Current research on dependability aspects of TSN at UIB

Inés Álvarez Vadillo
Julián Proenza, Manuel Barranco, Alberto Ballesteros
Outline of the presentation

Work on TSN
- Time redundancy of frames
- Mixing time and spatial redundancy
- Design a dependable network architecture
- Model checking of AVB’s SRP using Uppaal

Work on FTT to be adapted to TSN
- Dynamic fault-tolerance in the system
- Dependability evaluation
Outline of the presentation

Work on TSN
- Time redundancy of frames
- Mixing time and spatial redundancy
- Design a dependable network architecture
- Model checking of AVB’s SRP using Uppaal

Work on FTT to be adapted to TSN
- Dynamic fault-tolerance in the system
- Dependability evaluation
Introduction

• TSN devises the use of spatial redundancy to increase reliability

• IEEE 802.1Qca amendment to Path Control and Reservation. Creation of multiple paths.

• IEEE 802.1CB standard for Frame Replication and Elimination for Reliability. Send frames through multiple paths in parallel.
Time redundancy of frames: current state

• Time redundancy to tolerate temporary faults

• We proposed the Proactive Transmission of Replicated Frames mechanism

• Transmit several replicas in a preventive manner

• We proposed three different approaches
Time redundancy of frames: current state

End-to-end estimation and replication

T → B1 → B2 → L
Time redundancy of frames: current state

End-to-end estimation and replication

$k=3$
End-to-end estimation and replication

$k=3$
Time redundancy of frames: current state

End-to-end estimation and replication

$k=3$
Time redundancy of frames: current state

End-to-end estimation and replication

$k=3$
Time redundancy of frames: current state

End-to-end estimation and replication
Time redundancy of frames: current state

End-to-end estimation, link-based replication
Time redundancy of frames: current state

End-to-end estimation, link-based replication

$k'=3$
Time redundancy of frames: current state

End-to-end estimation, link-based replication

$k'=3$
Time redundancy of frames: current state

End-to-end estimation, link-based replication

$k' = 3$
Time redundancy of frames: current state

End-to-end estimation, link-based replication

$k'=3$
Time redundancy of frames: current state

End-to-end estimation, link-based replication
Time redundancy of frames: current state

Link-based estimation and replication

T ➞ B1 ➞ B2 ➞ L
Time redundancy of frames: current state

Link-based estimation and replication
Time redundancy of frames: current state

Link-based estimation and replication
Time redundancy of frames: current state

Link-based estimation and replication
Time redundancy of frames: current state

Link-based estimation and replication

T

B1

B2

L

$T_k''=3$

$B1_k''=2$

$B2_k''=3$
Time redundancy of frames: current state

Link-based estimation and replication
State of the work

• Compared with OMNeT++
  • Exhaustive fault injection
  • Case study

• Want to carry out a reliability analysis

• Want to implement a real prototype
Outline of the presentation

Work on TSN

- Time redundancy of frames
- Mixing time and spatial redundancy
- Design a dependable network architecture
- Model checking of AVB’s SRP using Uppaal

Work on FTT to be adapted to TSN

- Dynamic fault-tolerance in the system
- Dependability evaluation
Mixing time and spatial redundancy

Starting point
Mixing time and spatial redundancy

Starting point
Mixing time and spatial redundancy

Detect spatial redundancy
Mixing time and spatial redundancy

Detect spatial redundancy
Mixing time and spatial redundancy

Decide on the level of replication
Mixing time and spatial redundancy

Decide on the level of replication
Mixing time and spatial redundancy

Decide on the level of replication
Mixing time and spatial redundancy

Decide on the level of replication
Decide on the level of replication
Next steps

• We want this to be dynamic and autonomous.

• Design the mechanisms to extract information from the network and make decisions.

• Mix both mechanisms using simulation to measure the gain in reliability and bandwidth consumption.

• Develop a real prototype.
Outline of the presentation

Work on TSN
- Time redundancy of frames
- Mixing time and spatial redundancy
- Design a dependable network architecture
- Model checking of AVB’s SRP using Uppaal

Work on FTT to be adapted to TSN
- Dynamic fault-tolerance in the system
- Dependability evaluation
Design a dependable architecture

Starting point

N1 -> B -> N3
N2 -> B -> N3
Design a dependable architecture

Starting point

N1

N2

B

N3

SPoF
Design a dependable architecture

Starting point

Vulnerable

SPoF

N1

N2

B

N3
Design a dependable architecture

Eliminate SPoF
Design a dependable architecture

Add redundant paths

N1 → B1 → N3 → N2 → B2
Design a dependable architecture

Restrict the failure semantics

Crash failure semantics
Design a dependable architecture

What should we do if we want a CNC?
Design a dependable architecture

Introduce CNC in Switches
Design a dependable architecture

Introduce CNC in Switches

Replica determinism
Design a dependable architecture

Include interlinks for the CNCs to communicate
Design a dependable architecture

Include interlinks for the CNCs to communicate

How can we extend it to larger networks?
Outline of the presentation

Work on TSN
- Time redundancy of frames
- Mixing time and spatial redundancy
- Design a dependable network architecture
- Model checking of AVB’s SRP using Uppaal

Work on FTT to be adapted to TSN
- Dynamic fault-tolerance in the system
- Dependability evaluation
Introduction

• We are modelling the AVB version of SRP using Uppaal.

• SRP operation in talker, bridges and listeners.

• Through the development we detected consistency and reliability issues.

• How will the issues detected affect TSN’s SRP?
Outline of the presentation

Work on TSN
- Time redundancy of frames
- Mixing time and spatial redundancy
- Design a dependable network architecture
- Model checking of AVB’s SRP using Uppaal

Work on FTT to be adapted to TSN
- Dynamic fault-tolerance in the system
- Dependability evaluation
Introduction

• In our previous project we built a highly dependable distributed architecture based on FTT-Ethernet.

• We implemented fault-tolerance for the network and the nodes to increase the overall reliability of the system.

• GOAL: We want to build a self-reconfigurable infrastructure for critical adaptive distributed embedded systems.

• Include dynamic fault-tolerance mechanisms that can adapt
Dynamic fault-tolerance in the system

At the **node level**, our architecture is composed of **various components**
Dynamic fault-tolerance in the system

At the **node level**, our architecture is composed of **various components**

Tasks can be dynamically assigned to the nodes
Dynamic fault-tolerance in the system

At the node level, our architecture is composed of various components

Tasks can be dynamically assigned to the nodes. E.g. any set of nodes can be configured for TMR.
Dynamic fault-tolerance in the system

Potential change triggers

• Human commands
• Phase of the mission
• Environment
• State of the architecture
Dynamic fault-tolerance in the system

Potential change triggers

- Human commands
- Phase of the mission
- Environment
- State of the architecture
Dynamic fault-tolerance in the system

Potential change triggers

- Human commands
- Phase of the mission
- Environment
- State of the architecture

Phases in a commercial flight

- Engine start and warm-up
- Taxi
- Takeoff
- Climb to 45 kft
- Cruise
- Descent
- Landing
- Taxi
- Shutdown
Dynamic fault-tolerance in the system

Potential change triggers

• Human commands
• Phase of the mission
• Environment
• State of the architecture
Dynamic fault-tolerance in the system

Potential change triggers

• Human commands
• Phase of the mission
• Environment
• State of the architecture
Dynamic fault-tolerance in the system

Potential change triggers

• Human commands
• Phase of the mission
• Environment
• State of the architecture

More hostile environment more replication
Dynamic fault-tolerance in the system

**Potential change triggers**

- Human commands
- Phase of the mission
- Environment
- **State of the architecture**
Dynamic fault-tolerance in the system

Potential change triggers

- Human commands
- Phase of the mission
- Environment
- State of the architecture

When one node is faulty it can be replaced for *redundancy preservation*
Dynamic fault-tolerance in the system

Potential change triggers

- Human commands
- Phase of the mission
- Environment
- State of the architecture

When one node is faulty it can be replaced for *redundancy preservation*
Dynamic fault-tolerance in the system

Potential change triggers

- Human commands
- Phase of the mission
- Environment
- State of the architecture

When one node is faulty it can be replaced for redundancy preservation

This seriously increases reliability
Dynamic fault-tolerance in the system

Changing the configuration

State of the system → Fulfilment? → Requirements of the system

Configuration change

List of tasks
RT requirements
R(t) requirements
Dynamic fault-tolerance in the system

Performing changes
Dynamic fault-tolerance in the system

Performing changes
Dynamic fault-tolerance in the system

Performing changes

- Monitoring
- Decision
- Conf change
Next steps

• Extend this work to TSN-based systems.

• We would like to integrate the node manager operation with the Centralised Network Configurator.
Outline of the presentation

Work on TSN
- Time redundancy of frames
- Mixing time and spatial redundancy
- Design a dependable network architecture
- Model checking of AVB’s SRP using Uppaal

Work on FTT to be adapted to TSN
- Dynamic fault-tolerance in the system
- Dependability evaluation
Introduction

• Explore the design space for the communication subsystem of FTTRS.

• Graph-based modelling of the network.

• Generate all networks that meet a set requirements.

• Find the one with the highest reliability for the given requirements.
Introduction
Introduction
Introduction
Introduction
Introduction
Next steps

• Complete the implementation of the algorithms.

• Extend the work to support the dependability evaluation of TSN networks.

• Extend the work to support temporary faults.
Current research on dependability aspects of TSN at UIB

Inés Álvarez Vadillo