openwifi: a free and open-source IEEE802.11 SDR implementation on SoC

Xianjun Jiao, Wei Liu, Michael Mehari, Muhammad Aslam, Ingrid Moerman
IDLab, Ghent Univeristy - imec, Gent, Belgium

***Abstract*—Open source Software Defined Radio (SDR) project, such as srsLTE and Open Air Interface (OAI), has been widely used for 4G/5G research. However the SDR implementation of the IEEE802.11 (Wi-Fi) is still difficult. The Wi-Fi Short Inter-Frame Space (SIFS) requires acknowledgement (ACK) packet being sent out in 10μs/16μs (2.4GHz/5GHz) after receiving a packet successfully, thus the Personal Computer (PC) based SDR architecture hardly can be used due to the latency ($\geq 100\mu$s) between PC and Radio Frequency (RF) front-end. Researchers have to do simulation, hack a commercial chip or buy an expensive reference design to test their ideas. To change this situation, we have developed an open-source full-stack IEEE802.11a/g/n SDR implementation — openwifi. It is based on Xilinx Zynq System-on-Chip (SoC) that includes Field Programmable Gate Array (FPGA) and ARM processor. With the low latency connection between FPGA and RF front-end, the most critical SIFS timing is achieved by implementing Physical layer (PHY) and low level Media Access Control (low MAC) in FPGA. The corresponding driver is implemented in the embedded Linux running on the ARM processor. The driver instantiates Application Programming Interfaces (APIs) defined by Linux mac80211 subsystem, which is widely used for most SoftMAC Wi-Fi chips. Researchers could study and modify openwifi easily thanks to the modular design. Compared to PC based SDR, the SoC is also a better choice for portable and embedded scenarios.**

***Index Terms*—SDR, Wi-Fi, IEEE802.11, FPGA, mac80211, SoftMAC, Linux driver, AD9361, Zynq, SoC, open source**

I. Introduction

SDR has brought a paradigm shift to research by implementing traditional radio hardware/chip functionality in software running on PC. For mobile communication standards, this type of SDR platform works well, because the latency between PC and RF front-end (like USRP) is much less than the ACK latency. For example, the ACK is expected 4ms after sending a packet in Hybrid Automatic Repeat Request (HARQ) procedure of Long Term Evolution (LTE) system. However the SIFS of Wi-Fi/IEEE802.11 [1] makes the PC based SDR implementation difficult. This big difference between two systems comes from the different spectrum character. In licensed spectrum, everything can be centrally controlled by the operator; while in shared spectrum, random access is an effective strategy for distributed coordination among nodes contending for the medium without central coordination and interference mitigation. SIFS ensures that ACK packet grabs the medium before any other potential transmissions and each pair of data-ACK occupies the channel as short as possible. Lacking an easy SDR solution, simulators (like NS3) are widely used for research. Researchers also hack commercial Wi-Fi chips [2] for experiment. Commercial Wi-Fi SDR reference designs [3], [4] are also used if the budget can be afforded. To help the community, we have developed the free and open source full-stack IEEE802.11 SDR implementation — openwifi [5]. The current version supports 802.11a/g/n standards and also can be changed to different bandwidth modes (802.11p DSRC, 802.11ah) thanks to the flexibility of SDR. With this project, researchers can test new ideas more easily than before.

II. System architecture and building blocks

Fig. 1 shows the openwifi implementation architecture. ARM, FPGA and RF are the 3 main physical blocks. ARM and FPGA actually are in a single chip: Zynq SoC. The AD9361 front-end is connected to Zynq via high speed FPGA Mezzanine Card (FMC) interface. The embedded Linux running on ARM offers a user friendly wireless network research environment where openwifi is seen as a normal Wi-Fi card in Linux. Openwifi supports Off-the-shelf SDR platform, such as Xilinx ZC706 board with AD-FMCOMMS2 plugin, ADRV9361-Z7035 and ADRV9364-Z7020.

In FPGA, low MAC and PHY (openofdm_rx, openofdm_tx) are implemented. The receiver is based on openofdm [11] with the necessary bug fixes and extra functionalities made by openwifi project. rx_intf routes I/Q samples to the receiver and passes the demodulated packet to Linux via master AXI4-Stream Direct Memory Access (AXIS DMA) with necessary information inserted. tx_intf get packets from Linux via slave AXIS DMA and queues them waiting for the right transmission opportunity decided by the xpu. Xpu implements Distributed Coordination Function (DCF) MAC defined in section 10.3 of [1], such as RSSI and preamble based Clear Channel Assessment (CCA), virtual carrier sensing, Network Allocation Vector (NAV), random back off, Timing Synchronization Function (TSF), ACK reply, Request-to-Send/Clear-to-Send(RTS/CTS), re-transmission, etc.

Linux kernel driver is developed to access the low level modules via AXI Lite (for FPGA register), AXIS DMA (for data transfer) and Serial Peripheral Interface (for RF). The top level "SDR driver" instantiates Linux mac80211 [12] APIs (in struct ieee80211_ops of Linux source code). "sdrctl" user space tool can access driver and FPGA modules via Linux 802.11 netlink-based userspace interface (nl80211). Other native Linux tools, such as iw, iwconfig, wpa_supplicant and hostapd, can also run in the same way as other commercial Wi-Fi chips.

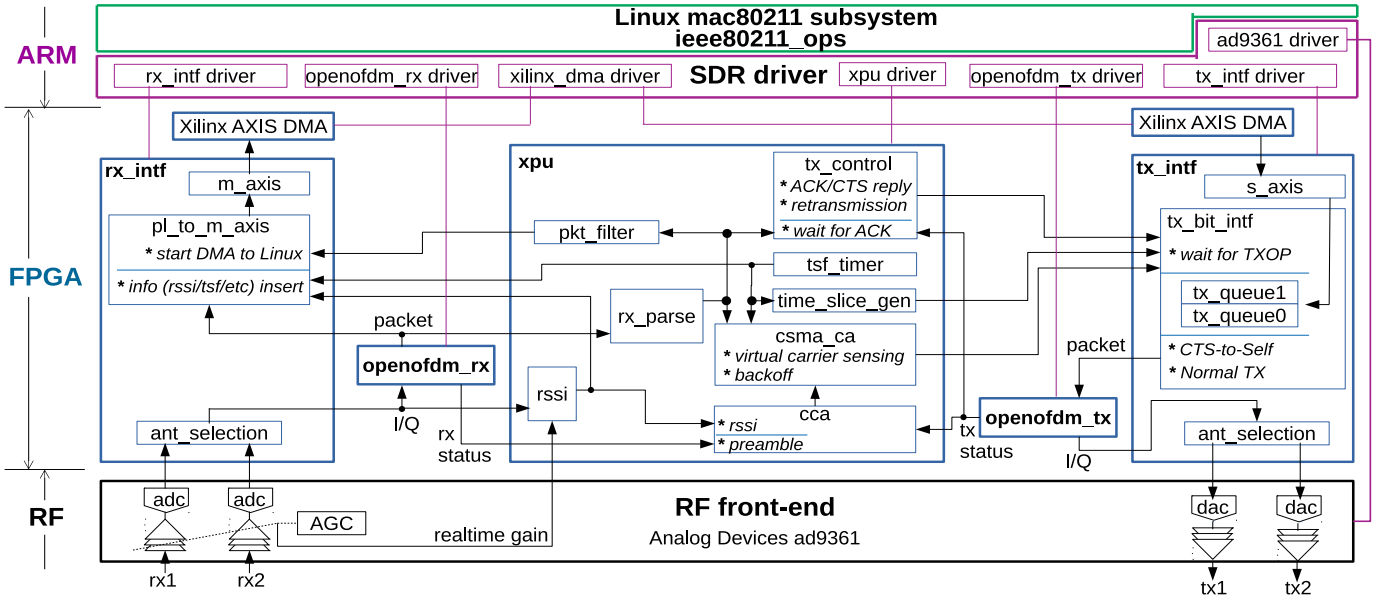

Fig. 1. System architecture of openwifi

	Baseband platform	PHY layer	CSMA Low MAC	High MAC and upper	SIFS	Free&Open
imec, openwifi [5]	SoC (FPGA+ARM)	FPGA	FPGA (State machine)	ARM (Linux)	10μs	Yes
WARP, 802.11 design [3]	FPGA	FPGA	FPGA Microblaze (C)	FPGA Microblaze (C)	16μs	No
NI, Labview 802.11 [4], [6]	FPGA + PC	FPGA	FPGA (State machine)	PC (NS3)	16μs	No
H. Wu, Tick Mobicom17 [7]	FPGA + PC	FPGA	FPGA Microblaze (C)	PC (Linux)	16μs	No
Microsoft, SORA/Ziria [8][1], [9]	RCB board + PC	C/Ziria	C/Ziria	C/Ziria	10μs	Yes
B. Bloessl, gr-ieee802-11 [10]	PC	Gnuradio	/	/	/	Yes

1. RCB: Radio Control Board. Need patched Windows OS. 10μs ACK can't be achieved for short incoming packet due to insufficient calculation time.

TABLE I
OPENWIFI VERSUS RELATED PROJECTS

III. Related works

Table I summarizes the differences between openwifi and the related works. SIFS means the shortest SIFS achieved. The combination of SoC and embedded Linux makes openwifi unique amongst the related works.

IV. Conclusion

An SoC based open-source full-stack IEEE802.11 SDR implementation is developed for the community. The module based design can help implementing innovative ideas on different aspects of wireless system. The embedded design makes the project suitable for the scenario where power consumption and form factor are constrained.

Acknowledgment

The work was funded by the European Union's Horizon 2020 framework under grant agreement no. 732174 (ORCA project).

References

[1] IEEE, "Part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications," *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, pp. 1–3534, Dec 2016.

[2] M. Schulz, D. Wegemer, and M. Hollick. (2017) Nexmon: The c-based firmware patching framework. [Online]. Available: https://nexmon.org

[3] Mango Communications, Inc. 802.11 mac/phy design. [Online]. Available: https://mangocomm.com/802.11-mac-phy/, http://warpproject.org/trac/wiki/802.11

[4] National Instruments. (2016) Labview communications 802.11 application framework 2.0 and 2.0.1. [Online]. Available: http://www.ni.com/product-documentation/53279/en/

[5] J. Xianjun, L. Wei, and M. Michael. (2019) open-source ieee802.11/wi-fi baseband chip/fpga design. [Online]. Available: https://github.com/open-sdr/openwifi

[6] National Instruments. (2018) Multi-layer prototyping: Hardware and software. [Online]. Available: https://orca-project.eu/wp-content/uploads/sites/4/2018/10/Multi-Layer-Prototyping.pdf

[7] H. Wu, T. Wang, Z. Yuan, C. Peng, Z. Li, Z. Tan, B. Ding, X. Li, Y. Li, J. Liu *et al.*, "The tick programmable low-latency sdr system," in *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*. ACM, 2017, pp. 101–113.

[8] K. Tan, H. Liu, J. Zhang, Y. Zhang, J. Fang, and G. M. Voelker, "Sora: High-performance software radio using general-purpose multi-core processors," *Commun. ACM*, vol. 54, no. 1, pp. 99–107, Jan. 2011. [Online]. Available: http://doi.acm.org/10.1145/1866739.1866760

[9] G. Stewart, M. Gowda, G. Mainland, B. Radunovic, D. Vytiniotis, and C. L. Agullo, "Ziria: A dsl for wireless systems programming," *ACM SIGPLAN Notices*, vol. 50, no. 4, pp. 415–428, 2015.

[10] B. Bastian. (2013) An ieee 802.11a/g/p ofdm receiver for gnu radio. [Online]. Available: https://github.com/bastibl/gr-ieee802-11

[11] S. Jinghao. (2017) Openofdm: Synthesizable, modular verilog implementation of 802.11 ofdm decoder. [Online]. Available: https://openofdm.readthedocs.io/en/latest/

[12] The kernel development community. mac80211 subsystem. [Online]. Available: https://www.kernel.org/doc/html/v4.16/driver-api/80211/mac80211.html