Failure Diagnosis in Large Distributed System

(CS Master Thesis)

Subject : Many systems we use in everyday life are composed of many software, functions, components etc. that interact to deliver the service we expect from them. Think of telecommunication networks, plane ticket reservation systems, web services, systems on a chip, large plants, etc. Their size is such that it becomes impossible to consider them as a single large system, for matters like checking the integrity of the system, ensuring that nothing "bad" can happen, etc. It is therefore necessary to design distributed and scalable methods to analyze such distributed systems. While theories for modeling, monitoring and controling systems in a "centralized" setting are well developed, the field is much more open when one wants to address the same problems with distributed methods. Despite the urgent needs, little is known, and questions of intractability or undecidability arise very rapidly.

In this subject, we propose to address the diagnosability problem of distributed systems. These systems will be modeled as networks of automata. Diagnosing a distributed system consists in deciding whether a specific (hidden) event of interest did or didn't occur in a run of the system, given a set of observations collected during this run. The diagnosability property ensures that as soon as this event occurs, it will be possible to detect it by a bounded number of observations after its occurrence. It is therefore a very desirable property! Checking the diagnosability of a large system is intractable, because of the combinatorial explosion induced by the size of the system. The objective of this thesis is to propose a modular (or distributed) method, to address this problem, in order to make such large systems tractable.

The extension of this work into a PhD topic will be possible.

Keywords : system verification, networks of automata, distributed algorithms, formal methods, diagnosis

Contact : Eric Fabre, Eric.Fabre@irisa.fr, +33 (0)2 99 84 73 26
http://www.irisa.fr/distribcom/Personal_Pages/fabre/fabre.html

Diagnostic de panne pour les grands systemes distribues

(Stage de Master Informatique)

Sujet : Beaucoup des systemes que nous utilisons quotidiennement sont des systemes distribues, formes d'un assemblage d'elements, de logiciels, de fonctions, etc. qui interagissent pour nous rendre le service que nous attendons d'eux. Il suffit de penser par exemple a des reseaux de telecommunications, a des systemes de reservation de billets d'avion, a des services web, a des systemes sur puce, a de grandes usines, etc. La taille de tels systemes est parfois telle qu'il devient impossible de les considerer dans leur ensemble, comme un systeme unique, pour des questions comme s'assurer de l'integrite du systeme, prouver qu'aucun comportement dangereux n'est possible, etc. Il est par consequent necessaire de developper des methodes adequates, c'est a dire reparties et passant a l'echelle, afin d'analyser de tels systemes distribues. Alors que les theories pour la supervision et le controle centralises sont

bien etablies, les methodes reparties pour s'attaquer a ces problemes manquent encore, malgre leur urgente necessite. Peu de resulats sont connus, et des questions comme la complexite de calcul ou la non decidabilite apparaissent tres vite quand on passe en distribue.

Dans ce stage, on propose de s'interesser a la diagnosticabilite d'un systeme distribue. Ces systemes seront modelises par des reseaux d'automates. Diagnostiquer un systeme distribue consiste a decider si un evenement (cache) particulier s'est produit ou non dans une execution du systeme, au vu d'un ensemble d'observations collectees au cours de cette execution. La propriete de diagnosticabilite exprime que, a partir du moment ou cet evenement se produit, il suffit d'un nombre fini d'observations pour le detecter. C'est donc une propriete tres interessante du systeme! Tester la diagnosticabilite d'un systeme distribue est un probleme decidable, mais dont la complexite explose avec la taille du systeme. Il est donc important de concevoir des methodes modulaires/distribuees pour cela, operant a l'echelle d'un composant, afin d'exploiter la struture du systeme pour reduire la complexite du test.

Ce sujet pourra constituer un premier pas pour un travail de these.

Mots clés : verification de systeme, reseaux d'automates, algorithmique repartie, methodes formelles, diagnostic

Contact : Eric Fabre, Eric.Fabre@irisa.fr, +33 (0)2 99 84 73 26
http://www.irisa.fr/distribcom/Personal_Pages/fabre/fabre.html