An FPGA Based 24 GHz Radar Testbed for Physical-layer Cyberattack Research

Onur Toker
Electrical and Computer Engineering
Florida Polytechnic University
Lakeland FL, 33805
Email: otoker@floridapoly.edu

2021 IEEE Radar Conference (RadarConf21) | 978-1-7281-7609-3/20/$31.00 ©2021 IEEE | DOI: 10.1109/RadarConf2147009.2021.9455199

Abstract*—In this paper, we present a low cost Ka-band radar testbed using commercial off-the-shelf components. The motivation for this design comes from the popular S-band radar known as the MIT radar or coffee-can radar. To be able to do experimental research and real-time tests with a radar, we need two critical subsystems (1) A microwave circuit with I/Q outputs, and (2) A baseband processing system with high-speed ADC/DACs. Our main objective for building this testbed is to use it for physical-layer cyberattack research, attack resilience testing, OFDM radar and joint radar-communication tests. The proposed microwave circuit is built using commercial off-the-shelf microwave parts, and the baseband system is another commericial off-the-shelf FPGA board with Zynq SoC and 100 mega-sample per second dual ADC and dual DAC. There are three possible workflows for this testbed (1) All DSP processing is done on the FPGA fabric, (2) A baremetal system is running on the ARM side, and part of the DSP is done on the ARM, and the rest is done on the FPGA fabric, (3) An embedded linux system is running on the ARM for better connectivity and multitasking capability, and DSP workload is shared between the FPGA fabric and the ARM cores. In a future version of this paper, more detailed examples with FPGA design and ARM source codes will be presented.

I. Introduction

Automotive radars are critical sensors for advanced driver assistance systems (ADAS) and autonomous vehicle (AV) applications [1]. Frequency modulated continuous wave (FMCW) radars have a simple architecture, but orthogonal frequency division multiplexing (OFDM) radars have a different and more advanced architecture, and offer joint radar and communication capability [2], [3], [4]. OFDM radar algorithms and joint radar-communication methods have been studied in [5], [6], [7], [8], and [9], [4], [10]. Physical-layer cyberattacks is also an important problem for automotive radars [11], [12]. Cyberattack resilient FMCW designs have been investigated in [13], [14], and interference is studied in [15]. For both physical-layer cyberattack resilient radar tests, as well as OFDM based joint radar-communication experiments, an easy to use, low-cost testbed using only commercial off-the-shelf components will be highly valueable for the research community. To the best of author's knowledge, there are really very limited options for experimental testbeds, and the main motivation for this paper is to introduce one such feasible option.

This paper is organized as follows: In Section II we present the microwave subsystem, and in Section III the FPGA subsystem. The complete radar system with real experimental data and analysis is presened in Section IV. Finally, in Section V, we make some concluding remarks and suggest future research directions.

II. Microwave subsystem

The proposed microwave subsystem block diagram is shown in Fig. 1. This is basically a frequency modulated continuous wave (FMCW) radar system, which has voltage controlled oscillator (VCO), splitter, mixer, and a single amplifier. Indeed, this system has been tested without any amplifier at all, and it has been observed that for a reflector of size 50 cm by 50 cm and approximately 1 meter away from the TX/RX antennas (See Fig. 6) the I-channel output of the mixer has peak-to-peak amplitude less than 1 mV, but still clearly visible when measured with a Tektronix MDO 3104. The configuration presented in this paper has a single amplifier, and has been used only for short range experiments. However, an amplifier before the TX antenna, and another one before the mixer LO input will result improved performance for longer range experiments. Alternatively, a single amplifier between the VCO and the splitter may also be used to improve long range detection performance.

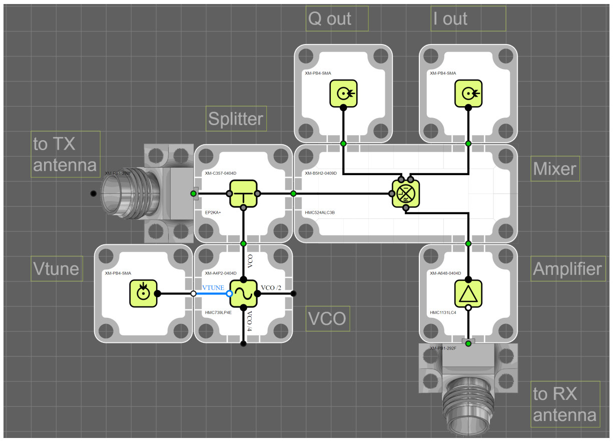

Fig. 1. The microwave subsystem block diagram.

A. The VCO

The VCO used in this system is Analog Devices HMC739LP4 based with 8 dBm output, and is available in

PCB format from X-microwave with part number XM-A4P2-0404D. The voltage regulator circuit needed to operate the VCO is below the prototyping plate (See Fig. fig:vco). For V_{tune} between 1 V and 13 V, the output frequency changes from approximately 23 GHz to 28 GHz, but there is a noticeable nonlinearity in the frequency/voltage characteristics [16]. For V_{tune} between 2 V and 8 V, the VCO frequency/voltage characteristics are quite linear, but when operated outside this range, a nonlinearity correction algorithm can be used to achieve better range accuracy [17]. In Fig. 2, the VCO's V_{tune} input is driven with a 2 V to 6 V ramp signal using a Tektronix AFG 3052C, and the VCO output is monitored with a Keysight spectrum analyzer.

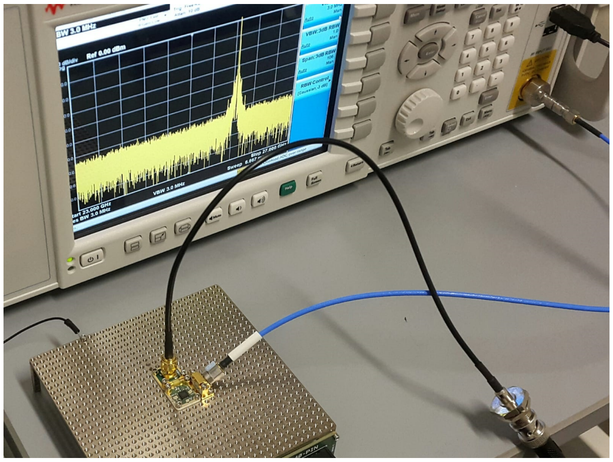

Fig. 2. Testing the VCO with a spectrum analyzer. Output frequency is measured as 26 GHz when V_{tune} is 6 V.

B. The Splitter

The splitter used in this system is a Mini-circuits EP2KA+ based passive device, and is available in PCB format from X-microwave with part number XM-B7P4-0404D. This device has a typical 0.9 dB insertion loss over 3 dB, therefore, the output signal going to the TX antenna will be typically at 4 dBm level. Similarly, the LO input of the mixer will be typically at 4 dBm.

C. The Mixer

The mixer used in this system is an I/Q mixer with two double-balanced mixers. It is based on Analog Devices HMC524ALC3B, and is available in PCB format from X-microwave with part number XM-B5H2-0409D. At LO level of 17 dBm, the conversion loss is around 9 dBm. For the configuration used in this paper, the LO input of the mixer is around 4 dBm, which is well below the 17 dBm level. However, for short range experiments, the I-channel output of the mixer is still large enough to be measured easily, see Fig. 3

D. The Amplifier

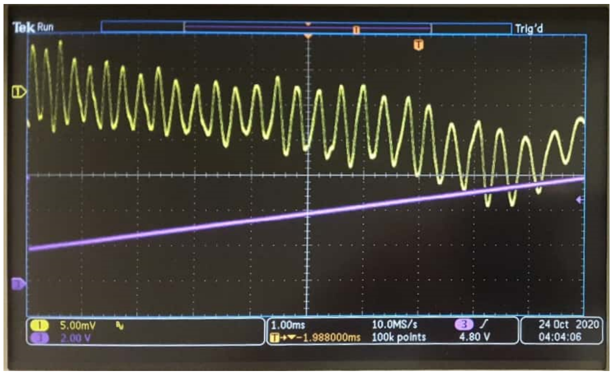

Fig. 3. The I-channel output of the mixer for a 50 cm by 50 cm target at 1 m distance. Oscillations are around 10 mV peak-to-peak, the ramp signal is from 2 V to 6 V and has 10 ms period.

The amplifier stage is based on Analog Devices HMC1131LC4, and is available in PCB format from X-microwave with part number XM-A648-0404D. The gain of the amplifier stage is 22 dB with P1=24 dBm. The biasing circuit needed to operate the amplifier is below the prototyping plate. For the configuration used in this paper, there is a single amplifier used to amplify the RX signal, however for longer range experiments, a secondary amplifier between the VCO and the splitter will result better performance for long range experiments.

E. Fully assembled microwave subsystem

The fully assembled microwave system is shown in Fig. 4. All voltage regulator and bias circuits are under the prototyping plate. There are two 2.92 mm K-connectors for TX and RX antennas, and two SMA connectors for V_{tune} input and mixer I-channel output. For the configuration used in this paper, we don't have an SMA connector mounted at the Q channel output of the mixer.

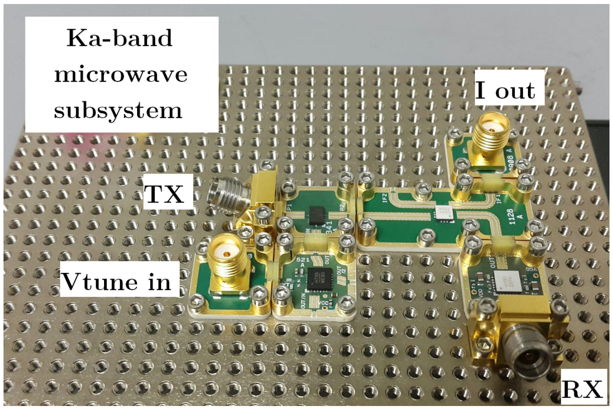

Fig. 4. Photo of the fully assembled Ka-band microwave subsystem. All voltage regulator and bias circuits are under the prototyping plate.

III. FPGA SUBSYSTEM

The FPGA system is based on a Zynq System-on-Chip, and is shown in Fig. 5 as a standalone board, and in Fig. 6 as part of the complete radar testbed. The FPGA board, Zmod connector based ADC and DACs, and the case are all available from Digilent as Eclypse Z7. Compared to FMC connector based solutions, and higher end RFSoC alternatives, this is a low-cost baseband system under $1K. The Zmod ADCs can operate at $\pm 1V$ range with 14-bit resolution and achieve 0.13 mV absolute resolution. Even without any baseband amplification, a 10 mV peak-to-peak signal (See Fig. 3) means 6.2-bit resolution.

The FPGA subsystem can be used with three different workflows:

(1) All DSP processing is done on the FPGA fabric,
(2) A baremetal system is running on the ARM, and all DSP tasks are shared between the FPGA fabric and the ARM,
(3) An embedded linux system is running on the ARM cores, and DSP workload is shared between the FPGA fabric and the ARM cores.

In this paper, we used the second workflow. Both Zmod ADC and DAC devices are operated by using a high-speed logic circuit realized on the FPGA fabric. Both of these circuits have internal buffers capable of storing more than 16000 samples per channel, and designs are provided in open source format by Digilent. There are also two AXI DMA engines realized on the FPGA fabric, and these are used for high-speed data transfers between the DDR RAM of the ARM and the BRAMs of the FPGA.

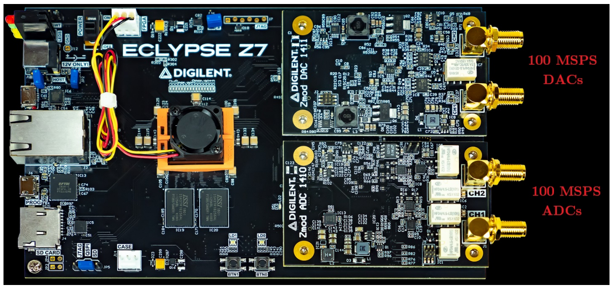

Fig. 5. Photo of the FPGA subsystem with 100 MSPS DAC and ADCs.

The programming model is quite simple. For the Zmod DAC, we first transfer the desired data from the DDR RAM to the internal BRAM of the FPGA using an AXI DMA. Once started, it operates in standalone mode and generates a periodic waveform till it is stopped by the processor. During regular operation, it does not use the processor or the DDR RAM. The Zmod ADC also has an internal buffer, and once started it acquires dual channel data every 10 ns. When the internal buffer is full, all data in the BRAM can be transfered to DDR RAM using another AXI DMA. Digilent GitHub has open source example designs for both Zmod DACs and ADCs, and the author simply customized these examples for the experimental results presented in the next section.

IV. The Complete Radar Testbed

The complete radar testbed is shown in Fig. 6. There are two horn antennas connected to the 2.92 mm K-connectors on the microwave subsystem. The V_{tune} input and the I-channel output of the mixer are connected to the FPGA subsystem using short SMA cables. The Eclypse Z7 can be used as a standalone device, or can be used with a host PC using gigabit ethernet and serial connectivity.

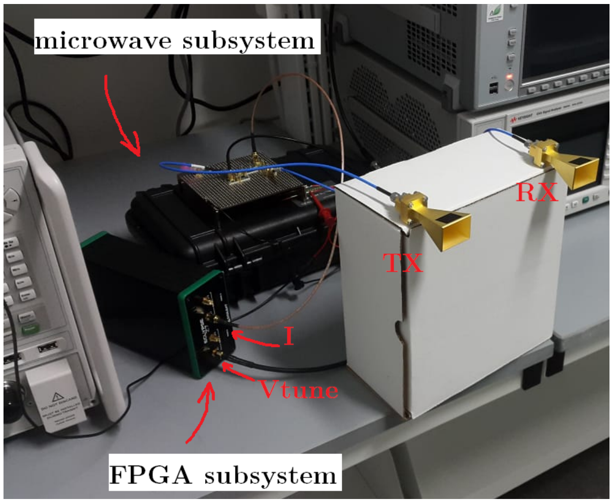

Fig. 6. Photo of the Ka-band radar testbed. None of the lab VNA or spectrum analyzers are needed to operate the system, only DC power supplies are needed.

For the experimental results presented in this section, we simply acquired the mixer I-channel output and transfered it to the host PC for MATLAB based analysis. For real-time hardware-in-the-loop tests, Eclypse Z7 can also be used either as a baremetal or as an embedded linux standalone system without a host PC. This requires the DSP algorithms to be realized on the FPGA fabric and the ARM cores, rather than as MATLAB scripts running on the host PC.

A. Experimental results

In Fig. 7, we present a basic test result obtained using the proposed testbed. This is for a 50 cm by 50 cm target at 1 m distance, and the plot shown in the figure is the normalized FFT of the I-channel output of the mixer. The VCO's V_{tune} input is driven by a 2 V to 5 V ramp signal resulting a 1.5 GHz sweep. However, a 0 V to 5 V ramp will result a wider sweep and hence a better range resolution, but needs to be used with a nonlinearity correction DSP algorithm.

In Fig. 7, we see a strong line-of-sight coupling peak around 0 m, and another peak at 2 m possibly because of secondary reflections.

V. Conclusion

In this paper, we presented a low-cost FPGA based 24 GHz radar testbed for physical-layer cyberattack research, and OFDM based joint radar-communication experiments. There are two critical subsystems, a Ka-band microwave subsystem and an FPGA subsystem with high-speed ADC and DACs. Both subsystems are available as commercial of-the-shelf products, and are well documented. Compared to the Texas Instruments AWR series 77 GHz radars studied in [18], the proposed system is highly flexible, and has a simple and open architecture, which makes it ideal for experimental research and real-time testing. In a future version of this paper, more

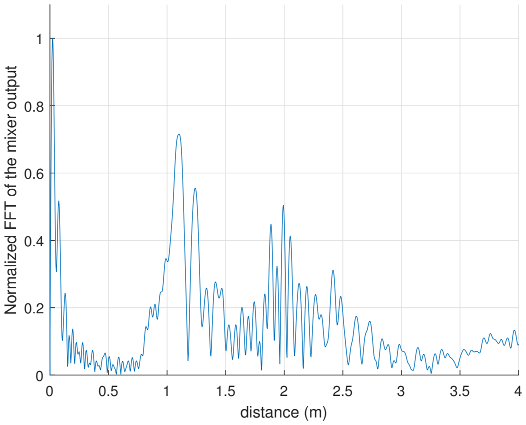

Fig. 7. Normalized FFT of the mixer output for a 50 cm by 50 cm target at 1 m distance. This is without any nonlinearity correction, and calibration.

detailed examples with FPGA design and source codes will be presented.

Acknowledgment

This work has been supported in part by NSF grant 1919855, Advanced Mobility Institute grants GR-2000028, GR-2000029, and the Florida Polytechnic University grant GR-1900022.

References

[1] S. M. Patole, M. Torlak, D. Wang, and M. Ali, "Automotive radars: A review of signal processing techniques," *IEEE Signal Proc. Mag.*, vol. 34, pp. 22–35, Mar. 2017, https://doi.org/10.1109/MSP.2016.2628914.

[2] D. Garmatyuk and K. Kauffman, "Radar and data communication fusion with uwb-ofdm software-defined system," in *2009 IEEE International Conference on Ultra-Wideband*, 2009, pp. 454–458.

[3] C. Sturm and W. Wiesbeck, "Waveform design and signal processing aspects for fusion of wireless communications and radar sensing," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1236–1259, 2011.

[4] C. D. Ozkaptan, E. Ekici, and O. Altintas, "Demo: A software-defined ofdm radar for joint automotive radar and communication systems," in *2019 IEEE Vehicular Networking Conference (VNC)*, 2019, pp. 1–2.

[5] N. Levanon, "Multifrequency radar signals," in *The Record of the IEEE 2000 International Radar Conference*, 2000, pp. 683–688.

[6] G. E. A. Franken, H. Nikookar, and P. van Genderen, "Doppler tolerance of ofdm coded radar signals," in *Proc. 3rd European Radar Conference*, 2006.

[7] B. Donnet and I. Longstaff, "Combining mimo radar with ofdm communications," in *3rd European Radar Conference (EuRAD 2006)*, 2006.

[8] M. Braun, "Ofdm radar algorithms in mobile communication networks," Ph.D. dissertation, Karlsruher Instituts für Technologie, 2014.

[9] C. D. Ozkaptan, E. Ekici, O. Altintas, and C. Wang, "Ofdm pilot-based radar for joint vehicular communication and radar systems," in *2018 IEEE Vehicular Networking Conference (VNC)*, 2018, pp. 1–8.

[10] C. D. Ozkaptan, E. Ekici, and O. Altintas, "Enabling communication via automotive radars: An adaptive joint waveform design approach," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*. IEEE Press, 2020, p. 1409–1418. [Online]. Available: https://doi.org/10.1109/INFOCOM41043.2020.9155527

[11] C. Bhat, "Cybersecurity challenges and pathways in the context of connected vehicle systems," Data-Supported Transportation Operations & Planning Center (D-STOP), Austin, TX, Tech. Rep. 134, Feb. 2018, https://ctr.utexas.edu/wp-content/uploads/134.pdf.

[12] S. Alland, W. Stark, M. Ali, and M. Hegde, "Interference in Automotive Radar Systems: Characteristics, Mitigation Techniques, and Current and Future Research," *IEEE Signal Proc. Mag.*, vol. 36, pp. 45–59, Sep. 2019, https://doi.org/10.1109/MSP.2019.2908214.

[13] O. Toker, S. Alsweiss, J. Vargas, and R. Razdan, "Design of an Automotive Radar Sensor Firmware Resilient to Cyberattacks," in *Proceedings of the 2020 IEEE SoutheastCon*, Raleigh, NC, 2020.

[14] O. Toker and S. Alsweiss, "Design of a Cyberattack Resilient 77 GHz Automotive Radar Sensor," *MDPI, Electronics*, 2020, https://doi.org/10.3390/electronics9040573.

[15] F. Jin and S. Cao, "Automotive radar interference mitigation using adaptive noise canceller," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 3747–3754, 2019.

[16] "HMC739LP4/739LP4E," Data Sheet, Analog Devices.

[17] O. Toker and M. Brinkmann, "A Novel Nonlinearity Correction Algorithm for FMCW Radar Systems for Optimal Range Accuracy and Improved Multitarget Detection Capability," *MDPI, Electronics*, 2019, https://doi.org/10.3390/electronics8111290.

[18] O. Toker, S. Alsweiss, and M. Abid, "A Computer Vision Based Testbed for 77 GHz mmWave Radar Sensors," in *Proceedings of the 2020 IEEE SoutheastCon*, Raleigh, NC, 2020.