents aspects of this best approximation techniques will also be examined. Along with the design of such abstraction techniques, the thesis could also examine the interest of the dual approach, where instead of approximating the model, one rather uses approximate inference techniques on the exact large and complex model of the system.

The research directions mentioned above are illustrative. The specific topic will be adapted to the taste and skills of the candidate.

This thesis will be hosted by the SUMO team of INRIA Rennes, but will involve collaborations with several computer science labs in Paris.

Ideal profile : Master in computer science or mathematics, with a taste for formal methods and automata theory.

Contact : Eric Fabre, eric.fabre@inria.fr, +33 (0)2 99 84 73 26
http://people.rennes.inria.fr/Eric.Fabre/

Bibliography :

- David Thorsley, Demosthenis Teneketzis, "Diagnosability of Stochastic Discrete Event Systems," IEEE TRANSACTIONS ON AUTOMATIC CONTROL, VOL. 50, NO. 4, APRIL 2005
- Mario Alvim, "Formal approaches to information hiding: An analysis of interactive systems, statistical disclosure control, and refinement of specifications," PhD thesis, 2011.
- Loig Jezequel, Eric Fabre, "Turbo-planning,", WODES 2012.