Comparative Safety Analysis of Wireless Communication Networks in Avionics

Rohit Dureja and Kristin Yvonne Rozier, Iowa State University

Laboratory for Temporal Logic

Motivation

- The amount of fuel consumed by an aircraft is directly proportional to its weight.
- The Airbus A380 has around ∼100,000 wires totaling 470 km and weighing 5,700 kg.
  - Some weight can be reduced by using aluminum wiring instead of copper.

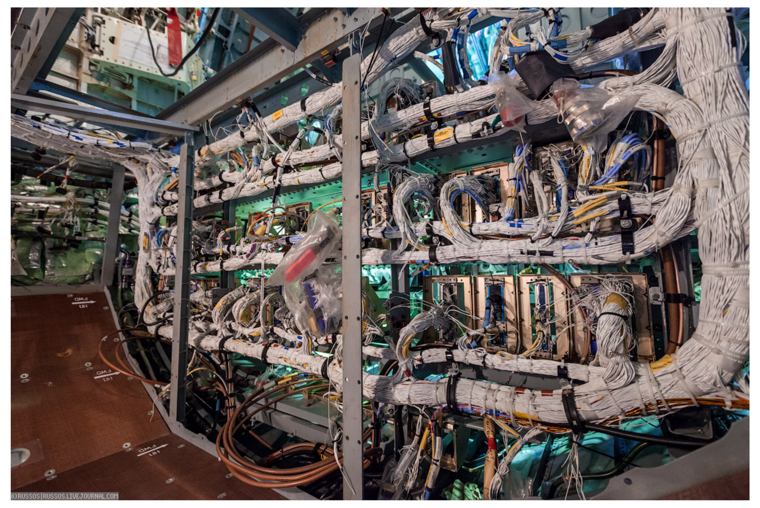

Figure 1: Airbus A380 wiring harness

- Major reduction in weight is possible if wires are eliminated, and replaced with wireless components.
- **The wireless network needs to be at least as reliable and fault tolerant as the existing wired network.**
- The modest goal is to **reduce wiring so as to decrease aircraft weight by at least a ton.**
- Reduced weight leads to savings for the airline company, cheaper flights, and improved fleet management.

Contributions

❶ The problem of migrating communication technology in terms of system safety is addressed.

❷ The proposed formal framework aids system designers to compare different communication networks simultaneously, and explore viable fault tolerant mechanisms.

❸ The framework builds upon existing model checking and safety assessment tools, and is plug-and-play.

❹ As proof of concept, the ZigBee protocol is analyzed using the framework.

Proposed Framework

OCRA — Used for component-based modeling and contract refinement.

Used for specifying and checking the behavior of a component

Used for safety assessment of the faulty model.

Important Observation

Network protocols are suitable candidates for contract-based verification since their layered architecture makes them amenable to compositional modeling.

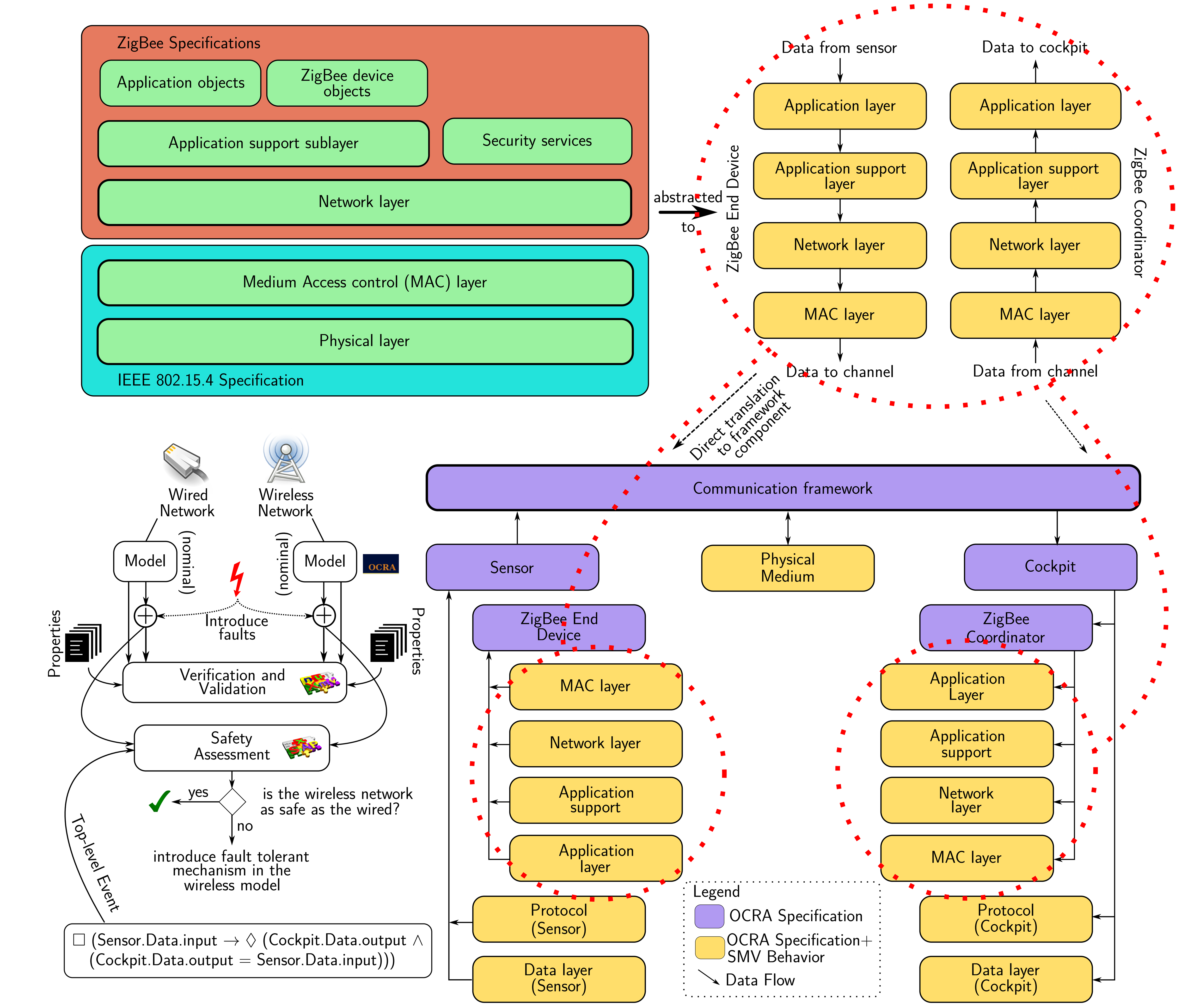

Figure 2: *Top-left*: Zigbee protocol stack specification. *Top-right*: Modeling abstraction for the protocol stack. *Bottom-right*: The abstraction made part of the framework without any modifications. *Bottom-left*: Flow diagram for safety assessment using the framework.

Preliminary Experiments

- The top-level property (TLE) is the negation of our main system requirement.
- Faults modeled in the wireless system deal with communication failures. *Permanent* faults persist, while *transient* faults are non-deterministic.

Table 1: Faults associated with the ZigBee network

Fault	Description	Mode	Authority
Z1	Signal interference	Transient	Physical Medium
Z2	End-Device not discoverable	Transient	Network Layer (Sensor)
Z3	Coordinator cannot accept new connections	Transient	Network Layer (Cockpit)
Z4	Coordinator fails to set up network	Permanent	Application Layer (Cockpit)
C1	Error recovery mechanism fails	Transient	Protocol (Cockpit/Sensor)
S2	Sensor fails	Permanent	Data Layer (Sensor)

- In the wired system, the faults modeled deal with breaking of the wired medium, failure of the sensor system, and failure of the error recovery mechanism.
- Sample cutset and minimal cutsets (cardinality = 1).

$$Cutsets = (\{Z4, S2, Z1, C.C1, Z2\}, \{Z4, Z1, C.C1, Z2\}, \{S2, Z1, C.C1, Z2\}, Z4, S2, \{Z1, C.C1\}, \{Z2, Z4\} \ldots)$$
$$Minimal = (Z4, S2, \{Z1, C.C1\}, \{Z2, Z4\})$$

- After the points of failure are determined, a failure function assigns probabilities to individual faults.

Future Work

The work is still incomplete in terms of quantitative evaluation. Future extensions of the work include

- quantitative assessment of failure probabilities,
- addition of more behavior and fault extensions to the models,
- and identification of aircraft components that can be migrated to wireless.

Automatic introduction of fault tolerant architectures to achieve a desired probability.

{dureja, kyrozier}@iastate.edu