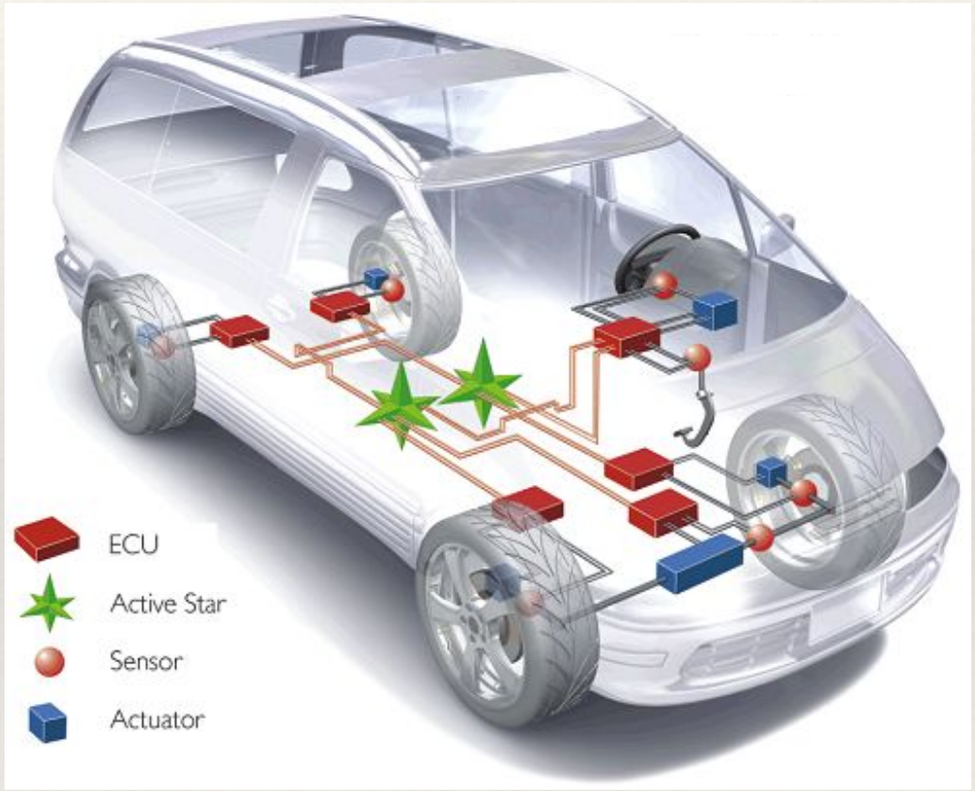
Japan Advanced Instituted of Science and Technology

Model Checking of Automotive System in the Presence of Multiple Communication Protocols

Xiaoyun Guo
Aoki Laboratory
School of Information Science

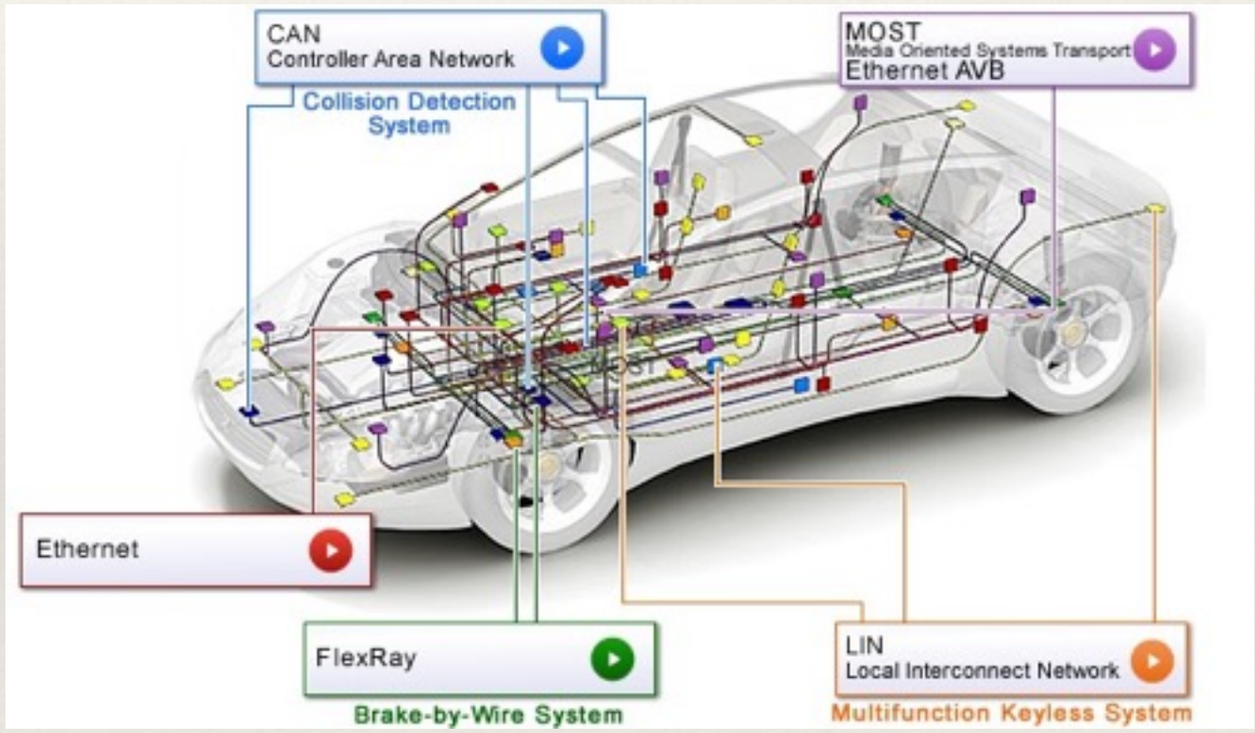
Automotive System

- Automotive system is a real-time distributed control system to realize a variety of functions with electronic component in the vehicle.
  - Body control function —— LIN
  - Braking control function —— CAN
  - Multimedia control function —— MOST
  - Adoptive cruise control function —— FlexRay
- Consisting of
  - Nodes
    - Sensors(human-machine interfaces), controllers and actuators(electromechanical actuators)
  - Buses



Automotive System

- Automotive system consists of multiple subsystems with different communication protocols.
  - CAN, LIN, FlexRay, MOST
- If we consider the communication between different protocols, the timing of message transmission will be affected.
  - Transmission delay by gateway
  - Different communication regulations



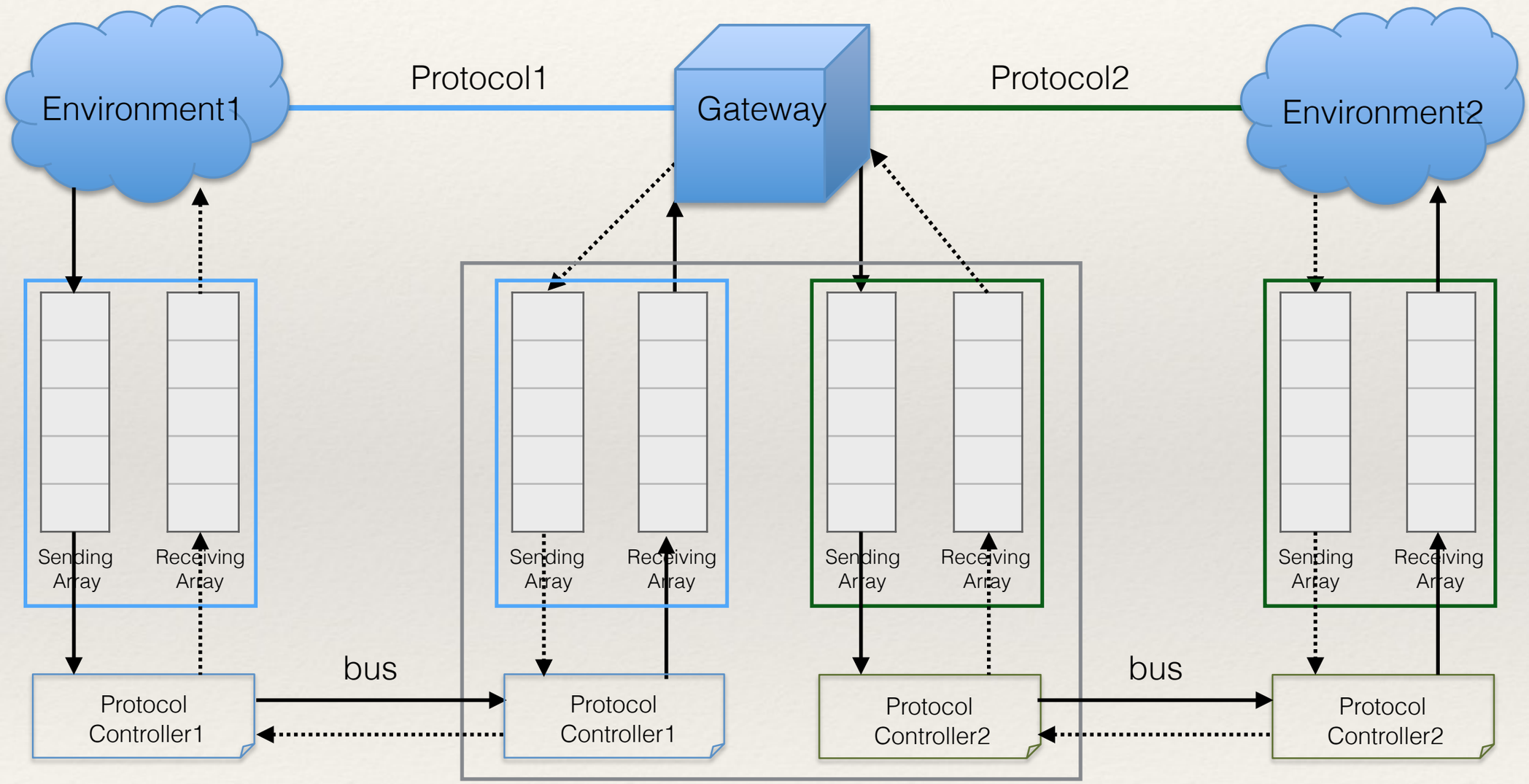
Objective

- The objective of this research is verifying communication of automotive systems in the presence of multiple communication protocols.
  - Considering multiple protocols in an automotive system.
  - Verifying time property and safety property.
    - Message response time.
    - Whether the message has been lost.
  - Improving verification capability and efficiency.

Approach

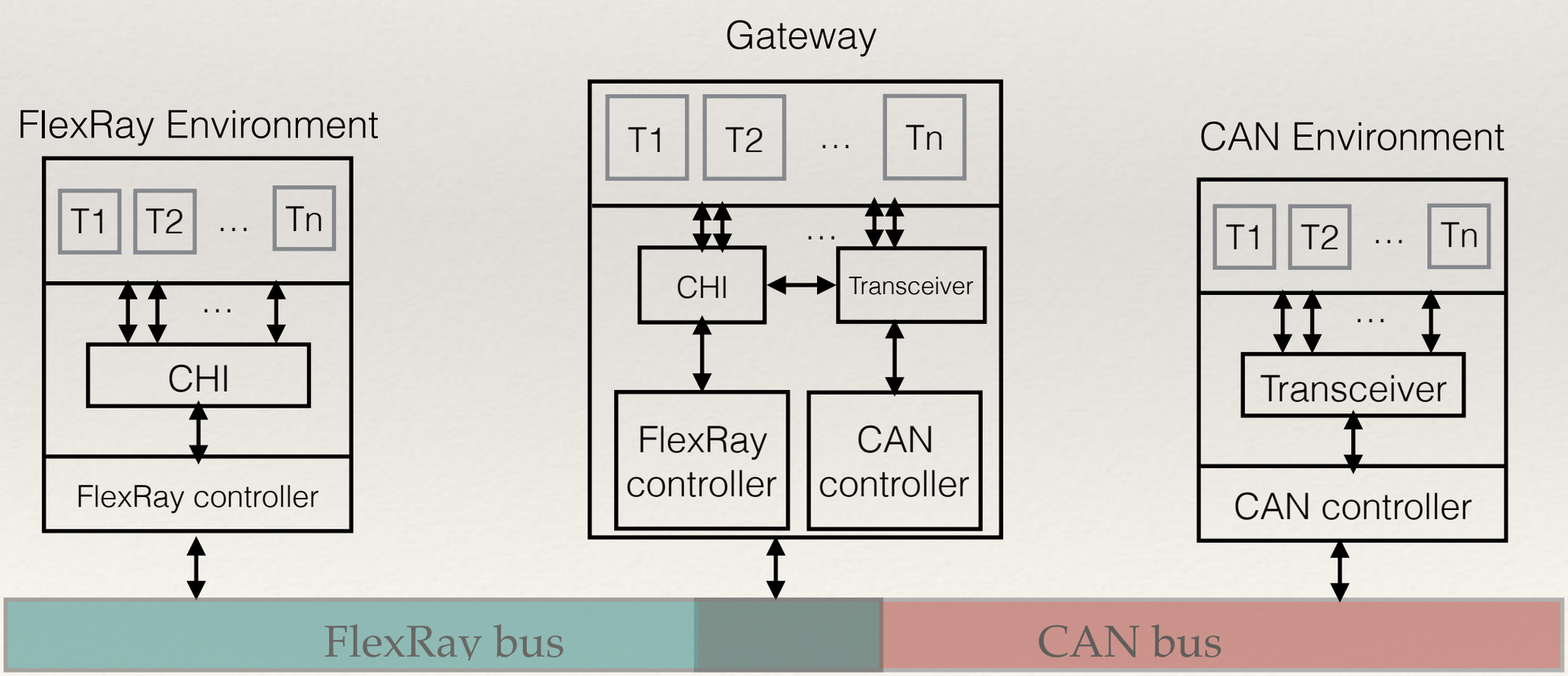
- We proposed a framework to verify the communication between subsystems in present of different protocols.
  - A gateway connect two environments as a protocol translator .
  - The gateway follows two protocols to receive messages from an environment and forward messages to other environment.
  - One environment represents a protocol subsystem with arbitrary topology and the number of nodes.
  - Messages can be sent at any time.

Framework


Environment1
Protocol1
Gateway
Protocol2
Environment2
Sending Array
Receiving Array
Sending Array
Receiving Array
Sending Array
Receiving Array
Sending Array
Receiving Array
bus
bus
Protocol Controller1
Protocol Controller1
Protocol Controller2
Protocol Controller2

Experiments

- The communication between CAN and FlexRay networks.
  - CAN and FlexRay protocol model are abstracted
  - Gateway model is established based on general functions.
  - The automotive system model is checked by UPPAAL.



Results

- State space explosion problem
  - Related factors : the number of messages
    - Not deadlock (satisfied)

The number of messages	Time (s)	Memory(KB)
4	0.026	34,808
8	1.067	36,236
10	9.708	102,984
12	104.271	919,712

- Some message may be lost in the gateway. Because CAN network and FlexRay network randomly send a message.
- The highest priority of the message alway can be send.