Ecole Doctorale STIC

Sciences & Technologies de l'Information et de la Communication

ED STIC - Proposition de Sujets de Thèse

pour la campagne d'Allocation de thèses 2011

Titre du sujet :	Preuves de sureté des applications distribuées à grande échelle
Mention de thèse :	Informatique
HDR Directeur de thèse inscrit à l'ED STIC :	Baude Françoise

Co-encadrant de thèse éventuel :

Nom :	Madelaine
Prénom :	Eric
Email :	eric.madelaine@inria.fr
Téléphone :	0492387807

Email de contact pour ce sujet :	eric.madelaine@inria.fr
Laboratoire d'accueil :	I3S/INRIA

Description du sujet :

Le but de cette thèse est de modéliser les applications, mais aussi l'évolution des applications au cours de leur exécution, afin de garantir la sûreté de leur exécution.
Le travail portera sur plusieurs aspects complémentaires: la spécification des propriétés comportementales des services; la preuve, à l'aide d'outils de preuve interactifs, des propriétés génériques garanties par le middleware; puis la validation par model-checking des propriétés des applications.
Au final, les propriétés prouvées sur les applications portent à la fois sur leur logique propre et sur leurs interations avec les composants du middleware.

En composant des techniques de type theorem proving pour prouver des propriétés génériques d'une classe d'applications et des techniques de type model-checking pour explorer l'ensemble des états d'un service particulier, nous pourrons assurer la fiabilité de bout en bout de systèmes de grande taille. Pour atteindre ces objectifs, nous proposons de nous concentrer sur un modèle à

composants reconfigurables, le GCM [1].

Plus particulièrement les objectifs de cette thèse sont les suivants:
- étendre les modèles comportementaux proposés dans l'équipe pour les componsants distribués reconfigurables,
- contribuer à la génération de modèles comportementaux pour systèmes à composants,
- spécifier le modèle à composants et prouver des propriétés génériques sur la reconfiguration des composants (par exemple sur l'importance de l'ordonnancement des tâches de reconfiguration, ou sur l'entrelacement entre phases d'adaptation et phases d'exécution des services),
- utiliser les propriétés prouvées pour vérifier par model-checking le comportement correct d'applications largement distribuées. Les propriétés génériques servent à limiter l'explosion combinatoire de l'ensemble des états à explorer pour vérifier le comportement de l'application.

Ce travail est conséquent mais de nombreuses briques de base sont déjà présentes, comme le prouvent les travaux [2], [3], et [4]

Encadrants:
Francoise Baude et Eric Madelaine

Références:
[1] GCM: A Grid Extension to Fractal for Autonomous Distributed Components
Françoise Baude, Denis Caromel, Cédric Dalmasso, Marco Danelutto, Vladimir Getov, Ludovic Henrio and Christian Pérez
Annals of Telecommunications - Special Issue on Software Components - The Fractal Initiative, Springer, 2009
[2] Behavioural Models for Group Communications
Rabéa Ameur Boulifa, Ludovic Henrio, and Eric Madelaine,
WCSI-10: International Workshop on Component and Service Interoperability, 2010.
[3] A Framework for Reasoning on Component Composition
Ludovic Henrio, Florian Kammüller, and Muhammad Uzair Khan - FMCO 2009, Springer
[4] Behavioural Models for Distributed Fractal Components
Antonio Cansado, Ludovic Henrio, and Eric Madelaine
Annals of Telecommunications - Special Issue on Software Components - The Fractal Initiative, Springer, 2009

English version:

Title: Safety proofs for large scale distributed applications

Subject:
The objective of this thesis is to provide models for applications and their runtime evolution, to guarantee their safe execution.
The work will consist in several complementary aspects: specification of behavioural properties for services; the use of interactive theorem provers to prove generic properties on the

middleware; then the validation of the application properties using model-checking tools. Finally, properties proven on applications concern both their internal logic and the interactions with the middleware.

Composing theorem proving techniques to prove generic properties on a kind of applications, model-checking techniques to explore the reachable states of a given service, we will ensure reliability from end to end of large scale systems.
To reach those objectives, we will focus on a given adaptable component model: GCM[1].

More precisely the objectives of the thesis are the following:
- Extend existing behavioural models for reconfigurable component models
- contribute to the generation of behavioural models for component systems
- specify the component model, and prove generic properties on reconfiguration (eg concerning the ordering of reconfiguration and functional events)
- use the proven properties to verify, by model-checking techniques, the correct behaviours of large-scale distributed applications. Generic properties reduce the set of states to be explored to ensure the correct behaviour of the application.

The amount of work to fulfill these goals is consequent, but many basic blocks are already developed, as shown in [2], [3], and [4].

Directors:
Francoise Baude and Eric Madelaine

References:
[1] GCM: A Grid Extension to Fractal for Autonomous Distributed Components
Françoise Baude, Denis Caromel, Cédric Dalmasso, Marco Danelutto, Vladimir Getov, Ludovic Henrio and Christian Pérez
Annals of Telecommunications - Special Issue on Software Components - The Fractal Initiative, Springer, 2009
[2] Behavioural Models for Group Communications
Rabéa Ameur Boulifa, Ludovic Henrio, and Eric Madelaine,
WCSI-10: International Workshop on Component and Service Interoperability, 2010.
[3] A Framework for Reasoning on Component Composition
Ludovic Henrio, Florian Kammüller, and Muhammad Uzair Khan - FMCO 2009, Springer
[4] Behavioural Models for Distributed Fractal Components
Antonio Cansado, Ludovic Henrio, and Eric Madelaine
Annals of Telecommunications - Special Issue on Software Components - The Fractal Initiative, Springer, 2009