instituto de telecomunicações

FCT Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA EDUCAÇÃO E CIÊNCIA
PEst-OE/EEI/LA0008/2011
PEst-OE/EEI/LA0008/2013

Applications of Probabilistic Logics

Background and challenges

Formal Logic is used as a tool for reasoning about systems with **mathematical precision**. **Automation** of formal methods is possible since **symbolic reasoning** does not need to be creative.

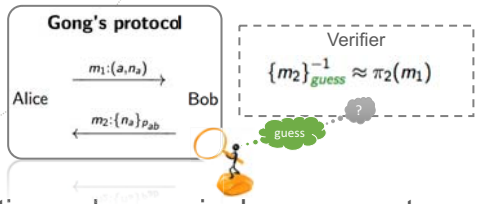
Many real life systems are realistically modeled by considering **stochastic behavior**, either because they have quantifiable **environmental uncertainties** or because they are **probabilistic by design**.

Logic has been chronically underdeveloped in the context of probabilistic systems. We develop logics to allow the verification of **protocols for cyberphysical systems**, to reason about **security of cryptographic protocols** and to prove ergodic properties of **Markovian models**.

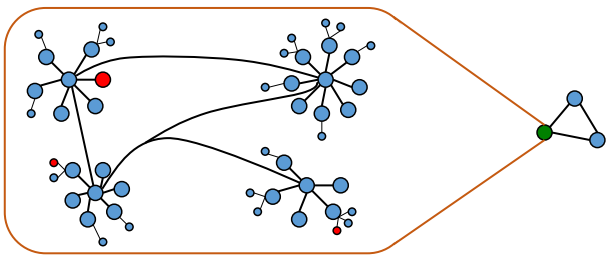
Description and main innovation

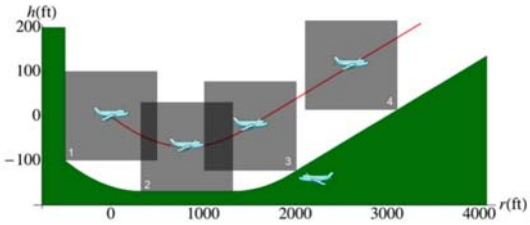
New approach to logic design: internalizing probabilistic analysis grants
- More precise abstractions, bringing the model closer to reality,
- Unlikely scenarios to be judged negligible, allowing for meaningful counterexamples to be found.

Innovative applications: enhanced descriptive capabilities enables natural modeling of a wide range of settings in telecommunications and security, namely



- Offline guessing attacks in security protocols, by attackers with cryptanalytic power,
- Aircraft collision avoidance protocols, with dynamic, stochastic, and numerical components,
- Ergodic properties regarding Markovian channel evolutions.





Achievements

- Formal safety verification of next generation aircraft collision avoidance protocols
- Proof-assisted precondition extraction
- Exact & numerical guarantees
- Approximate solution to long standing open problem
- Modeling & analyzing offline guessing attacks
- Reasoning about attackers with cryptanalytic capabilities
- Generalization of PSAT solver
- Novel framework for Markov chains Model Checking

Biscaia M., Henriques D., Mateus P. - Decidability of Approximate Skolem Problem
Conchinha B., Caleiro C., et al. - Symbolic Probabilistic Analysis of Off-Line Guessing
Biscaia M., Henriques D., Mateus P. - ω-Regular Properties for Stochastic Systems
Henriques D., Mateus P. et al. - Nondeterministic Stochastic Differential Dynamic Logic
Henriques D., Mateus P. et al. - Explicit errors in approximations of killed-diffusions
Mordido A., Caleiro C. - Equation-Based Probabilistic Logic and Applications

FCT Scholarship SFRH/BD/ 73315/2010 77648/2011 51846/2012