



## UvA-DARE (Digital Academic Repository)

### Epistemic modelling and protocol dynamics

Wang, Y.

**Publication date**  
2010

[Link to publication](#)

#### **Citation for published version (APA):**

Wang, Y. (2010). *Epistemic modelling and protocol dynamics*. [Thesis, fully internal, Universiteit van Amsterdam]. Institute for Logic, Language and Computation.

#### **General rights**

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

#### **Disclaimer/Complaints regulations**

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

---

## Samenvatting

Dit proefschrift behelst een logisch onderzoek van kennisgerelateerde protocollen, met aandacht voor protocol-dynamiek, voor epistemisch modelleren en voor het bevragen van epistemische modellen ('model checking').

In Deel I presenteren we logische systemen voor het specificeren van epistemische protocollen, met inbegrip van protocol-doel en protocol-verandering. Hoofdstuk 3 verruimt het perspectief ten opzichte van bestaande behandeling van protocollen in Dynamische Epistemische Logica, door een logica te introduceren die zowel het protocol als het doel van het protocol kan specificeren *in de logische taal zelf*. We formaliseren het verificatieprobleem voor epistemische protocollen onder de aanname van meta-kennis over het beoogde doel van het protocol. De subtiliteit van dit verificatieprobleem wordt geïllustreerd met theorievorming en in praktijkvoorbeelden. In Hoofdstuk 4 snijden we de vraag aan hoe mensen een protocol kunnen leren. Hiervoor worden logische systemen geïntroduceerd die geschikt zijn voor het redeneren over kennisverandering en over protocolverandering. Door gebruik te maken van verschillende operatoren om protocollen te veranderen kunnen we dynamiek van protocollen behandelen en kunnen we formaliseren hoe handelingen nieuwe betekenis krijgen als gevolg van verandering in een protocol. We laten zien dat elk van de drie logische systemen die we introduceren terugvertaald kan worden naar Propositionele Dynamische Logica (PDL) op standaard Kripke modellen. Hiermee is aangetoond dat de technieken die we in andere delen van het proefschrift ontwikkelen van toepassing zijn op de drie nieuwe logische systemen.

In Deel II richten we ons op epistemisch modelleren, met als doel het bestuderen van 'model checking' voor de logische systemen die we in Deel I hebben geïntroduceerd. In Hoofdstuk 5 stellen we nieuwe compositie-operatoren voor op statische modellen en op gebeurtenismodellen met willekeurig vocabulair, met als doel een compositionele methode te ontwikkelen voor het genereren van initiële kennismodellen. We bewijzen een aantal decompositie-stellingen voor de nieuwe operatoren, en we laten aan de hand van voorbeelden zien hoe onze methoden kunnen worden gebruikt. Hoofdstuk 6 rapporteert over resultaten met betrekking tot het aantal verschillende modellen dat kan worden verkregen, gegeven een eindige omschrijving van een begintoestand. Voor 'image-finite models' laten we zien dat als

een formule uit de modale  $\mu$ -calculus een oneindig model heeft modulo bisimulatie, die formule  $2^{\aleph_0}$  verschillende modellen heeft modulo bisimulatie (de cardinaliteit van het continuüm). Aan de andere kant is het zo dat als een formule waarmee we beginnen *geen* oneindige modellen heeft modulo bisimulatie, dat wil zeggen als alle bisimulatie-minimale modellen van de formule eindig zijn, alle modellen voor die formule kunnen worden gerepresenteerd in een standaardvorm.

Deel III introduceert abstractie-technieken die van belang zijn om ‘model checking’ efficiënter te maken. In Hoofdstuk 7 wordt een driewaardige semantiek voor de logica van openbare aankondigingen (‘public announcement logic’) gedefiniëerd en bestudeerd. Het doel hiervan is om abstractie over modellen te vergemakkelijken. Met behulp van propositionele en agent afbeeldingen definiëren we een relatie tussen concrete modellen en hun abstracties. We laten daarmee zien dat het mogelijk is om te abstraheren van de signatuur van een model. We geven vervolgens een logische karakterisering van de abstractie relatie, en we tonen daarmee aan dat het veilig is om eigenschappen op het abstracte model te checken in plaats van op het originele concrete model. Hoofdstuk 8 bestudeert de PDL op zogenaamde *versnelde Kripke modellen* (‘accelerated Kripke models’), waar de toestandsovergangen in de modellen geëtiketteerd zijn met reguliere uitdrukkingen die meer informatie geven dan de enkelvoudige etiketten uit gewone Kripke modellen. Met behulp van een herschrijf-techniek voor reguliere uitdrukkingen analyseren we de complexiteit van het ‘model checking’ probleem en het vervulbaarheidsprobleem voor deze logica, en geven we een volledige axiomatisering.

In Deel IV (Hoofdstuk 9) geven we een overzicht van de epistemische invalshoeken op het verificatieprobleem voor beveiligingsprotocollen. We vatten de belangrijkste technieken hiervoor uit epistemische temporele logica en uit dynamische epistemische logica samen, en we vergelijken de twee soorten van technieken. We beargumenteren waarom sommige veiligheidseigenschappen betrouwbaar kunnen worden geformaliseerd met temporele logica plus kennisoperatoren, maar niet met standaard temporele logica. De extra expressiviteit heeft echter een prijs: ‘model checking’ met epistemische temporele logica is complexer dan met standaard temporele logica.