Statistical Model Checking
with
Uppaal

Peter Höfner

NICTA

Australian Government
Department of Broadband, Communications and the Digital Economy
Australian Research Council

NICTA Funding and Supporting Members and Partners

Conclusion

- (Exhaustive) Model Checking
  - efficient
  - fully automated
  - many case studies (hardware, software) …

  - variety of tools
    - Uppaal
    - Tiga
    - Spin
    - …

Conclusion (by E. Clarke)

NICTA

- But …

"State explosion is a major problem. This is absolutely true. The number of global system states of a concurrent system with many processes or complicated data structures can be enormous. All Model Checkers suffer from this problem. In fact, the state explosion problem has been the driving force behind much of the research in Model Checking and the development of new Model Checkers."

Conclusion

- But …
  - problem of state space explosion
    - model checking checks all reachable paths (more or less efficient)
    - as soon as a system is highly distributed, it is hard to check fully automated
  - quantitive analysis
    - hardly possible
    - qualitative reasoning only indicated that there is a problem; but not how serious it is

Motivation

- do we need verification guaranteeing 100%?
  - –for safety-critical systems/trustworthy systems
    YES
  - –for “standard” applications
    MAYBE NOT
    - –examples
      - the game console crashes
      - auto-save fails once in a while
      - protocols: packet loss, loops, …
- often high evidence/confidence sufficient

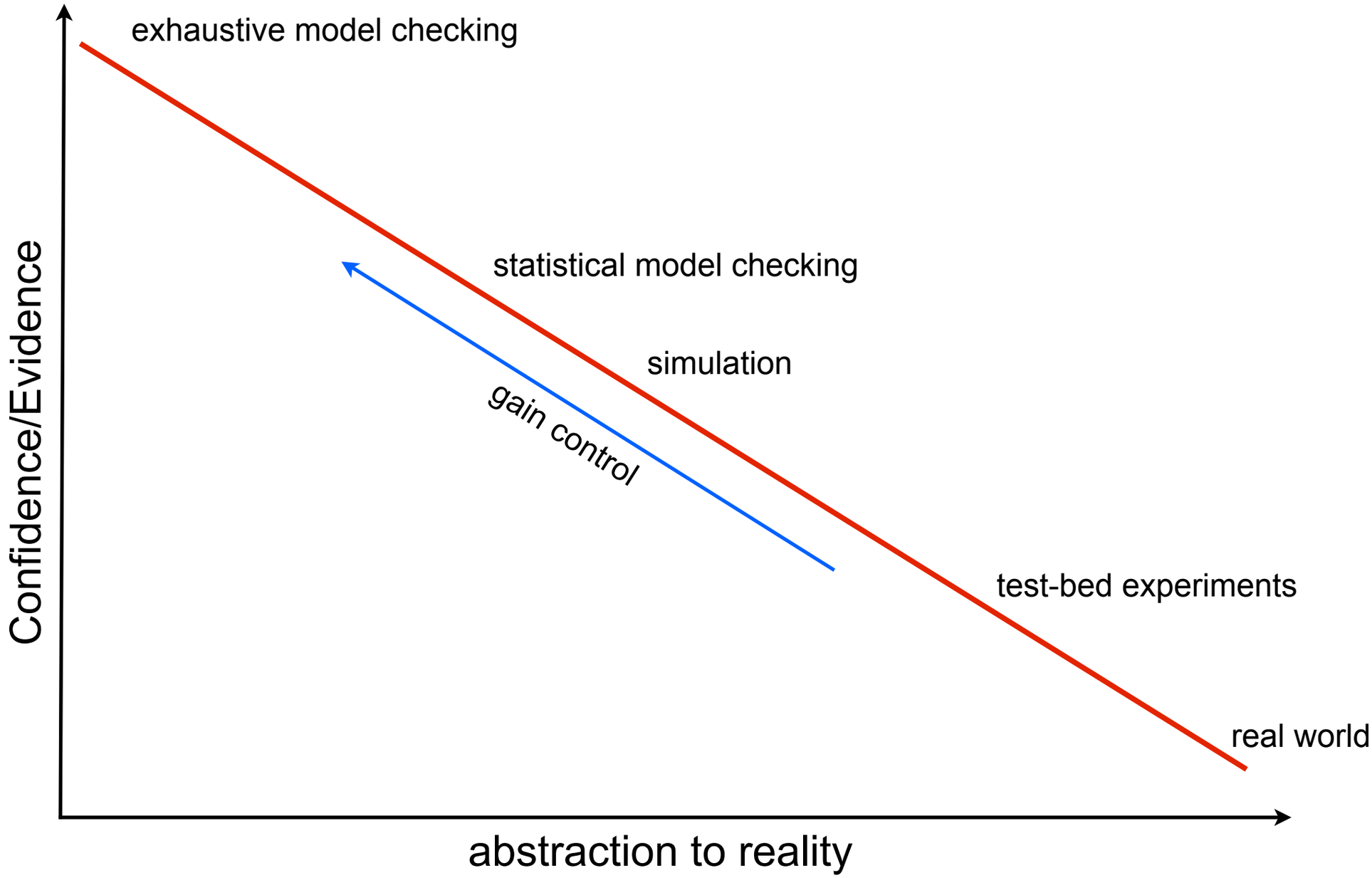
Statistical Model Checking

NICTA

- combines ideas of model checking and simulation
- supports quantitative analysis
- overcomes size barrier

- SMC trades certainty for approximation
  - using Monte Carlo style sampling, and hypothesis testing

Simulation vs SMC vs MC



- SMC allows more control on an abstract level
- for example abstracts from other network layers

SMC-Uppaal

NICTA

- Uppaal
  - timed automata as input
  - broadcast and binary handshake mechanisms
  - allows also probabilities on transactions

- SMC-Uppaal
  - extension of Uppaal
  - same input language (timed automata)
  - offers several parameters for set up (e.g. confidence level)
  - technicality: confidence depends mainly on number of runs; NOT on the size of the model

Case Study: AODV vs DYMO

NICTA

- AODV and DYMO are routing protocols for WMNs
  - ad hoc (network is not static)
  - on demand (routes are established when needed)

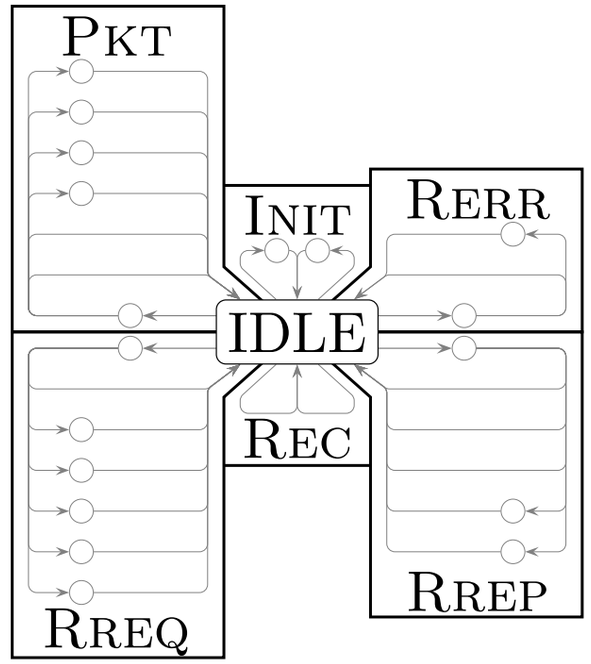
- Ad Hoc On-Demand Distance Vector (AODV)
  - 1997-2001 by Perkins, Beldig-Royer and Das (University of Cincinnati)
  - One of the four protocols currently standardised by the IETF MANET working group (IEEE 802.11s)

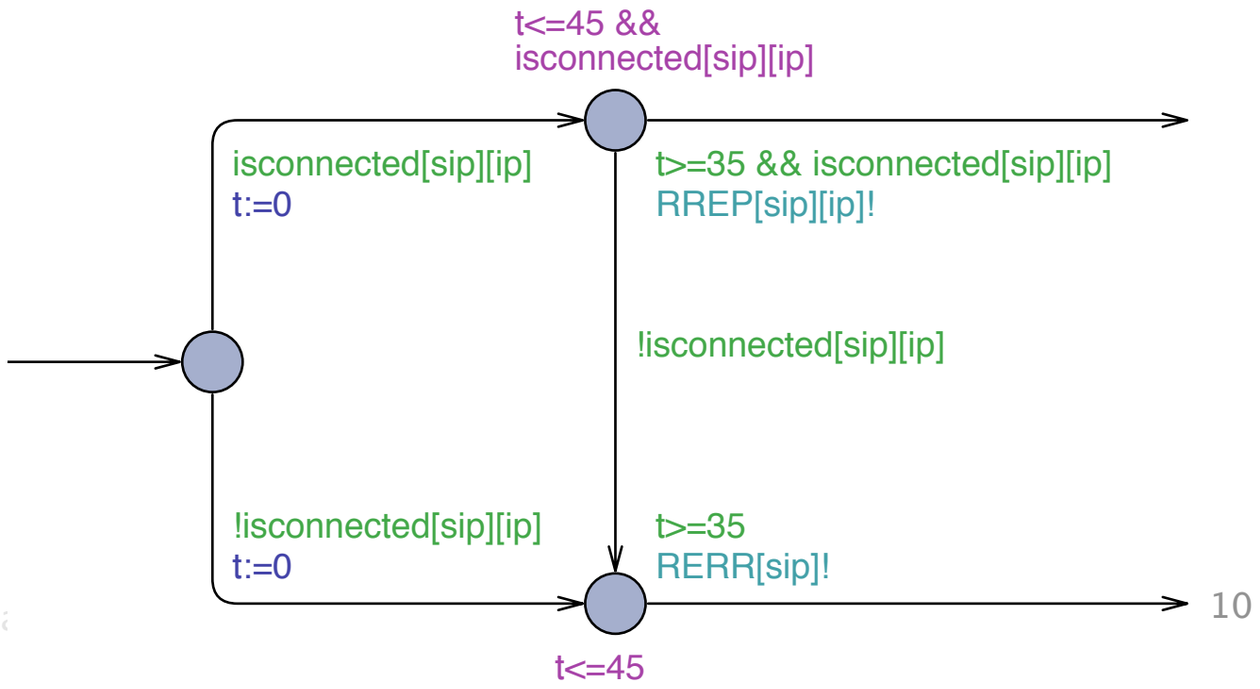
- Dynamic MANET On-demand (DYMO) Routing
  - successor of AODV
  - “supposed to be better”

Uppaal Models

NICTA

- created Uppaal models for AODV and DYMO
  - from unambiguous algebraic specifications
  - each node runs two processes
    - message queue
    - main processes, handling the received messages (takes time)
  - time only elapse while sending messages (some randomness)
  - technicality
    - SMC-Uppaal only allows broadcast





From ima

Experiments

- a timing analysis of AODV
- a comparison between AODV and DYMO
- a quantitative analysis of AODV and DYMO
- pushing the limits of network size

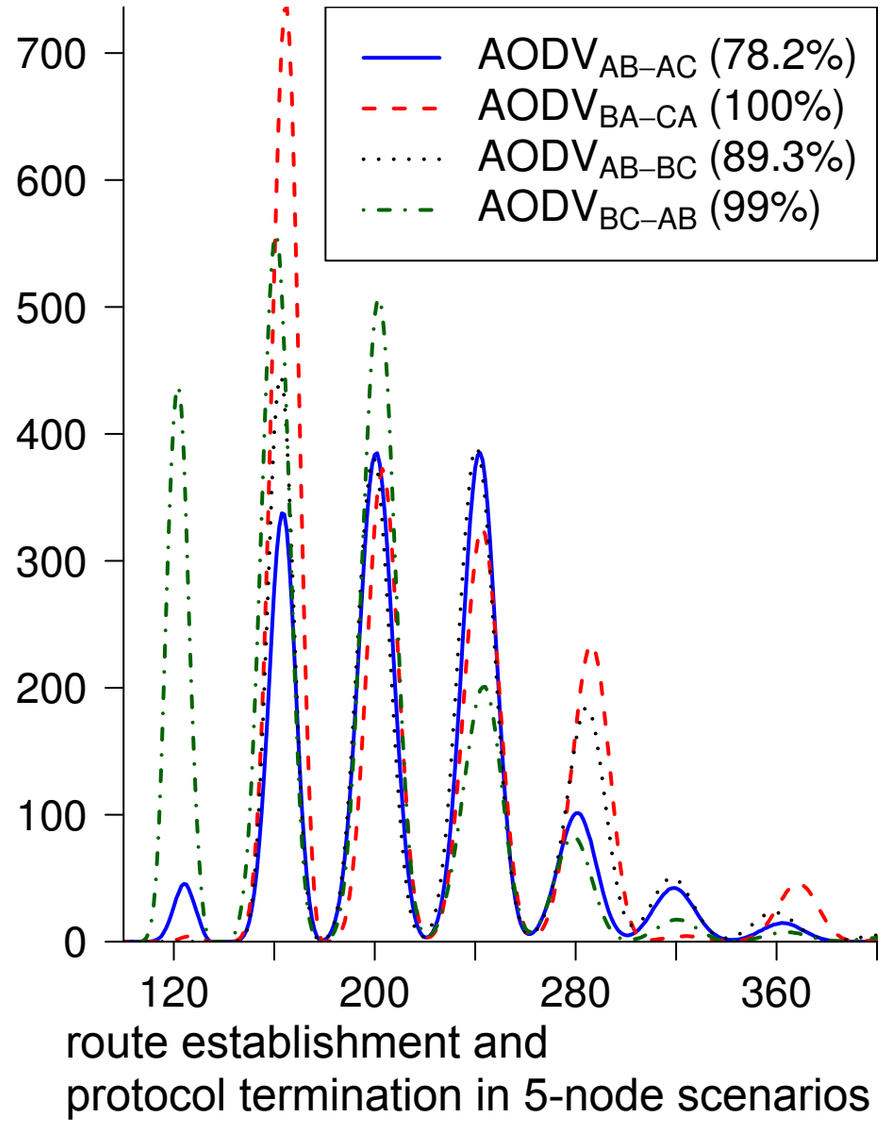
A Timing Analysis of AODV

NICTA

- AODV fails to establish some routes
  - in 47% of all scenarios
    - from exhaustive (non-timed) MC
    - non-quantitative values
      (does not state how often failure happens)
  - might depend on missing time
- replay some of the experiments
  - all topologies up to 5 nodes
    (similar to former experiments)
  - about 4000 experiments on 444 topologies
  - two requests, one topology change

A Timing Analysis of AODV

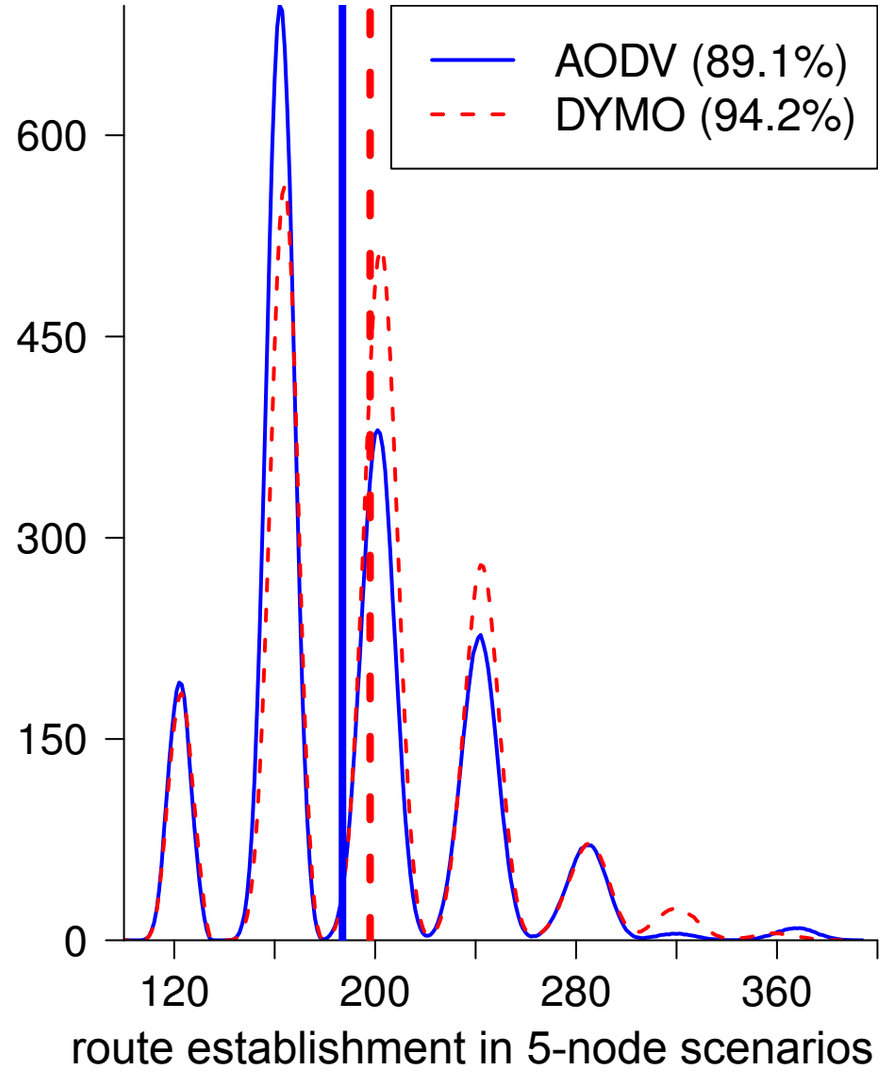
- results
  - failure rate around 10%
  - dependent on scenario
  - reasons
    - time has been added
    - we now have quantitative measurement



Comparison AODV vs DYMO

NICTA

- protocols vary in details, e.g.
  - different handling of sequence numbers
  - path accumulation
    (to decrease the number of messages sent)
- former experiments show that
  - DYMO behaves better
  - AODV behaves better
- results
  - DYMO fails less often



Quantitative Comparison AODV vs DYMO

NICTA

- quantitative measurements
  - route quantity
    - nodes gain knowledge by received messages
  - route quality
    - how good/useful is the knowledge learned
- results
  - DYMO establishes fewer routes
    - that was a surprise since it uses path accumulation
    - fewer messages sent means fewer opportunities to learn alternative routes
  - DYMO's route quality is worse than that for AODV
    - conjecture: big consequences in larger networks

	3 nodes	4 nodes	5 nodes
AODV	5.28	8.83	13.99
DYMO	5.25	7.87	11.94
max	6	12	20

Average number of routes established

Experiments (Intermediate) Summary

NICTA

- exhaustive analysis of topologies up to 5 nodes
  - could be handled by exhaustive MC
  - allowed quantitative analysis
  - some surprising insights in AODV and DYMO
    - although these protocols have been implemented and analysed for years
  - (network sizes with 6 or 7 nodes are possible)
- can SMC really can overcome the size barrier
  - last experiment

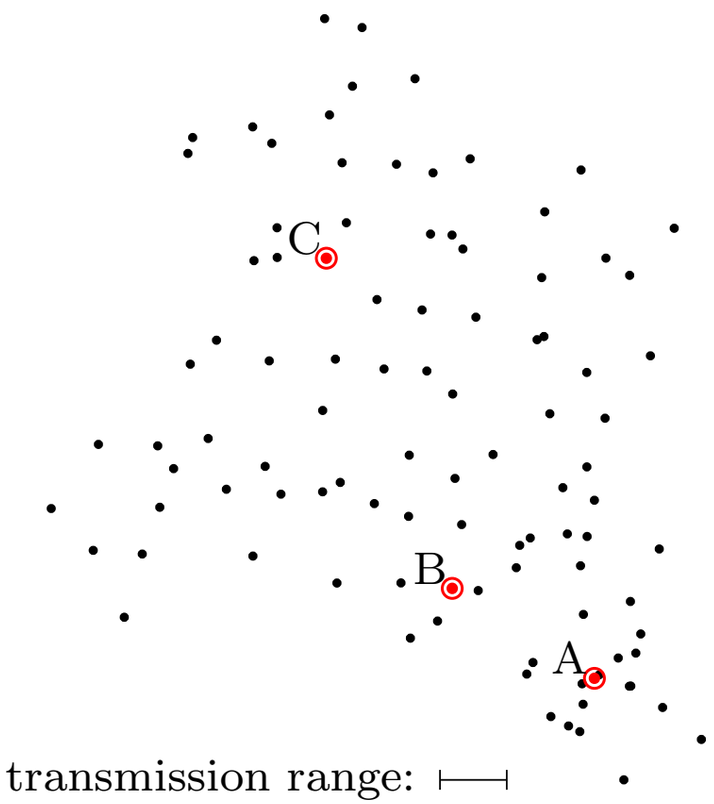
Networks of Realistic Size

NICTA

- WMNs consist of 20-100 nodes
  - some problems seem to occur only in larger networks
- analysis of topologies with 100 nodes feasible
  - problem: topology choice
  - node placement algorithm for realistic topologies (NPART)

#nodes	50	75	100
memory (Gb)	14	30	80
run time (m)	270	328	1777

Memory consumption



a network with 100 nodes

The Other Side of the Coin

NICTA

- we can analyse realistic size networks
  - which topology to be chosen (there are too many)
    - (small network topologies can be iterated)
  - dynamic topology
    - link failures could be modelled by probabilities
    - mobile nodes should be modelled

Another Conclusion

- timed models of AODV and DYMO
  - systematic analysis across all small networks
  - examine reasons for observed differences in performance

- examined the feasibility of SMC w.r.t. scalability
  - first analysis of WMNs of realistic size

- what's next
  - catalogue of topology (shape, density, ...)
  - mobility model
  - (multicore Uppaal)

NICTA

THE END