Comparative Safety Analysis of Wireless Communication Networks in Avionics

Rohit Dureja, Kristin Yvonne Rozier
Iowa State University
Ames, Iowa 50011
Email: {dureja, kyrozier}@iastate.edu

***Abstract*—Existing wired networks add weight and complexity to current aircraft design. To reduce weight of aircraft, it is essential to decrease the number of wired components and move them to wireless. However, migration of wired to wireless needs to be supported by a thorough analysis of the complexities and failure aspects of the two mediums. The wireless network needs to be at least as reliable and fault tolerant as the existing wired network. This paper proposes a formal framework for a comparative safety analysis of wired and wireless networks. Due to the plug-and-play nature of the framework, it is adaptable to a wide variety of network protocols. It facilitates identification of the minimum set of events that lead to system failure, and using quantified failure probabilities recommends fault tolerant mechanisms that increase system reliability. Designers can then compare candidates for wireless protocols among each other, as well as the wired network, and make informed design decisions.**

I. Introduction

Increasing complexity and limitations of wired networks is driving innovation towards adoption of wireless technology. Wireless networks scale better than wired networks, cost of setting up a wireless network is lower compared to a wired network, and wireless networks are essentially plug-and-play. Although the cost of equipment for wireless networks is higher compared to wired, it is outweighed by the benefits of ease-of-use, scalability, and weight. The proposed framework aims to analyze wireless networks in terms of fault propagation and perform a comparative fault analysis of wired and wireless networks.

Migration of wired networks to wireless requires a thorough study of the wired system, choosing an appropriate wireless communication protocol, assessing faults associated with the wireless communication, and analysis of the quantitative benefits of using a wireless network. The formal framework allows to analyze different wireless network models, and compare them to existing wired network models in terms of fault tolerance, and fault propagation. The Airbus A380 has around $\sim$100,000 wires totaling 470 km and weighing 5,700 kg. Some weight can be reduced by using aluminum wiring instead of copper. However, major reduction in weight is possible if wires are eliminated altogether. The modest goal of the proposed framework is to reduce wiring so as to decrease aircraft weight by at least a ton, and help in the design of a wireless network that is at least as safe as the existing wired network.

The contributions of the work in this paper are manifold. To the best of our knowledge, this is the first work that addresses the problem of communication technology migration in terms of system safety. The formal framework aids system designers to compare different communication networks simultaneously and explore viable fault tolerant mechanisms. The framework builds upon existing model checking and safety assessment tools, and is plug-and-play. As proof of concept, the ZigBee protocol is analyzed using the framework in the paper.

A. Related Work

Fault tolerant mechanisms for ZigBee wireless sensor networks [1] help establish safe network topologies. On the other hand, fault detection and recovery mechanisms [2] increase the reliability of existing sensor networks. While both these approaches lead to safer systems, they do not support any sort of comparative analysis between different networks. Wireless avionics, and human interfaces for spacecraft [3] are pushing towards migration of wired networks to wireless. Experimental performance evaluation [4] is another way to assess network reliability. However, such experimentation is limited in terms of scenarios explored, environmental conditions, and does not scale. The formal framework proposed in this paper focusses on inter-component communication rather than protocol behavior, allows the comparison of different networks in terms of safety, and is fully automatic and scalable.

II. Proposed Framework

Network protocols are suitable candidates for contract-based verification since their layered architecture makes them amenable to compositional modeling. Figure 1 shows a layered model for a ZigBee communication network.

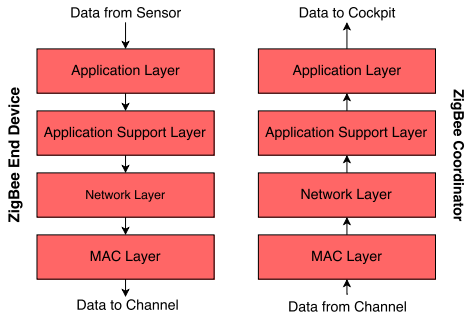

Fig. 1. Abstracted and layered ZigBee communication network model showing data flow across layers.

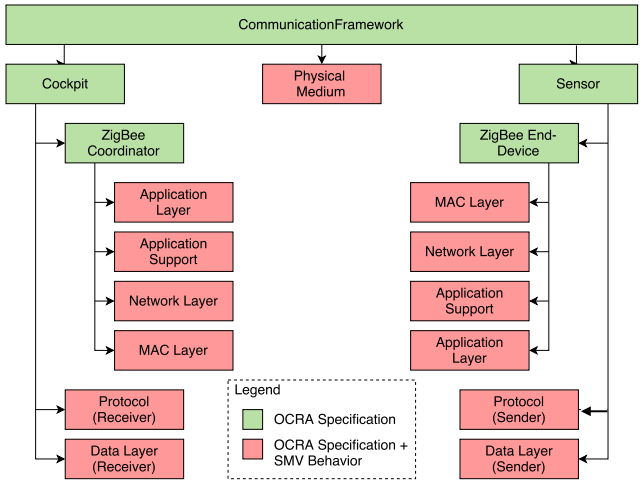

Fig. 2. Framework model for the ZigBee wireless communication system

We use OCRA [5] for component-based specification of the network architecture, and contract refinement. The individual behavior for a component is specified in SMV and checked using nuXmv [6] The complete system model with a bi-directional ZigBee interface is shown in figure 2. The model can be adapted to any protocol by modifying the behavior of the layered network components. For wired systems, the model can be modified by removing the wireless components altogether. We classify the models as *nominal* and *extended*. *Nominal* models model the ideal behavior of the system (useful for system validation), whereas, *extended* models have faults introduced in them. We use xSAP [7] to perform safety assessment and analysis of the extended model.

To derive the extended models from the nominal models of the system, faults are introduced in some components of the nominal model of figure 2. Table I shows the faults modeled in the wireless system. *Permanent* faults persist during the entire operation of the system, while on the other hand, *transient* faults are non-deterministic. In the extended model for 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. The main requirement for the system is to faithfully reproduce the data sensed by the sensor at the cockpit, and is represented using the LTL formula

$$\Box(Sensor.Data.input \rightarrow \Diamond(Cockpit.Data.output \wedge (Cockpit.Data.output = Sensor.Data.input)))$$

III. Preliminary Experiments

For safety assessment using fault trees, our top-level property (TLE) is the negation of our main system requirement. The framework identifies single and multiple points of failure (cardinality) of the TLE and introduces redundancy and other fault tolerant architectures to make the wireless system at least as safe as the wired system. For the wireless system of figure 2, a sample output for cutsets and minimal cutsets of cardinality 1 and 2 is

TABLE I
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)

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

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

After the points of failure are determined, a failure function assigns probabilities to individual faults. The overall failure probability needs to be equal to or less than the failure probability of the wired system. Similarly, multiple wireless systems can also be compared.

IV. Future Work

This paper presents a plug-and-play formal framework to perform comparative safety analysis of wired and wireless communication networks. 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. A desirable extension will be automatic introduction of fault tolerant architectures to achieve a desired probability.

References

[1] S. B. Attia, A. Cunha, A. Koubâa, and M. Alves, "Fault-tolerance mechanisms for zigbee wireless sensor networks," in *Work-in-Progress (WiP) session of the 19th Euromicro Conference on Real-Time Systems (ECRTS 2007), Pisa, Italy*, no. 1, 2007, pp. 37–40.

[2] J. Wan, J. Wu, and X. Xu, "A novel fault detection and recovery mechanism for zigbee sensor networks," in *Future Generation Communication and Networking, 2008. FGCN'08. Second International Conference on*, vol. 1. IEEE, 2008, pp. 270–274.

[3] R. Alena, S. R. Ellis, J. Hieronymus, and D. Maclise, "Wireless avionics and human interfaces for inflatable spacecraft," in *Aerospace Conference, 2008 IEEE*. IEEE, 2008, pp. 1–16.

[4] R. Alena, R. Gilstrap, J. Baldwin, T. Stone, and P. Wilson, "Fault tolerance in zigbee wireless sensor networks," in *Aerospace Conference, 2011 IEEE*. IEEE, 2011, pp. 1–15.

[5] A. Cimatti, M. Dorigatti, and S. Tonetta, "OCRA: A tool for checking the refinement of temporal contracts," in *Automated Software Engineering (ASE), 2013 IEEE/ACM 28th International Conference on*. IEEE, 2013, pp. 702–705.

[6] R. Cavada, A. Cimatti, M. Dorigatti, A. Griggio, A. Mariotti, A. Micheli, S. Mover, M. Roveri, and S. Tonetta, "The nuXmv symbolic model checker," in *CAV*, ser. Lecture Notes in Computer Science, A. Biere and R. Bloem, Eds., vol. 8559. Springer, 2014, pp. 334–342.

[7] B. Bittner, M. Bozzano, R. Cavada, A. Cimatti, M. Gario, A. Griggio, C. Mattarei, A. Micheli, and G. Zampedri, "The xSAP safety analysis platform," in *Proceedings of TACAS 2016*, 2016.