Deterministic and cognitive wireless communication system with jamming-resistant capabilities for tactical or industrial communications

Raul Torrego, Ander Etxabe, Pedro M.Rodriguez, Iñaki Val
Information and Communication Technologies
IK4-IKERLAN
Arrasate-Mondragon, Spain
{rtorrrego, aetxabe, pmrodriguez, ival}@ikerlan.es

Abstract—**This work presents a jamming-resistant and deterministic wireless communication system, which is intended to be used in tactical or industrial communications. These kind of applications require data communication to be bounded in the time and reliability domains, no matter which is the harshness of the environment or the presence of malicious interferences. In harsh propagation environments, communication systems suffer from severe signal degradation, including delay spread, deep fading and Doppler spread. Besides, they must also deal with other system's interference and jammer attacks. The aim of this work is to propose a new communication system, which is based on the IEEE 802.11a/g physical layer, implemented on a FPGA. On top of this physical layer, a cognitive Time Division Multiple Access (TDMA) MAC layer is proposed, fulfilling real-time requirements. The radio cognitive capabilities implemented in the MAC layer allow the communication system to detect the interference generated by a jammer or other spectrum users, switching the communication to a safe frequency band. Both, simulations in OPNET network simulator and measurements on real hardware are provided in order to characterize the performance of the presented system. The results prove the capability of the system to guarantee delay bounds in tactical or industrial environments with interference.**

Keywords—Wireless communications; Deterministic, Real-time; Jamming-resistant; OFDM; TDMA; MAC; Cognitive Radio; Tactical radio; Industrial environment; FPGA

I. Introduction

The replacement of wired communication systems by wireless ones is a common trend nowadays. The benefits in terms of lower costs in materials, deployment and maintenance that wireless systems provide over their wired counterparts are highly appreciated in many fields. Specifically, industrial applications, in which the aforementioned costs are highly elevated, or tactical communications are one of the main beneficiaries of this technology.

Time-critical and mission-critical applications (automotive, aerospace, military…) require data communication to be bounded in the time and reliability domains. Communications carried out in such applications demand short latency, minimal jitter, deterministic data delivery time and high reliability. Due to the nature of these applications, these requirements must be imperatively met in order to avoid material damages or even personal injuries.

However, communications in industrial or tactical environments have to deal with harsh environments that complicate this goal. The presence of severe multipath due to reflections in metallic structures or surfaces, or the presence of multiple sources of electro-magnetic interference (high power electric motors, other wireless communication systems present nearby…) are two of the difficulties that have to be get over. Besides, a new threat has arisen in the last years: signal jammers. These devices and their users are able to generate malicious interference in order to disrupt wireless communications on purpose.

Unfortunately, traditional wireless communication systems are not able to overcome all these difficulties and, at the same time, fulfill with the aforementioned requirements needed by control application or tactical communications. As a consequence, it is necessary to deploy new wireless communication systems like the one presented in this work, based on cognitive radio technology [1].

The proposed wireless communication system, shown in Fig. 1, is based on a custom Orthogonal Frequency Division Multiplexing (OFDM) modem design which has been implemented on the programmable logic of a Xilinx Zynq Field Programmable Gate Array (FPGA). The modem is fully customizable, in case it is needed to add new features, and it is compliant with the IEEE 802.11a/g physical layer standard. On top of this modem, and being the main contribution of this paper, a deterministic, real-time and cognitive Medium Access Control (MAC) layer has been implemented and evaluated. Based on a Time Division Multiple Access (TDMA) MAC, which ensures deterministic communications in the absence of interference, cognitive capabilities have been added. Unlike traditional cognitive radios, which are used in order to enhance spectrum utilization, the presented wireless communication system is able to detect interference (malicious or coming from other wireless communication systems) and switch the communication to an unoccupied and safe frequency band. Simulations in OPNET and measurements on real hardware are

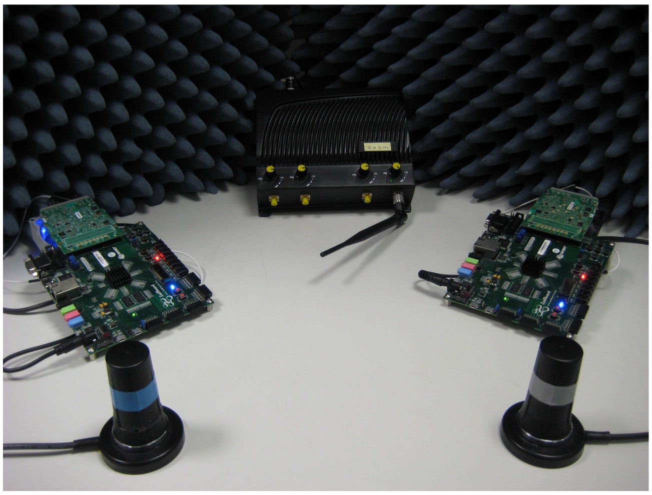

Fig. 1. Detail of the test setup: OFDM modem and jammer.

also presented, which demonstrate the capability of the system to guarantee deterministic data delivery time even in the presence of interference.

The remainder of the paper is organized as follows: related work is presented in Section II. In Section III the FPGA implementation of the OFDM physical layer, base of the presented wireless communication system, is described. The deterministic, real-time and cognitive MAC, main contribution of this paper, is explained in Section IV. In Section V, system performance results of the implementation are presented; all of them in terms of delay and system recovery time against interference. Finally, concluding remarks and future work are summarized in Section VI.

II. Related work

There are several wireless communication systems in the literature which aim to fulfill some of the aforementioned requirements of industrial applications or tactical communications. Unfortunately, at the best of authors' knowledge, they do not cover all of them in the way the presented communication system does. This section aims to gather and explain some of these wireless communication systems in order to contextualize and give value to the presented work.

In the field of customizable radio modems, the WARP project [2] aims to develop a scalable and extensible programmable wireless platform. It offers a real-time FPGA implementation of the IEEE 802.11 OFDM PHY and Distributed Coordination Function (DCF) MAC. Unfortunately, this project does not go further in the implementation of higher Open System Interconnection (OSI) layers. Besides, it does not provide at the moment the necessary hardware blocks so as to implement the time synchronization mechanisms needed for deterministic and real-time communications.

The MAC is one of the most important layers in a communication system for ensuring data reliability and time bounds. Several MACs have been proposed in the literature from both cognitive and non-cognitive approaches. P. Suriyachai, et al. present a MAC layer called GinMAC [3]. It is based on a TDMA and includes mechanisms to obtain the required end-to-end reliability and delay bounds. Unfortunately, during some tests in an industrial environment in Portugal, functional problems related with the presence of interference arose. W. Shen, et al. propose another relevant critical MAC: PriorityMAC [4]. Also based in a TDMA access, it handles four priorities for data to be sent: data for emergency safety actions, extremely critical control, critical control and periodic monitoring. Despite implementing mechanisms to prioritize a particular type of traffic, no time bound is ensured using this MAC. Besides, it does not have mechanisms to overcome the effects of interference. Among the cognitive radio approaches, which do take into account the presence of interference, the MAC presented by K. Kunert, et al. [5] is the most interesting. It is based on a TDMA scheme, and it reserves time within a frame to exchange control/spectrum sensing information. This MAC aims to select the most suitable frequency for the communication at any given moment. Unfortunately, it does not foresee the possibility of a destructive interference that blocks the complete transmission of data. Consequently, in case of interference, the network has to be formed again which leads to recovery times unsuitable for time-critical applications.

With regard to jamming-resistant wireless communication systems, several approaches have been presented. [6], [7] and [8] address the jamming problem from a signal processing point of view. They present several strategies, based on spread spectrum techniques, which do not try to avoid the interference but mitigate its effects. Unfortunately, none of the systems deal with real-time and deterministic data delivery time. Other approaches take advantage of cognitive radio capabilities. Q. Wang et al. [9] present a system which, unlike other Cognitive Radio implementations, assumes that malicious interference may not be predictable and may completely disrupt communication. On this basis, the proposed system implements an algorithm that continuously keeps exploring the best set of channels for transmission. Available channels are sorted based on both, spectrum sensing and a reward policy applied each time a successful communication is achieved in a particular channel. In case of a disruptive interference, the whole system switches to the next frequency band in the set. Although this algorithm is able to avoid interference, no further information is given with regard to system recovery time or medium access strategy, thus not being able to determine if the system ensures deterministic data delivery time and real-time characteristics.

Communications in tactical or industrial close-loop control applications require short latency, minimal jitter, deterministic data delivery time and high reliability, even in the presence of malicious interference. Therefore, our proposed wireless communication system implements a MAC layer that fulfills all these requirements as a whole, unlike previous systems that address them individually.

III. OFDM modem over FPGA

The physical layer of the proposed communication system is an OFDM transmitter and receiver implemented in FPGA

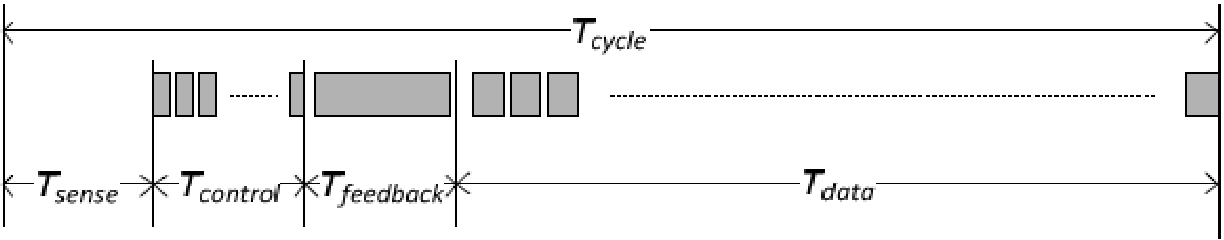

Fig. 2. Frame structure of DRMAC [5].

programmable logic. This type of implementation takes advantage of the parallelization possibilities of the FPGA, thus achieving low latency in the transmission and reception processes. Besides, the reconfigurable nature of FPGAs allows a complete customization of any of the signal processing algorithms present in the modem and the possibility of adding new features in case it is necessary. The modem has been designed, tested and implemented using the rapid prototyping tool named Xilinx System Generator.

The OFDM modem is compatible with the IEEE 802.11a/g standard at the physical level. It implements a 52 subcarrier OFDM scheme (48 data subcarriers and 4 pilot subcarriers) which can be modulated with BPSK, QPSK, 16-QAM or 64-QAM constellations. The modem in configurable to the following data rates: 6, 12, 24, 36 and 54 Mbits/s. These rates are high enough for the small amount of data that close-loop control applications demand (short messages of several bytes length).

Harnessing the aforementioned customization characteristics that FPGAs offer, and in order to enable cognitive features in the MAC layer, an energy detector (ED) has been included in the OFDM modem. The detector analyses the energy present in the current channel. If the energy is greater than a certain threshold, the ED decides that the sensing is under the hypothesis that a transmission is taking place in that channel. The performance of an ED is reduced under uncertainty noise, so an estimator of the noise power has been implemented. The noise information is estimated using recursive averaging.

The presented wireless communication system has been implemented in the Nutaq ZeptoSDR platform [10]. The ZeptoSDR consists of a ZedBoard, a low-cost development board for the Xilinx Zynq-7000 all programmable SoC, and a Radio420S module, a reconfigurable RF front-end which is able to select a frequency band between 300 MHz and 3 GHz. The OFDM modem has been implemented in the programmable logic of the Zynq SoC while the upper communication layers, i.e. the real-time, deterministic and cognitive MAC layer, have been software-implemented in the ARM core present in the Zynq SoC.

Despite the reconfigurable front-end is able to work in any frequency between 300 MHz and 3 GHz, the current implementation is limited to work only in 4 different frequencies: 2.4 GHz, 1.2 GHz, 1.1 GHz and 868 MHz. It should be noted that the communication system has been tested in an anechoic chamber, without interfering with the licensed bands of 1.2 and 1.1 GHz.

IV. Deterministic, Real-Time and Cognitive MAC

The proposed MAC is based on the MAC presented by K. Kunert, et al. [5] to which a novel handoff algorithm has been added. This improvement allows interference avoidance in a deterministic way. This MAC, also known as DRMAC, follows the general TDMA frame structure depicted in Fig. 2. At the beginning of the frame, each node senses the spectrum using the ED. During the control period, each node sends the spectrum sensing results to the coordinator of the network in its corresponding control slot. Besides, the coordinator sends an acknowledgement (ACK) to each node to confirm the reception of the ED results. Then, the coordinator generates a Sorted Channel List (SCL) using the channel information gathered by the nodes, and transmits it during the feedback period. In this list, the channels are sorted in function of its occupation, in a way that the least busy channel is the first channel in the list. If the occupation difference between the first and second channel exceeds a given threshold, the system changes its transmission band. Finally, a normal TDMA slot is used to transmit data traffic. Moreover, a frame start slot has been added at the beginning, to synchronize the network and a service slot at the end to send configuration packets.

In order to avoid a possible jammer, in our implementation the control period is used to monitor whether the channel is interfered or not as well as to generate the SCL. During this period, the coordinator receives in each control slot a packet from a node, while the node receives an ACK packet if the transmission was carried out correctly. Therefore, if the coordinator does not receive a packet, an error is considered. In the same way, nodes consider an error if no ACK packet is received. As a jammer causes bursty losses, it is considered that a jammer is interfering the band after a certain number of consecutive errors (N). When this number of consecutive errors is detected, every node in the networks hops to another band. The SCL is used to decide the band to hop, therefore, every node in the network hops to the same frequency band.

To characterize the real-time behavior of the MAC, a theoretical analysis using Network Calculus [11] has been carried out. This analysis establishes a theoretical delay bound considering the input traffic and the traffic which the network is capable of handling. A periodic input traffic and a maximum number of retransmissions M have been considered. Each packet is transmitted M times and, after this time, it is discarded because a transmission timeout is considered as an error in real-time applications. Therefore, the maximum delay d is obtained taking into account these conditions is

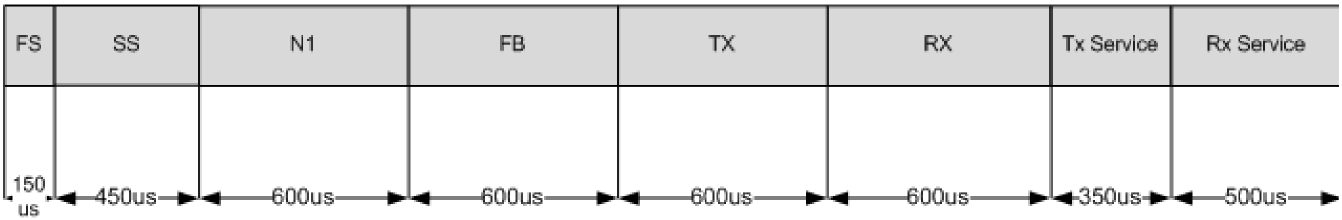

Fig. 3. Frame structure of the implemented MAC.

$$d \leq M \cdot c + t_{tx} \tag{1}$$

where M is the maximum number of retransmissions, c is the frame length and t_{tx} the transmission time which depends on the packet length and the bit rate. This bound will be ensured if the closed-loop control cycle time is higher than d.

The MAC layer and the wireless network have been modeled in the OPNET network simulator. A simple network composed by a coordinator and a node has been deployed. Note that the network design is scalable for several network devices in a star topology, but this example serves to represent the backbone link of a train communication network (link between two train consists). Concerning the TDMA scheduler configuration, the number of consecutive errors to hop to another channel has been set up to 3 and the maximum number of retransmissions of a packet to 4. This way, in case of the appearance of jamming interference in the transmission band, after the system hops to an interference free band, still a packet retransmission would be left, thus guaranteeing its deliver.

With this setup, the resulting TDMA frame structure and timing can be seen in Fig. 3, with a total frame length of 3850 us. Besides, with the OFDM modem configured with a data rate of 12 Mbps and sending 50 Byte messages, the maximum theoretical delay obtained with network calculus, even in the presence of a jamming interference in the transmission band, is

$$d \leq 4 \cdot 3850 + 600 \xrightarrow{yields} d \leq \ 16\, ms \tag{2}$$

The situation in which more than one band is being interfered has not been considered in the above analysis due to the life-cycle that data in closed-loop control application has. Packets arriving after two or more consecutive frequency hops would be discarded for this reason. However, it is interesting to know the time in which the system recovers after the appearance of interference. This analysis has also been carried out with network calculus. This recovery time *rt* is given by

$$rt \leq N \cdot l \cdot c + t_{tx} \tag{3}$$

where N is the numbers of bands that are simultaneously being interfered and l the number of consecutive communication errors that the network accepts after hopping to a new band.

For example, with the aforementioned setup, and considering that 2 out of the 4 available bands are being interfered, the maximum system recovery time is:

$$rt \leq 2 \cdot 3 \cdot 3850 + 600 \xrightarrow{yields} rt \leq \ 23.7\, ms \tag{4}$$

This theoretical delay bounds will be verified via simulations and measurements in real hardware in the next section.

V. Implementation, simulations and Measurements

This section presents the FPGA implementation results, and the simulations and measurements carried out that demonstrate the deterministic, real-time and jamming-resistant capacities of the presented wireless communication system.

A. *FPGA implementation*

Table I shows the FPGA logical resources consumed by the OFDM modem implementation. It can be seen how the modem fits in the available resources of the low-cost Xilinx XC7Z020 FPGA that has been used.

The physical layer implementation of the modem achieves a minimum input sensitivity level of -79 dBm, for a QPSK modulation per each OFDM subcarrier.

B. *Deterministic and real-time behaviour*

Fig. 4 shows the simulation and measurement results that demonstrate the deterministic behavior of the proposed system. The figures depict the probability Density Function (PDF) of the end-to-end time latency from the generation of a data packet to be transmitted (control cycle time of 30 ms) to its reception in the receiver. Two scenarios have been measured: the first scenario is an ideal one, with no interference, in which no packets are lost. Thus, no retransmissions happen. In the second one, two antennas have been plugged to the system and a controlled sporadic interference has been introduced in order

TABLE I: FPGA RESOURCE UTILIZATION

	SLICE	**REGISTER**	**LUT**	**DSP**	**BRAM 18 kbits**
Number	11612	38637	33805	180	140
Percentage	87%	36%	63%	81%	25%

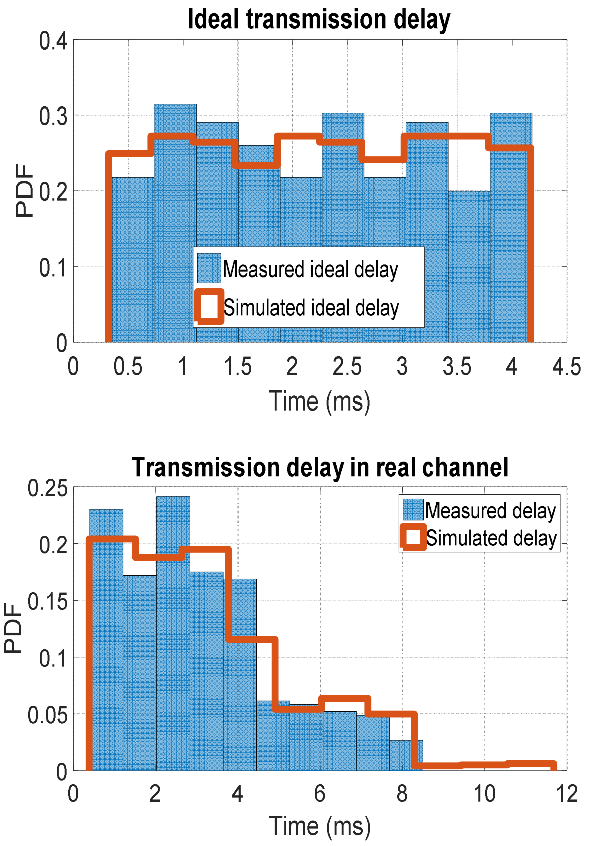

Fig. 4. Transmission delay simulations and measurements.

to generate packet losses and retransmissions. This interference could emulate the WiFi traffic environment that can be found in a train station. The aim of this test is to measure the deterministic behavior of the MAC against sporadic packet losses. Therefore, the handoff algorithm has been disabled so that the system does not hop to an interference free band where no retransmissions would happen.

As it can be seen in Fig. 4, in the ideal scenario, the transmission delay is bounded to the length of a single frame plus a small processing time. In the real scenario, as some packets are lost and retransmissions take place, the delay increases. Most of data packets are received during the first frame but some of them arrive during the second one after one retransmission. In any case, the system behaves in a real-time and deterministic way, fulfilling the control cycle time requirements and remaining below the theoretical maximum delay calculated with network calculus of 16 ms.

C. Jamming-resistant behaviour

Table II shows the time needed by the system to change its transmission/reception frequency. Due to the RF front-end characteristics, two different times are considered. “Channel change time” if the frequency hop is smaller than 50 MHz and “Band change time” if the frequency hop is greater. As it can be seen, the achieved frequency reconfiguration times are smaller than a single TDMA frame. Thus, it is possible to implement agile cognitive algorithms.

Fig. 5 presents the simulations and measurements carried out in order to test the behavior of the jamming-resistant feature. In the appearance of interference, the time needed to hop to a safe frequency band and recover the communication is measured. With this purpose, a commercial jammer (TX4CA from Projammers) has been added to the real scenario presented in the previous section. Three different jamming scenarios have been tested:

- *Scenario A*: Only the frequency in which the communication system is working is interfered. A singe frequency hop is forced. Under these circumstances it can be seen, both in simulations and in the measurements, how the recovery time is bounded between 8.5 and 12.5 ms. This time corresponds to the loss of 2 to 3 frames plus a slot of the next one. That is, the necessary time so as to lose 3 consecutive feedback messages or ACKs.

- *Scenario B*: The frequency in which the communication system is working and the next one in the SCL are interfered. Two frequency hops are forced. In this case, recovery time is bounded between 20 and 23.7 ms. This time corresponds to two consecutive recovery processes. That is, to the loss of 5 to 6 consecutive frames.

- *Scenario C*: The frequency in which the communication system is working and another band are interfered. Randomly, depending on the state of the SCL, one or two frequency hops are forced. In this last scenario, a mixture of the results of the above two scenarios can be observed. Taking into account that the state of the SCL table is not controlled in this test, after the first frequency change, the system can randomly hop into a free or interfered band. Therefore, system recovery times are distributed between this two possibilities, achieving the same time boundaries of the aforementioned two scenarios. It should be noted that in the simulations, the SCL status is completely random. Therefore, after the first frequency change, the probability of hopping to the second interfered band is 1/3, as can be seen in Fig. 5. However, in the real scenario, the SCL is updated with the spectrum sensing data, thus penalizing the interfered band. Accordingly, the probability of hopping to this band gets reduced.

It should be noted that the obtained maximum system recovery times match the maximum time of 23.7 ms estimated via network calculus theoretical analysis.

VI. CONCLUSIONS

TABLE II: FREQUENCY CHANGE TIME

	Change Time
Band change	191 us
Channel change	50 us

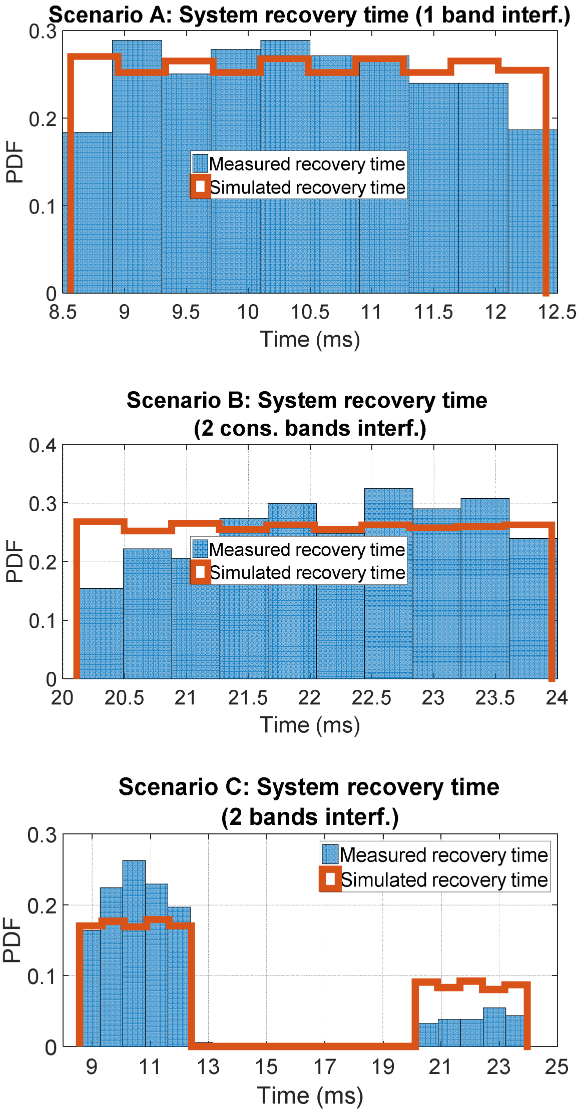

Fig. 5. System recovery time simulations and measurements.

In this paper a jamming-resistant and deterministic wireless communication system has been presented. A custom implementation of an OFDM modem design has been carried out into the low-cost Xilinx XC7Z020 FPGA. The proposed MAC layer, which includes a novel spectrum handoff algorithm for interference avoidance, has proven to behave in a real-time and deterministic way, achieving bonded data delivery times. Besides, the cognitive features added to the MAC, provide the system with jamming-resistant features that allow the wireless communication system to recover from a malicious interference in a short and deterministic time. All these features allow the presented system to be used in time-critical and mission critical industrial or tactical applications, in which data delivery has to be bonded in the reliability and time domains. With regard to future work, the improvement of the spectrum sensing algorithm is planned. The integration of cyclostationary signal detectors would allow the system to distinguish different interference types (users and jammers) and act accordingly.

ACKNOWLEDGMENT

This work was partly supported by TIPOTRANS (ETORTEK) and CIIRCOS (PC2013-68) projects of the Basque Government (Spain), and by COWITRACC (TEC2014-59490-C2-1-P/2-P) project of the Spanish Ministry of Economy and Competitiveness.

REFERENCES

[1] Rodriguez, P., Torrego, R., Casado, F., Fernandez, Z., Mendicute, M., Arriola, A., Val, I.: 'Wideband cognitive wireless communication system: implementation of an RF-Ethernet bridge for control applications'. Proc. Wireless Innovation Forum European Conference on Communication Technologies and Software Defined Radio (SDR'14 – WInnComm – Europe), Rome (Italy), Year 2014

[2] https://warpproject.org/, accessed 2016

[3] P. Suriyachai, et al., "Time-critical data delivery in wireless sensor networks," in Distributed Computing in Sensor Systems, 2010, pp. 216-229

[4] W. Shen, et al., "PriorityMAC: A priority-enhanced MAC protocol for critical traffic in industrial wireless sensor and actuator networks," IEEE Transactions on Industrial Informatics, vol. 10, pp. 824-835, 2014

[5] K. Kunert, et al., "Deterministic real-time medium access for cognitive industrial radio networks," in IEEE International Workshop on Factory Communication Systems - Proceedings, WFCS , art. no. 6242549 , pp. 91-94, 2012.

[6] Q. Dong, et al., "Adaptive Jamming-Resistant Broadcast Systems with Partial Channel Sharing" in IEEE 30th International Conference on Distributed Computing Systems (ICDCS), 2010

[7] M. Liechti et al., "Jamming Mitigation by Randomized Bandwidth Hopping" in The 11th International Conference on emerging Networking EXperiments and Technologies (ACM CoNEXT 2015), 2015

[8] C. Pöpper et al., "Jamming-resistant Broadcast Communication without Shared Keys" in Proceedings of the 18th conference on USENIX security symposium (SSYM'09), 2009

[9] Q. Wang et al., "Anti-jamming Communication in Cognitive Radio Networks with Unknown Channel Statistics" in 19th IEEE International Conference on Network Protocols (ICNP), 2011

[10] http://www.nutaq.com/blog/zeptosdr-architecture-and-api, accessed 2017

[11] J.-Y. Le Boudec and P. Thiran, *Network Calculus: A Theory of Deterministic Queuing Systems for the Internet*. Berlin, Heidelberg: Springer-Verlag, 2001.