Poster: Medium Guardian - the Bus Guardian Concept applied to Wireless Communications Systems

João Almeida[*,†] jmpa@ua.pt
Joaquim Ferreira[*,‡] jjcf@ua.pt
Arnaldo S. R. Oliveira[*,†] arnaldo.oliveira@ua.pt

[*]Instituto de Telecomunicações, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal
[†]DETI - Universidade de Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal
[‡]ESTGA - Universidade de Aveiro, 3754-909 Águeda, Portugal

Abstract

The fifth generation of mobile networks holds the promise to enable new wireless applications, including the operation of dependable and real-time safety-critical systems. However, the strict latency and reliability requirements associated to these systems demand for innovative solutions that enhance the dependability attributes of wireless networks. With this in mind, the adaptation of the bus guardian concept to the wireless context is proposed in this work. This novel mechanism - the medium guardian - is responsible for monitoring and control the operation of a wireless device in the value, time and frequency domains. In this way, fail-silent behaviour can be enforced in the nodes of the network by disabling their interfaces whenever a fault is detected.

1 Proposal

With the future development of the next generation of mobile networks (5G), more and more application domains could be leveraged by wireless technologies. For instance, the target requirements of small latency (round trip times lower than 1 ms) and high reliability ($> 99.999\%$) envisioned by the 5G community [1], will provide the basis for the Tactile Internet (real-time cyber-physical control) and will enable the operation of mission-critical systems (e.g. remote surgery), cooperative self-driving cars, advanced industrial automation, smart grid management, etc. [6]. Nevertheless, the path to achieve these goals is not trivial and innovative solutions are needed in order to solve the inherent problems of wireless environments, such as unpredictable channel conditions, dynamic network topologies (e.g. road traffic scenarios), security, spectrum interference and so forth. For example, to cope with the high data rate (10 Gb/s), low latency and the massive number of radio units expected in the future 5G, novel signal waveforms have been proposed. Generalized OFDM (G-OFDM) [8] is one of the most promising approaches, since its flexibility allows a large number of devices with different communications requirements to exchange information in the same wireless channel. Furthermore, G-OFDM seamlessly supports dynamic resource allocation (e.g. bandwidth) according to the current network demands. Non-Contiguous OFDM (NC-OFDM) [2] is another interesting technique originally designed for opportunistic spectrum access, in order to enable the Cognitive Radio concept, where secondary users may transmit messages by utilizing the subcarriers not occupied at a certain moment by the primary channel users. In addition to these new waveforms, full duplex wireless communications [4], besides increase the overall throughput of the network, could also facilitate the development of Cognitive Radio strategies, since in this way a node is able to listen the signal sent by the other devices while transmitting.

On the dependability side, the high reliability and availability requirements defined in 5G can only be attained if new fault-tolerance mechanisms are included in the network protocols and communication devices. In safety-critical contexts, a malicious or malfunctioning node may compromise the operation of the entire system, causing a catastrophic event with irreversible damage. For that purpose, the design of fail-safe strategies for the communications devices is of uttermost importance, in order to limit the impact caused by a fault arising in one of the node's components. This topic is well studied for the case of fieldbus technologies and wired networks, but there is few research conducted in wireless systems. One of the most common methods used to enhance dependability in cabled networks is to guarantee that nodes only exhibit a single failure mode: the fail silent failure mode [9]. In this way, a node can only produce correct results or no results at all, avoiding for instance situations in which a faulty node starts sending unsolicited packets at random instants without respecting the medium access rules (babbling idiot failure mode). Traditionally, fail-silent behaviour can be enforced in the value domain, i.e. the transmitted packets only contain correct values, in the time domain, i.e. the messages are only transmitted at the right moments, or in both of them. If omissions are properly handled, a fault inside a fail-

International Conference on Embedded Wireless Systems and Networks (EWSN) 2017
20–22 February, Uppsala, Sweden

ISBN: 978-0-9949886-1-4

silent node can not propagate to others nodes of the system, thus creating distinct fault confinement regions.

The bus guardian concept is a well-known technique used to guarantee fail-silent behaviour in the nodes of a network by implementing behavioural error detection mechanisms. In order to be fail-independent with respect to the node it monitors, the guardian must belong to a different fault containment region (e.g. separate hardware, power supply, clock, etc.). However, full independence can only be achieved at a high cost and therefore a trade-off is usually made between the total price of the system and the sources and probability of common mode failures. Bus guardians were first mentioned in [7], where they are used to govern the status of their associated modules (i.e. a processor or memory module) in a fault-tolerant multiprocessor architecture for aircraft. In this case, the guardians are able to control the power supplied to the modules and the access to the communication buses, disabling it if a malfunction is detected. In [9], bus guardians are employed to protect against violations in the temporal domain, guaranteeing that the TDMA scheduling of a time-triggered communication system is respected. This way, the nodes are only able to transmit in the time slots specifically allocated to them, avoiding e.g. babbling idiot failures. It is also possible to deploy bus guardians for event-triggered communications, by limiting the minimum inter-arrival time between the generation of two consecutive messages in a node [3]. Typically, the parameters utilized by the guardian to monitor node's activity, such as time slot allocation or minimum inter-arrival time, are static and known a priori or eventually acquired during network startup. Nevertheless, more flexible solutions were also envisaged to cope with the operation of communication protocols with dynamic scheduling [5], in which the time slot allocation varies in run-time and possibly every cycle. Another interesting property of the bus guardians architectures resides in the fact that if the network can be organized in a star topology, it is possible to replace the individual guardians dedicated to each node, by a single central guardian.

The main idea of this work is to apply the bus guardian concept to wireless communication systems, in order to improve the dependability attributes of this type of networks. The proposed mechanism, called medium guardian, consists in a generic device that could be included in the architecture of any wireless transceiver, with the main goal of verifying the correctness of its output to the wireless medium. Starting from this broad objective, its design and implementation could then be adapted to cope with the requirements of any system, protocol or modulation scheme (time or event triggered communications, single or multi carrier modulations, cognitive radios, full duplex devices, etc.). For instance, with the new protocols and waveforms that have been proposed for the next generation of mobile networks (e.g. GFDM or NC-OFDM), resource allocation in the frequency domain, both at the channel level and for the different subcarriers inside the same channel, becomes extremely important. In such scenarios, a medium guardian should not only supervise the node's operation in the value and time domains, but also in the frequency one. This can be easily achieved, by plotting the frequency representation of the signal the node wants to transmit or has already transmitted, depending on the specified policy, and verifying its compliance with the allocation previously defined by the network coordination mechanism, which could be centralized or distributed. In cognitive radio frameworks for example, the medium guardian can independently verify if the primary users are not occupying the desired channels/subcarriers, and allow message transmission based on this separate observation. Another important difference when compared to wired systems lies in the fact that the analog part of wireless transceivers constitutes a critical source of faults [10]. This is typically not the case for e.g. CAN, Ethernet or Flexray controllers. Therefore, the validation of the correct behaviour of analog components can not be done in the digital domain a priori, i.e. before the message is actually transmitted to the air. This verification can only be performed during or after node's transmission by an independent or loosely coupled guardian, according to the taxonomy presented in [3], with a certain antenna separation in order to prevent the saturation of the input RF signal. Finally, one should also note that in the wireless context, the central guardian architecture can not be followed since a physical star topology can never prevent nodes from receiving messages transmitted by misbehaving units. In this case, the distributed approach needs to be employed, with an individual guardian per wireless node.

Acknowledgments

This work is funded by National Funds through FCT - Fundação para a Ciência e a Tecnologia under the PhD scholarship ref. SFRH/BD/52591/2014.

2 References

[1] 5GPP. The 5G Infrastructure Public Private Partnership: the next generation of communication networks and services. https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf. Accessed 6 January 2016.

[2] H. Bogucka, A. M. Wyglinski, S. Pagadarai, and A. Kliks. Spectrally agile multicarrier waveforms for opportunistic wireless access. *IEEE Communications Magazine*, 49(6):108–115, June 2011.

[3] I. Broster and A. Burns. An analysable bus-guardian for event-triggered communication. In *Real-Time Systems Symposium, 2003. RTSS 2003. 24th IEEE*, pages 410–419, Dec 2003.

[4] J. I. Choi, M. Jain, K. Srinivasan, P. Levis, and S. Katti. Achieving Single Channel, Full Duplex Wireless Communication. In *Proceedings of the Sixteenth Annual International Conference on Mobile Computing and Networking*, MobiCom '10, pages 1–12, NY, USA, 2010. ACM.

[5] J. Ferreira, L. Almeida, A. Fonseca, P. Pedreiras, E. Martins, G. Rodriguez-Navas, J. Rigo, and J. Proenza. Combining operational flexibility and dependability in FTT-CAN. *IEEE Transactions on Industrial Informatics*, 2(2):95–102, May 2006.

[6] G. P. Fettweis. The Tactile Internet: Applications and Challenges. *IEEE Vehicular Technology Magazine*, 9(1):64–70, March 2014.

[7] A. L. Hopkins, T. B. Smith, and J. H. Lala. FTMP - A highly reliable fault-tolerant multiprocess for aircraft. *Proceedings of the IEEE*, 66(10):1221–1239, Oct 1978.

[8] N. Michailow, M. Matth, I. S. Gaspar, A. N. Caldevilla, L. L. Mendes, A. Festag, and G. Fettweis. Generalized Frequency Division Multiplexing for 5th Generation Cellular Networks. *IEEE Transactions on Communications*, 62(9):3045–3061, Sept 2014.

[9] C. Temple. Avoiding the babbling-idiot failure in a time-triggered communication system. In *Fault-Tolerant Computing, 1998. Digest of Papers. Twenty-Eighth Annual International Symposium on*, pages 218–227, June 1998.

[10] S. Worrall, G. Agamennoni, J. Ward, and E. Nebot. Fault Detection for Vehicular Ad Hoc Wireless Networks. *IEEE Intelligent Transportation Systems Magazine*, 6(2):34–44, Summer 2014.