Projet ANR-06-SETI-015
RIMEL (Raffinement Incrémental de Modèles événementiELs)
Rapport intermédiaire semestriel décembre 2008

Coordonnateur Dominique Méry
LORIA,Université Henri Poincaré Nancy 1

Partenaire 2 Thierry Lecomte
ClearSy

Partenaire 3 Mohamed Mosbah
LABRI, Université Bordeaux I

Janvier 2009 à 6:13pm

Résumé

Ce document présente une synthèse des résultats obtenus par les partenaires du projet RIMEL au cours des six dernier mois ; il comprend un rappel des objectifs de ce projet et une analyse des tâches associées aux livrables. En particulier, une description plus détaillée a été apportée dans les rapports précédents ; les résultats obtenus sont principalement attestés par des publications, des archives de modèles B et des spécifications de logiciels en cours de développement, notamment BART qui est diffusé par la société ClearSy.

1 Introduction au projet

Le projet RIMEL (Raffinement Incrémental de Modèles événementiELs) concerne principalement le raffinement de modèles événementiels et la systématisation de cette technique dans le cadre d'applications ciblées notamment la conception d'algorithmes ou systèmes répartis. La systématisation de cette technique repose sur le développement de schémas conceptuels appelés *patrons de développement* s'appuyant sur une validation par la preuve (patrons de développement prouvés). Le développement du protocole IEEE 1394 a montré les limites du raffinement sur les aspects temps réel et probabilistes et conduit à rechercher à intégrer des extensions liées au traitement des aspects probabilistes et des contraintes éventuelles de temps. Le travail est organisé selon les directions scientifiques suivantes :

1. *Théorie du raffinement* : raffinement probabiliste, raffinement avec intégration de temps, prise en compte de contrainte de fatalité.
2. *Proof-based design patterns* : méthodologie d'ingénierie système formelle
3. *Self-Healing Systems et Algorithmes Répartis*
4. *Outils et diffusion*

Les motivations de ce projet concernent principalement l'intégration de la preuve mathématique dans le processus de développement de systèmes informatiques, pour en justifier la confiance. Deux domaines d'applications sont exploités pour inférer et valider les apports méthodologiques du raffinement.

Le projet comprend plusieurs étapes identifiées par des livrables et correspondant à des étapes du projet.

- **Deliverable 1 Development of distributed algorithms** [5] : le projet s'appuie sur des études de cas constituées principalement de problèmes de l'algorithmique répartie et l'objectif est de les développer en utilisant la technique du raffinement. Publication à T0+12.
- **Deliverable 2 Integration of timing constraints in an incremental proof-based development** [6] : l'objectif est de mieux comprendre l'introduction d'éléments temporels dans le cadre du raffinement; certains algorithmes répartis reposent sur des hypothèses temporelles et serviront d'études de cas. Publication à T0+18.

- **Deliverable 3 Proof-based design patterns** [7] : Le développement incrémental et prouvé de systèmes répartis posent des problèmes de preuves et certains développements peuvent être rejoués ou réutilisés ; la notion de patron reste à définir et à concrétiser dans le cadre du projet. Publication à T0+18.
- **Deliverable 4 Formal system engineering** : Il s'agit de considérer non seulement des systèmes comme des algorithmes mais aussi des systèmes au sens général et de considérer le développement incrémental et prouvé dans ce cadre. Publication à venir.
- **Deliverable 5 Probabilistic incremental proof-based development** : Il est aussi important de considérer les systèmes où une loi de probabilité intervient de manière explicite ou implicite. Publication à venir.
- **Deliverable 6 Tools** : Cette tâche s'échelonne tout au long de ce projet et vise à fournir des outils pour la méthode de développement. Publication à venir.

Chaque livrable correspond à une étape accomplie au cours du projet ; la première année a permis des échanges sur les techniques de vérification (Coq et B) et sur la modélisation des systèmes répartis (Event B). Dans la proposition initiale, les systèmes *self healing* sont visés et les études de cas ont été poursuivies dans le cadre de ce type de systèmes. Au-delà des systèmes répartis logiciels, nous sommes aussi intéressés par les systèmes répartis intégrant des aspects matériels ; le challenge de ce projet est de combiner plusieurs approches complémentaires visant des systèmes de type algorithmique et de type industriel ; ainsi, une méthodologie fondée sur le raffinement, la preuve et la représentation des systèmes répartis est au cœur de nos travaux et en constitue un des objectifs. La mise en évidence de patrons [7] devrait permettre de mieux expliquer cette méthodologie de développement et la rendre opérationnelle pour des utilisateurs moins experts. Rappelons que l'intérêt des systèmes algorithmiques est d'être maîtrisés par les partenaires académiques et que ces systèmes constituent un vivier très important d'études de cas non-triviales.

Nous allons revoir les actions du projet et nous allons commenter les résultats obtenus dans les derniers mois mais aussi préciser ce qui reste à faire dans les tâches mentionnées.

2 Actions du projet

Dans cette section, nous faisons un bilan intermédiaire de chaque action identifiée et en cours de réalisation ou terminée. Les réunions d'avancement nous ont permis d'échanger sur les techniques, modèles et outils utilisés par les différents groupes. Nous donnons une description des actions menées ou qui sont apparues au cours du dernier semestre.

2.1 Action Algorithmes répartis développés incrémentalement et prouvés

Cette action a permis aux membres du projet d'échanger sur les algorithmes répartis et sur les techniques de vérification et de conception incrémentale prouvée pour les systèmes événementiels. Cette action aboutit à un livrable qui a repris les études de cas développées selon la méthode incrémentale prouvée et qui va aussi situer cette approche par rapport à l'approche suivie par le partenaire LABRI. Il est clair que le partenaire LABRI s'appuie sur une vérification *a posteriori* des algorithmes répartis et que cette vérification n'est pas encore effective sur le plan des outils de preuve ; l'assistant de preuve utilisé est Coq et une partie du travail de ce partenaire est de développer des bibliothèques de théories liées aux graphes et aux algorithmes répartis étudiés. Cependant, l'intérêt de la collaboration réside dans les échanges portant sur les algorithmes répartis et la description des principes de ces algorithmes. Ainsi, les échanges entre le partenaire LORIA et le partenaire LABRI ont permis de modéliser des algorithmes réputés non-triviaux dans un temps raisonnable. Au cours de notre exposé devant la commission d'évaluation, nous avons été interpellés sur les algorithmes de consensus et la question de les traiter a été posée par cette commission. D'une part nous avons des relations régulières avec L. Lamport sur ce type d'algorithme et d'autre part, il ne constitue pas un objectif en soi du projet initialement. Ce n'est pas le cas des algorithmes autostabilisants qui sont très complexes à vérifier et sont donc de vrais challenges pour leur conception incrémentale. Nous avons limité le livrable 1 [5] à quelques études de cas qui nous ont permis de comprendre le savoir-faire des uns et des autres au niveau des algorithmes répartis; la liste a été arrêtée en janvier 2008 mais les développements se sont poursuivis sur d'autres exmples. Si le partenaire LORIA reste plus familier avec le développement incrémental, il est assez clair que la comparaison des approches notamment avec des outils comme VISIDIA [**?**] est prometteuse. Les deux partenaires de cette tâche ont poursuivi le dévelopement d'études de cas [9] et échangent des expériences pédagogiques en lien avec les cours donnés en master à Nancy et à Bordeaux. Cet échange est important pour étudier le lien entre le plateforme RODIN et l'environnement VISIDIA. Notons que le LABRI et le LORIA ont poursuivi cet exercice de développement d'algorithmes répartis en lien avec la tâche des outils, notamment l'intégration de B et VISIDIA. Le bilan contractuel de cette action est consigné dans le livrable 1 [5].

Perspectives : Cette action a conduit au livrable [5] **Development of distributed algorithms** ; il présente une collection d'études de cas, afin de mieux comprendre les algorithmes répartis et leur conception mais aussi de dégager des patrons liés à ces

algorithmes. Le travail de développement d'études de cas se poursuit en lien avec le partenaire LABRI. L'idée est d'échanger ces études de cas, afin de produire une description d'algorithmes répartis pour les étudiants de nos universités. Il s'agit aussi de développer des patrons ad hoc., notamment pour prendre en compte les notions de probabilités. Nous pensons aussi poursuivre les développments d'algorithmes cryptologiques [8], puisque nous avons acquis un certain succès dans cette voie; ces développements ont montré aussi les limites du prouveur.

2.2 Action Intégration du temps dans le raffinement

Le temps joue un rôle fondamental dans de nmbreux algorithmes répartis et nous étudions dans cette action l'introduction du temps au cours du développement incrémental. Des résultats préliminaires ont été donnés et publiés [14, 15] et nous avons publié des éléments étendant le modèle Event B avec des contraintes temps réel. Cette étude a mis en avant quelques patrons pour concevoir des modèles intégrant des aspects temps réel. Ainsi, la notion d'agenda a été mis en avant dans une telle démarche de modélisation. Nous avons aussi noté l'utilisation des patrons proposés dans cette tâche dans le projet TACOS, tout particulièrement l'équipe DEDALE de notre laboratoiree; cela poermet ainsi de montrer la généralité des patrons développés.

Perspectives : Cette action se focalise sur le temps dans les systèmes répartis mais au travers du raffinement et il convient de développer des solutions réparties en prenant soin de comprendre comment des patrons de développement peuvent aider dans cette démarche. Un livrable [6] a fait le point sur les éléments apportés et un article de revue [15]; ce document est accepté pour publication. Son encadrant est Dominique Cansell qui supervise ses travaux mais qui ne publie pas.

2.3 Action Ingénierie système formelle

Cette action est aussi fondée sur le développement d'études de cas mais ces études de cas sont liées à des systèmes s'appuyant sur des éléments algorithmiques ou logiciels. Nous avons plusieurs résultats intermédiaires :

- le développement de systèmes de vote électronique et leur analyse
- l'étude du contrôle d'accès dans le cadre du raffinement
- l'étude de patrons de développement
- le développement de programmes séquentiels structurés [12] a mis en évidence un patron de développement que nous sommes en train de mettre en œuvre dans la la plateforme RODIN

Ces travaux ont abouti à la mise en évidence de patrons de conception prouvés et ces premiers patrons sont décrits dans le livrable 3 [7]. L'idée est de clarifier la notion de patron dans le cadre du développement incrémental prouvé de systèmes. Nous considérons que ce point est assez central dans notre projet dans la mesure où il s'agit d'apporter une aide aux utilisateurs dans le développement incrémental prouvé. Dans cette action, nous avons utilisé les modèles d'attaques pour intégrer cet aspect dans le développement d'algorithmes cryptoloogiques et nous avons ainsi identifié un patron permettant de fusionner deux développements; cette technique a été utilisée dans le cas du modèle de Dolev et Yao et des algorithmes de transaction dont le Mondex avec cryptologie.

Perspectives Cette action se poursuit avec notammant les algorithmes répartis qui devraient fournir des patrons propres à leur développement. Les protocoles cryptographiques constituent des algorithmes répartis et sont intégrés au livrable 3 mais il convient d'exploiter les algorithmes plus complexes à comprendre comme ceux liés à l'autostabilisation. Une étude d'un système va démarrer prochainement et apportera aussi des éléments sur l'ingénierie système formelle, notamment dans le cadre d'un projet associant le partenaire LORIA et des partenaires industriels comme EDF. Un nouveau doctorant a débuté une thèse sur ce sujet en considérant la modélisation d'un système complexe du Grand Challenge, le pacemaker. Ce travail devrait aussi permettre à notre partenaire industriel d'intégrer des transformations ou des règles dans son outil BART, en travaillant de concert avec le LORIA.

2.4 Action Outils

Cette action vise à réaliser des outils dans le cadre du développement prouvé ; elle aura sans doute comme support principal la plateforme RODIN qui supporte la notation Event B et qui est ouverte au développement d'applications dans le cadre de l'atelier ECLIPSE. Cependant, notre partenaire industriel a fait un effort de développement de la version 4.0 de l'Atelier B et cette outil n'intègre pas la même syntaxe que celle de RODIN; nous veillerons donc à être aussi cohérent que possible avec les deux plate-formes. Trois outils sont donc en cours de réalisation :

- le développement d'un outil de raffinement automatique par la société ClearSy : il s'agit de BART; cet outil doit encore être validé par une société partenaire de ClearSy. Nous pourrons sans doute y intégrer certains patrons mais cela devrait être analysé prochainement.

- l'intégration de VISIDIA dans le cadre de la notation Event B et de RODIN: un ingénieur a visité le partenaire LORIA pour acquérir les compétences nécessaires en B et poursuit son travail de mise en œuvre du traducteur; cependant, cet ingénieur a quitté le LABRI et a été remplacé par un nouveau doctorant qui va visiter le LORIA pour poursuivre le développement de B2VISIDIA.
- le développement d'une application dans RODIN : un stagiaire tunisien Internship INRIA a mis en œuvre le patron des programmes séquentiels structurés. Cependant, ce plugin n'est pas encore diffusable et doit être généralisé. Cela signifie qu'un développement logiciel est encore nécessaire.

Perspectives Cette action enrichira les applications disponibles sur la plate-forme RODIN notamment et VISIDIA. Il en va de même pour l'outil de raffinement automatique BART.

3 Evolution du projet

Les activités du projet se poursuivent par le démarrage de l'étude des aspects probabilistes des systèmes notamment des algorithmes répartis. Cette étude nécessitera de considérer les travaux de Carroll Morgan sur le raffinement probabilistes. Nous avons noté aussi que l'activité de développement et de redéveloppement est très importante et il est important de faire une place dans notre échéancier pour ces études de cas. Le livrable 4 apportera des éléments sur les systèmes autostabilisants du point de vue algorithmique. D'une certaine mesure, le livrable 3 ne clôt pas les travaux sur les patrons mais constitue un embryon qu'il conviendra d'enrichir et de fonder sur le plan sémantique. On peut ainsi résumer la poursuite du travail comme suit:

1. Poursuivre les travaux sur les aspects temps réel notamment par la question des synchroniseurs.
2. Enrichir les patrons de développement notamment pour les algorithmes répartis
3. Etudes de cas pour les Self-Healing Systems et Algorithmes Répartis
4. Mettre en œuvre le raffinement en intégrant des aspects probabilistes.
5. Outillage:
   - BART: développement de règles en lien avec les patrons de développement
   - B2VISIDIA: application intégrant à la fois les modèles Event B et les modèles Visidia
   - Bibliothèque Coq pour les graphes
   - Finalisation de l'outillage du patron pre/post
6. Diffusion: cours d'algorithmique répartie

References

[1] Monia Loulou Ahmed Hadj Kacem Mohamed Mosbah and Mohamed Jmaiel. A formal security framework for mobile agent systems: Specification and verification. In *Third International Conference on Risks ans Security of Internet and Systems (CRiSIS)*, pages 69–76. IEEE, 2008.

[2] M. A. Haddar Ahmed Hadj Kacem Yves Métivier Mohamed Mosbah Mohamed Jmaiel. Proving distributed algorithms for mobile agents: Examplesof spanning tree computation in anonymous networks. In *ICDCN*, volume 4904 of *Lecture Notes in Computer Science*, pages 286–291. Springer, 2008.

[3] Mohamed Mosbah Annegret Habel. Workshop on graph computation models. In *ICGT*, volume 5214 of *Lecture Notes in Computer Science*, pages 460–462. Springer, 2008.

[4] Bilel Derbel Mohamed Mosbah Stefan Gruner. Mobile agents implementing local computations in graphs. In *ICGT*, volume 5214 of *Lecture Notes in Computer Science*, pages 99–114. Springer, 2008.

[5] Projet ANR-RIMEL. Développement d'algorithmes répartis. Livrable rimel, LORIA, Janvier/Février 2008.

[6] Projet ANR-RIMEL. Intégration du temps dans le développement incrémental prouvé. Livrable rimel, LORIA, Juillet 2008.

[7] Projet ANR-RIMEL. Proof-based design patterns. Livrable rimel, LORIA, Juillet 2008.

[8] Nazim Benaissa. Modelling attacker's knowledge for cascade cryptographic protocols. In *ABZ2008*. Springer, 2008.

[9] Dominique Cansell. Développement incrémental et preuve de l'algorithme de Dijkstra d'autostabilisation. Rimel, LORIA, July 2008.

[10] ClearSy. Bart. www.clearsy.com, 2008.

[11] Dominique Méry. A simple refinement-based method for constructing algorithms. In J. Davies, J. Gibbons, M. Hinchey, and K. Taguchi, editors, *First International Workshop on Formal Methods Education and Training*, Report GRACE-TR-2008-03. GRACE Center, National Institute of Informatics,, 2008.

[12] Dominique Méry. Teaching programming methodology using event b. In *Conference The B Method: from Research to Teaching*, Nantes, 2008.

[13] Joris Rehm. A duration pattern for event-b method. In *2nd Junior Researcher Workshop on Real-Time Computing - JRWRTC 2008*, France Rennes, 2008.

[14] Joris Rehm. From absolute-timer to relative-countdown: Patterns for model-checking. Technical report, LORIA, 2008.

[15] Joris Rehm. Proved Development of the Real-Time Properties of the IEEE 1394 Root Contention Protocol with the Event B Method. Technical report, LORIA, 2008. Submited and under revision to STTT-Special Event ISOLA 2007.