Modelling and Verification of Protocols for Wireless Networks

(Lecture7)

Peter Höfner

(Lecture at University of Twente, Jan/Feb 2017)

www.data61.csiro.au

last update: Feb 2, 2017

Contents of this Lecture

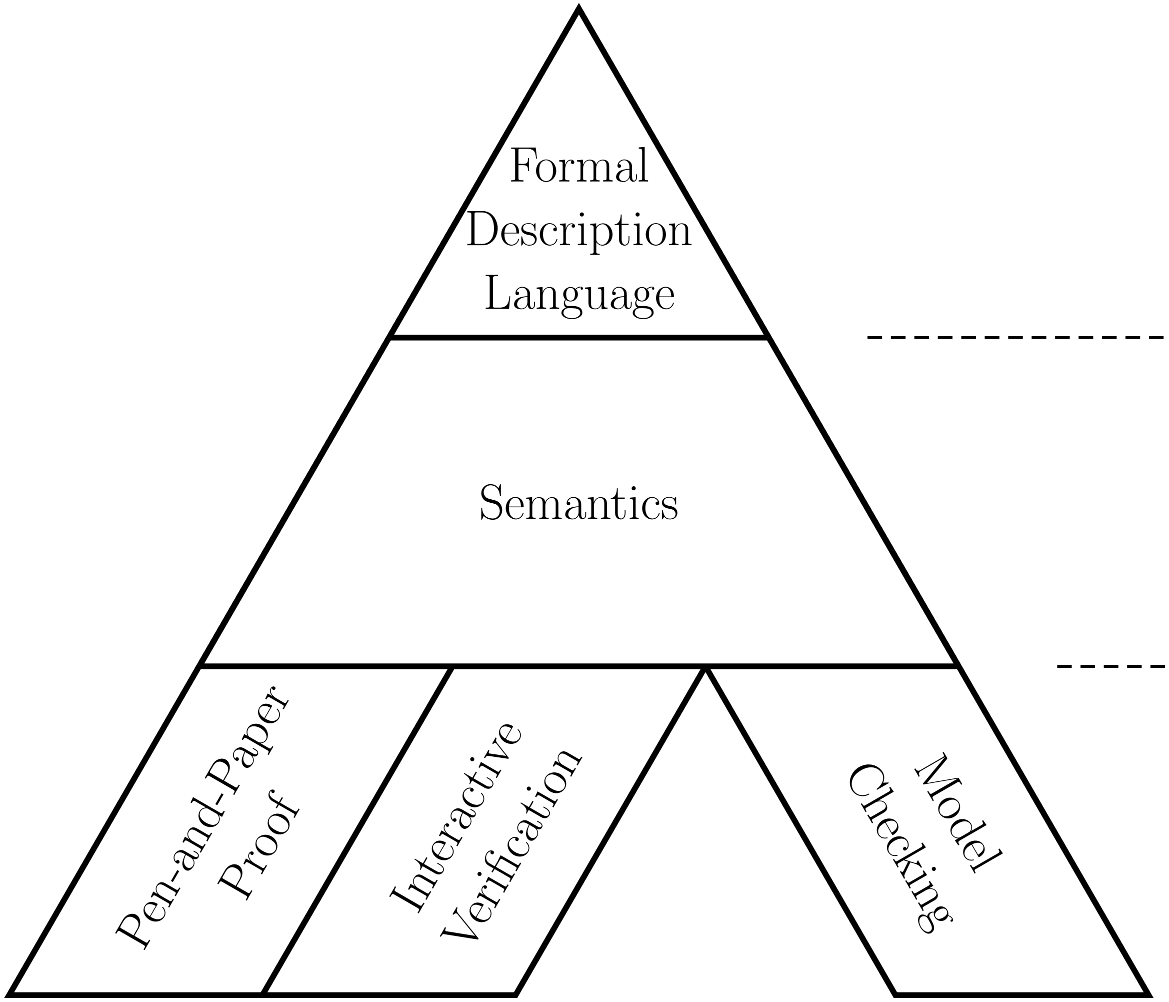
What should you have learnt

- nothing new
  - a quick overview of what we have done
  - open research challenges

- Q&As (Questions and Answers)

Summary

Modelling and Verifying Wireless Networks



Summary

- AWN
  - Layered approach
    - engineers only need to understand node-level
    - about 10 primitives, including 3 different sending mechanisms
    - easy to use?
- Formal Semantics
  - needed for formal reasoning
    (pretty complicated, becomes “ugly” when adding time)
- various tool support
  - Model Checking (quick feedback, “in-complete” guarantees)
  - Isabelle/HOL (full verification)

Be careful

- slides should be taken with a grain of salt
  - first time I taught this course (hence typos, etc)
  - some of the work is work in progress (mistakes, etc)

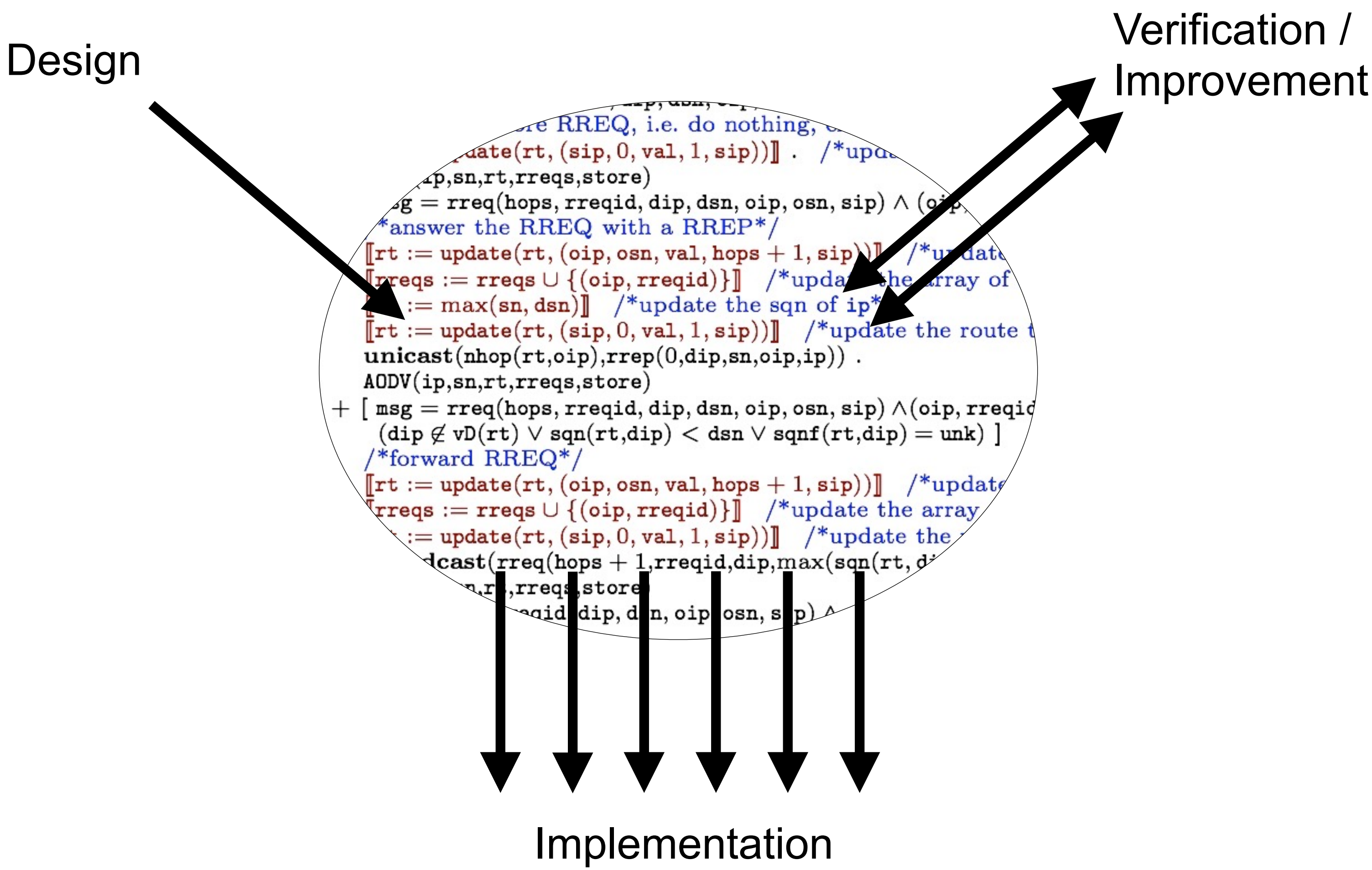
Disclaimer

- AWN is not the only modelling language
  - process calculi

Process algebra	Message loss	Type of broadcast		Connectivity model		
CBS	enforced synchr.	global broadcast				symmetric
$b\pi$	enforced synchr.	subscription-based broadcast				symmetric
CBS#	enforced synchr.	local bc.	dynamic top.	$n[P,S]$	op. sem.	symmetric
CWS	enforced synchr.	local bc.	static topology	$n[P]^{c}_{l,r}$	node	symmetric
CMAN	lossy broadcast	local bc.	dynamic top.	$\lfloor p \rfloor^{\sigma}_{l}$	node	symmetric
CMN	lossy broadcast	local bc.	dynamic top.	$n[P]^{\mu}_{l,r}$	node	symmetric
ω	lossy broadcast	local bc.	dynamic top.	$P : G$	node	symmetric
RBPT	lossy broadcast	local bc.	dynamic top.	$[\![P]\!]_{l}$	op. sem.	asymmetric
$bA\pi$	lossy broadcast	local bc.	dynamic top.	$\lfloor p \rfloor_{l}$	network	asymmetric
$b\psi$	lossy broadcast	local bc.	dynamic top.	P	op. sem.	asymmetric
AWN	enforced synchr. with guar. receipt	local bc.	dynamic top.	$ip{:}P{:}R$	node	asym./sym.

  - and many others
  - including tool support
  - (no uniform input language)

Vision - Practical Protocol Engineering



(Research) Challenges

Probability

- AWN
  - extension with time available
  - probability would be useful

- applications
  - probabilistic protocols, e.g. CSMA (Carrier sense multiple access) protocol

- quantitative analysis
  - what’s the probability that a route is found in *n* time steps

Comparing Protocols

- so far protocols are compared by test-bed experiments (or simulations)
  - limited set of network topologies
  - contradicting results

- wishful: catalogue of formally defined protocol measurements
  - packet overhead
  - time until route is found ….

  - problem: depends on topology and mobility

Handling Topology

- Model Checking Approaches usually have to take the topology into account
  - often connectivity matrix or something alike

- How to systematically list/use all topology
  - use symmetries in topologies
  - can reduction techniques for “equivalent” nodes be used

- How to model mobility (link changes)
  - encode concrete mobility models
  - choose some mobile and some stationary nodes
    (how to list them systematically)
  - one approach by Fokkink allows arbitrary topologies (or a given size);
    but did require the development of a new model checking algorithm

Getting the Technology Out

- Great formalisms available
- today’s practice in industry differs a lot (cf. TORA spec)

- how do we convince industry to be more formal?
  (not necessary use of formal methods)

Q&A