

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA, 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY) 06-04-2022	2. REPORT TYPE Final Report	3. DATES COVERED (From - To) 30-May-2016 - 29-May-2018
---	--------------------------------	---

4. TITLE AND SUBTITLE Final Report: Design and Building an Opportunistic Communications Prototype with Spectrum Contention and Cascades	5a. CONTRACT NUMBER W911NF-16-1-0323
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER 611103

6. AUTHORS	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES North Carolina State University Office of Sponsored Programs and Regulatory Compli: Campus Box 7514 Raleigh, NC 27695 -7514	8. PERFORMING ORGANIZATION REPORT NUMBER
--	--

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES) U.S. Army Research Office P.O. Box 12211 Research Triangle Park, NC 27709-2211	10. SPONSOR/MONITOR'S ACRONYM(S) ARO
	11. SPONSOR/MONITOR'S REPORT NUMBER(S) 68592-NS-RIP.1

12. DISTRIBUTION AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.
--

13. SUPPLEMENTARY NOTES The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Wenye Wang
a. REPORT UU	b. ABSTRACT UU	c. THIS PAGE UU			19b. TELEPHONE NUMBER 919-513-2549

RPPR Final Report

as of 11-Apr-2022

Agency Code: 21XD

Proposal Number: 68592NSRIP

Agreement Number: W911NF-16-1-0323

INVESTIGATOR(S):

Name: Wenye Wang
Email: wwang@ncsu.edu
Phone Number: 9195132549
Principal: Y

Organization: **North Carolina State University**

Address: Office of Sponsored Programs and Regulatory Compliance, Raleigh, NC 276957514

Country: USA

DUNS Number: 042092122

EIN: 566000756

Report Date: 29-Aug-2018

Date Received: 06-Apr-2022

Final Report for Period Beginning 30-May-2016 and Ending 29-May-2018

Title: Design and Building an Opportunistic Communications Prototype with Spectrum Contention and Cascades

Begin Performance Period: 30-May-2016

End Performance Period: 29-May-2018

Report Term: 0-Other

Submitted By: Wenye Wang

Email: wwang@ncsu.edu

Phone: (919) 513-2549

Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees: 2

STEM Participants: 2

Major Goals: (1) The proposed infrastructure is composed of three subnets that are interconnected, each of which allows both single-hop and multi-hop communications, which can support a variety of settings with dynamic spectrum detection and occupation in case of malicious interference and wireless jamming. Therefore, we will be able to collect very comprehensively, versatile data sets when spectrum sensing and scheduling information.

(2) The proposed infrastructure is quite comprehensive and advanced in the sense that there are two co-existing networks: (i) the cognitive radio network operating over the TV white spectrum frequencies of 54-60 MHz, 76-88 MHz, 174-216 MHz, 470-608MHz, and 614-698 MHz [1], and (ii) The 4G cellular, Long Term Evolution (LTE) network operating on bands 12 and 17 of the 700MHz LTE spectrum. We will use an 8-node computing cluster, universal software radio peripheral (USRP) X300, LTE base station (BS), and LTE user equipment (UEs). Therefore, this prototype allows us to study inhomogeneous wireless networks and evaluate the vulnerability of different combinations.

(3) The proposed infrastructure prototype is an open access system in that each wireless device is allowed to dynamically explore the spectrum under attacks and severe interference, achieving opportunistic communications in real settings rather than in theory or principle. To some extent, this infrastructure is a 'proof-of-concept' platform, which enables us to practice a large body of research outcomes. Furthermore, this project will be used for research-related education, that is, undergraduate and graduate students will be involved in building the prototype, thus gaining experience through participating in the project.

Accomplishments: We have accomplished the following tasks in the period of this project:

1. We have purchased the desirable equipment that is used to support a variety of settings with dynamic spectrum detection and occupation for 5G and beyond wireless use cases, as well as for detection of malicious interference and wireless jamming.
2. We have designed and implemented a measurement tool, namely U-CIMAN, using Universal Software Defined Radio Peripheral (USRP) and a Linux host computer in order to measure the spectrum occupancy of a commercial LTE cell, we set up two LTE cells under our control to facilitate the development of the Software Defined Radio (SDR) enabled tool and to validate its performance.
3. For the research front, we have published 4 papers that take the advantage of the equipment and this support was acknowledged. In addition, we have received two NSF grants for which the equipment from this grant was

RPPR Final Report

as of 11-Apr-2022

used as our essential facility.

NSF SpecEES: "Efficient Monitoring and Spectrum Utilization of Multi-Layer Wireless Networks " (2018-2022)

NSF SWIFT Large: MAC-on-MAC: A Spectrum Orchestrating Control Plane for Coexisting Wireless Systems (2021-2024).

4. For the education front, we have prepared a manual that is ready for courses of "Introduction to Wireless Networking" and "LTE Advances".

Training Opportunities: We have two graduate students involved in learning the up-to-date wireless equipment for research development.

Results Dissemination: We have published 4 papers and developed one hands-on manual for wireless teaching courses.

R. Zou and W. Wang, 'Downlink decoding based accurate measurement of LTE spectrum tenancy,' IEEE Transactions on Mobile Computing, 2021, [19].

R. Zou, W. Wang, and H. Dai, 'Temporal and spectral analysis of spectrum hole distributions in an LTE cell,' in 2021 IEEE Global Communications Conference: Cognitive Radio and AI-Enabled Network Symposium (Globecom2021 CRAEN), Madrid, Spain, 2021, [20]

R. Zou and W. Wang, 'U-CIMAN: Uncover spectrum and user information in LTE mobile access networks,' in IEEE INFOCOM 2020-IEEE Conference on Computer Communications. IEEE, 2020, pp. 1459–1468, [21]

• R. Zou and W. Wang, 'Change detection based segmentation and modeling of LTE spectrum tenancy' in 2019 IEEE Global Communications Conference (GLOBECOM). IEEE, 2019, pp. 1–6, [22].

Honors and Awards: Nothing to Report

Protocol Activity Status:

Technology Transfer: Nothing to Report

PARTICIPANTS:

Participant Type: PD/PI

Participant: Wenye Wang

Person Months Worked: 2.00

Project Contribution:

National Academy Member: N

Funding Support:

Participant Type: Graduate Student (research assistant)

Participant: Rui Zou

Person Months Worked: 6.00

Project Contribution:

National Academy Member: N

Funding Support:

Participant Type: Graduate Student (research assistant)

Participant: LoyCurtis Smith

Person Months Worked: 6.00

Project Contribution:

National Academy Member: N

Funding Support:

RPPR Final Report
as of 11-Apr-2022

Partners

,

I certify that the information in the report is complete and accurate:

Signature: Wenye Wang

Signature Date: 4/6/22 7:58PM

W911NF1610323 68592-NS-RIP: Final Technical Report

1 Research Objectives

The main objective of this project is to *design and build an opportunistic communication prototype* based on software defined radio networks, which is an integral engineering effort. We plan to explore new understandings and take first-hand measurements of spectrum sensing, spectrum detection and switching, spectrum contention, and spectrum cascades under interference and jamming such that we are able to transform our fundamental results into practical applications and further broaden the impact on wireless network design and reliable, secure communications. This infrastructure prototype is expected to be an example of using the latest off-the-shelf radio products to deploy guidelines from theoretical studies, intelligent algorithms of spectrum discovery and scheduling, and a variety of wireless attack strategies. In addition, we will use a cloud server and mobile cloud user terminals to examine the cloud computing techniques, as well as single- and multi-hop communications based on opportunistic spectrum acquisition. Therefore, our prototype will be able to offer innovative, solid insights with well-designed, comprehensive and controllable experiments and cross-verification of theoretical studies, while facilitating our curriculum development and mentoring activities. Therefore, the proposed infrastructure will contribute to both research and research-related education that are currently of the areas of interest to the DoD. In particular, the proposed work will contribute to the following areas for wireless research toward reliable and resilient communications and networking.

- The proposed infrastructure is composed of three subnets that are interconnected, each of which allows both single-hop and multi-hop communications, which can support a variety of settings with dynamic spectrum detection and occupation in case of malicious interference and wireless jamming. Therefore, we will be able to collect very comprehensive, versatile data sets when spectrum sensing, scheduling, and routing algorithms are applied, which will further provide guidelines for future wireless networks.
- The proposed infrastructure is quite comprehensive and advanced in the sense that there are two co-existing networks: (i) the cognitive radio network operating over the TV white spectrum frequencies of 54-60 MHz, 76-88 MHz, 174-216 MHz, 470-608MHz, and 614-698 MHz [1], and (ii) The 4G cellular, Long Term Evolution (LTE) network operating on bands 12 and 17 of the 700MHz LTE spectrum. We will use an 8-node computing cluster [2], universal software radio peripheral (USRP) X300 [3], LTE base station (BS) [4], and LTE user equipment (UEs) [5, 6, 7]. Therefore, this prototype allows us to study *inhomogeneous* wireless networks and evaluate the vulnerability of different combination.
- The proposed infrastructure prototype is an *open* access system in that each wireless device is allowed to dynamically explore spectrum under attacks and severe interference, achieving opportunistic communications in real settings rather than in theory or principle. To some extent, this infrastructure is a ‘proof-of-concept’ platform, which enables us to practice a large body of research outcomes. Furthermore, this project will be used for research-related education, that is, undergraduate and graduate students will be involved in building the prototype, thus gaining experience through participating in the project.

2 Devices and Equipment

The devices involved in our measurement system are listed in Table 1. The web page for the corresponding item can be opened by clicking the device name shown in the first column in blue.

Table 1: List of equipments in the Wireless Research Lab

Equipment	Brief description
Amarisoft OTS 100 Software (×1)	A complete LTE system bundle with the LTE core network software and base station software installed in a PC with an SDR card, and a COTS mobile device with a test SIM card. The software LTE core network includes MME with built-in SGW, PGW and HSS. The LTE base station software is release 13 compliant.
Amarisoft UE 100 Software (×1)	The LTE UE simulator that can simulate up to 1000 LTE mobile devices when installed in a powerful PC connected to an appropriate SDR device.
R&S FSH8.08 Spectrum analyzer (×1)	Hand-held spectrum analyzer with a built-in pre-amplifier, and a measurement range of 9kHz to 8GHz. When analyzing LTE signals, it has 20 MHz demodulation bandwidth.
R&S FSH-K50 LTE FDD pilot analyzer software (×1)	Software for FDD LTE downlink over-the-air signals analysis. It provides the spectrum overview, result summary, total power, carrier frequency error, I/Q offset, cell identity, cyclic prefix, reference signal power, PSS power, SSS power, PBCH power, PCFICH power, PDSCH power, reference signal EVM, PSS EVM, SSS EVM, PBCH EVM, PCFICH EVM, PDSCH EVM.
R&S FSH-K50E LTE FDD modulation analyzer software (×1)	Software for more advanced FDD LTE downlink signal analysis and advanced carrier aggregation. Display options include the constellation diagram (graphical), measured EVM value, modulation types and LTE signal components. Measurement results of up to three carriers can be displayed simultaneously. When measuring via the air interface, an LTE-BTS scanner is available, showing the performance of up to eight strongest LTE signals and provides an overview of all existing LTE base stations.
R&S FSH-K51 LTE TDD pilot analyzer software (×1)	Software for TDD LTE downlink over-the-air signals analysis. It provides the spectrum overview, result summary, total power, carrier frequency error, I/Q offset, cell identity, cyclic prefix, reference signal power, PSS power, SSS power, PBCH power, PCFICH power, PDSCH power, reference signal EVM, PSS EVM, SSS EVM, PBCH EVM, PCFICH EVM, PDSCH EVM.
R&S FSH-K51E LTE TDD modulation analyzer software (×1)	Software for more advanced TDD LTE downlink signal analysis and advanced carrier aggregation. Display options include the constellation diagram (graphical), measured EVM value, modulation types and LTE signal components. Measurement results of up to three carriers can be displayed simultaneously. When measuring via the air interface, an LTE-BTS scanner is available, showing the performance of up to eight strongest LTE signals and provides an overview of all existing LTE base stations.
R&S HL300.02 Spectrum analyzer antenna (×1)	Directional antenna for the R&S spectrum analyzer, supporting direction finding by orienting antenna toward maximum field strength. Its operational frequency range is 9 kHz to 7.5 GHz, in a compact size.
Dell Precision Tower 5810 data storage/processing workstation (×2)	Equipped with Intel Xeon Processor E5-1680 v3 (8C, 3.2GHz, Turbo, 20M, 140W), 32GB (4x8GB) 2133MHz DDR4 RDIMM ECC, 2.5" 256GB SATA Class 30 Solid State Drive, 1TB 3.5" Serial-ATA (7,200 RPM) Hard Drive, NVIDIA® Quadro® M2000 4GB (4 DP) (1 DP to SL-DVI adapter). The power requirement is 685W.
Rack shelf (×2)	The two rack mounts are 1U, 19 inches, to hold the two 5810 workstations in the rack.
Dell Precision Tower 3420 host workstation for USRP (×4)	Equipped with 6th Gen Intel Core i7-6700 (Quad Core 3.40GHz, 4.0Ghz Turbo, 8MB, w/ HD Graphics 530), 16GB (2x8GB) 2133MHz DDR4 Non-ECC, 1TB, 3.5" SATA (7,200 RPM) Hard Drive, HDMI, display-port, keyboard, mouse connector. Its three dimensions are 11.41, 3.64, 11.49 inches respectively. The power requirement is 180W.

to be continued on next page

Table 1 – continued from previous page

Equipment	Brief description
Dell Latitude E5570 host laptop for USRP (×5)	Equipped with Intel Core i7-6820HQ (Quad Core, 2.7GHz, 8M cache, 45W, vPro) processor, 16GB (2x8GB) 2133MHz DDR4 Memory.
Dell Latitude E7270 laptop (×1)	Equipped with Intel Core i7-6600U (Dual Core, 2.6GHz, 4M cache, 15W) processor, 16GB (2x8GB) 2133MHz DDR4 Memory.
Dell E2316H Monitors (×6)	23" display for USRP hosts.
NI X310 USRP system (×9)	High end USRPs to emulate cellular system radios. They have two wide-bandwidth RF daughterboard slots, each supporting DC to 6GHz. They have large customizable Xilinx Kintex-7 FPGA for high performance DSP (XC7K410T).
NI SBX-120 USRP daughterboard (×18)	Daughter board for X310. A full-duplex, wideband transceiver that covers a frequency band from 400 MHz to 4.4 GHz with an instantaneous bandwidth of 120 MHz. The local oscillators for the receive and transmit chains operate independently, allowing frequency-duplex operation.
NI VERT2450 antenna (×18)	Dual Band 2.4 to 2.48 GHz and 4.9 to 5.9 GHz omni-directional vertical antenna for USRP devices, at 3dBi Gain.
NI Loop back cable kit (×18)	Kit for USRP systems includes 2 SMA-M to SMA-M cables (60cm/2ft) and 2 SMA-F to SMA-M Attenuators (30dB, 50Ohm, DC-6GHz).
NI 10-Gigabit Ethernet card (×4)	Ethernet Connectivity adapter card providing high-speed network connectivity between a PC and a USRP X300/310. The kit includes a PCI-Express adapter card with two SFP+ ports, and can stream up to 200 MS/s of RX streaming bandwidth.
Netgear JGS516NA switch (×1)	1U rack-mountable automatic switch with 16 auto-sensing port. It is used to interconnect devices to spectrum analyzer, Amarisoft OTS and UE to hosts, etc.
SanDisk USB stick USB3.0 16GB (×4)	They are used to transfer data between hosts, as booting devices to re-image computers with new operating systems.
Tripp Lite B004-DP2UA2-K KVM switch (×1)	Two-port display/audio/cable/USB switch, to connect two computers to one set of shared monitor, mouse, and keyboard to save space.
R1300C Cat-6 Ethernet cables (×2)	Connecting nearby hosts to the switch or USRPs.
Mediabridge Cat-5e Ethernet cables (×1)	Connecting far-away hosts to the switch.
VELCRO 91140 Cable ties (×1)	Organizing power cables, network cables.
Kensington K64673AM lock (×4)	Lock laptops, USRPs on cart for safe keeping.
Belkin BV107200 Power strip (×6)	Provide power outlets.
400001-25 Power cord (×3)	Providing power outlet for far-away or mobile devices.
APC SMT1500RM2U UPS (×2)	Rack-mountable UPS with 1500 VA power capacity, 7.2 min battery run time (up to), 1 kW power provided at 120 V. They power the 5810s, switches and other devices in the server rack.
APC Back-UPS Pro 1500VA (×3)	Provide 1500 VA power capacity, 3 min battery run time. Mounted on carts to power USRPs in mobile test scenarios.
Server rack (×1)	24U mid-depth rack enclosure cabinet.

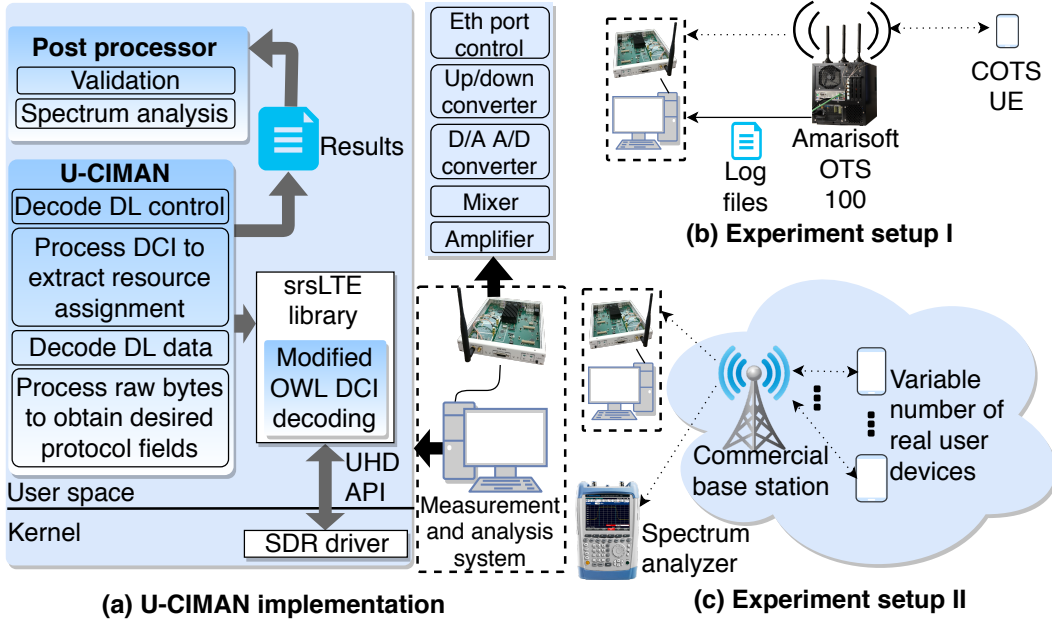


Figure 1: Systems overview

3 Prototype Description

In this project, we aim to conduct fine grained measurement and analysis of the spectrum tenancy of a commercial LTE cell. To achieve the objective, we implement the measurement tool, namely U-CIMAN, using Universal Software Defined Radio Peripheral (USRP) and a Linux host computer. Before measuring the spectrum occupancy of a commercial LTE cell, we set up two LTE cells under our control to facilitate the development of the Software Defined Radio (SDR) enabled tool and to validate its performance. The setup of the entire system is illustrated in Fig. 1. The goal is to measure the fine grained spectrum tenancy of an LTE cell. In order to achieve that, we first develop U-CIMAN with the architecture shown in Fig. 1(a), and then validate its accuracy using the setup illustrated in Fig. 1(b). Spectrum tenancy under different physical diversities are measured to further validate its performance and demonstrate its applications. As shown in Fig. 1(c), the spectrum occupancy of Commercial off-the-shelf (COTS) User equipment (UE) is measured under physical diversities of different extra noise, distance, scheduling algorithm, and user traffic. In the following paragraphs, each component and its functions will be explain.

As depicted in Fig. 1(a), U-CIMAN is implemented in the user space of a Linux host based on the Downlink Control Information (DCI) deciphering functions of [8] and the LTE library provided by [9]. The radio front is enabled by Ettus USRP X310 and the UHD library. U-CIMAN calls the srsLTE DCI decoding functions to obtain the DCI messages, then extracts the LTE resource assignment information from the DCIs. In this way, the measured spectrum tenancy is in the same time frequency granularity with LTE scheduling. The measurement results of U-CIMAN are saved as input for post processor which analyze and visualize the measurement results and is also capable to evaluate the measurement precision through comparing with actual spectrum occupancy.

To validate the measurement accuracy of U-CIMAN, we design the experiment setup as shown in Fig. 1(b). In this experiment, we use the commercial grade LTE system Amarisoft OTS100 [10] and a COTS UE. OTS100 is a full functioning LTE core network and a base station. Configuration files and operation logs of OTS100 are available to users. By enabling the physical layer system logs, all the physical layer data, including the resource assignments are recorded. We measure the spectrum occupancy of the Amarisoft cell using U-CIMAN, and then compare the measured tenancy with the ground truth, the occupancy recorded in the log files.

To further evaluate the accuracy of U-CIMAN and demonstrate its applications, we measure LTE spectrum tenancy under physical diversities. We set up eNB using the open-source LTE implementation provided

by srsLTE and a COTS UE. In every single measurement, the UE requests the eNB to stream the same video or starts a Skype conversation. The spectrum occupancy, data rate at the UE, and data rate at the eNB are measured. The physical diversities in the experiments are distance between UE and eNB, added noise, different traffic, and different scheduling algorithms. Different distances are realized by putting the two ends at different distances. Another set of USRP PC set (not shown in Fig. 1(c)) generates noise with different powers. Two types of traffic are video streaming and VoIP. Different scheduling algorithms are realized by modifying the scheduling code in srsLTE.

When measuring the spectrum occupancy of a commercial LTE cell, both spectrum analyzer and U-CIMAN are used. We first use the spectrum analyzer to measure the signals strength of nearby LTE cells, and then measures the spectrum occupancy of the cell with the best signal strength using both the analyzer and U-CIMAN.

4 Trials and Hands-On Manual

Initial trials to set up the test bed and teaching lab manuals are as follows.

4.1 Preliminary trials

As introduced earlier, the system is composed of several components and each of them requires some initial trials in their setup.

4.1.1 USRP basic setup and tests

The basic setup of USRPs includes choosing the compatible hardware, connecting the hardware, installing the USRP Hardware Driver (UHD) in the host computer, and validations of the setup. The recommended applications for various USRP hardware are outlined in [11]. Considering to support diverse research needs, we adopt the combination of X310 motherboard and SBX120 daughter boards owing to their versatility. The USRP hardware requires some assembling to piece them together, and the steps are explained in this tutorial [12]. The software tool chain installations are introduced in [13]. After the installations, the operation conditions of the hardware and software can be verified using the steps [14]. Most of the aforementioned procedures require just carefully following the steps, and problems rarely occur. However, these two points are worth special attentions.

- The **choice of UHD version and the corresponding FPGA image** in the flash on the USRP motherboard should be selected with care. This is because we may run different applications on the USRP and the applications may require certain versions of UHD which may or may not be explicitly stated.
- The **host configuration steps** by the end of the software tool chain installation tutorial [13] may not be sufficient to enable in time scheduling of USRP applications, which may cause late packets and underflow issues [15] leading to crashes. The solutions are using low latency kernel versions and configuring CPU governor and other power managements, and the step by step instructions can be found here [16].

4.1.2 Setting up an open source LTE cell

In our experiment, we need an LTE base station with controllable behavior to measure the spectrum occupancy under physical diversities, such as variation of spectrum occupancy caused by changing traffic types, noise levels, and signal strengths.

We have tried two popular open source LTE implementations, srsLTE [9] and OpenAirInterface [17], both of which include the core network, base stations and user devices. The srsLTE is chosen due to its stable operations. The key steps for installing and running srsLTE are described in [18]. We used to have a difficult time trying to connect a commercial LTE user device to the srsLTE base station. This issue was solved by switching to an older version of UHD.

4.1.3 The setup of Amarisoft cell

To validate the measurement accuracy of U-CIMAN on commercial LTE cell, a commercial grade LTE system implementation with accessible configurations and logs are desired. Amarisoft system is ideal for such test and measurement applications due to its compliance with up to date LTE protocols.

Since Amarisoft system is a commercial product, its setup is smooth with the help of its documentation. After powering on the Linux computer loaded with OTS100, the base station and Mobility Management Entity (MME) will be turned on. The corresponding configuration files reside in the directories named by network entity names such as mme or enb under root directory. The log files being written is in the tmp file in root directory, and the archived log files are in the lte folder in log folder in the var folder. The relevant configurations for the validation purposes are the level of recorded logs which should include all the physical layer details.

The user device simulator of Amarisoft is known as UE100 which is advertised to be able to simulate up to 1000 users. According to the user manual, UE100 is officially supported to be installed on a fast PC loaded with Fedora 25, and the recommended radio front includes Ettus USRP X310. Included in the package is an installation script for UE100, and it should run with smoothly if the USRP is set up correctly. To facilitate the configuration of multiple users, Amarisoft provides a utility web interface to manage the simulations of user traffic. To set up the management web interface, the main inputs are the IP addresses and the port numbers of the UE100, LTE base station and the MME. After setting up, the main trouble shooting at run time is the time advance configuration which should be 1ms smaller than the smallest time advance values seen at the base station side.

4.2 Hands-on manuals

In addition research activities, we have created following teaching lab document enabled by the equipment.

4.2.1 Amarisoft LTE basic operations

1. Login, and start the Amarisoft LTE network with the following command.
`service lte start`
2. Monitor the network components.
`screen -x lte`
3. Check the configuration files in the following locations.
`/root/enb/config/enb.cfg`
`/root/mme/config/mme.cfg`
`/root/mme/config/ims.cfg`
`/root/mbms/config/mbmsgw.cfg`
4. Configure log visualization, and open the visualization web page with Firefox, <http://<server name>/lte/>.
5. Answer the questions with screenshots of visualized logs.
 - (a) What is transmitted by eNB even if the UE does not have any application layer traffic? Your answer should contain the screenshots of relevant visualized logs, and explanations in your own words.
 - (b) What is transmitted by the UE even if the UE does not have any application layer traffic? Your answer should contain the screenshots of relevant visualized logs, and explanations in your own words.
 - (c) What are the message exchanges in the RRC layer or above when a UE powers on, gets registered to the network, and then powers off? You can either filter the log in the visualization tool, or control the log output by editing the configuration files of LTE network components. Your answer should contain the screenshots of relevant visualized logs, and explanations in your own words.

4.2.2 Amarisoft LTE traffic generation

1. iPerf install on network side. Log onto the PC running the LTE core network, and install iPerf using the command below.

```
sudo yum install iperf
```
2. iPerf install on UE side. You also need to install iPerf on the provided smart phone. iPerf is available in Google Play for Android.
3. Generate downlink data.
 - run iPerf in server mode at the UE side.

```
iperf -s -u -i 1
```
 - Run iPerf in client mode on your core network PC.

```
iperf -c <UE IP address> -u -b 150M -i 1 -t 100
```
4. Generate uplink data.
 - Run the following command on your core network PC.

```
iperf -s -u -i 1
```
 - run iPerf in client mode at the UE side.

```
iperf -c <PDN Gateway IP address> -u -b 50M -i 1 -t 100
```

5 Measurements and Publications

With the purchased equipment, we have conducted the following measurements, which result in several publications.

5.1 Measurements

In this project, we have conducted three spectrum tenancy measurements and they are introduced in the corresponding subsections below.

5.1.1 Measurements conducted using spectrum analyzer

The Rohde & Schwarz FSH8.08 spectrum analyzer is equipped with the HL300 antenna, and the necessary software for LTE signal processing as shown in Table 1. As a result, the spectrum analyzer is capable of synchronizing with the LTE base station and measure the power level of each LTE resource block. Though the claimed the measurement interval can be as small as 1ms, but there are at most five to six records per minute. Compared with U-CIMAN, the spectrum analyzer has larger measurement time granularity and the measurement results do not reveal occupancy status directly since the measurement results are power readings.

5.1.2 U-CIMAN measurements for a commercial cell

Spectrum tenancy measurements of a commercial LTE cell is conducted using U-CIMAN. We measure the spectrum tenancy of a nearby LTE cell for 24 hours and the time frequency granularities are the same with LTE scheduling. Various metrics are analyzed and visualized. Tenancy metrics show intuitive trends. For example, the trend of downlink RB occupancy in Fig. 2 roughly follows the fluctuation of human activities, showing three stable periods and three transition periods in between. However, the on time of downlink RBs in Fig. 3 do not show the same trend.

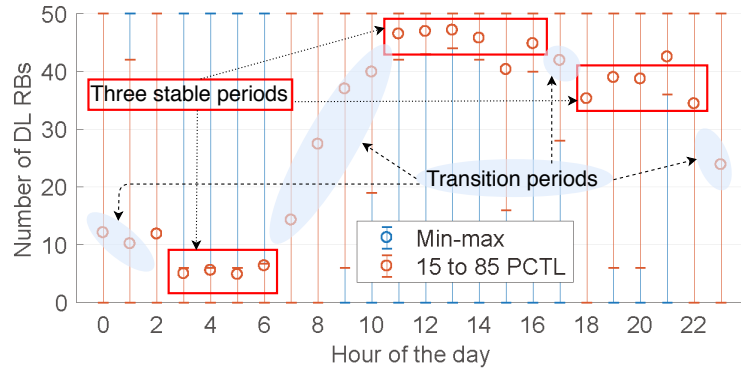


Figure 2: Statistics of per hour total occurrence of TTI with different number of DL RB

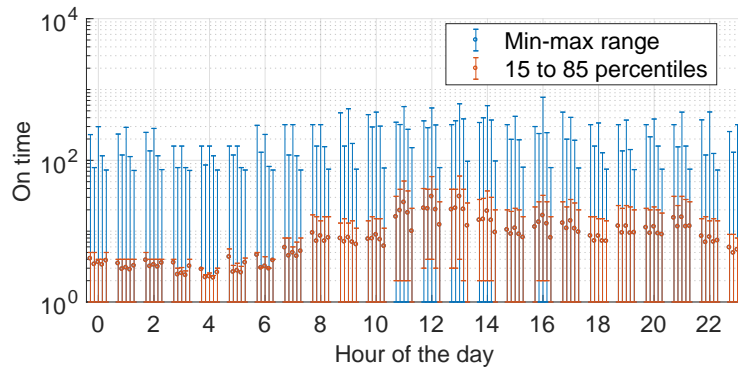


Figure 3: 24-hour on time statistics of 5 DL RBs

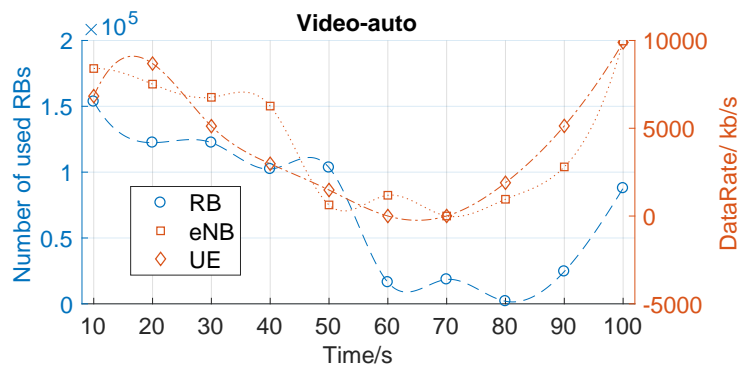


Figure 4: Spectrum occupancy and data rate of video transmission using default MCS algorithm

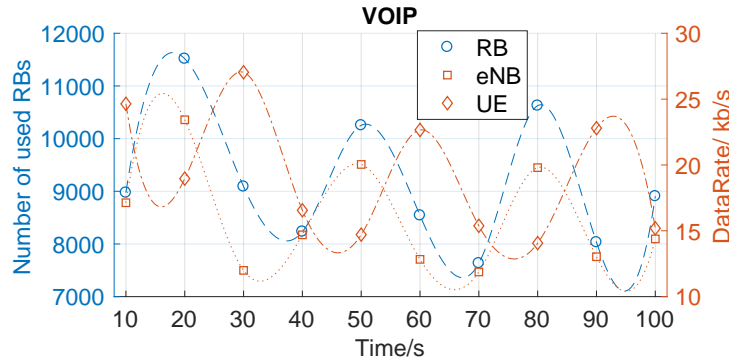


Figure 5: Spectrum occupancy and data rate of VoIP traffic

5.1.3 Physical diversity measurements

The measurement results of spectrum occupancy and data rate under the four diversities are obtained using U-CIMAN and Wireshark. The measurement results for different traffic types are presented as an example. The spectrum occupancy of two types of traffic, video streaming and Voice over IP (VoIP) are measured. Fig. 4 and 5 show the measurement results for video streaming and VoIP respectively. The horizontal axis is time in seconds. The blue vertical axis is the number of occupied LTE RBs, and the orange vertical axis is the data rate. Comparing the two figures, we find that the spectrum usage of video streaming changes more drastically than that of VoIP traffic as time proceeds. The RB usage of VoIP have sinusoid shape line fluctuating between 12000 and 7000, while video streaming sometimes occupies as many as 15000 RBs, and as few as 2000 RBs at some other times. The data rate of video streaming is around 200 times that of VoIP, but the number of occupied RBs of video streaming is only about 10 times that of VoIP. Thus, the traffic types affect the efficiency of the spectrum assignment.

5.2 Publications

- R. Zou and W. Wang, ‘Downlink decoding based accurate measurement of lte spectrum tenancy,’ *IEEE Transactions on Mobile Computing*, 2021, [19].
- R. Zou, W. Wang, and H. Dai, ‘Temporal and spectral analysis of spectrum hole distributions in an LTE cell,’ in *2021 IEEE Global Communications Conference: Cognitive Radio and AI-Enabled Network Symposium (Globecom2021 CRAEN), Madrid, Spain, 2021*, [20]
- R. Zou and W. Wang, ‘U-CIMAN: Uncover spectrum and user information in lte mobile access networks,’ in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*. IEEE, 2020, pp. 1459–1468, [21]
- R. Zou and W. Wang, ‘Change detection based segmentation and modeling of lte spectrum tenancy’ in *2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2019, pp. 1–6, [22].

References

- [1] A. N. Mody and G. Chouinard, “IEEE 802.22 Overview and Core Technologies,” <http://www.ieee802.org/22/Technology/22-10-0073-03-0000-802-22-overview-and-core-technologies.pdf>, accessed: 2015-09-13.
- [2] Supermicro, “SuperServer 5038MR-H8TRF,” <http://www.supermicro.com/products/system/3U/5038/SYS-5038MR-H8TRF.cfm>, accessed: 2015-09-23.
- [3] E. Research, “USRP X300,” <http://www.ettus.com/product/details/X300-KIT>, accessed: 2015-09-23.

- [4] Amarisoft, “Amari LTE 100 / Amari OTS 100 Software 4G network on PC,” <http://amarisoft.com/?p=amarilte>, accessed: 2015-09-23.
- [5] —, “Amari UE 100 Software 4G UE Simulator on PC,” <http://amarisoft.com/?p=amarilte2>, accessed: 2015-09-23.
- [6] Amazon, “Samsung Galaxy S6 G920I Factory Unlocked Cellphone, 32GB, Platinum Gold,” http://www.amazon.com/Samsung-Galaxy-S6-G920I-Unlocked/dp/B00VIVU2N0/ref=sr_1_1?ie=UTF8&qid=1442438509&sr=8-1&keywords=galaxy+s6+factory+unlocked, accessed: 2015-09-23.
- [7] G. Store, “Nexus 9 - 16 GB or 32 GB. Wi-Fi or LTE. Indigo Black, Lunar White, or Sand,” https://store.google.com/product/nexus_9?utm_source=google-com-nexus&utm_medium=index&utm_campaign=nexus-9, accessed: 2015-09-23.
- [8] N. Bui and J. Widmer, “OWL: a Reliable Online Watcher for LTE Control Channel Measurements,” in *ACM All Things Cellular (MobiCom Workshop)*, Nov. 2016.
- [9] I. Gomez-Miguel, A. Garcia-Saavedra, P. D. Sutton, P. Serrano, C. Cano, and D. J. Leith, “srslte: an open-source platform for lte evolution and experimentation,” in *Proceedings of the Tenth ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation, and Characterization*. ACM, 2016, pp. 25–32.
- [10] Amarisoft, “Amarisoft ots 100,” December 2017. [Online]. Available: <https://www.amarisoft.com/2016/12/28/amarisoft-presents-amari-ots-100/>
- [11] Ettus, “Selecting an usrp device.” [Online]. Available: https://kb.ettus.com/Selecting_an_USRP_Device
- [12] —, “Usrp x series quick start.” [Online]. Available: [https://kb.ettus.com/USRP_X_Series_Quick_Start_\(Daughterboard_Installation\)](https://kb.ettus.com/USRP_X_Series_Quick_Start_(Daughterboard_Installation))
- [13] —, “Building and installing the usrp open-source toolchain.” [Online]. Available: [https://kb.ettus.com/Building_and_Installing_the_USRP_Open-Source_Toolchain_\(UHD_and_GNU_Radio\)_on_Linux](https://kb.ettus.com/Building_and_Installing_the_USRP_Open-Source_Toolchain_(UHD_and_GNU_Radio)_on_Linux)
- [14] —, “Verifying the operation of the usrp using uhd and gnu radio.” [Online]. Available: https://kb.ettus.com/Verifying_the_Operation_of_the_USRP_Using_UHD_and_GNU_Radio
- [15] —, “usrp x3x0 config.” [Online]. Available: https://files.ettus.com/manual/page_usrp_x3x0_config.html
- [16] OpenAirInterface, “Openair kernel main setup.” [Online]. Available: <https://gitlab.eurecom.fr/oai/openairinterface5g/wikis/OpenAirKernelMainSetup>
- [17] N. Nikaein, M. K. Marina, S. Manickam, A. Dawson, R. Knopp, and C. Bonnet, “Openairinterface: A flexible platform for 5g research,” *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 5, pp. 33–38, 2014.
- [18] softwareradiosystems, “srslte.” [Online]. Available: <https://github.com/srsLTE/srsLTE>
- [19] R. Zou and W. Wang, “Downlink decoding based accurate measurement of lte spectrum tenancy,” *IEEE Transactions on Mobile Computing*, 2021.
- [20] R. Zou, W. Wang, and H. Dai, “Temporal and spectral analysis of spectrum hole distributions in an lte cell,” in *2021 IEEE Global Communications Conference: Cognitive Radio and AI-Enabled Network Symposium (Globecom2021 CRAEN)*, Madrid, Spain, 2021.
- [21] R. Zou and W. Wang, “U-ciman: Uncover spectrum and user information in lte mobile access networks,” in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*. IEEE, 2020, pp. 1459–1468.
- [22] —, “Change detection based segmentation and modeling of lte spectrum tenancy,” in *2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2019, pp. 1–6.