The Time-Triggered Architecture

Peter Böhm

28.9.05

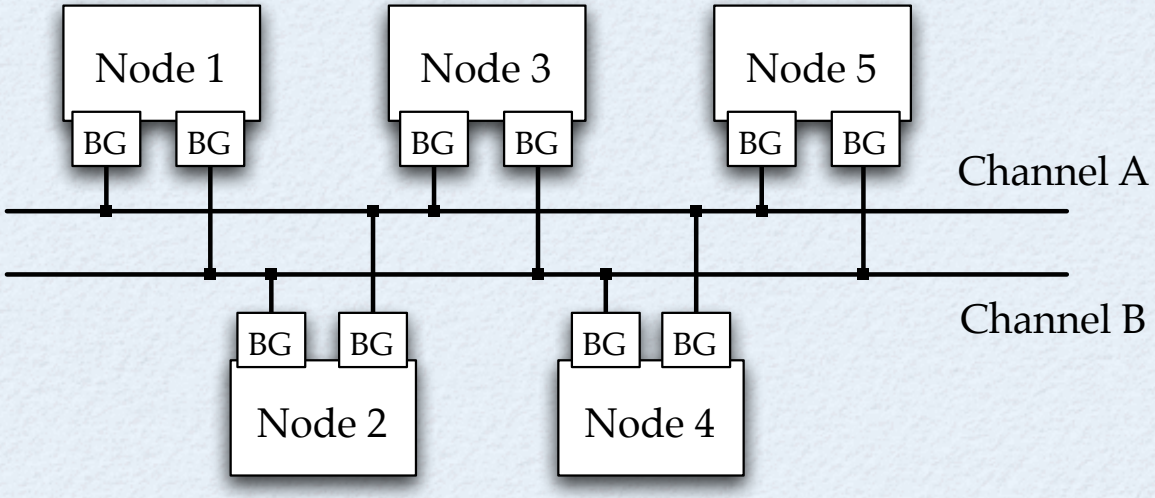
Overview

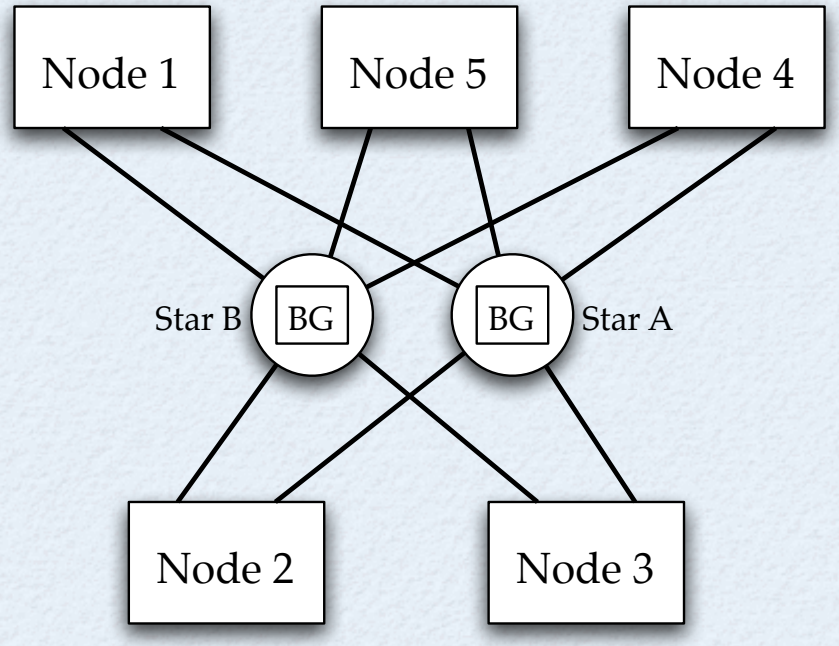
1. Introduction
2. Network Topology
3. Schedule
4. Frame Format
5. Operation Modes
6. Group Membership
7. Clock Synchronization
8. Controller State
9. Summary

1. Introduction

- as FlexRay, TTA provides functionality of a communication bus
- architecture for fault-tolerant, safety-critical real-time systems
- developed by Prof. Kopetz at the Technical University of Vienna (started in 1979)
- first published in 1993, launched in 1998
- deterministic protocol behind TTA: TTP
  - TTP/C:
    full version of TTP; for real-time busses in fault-tolerant distributed systems
  - TTP/A:
    low cost version; to connect sensors and actuators

2. Network Topology



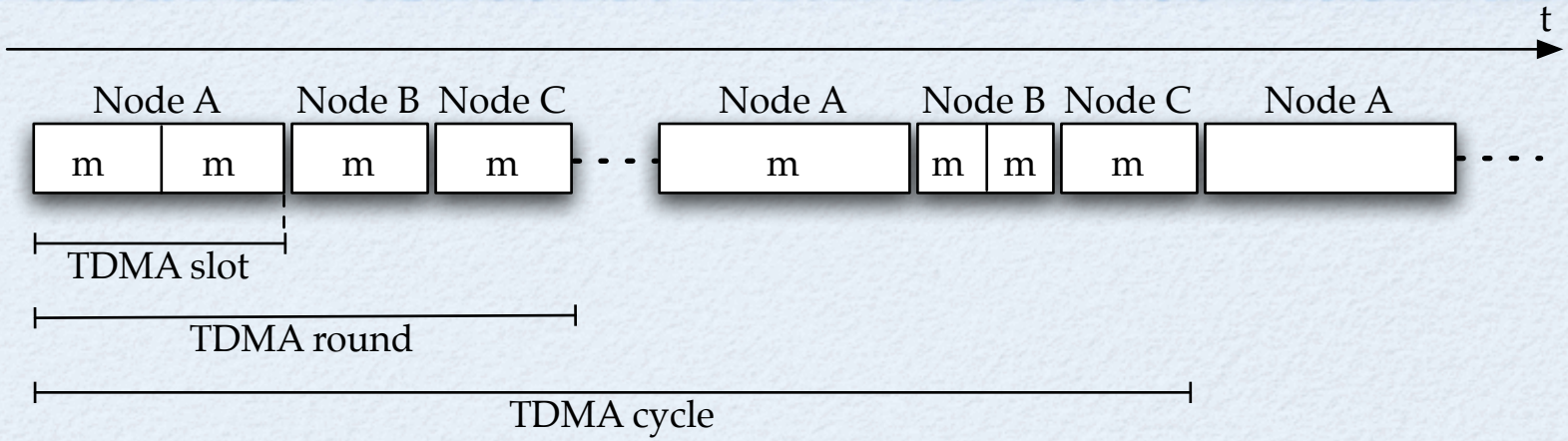


Differences to FlexRay:

- no bus and star combination
- dual-channel only
- bus guardian (BG) obligatory

➡ not as flexible as FlexRay

3. Schedule



- TDMA-schedule
- TDMA cycle: periodically, recurring time unit in TTP
- TDMA slots
  - can have different length
  - more than 1 message per slot
- TDMA round
  - node sequence and slot length same each round
  - message length within slots may differ

3. Schedule

- different approach to start-up, reintegration and clock synchronization
  - ➡ no symbol window and network idle time
- each node: message descriptor list (MEDL)
  - common knowledge of all nodes
  - specifies TDMA cycle (1 per operating mode)
  - assignment node → slot
  - marking of sync nodes (SYF-flag) and synchronization slots (CS-flag)
  - defines when mode changes are allowed

➡ schedule more complex than FlexRay's

4. Frame Format

- 2 different frame formats
- N-frame (normal frame):
  - used during normal operation
  - contains application data
  - acknowledgment bits
    information about message reception of predecessor and pre-predecessor
- I-frame (initialization frame):
  - contain internal controller state
    ➡ integrating nodes can join by taking over the data
  - transmission
    1. during start-up phase
    2. as defined in MEDL during normal operation

5. Operation Modes

- join mode
  - after start-up
  - node transmits I-frames
  - I-frame reception ➡ adoption of controller state and time

  ➡ fast synchronization of all nodes after power-on ➡ change to application mode
- application modes
  - support of more then 1
  - application data transmission
  - mode changes requested with N-frames
  - N- and I-frames as specified in static schedule
- blackout mode
  - error state
  - reintegration

6. Group Membership

- not implemented in FlexRay
- aim: identification of faulty nodes
- each node: private membership list
  records all nonfaulty nodes incl. node itself
- fault hypothesis:
  1. faults 2 or more rounds apart
  2. all or exactly 1 node fail to receive (send or receive fault)

6. Group Membership

- reliability characterized by:

  1. agreement:
     membership lists of all nonfaulty nodes are the same

  2. validity:
     membership lists of all nonfaulty nodes contain all nonfaulty nodes and at most one faulty node

- only satisfiable under the restricted fault hypothesis
  e.g. faults occur too rapidly ➡ validity not guaranteed

- system-wide schedule knowledge
  ➡ easy detection of a not sending node
  ➡ exclusion in membership list

6. Group Membership

- self-diagnostic: send and receive faults
- send fault:
  - Acknowledgment bits of first and second successor
  - if both exclude the node and the second includes the first
    - ➡ send fault
- receive fault:
  - message CRC: generated with help of sender's membership list
    - ➡ receiver: same membership list to pass CRC check
  - counters for CRC fails and passes
  - fail rate larger than pass rate
    - ➡ receive fault

7. Clock Synchronization

- MEDL: nodes with SYF-flag and slots with CS-flag
- clock deviation value of a message: similar to FlexRay
  - MEDL: expected arrival of message i (exp(i))
  - time-stamp on actual arrival of message i (act(i))
    - ➡ deviation(i) = exp(i) - act(i)
- queue with the four latest clock deviation values
  - deviation(i) stored if sender has same group membership and his SYF-flag is set
- clock correction value: fault-tolerant average
  - discard the smallest and biggest values
  - average of the 2 remaining values
- adjustment if current slot's CS-flag is set

8. Controller State (C-State)

- problems in TTA systems: agreement on
  1. operation mode
     data only interpretable if receiver's mode = sender's mode
  2. time view
     communication based on view of time
  3. membership
- aim: only nodes with same C-state can communicate
- solution: CRC of N-frames generated with the sender's current C-state

  ➡ CRC-check can uncover different C-states and message can be dropped

9. Summary

- network topology not as flexible as in FlexRay
- schedule more complex and system-wide common knowledge
- support of different application modes
- different approach to start-up, reintegration and clock synchronization:
  - I-frames
  - rounds marked as sync rounds
- global schedule ➡ group membership

➡ fault-tolerance and functionality more important than flexibility