Software-Defined Radio (SDR) as a Mechanism for Exploring Cyber-Electronic Warfare (EW) Collaboration

Warren P. du Plessis
Department of Electrical, Electronic and Computer Engineering
University of Pretoria
Pretoria, South Africa
Email: wduplessis@ieee.org

***Abstract*—Cyber is concerned with networks of systems in all their possible forms. Electronic warfare (EW) is focused on the many different uses of the electromagnetic spectrum (EMS). Given that many networks make use of the EMS (wireless networks), there is clearly large scope for collaboration between the cyber-warfare and EW communities. Unfortunately, such collaboration is complicated by the significant differences between these two realms. Software-defined radio (SDR) systems are based on interfaces between the EMS and computers and thus offer tremendous potential for encouraging cyber-EW collaboration. The concept of SDR is reviewed along with some hardware and software SDR systems. These are then used to propose a number of projects where SDR systems allow collaboration between the cyber and EW realms to achieve effects which neither realm could achieve alone.**

***Keywords*—Electronic warfare (EW), cyber, software-defined radio (SDR), electromagnetic spectrum (EMS).**

I. Introduction

Electronic warfare (EW) deals with maximising the value of the electromagnetic spectrum (EMS) for friendly users while denying similar benefits to adversaries. In this way, the EMS is used as the vehicle to achieve desired tactical or strategic outcomes. These seemingly simple statements hide a wealth of complexity and controversy, as seen by the large number of articles and letters published on the role of EW in the Journal of Electronic Defense (JED) over the last few years [1]–[8].

Cyber has similar objectives to EW, but differs in that the mechanism used to achieve desired outcomes is information technology and networks rather than the EMS. This difference in mechanism means that the barrier to entry for cyber is lower than for EW leading to a wide range of actors, source locations, motivations, etc. [9], [10]. As a result of this diversity, even books on cyber note the difficulty in obtaining a clear definition of what cyber really is [11]–[14].

A number of papers have explored the relationship between cyber and EW and noted a significant overlap between these realms [15]–[17]. This overlap arises from the widespread use of wireless technologies in networks. This use of the EMS in wireless networks introduces EW considerations into the cyber realm. Equally, the potential use of EW techniques and technologies to achieve outcomes in the cyber realm mean that cyber considerations are relevant to EW. The overlap between cyber and EW is thus becoming increasingly important to achieve the full potential of both.

More importantly, commanders require a clear understanding of implications of the different approaches to achieving a given objective, be they cyber, EW, kinetic, propaganda and others. The required understanding cannot be gained without understanding the relationship between cyber and EW. The large number of sources considering the definitions of cyber and EW noted above is a clear indication that this relationship is not clearly understood.

While studies considering the relationship between cyber and EW could be useful, such studies alone are unlikely to provide the required answers. Again, the large number of references considered above bear this observation out. What is really required is that cyber and EW professionals collaborate on projects from one another's realms. In this way, the people developing the technologies driving these fields can explore how best to collaborate. The results of such explorations are likely to be more useful, as they would be driven by technical and operational considerations rather than issues such as politics, inter-service rivalry and the like.

Before such collaboration can be contemplated, a platform suitable for the rapid implementation and testing of cyber-EW concepts is required. Such a platform should ideally allow both cyber and EW professionals to use the tools with which they are familiar, while simplifying the sharing of information. Furthermore, any collaborative platform should allow changes to be rapidly implemented and tested to facilitate the speedy evaluation of new cyber-EW concepts as they are developed. While these requirements for a suitable platform may appear fanciful, modern software-defined radio (SDR) systems have the potential to achieve all these requirements.

This paper will argue that SDR systems should be used as a means to explore collaboration between cyber and EW. This will be done by considering the basic concepts behind SDR in Section II as a prelude to an evaluation of the suitability of some SDR hardware and software platforms to the imple-

This work is based on the research supported in part by the King Abdulaziz City for Science and Technology (KACST) and by the National Research Foundation of South Africa (NRF) (Grant specific unique reference number (UID) 85845). The NRF Grantholder acknowledges that opinions, findings and conclusions or recommendations expressed in any publication generated by the NRF supported research are that of the author(s), and that the NRF accepts no liability whatsoever in this regard.

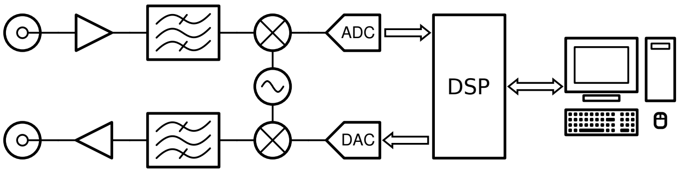

Fig. 1. SDR system architecture.

mentation of cyber-EW systems in Sections III and IV. This information will then be used as the basis of suggestions for future work which are provided in Section V. Lastly, a brief summary and conclusion are provided in Section VI.

II. Description of SDR

The main concept underlying SDR is that digital signal processing (DSP) algorithms can relatively easily be modified to accommodate new functionality [18], [19]. In terms of communications systems, this means that a new protocol (modulation, handshaking, encryption, etc.) can be implemented on a system as long as the DSP hardware is capable of performing the relevant processing and the radio frequency (RF) hardware is capable of operating at the correct frequency with the required bandwidth.

Figure 1 shows a simplified functional diagram of the SDR systems considered in Section III. The input signal is first amplified and filtered before being mixed down to a lower frequency where it is sampled by a analogue-to-digital converter (ADC). The output signal is converted to analogue form by a digital-to-analogue converter (DAC), mixed up to the operating frequency, filtered and amplified. Given that signals are digitised, signal processing can be performed digitally using a device such as a field-programmable gate array (FPGA). This digital processing of the signal is the main reason for the versatility of SDR systems as all modulation, demodulation, coding, decoding, handshaking and other processing are performed digitally.

As shown in Figure 1, the digitised signals can also be transferred to a computer and further processed and/or stored there. While this is not a requirement for an SDR system, it is useful here because this allows RF signals to be manipulated on a computer. This approach also speeds the development of new systems as the signal processing can be implemented on a computer, rather than requiring the time-consuming development of FPGA firmware, for example. While this approach is inherently inefficient because it is based on a computer with far greater processing power than required, it is nonetheless a useful approach to rapidly implement and test new concepts.

III. SDR Hardware

This section will provide a short overview of some SDR hardware platforms with the emphasis on their suitability for cyber-EW system implementation. The focus in this section will be on low-cost, open-source devices for which information such as the firmware and driver code, and circuit schematics are available. However, a number of other options exist, including those based on the PCI extensions for instrumentation (PXI) and LAN extensions for instrumentation (LXI) interface standards [20], [21].

A. Ettus Universal Software Radio Peripheral (USRP) Range

The best-known SDR hardware platforms are almost certainly those manufactured by Ettus Research [22]. The popularity and success of Ettus' systems is highlighted by the fact that Ettus Research has been part of National Instruments since 2010.

Arguably the best combination of performance and price is to be found in the USRP B200 and B210 systems based on the Analog Devices AD9361 and AD9364 RF transceiver chips [23]. The main difference between these two devices is that the B210 has two transmitters and two receivers, while the B200 has only a single transmitter and a single receiver. These systems can operate over an extremely wide range of frequencies (70 MHz to 6 GHz) and have high-speed ADCs and DACs allowing 56 MHz of bandwidth to be considered at a time. Despite this high performance, the cost of these devices is only $675 for the B200 and $1,100 for the B210. The main drawback of the B200 and B210 is that they are supplied without a housing and the printed circuit board (PCB) does not have mounting holes, thereby complicating the development of custom housings.

Other interesting devices within the USRP range are the E100 and E110 stand-alone SDR systems. The only difference between the E100 and E110 is that the E110 has a more powerful FPGA to allow more complex signal processing to be performed. These devices run a version of Linux and are thus able to operate without requiring an interface to a computer, though an Ethernet interface is provided. The E100 and E110 require RF daughterboards which determine the range of frequencies over which the devices can operate, and available daughterboards allow operation from 0 Hz to 6 GHz (though different daughterboards are required to cover this full range). The E100 and E110 are capable of operating over bandwidths of 50 MHz or more depending on the daughterboard used. The E100 and E110 are packaged in a metal housing. The current pricing of the E100 is $1,300 and the E110 is $1,500. The one concern here is that the similar B100 SDR system has been discontinued [24], suggesting that the E100 and E110 may also be discontinued in the near future.

B. Nuand bladeRF

The Nuand bladeRF is a comparatively new SDR system and has been available since mid-2013 [25]. Interestingly, much of the development work on the bladeRF was crowd-funded demonstrating the high-level of interest in SDR systems [26].

The bladeRF is based on the Lime Microsystems LMS6002D RF transceiver chip [27]. This allows the bladeRF to operate from 300 MHz to 3.8 GHz and to can instantaneously operate over a bandwidth of 28 MHz. The bladeRF is supplied without a housing, but the PCB does have mounting holes to simplify the development of custom housings.

The bladeRF is available in two versions, the x40 which costs $420 and the x115 which costs $650, with the only difference being that the x115 has a more powerful FPGA.

C. HackRF

The HackRF is an SDR system developed by Michael Ossmann [28], and was initially funded by the Defense

Advanced Research Projects Agency (DARPA) and later by crowdfunding [29].

The HackRF is capable of operating from 10 MHz to 6 GHz and has an instantaneous bandwidth of 20 MHz. The main drawback of the HackRF is that it is only capable of half-duplex operation and is thus not capable of simultaneously transmitting and receiving. However, this limitation is not anticipated to be significant in the majority of cyber-EW systems as most communications links operate in half-duplex mode. The HackRF is the smallest of the SDR systems considered here and is supplied in a injection-molded enclosure with metal housings available as optional extras.

While not currently available, the HackRF can be preordered for $299.

D. RTL-SDR

The RTL-SDR range of systems arises from the use of the Realtek RTL2832U Digital Video Broadcasting – Terrestrial (DVB-T) demodulator and Universal Serial Bus (USB) interface chip in a number of USB DVB-T receivers [30]. The RTL2832U is able to stream raw ADC samples over a USB interface.

The main difference between the RTL-SDR devices and the other SDR devices considered here is that the RTL-SDR systems do not include a transmitter and are thus only capable of receiving signals. The frequency range over which a specific RTL-SDR device operates is determined by the tuner used, and the Rafael R820T operates over a range of approximately 24 MHz to 1.75 GHz [30], for example. Unfortunately, none of the RTL-SDR devices cover the 2.4 GHz band used by wireless local-area networks (LANs). Furthermore, RTL-SDR devices are limited to bandwidths of 3.2 MHz, and in practice, the bandwidth is limited to only 2.4 MHz because attempting to use wider bandwidths results in lost samples.

These disadvantages are counteracted somewhat by the extremely low cost of RTL-SDR devices, which is on the order of $20 depending on the supplier. This extremely low cost has meant that RTL-SDR devices have been used for a large number of receiver-based SDR applications [31]. For example, the author has found these devices extremely useful to demonstrate how easily RF signals can intercepted and how congested the EMS is.

IV. SDR Software

Given the wide range of open-source SDR hardware available and the tremendous importance of radio technologies, it is not surprising that a large number of SDR software packages exist. This section will mainly focus on free and open-source software (FOSS) SDR packages, but again, it is worth noting that a number of powerful commercial packages also exist.

A. Driver Code

The SDR hardware platforms described in Section III are all provided with FOSS drivers. This allows tremendous flexibility because users of these platforms can write their own code based on these drivers.

All the drivers for the platforms considered in Section III can be compiled using the FOSS GNU's Not Unix! (GNU) Compiler Collection (GCC) tools. This allows FOSS libraries useful for signal processing, such as GNU Scientific Library (GSL) [32] and Fastest Fourier Transform in the West (FFTW) [33], to be exploited when implementing the necessary signal-processing algorithms. Data can then be shared between this EW RF interface and the higher-level cyber functionality using the developers' language of choice. For example, GNU Radio (see Section IV-B) includes functions for GNU Octave [34], allowing the powerful libraries available for Octave, including signal-processing functionality [35], to be exploited.

B. GNU Radio

GNU Radio is a FOSS platform intended to facilitate the implementation of SDR applications by providing standard signal-processing blocks [36].

GNU Radio-based applications are primarily developed in Python [37], but a graphical interface (the GNU Radio Companion) and a GNU Octave interface are also available. Performance-critical paths are coded in C++, allowing high performance to be achieved while relying on relatively simple interfaces.

The success of GNU radio is demonstrated by the number of applications developed using the building blocks it provides. These include

- decoding transponder signals from commercial aircraft [38],
- decoding of the Automatic Identification System (AIS) tracking and identification transmissions from ships [39],
- decoding images from weather satellites [40],
- Wi-Fi interfaces [41],
- decoding Long-Term Evolution (LTE) signals [42], and
- many others [43].

C. Standard Interfaces

Probably the most useful software packages for cyber-EW collaboration are those which implement standard communications protocols. Despite the complexity of many standards, a surprisingly large number of FOSS implementations of these standards are available.

Arguably the most interesting of these from the perspective of cyber-EW collaboration is the WiME project which implements the Institute of Electrical and Electronics Engineers (IEEE) 802.11a/g/p Wi-Fi protocols [41]. This software implements a full orthogonal frequency division multiplexing (OFDM) transceiver, thereby allowing access to Wi-Fi networks.

Probably more impressive are the FOSS implementations of a Global System for Mobile Communications (GSM) base station and extensions to allow General Packet Radio Service (GPRS) and Enhanced Data Rates for GSM Evolution (EDGE) to be implemented [44], [45]. These packages offer the possibility of implementing small GSM networks.

More recently, a number of LTE implementations have emerged [42], [46]–[49]. While many of these implementations are still relatively immature, they can be expected to mature rapidly.

Implementations of other protocols including Terrestrial Trunked Radio (TETRA) [50] and Digital Enhanced Cordless Telecommunications (DECT) [51] also exist.

V. Possibilities for Further Research

This section outlines some possibilities for cyber-EW collaboration enabled by the SDR systems described above.

A. Long-Range Hacking

One of the major challenges in EW is intercepting extremely weak signals from distant transmitters and interfering with the operation of distant transmitters and receivers. The importance of stand-off capabilities to EW has led to the development of a number of relevant technologies.

These technologies could be exploited by cyber professionals to gain access to distant networks, thereby removing the need for proximity to a target for cyber attacks to be successful.

SDR systems allow the signal-processing aspects of long-range EW technologies to be implemented in a relatively simple way. Furthermore, the versatility of SDR systems allows the integration of low-noise amplifiers (LNAs), high-power amplifiers, antenna arrays, direction finding (DF) systems and other technologies familiar to EW professionals. The fact that the output of the system is available on a computer will greatly facilitate allowing cyber professionals to gain the full benefit of these EW technologies.

In this way, existing EW technologies can be exploited to create a new method of attacking vulnerable systems using cyber techniques. This would allow the effectiveness of both cyber and EW to be greatly enhanced.

B. Interdisciplinary Attacks

The overlap between cyber and EW has already been noted in Section I of this document. Vulnerabilities within this overlap region are likely to be more difficult to analyse and evaluate due to the need for expertise from both the cyber and EW realms.

The higher levels of the Open Systems Interconnection (OSI) model are clearly the domain of cyber, while the lower levels are equally clearly the domain of EW [15]–[17]. It is between these extremes where many interesting possibilities lie due to overlap between cyber and EW. This overlap region is characterised by signals having been demodulated and decoded, but still including significant aspects related to their transmission through the EMS. While EW professionals will understand the implications of the EMS on the data, the actual processing of those data is more strongly in the cyber realm. There is thus a clear need for both cyber and EW expertise here.

SDR systems, especially the protocol implementations outlined in Section IV-C allow a unique opportunity to operate in this overlap region. As full protocols – or at least large portions of those protocols – are implemented in a FOSS way, modifications to standard signals become relatively simple to implement. Once implemented, access to the internal workings of a system complaint to the relevant protocol will facilitate the evaluation of such modifications on the operation of the system.

By encouraging cyber and EW professionals to collaborate in the region where both move outside the clear definitions of their normal realms, complex new attacks are likely to be developed. As these attacks will lie in the overlap between cyber and EW, they are likely to be extremely successful as adversaries' responses could hindered by uncertainty as to which realm should address the relevant vulnerability.

C. Experimental Networks

The nature of cyber and EW attacks is that the goal is to disrupt the operation of the systems they attack. This leads to obvious difficulties where the effect of such attacks on important commercial or military networks is evaluated.

SDR systems offer the potential to construct small networks which are representative of their larger cousins. The versatility of SDR hardware platforms is such that these experiments could be conducted at frequencies which differ from those of the networks being modelled, thereby removing the possibility of unintentional interference. For example, a small GSM network could be constructed based on the software described in Section IV-C, allowing experiments which would never be approved on commercial GSM networks to be conducted.

By enabling such experiments to be conducted, SDR systems will allow cyber and EW professionals to gain a greater understanding of the different approaches which can be used to attack a network.

D. Vulnerability Assessment

Vulnerability of networks is a major consideration in both cyber and EW. A significant challenge in vulnerability assessment is obtaining the full picture of all the RF transmissions of a specific network. These transmissions can cover an extremely wide frequency range and comprise a large variety of communication protocols.

While it is possible to utilise an extremely large number of different systems to evaluate each of the frequency bands and communications protocols a network may use, this approach is unlikely to be practical. SDR systems offer the possibility of using a single piece of hardware coupled with a computer to completely evaluate the vulnerabilities of a network.

In this case, the EW professional's knowledge of communications systems and how to both intercept and interfere with them are likely to be valuable to their cyber colleagues. Similarly, the cyber professional's understanding of how attacks on a specific communications link affect the networks those links part of can help guide their EW colleagues' attacks. In this way, far more effective attacks can be devised, and more importantly, more robust networks can be developed.

E. Academic Research

The global community of academics is enormous and represents a tremendous resource to technology-based realms such as cyber and EW.

Unfortunately, encouraging academics to become involved with relevant research is often complicated by the understandable desire to keep information about operational systems, capabilities and techniques secret. Even if this problem can be overcome, the high cost and value of operational systems mean that their use for academic research is unlikely to be approved.

SDR systems allow capabilities similar to those of operational systems to be recreated at relatively low cost. The use of FOSS-based systems will allow secrecy concerns to be largely addressed because no information about operational systems is required to perform useful research. The lower cost and versatility of SDR systems will also lower the barrier to entry from a cost perspective. Furthermore, the cost of SDR systems is more acceptable because SDR systems can be used in many different applications.

SDR systems thus allow both cyber and EW professionals to involve their academic counterparts more strongly in their work. This could greatly facilitate the collaboration between the cyber and EW realms by allowing academics to explore the overlap between these fields while still being able to meet the academic requirement for publication.

VI. Conclusion

EW is concerned with the exploitation of the EMS, while cyber deals with networks of systems. The fact that many networks, especially those used by the military and security services, make use of the EMS clearly demonstrates the need for collaboration between cyber and EW professionals. Unfortunately, the very different technologies used by these two groups complicates such collaboration.

SDR systems are proposed as a means to facilitate cyber-EW collaboration. The fact that SDR systems provide a direct link between the EMS – the realm of EW – and computers – the realm of cyber – offers unique opportunities to grow cyber-EW collaboration.

A number of SDR hardware platforms and a wide range of SDR software packages were briefly summarised. Despite the low cost of these systems, the performance obtained is still remarkably good. The focus here was on open-source systems as this openness greatly simplifies complex modifications to existing systems. This openness takes the form of the availability of circuit diagrams and firmware source code for SDR hardware platforms, and of the full source code for SDR software packages.

Proposals for number of possible cyber-EW collaborative projects which are facilitated by the unique benefits of SDR systems were provided. Each of these proposals emphasises the complementary nature of cyber and EW and shows how each realm can benefit from collaboration with the other.

References

[1] J. Bourque, “A structural view of EM spectrum warfare,” *Journal of Electronic Defence (JED)*, vol. 33, no. 10, pp. 82–90, October 2010.

[2] J. Clifford, “What electronic warriors should know about physics, language and concepts,” *Journal of Electronic Defence (JED)*, vol. 34, no. 3, pp. 40–47, March 2011.

[3] J. Clifford, “Maneuver in the electromagnetic domain,” *Journal of Electronic Defence (JED)*, vol. 33, no. 1, pp. 33–36, January 2010.

[4] R. Hahn, “Physics of the Cyber-EMS problem – Why we have the language wrong,” *Journal of Electronic Defence (JED)*, vol. 33, no. 11, pp. 40–47, November 2010.

[5] J. Knowles, “Why two domains are better than one,” *Journal of Electronic Defense (JED)*, vol. 36, no. 5, pp. 48–50, May 2013.

[6] A. D. Givens and J. Knowles, “Questioning the two domains concept and response,” *Journal of Electronic Defense (JED)*, vol. 36, no. 8, p. 14, August 2013.

[7] E. Fisher, “More on Cyber and the EMS,” *Journal of Electronic Defense (JED)*, vol. 36, no. 10, p. 14, October 2013.

[8] T. Curby-Lucier, “Continuing the discussion of “two domains”,” *Journal of Electronic Defense (JED)*, vol. 36, no. 11, p. 14, November 2013.

[9] R. P. Van Heerden, B. Irwin, and I. Burke, “Classifying network attack scenarios using an ontology,” *Proceedings of the 7th International Conference on Information Warfare and Security (ICIW)*, p. 311, 2012.

[10] R. van Heerden, H. Pieterse, and B. Irwin, “Mapping the most significant computer hacking events to a temporal computer attack model,” in *ICT Critical Infrastructures and Society*. Springer Berlin Heidelberg, 2012, pp. 226–236.

[11] J. Andress and S. Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Elsevier Science, 2011.

[12] J. Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld*. O'Reilly Media, 2011.

[13] S. Winterfeld and J. Andress, *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*, ser. Syngress basics series. Elsevier Science, 2012.

[14] P. Shakarian, J. Shakarian, and A. Ruef, *Introduction to Cyber-Warfare: A Multidisciplinary Approach*. Elsevier Science, 2013.

[15] F. D. W. Maasdorp and W. P. du Plessis, “Using a layered model to place EW in its proper context,” in *Workshop on ICT uses in Warfare and the Safeguarding of Peace (IWSP)*, 16 August 2012.

[16] F. D. W. Maasdorp and W. P. du Plessis, “Using a layered model to place EW in context within the information sphere,” *Journal of Information Warfare*, vol. 11, no. 3, pp. 1–6, November 2012.

[17] F. D. W. Maasdorp and W. P. du Plessis, “Using a layered model to place EW in its proper context,” in *AOC International Symposium and Convention*, November 2011.

[18] W. H. W. Tuttlebee, “Software-defined radio: facets of a developing technology,” *IEEE ASSP MagazinePersonal Communications*, vol. 6, no. 2, pp. 38–44, Apr 1999.

[19] T. Ulversoy, “Software defined radio: Challenges and opportunities,” *IEEE ASSP MagazineCommunications Surveys Tutorials*, vol. 12, no. 4, pp. 531–550, April 2010.

[20] (2014, May) PXI Systems Alliance – Home > About PXI > PXI Architecture. PXI Systems Alliance. [Online]. Available: http://www.pxisa.org/About/Architecture/Default.aspx

[21] (2014, May) LXI Consortium – The Power of LAN, Ethernet and the Web Applied to Test & Measurement Instruments. LXI Consortium. [Online]. Available: http://www.lxistandard.org/

[22] (2013, July) Ettus Research. Ettus Research. [Online]. Available: http://www.ettus.com

[23] (2014, May) Analog Devices | Semiconductors and Signal Processing ICs. Analog Devices. [Online]. Available: http://www.analog.com/en/index.html

[24] (2014, May) Ettus Research – Product Detail. Ettus Research. [Online]. Available: https://www.ettus.com/product/details/UB100D-BDL

[25] (2013, July) Nuand | bladeRF. Nuand LLC. [Online]. Available: http://www.nuand.com

[26] (2013, July) bladeRF – USB 3.0 software defined radio by Nuand – Kickstarter. Nuand LLC. [Online]. Available: http://www.kickstarter.com/projects/1085541682/bladerf-usb-30-software-defined-radio

[27] (2014, May) Lime Microsystems. Lime Microsystems. [Online]. Available: http://www.limemicro.com/

[28] (2013, September) Great Scott Gadgets HackRF. [Online]. Available: http://greatscottgadgets.com/hackrf/

[29] (2013, September) HackRF, an open source SDR platform by Michael Ossmann – Kickstarter. [Online]. Available: http://www.kickstarter.com/projects/mossmann/hackrf-an-open-source-sdr-platform

[30] (2013, July) rtl-sdr – OsmoSDR. [Online]. Available: http://sdr.osmocom.org/trac/wiki/rtl-sdr

[31] (2014, May) rtl-sdr.com – A blog about RTL-SDR (RTL2832U) and cheap software defined radio. [Online]. Available: http://www.rtl-sdr.com/about-rtl-sdr/

[32] (2014, May) GSL – GNU Scientific Library – GNU Project – Free Software Foundation (FSF). Free Software Foundation (FSF). [Online]. Available: http://www.gnu.org/software/gsl/

[33] (2014, May) FFTW Home Page. [Online]. Available: http://www.fftw.org/

[34] (2013, August) GNU Octave. GNU. [Online]. Available: http://www.gnu.org/software/octave/

[35] (2013, August) Octave-Forge. [Online]. Available: http://octave.sourceforge.net/

[36] (2013, July) GNU Radio – WikiStart – gnuradio.org. [Online]. Available: http://gnuradio.org/redmine/projects/gnuradio/wiki

[37] (2013, August) Python Programming Language – Official Website. [Online]. Available: http://www.python.org/

[38] (2014, May) bistromath/gr-air-modes – GitHub. [Online]. Available: https://github.com/bistromath/gr-air-modes

[39] (2014, May) GNU AIS – Automatic Identification System for Linux. [Online]. Available: http://gnuais.sourceforge.net/

[40] (2014, May) Noaa weather satellite reception with gnu radio and usrp. [Online]. Available: http://www.oz9aec.net/index.php/gnu-radio-blog/350-noaa-weather-satellite-reception-with-gnu-radio-and-usrp

[41] (2014, May) Distributed Embedded Systems – Projects. Universität Paderborn Department of Computer Science. [Online]. Available: http://www.ccs-labs.org/projects/wime/

[42] (2014, May) kit-cel/gr-lte – GitHub. Communication Engineering Lab (CEL) at the Karlsruhe Institute of Technology (KIT). [Online]. Available: https://github.com/kit-cel/gr-lte

[43] (2014, May) AcademicPapers – GNU Radio – gnuradio.org. [Online]. Available: http://gnuradio.org/redmine/projects/gnuradio/wiki/AcademicPapers

[44] (2014, May) OpenBTS open-source project. Range Networks. [Online]. Available: http://openbts.org/

[45] (2014, May) OpenBSC – openBSC. Osmocom. [Online]. Available: http://openbsc.osmocom.org/

[46] (2014, May) OpenLTE. [Online]. Available: http://openlte.sourceforge.net/

[47] (2014, May) OSLD Project. [Online]. Available: https://sites.google.com/site/osldproject/

[48] (2014, May) Overview | Open Air Interface. EURECOM. [Online]. Available: http://www.openairinterface.org/

[49] (2014, May) LTE Base Station Software. [Online]. Available: http://bellard.org/lte/

[50] (2014, May) Osmocom TETRA. Osmocom. [Online]. Available: http://tetra.osmocom.org/trac/

[51] (2014, May) Osmocom DECT. Osmocom. [Online]. Available: http://dect.osmocom.org/