Modeling PGM: From huge code to smaller models for relevant properties

Marc Boyer

LIAFA - Univ. Paris 7 - France

Work done

VERIMAG IF 2.0 Spec [VerIF]

- the translation of the SDL version from FT, in IF 2.0, have been commented (Join work from LIAFA & VERIMAG)
  available at
  `http://liafa.jussieu.fr/~haberm/ADVANCE/main`
- too “huge” to be handled:
- written in IF 2.0

⇒ need to write from the scratch smaller models

IETF draft [DRAFT]

- natural language
- 116 pages
- no details about the data structure
- few details about the underlying network

⇒ an abstract automata in pseudo-IF

Differences [VerIF] [DRAFT]

- No `NAK` filtering in nodes
- `NAK` policy in node and receiver different
- Receiver must receive a SPM as first message
- Reset `IHB_TMR` once `IHM_MAX` overtaken
- Enhancement of the window advance anticipation
  $\Rightarrow$ add of a `spm_inc` in SPM packets
- No communication delay

Properties to be verified

Basic tests

Just designed to test if the modeling is not 'too bugged'

- **Finite memory need:**

$$\texttt{TXW\_LEAD} - \texttt{TXW\_TRAIL} \leq k$$

$$\texttt{RXW\_LEAD} - \texttt{RXW\_TRAIL} \leq k$$

$$\text{number of } \texttt{NAK} \text{ states in each node} \leq k'$$

$$\text{number of } \texttt{NAK} \text{ states in each receiver} \leq k''$$

- **No time lock**

The property

A receiver in the group either receives all data packets from transmissions and repairs, or is able to detect unrecoverable data packet loss.[DRAFT]

Other properties (1/2)

Protocol efficiency:

- **Under which assumption are all losses recovered?**
- **Synthesis of parameters ?**

Protocol load:

- **How many useless `RDATA`?**
- **Are `NAK` filtered? (if filtering is on)**
- **number of `NAK` received by the source (compared to number of receivers and nodes)**

Other properties (2/2)

Flow control:

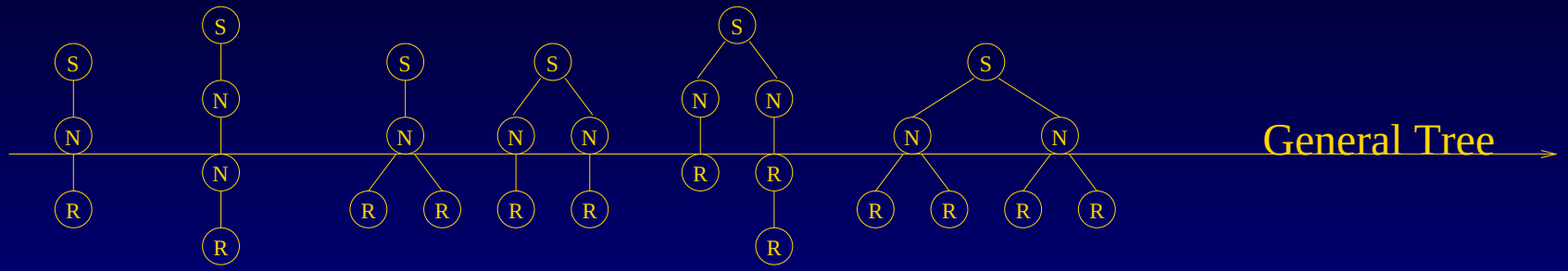
- **no (or few) loss in buffers**

Circular sequence number space:

- 2^{31} **can only be checked using abstraction...**

Complexity dimensions (1/3)

Architecture:



Policy of loss:

1 fixed loss — 1 random loss — 1 loss per window — N over M

ODATA — NACK — RDATA — NCF

Buffers:

1−buffer — 1−buffer + delay — N−bouded buffer — unbounded buffers

(+delay)

Complexity dimensions (2/3)

Transmission length:

Few messages — 1 window — 2 windows — 3 windows — infinite

Data flow:

Generator rate = bandwith — Generator rate >> bandwith — Generator rate << bandwith — Bursty generator rate — Random generator rate

Joining:

All members from the start — Late Join — Random Join/Quit

Complexity dimensions (3/3)

- Adding/Removing mechanisms:
  - Complex NAK generation
    (2-3 states based + random)
  - Heartbeat SPM
  - NAK filtering
- Implementation choices:
  - Ambient SPM rate
  - Window advance

Abstraction

- Un-timed version:

  but time-triggered protocol

  - periodic ambient SPM as discrete time
  - bounded buffers + blocking writing $\Rightarrow$ some time-progress

- Undeterministic:
  - do not store messages numbers
  - send randomly some messages

  $\Rightarrow$ which kind of property preserved

Configuration comparisons

Scalability of the protocol ? How is the load for the source ?

- **Same behavior for one or two receivers ?**
- **Same behavior for one or two network nodes ?**
- **...**

Work under progress

very-simple-pgm.if

- 1 source – 1 network node – 1 receiver
- 1 ODATA loss
- 1-bounded buffer (without delay)
- no heartbeat
- no NAK filtering in nodes
- 1-state NAK repeat rate
- no NAK repeat in nodes
- the receiver is member from the start