


The imagination driving Australia's ICT future. 


## Performance Analysis with Prism

Formal Verification and Simulation for Performance Analysis for Probabilistic Broadcast Protocols

Ansgar Fehnker,  
joint work with Peng Gao

(accepted at Ad-Hoc Now 2006)


27/10/2006 FM Workshop 1

The imagination driving Australia's ICT future. 

## The Content

- The project
- The problem
- The protocol
- The assumptions
- The approach
- The results
- The future

27/10/2006 FM Workshop 2


The imagination driving Australia's ICT future. 

## The PEWNA project


### Wireless sensor networks

Aggregate of small, portable devices

- battery-operated computing power
- gather sensor information distributedly
- wireless communications
- multi-hop communication



27/10/2006 FM Workshop 3

The imagination driving Australia's ICT future. 

## The PEWNA project

### Challenges for network and application design

- Unpredictable behaviour of the environment.
- Dynamic nature of network with respect to spatial distribution and ad hoc addition of nodes.
- Resilience to message loss and node failure.
- Power efficiency to maximise battery life and network lifetime.

27/10/2006 FM Workshop 4

The imagination driving Australia's ICT future.

**The PEWNA project**

**Project Goals**

- Notations, analysis tools and reusable formal models for wireless network protocols.
- Application of probabilistic and hybrid model checking techniques for performance evaluation.
- Abstraction techniques to scale probabilistic and hybrid model checking techniques.

27/10/2008 FM Workshop 5

The imagination driving Australia's ICT future.

**The problem**

Simulation is an imperfect tool

27/10/2008 FM Workshop 6

The imagination driving Australia's ICT future.

**Current Best Practice**

**Model-Based Design**

**Advantages of Model-Based Design**

Requirements and Specs    Design    Implementation    Test and Verification

**Executable models**  
-unambiguous  
-only "one truth"

**Simulation**  
-reduces "real" prototypes  
-systematic "what-if" analysis

**Test with Design**  
-detects errors earlier

Courtesy by cseanet

27/10/2008 FM Workshop 7

The imagination driving Australia's ICT future.

**Related Work**

**On the Accuracy of MANET Simulators**  
*Cavin, Sasson and Schiper (2002)*

- Different simulators give different answers
- Even for simple protocols
- Semantics defined by simulator.
- Low level details as important as high level protocol

Protocol steps	NS2	NS3	NS3+
10	100	100	100
20	100	100	100
30	100	100	100
40	100	100	100
50	100	100	100
60	100	100	100
70	100	100	100
80	100	100	100
90	100	100	100
100	100	100	100

27/10/2008 FM Workshop 8

## Related Work

### Experimental Evaluation of Wireless Simulation Assumptions

*Kotz, Newport et al. (2004)*

- Assumptions render results useless
- Common assumptions:
  1. The earth is flat
  2. The transmission area is circular.
  3. All radios have equal range.
  4. If I can hear you, you can hear me.
  5. If I can hear you at all, I can hear you perfectly.
  6. Signal strength is a simple function of distance.



## The Problem

### Common Solution

- More details
- Hardware in the loop simulation
- Precise specific assumptions
- Specific results for specific instance of a system

## The Problem

### Our Approach

- More abstract model
- Formal model with well defined semantics
- Precise assumptions
- General results for a range of systems

## The Protocol

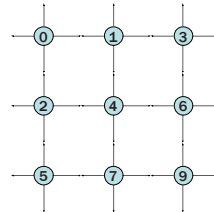
Gossiping is simple

### The Protocol

#### Flooding and Gossiping

- Simple protocols
- Commonly used in some phase of wireless protocols
- Many ambiguous and conflicting simulation models

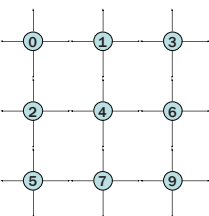
### Flooding and Gossiping



- Flooding protocol
- listen to medium
  - if you receive a message
    - send message
  - go to sleep

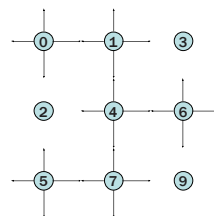
- Properties of flooding
- simple
  - used for routing
  - redundant
  - prone to collisions
  - inefficient

### Flooding and Gossiping




- Gossiping protocol
- listen to medium
  - if you receive a message
    - send message with probability  $p$
  - go to sleep

### Flooding and Gossiping



- Gossiping protocol
- listen to medium
  - if you receive a message
    - send message with probability  $p$
  - go to sleep


- Properties of gossiping
- still simple
  - reduces redundancy
  - reduces collisions
  - improves efficiency

The imagination driving Australia's ICT future. 

## The assumptions

What else?

27/10/2008 FM Workshop 17


The imagination driving Australia's ICT future. 

## Common assumption

### Common assumptions

- Absence of collisions
- Perfectly synchronous execution
- No clock drift
- Perfect medium

27/10/2008 FM Workshop 18


The imagination driving Australia's ICT future. 

## Our approach

### For a simple protocol show

- The effect of common assumptions on performance results
- How to model a wireless protocol
  - a less ambiguous model
  - with explicit assumptions
  - abstracting from low level detail
- How to use a probabilistic model checker (PRISM)
- How to obtain performance style results

27/10/2008 FM Workshop 19

The imagination driving Australia's ICT future. 

## Modelchecking

### PRISM

A Probabilistic Symbolic Model Checker (Uni Birmingham)

Supports:

- Discrete-Time Markov Chains (DTMCs)
- Continuous-Time Markov Chains (CTMCs)
- Markov Decision Processes (MDPs)

Checks:

- Probabilistic temporal logic (PCTL)
- Example: node 7 receives a message with probability > 0.8

27/10/2008 FM Workshop 21

## Formal Model

### Model protocols as formal models (in Prism)

- Well defined semantics,
- Abstraction from low level detail

### Example

```

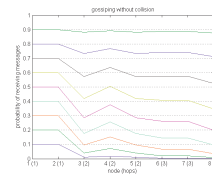
module node4
act4: bool init true;
send4: bool init false;
[tick] act4 & !send4 & (send1|send3|send5|send7)
-> psend: (act4=true)&(send4=true) + (1-psend):(act4=false)&(send4=false);
[tick] act4 & !send4 & !(send1|send3|send5|send7)-> (act4=true) & (send4=false);
[tick] act4 & send4 -> (act4=false) & (send4=false);
[tick] !act4 -> (act4=false) & (send4=false);
endmodule
    
```

PRISM model of gossiping protocol

## Performance Evaluation

### Model protocol as formal models

- Well defined semantics, allows abstraction from low level detail
- Verification produces exact answers
- Makes assumptions explicit



- PRISM results for gossiping w/o collision
- Results are exact probabilities rather than approximations

## Common assumption

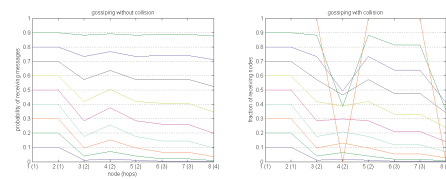
### Common assumptions

- Absence of collisions
- Perfectly synchronous execution
- No clock drift
- Perfect medium
- Random choice equals lossy channel

## Collisions

### Model protocol as formal models

- Well defined semantics, allows abstraction from low level detail
- Verification produces exact answers
- Makes assumptions explicit



## Common assumption

### Common assumptions

- Absence of collisions
- Perfectly synchronous execution
- No clock drift
- Perfect medium

## Synchronization

### Model protocols as formal models

- Well defined semantics, allows abstraction from low level detail
- Verification produces exact answers
- Makes assumptions explicit
- Clean understanding of concurrency

```

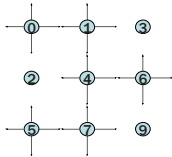
for i=find(sending) %for all nodes that are sending
    if(rand <= p)
        for j=1:4
            if(C(i,j) == 0) % if it has a neighbour
                receive(C(i,j)) = 1; %then neighbour receives a msg
            end
        end;
    end;
end;
    
```

Matlab code for Monte-Carlo simulation: *implicitly synchronous*

## Synchronization

### Model protocols as formal models

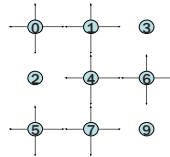
- Well defined semantics, allows abstraction from low level detail
- Verification produces exact answers
- Makes assumptions explicit
- Clean understanding of concurrency



## Synchronization

### Model protocols as formal models

- Well defined semantics, allows abstraction from low level detail
- Verification produces exact answers
- Makes assumptions explicit
- Clean understanding of concurrency

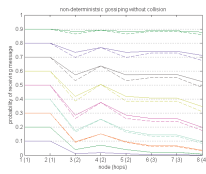


Does it matter?

## Synchronization

### Model protocols as formal models

- Well defined semantics, allows abstraction from low level detail
- Verification produces exact answers
- Makes assumptions explicit
- Clean understanding of concurrency

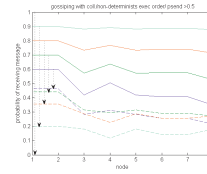


- PRISM results for gossiping w/o collision
- Model with non-deterministic execution order
- Minimal and maximal probability cover all possible execution orders

## Synchronization

### Model protocols as formal models

- Well defined semantics, allows abstraction from low level detail
- Verification produces exact answers
- Makes assumptions explicit
- Clean understanding of concurrency

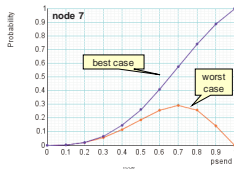


- PRISM results for gossiping with collision
- Model with non-deterministic execution order
- Minimal and maximal probability cover all possible execution orders
- Model checking gives guarantees that simulation cannot.

## Synchronization

### Model protocols as formal models

- Well defined semantics, allows abstraction from low level detail
- Verification produces exact answers
- Makes assumptions explicit
- Clean understanding of concurrency



- PRISM results for gossiping with collision
- Model with non-deterministic execution order
- Minimal and maximal probability cover all possible execution orders
- Model checking gives guarantees that simulation cannot.

## Common assumption

### Common assumptions

- Absence of collisions
- Perfectly synchronous execution
- No clock drift
- Perfect medium

The imagination driving Australia's ICT future.

**Timing**

Unreliable timing

- Modelled as probabilistic waiting
- Compared different variants of the timing model

Example

```
[tick] active4=1 & send4=0 & send1+send3+send5+send7 =1
-> (1-psend): (active4'=0)&(send4'=0)
+ psend*(1-pdelay): (active4'=1)&(send4'=1)
+ psend* pdelay: (active4'=2)&(send4'=0);
[tick] active4=2 ->(1-pdelay): (active4'=1)&(send4'=1)
+ pdelay: (active4'=2)&(send4'=0);
```

PRISM model of simple delay

27/10/2008 FM Workshop 34

The imagination driving Australia's ICT future.

**Timing**

Unreliable timing

- Modelled as probabilistic waiting
- Compared different variants of the timing model

Model checking results for comparing with collision and delay

- PRISM results for simple timing model
- Effect of collisions vanishes with an increasing probability for delay
- Firm upper and lower bound provided by non-deterministic model

27/10/2008 FM Workshop 35

The imagination driving Australia's ICT future.

**Common assumption**

Common assumptions

- Absence of collisions
- Perfectly synchronous execution
- No clock drift
- Perfect medium

27/10/2008 FM Workshop 36

The imagination driving Australia's ICT future.

**Imperfect Medium**

Model medium by lossy channels

- Abstract from actual topology
- Nodes are connected by channels
- Messages are received with a certain probability

Rather than sending with a certain probability

27/10/2008 FM Workshop 37

The imagination driving Australia's ICT future. NATIONAL ICT AUSTRALIA

## Imperfect Medium

### Model medium by lossy channels

- Performance of lossy channels better than probabilistic broadcast

27/10/2008 FM Workshop 38

The imagination driving Australia's ICT future. NATIONAL ICT AUSTRALIA

## Intermediate Summary

### Results

- Prism model for gossiping protocols
- Well defined semantics
- Abstraction from low level detail
- Verification produces exact answers
- Makes assumptions explicit
- Results for small networks (up to 20 nodes)

What about large networks (1000 nodes)?

27/10/2008 FM Workshop 39

The imagination driving Australia's ICT future. NATIONAL ICT AUSTRALIA

## Matlab model

### Monte-Carlo simulation

- Derived a simulation model (manually) from PRISM model
- Observed effects are only visible for large models/models

27/10/2008 FM Workshop 40

The imagination driving Australia's ICT future. NATIONAL ICT AUSTRALIA

## Matlab model

### Monte-Carlo simulation

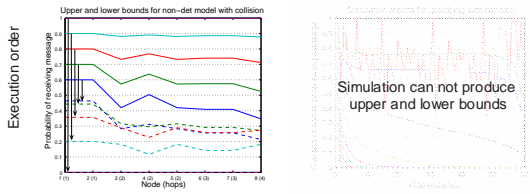
- Derived a simulation model (manually) from PRISM model
- Observed effects are only visible for large models/models

27/10/2008 FM Workshop 41

## Matlab model

### Monte-Carlo simulation

- Derived a simulation model (manually) from PRISM model
- Observed effects are only visible for large models/models



27/10/2008

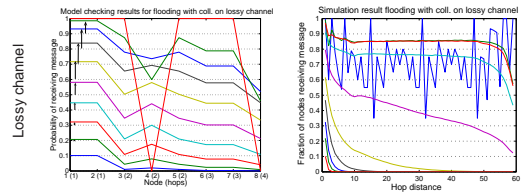
FM Workshop

42

## Matlab model

### Monte-Carlo simulation

- Derived a simulation model (manually) from PRISM model
- Observed effects are only visible for large models/models



27/10/2008

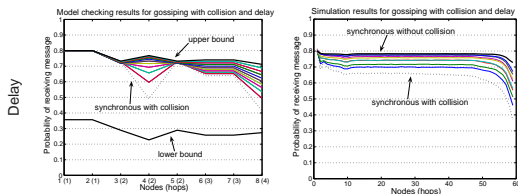
FM Workshop

43

## Matlab model

### Monte-Carlo simulation

- Derived a simulation model (manually) from PRISM model
- Observed effects are only visible for large models/models
- Only approximate results




27/10/2008

FM Workshop

44

## Observations


The imagination driving Australia's ICT future. 

## Observations

### Gossiping

- Collisions matter
- Collisions are worst in synchronous networks
- Clock jitter mitigates effect of collisions
- Lossy channels is not random broadcast

27/10/2008 FM Workshop 47


The imagination driving Australia's ICT future. 

## Observations

### Verification

- Simulation models based on implicit assumptions
- Different behaviour for "same" protocol
- Formal model helps to reveal hidden assumptions
- Formal model can serve as "golden" model
- Model checking can be used for performance evaluation

27/10/2008 FM Workshop 48


The imagination driving Australia's ICT future. 

## Observations

### Simulation and Verification


- Simulation complements model checking
- We are currently two different models (artifacts) Prism/Simulink
  - Straightforward translation yields inefficient simulator
  - Prism sparse matrix model infeasible for large networks
  - Sparse matrix model hides the structure of the problem
- The problem can be solved
- Future work
  - Prism to of-the-shelf simulator translation

27/10/2008 FM Workshop 49

The imagination driving Australia's ICT future. 

## The End

27/10/2008 FM Workshop 50


The imagination driving Australia's ICT future. 

## Towards part 2

### Model checking

- For debugging
  - Better descriptions for improved protocols
- For performance evaluation
  - Exact results under known assumptions
- For optimization
  - Ask Annabelle

27/10/2008 FM Workshop 51

The imagination driving Australia's ICT future. 

## Baseline Model for Packet Collision


```

module node4
act4: bool init true;
send4: bool init false;

[tick] act4 & !send4 & (send1+send3+send5+send7=1)
-> psend: (act4=true)&(send4=true) +
(1-psend):(act4=false)&(send4=false);
[tick] act4 & !send4 & !(send1+send3+send5+send7=1)
-> (act4=true) & (send4=false);
[tick] act4 & send4
-> (act4=false) & (send4=false);
[tick] !act4
-> (act4=false) & (send4=false);

endmodule
    
```

27/10/2008 FM Workshop 52

The imagination driving Australia's ICT future. 


## Summary

### Project focus


- Notations, analysis tools and reusable formal models
- Model checking techniques for performance evaluation.
- Abstraction techniques to scale probabilistic and hybrid model checking techniques.

### Tasks

- Identification of case studies
- Formalisation of network behaviour
- Analysis with existing model checkers
- Modelling notation and semantics
- Mapping to existing tools
- Integration with proof-based techniques



27/10/2008 FM Workshop 53

The imagination driving Australia's ICT future. 

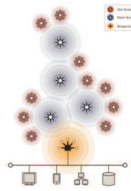
## Summary

### Project focus

- Notations, analysis tools and reusable formal models
- Model checking techniques for performance evaluation.
- Abstraction techniques to scale probabilistic and hybrid model checking techniques.

### Tasks

- Identification of case studies
- Formalisation of network behaviour
- Analysis with existing model checkers
- Modelling notation and semantics
- Mapping to existing tools
- Integration with proof-based techniques



27/10/2008 FM Workshop 54