Probabilistic Model Checking

Marta Kwiatkowska
Gethin Norman
Dave Parker

University of Oxford

Part 8 – PTA Case Studies

Overview

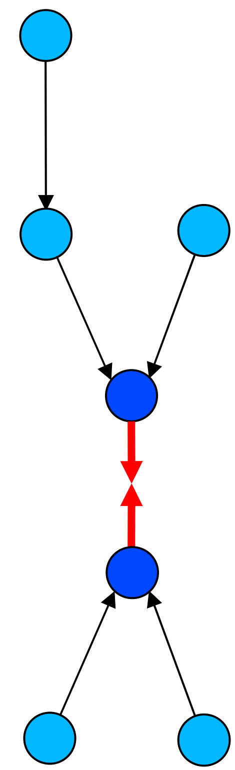
- Discuss two real-world protocol examples
  - modelled as probabilistic timed automata
  - quantitatively analysed with PRISM
  - compare experimental results (digital clocks, symbolic, sampling-based)

- IEEE 1394 FireWire root contention
  - randomised leader election protocol, widely used
  - confirmed a peculiarity…

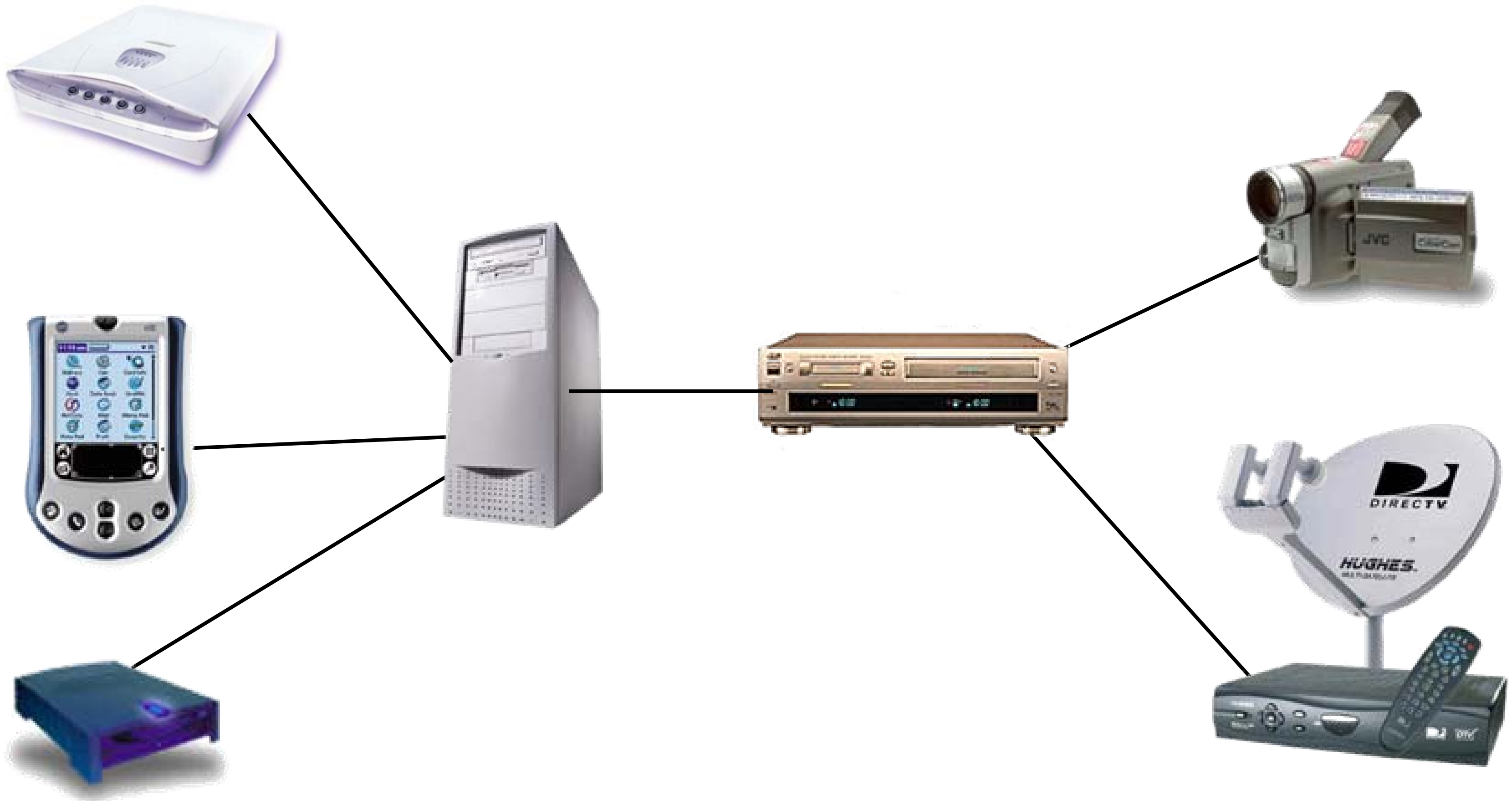
- IEEE 802.3 CSMA/CD
  - distributed network arbitration protocol
  - uses random backoff scheme, typical of Medium Access Control protocols

IEEE 1394 (FireWire) root contention

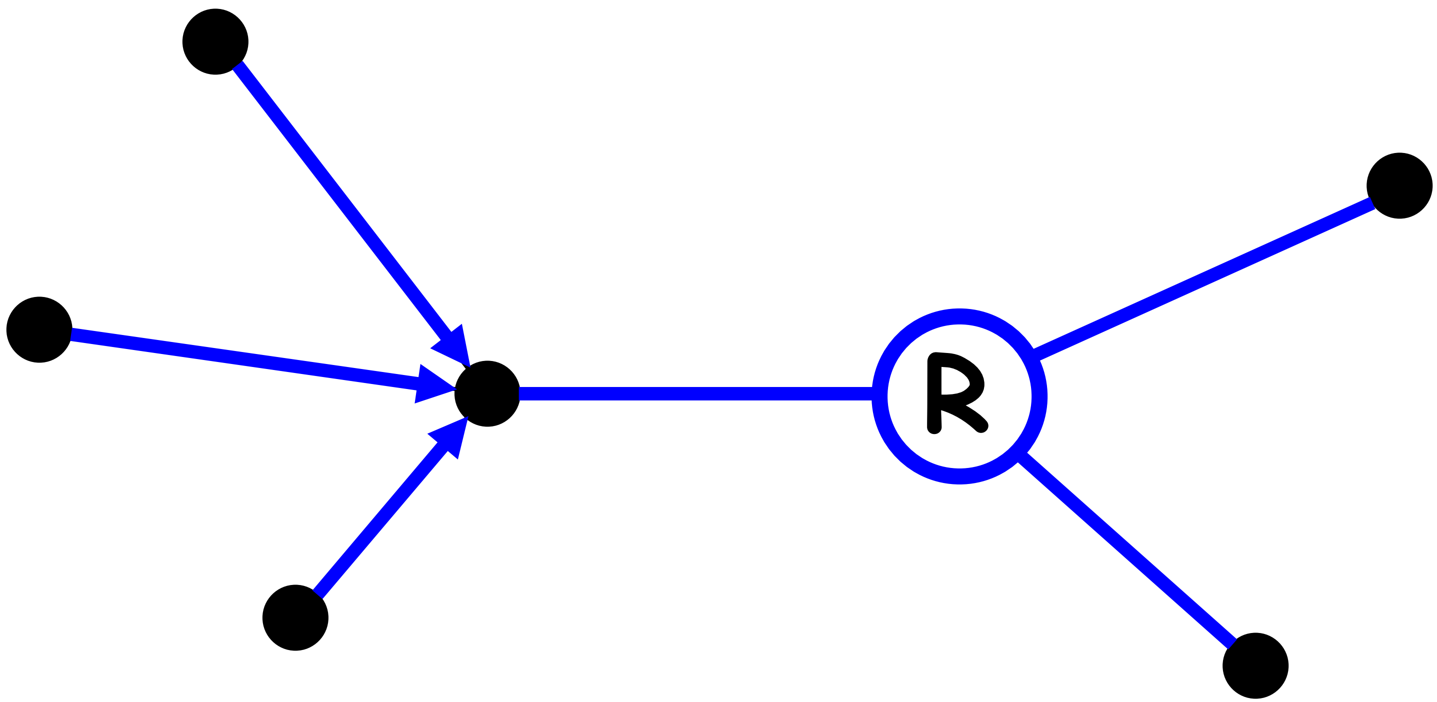
- Serial bus for networking multimedia devices
  - "hot-pluggable" - add/remove devices (nodes) at any time
- Root contention protocol
  - leader election algorithm, when nodes join/leave
  - nodes send messages: "be my parent"
  - root contention: when nodes contend leadership
  - random choice: "fast"/"slow" delay before retry
- Properties of interest
  - time taken for leader election
  - effect of using biased coin
  - conjecture [Sto02]



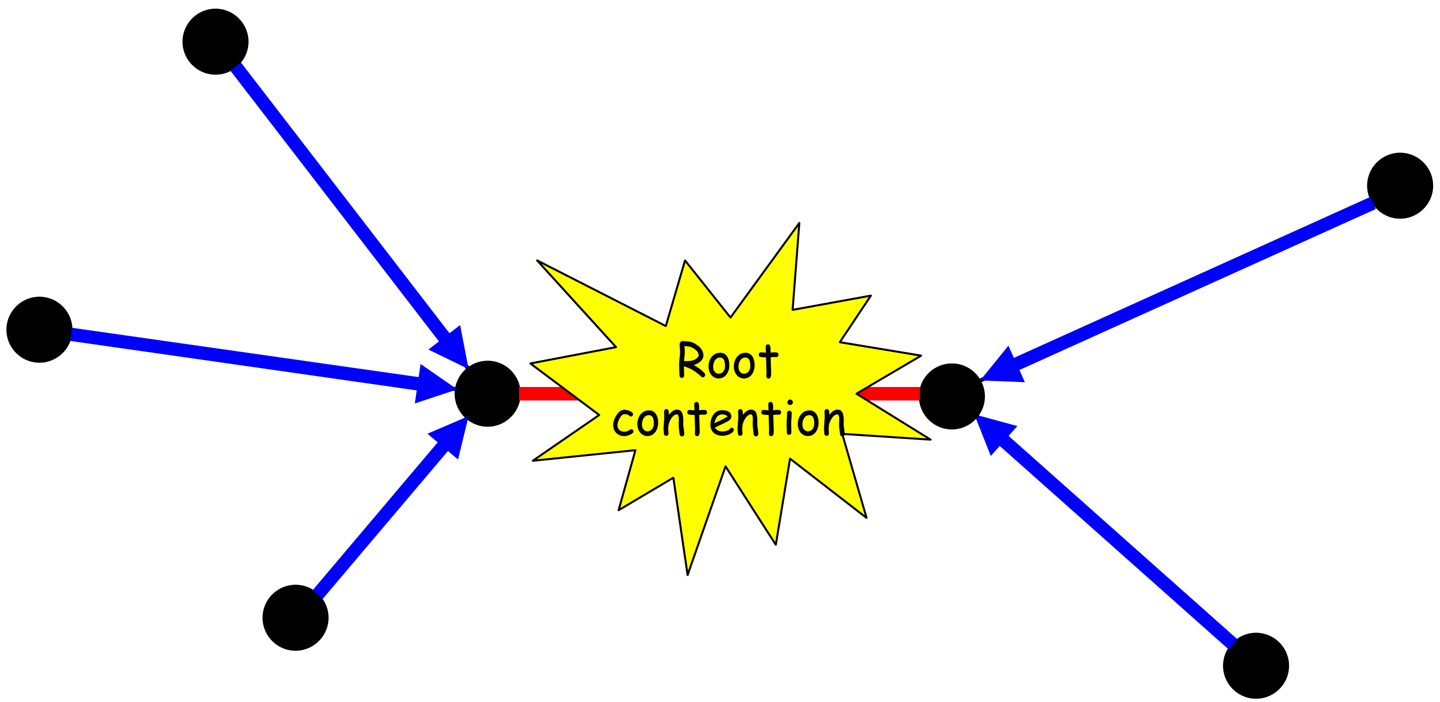
Typical FireWire configuration



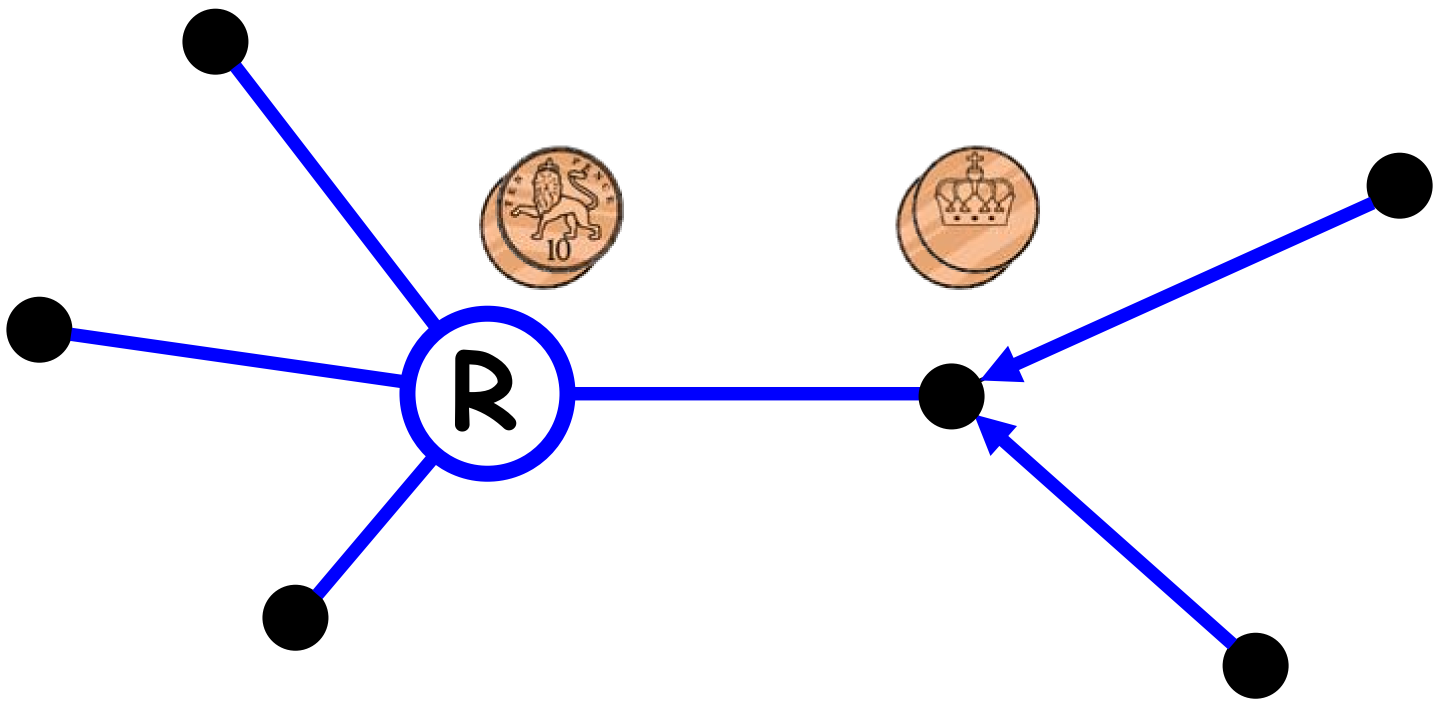
FireWire initial configuration



FireWire Root Contention



FireWire Root Contention

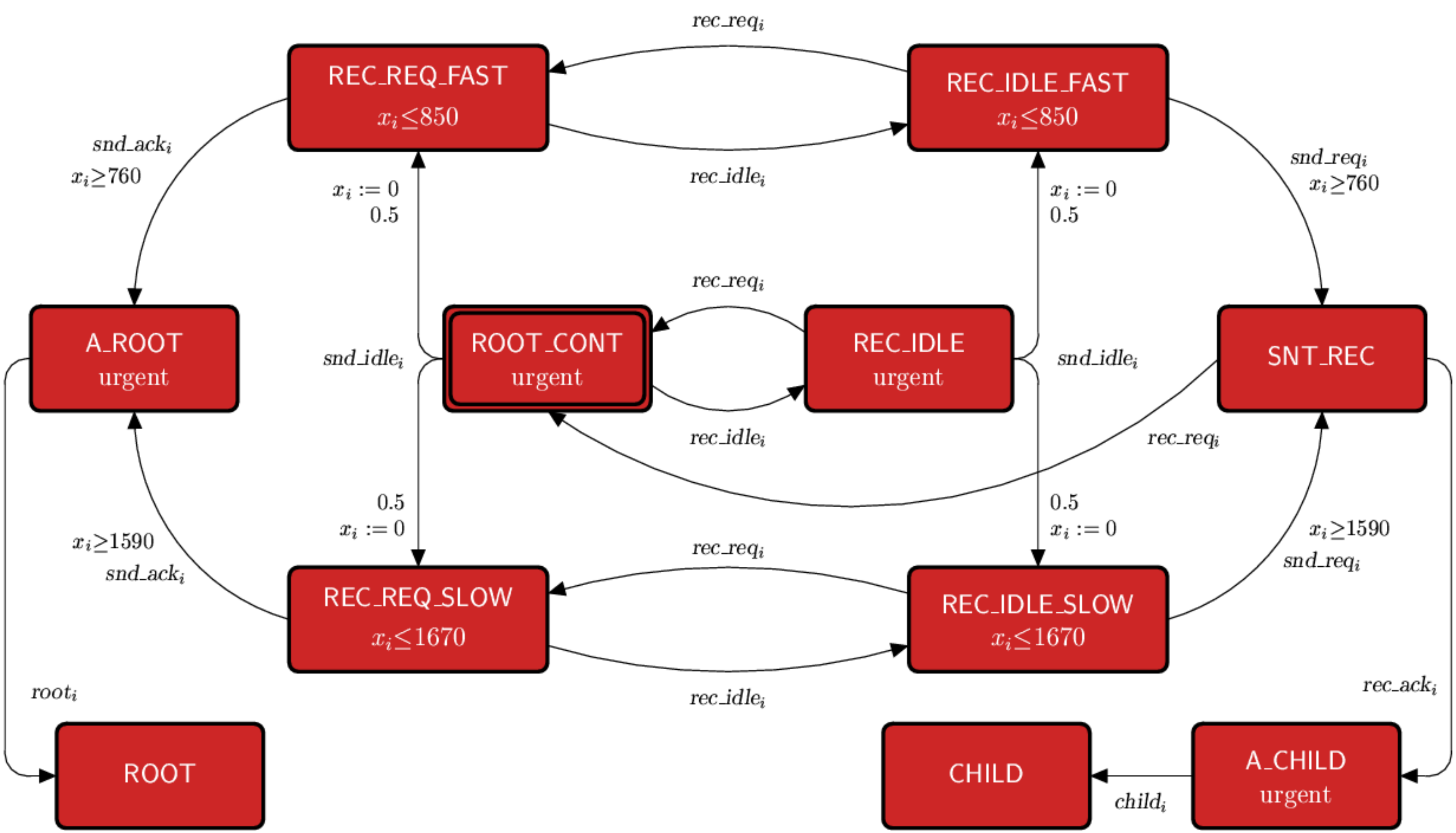


FireWire – PRISM model

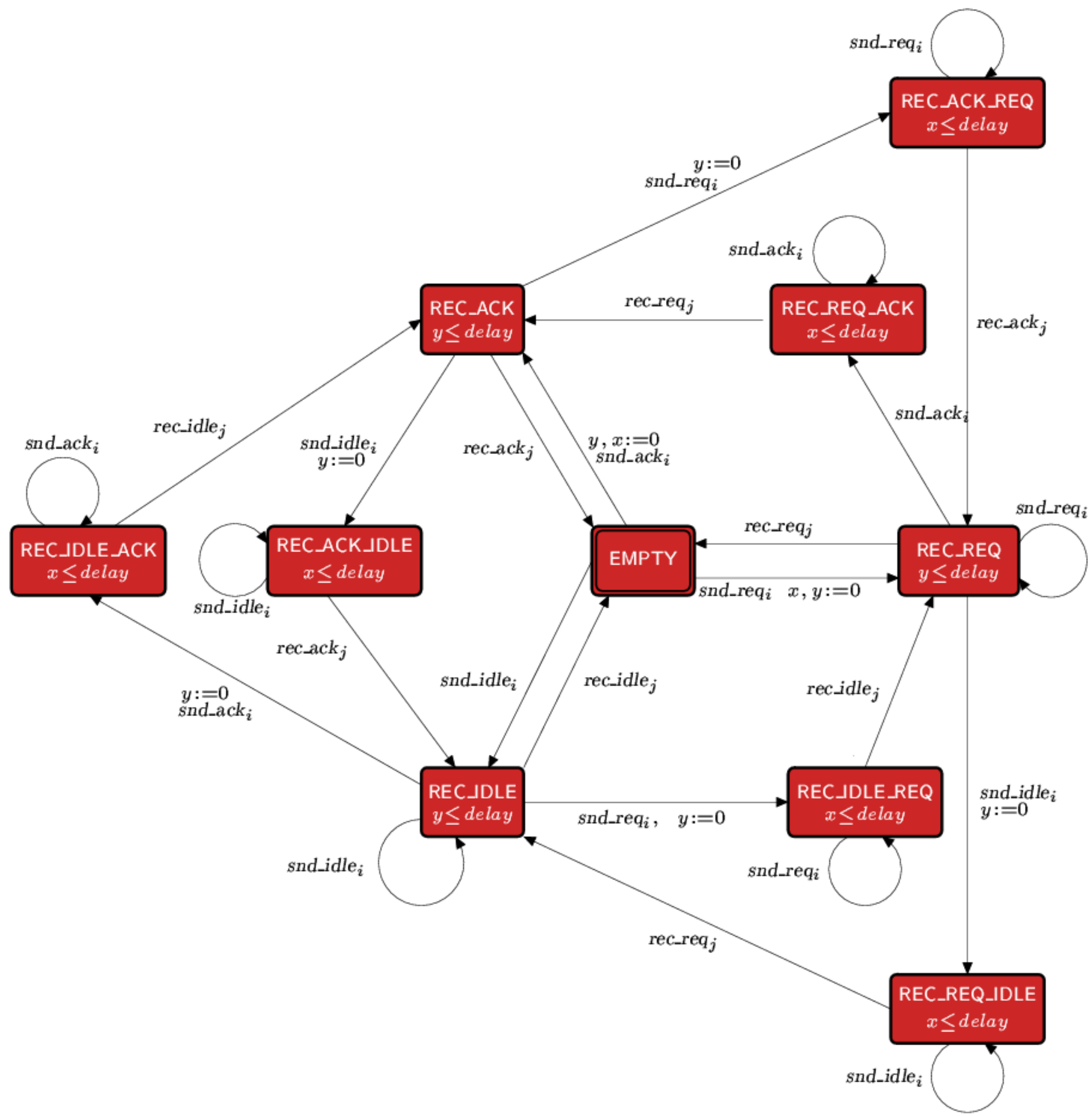
- Based on probabilistic timed automata (PTA) model
  - by Stoelinga et al. [SV99, SS01]
  - infinite state (real-time)
  - concurrency: messages between nodes and wires
  - underspecification of delays (upper/lower bounds)
  - probability: coin toss

- Applied three PTA model checking approaches
  - Symbolic forwards
  - Symbolic backwards
  - Digital clocks

FireWire – PTA model of a node



FireWire – PTA model of the wire

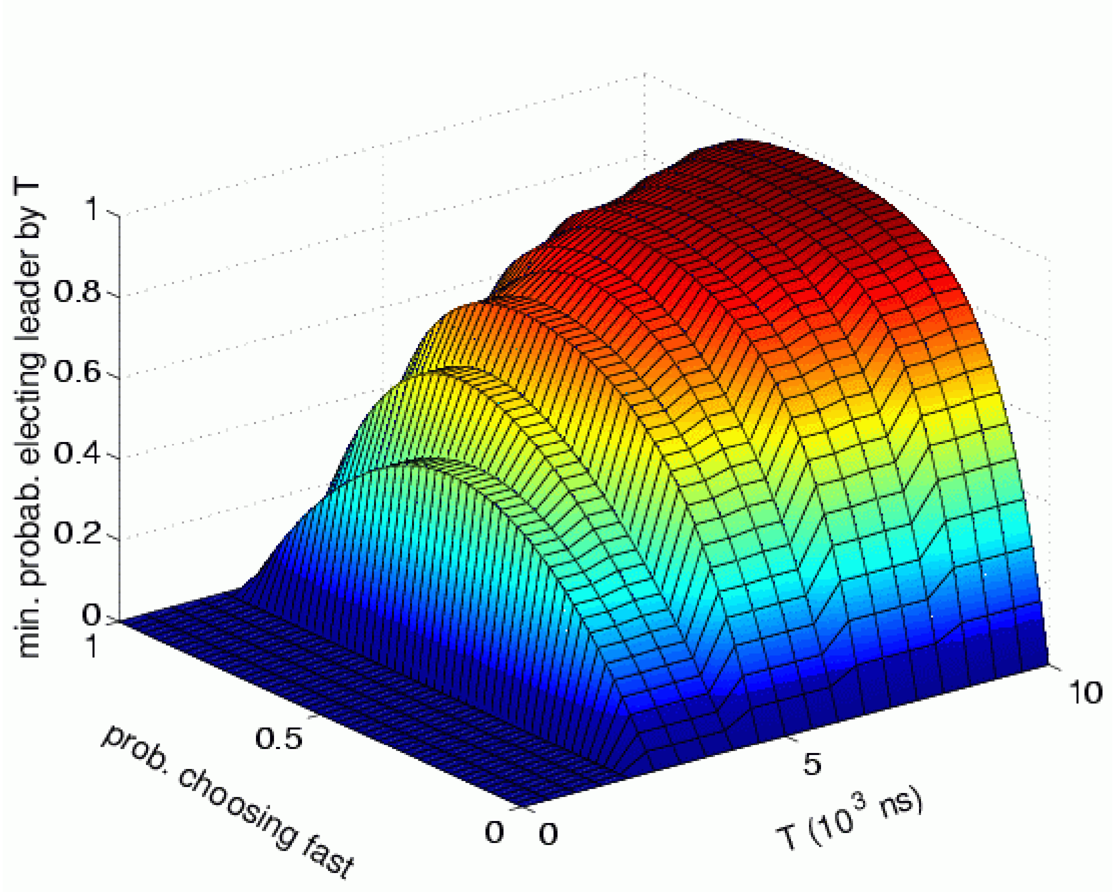


FireWire - Properties

- Minimum probability that a leader is elected by time T
  - $z.Pmin_{=?}$ [true U elected$\wedge z \leq T$]
  - vary: T, coin bias: probability of choosing "fast“
- Maximum expected time to elect a leader
  - add reward structure for elapsed time
  - assign reward one to each location
  - $Rmax_{=?}$ [F elected]
  - vary: coin bias
  - only the digital clocks is applicable

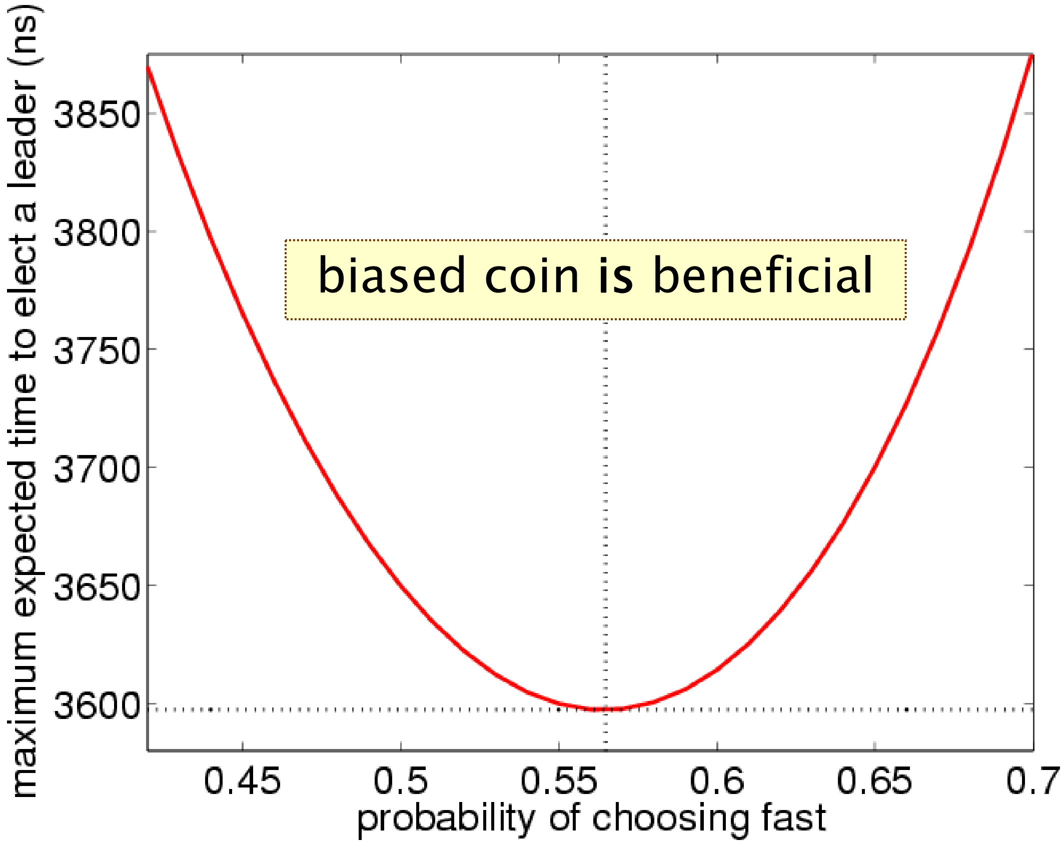
FireWire - Results

- Minimum probability of electing leader by time T
  - z.Pmin$_{=?}$ [true U elected$\wedge z \leq T$]



FireWire – Results

- Maximum expected time to elect a leader
  - $Rmax_{=?}$ [F elected]



FireWire – Number of states

time bound	backwards		forwards		digital clocks	
	states	size (KB)	states	size (KB)	states	size (KB)
2	1,219	7.24	825	18.9	80,980	554
4	4,844	30.6	2,329	35.2	434,364	730
6	10,981	55.0	3,833	51.9	1,093,658	860
8	–	–	6,841	74.1	1,915,291	875
10	–	–	9,661	90.1	2,746,691	875
20	–	–	35,041	204	6,903,691	890

FireWire - Computation time

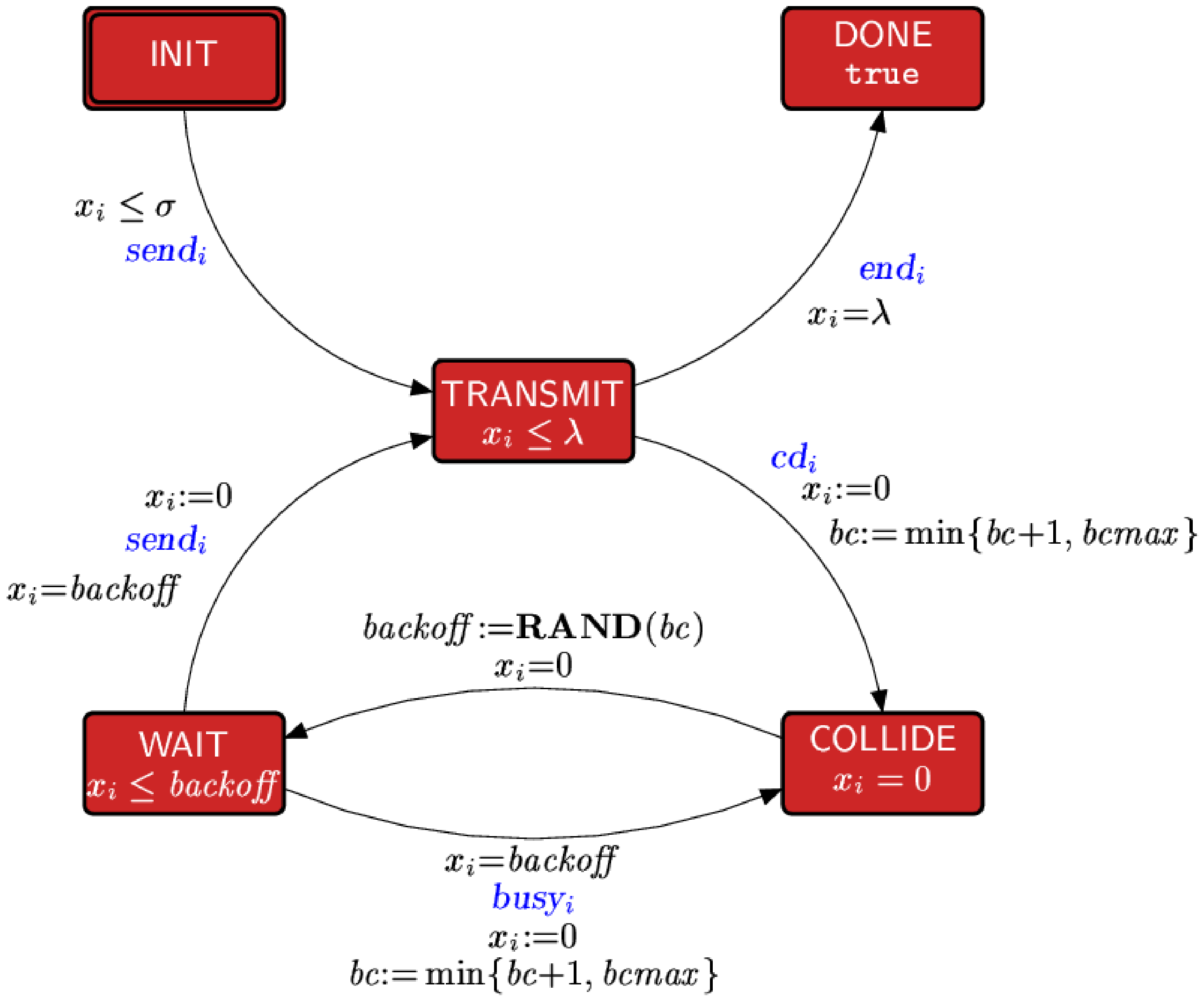
time bound	backwards		forwards		digital clocks	
	construct.	m/c	construct.	m/c	construct.	m/c
2	544+33.0	0.10	0.4+0.6	0.38	10.2	7.8
4	26,992+753	0.34	0.9+2.0	0.80	38.3	43
6	618,493+4,388	1.3	1.6+3.7	1.4	85.8	145
8	–	–	2.9+10	1.6	145	228
10	–	–	4.2+20	2.5	205	335
20	–	–	18+226	5.1	549	469

Experimental results: CSMA/CD

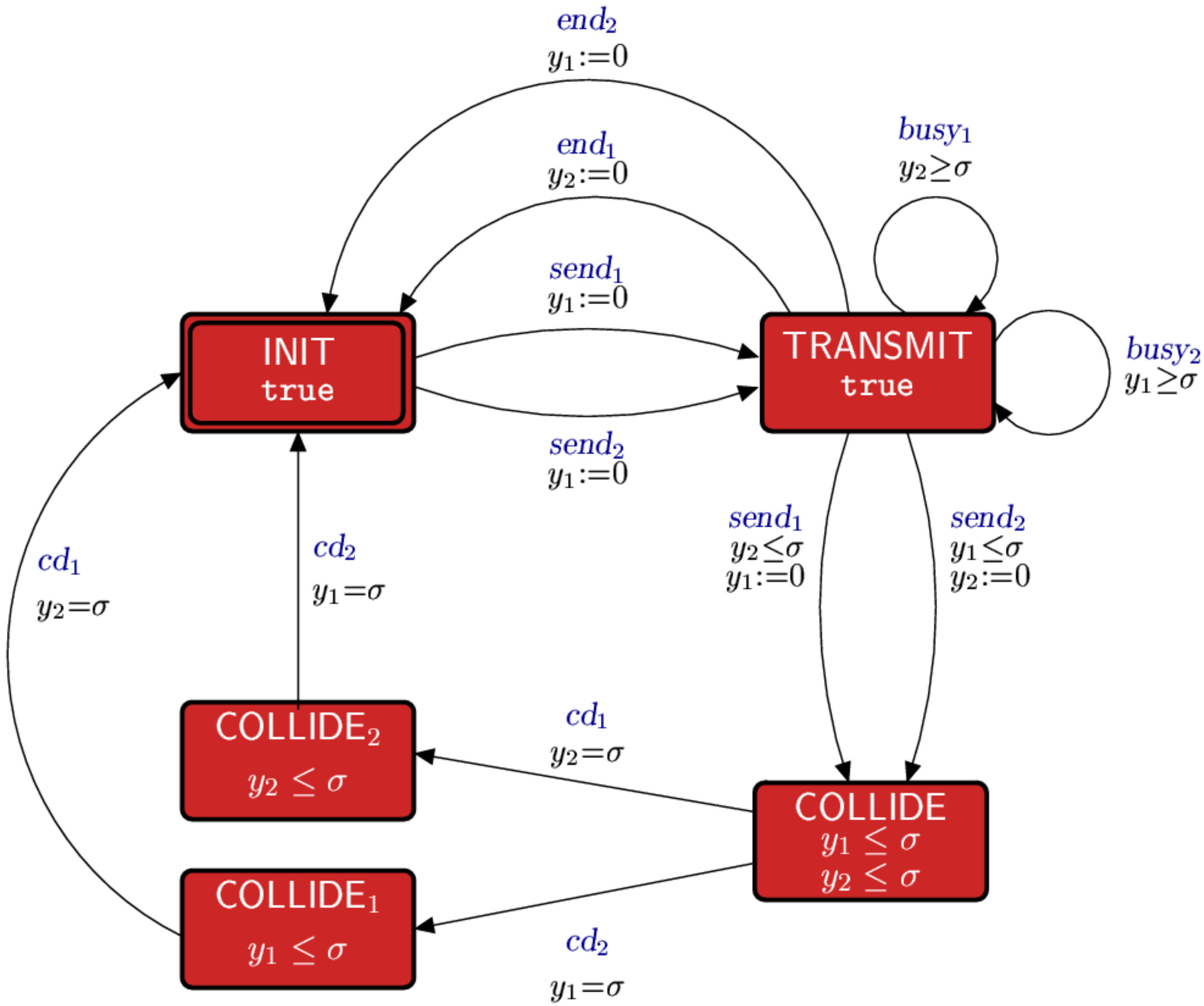
- IEEE 802.3 CSMA/CD (Carrier Sense, Multiple Access with Collision Detection)
  - model of [NSY92], without probabilities
  - when a station has data to send, it listens to the medium
  - if the medium was free (no one transmitting), the station starts to send its data
  - if the medium was sensed busy, the station waits a random amount of time and then repeats this process

- Exponential backoff scheme
  - wait for a random delay between $0,\ldots,2^k-1$
  - where k counts number of collisions up to a bound K

CSMA/CD – PTA model of a station

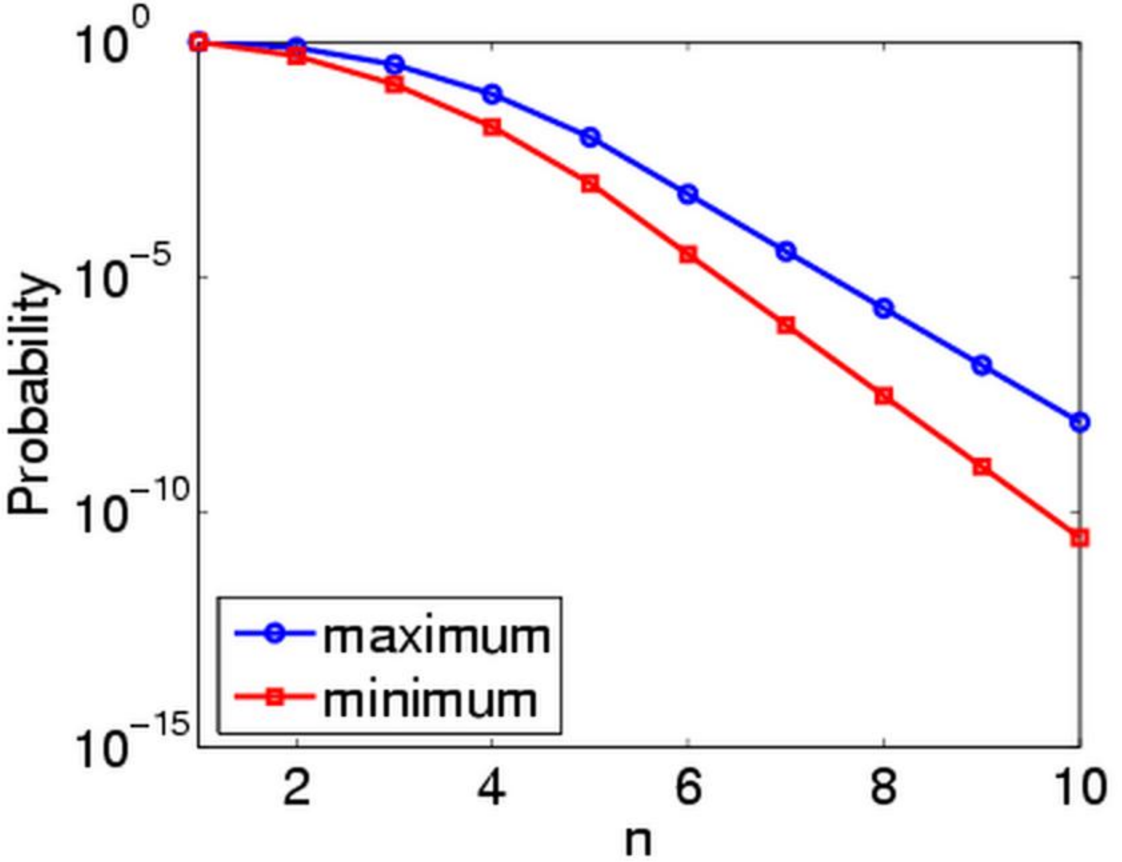


CSMA/CD – PTA model of the medium



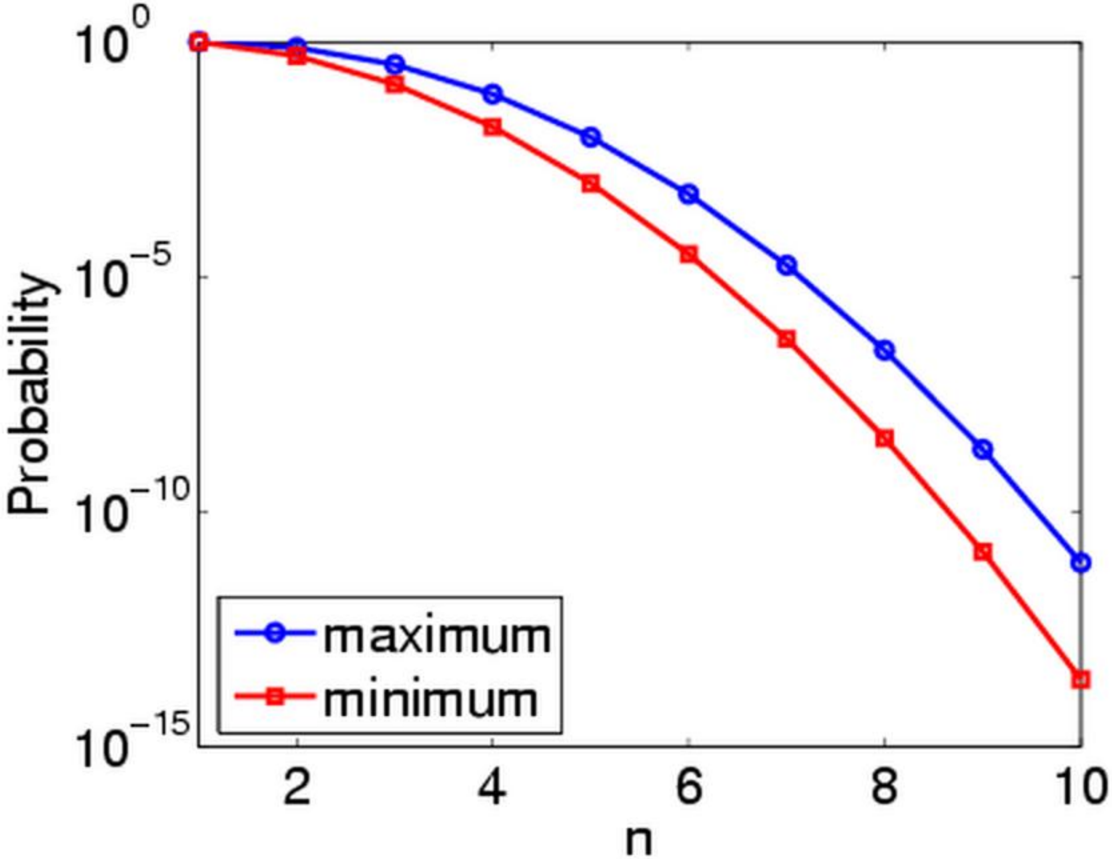
CSMA/CD –Results

- Probability n collisions before a packet is sent (K=5)
  - $P_{=?}$ [true U (collisions≥n ∧ unsent)]



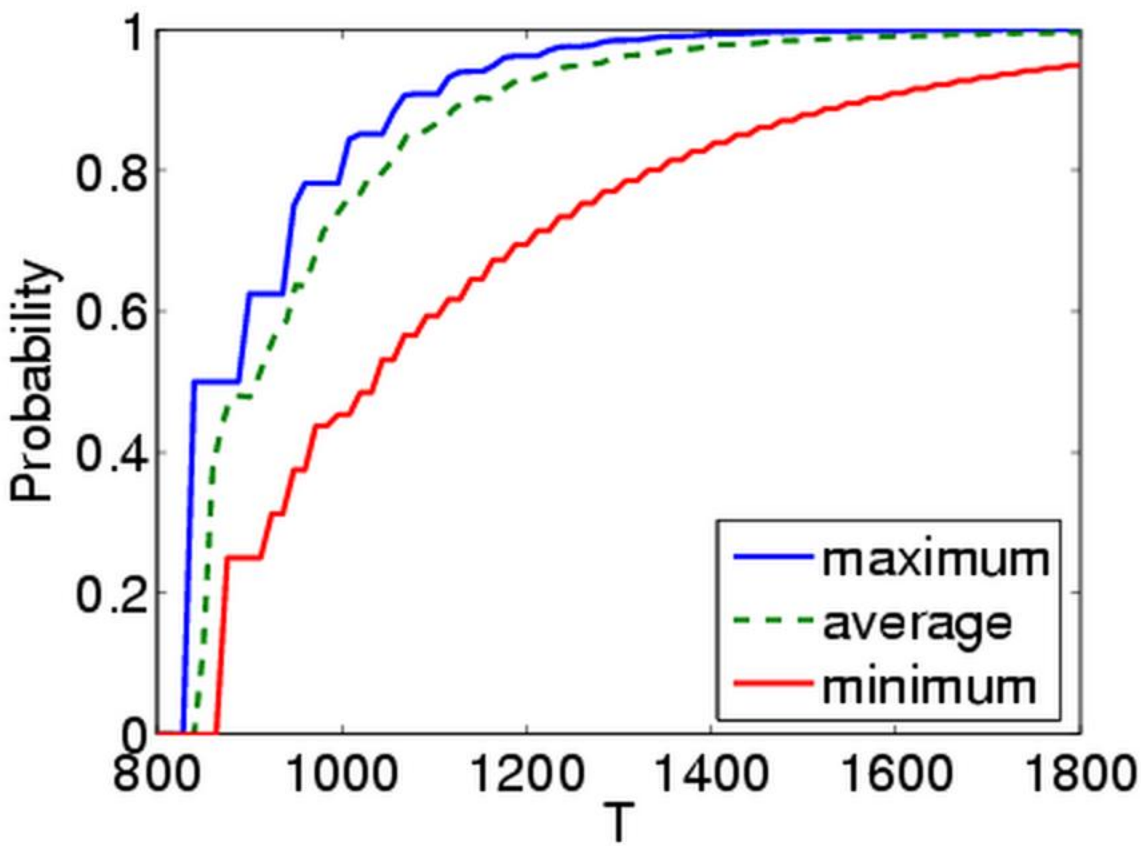
CSMA/CD –Results

- Probability n collisions before a packet is sent (K=10)
  - $P_{=?}$ [true U (collisions$\geq$n $\wedge$ unsent)]



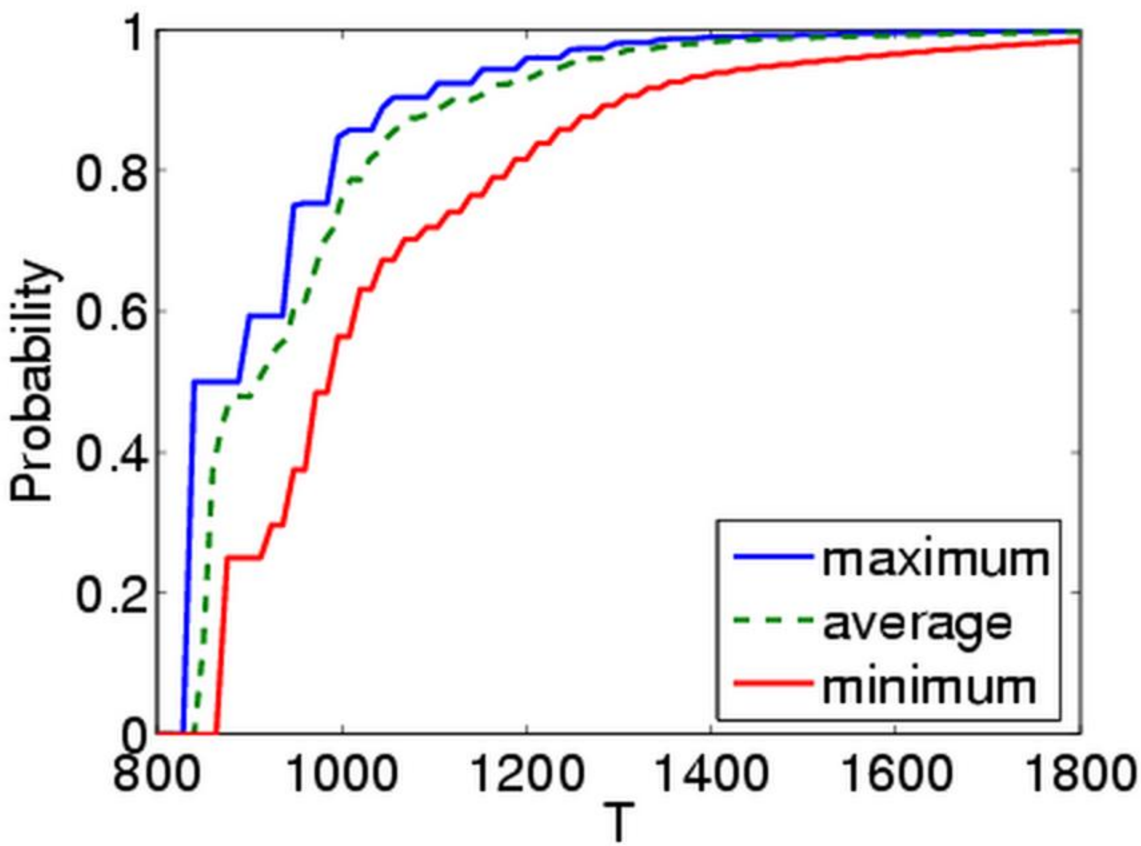
CSMA/CD –Results

- Probability packet is sent before time T (K=5)
  - $z.P_{=?}$ [true U ($z \leq T \wedge$ sent)]



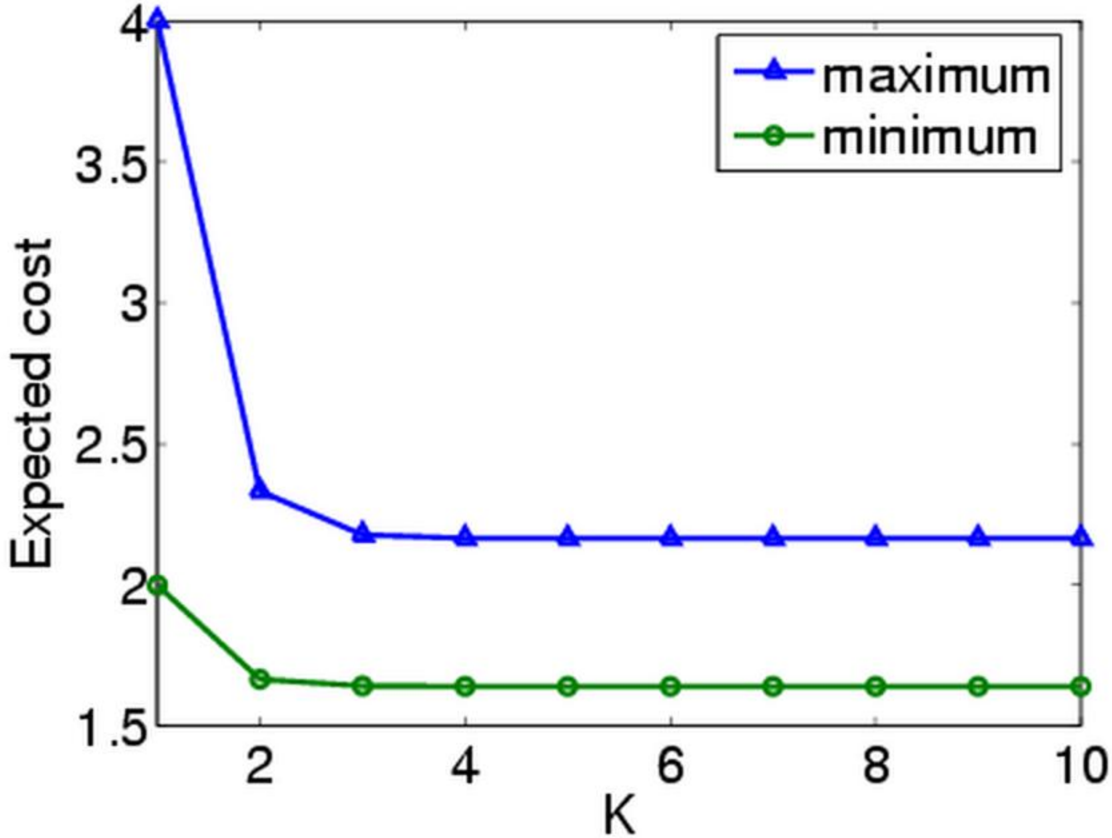
CSMA/CD –Results

- Probability packet is sent before time T (K=10)
  - z.$P_{=?}$ [true U (z≤T ∧ sent)]



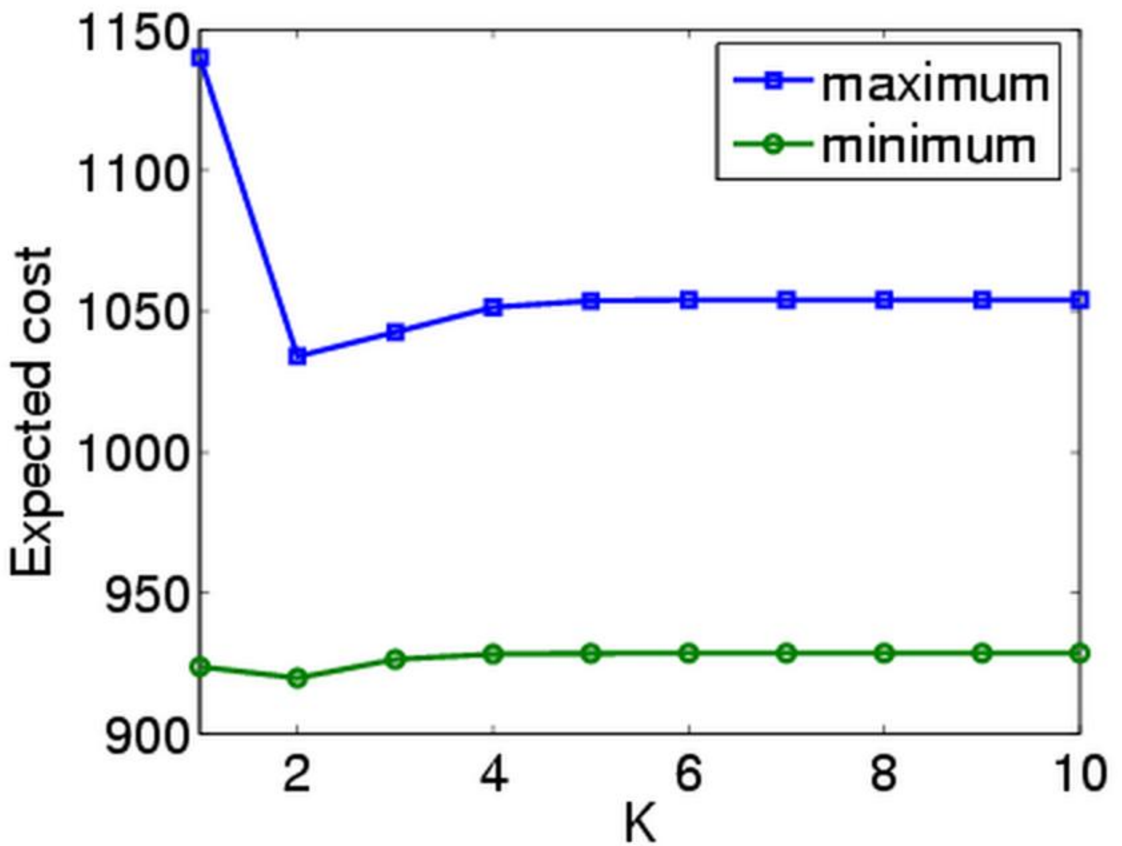
CSMA/CD –Results

- Expected number of collisions before a packet is sent
  - $R_{=?}$ [F sent]



CSMA/CD –Results

- Expected time until a packet is sent
  - $R_{=?}$ [F sent]



Summing up…

- What have we achieved?

- Probabilistic timed automata
  - appropriate model for distributed coordination protocols that use randomisation

- Developed a methodology for quantitative analysis and verification
  - theory of probabilistic model checking: symbolic, digital clocks, sampling-based
  - resource usage and expectations
  - implementation of the techniques and experimental results

Further information

- More on FireWire root contention
  - see [KNS03b,KNPS06,KNSW07]
- More on CSMA/CD
  - see [DKN+06]

- More on similar protocols
  - 802.11 WiFi [KNS03b]
  - IPv4 Zeroconf [KNS03b]
  - 802.15.4 Zigbee [Fru06]

- More information, see the PRISM web page

  www.prismmodelchecker.org