Composition et raffinement de systèmes sûrs

Mamoun Filali

SVF-FéRIA

PaRISTIC - ACI Sécurité Informatique
21-23 novembre 2005
Bordeaux

Plan

Plan

Plan

Plan

Introduction

Participants:

- ARLES-INRIA: Valérie Issarny.
- COMPOSE-INRIA: Charles Consel.
- OBASCO-EMN: Gilles Muller.
- DIKU: Julia Lawall.
- MOSEL-LORIA: Dominique Méry.
- SVF-FéRIA: Mamoun Filali.

Etudes:

But: Coopération équipes système et équipes méthodes formelles.

- Ordonnancement: DIKU, OBASCO, FéRIA, MOSEL.
  - Bossa,
  - VHDL.
- Protocoles de groupes: ARLES, FéRIA, MOSEL.
  - modèle synchrone.
  - modèle asynchrone.
- Téléphonie: COMPOSE, FéRIA.
  - SPL/SIP.

Le DSL Bossa

- Langage de spécification pour décrire l'ordonnancement d'un système.
- Langage d'implantation de politiques d'ordonnancement.
- Environnement de développement d'ordonnanceurs.

Descriptions Bossa

- Spécification:
  - interaction noyau-ordonnanceur: **events**, **state classes**.
  - interaction environnement-ordonnanceur: **interrupts**,
  - contexte d'interaction: **automaton**.
- Implantation: **handlers, process states**.

Etude Bossa

- Expression de la méthodologie de développement Bossa.
- Expression des vérifications Bossa.
- Automatisation des preuves de propriétés Bossa.

Outline

La méthodologie Bossa en B

Méthode:

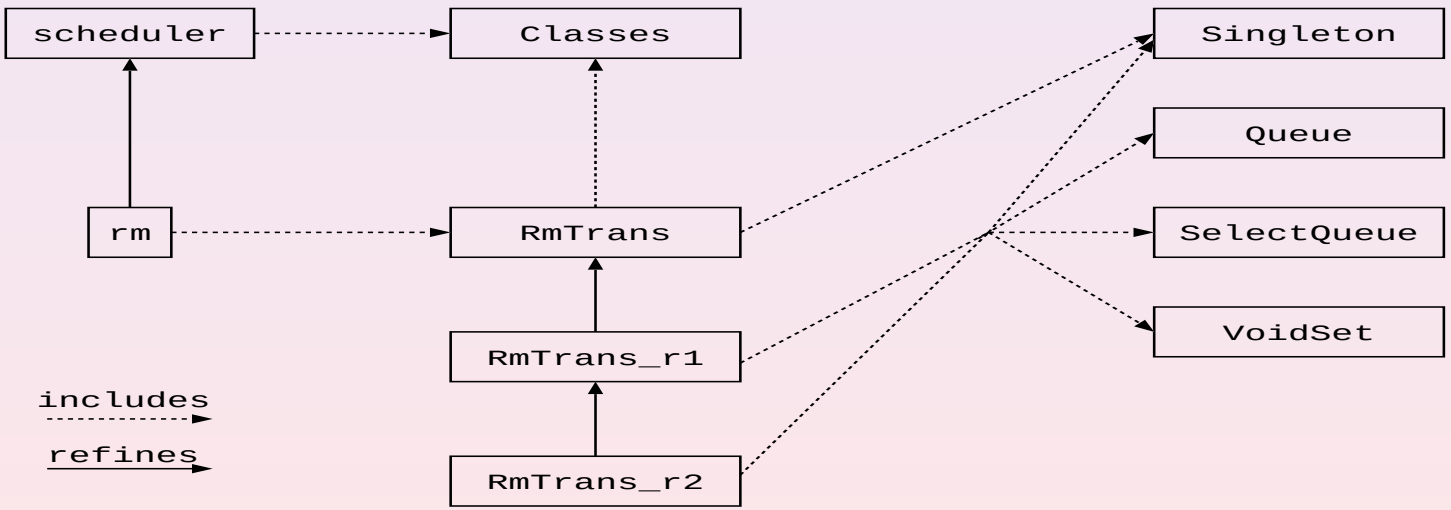
- machine B associée aux types d'événements: ordonnanceur abstrait.
- Raffinements B associés aux implantations de politiques d'ordonnancement.

$\rightsquigarrow$ Vérification des propriétés statiques des politiques d'ordonnancement.

- Vérification de propriétés sur les états (au sens Bossa), e.g. états `Singleton`.
- Vérification de pré-post conditions sur les événements.

Outline

Architecture des machines B



Les machines B

MACHINE Classes
SETS Process
VARIABLES
Running, Ready, Blocked, Terminated, running
INVARIANT
Running ⊆ Process
& Ready ⊆ Process
& Blocked ⊆ Process
& Terminated ⊆ Process
& running ∈ Process
& Running ∩ Ready = ∅
& Running ∩ Terminated = ∅
& Running ∩ Blocked = ∅
& Ready ∩ Terminated = ∅
& Ready ∩ Blocked = ∅
& Terminated ∩ Blocked = ∅

Outline

Automatisation des preuves Bossa

- Expression en WS1S d'obligations de preuve:
  - invariance,
  - raffinement.
- Expression et validation d'abstraction en WS1S.

Outline

Conclusion (I)

Etude en deux étapes:

- étape 1: spécification et développement.
  - Expression de la méthodologie Bossa et des propriétés Bossa en B.
  - Preuves laborieuses.
- étape 2: automatisation des preuves.
  - Meilleure couverture des propriétés Bossa.
  - model checking, techniques d'abstraction, logique décidable (WS1S).

Conclusion (II)

Expérience Bossa:

- raffinement, abstraction techniques de base utilisées par le DSL Bossa.
- Réutilisation de B pour l'expression du raffinement.
- Expression de propriétés de bases de l'ordonnancement à l'aide de WS1S.
- Réutilisation de Dixit, FMona pour l'expression de l'abstraction et de techniques de vérification.

Futur:

- Spécification et preuve de propriétés du niveau applicatif.
- Code annoté par la preuve.

Protocoles de groupes

Buts:

- coordinnation multi-agents,
- tolérance aux fautes.

Contextes d'étude : Réseaux ad hoc ($\neq$ WAN)

- A tout moment un site peut rejoindre ou quitter le système,
- problème d'échelle,
- communication par diffusion,
- problèmes d'autonomie.

$\Rightarrow$ nouveaux protocoles de groupes pour les réseaux ad hoc.

Point de départ: protocole de l'équipe ARLES.

Outline

Notion de clique:

Le protocole construit une **vue** pour chaque site. Les sites d'un groupe ont une même vue.

- communication robuste,
- partitionnement : chaque processus appartient à exactement un groupe.

Clique:

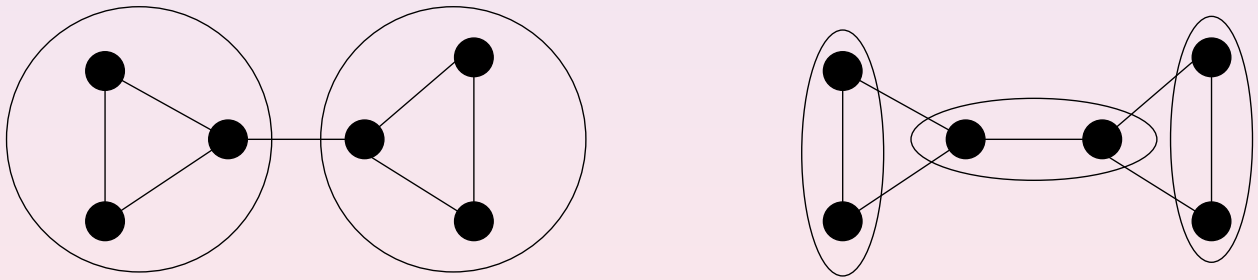
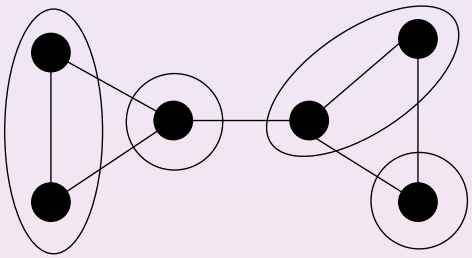


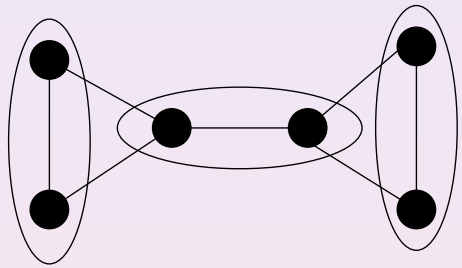
Figure: Partition de cliques

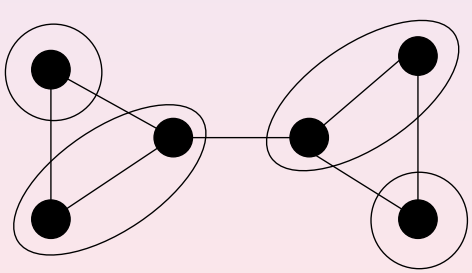
Cliques maximales

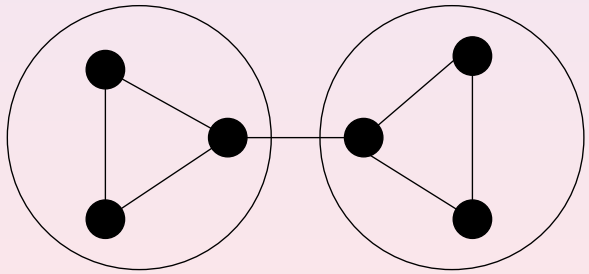
Critère de maximalité: deux cliques ne peuvent être fusionnées pour constituer une nouvelle clique.



Non maximal partitions







Maximal partitions

Outline

Vues

$$Graph \subseteq Node \times Node$$
$$\forall p \in Node : \langle p, p \rangle \in Graph$$
$$\forall p, q \in Node : \langle p, q \rangle \in Graph \Rightarrow \langle q, p \rangle \in Graph$$
$$View \in [Node \rightarrow \text{SUBSET } Node]$$

View specification

$\Box \forall p \in Node : View[p] \neq \emptyset \Rightarrow p \in View[p]$
$\Box \forall p \in Node : View[p] \times View[p] \subseteq Graph$
$\Box \forall p, q \in Node : (View[p] = View[q]) \vee (View[p] \cap View[q] = \emptyset)$
$\Box \forall p, q \in Node : View[p] \neq \emptyset \wedge View[q] \neq \emptyset \Rightarrow$
$(View[p] \times View[q] \subseteq Graph) \Rightarrow View[p] = View[q]$
$\text{TRUE} \rightsquigarrow \forall p : View[p] \neq \emptyset$

Outline

Protocole

Comportement de base:

- comportement périodique: à partir d'un état *singleton*, un site exécute des étapes successives bornées par un délai avant d'atteindre l'état final *grouped*. Après un laps de temps, il repasse dans l'état *singleton*.
- La durée de vie d'un groupe est beaucoup plus importante que celle de la constitution d'un groupe.

Etats de bases du protocole

idée de base: un noeud doit connaître son voisinage à distance 2.

- Singleton: un noeud est seul.
- Discovering: connaissance des voisins.
- Publishing: connaissance des voisins à distance 2.
- Expecting: construction d'une vue.
- Grouped: le noeud a une vue.

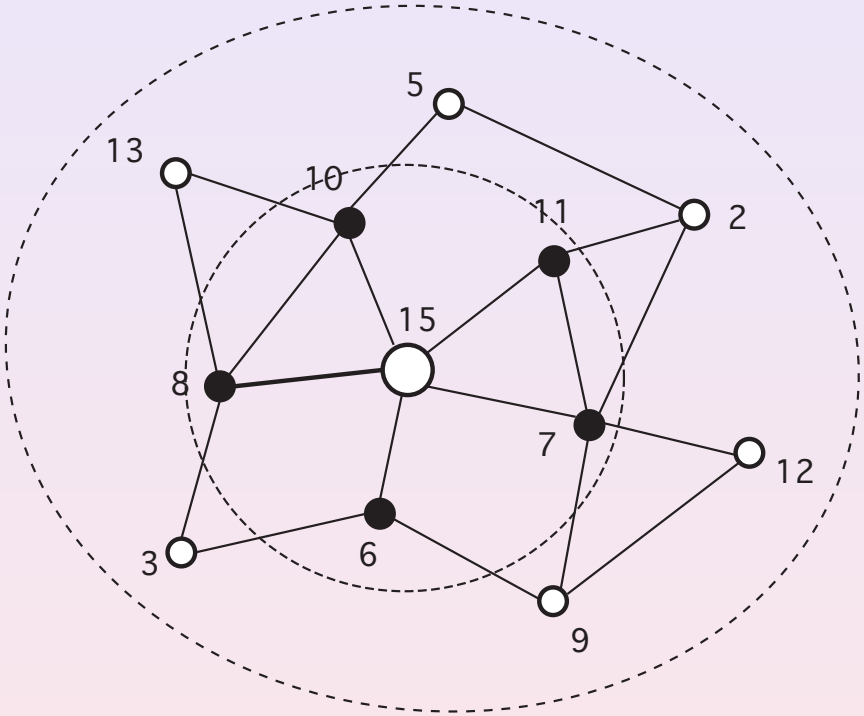


Figure: Construction de voisinage

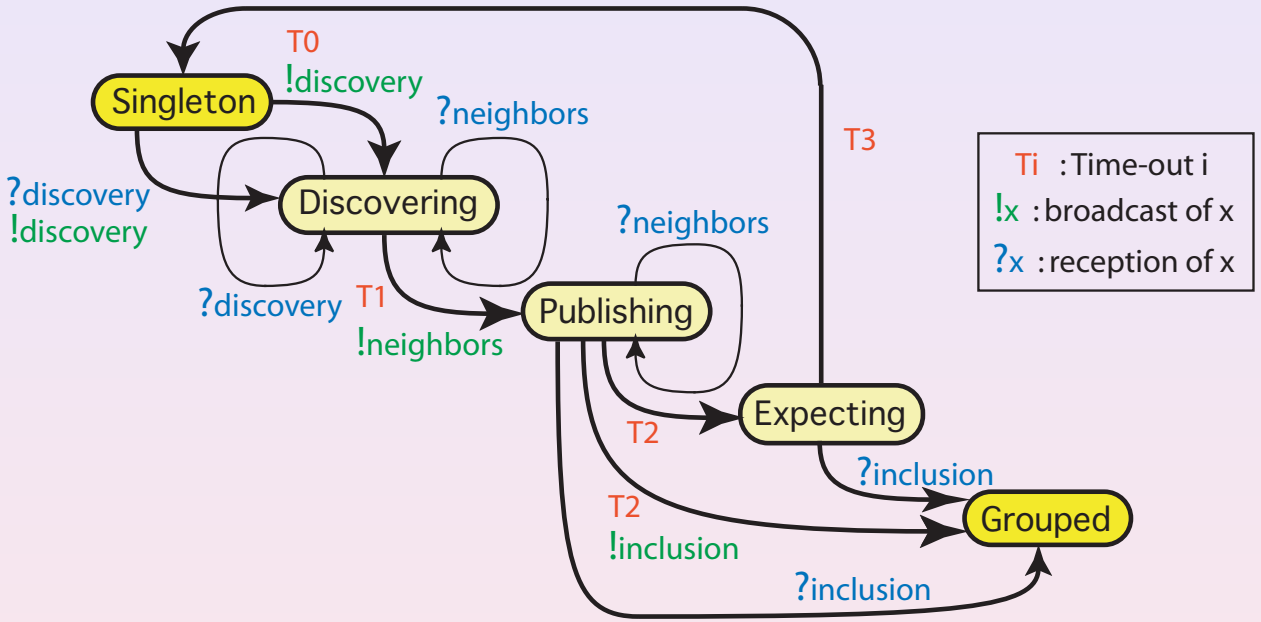


Figure: transitions du protocole de construction de vues

Outline

Validation du protocole

Développements du protocole

- communication asynchrone
- communication synchrone: diffusion instantanée.

Outline

Conclusion

- Spécification d'un protocole de groupe pour réseau ad hoc avec un critère de maximalité.
- Expression en TLA, validation en TLC (model checker de TLA+).
- Comparaison avec d'autres protocoles pour réseaux ad hoc (Issarny et al., Agha et al.).

Travail en cours: validation par raffinement du protocole.

Conclusion

Expérience

- Utilisation *conjointe* des DSL et des méthodes formelles.
- Expression dans une logique décidable de propriétés de modèles d'ordonnancement.
- Spécification des propriétes de construction de groupes dans les réseaux ad hoc.
- Protocole de construction de groupes dans les réseaux ad hoc.

Perspectives:

- Développement de services de téléphonie.
- Génération de code certifié.
- Meilleure prise en compte des hypothèses sur l'environnement.