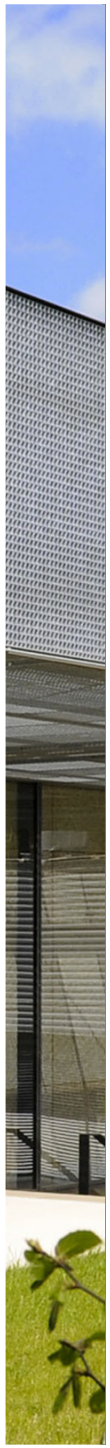
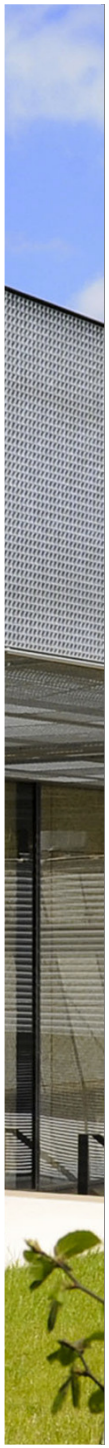


Model Checking for Probabilistic Hybrid Systems

Marta Kwiatkowska, Ernst Moritz Hahn
Oxford University Computing Laboratory

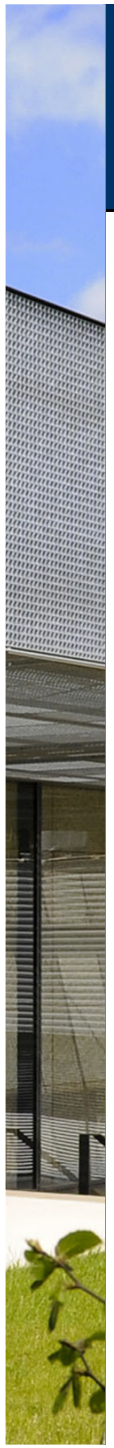
Holger Hermanns, Arnd Hartmanns
Saarland University, Dependable Systems and Software

CPSWeek'13, Philadelphia, April 2013



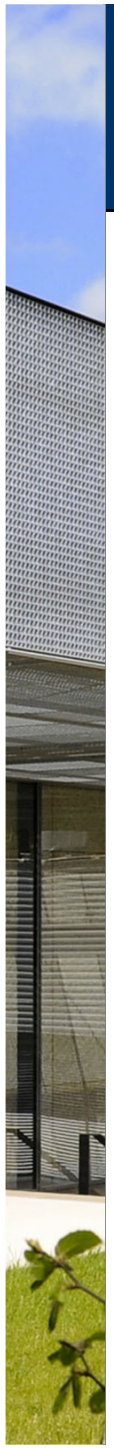
Part 1b

MDP demos



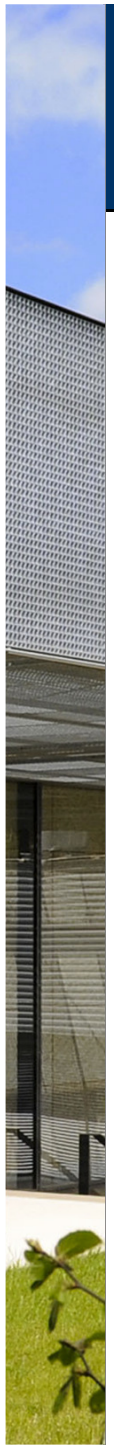
Overview (Part 1b)

- Tools for MDPs
- Analysis of the simple communication protocol
- Case study: Bounded retransmission protocol (BRP)



Tools for MDPs

- PRISM: Probabilistic symbolic model checker
  - developed at Birmingham/Oxford University since 1999
  - modelling of CTMCs, DTMCs, MDPs, PTAs + costs & rewards
  - modelling language: guarded commands
  - property language: PCTL + extensions + costs/rewards
- The Modest Toolset: mcpta frontend for PRISM
  - supports stochastic and hybrid models beyond PTA
  - more in third part of talk



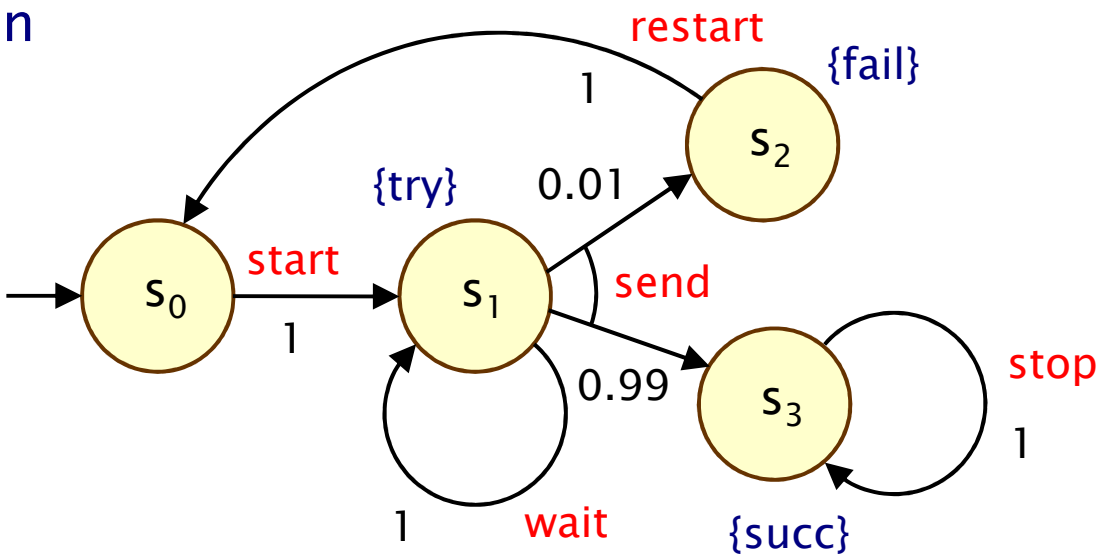
Overview (Part 1b)

- Tools for MDPs
- Analysis of the simple communication protocol
- Case study: Bounded retransmission protocol (BRP)

Simple MDP example

- Simple communication protocol
  - probability of success

$Pmin_{=?}$ [F (s = 3)]
$Pmax_{=?}$ [F (s = 3)]

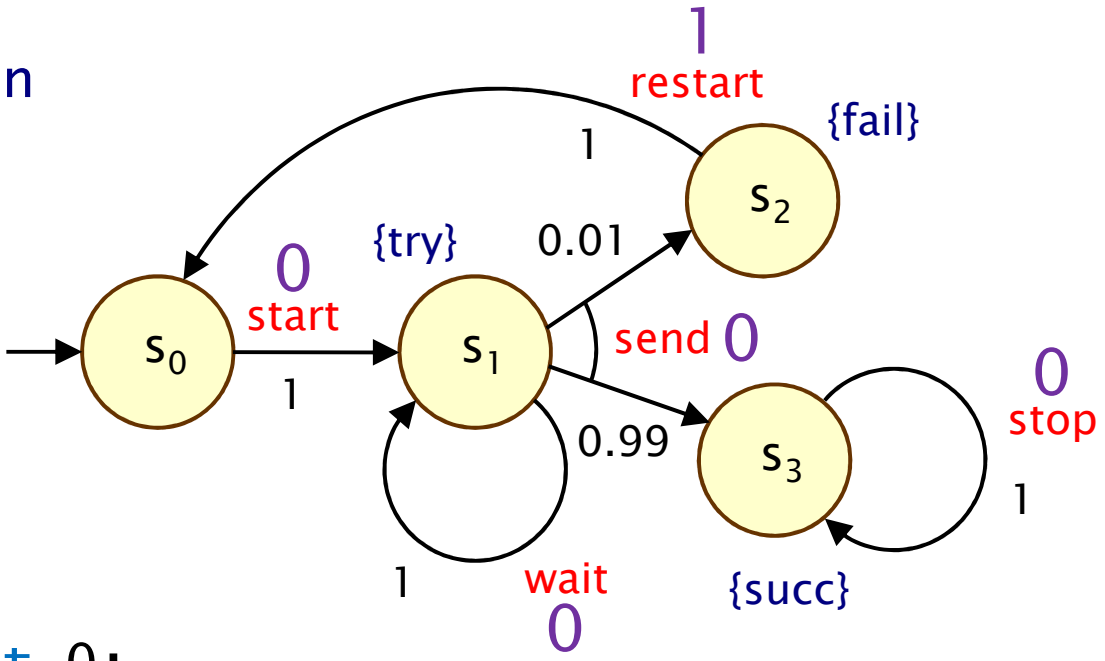



```
module example
   s : [0..3] init 0;
   [start]   (s = 0) -> (s' = 1);
   [wait]    (s = 1) -> true;
   [send]    (s = 1) -> 0.01: (s' = 2) + 0.99: (s' = 3);
   [restart] (s = 2) -> (s' = 0);
   [stop]    (s = 3) -> true;
endmodule
```

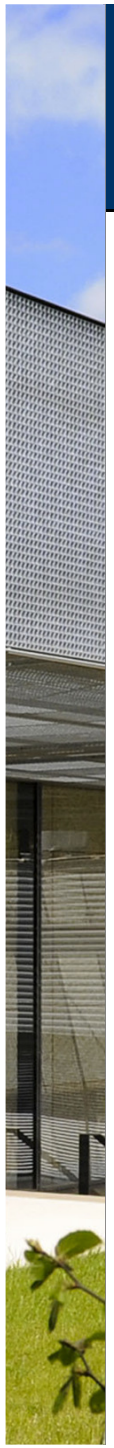
Simple MDP example

- Simple communication protocol
  - expected number of restarts

$Rmin_{=?}$ [F (s = 3)]
$Rmax_{=?}$ [F (s = 3)]




```
module example
   s : [0..3] init 0;
   [start]   (s = 0) -> (s' = 1);
   [wait]    (s = 1) -> true;
   [send]    (s = 1) -> 0.01: (s' = 2) + 0.99: (s' = 3);
   [restart] (s = 2) -> (s' = 0);
   [stop]    (s = 3) -> true;
endmodule
```



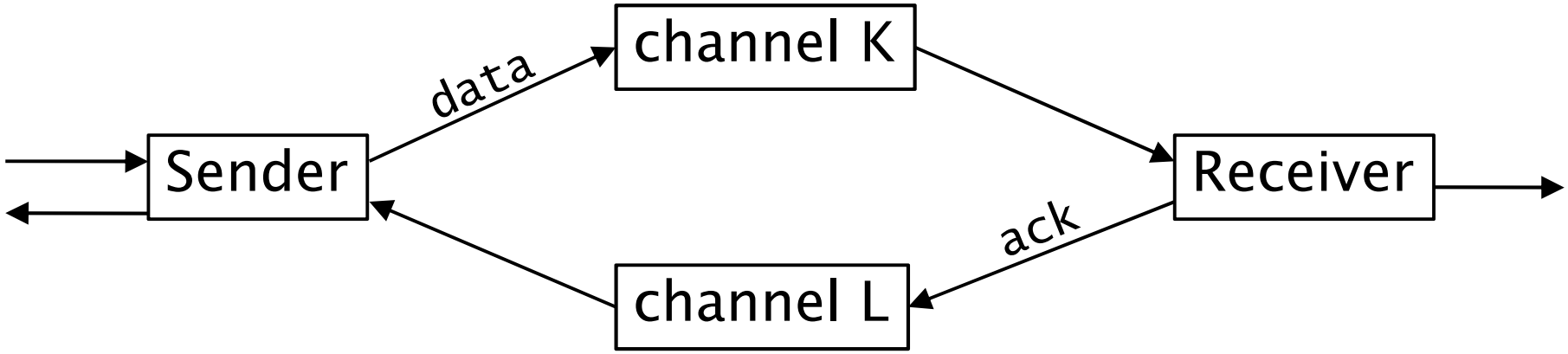
Overview (Part 1b)

- Tools for MDPs
- Analysis of the simple communication protocol
- Case study: Bounded retransmission protocol (BRP)

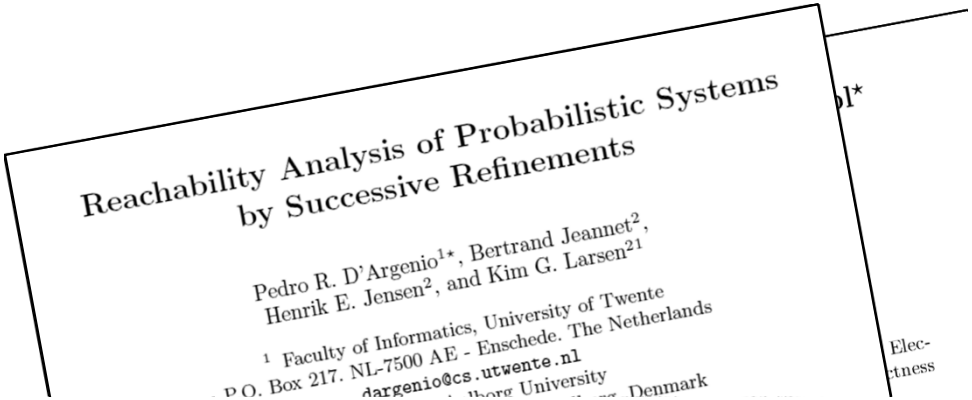
Case Study: BRP

- Bounded Retransmission Protocol

PHILIPS



- transmit files in chunks (frames) over lossy channels
- alternating bit protocol with $\leq$ MAX retries per frame
- studied extensively



Reachability Analysis of Probabilistic Systems by Successive Refinements

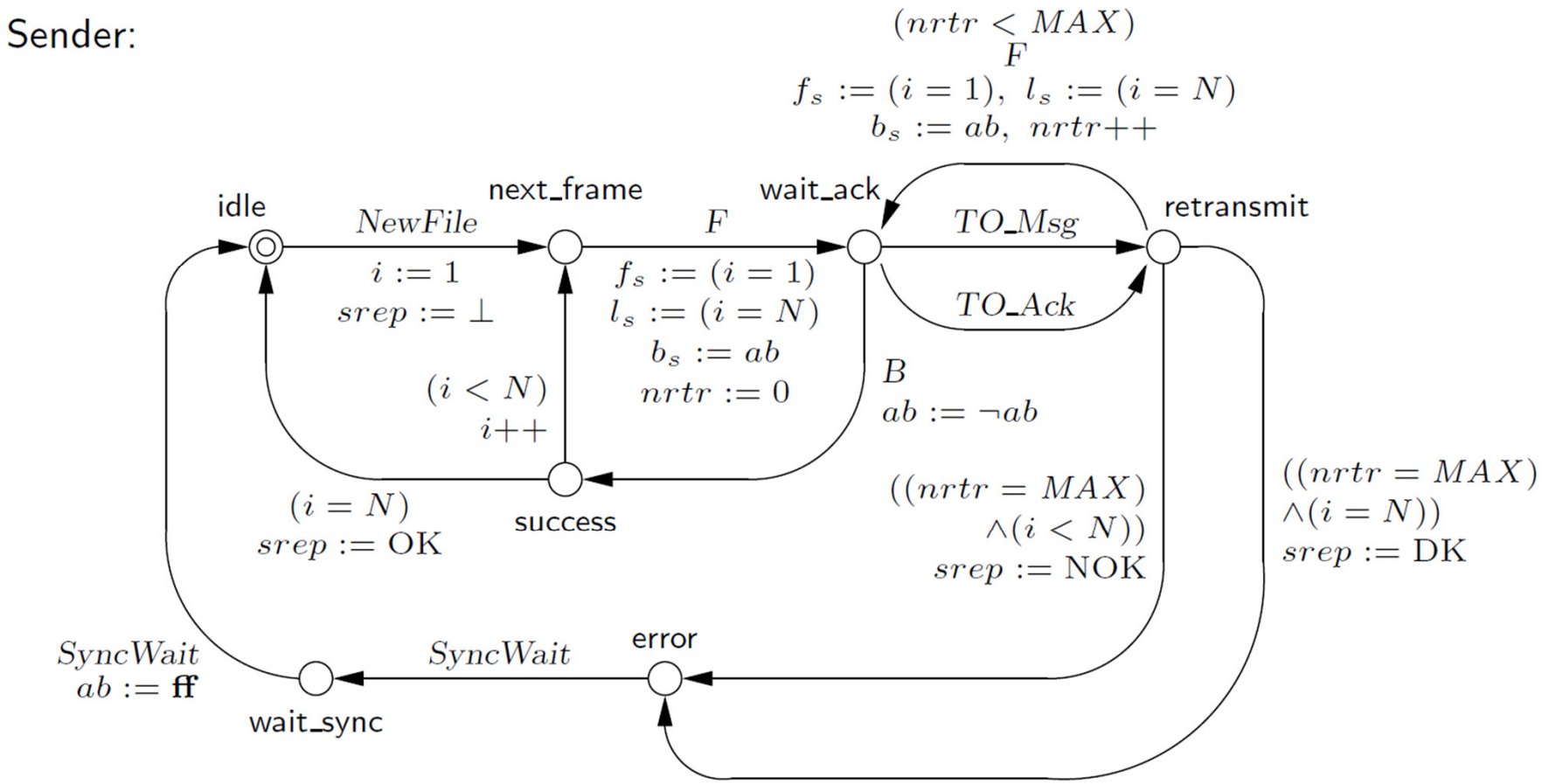
Pedro R. D'Argenio[1⋆], Bertrand Jeannet[2], Henrik E. Jensen[2], and Kim G. Larsen[21]

[1] Faculty of Informatics, University of Twente, P.O. Box 217. NL-7500 AE - Enschede. The Netherlands
dargenio@cs.utwente.nl

Case Study: BRP

- Sender
  - upper bound MAX on number of retransmissions

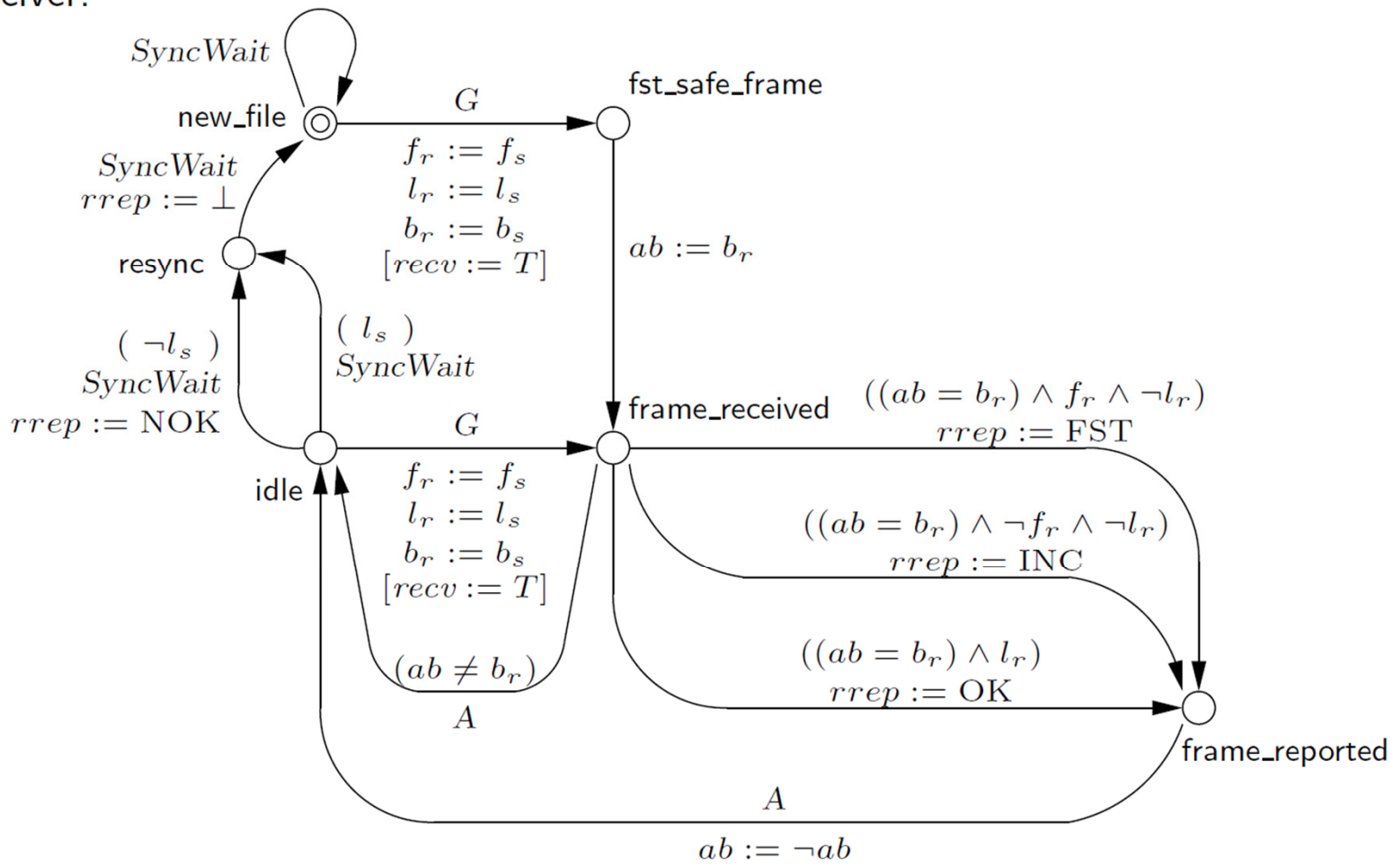
Sender:



Case Study: BRP

- Receiver
  - uses alternating bit to distinguish between new and old data

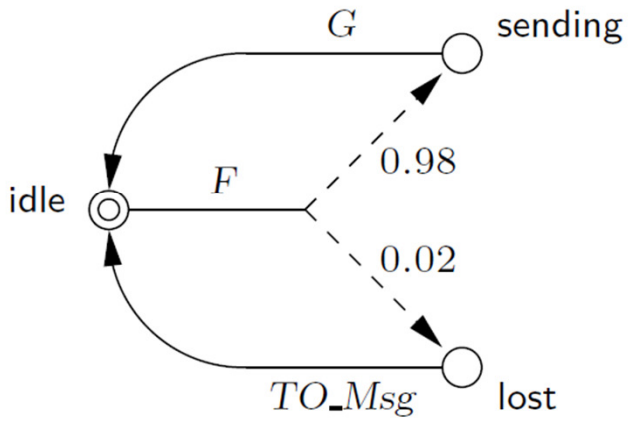
Receiver:



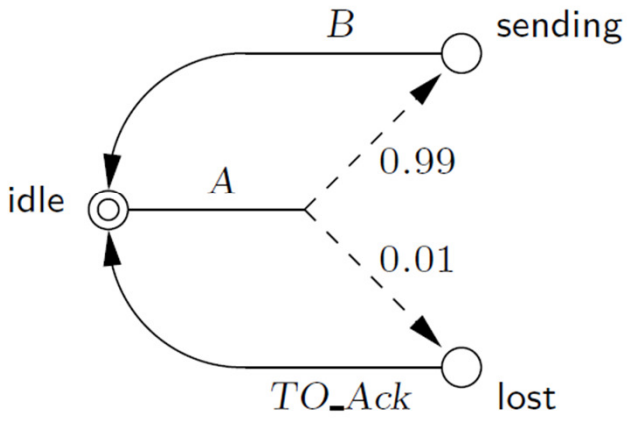
Case Study: BRP

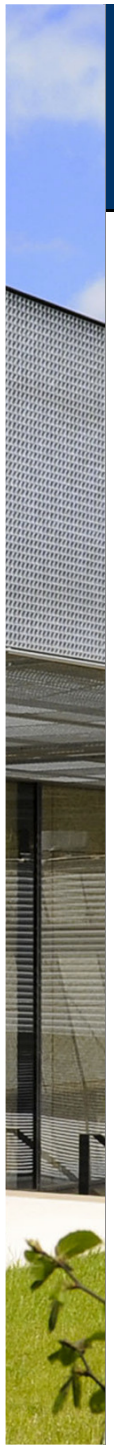
- Channels
  - different message loss probability
  - timeouts modelled with explicit synchronisation

Channel K:



Channel L:





Case Study: BRP

- Properties
  - maximum (= worst-case) probabilities for:
  - sender report failure in case of success (A)
  - sender reports success in case of failure (B)
  - sender does not report success (1)
  - sender reports uncertainty (2)
  - ...

⇨ DEMO