

Probabilistic Model Checking of Contention Resolution in the IEEE 802.15.4 Low-Rate Wireless Personal Area Network Protocol

Matthias Fruth

School of Computer Science
University of Birmingham

Dagstuhl-Seminar
Quantitative Aspects of Embedded Systems
4-9 March 2007

Outline

The protocol

- Low-rate wireless personal area networks
- Contention resolution
- CSMA-CA

Probabilistic model checking

- Definitions
- PRISM: Probabilistic Symbolic Model Checker
- Probabilistic timed automata
- Probabilistic model checking of probabilistic timed automata

Modelling

- Network configuration and modelling assumptions
- Probabilistic timed automata models

Verification and results

Summary and future work

Low-rate wireless personal area networks

Definition

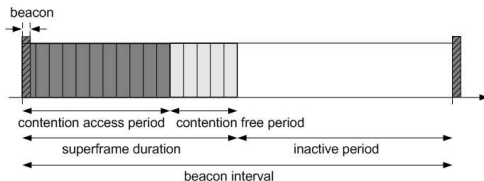
- ▶ **short range** (10 metres radius) wireless networks
- ▶ devices of **low power**, **low data rates**, and **low complexity**

Standards

- ▶ **IEEE 802.15.4** (2003) for lower network layers
- ▶ **ZigBee** (2005) for upper network layers

Optional beacon synchronisation

- ▶ requires a **superframe structure**



- ▶ **guaranteed timeslots** in the **contention free period**
- ▶ optional **battery life extension**

Contention resolution

Problem

- ▶ more than one station attempts to transmit data at nearly the same time \rightsquigarrow collision

Contention resolution mechanism

- ▶ carrier-sense multiple access (CSMA)
 - ▶ with collision detection (CD) – for wired networks
 - ▶ with collision avoidance (CA) – for wireless networks

Contention resolution protocols

- ▶ CSMA/CD – for IEEE 802.3 Ethernet
- ▶ CSMA/CA – for IEEE 802.11 WLAN
- ▶ CSMA-CA – for IEEE 802.15.4

CSMA-CA

Idea

- ▶ before transmitting a frame, a sending station has to wait for a random time which is called **backoff**

Protocol

1. initialise **backoff exponent** BE (default 3)
2. **backoff**: wait for a random time between 0 and $2^{BE} - 1$ backoff periods
3. **clear channel assessment**
4. channel busy
 - ▶ $BE := BE + 1$ (up to given maximum)
 - ▶ maximum number of backoffs exceeded \rightsquigarrow **failure**
 - ▶ maximum number of backoffs not exceeded \rightsquigarrow **back to (2)**
5. channel free \rightsquigarrow **transmission**

Probabilistic model checking

Definition

- ▶ formal method for the automatic verification of probabilistic systems

Probabilistic models

- ▶ discrete-time Markov chains (DTMCs) – discrete time, det.
- ▶ continuous-time Markov chains (CTMCs) – cont. time, det.
- ▶ Markov decision processes (MDPs) – discrete time, nondet.
- ▶ prob. timed automata (PTAs) – cont. time, nondet.

Probabilistic temporal logics

- ▶ prob. computation tree logic (PCTL) – for DTMCs/MDPs
- ▶ continuous stochastic logic (CSL) – for CTMCs
- ▶ prob. timed computation tree logic (PTCTL) – for PTAs

PRISM: Probabilistic Symbolic Model Checker

Software

- ▶ probabilistic model checking tool
- ▶ developed at the University of Birmingham since 1999
- ▶ free, open source; for Linux, Unix, Mac OS, Windows

Supported models

- ▶ DTMCs, CTMCs, and MDPs
- ▶ PTAs with digital clocks by manual translation
- ▶ augmented by costs/rewards

Supported specification languages

- ▶ PCTL and CSL
- ▶ extension for quantitative properties
- ▶ extension for costs/rewards

More information

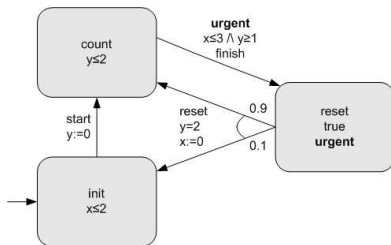
- ▶ PRISM website (publications, case studies, tutorials, etc):
<http://www.cs.bham.ac.uk/~dxp/prism/>

Syntax of PTAs

Syntax

$$\text{PTA} = (L, \bar{l}, \mathcal{X}, \Sigma, \text{inv}, \text{prob})$$

- ▶ finite set of **locations** L
- ▶ **initial location** $\bar{l} \in L$
- ▶ finite set of **clocks** \mathcal{X}
 - ▶ for a clock $x \in \mathcal{X}$ and an integer c , the **atomic clock constraints** are $x \leq c$, $x = c$, and $x \geq c$
 - ▶ set of **clock constraints** $\mathcal{C}(\mathcal{X})$, that is, conjunctions of atomic clock constraints
- ▶ finite sets of **events** Σ and **urgent events** $\Sigma_u \subseteq \Sigma$
- ▶ **invariant condition** $\text{inv} : L \rightarrow \mathcal{C}(\mathcal{X})$
- ▶ **prob. transition relation** $\text{prob} \subseteq L \times \mathcal{C}(\mathcal{X}) \times \Sigma \times \text{Dist}(2^{\mathcal{X}} \times L)$



Semantics of PTAs

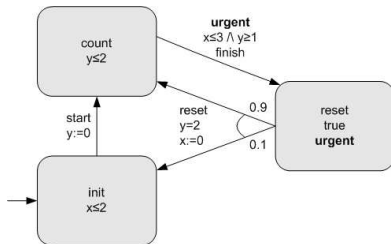
Transitions

▶ delay transitions

- ▶ elapsing of time in a location
- ▶ permitted as long as invariant condition satisfied and no transitions under urgent events enabled

▶ event transitions

- ▶ execution of a probabilistic transition $(l, g, \sigma, p) \in \text{prob}$
- ▶ permitted if current location is l , current event is σ , and clock constraint g is satisfied
- ▶ then $p((X', l'))$ is the probability of resetting all clocks in X' to 0 and moving to location l'



Higher-level features

- ▶ **urgent locations** (to be left without time elapsing)
 - ▶ modelled using an additional clock
[Daws & Yovine 1995, Tripakis 1999]
- ▶ **integer variables with bounded ranges**
 - ▶ represented by encoding their values within locations
[Tripakis 1998]

Probabilistic model checking of PTAs

Properties

- ▶ expressed in **PCTL with costs/rewards**
- ▶ **probabilistic reachability** properties
e.g. “What is the probability that there are at most 4 collisions?”
- ▶ **expected reachability** properties
e.g. “What is the maximum number of collisions?”

Available approaches

- ▶ region equivalence: prohibitively large state spaces
- ▶ forward reachability: approximate results
- ▶ backwards reachability: not for expected reachability
- ▶ **digital clocks**

Digital clocks

Digital clocks approach

- ▶ **dense-time semantics** (real-valued time) uncountable
- ▶ **integral-time semantics** (integer-valued time)
[Kwiatkowska, Norman, Parker, Sproston 2006]
 - ▶ modified increment operation: $v \oplus_{\mathbb{N}} t \stackrel{\text{def}}{=} \min\{v(x) + t, k_x + 1\}$
where k_x is the largest value x is compared to
 - ▶ finite representation as **Markov decision process**
 - ▶ preserves **prob. reachability** and **expected reachability**
 - ▶ often leads to very large state spaces
- ▶ **timescale abstraction** [Alur, Itai, Kurshan, Yannakakis 1995]
 - ▶ dividing all values constants by a new time unit, then rounding lower/upper bounds down/up
 - ▶ maximum/minimum probability measures are upper/lower bounds of those for the original model
- ▶ **compositionality property**
 - ▶ parallel composition of PTAs can be modelled as the parallel composition of their MDPs

Network configuration and modelling assumptions

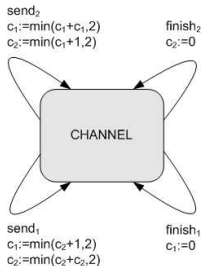
Network configuration

- ▶ sending stations s_1 and s_2 , receiving stations r_1 and r_2
- ▶ each sending station s_i intends to send a single data frame to its corresponding receiving station r_i , using CSMA-CA
- ▶ both stations start sending at the same time

Modelling assumptions

- ▶ **destination stations incorporated into sending stations**, as the former have deterministic behaviour [Kwiatkowska, Norman, Sproston 2002]
- ▶ **ideal channel**: messages do not get lost, no PAN conflicts, no synchronisation problems
- ▶ **vulnerable period**: $VULN \stackrel{def}{=} CCA + aTurnaroundTime$ for unslotted mode (adaptation of [Heindl & German 2001])

Probabilistic timed automaton model for the channel



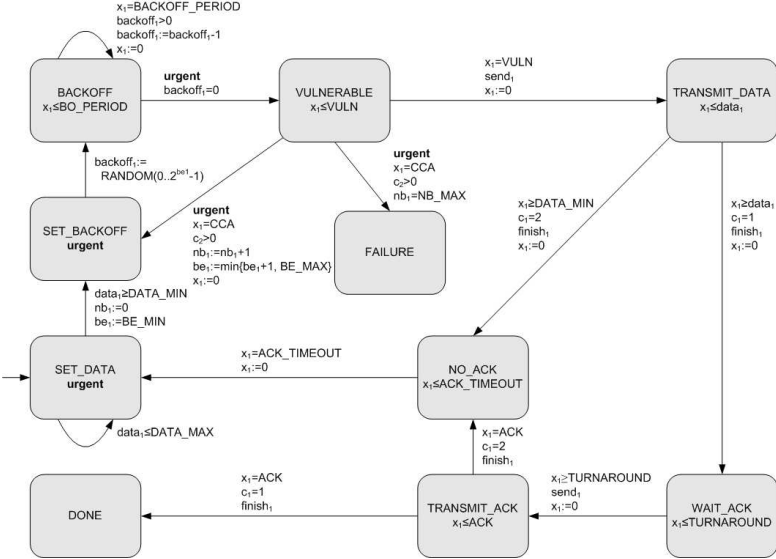
Events

- ▶ $send_i$ – station i starts sending
- ▶ $finish_i$ – station i finishes sending

Collisions

- ▶ integer variable c_i corresponds to frames sent by station i
 - ▶ 0 – nothing being sent
 - ▶ 1 – frame being sent correctly
 - ▶ 2 – frame being sent garbled

Probabilistic timed automaton model for a station



Performance and accuracy of model abstractions

Assumptions

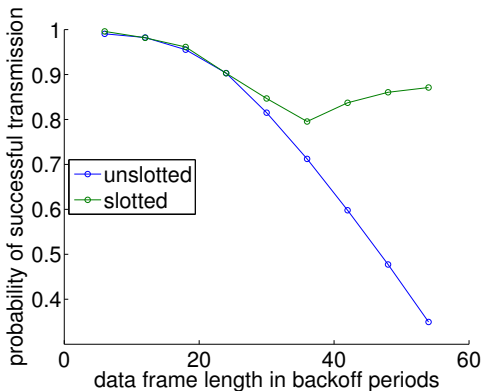
- ▶ 20 kbit/s channel
- ▶ transmissions without acknowledgement
- ▶ maximum number of backoffs set to infinity
- ▶ macBeaconOrder=1, macSuperframeOrder=1 for slotted mode

| data frame length | time unit | min. exp. no of collisions | | | min. exp. time | | |
|-------------------|-----------|----------------------------|-----------|--------|----------------|-----------|----------|
| | | nodes | min-terms | result | nodes | min-terms | result |
| <i>unslotted</i> | | | | | | | |
| fixed | 4 | 22k | 120k | 0.125 | 93k | 210k | 112.8 ms |
| nondet | 4 | 180k | 960m | 0.125 | 280k | 1.6bn | -(2 GB) |
| fixed | 20 | 6.9k | 13k | 0.125 | 10k | 17k | 123.1 ms |
| nondet | 20 | 56k | 19m | 0.125 | 83k | 26m | 123.1 ms |
| <i>slotted</i> | | | | | | | |
| fixed | 20 | 29k | 27k | 0.125 | 45k | 67k | 166.0 ms |
| nondet | 20 | 1m | 130m | 0.125 | 1.6m | 180m | 166.0 ms |

Probability for successful transmission

Assumptions

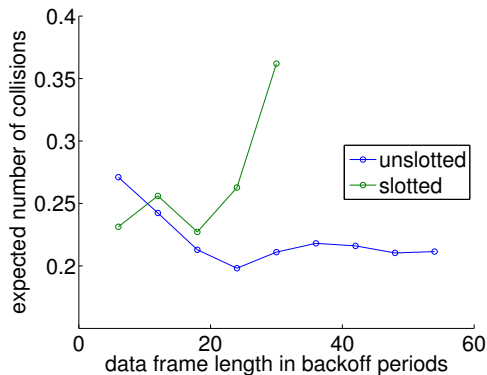
- ▶ 20 kbit/s channel
- ▶ transmissions with acknowledgement
- ▶ macBeaconOrder=1, macSuperframeOrder=1 (slotted mode)
- ▶ beacon frame length set to minimum value (slotted mode)
- ▶ CAP length set to maximum value (slotted mode)
- ▶ timescale abstraction: 20 symbol periods



Expected number of collisions until successful transmission

Assumptions

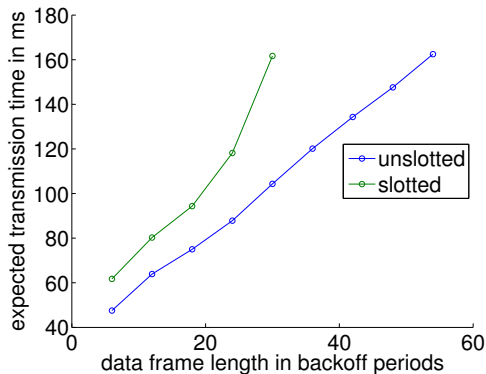
- ▶ 20 kbit/s channel
- ▶ transmissions with acknowledgement
- ▶ maximum numbers of backoffs and of retransmissions set to infinity
- ▶ macBeaconOrder=1, macSuperframeOrder=1 (slotted mode)
- ▶ beacon frame length set to minimum value (slotted mode)
- ▶ CAP length set to maximum value (slotted mode)
- ▶ timescale abstraction: 20 symbol periods



Expected time until successful transmission

Assumptions

- ▶ 20 kbit/s channel
- ▶ transmissions with acknowledgement
- ▶ maximum numbers of backoffs and of retransmissions set to infinity
- ▶ macBeaconOrder=1, macSuperframeOrder=1 (slotted mode)
- ▶ beacon frame length set to minimum value (slotted mode)
- ▶ CAP length set to maximum value (slotted mode)
- ▶ timescale abstraction: 20 symbol periods



Summary

- ▶ **First application of probabilistic model checking to IEEE 802.15.4/ZigBee**
 - ▶ small models with realistic behaviour
 - ▶ interesting performance properties
- ▶ **Modelling task more difficult** than for previous contention resolution protocols
 - ▶ this model includes beacon synchronisation
 - ▶ timing constraints for backoff procedure more intricate
 - ▶ timescale abstraction technique has been extended to sequences of delays
- ▶ **Generic and parametric model**
 - ▶ generic model includes almost all timing parameters
 - ▶ individual models can be constructed from generic model by enabling/disabling features such as acknowledgement, backoff limit, retransmission limit on demand

Future work

Future work

- ▶ development and application of new techniques for state-space reduction, symbolic representation, and compositional reasoning (PRISM project, University of Birmingham)
- ▶ development of a high-level description framework for wireless sensor networks (PEWNA project, National ICT Australia)

More information

- ▶ PRISM website:
<http://www.cs.bham.ac.uk/~dxp/prism/>
- ▶ PEWNA website:
<https://www.cse.unsw.edu.au/~ansgar/pewna/>