Epistemic modelling and protocol dynamics

Wang, Y.

Citation for published version (APA):
Contents

Acknowledgments xi

1 Introduction 1
  1.1 Background ................................................. 2
  1.2 Overview of the Dissertation ............................ 6
  1.3 Origins of the Material .................................. 8

2 Preliminaries 9
  2.1 Finite Automata and Regular Expressions ................. 9
  2.2 Kripke Models and Bisimulation .......................... 10
  2.3 Three Logics .................................................
      2.3.1 Propositional Dynamic Logic ..................... 13
      2.3.2 Epistemic Temporal Logic ......................... 15
      2.3.3 Dynamic Epistemic Logic ......................... 15

I Logics of Epistemic Protocols 19

3 Meta-knowledge Matters 21
  3.1 Introduction ................................................. 21
  3.2 Preliminaries ................................................. 22
  3.3 Announcement Protocol and Verification ................. 24
  3.4 Deterministic Protocols for RCP_{3,1} .................... 29
  3.5 Conclusion and Discussion ................................ 34

4 Logics of Knowledge and Protocol Change 37
  4.1 Introduction ................................................. 37
  4.2 Basic Logic PDL ............................................ 39
  4.3 Public Event Logic PDL^∞ ................................ 43
  4.4 Update Logic PDL^∞ ....................................... 49
  4.5 Conclusion and Future Work ............................... 55
IV Modelling Security Protocols

9 Epistemic Approaches to Security Protocol Verification 139
  9.1 Knowledge in Security Protocols 139
    9.1.1 Different Aspects of Knowledge 140
    9.1.2 Tension Between Epistemic and Temporal Structure 141
  9.2 Epistemic Approaches: A Brief Survey 142
    9.2.1 BAN logic 142
    9.2.2 Basics of Epistemic Approaches 144
    9.2.3 Epistemic Temporal Approaches 146
    9.2.4 Dynamic Epistemic Logic Approaches 148
    9.2.5 Tools 149
  9.3 Comparisons 149
    9.3.1 On Equivalences 149
    9.3.2 ETL vs. DEL in Modelling 151
  9.4 To Know or Not, Towards a Technical Answer 155
    9.4.1 On Expressivity of ETL 155
    9.4.2 Model Checking ETL 157
  9.5 Conclusion 158

A Alloy Code for Russian Cards Problem (3.3.1) 159

Bibliography 161

Abstract 177

Samenvatting 179

Index 181