HAUT COMMISSARIAT A LA RECHERCHE

THESE

Presentee au _____

CENTRE DE DEVELOPPEMENT DES TECHNOLOGIES AVANCEES

en vue de l'obtention

du GRADE de MAGISTER en CYBERNETIQUE

Option : **ARCHITECTURE des SYSTEMES**

**Reseaux de petri et logique
temporelle pour la verification
des systemes repartis**

Par :

Mr. Fawzi GUERROUMI

Soutenue le 14 Octobre 1990, devant le jury compose de :

MM. C. BENMEHREZ President
B. BOUZOUIA Examineur
A. MADDI Examineur
H. BESSALAH Rapporteur
M. BENHAMMADI Invite

RESUME

La répartition et le partage du travail d'une communauté d'utilisateurs d'un système informatique sont obtenus en couplant des systèmes relativement autonomes autour de réseaux. On obtient ainsi des architectures faiblement couplées ou **systèmes distribués**. Notre travail porte sur la vérification de tels systèmes informatiques. Une technique consiste à comparer une **entité opérationnelle**, dont l'évolution est observable, avec une **entité de référence** qui sert d'oracle sur le comportement attendu. L'approche proposée utilise les **réseaux de Pétri** pour décrire l'entité opérationnelle, et une **logique temporelle arborescente** pour décrire l'entité de référence. Un prototype de vérification assistée basé sur ces deux représentations a été développé dans un environnement PROLOG. Ce prototype a été utilisé pour l'analyse de trois applications: un algorithme distribué d'exclusion mutuelle, un protocole d'ouverture-fermeture de connexion(N) dans l'architecture en couches ISO pour l'interconnexion de systèmes ouverts, la phase transfert de données d'un protocole transport de classe 2.

ABSTRACT

This thesis deals with verification techniques of **distributed computer systems**. The purpose is to compare an **operationnal entity** with respect to **specifications**. The proposed approach consists in checking the behavior of a **Petri net** with respect to **branching time temporal logic** assertions. A PROLOG environment prototype is developed to manipulate both representations. Three applications (a distributed algorithm for mutual exclusion, a connection-disconnection protocol in the ISO layered architecture for the interconnection of open distributed systems, data transfer phase in a transport protocol) are analysed by using this prototype.

REMERCIEMENTS

RESUME

INTRODUCTION

CHAPITRE 1 : UN ENVIRONNEMENT LOGICIEL POUR LA CONCEPTION DE SYSTEMES DISTRIBUES HETEROGENES

I.1	INTRODUCTION.....	1
I.2	LE PROJET SEDOS.....	2
I.2.1	Objectifs et intérêts.....	2
I.2.2	Description du projet.....	4
I.2.2.1	Vérification.....	4
I.2.2.2	Techniques de description formelle....	6
I.3	VERS UN ENVIRONNEMENT DE PROTOTYPAGE RAPIDE ET VALIDATION DE PROTOCOLES.....	7
I.3.1	L'environnement PIPN.....	8
I.3.2	Spécifier.....	8
I.3.2.1	Description.....	8
I.3.2.2	Mise en oeuvre.....	9
I.3.3	Analyser.....	10
I.3.4	Prototype logiciel (noyau).....	12
I.3.5	Critiques.....	14

CHAPITRE 2 : MODELE OPERATIONNEL: LE LANGAGE RESEAU DE PREDICATS ET SON INTERPRETATION

II.1	INTRODUCTION.....	16
II.2	QUELQUES MOTS SUR LES RESEAUX DE PETRI.....	18
II.2.1	Définitions formelles.....	19
II.2.2	Franchissement de transition.....	20
II.3	RESEAUX DE PREDICATS.....	21

II.3.1	Définition du réseau de prédicats.....	21
II.3.2	Définition du langage réseau de prédicats...	24
II.3.3	Codage PROLOG d'une transition.....	26
II.4	QUELQUES EXEMPLES SIMPLES D'APPLICATION.....	28
II.4.1	Exemple 1: envoi d'un message.....	28
II.4.2	Exemple 2: exclusion mutuelle.....	30
II.5	INTERPRETATION PROLOG D'UN RESEAU DE PREDICATS	33
II.5.1	La base des faits exprimant un réseau de predi- cats.....	33
II.5.2	Interprétation de la règle de tir et dynamique d'un réseau de prédicats.....	35
II.6	CONCLUSION.....	39

**CHAPITRE 3 : DEFINITION D'UN NOYAU D'INTERPRETATION DE LA LOGIQUE
CONDITIONNELLE DU TEMPS ARBORESCENT CTL**

III.1	INTRODUCTION.....	42
III.2	LA LOGIQUE CONDITIONNELLE DU TEMPS ARBORESCENT	44
III.2.1	Définition des opérateurs temporels.....	44
III.2.2	Sémantique.....	46
III.3	INTERPRETATION PROLOG DE LA LOGIQUE CTL.....	47
III.3.1	Opérateurs de base PRE et PRETILDA.....	48
III.3.2	Interprétation PROLOG des opérateurs tempo- rels.....	49
III.3.2.1	Interprétation de l'opérateur POT.....	50
III.3.2.2	Interprétation de l'opérateur ALL.....	53
III.3.2.3	Interprétations des opérateurs INEV et SOME.....	56
III.3.2.4	Quelques simplifications.....	57
III.3.2.5	Opérateurs non temporels.....	58

III.4	OPERATEURS TEMPORELS DANS LE PASSE.....	59
III.4.1	Définition des nouveaux opérateurs.....	60
III.4.2	Interprétation PROLOG des opérateurs dans le passé.....	61
III.4.2.1	Interprétation de l'opérateur POT_PASSE.....	63
III.4.2.2	Interprétation de l'opérateur ALL_PASSE.....	63
III.4.2.3	Interprétation de l'opérateur SOME_PASSE.....	64
III.4.2.4	Interprétation de l'opérateur INEV_PASSE.....	64
III.4.2.5	Simplifications.....	65
III.5	EXEMPLES D'APPLICATION.....	65
III.5.1	Expression d'une propriété invariante.....	66
III.5.2	Un algorithme simple d'exclusion mutuelle entre deux sites.....	67
III.5.3	Atteignabilité inévitable.....	70
III.5.4	Absence de blocage, vivacité.....	71
III.6	CONCLUSION.....	72

CHAPITRE 4 : APPLICATIONS

IV.1	INTRODUCTION.....	75
IV.2	ALGORITHME D'EXCLUSION MUTUELLE.....	78
IV.2.1	Exécution symbolique.....	78
IV.2.1.1	La relation d'équivalence.....	79
IV.2.1.2	Interprétation PROLOG de la relation d'équivalence.....	80
IV.2.2	Spécification informelle.....	81
IV.2.3	Description formelle.....	82
IV.2.4	Expression des propriétés en logique CTL....	86
IV.3	COUPLE SERVICE-PROTOCOLE D'OUVERTURE-FERMETURE (NORME ISO).....	92

IV.3.1	Spécification informelle.....	93
IV.3.2	Description formelle.....	95
IV.3.3	Expression et vérification des propriétés en logique CTL.....	101
IV.4	PROTOCOLE DE TRANSPORT: LA PHASE DE TRANSFERT DE DONNEES.....	110
IV.4.1	Spécification informelle du protocole.....	112
IV.4.1.1	Le service transport: phase trans- fert de données.....	112
IV.4.1.2	Description du protocole.....	113
IV.4.2	Spécification du protocole par réseaux prédicats-transitions.....	117
IV.4.2.1	Modèle émetteur.....	117
IV.4.2.2	Modèle récepteur.....	120
IV.4.3	Vérification du modèle global.....	121
CONCLUSION		123

ANNEXE A: REALISATION DE L'OUTIL PIPN

A.1	INTRODUCTION: PRESENTATION DE L'OUTIL
A.2	LA SIMULATION DU FONCTIONNEMENT D'UN RESEAU DE PREDICATS
A.2.1	L'utilité de la simulation
A.2.2	Fonctionnement du simulateur
A.3	LA GENERATION DE L'AUTOMATE A ETATS FINIS
A.3.1	Méthodes de génération
A.3.2	L'automate généré
A.4	L'ENVIRONNEMENT DE VERIFICATION
A.4.1	Formulation d'une spécification
A.4.2	Opérateurs temporels exprimant l'accessibilité de transitions
A.4.2.1	Potentialité d'un ensemble de transi-

tions

A.4.2.1.1 Opérateurs préliminaires

A.4.2.1.2 Interprétation PROLOG de
de l'opérateur POTT

A.4.2.2 Inévitabilité d'un ensemble de transi-
tions

A.4.2.2.1 Opérateurs préliminaires

A.4.2.2.2 Interprétation PROLOG de
de l'opérateur INEVT

A.4.2.2.3 Simplification

ANNEXE B: L'ALGORITHME D'EXCLUSION MUTUELLE DE RICART AGRAWALA

B.1 PRINCIPE

B.2 L'ALGORITHME

ANNEXE C: FORME INTERNE DE L'AUTOMATE

ANNEXE D: SYNTAXE DU LANGAGE RESEAU DE PREDICATS

BIBLIOGRAPHIE