Distributed Diagnosability Test in Large Distributed Systems

(CS Master Thesis)

Subject : We consider a possibly large distributed system, modeled as a network of automata. This type of models captures a vast family of applications, for example large distributed software, systems obtained by assembling components, like telecommunication networks, networks of embedded systems (cars, planes,...), choreographies of web services, and the like.The diagnosis problem can be stated as follows. One assumes that some actions of the system correspond to failures. Moreover, as the system evolves, it produces observable events that are collected in a distributed manner, by sensors located on the different components of the system. One wishes to determine whether a failure occured or not in the system, given a set of observations. The answer can be yes, no or maybe. A system is diagnosable whenever, after a failure, a finite number of observations allows one to detect the failure.

The objective of this master thesis is to design a distributed diagnosability test, that is by handling the system at the scale of components. Then, this construction will be used to derive a distributed diagnosis procedure, based on message exchanges between local supervisors. When the system is not diagnosables, strategies to recover this property will be studied. Finally, the approach will be extended to larger classes of systems, like networks of timed automata or of stochastic automata.

Keywords : networks of automata, distributed algorithms, formal methods, diagnosis, diagnosability

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 réparti dans les systèmes distribués

(Stage de Master Informatique)

Sujet : On considère un grand système réparti, modélisé sous forme d'un réseau d'automates. Ce genre de modèles permet de décrire une vaste palettes d'applications comme de grands logiciels répartis, des systèmes formés par assemblage de composants comme les réseaux de télécommunications, les réseaux de calculateurs embarqués (voitures, avions...), les orchestrations de services web, etc. Le problème du diagnostic dans de tels systèmes se pose de la manière suivante. On suppose que certaines actions du modèle correspondent a des défaillances. Par ailleurs, lorsque le système évolue, il produit un certain nombre d'événements observables, collectes de façon répartie. On souhaite alors déterminer si, au vu des observations, une défaillance s'est produite ou non. La réponse pouvant être positive, négative, ou incertaine. Un système est diagnosticable si, suite a une défaillance, celle-ci est détectée de façon certaine après un nombre fini d'observations.

L'objectif du stage est de mettre au point un test de diagnosticabilité réparti, c'est à dire manipulant le système à l'échelle de ses composants. Dans un second temps, on s'appuiera

sur cette construction pour en déduire une algorithmique répartie de diagnostic, procédant par échanges de messages entre les superviseurs de composants. Lorsque le système étudié n'est pas diagnosticable, on s'intéressera aux modifications permettant de retrouver cette propriété. Enfin on étendra le problème à une classe plus larges de modèles, par exemple au cas des automates temporisés ou des automates stochastiques.

Mots cles : reseaux d'automates, algorithmique repartie, methodes formelles, systemes concurrents, diagnostic, diagnosticabilite

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