

REPORT DOCUMENTATION PAGE			Form Approved OMB NO. 0704-0188		
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) 07-12-2016		2. REPORT TYPE Final Report		3. DATES COVERED (From - To) 11-Aug-2014 - 10-Aug-2016	
4. TITLE AND SUBTITLE Final Report: LTE-Enhanced Cognitive Radio Testbed			5a. CONTRACT NUMBER W911NF-14-1-0553		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER 611103		
6. AUTHORS Vuk Marojevic, Deven Chheda, Raghunandan Rao, Randall Nealy, Carl Dietrich, Jeffrey H. Reed, and Jerry Park			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAMES AND ADDRESSES Virginia Polytechnic Institute & State Univ North End Center, Suite 4200 300 Turner Street, NW Blacksburg, VA 24061 -0001			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) 65230-NS-RIP.6		
12. DISTRIBUTION AVAILABILITY STATEMENT Approved for Public Release; Distribution 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 Testbeds play a major role in developing and testing new wireless communications technologies and systems. Wireless@Virginia Tech has built a COgnitive Radio NETwork (CORNET), which consists of a 48-node indoor testbed, a 15-node outdoor testbed (O-CORNET) and a LTE testbed (LTE-CORNET). This document provides a system overview of the LTE-CORNET, its components, features, access and configuration mechanisms. LTE-CORNET is a standalone testbed that can be remotely accessed by registered users. Exclusive access to the entire testbed to an individual or group will be provided during the reservation period.					
15. SUBJECT TERMS System Performance Report, Amarisoft, CMW500, CORNET, GNU Radio, LTE, RFNEST, SDR, srsLTE, USRP					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT UU	b. ABSTRACT UU	c. THIS PAGE UU			Jung-Min Park
					19b. TELEPHONE NUMBER 540-231-8392

Report Title

Final Report: LTE-Enhanced Cognitive Radio Testbed

ABSTRACT

Testbeds play a major role in developing and testing new wireless communications technologies and systems. Wireless@Virginia Tech has built a Cognitive Radio NETwork (CORNET), which consists of a 48-node indoor testbed, a 15-node outdoor testbed (O-CORNET) and a LTE testbed (LTE-CORNET). This document provides a system overview of the LTE-CORNET, its components, features, access and configuration mechanisms. LTE-CORNET is a standalone testbed that can be remotely accessed by registered users. Exclusive access to the entire testbed to an individual or group will be provided during the reservation period.

The testbed's main components are several LTE base stations (eNodeBs) with their evolved packet cores (EPCs), two channel modes, and several LTE user equipment (UEs). One eNodeBs is the CWM500, Rohde & Schwarz's eNodeB emulator and UE tester. Three commercial software-defined LTE systems, Amarisoft's LTE100, are installed on two PCs and one mobile workstation. The open-source LTE library srsLTE is available on a third PC. A fourth PC can be used to implement interference waveforms, among others. The RF signals can access the wireless channel through 7 antenna ports. Five 5 fixed antennas are deployed in the ceiling of Wireless@VT's RF laboratory. Alternatively, the signals can be routed through a configurable channel emulator, RFnest's 8-port analog system A208, for non-radiating experiments in a controlled RF environment. Several UEs of different categories and types are available, including Cat. 4, 5 and 6 devices in the form of USB dongles, access points or smartphones. A shielded box can be used for over-the-air experiments. An FCC experimental license for several bands is available through O-CORNET.

Note that the testbed described in this report has been revised and merged into a larger testbed with a parallel DURIP award (Army Research Office DURIP Award Number W911NF-14-1-0554). The final report for W911NF-14-1-0554 describes the current state of the merged testbeds.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received

Paper

TOTAL:

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received

Paper

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations	
Vuk Marojevic, "Virginia Tech's Cognitive Radio Network (CORNET) Testbeds", White Paper and Presentations, Large-scale Networking Platforms "Communities of Practice" Workshop, Arlington, VA, Oct. 24-25, 2016, http://www.winlab.rutgers.edu/events/tbcopws/WP.html	
Number of Presentations:	1.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

<u>Received</u>	<u>Paper</u>
12/05/2016	2.00 M. Labib, V. Marojevic, J. Reed, A. Zaghloul. How to enhance the immunity of LTE systems against RF spoofing, 2016 International Conference on Computing, Networking and Communications (ICNC). 15-FEB-16, Kauai, HI, USA. : ,
12/05/2016	3.00 M. Labib, V. Marojevic, J. Reed. Analyzing and enhancing the resilience of LTE/LTE-A systems to RF spoofing, 2015 IEEE Conference on Standards for Communications and Networking (CSCN). 28-OCT-15, Tokyo, Japan. : ,
TOTAL:	2

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

<u>Received</u>	<u>Paper</u>
TOTAL:	

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts	
<u>Received</u>	<u>Paper</u>
TOTAL:	
Number of Manuscripts:	

Books	
<u>Received</u>	<u>Book</u>
TOTAL:	
<u>Received</u>	<u>Book Chapter</u>
TOTAL:	

Patents Submitted	
Patents Awarded	
Awards	

Graduate Students

<u>NAME</u>	<u>PERCENT SUPPORTED</u>	Discipline
Raghunandan M. Rao	0.00	
Jabar Kakar	0.00	
Deven Chheda	0.00	
Pradeep Reddy Vaka	0.00	
Sudeep Bhattarai	0.00	
Siddhartha Kundalkar	0.00	
Mina Labib	0.00	
Durga Laxmi Narayana Swamy Int	0.00	
Sai Nisanth Bodepudi	0.00	
Kevin Ryland	0.00	
Robert Kleine	0.00	
FTE Equivalent:	0.00	
Total Number:	11	

Names of Post Doctorates

<u>NAME</u>	<u>PERCENT SUPPORTED</u>
FTE Equivalent:	
Total Number:	

Names of Faculty Supported

<u>NAME</u>	<u>PERCENT SUPPORTED</u>	National Academy Member
Vuk Marojevic	0.00	
Jeffrey H. Reed	0.00	
Jerry Park	0.00	
Carl B. Dietrich	0.00	
FTE Equivalent:	0.00	
Total Number:	4	

Names of Under Graduate students supported

<u>NAME</u>	<u>PERCENT SUPPORTED</u>
FTE Equivalent:	
Total Number:	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:..... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):..... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields: 0.00

Names of Personnel receiving masters degrees

NAME

Deven Chheda (MEng)

Raghunandan M. Rao

Jaber Kakar

Siddhartha Kundalkar (MEng)

Total Number:

4

Names of personnel receiving PHDs

NAME

Total Number:

Names of other research staff

NAME

PERCENT SUPPORTED

Randall Nealy

0.41

Gregg Kelly

0.10

FTE Equivalent:

0.51

Total Number:

2

Sub Contractors (DD882)

Inventions (DD882)

5 Methods to protect the LTE control channel spoofing

Patent Filed in US? (5d-1) N

Patent Filed in Foreign Countries? (5d-2) N

Was the assignment forwarded to the contracting officer? (5e) N

Foreign Countries of application (5g-2):

5a: Jeffrey H. Reed

5f-1a: Virginia Tech

5f-c: 1145 Perry Street, Durham Hall (0350)

Blacksburg VA 24061

5a: Mina Labib

5f-1a: Virginia Tech

5f-c: 1145 Perry Street, Durham Hall (0350)

Blacksburg VA 24061

5a: Vuk Marojevic

5f-1a: Virginia Tech

5f-c: 1145 Perry Street, Durham Hall (0350)

Blacksburg VA 24061

Scientific Progress

This is an infrastructure grant and the statement of work consisted of building the testbed. The testbed and the enabled research and education is described in the project report.

Technology Transfer

LTE-Enhanced Cognitive Radio Network Testbed (LTE-CORNET)

System Overview and Performance Report

Vuk Marojevic, Deven Chheda, Raghunandan Rao, Randall Nealy, Carl Dietrich, Jeffrey H. Reed, and
Jerry Park

Document Control and Data Sheet

Document No.	1
Document Title	LTE-CORNET: System Overview and Performance Report
Date	November 2016
Type of document	Technical
No. of pages	53
Authors	Vuk Marojevic, Deven Chheda, Raghunandan Rao, Randall Nealy, Carl Dietrich, Jeffrey H. Reed, and Jerry Park
Abstract	This document presents an overview of the LTE-CORNET system and its components. The hardware and software aspects are described first, followed by networking and user access management.
Keywords	Amarisoft, CMW500, CORNET, GNU Radio, LTE, RFNEST, srsLTE, USRP.
Project	LTE-CORNET
Project Award	Army Research Office DURIP grant W911NF-14-1-0553

Executive Summary

Testbeds play a major role in developing and testing new wireless communications technologies and systems. Wireless@Virginia Tech has built a COgnitive Radio NETwork (CORNET), which consists of a 48-node indoor testbed, a 15-node outdoor testbed (O-CORNET) and a LTE testbed (LTE-CORNET). This document provides a system overview of the LTE-CORNET, its components, features, access and configuration mechanisms. LTE-CORNET is a standalone testbed that can be remotely accessed by registered users. Exclusive access to the entire testbed to an individual or group will be provided during the reservation period.

The testbed's main components are several LTE base stations (eNodeBs) with their evolved packet cores (EPCs), two channel modes, and several LTE user equipment (UEs). One eNodeBs is the CWM500, Rohde & Schwarz's eNodeB emulator and UE tester. Three commercial software-defined LTE systems, Amarisoft's LTE100, are installed on two PCs and one mobile workstation. The open-source LTE library srsLTE is available on a third PC. A fourth PC can be used to implement interference waveforms, among others. The RF signals can access the wireless channel through 7 antenna ports. Five 5 fixed antennas are deployed in the ceiling of Wireless@VT's RF laboratory. Alternatively, the signals can be routed through a configurable channel emulator, RFnest's 8-port analog system A208, for non-radiating experiments in a controlled RF environment. Several UEs of different categories and types are available, including Cat. 4, 5 and 6 devices in the form of USB dongles, access points or smartphones. A shielded box can be used for over-the-air experiments. An FCC experimental license for several bands is available through O-CORNET.

Note that the testbed described in this report has been revised and merged into a larger testbed with a parallel DURIP award (Army Research Office DURIP Award Number W911NF-14-1-0554). The final report for W911NF-14-1-0554 describes the current state of the merged testbeds.

Table of Contents

Abbreviations	5
List of Figures	6
List of Tables	8
1 System Overview	9
2 Hardware	11
2.1 CMW500	11
2.2 Computing Nodes	11
2.3 Software Radio Peripherals	13
2.4 RF Processing	13
2.5 Channel Emulator	14
2.6 RF Filters	15
2.7 Antenna system	16
2.8 User Equipment	16
2.9 Reference Oscillators and Clock Sources	17
2.10 RF Switch	17
3 Software	19
3.1 Operating System and Support Software	20

3.2	Wireless Communications Software	20
4	Networking and User Access	21
5	User Manual	23
5.1	User Registration and General Usage Instructions	23
5.2	Access the Testbed	23
5.3	Configure the Testbed	29
6	System Administration	37
7	Testbed Use in Research and Education	38
7.1	Education	38
7.2	Research	39
8	Conclusions and Lessons Learned	41
	References	43
 <u>Appendices</u>		
A	FCC Experimental License Application Process	44
B	FCC Emissions Table	48
C	Equipment List	50
D	Publications	53

Abbreviations

CEC	Channel Emulator Controller
COMWITS	Cognitive Medical Wireless Testbed System
CORNET	Cognitive Radio Network
CP	Cyclic Prefix
CQI	Channel Quality Indicator
DL	Downlink
FDD	Frequency Division Duplex
GRC	GNU Radio Companion
LTE	Long Term Evolution
MCS	Modulation and Coding Scheme
MIMO	Multiple-Input Multiple-Output
O-CORNET	Outdoor CORNET
OTS	Off-the-Shelf
PDSCH	Physical Downlink Shared Channel
PUSCH	Physical Uplink Shared Channel
PRB	Physical Resource Block
QAM	Quadrature Amplitude Modulation
QoS	Quality-of-Service
QPSK	Quadrature Phase Shift Keying
RB	Resource Block
RE	Resource Element
Rfnet	Radio Frequency Network channel Emulation Simulation Tool
RI	Rank Indication
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
SDR	Software-Defined Radio
SISO	Single Input Single Output
TBS	Transport Block Size
TDD	Time Division Duplex
TTI	Transmission Time Interval
UDP	User Datagram Protocol
UE	User Equipment
UHD	USRP Hardware Driver
UL	Uplink
USRP	Universal Software Radio Peripheral

List of Figures

Figure 1. LTE-CORNET: Photo (a) and identification of components (b).

Figure 2. RF diagrams: Functional diagram using RFnest (a) and functional diagram using antennas (b).

Figure 3. Outline of Wireless@Virginia Tech's RF laboratory indicating the antenna locations.

Figure 4. Photo of the Rohde & Schwarz CMW500.

Figure 5. Mobile node with B210 USRP.

Figure 6. RFnest hardware showing the 8 RF ports and Ethernet interface.

Figure 7. Omni-directional, ceiling mounted antenna [3].

Figure 8. UEs.

Figure 9. Internal network layout.

Figure 10: Sample SSH (putty) login screen and command prompt.

Figure 11: Sample command screen showing port number displayed after running `$ x11vnc`.

Figure 12: Sample TightVNC Viewer screen.

Figure 13: Ensuring OpenVPN software has Administrator privileges.

Figure 14: Connecting using OpenVPN.

Figure 15: Launching PuTTY.

Figure 16: Launching the remote desktop server.

Figure 17: Launching TightVNC Viewer.

Figure 18: Launching Remmina Client to connect to CMW500.

Figure 19: The CMW500 interface.

Figure 20: Launching CEC using the terminal.

Figure 21: Launching RFview script using the terminal.

Figure 22: RFview GUI showing a loaded scenario.

Figure 23: Initializing the RFnest hardware using RFview GUI.

Figure 24: Confirmation message displayed after successful initialization of the RFnest hardware.

Figure 25: Performing a reset on the CMW500 prior to an experiment.

Figure 26: Turning the Signal Generator ON/OFF using the CMW500 interface.

Figure 27: Configuring the Rogers UE.

Figure 28: Constellation diagram of the four 16-QAM data streams of the FMT-FBMC waveform.

Figure 29: Snapshot showing the stages of forced handover with the forced handover feature of LTE100.

Figure 30: Experiment setup for the LTE vulnerability analyses of [15] [16] [23].

List of Tables

Table 1. Computer Specifications.

Table 2. USRP specifications.

Table 3. RFnest specifications.

Table 4. Filter bank assignments.

Table 5. Electrical parameters of the antenna [3].

Table 6. UE specifications.

Table 7. RF switch settings.

Table 8. Software installed on processing nodes.

Table 9. LTE-CORNET networking specifications.

1. System Overview

The core of the LTE-CORNET testbed is located in 475 Durham Hall (server room). Figure 1a shows a photo. The testbed is remotely accessible through the Internet (Section 4).

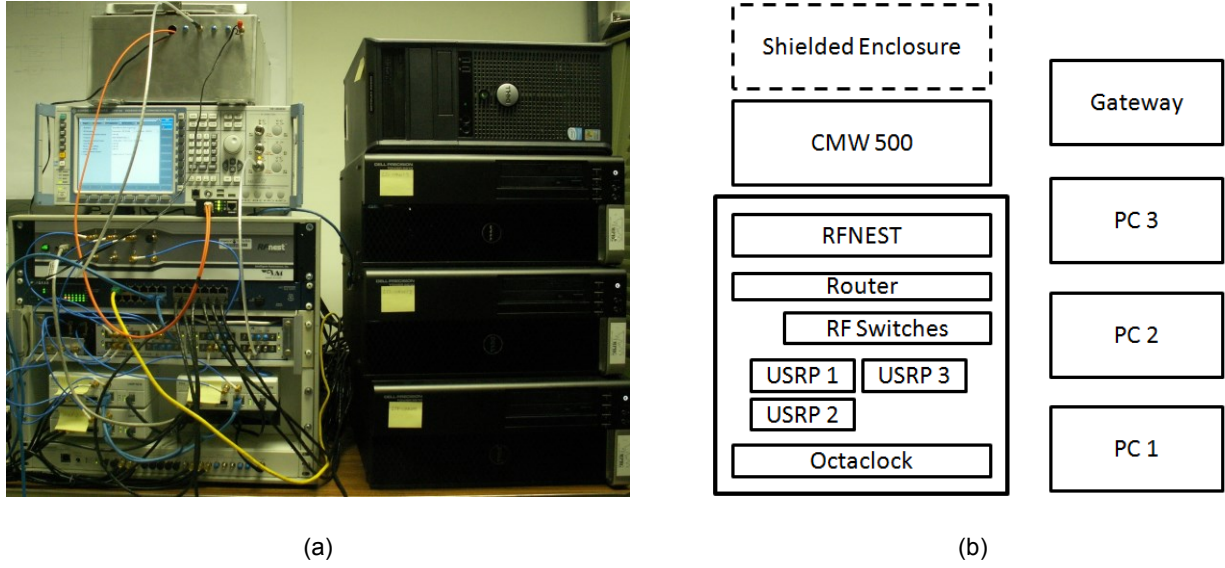


Figure 1. LTE-CORNET: Photo (a) and identification of components (b).

Figure 2 shows two configurations of the testbed, the cabled mode using the channel emulator (Fig. 2a) and over-the-air mode through antennas (Fig. 2a).

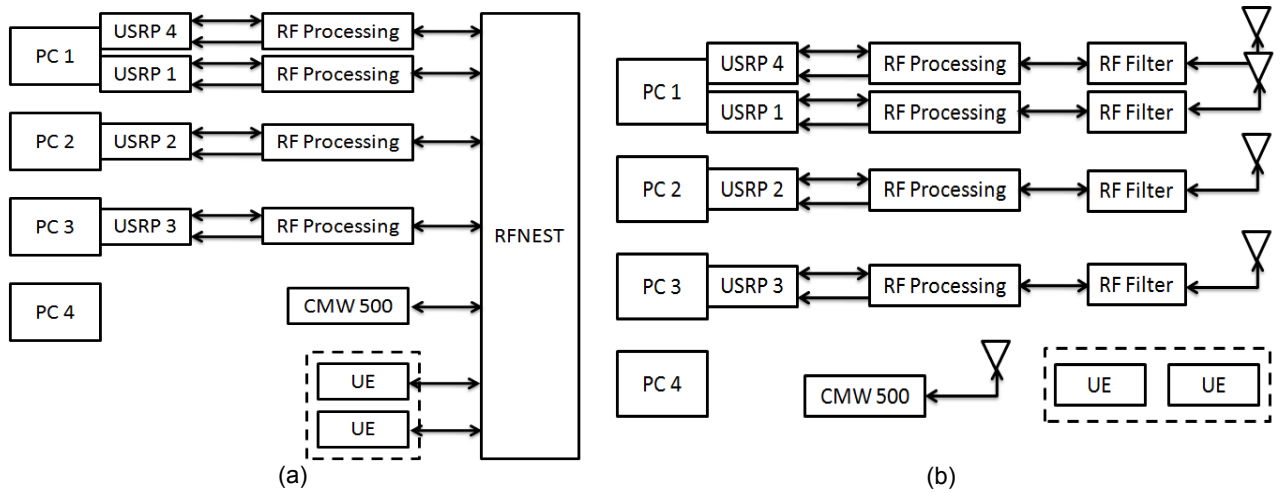


Figure 2. RF diagrams: Functional diagram using RFnest (a) and functional diagram using antennas (b).

The RF processing in Fig. 2 includes couplers and attenuators described in Section 2.4. The RF filters, which are described in Section 2.6, are separate blocks and are used in over-the-air mode to remove the

harmonics not filtered by the USRPs. Not shown is the RF switch which allows switching between the emulated channel and radiated modes. Section 2.11 provides more details.

Five fixed antennas are placed in the ceiling of the RF lab, 471 Durham Hall (Fig. 3). Section 2.7 describes the antenna system. An additional two RF cables are available for connecting user-provided equipment to the testbed. All 7 cables are connected to the testbed through the conduit in the wall.

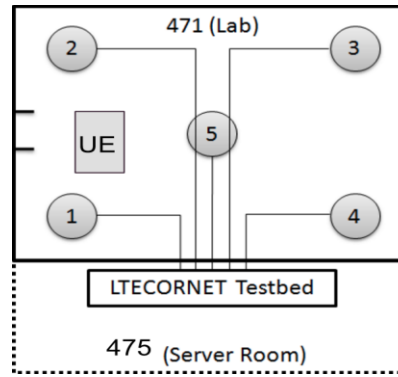


Figure 3. Outline of Wireless@Virginia Tech’s RF laboratory indicating the antenna locations.

Salient Features

LTE-CORNET is a unique facility for LTE research and education. It combines a modular set of hardware and software components to offer

- Remote access to a controlled experimental environment,
- Reproducible experimentation capability,
- Rapid setup of multiple emulated LTE cells (3GPP compliant, Releases 8-12), up to 5 simultaneously
- Real user equipment (UEs),
- Access to commercial and free open-source code,
- Over-the-air or nonradiating experiments,
- Flexibly configurable and easily upgradeable

System Components

The system consists of several hardware and software components that are integrated in the LTE-CORNET testbed, as described in the following sections. The list of purchased system components is provided in Appendix C. Note that the testbed described in this report has been revised and merged into a larger testbed with a parallel DURIP award, Army Research Office DURIP Award Number W911NF-14-1-0554. The final report for “Cognitive Medical Wireless Testbed System (COMWITS)” (W911NF-14-1-0554) describes the current state of the merged LTE-CORNET/COMWITS testbed.

2. Hardware

2.1 CMW500

The CMW500 from Rohde & Schwarz is a wideband communication tester. Figure 5 shows a photo of the front panel. LTE-CORNET's CMW500 is currently equipped with FD-LTE and TD-LTE firmware compliant with 3GPP Release 8. It allows monitoring LTE performance parameter, such as Throughput, block error rate (BLER), channel quality indicator (CQI), in real-time. Data logging is available for offline analysis. The CMW500 can also serve as a spectrum analyzer. Its main screen can be exported and all knobs and features remotely controlled or accessed.



Figure 4. Photo of the Rohde & Schwarz CMW500.

Future upgrades with additional functionality or to newer 3GPP Releases is possible, but may require shipment to factory. The available features are summarized in Appendix C.

2.2 Computing Nodes

Five PCs provide the software processing capabilities of the testbed (Table 1). PCs 1-4 share a monitor that can be accessed locally through a KVM switch for system administration. The mobile workstation is not integrated in the fixed testbed infrastructure. It can be connected to this infrastructure or used individually. Another PC serves as the gateway allowing remote access and is described in the networking section, Section 4.

Table 1a. Computer Specifications.

	PC 1-3	PC 4¹	Rackmount Workstation
Model	Dell Precision Tower 5810 Workstation	Dell Optiplex 9010	Dell Precision R7910
Architecture	64 bit	64 bit	64 bit
CPU	Intel Xeon Processor E5-1650 v3 (6C, 3.5 GHz, Turbo, HT, 15M, 140W)	Intel Core i7-3770 (3.4 GHz Quad Core, 77W)	Dual Intel Xeon E5-2695 v4 (18C, 2.1GHz, 3.3GHz Turbo, 2400MHz, 45MB, 120W)
RAM	32GB (4 x 8 GB) 2133 MHz DDR4 RDIMM ECC	16GB (4x4GB) 1600MHz DDR3 DIMM	128GB (8x16GB) 2400MHz DDR4 RDIMM ECC
Hard drive	256 GB SATA SSD 1 TB 7200RPM SATA HDD	500GB SATA 7200RPM HDD	512GB Dell 4*Drive PCIe x16 M.2 SSD + 2.5" 512GB SATA Class 20 SSD
Video Card	NVIDIA Quadro NVS 310 512 MB (2 DP)	Intel IvyBridge Desktop	Dual AMD FirePro™ W5100 4GB (4 DP) (4 DP to SL-DVI adapters)
Ports	2 Gigabit Ethernet 1+3 USB3 ports	2 Gigabit Ethernet 2+2 USB3 ports	Quad Port Network Daughter Card (2x10GbE, 2x1Gbit) Intel X540

¹ Available from another project**Table 1b.** Computer Specifications.

	Mobile Workstation 1	Mobile Workstations 7-8	Intel NUC-i5	Intel NUC-i7 (2)
Name	LTE-DURIP	comwits1-Precision-7510		
Model	Dell Precision M4800 Workstation	Precision-7510	NUC5i5RYH	NUC6i7KYK
Architecture	64 bit	64 bit	64 bit	64 bit
CPU	Intel i7-4910MQ (Quad core, 2.9GHz)	i7-6920HQ	Intel i5-5250U	Intel i7-6770HQ
RAM	16GB (4x4GB) 1600MHz DDR3	32 GB	8 GB	32 GB
Hard drive	256GB 6.0 Gbps SATA SSD	250 GB	Samsung 850 Evo 250 GB M.2 SSD	Samsung 950 Pro 256 GB M.2 SSD
Video Card	Gallium 0.4 on AMD Cape Verde	Nvidia Quadro M2200/PCIe/SSE2	Intel HD Graphics 6000	Intel Iris Pro
Ports	1 Gigabit Ethernet 2+2 USB3 ports	1 Gigabit Ethernet 2+2 USB3	1 Gigabit Ethernet 4 USB3	1 Gigabit Ethernet 3 USB3

2.3 Software Radio Peripherals

We use 3 N210s and 2 B210 Universal Software Radio Peripherals (USRP)s from NI/Ettus Research (Table 2). USRPs 1-4 are integrated in the fixed testbed located in 475 Durham Hall. USRP 5 is the mobile node's USRP.

Table 2. USRP specifications.

	USRP 1-3	USRP 4-5	USRP 6-13¹
Model	N210	B210	B210
Interface	1000BaseT	USB3	USB3
IP address	192.168.10.1	-	-
UHD Version	3.5.4 and above	3.7.0 and above	3.7.0 and above
Daughterboards	SBX (400-4400 MHz)	Integrated (100 MHz - 6 GHz)	Integrated (100 MHz - 6 GHz)
Bandwidth	40 MHz	60 MHz	60 MHz
RF chains	1 TX/RX + 1 RX	2 TX/RX + 2 RX	2 TX/RX + 2 RX
MIMO	No	2x2	2x2

¹ Shared with COMWITS, Army Research Office DURIP Award Number W911NF-14-1-0554

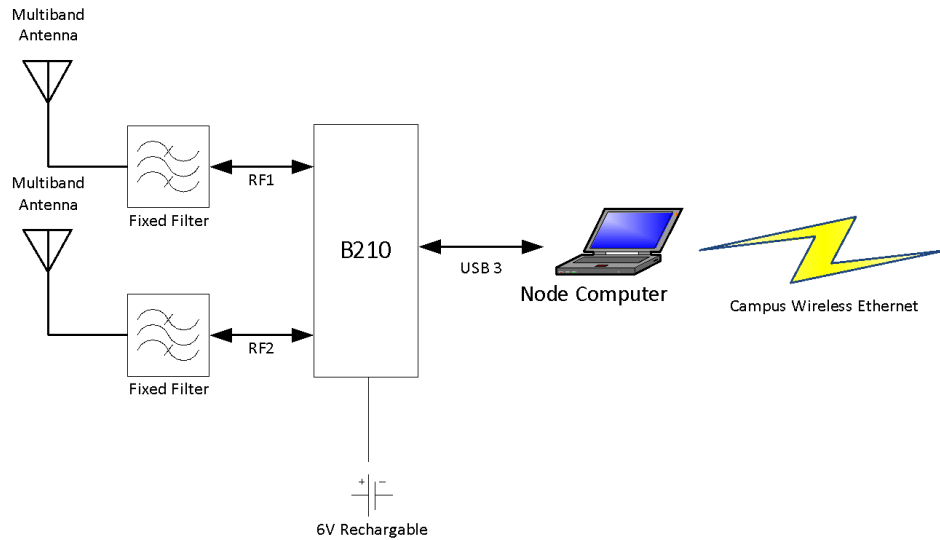


Figure 5. Mobile node with B210 USRP.

2.4 RF Processing

Each USRP N210 (USRP 1-3) has an RF processing block attached which consists of RF attenuators and combiners which allow both USRP ports to be utilized. The combiner takes the form of a wideband 10 dB directional coupler. The coupler through connection attaches to the USRP RX port. The coupled arm is

connected to the USRP TX/RX port. This configuration provides 10 dB of attenuation to the transmitted signal while allowing for reception with no additional attenuation. An additional 10 dB attenuator is provided at the RFnest port to reduce the transmitted signal a total of 10 dB. Since the USRP N210 with SBX daughterboard can source 100 mW, the total attenuation of 20 dB provides approximately 0 dBm maximum signal to the RFnest port. The directional couplers are Mini-Circuits labs model ZHDC-10-63-S+ which have a specified frequency range of 50-6000 MHz.

A conventional 3 dB hybrid combiner is used to connect the TX/RX and RX ports of USRP 4. B219 USRPs can be directly connected to any computer via USB, as illustrated in Fig. 5.

2.5 Channel Emulator

Our testbed includes a channel emulator called RFnest (Radio Frequency Network channel Emulation Simulation Tool) from Intelligent Automation, Inc. Figure 6 shows a photo. The channel emulator allows wireless nodes to experience realistic channel effects, and supports the integration of real radio nodes and virtual or simulator radio nodes. It comprises of four major components:

- **RFnest hardware:** The hardware carries out the digitization of the incoming RF signals, applies selected channel effects, generates RF signals digitally, and converts the resulting signals back to analog signals for all the connected radios in real-time. The model currently in use is the A208, and it allows up to 8 simultaneous RF connections, with support for up to 96 connections when cascaded with other RFnest hardware. The hardware communicates with other system components over the Ethernet interface.
- **RFview GUI:** It provides the user-interface for the system and allows for scenario modelling, analysis, and the recording and replay of scenarios. The GUI provides time-synchronized, geospatial graph-based displays of the scenario state, and the outcome of the scenario. Version 2.11 of the software is currently in use.
- **Channel Emulation Controller (CEC):** The CEC co-ordinates with the RFview and carries out initialization and updation of properties as the scenario changes over time.
- **Channel models:** The system supports the following built-in channel models: free space model, Hata model (suburban, urban, rural), Hata PCS (suburban, urban), log distance model, and flat fading model. The present system does not support modelling of individual multipath delays and Doppler spread in the channel.



Figure 6. RFnest hardware showing the 8 RF ports and Ethernet interface.

Table 3. RFnest specifications.

Parameter	Specification
No. of ports	8
RF configuration	SISO, SIMO, MISO, MIMO, MESH
Frequency bands	0 - 1 GHz, 1.2-1.9 GHz, 1.8-2.8 GHz , 2.7 - 3 GHz, 3.4 - 4 GHz, 3.4 - 4 GHz
Dynamic Range	37 dB (1 dB resolution)
Input Power	<1 dBm
RF Output Level	-30 dB to -67 dB
RF Output Accuracy	2 dB
Maximum propagation delay	2 seconds
Doppler Shift	Up To 2 kHz

2.6 RF Filters

Our testbed provides support for over-the-air transmission as well as through RF cables. RF filter banks are connected between the RF switch and the antennas located in the RF Lab for use when the over-the-air mode is selected by the RF switch.

Since the USRP RF components (daughterboards) only includes a single fixed filter (cutoff at the highest specified daughterboard frequency of 4.4 GHz), it is evident that additional filtering must be provided in order to suppress transmitted harmonics and spurious receiver responses. Configurable filter banks are provided for use in conjunction with the antenna system for controlled over-the-air operation. One filter bank is dedicated to each fixed system USRP. The RF filter banks are not required when using the RFnest and settings can be ignored in that case.

The filter banks may be manually set by accessing the switch at its assigned IP number on a web browser. Initial filter frequencies and IP numbers are shown in table 4.

Table 4. Filter bank assignments.

Switch Position (A,B)	Filter Bank 1	Filter Bank 2	Filter Bank 3	Filter Bank 4
1,1	800-1000 MHz	800-1000 MHz	800-1000 MHz	800-1000 MHz
2,2	2025-2075 MHz	2025-2075 MHz	2025-2075 MHz	2025-2075 MHz
3,3	2350-2550 MHz	2350-2550 MHz	2350-2550 MHz	not defined
4,4	3550-3650 MHz	3550-3650 MHz	3550-3650 MHz	3550-3650 MHz
IP Numbers	192.168.0.33	192.168.0.34	192.168.0.35	192.168.0.36
Other A,B combinations are invalid (disconnected).				

2.7 Antenna System

The system uses five ceiling mounted radome-enclosed, omni-directional, vertically polarized antennas operating over the range 698 - 6000 MHz. The antenna elements are procured from Galtronic Corporation Ltd., and the selected model is PEAR S4935i Pigtail – Broadband In-Building Omni Antenna (Fig. 7).

Each antenna is 1.65 lbs in weight, and has a diameter of 13.2” and height of 4.88”. Fig. 7 illustrates the antenna type, and its electrical specifications are presented in Table 5. For a more detailed list of antenna specifications and performance parameters, please refer to the antenna datasheet available online at [3].



Figure 7. Omni-directional, ceiling mounted antenna [3].

Table 5. Electrical parameters of the antenna [3].

Parameter	Frequency Band			
	698-790 MHz	790-960 MHz	1710-2700 MHz	2700-3200 MHz
VSWR	< 1.5:1			
Gain	1.5-2.5 dBi	2.0-3.5 dBi	4.5-7.0 dBi	5.0-6.0 dBi
Input	N-type connector with pigtail cable			
Input impedance	50 ohms			
Input Power	50 W at ambient temperature of 25 deg C			

2.8 User Equipment

The following UEs are currently available as part of our testbed:

1. Huawei B593s-22 [19]
2. Huawei E3276 LTE Dongle [18]
3. Huawei E8278 [20]
4. Rogers Aircard U330 [17]

Figure 8 illustrates the form factors of these UEs and Table 6 provides the specifications. All UEs use a test USIM from Rohde and Schwarz.

**Huawei B593s-22****Huawei E3276****Huawei E8278****Rogers Wireless U330****Figure 8. UEs.****Table 6. UE specifications.**

	Rogers USB Dongle	Huawei E3276	Huawei B593	Huawei E8278
Model	U330	E3276s-861	B593-s22	E8278
Interfaces	USB	USB	Ethernet, USB	USB
LTE mode	FDD	TDD	FDD/TDD	FDD/TDD
LTE bands	Band 3, 4, 7 and 17	Band 38	Band 1, 5, 7, 8, 9 (FDD); 38 (TDD)	Band 1, 5, 7, 8, 9 (FDD); 38 (TDD)
Build-in antenna	Yes	Yes	Yes	Yes
MIMO	No	Yes	Yes	Yes

2.9 Reference Oscillator and Clock Source

Ettus Research Octoclock. It has eight 10 MHz and eight 1 pulse per second reference signals. It distributes a common timing (1 pps) and 10 MHz reference signal to the USRPs and CMW500. The use of it is optional. You can select through the USRP hardware driver (uhd) whether to use an internal or external reference signals. Octoclock allows to provide an increase in frequency accuracy. The 1 pulse per second (1 pps) signal allows the sample clocks to be aligned.

2.11 RF Switch

LTE-CORNET provides support for over-the-air transmission as well as through RF cables. A switch allows switching between the cabled mode, going through the channel emulator, and the over-the-air transmission going through filters.

The default RF switch settings (position 1) connect the USRPs and CMW500 to the RFnest. By connecting switch sections A - D to position 2 the antennas are selected. Switch sections G and H may be used in concert to connect either the CMW500, antenna 5 or lab cable 7 to the RFnest.

The RF switch may be manually set by accessing the switch at its assigned IP number (192.168.0.30) on a web browser. Table 7 describes the switch settings.

Table 7. RF switch settings.

Switch Section	Common terminal	Position 1 (default)	Position 2
A	USRP 1	RFnest port 0	Antenna 1
B	USRP 2	RFnest port 1	Antenna 2
C	USRP 3	RFnest port 2	Antenna 3
D	USRP 4	RFnest port 3	Antenna 4
E	not defined	not defined	not defined
F	not defined	not defined	not defined
G	CMW500 in/out	RFnest port 8*	Cable 7 to lab
H	RFnest Port 8	CMW500 in/out*	Antenna 5

*only for 7A and 8A otherwise no connection

3. Software

Table 8 summarizes the software that is installed on the software processing nodes of LTE-CORNET.

Table 8a. Software installed on processing nodes.

	PC1	PC2	PC3	PC4 ¹	Rackmount Workstation	MW1 ²
User name	ltecornet1	ltecornet2	ltecornet3	wireless	ltecornet5	lte-durip
Operating System	Ubuntu 14.04 LTS	Ubuntu 14.04 LTS	Ubuntu 14.04 LTS	Fedora 20 (Heisenberg)	Ubuntu 14.04 LTS	Ubuntu 14.04 LTS
UHD	3.8.1	3.5.4	3.5.4	3.5.4	3.8.1	3.7.0
GNU Radio Companion	3.7.6.1	3.7.0	3.7.0	-	-	3.7.5
Amarisoft	June 1st, 2015 (3GPP Rel. 12)	-	-	January 20th, 2015 (3GPP Rel. 12)	June 23rd, 2016; Amarisoft 64 UE Emulator	3GPP Rel. 9 and 12
srsLTE	-	yes	yes	-	-	yes (libLTE)
OAI	-	yes	yes	-	-	-
RFnest	yes (RFveiw version 2.11)	-	-	-	-	-

¹ Available from another project.

² Mobile workstation (MW)

Table 8b. Software installed on processing nodes.

	MW7 ²	MW8	NUC-i5	NUC-i7-1	NUC-i7-2
Operating System	Ubuntu 14.04 LTS	Ubuntu 14.04 LTS	Windows 7 + Ubuntu 14.04 LTS	Windows 7	Windows 10
UHD	3.11.0 ¹	3.11.0 ¹	-	-	-
GNU Radio¹	3.7.10.1 ¹	3.7.10.1 ¹	-	-	-
Huawei UE Software	-	-	Yes	Yes	-

¹ On Ubuntu host virtual machine accessed via VMware Player

² Mobile workstation (MW)

3.1 Operating System and Support Software

3.1.1 Operating System

PC 1-3 run Linux Ubuntu 14.04, 64 bit version, Unity desktop. PC4 runs Fedora 20 (Heisenberg), Gnome.

3.1.2 USRP Hardware Driver

The USRP hardware driver (UHD) is the standard driver to access the USRP radio front end. UHD needs to be compatible with GNU Radio and other software libraries that access USRPs, such as Amarisoft or srsLTE. PC 1 runs the fairly latest UHD 3.8.1, while PCs 2-4 run UHD 3.5.4. The mobile workstations have UHD versions 3.7. and 3.11 installed, respectively.

3.2 Wireless Communications Software

3.2.1 Amarisoft

Amarisoft Software LTE eNodeB is installed currently on server 1 inside Durham 475. It supports operation with USRPs B210 and N210. While N210 needs a UHD version greater than 3.5.0, USRP N210 needs a UHD version 3.7.0 or greater. Any versions that do not satisfy these are incompatible with Amarisoft. In the tests that have been carried out so far, Amarisoft is able to connect to 2 UEs.

3.2.2 srsLTE

srsLTE (formerly libLTE) is an open-source and free SDR library for implementing 3GPP compliant LTE system on PCs connected to USRPs. It has a modular structure with minimal inter-modular and external dependencies. The current version is compliant with LTE Release 8, and is written entirely using C language. For more information, refer to the documentation in the website of the srsLTE project at [4].

3.2.3 Open Air Interface

The OpenAirInterface Software Alliance (OSA) is a French non-profit organisation that provides a standard-compliant implementation of a subset of Release 10 LTE for Linux-based general purpose computers. It is freely distributed by the Alliance and can be used with Ettus USRPs and PXIe platforms, in addition to custom hardware from EURECOM. More details about the OSA initiative can be found on their website at [5].

3.2.4 GNU Radio

GNURadio is a free and open-source SDK meant for implementing and rapid prototyping of DSP algorithms on Software Defined Radios. It can be used with a) low-cost external RF hardware to create a software radio, or b) used without any external hardware in a purely simulation-based setting.

GNURadio companion (GRC) version 3.7.6.1 is installed on server 1. To install GNURadio, it is recommended to use a version of UHD that is compatible with both Amarisoft (running on server 1) and GNURadio. Currently, UHD version 3.8.1 is running on this system, that has been found to be compatible with all other software tools on Server 1. For more details regarding the installation of GNURadio, please refer to the [path where the installation steps are described].

GNU Radio version 3.6, including GNU Radio Companion (GRC), is installed on most nodes. The mobile nodes M1 and M2 run the latest GNU Radio version, version 3.7. Upgrades to newer versions are planned based on the users' needs. We recommend using the build-gnuradio script available at [6]. See the GNU Radio Web site for more information, tutorials and related links.

4. Networking and User Access

Users will access the LTE-CORNET testbed remotely. Users can register and reserve the testbed for a reasonable duration. If approved, the single user or user group is granted exclusive access to the tested for the defined period. This section describes the user access mechanism and the internal testbed network that allows remotely controlling the different components of the system.

Table 9. LTE-CORNET networking specifications.

Computer/Device	MAC Address	IP Address 1	IP Address 2	Access software
Gateway	-----	192.168.0.1	128.173.94.254	OpenVPN
PC 1	eth0 - a0:36:9f:5e:c4:19 eth1 - 98:90:96:9c:be:24	192.168.10.1	192.168.0.11	VNC server
PC 2	eth0 - a0:36:9f:5e:c1:ac eth1 - 98:90:96:9c:c1:8c	192.168.10.1	192.168.0.12	VNC server
PC 3	eth0 - a0:36:9f:5e:c5:13 eth1 - 98:90:96:9c:bf:d7	192.168.10.1	192.168.0.13	VNC server
PC 4 (Fedora PC)	-----	192.168.10.1	N/A	----
Mobile workstation	eth0 - 00:0a:cd:21:49:8a eth1 - 34:e6:d7:06:38:53 wlan: 80:19:34:60:29:q8	192.168.10.1	N/A	----
CMW 500	-----	192.168.0.14	-----	Remmina
USRP 1-3	-----	192.168.10.2	-----	-----
RF Switches 1-7	-----	192.168.0.30-37	-----	-----
RF Attenuators 1-7	-----	192.168.0.40-47	-----	-----

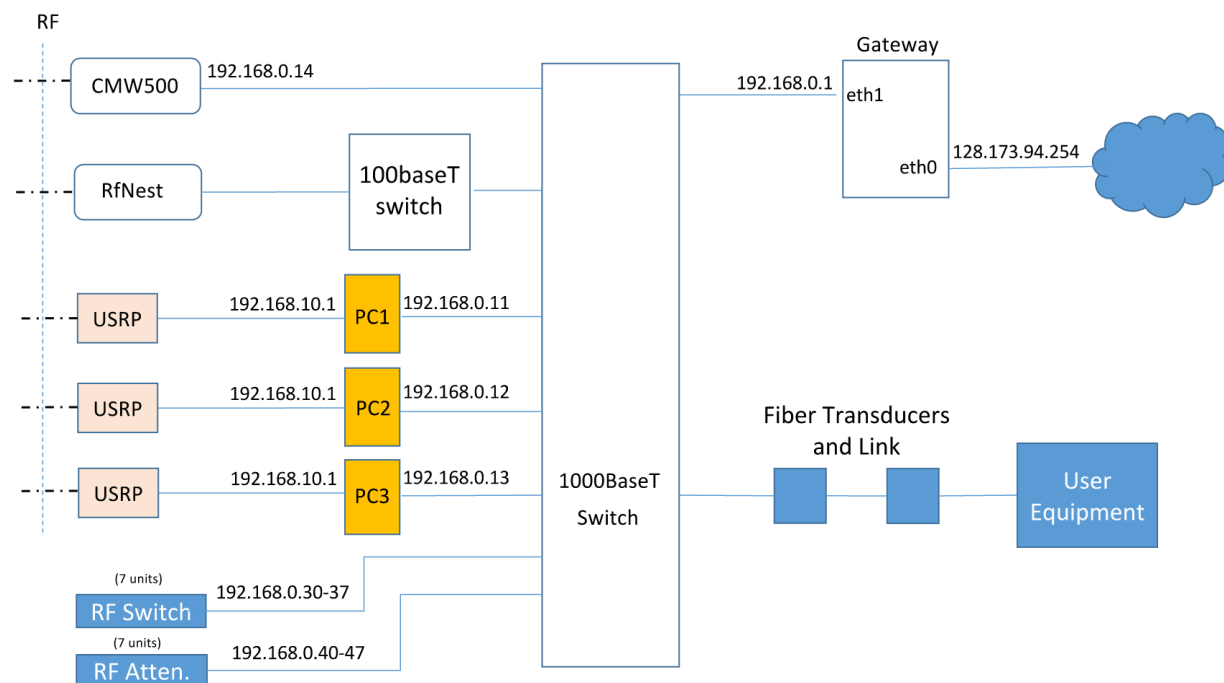


Figure 9. Network layout of the system

5. User Manual

5.1 User Registration and General Usage Instructions

Each testbed user is required to obtain a *username* and *password* from the system administrators. Users will be required to sign a user agreement that outlines their responsibilities and duties towards the operation of the testbed.

Being a very specialized experiment environment, users should familiarize themselves with a few important ideas:

- As with the operation of any radio equipment, there is always the possibility of accidentally creating harmful interference to other spectrum users. Hence, it is necessary for the testbed users to always be aware and considerate of other users and always consult the frequency plan before transmitting over-the-air.
- In normal operation, a normal user would not be required to update/install any software package on the systems. If such a need is sought, the user should please consult with the system administrator and seek his approval before proceeding with the experiment. There are complex interactions/dependencies between the various software modules installed on the testbed computers, and any attempt at updating/modifying them can likely break some functionality.
- Any data generated by the user and stored on the systems would be the user's' responsibility, and would have to be backed up elsewhere after the duration of the experiments. All systems are re-imaged and reset to the original state after the end of a user's approved experiment duration, and the administrators would not be responsible for any data loss that results from the same. Users are requested to work with the administrators towards data management and efficient utilization of system resources.

5.2 Access the Testbed

The testbed can be accessed remotely by authorized users over a Virtual Private Network (VPN) by using a valid .OVPN certificate that was issued by the testbed administrators. The certificate is verified by the gateway computer, and once authenticated, users are granted access to all the hardware systems of the testbed.

After obtaining an .OVPN certificate, the user would have to setup the OpenVPN software to access the testbed as follows:

- For Windows Users:
 1. Download and install the OpenVPN Windows Installer (64-bit) here:
<http://openvpn.net/index.php/open-source/downloads.html>
 2. During the OpenVPN install, accept the default options, and install the TAP-Windows device software when prompted.

3. Create and download your OpenVPN certificate here: <https://cornet.wireless.vt.edu/vpn>
 4. Move your ovpn file (<pid>.ovpn) to the C:\Program Files\OpenVPN\config folder
 5. Right click on the OpenVPN GUI icon on your desktop and select Properties
 6. Open the Compatibility tab
 7. Under Privilege Level, check the box for "Run this program as an Administrator" and click OK
 8. Open OpenVPN GUI
 9. You should now see a new network icon in the system tray on the lower right. Right click and select Connect
- For OS X Users:
 1. Download and install Tunnelblick
 2. Create and download your OpenVPN certificate here: <https://cornet.wireless.vt.edu/vpn>
 3. Double click your ovpn file (<pid>.ovpn) to install
 4. Select the Tunnelblick icon in the top right of the menu bar and connect

After setting up OpenVPN correctly, and connecting to the testbed using the certificate, users should be able to notice a 10.25.0.* IP address in their list of IP addresses. (*for windows: ipconfig /all, *nix: ifconfig*)

Note at this stage, the user has successfully connected to the main network switch of the testbed, and his or her computer would behave as if it was physically on the same network as the testbed components. The next step is to access the PCs for running the software, and have their GUIs displayed on the user's computer. These two steps are accomplished by using the software packages of PuTTY and TightVNC respectively.

5.2.1 PuTTY

PuTTY is an open-source SSH and telnet client for the Windows platform that is developed and supported by a group of volunteers. It was developed originally by Simon Tathan, and can be downloaded from [7]. Once connected over the VPN, Windows users may use PuTTY to access any of the three testbed computers as follows:

1. Open a PuTTY session (or similar utility). Enter the testbed computer's IP address and SSH.
2. When a terminal window opens you should see a login prompt. Enter your assigned user name.
3. Enter your password at the prompt. You will get a welcome screen. Do not run upgrades!
4. This is a command line on the testbed computer. You will have user and limited sudo privileges. Using TightVNC Viewer (described in the next section), users would be able to work with software GUIs.
5. To exit, halt all user programs and logout. Caution: Do not use "Shutdown" with no options from the command line. This will disable the node and require restarting it physically.

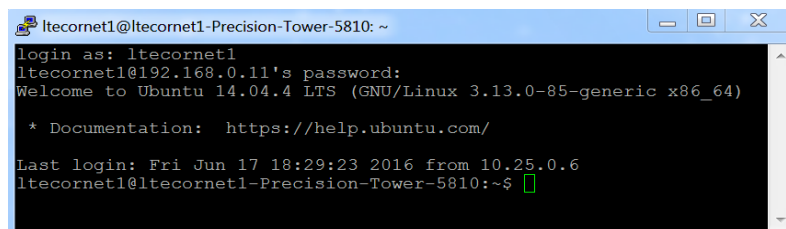


Figure 10: Sample SSH (putty) login screen and command prompt.

5.2.2 TightVNC Remote Desktop

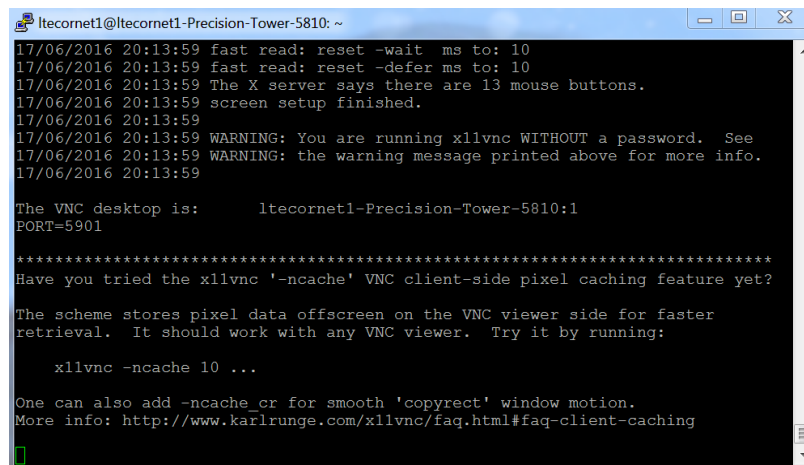
TightVNC is an open-source software allowing remote desktop export based on ssh. It allows one to control a remote machine with a local mouse and keyboard just like a user sitting in front of that computer.

Once the user has used PuTTY to access the testbed computers, the GUI screen can be accessed using TightVNC as follows:

1. At the command prompt, type the following:

```
$ x11vnc
```

This launches the remote desktop server on the machine, and the terminal window displays confirmation messages and a port number for the machine.



```
ltecornet1@ltecornet1-Precision-Tower-5810: ~
17/06/2016 20:13:59 fast read: reset -wait ms to: 10
17/06/2016 20:13:59 fast read: reset -defer ms to: 10
17/06/2016 20:13:59 The X server says there are 13 mouse buttons.
17/06/2016 20:13:59 screen setup finished.
17/06/2016 20:13:59
17/06/2016 20:13:59 WARNING: You are running x11vnc WITHOUT a password. See
17/06/2016 20:13:59 WARNING: the warning message printed above for more info.
17/06/2016 20:13:59

The VNC desktop is:      ltecornet1-Precision-Tower-5810:1
PORT=5901

*****
Have you tried the x11vnc '-ncache' VNC client-side pixel caching feature yet?

The scheme stores pixel data offscreen on the VNC viewer side for faster
retrieval. It should work with any VNC viewer. Try it by running:

    x11vnc -ncache 10 ...

One can also add -ncache_cr for smooth 'copyrect' window motion.
More info: http://www.karlrunge.com/x11vnc/faq.html#faq-client-caching
```

Figure 11: Sample command screen showing port number displayed after running `$ x11vnc`.

2. If not installed, users would have to install a VNC client on their computer. TightVNC has been tested extensively for accessing the testbed computers. It can be downloaded from [8].
3. Next, open the TightVNC Viewer and for the Remote Host, use the IP address of the testbed computer and the port number displayed earlier in the format: *ip_address :: port_number* and hit 'Connect'.

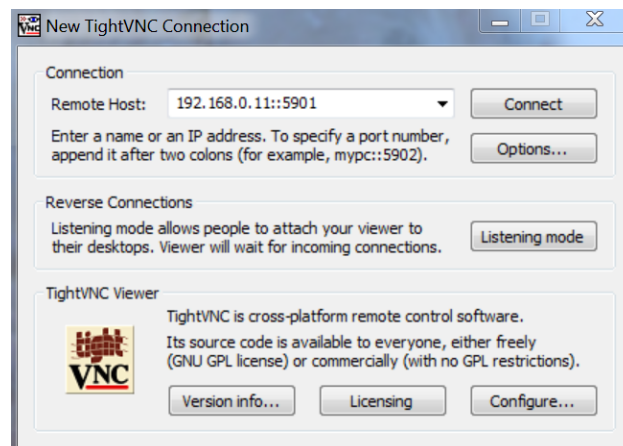


Figure 12: Sample TightVNC Viewer screen.

4. You should be viewing the remote desktop.
5. To exit the session, close your user software and exit Tight VNC.
6. Return to the terminal or putty and close your vnc session by using the command:

```
$ x11vnc -kill
```

5.2.3 Example of accessing the testbed

This section presents a screen-by-screen visual summary of the steps outline above for remote access of the testbed. After successfully completing this procedure, launching and remote operation of the CMW500 is also presented as an example. For each screen, the relevant menus and options are highlighted by a green outline for clarity.

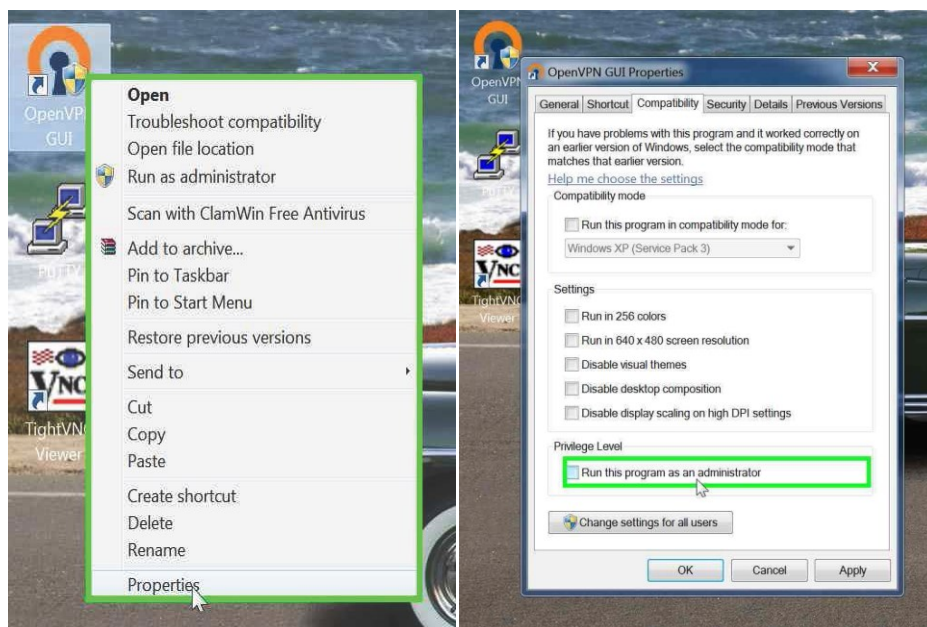


Figure 13a,b: Ensuring OpenVPN software has Administrator privileges.

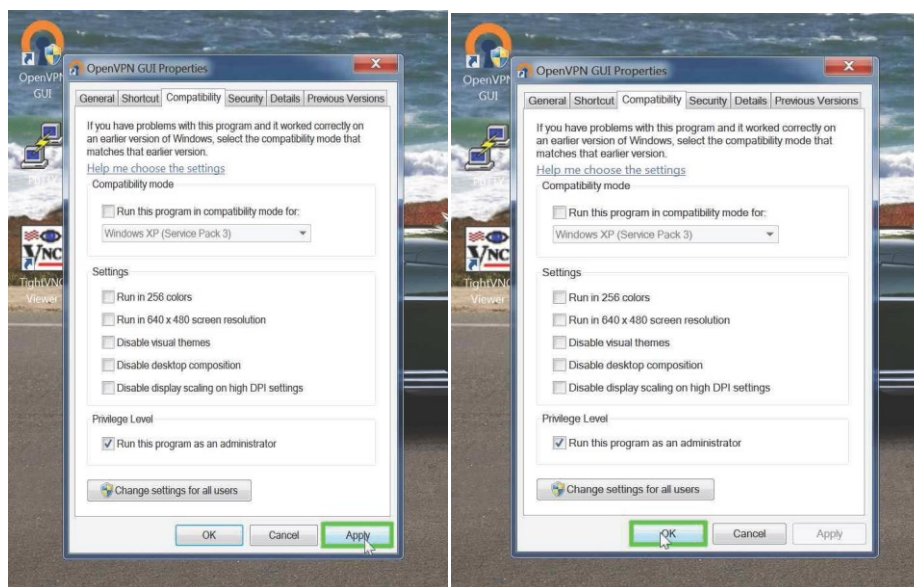


Figure 13c,d: Ensuring OpenVPN software has Administrator privileges (continued).

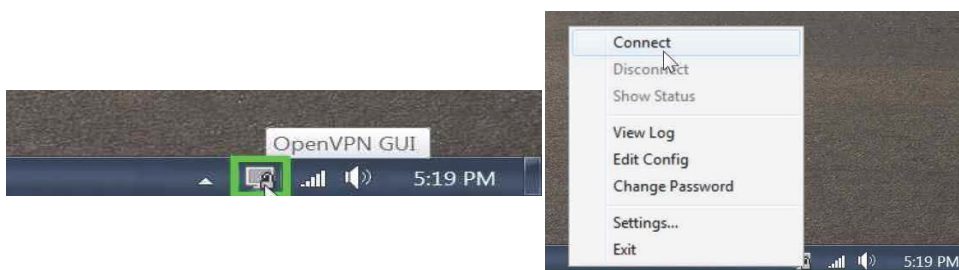


Figure 14a,b: Connecting using OpenVPN.

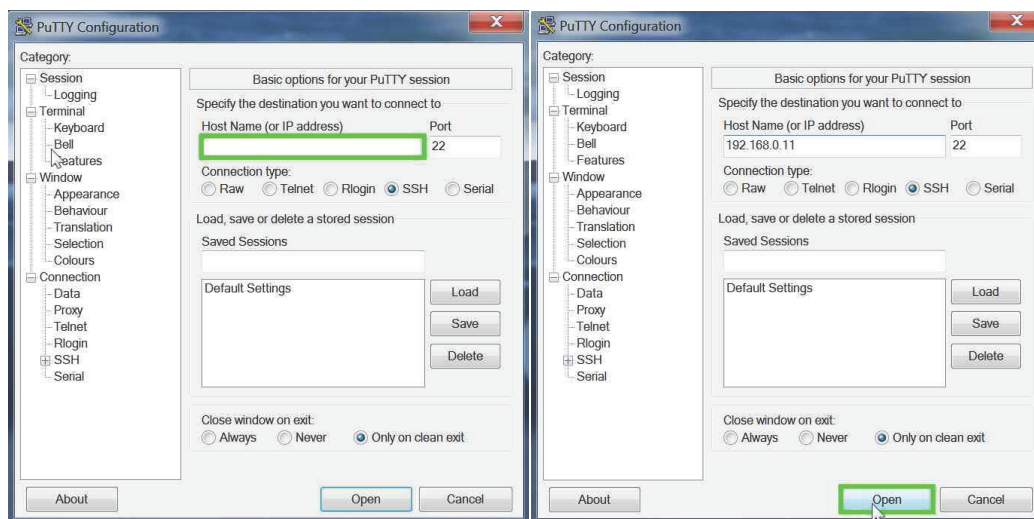
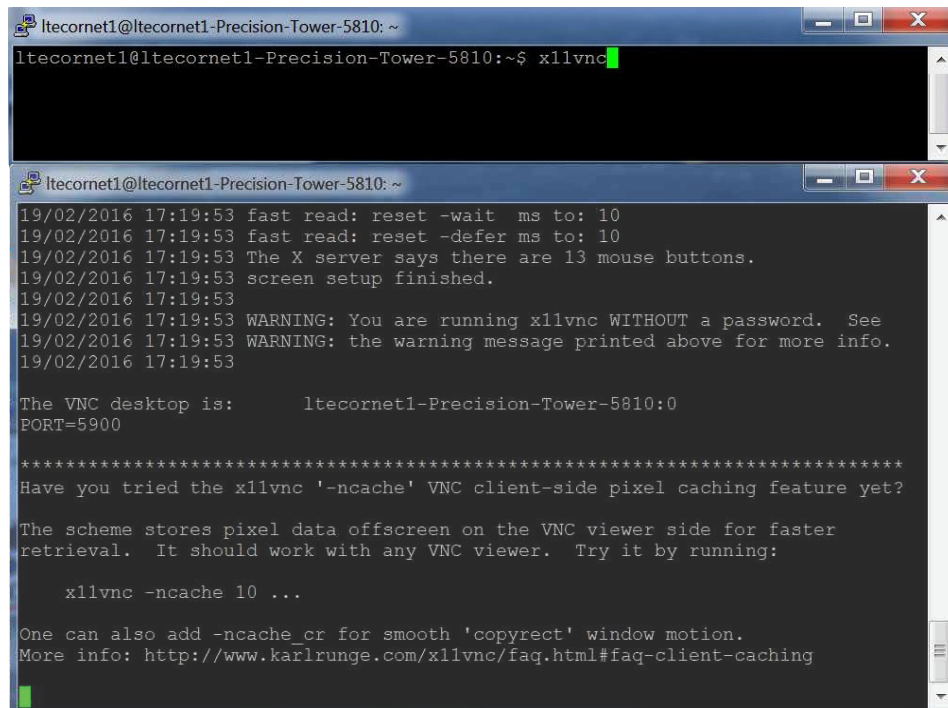


Figure 15a,b: Launching PuTTY.



The top terminal window shows the command `x11vnc` being executed in a shell on a system named `ltecornet1@ltecornet1-Precision-Tower-5810`.

The bottom terminal window shows the output of `x11vnc`, including timestamps, log messages, and a warning about running without a password. It also displays the VNC desktop address as `ltecornet1-Precision-Tower-5810:0` and `PORT=5900`. A message suggests using the `-ncache` option for better performance.

```
ltecornet1@ltecornet1-Precision-Tower-5810: ~
ltecornet1@ltecornet1-Precision-Tower-5810:~$ x11vnc

19/02/2016 17:19:53 fast read: reset -wait ms to: 10
19/02/2016 17:19:53 fast read: reset -defer ms to: 10
19/02/2016 17:19:53 The X server says there are 13 mouse buttons.
19/02/2016 17:19:53 screen setup finished.
19/02/2016 17:19:53
19/02/2016 17:19:53 WARNING: You are running x11vnc WITHOUT a password. See
19/02/2016 17:19:53 WARNING: the warning message printed above for more info.
19/02/2016 17:19:53

The VNC desktop is:      ltecornet1-Precision-Tower-5810:0
PORT=5900

*****
Have you tried the x11vnc '-ncache' VNC client-side pixel caching feature yet?

The scheme stores pixel data offscreen on the VNC viewer side for faster
retrieval. It should work with any VNC viewer. Try it by running:

    x11vnc -ncache 10 ...

One can also add -ncache_cr for smooth 'copyrect' window motion.
More info: http://www.karlrunge.com/x11vnc/faq.html#faq-client-caching
```

Figure 16a,b: Launching the remote desktop server.

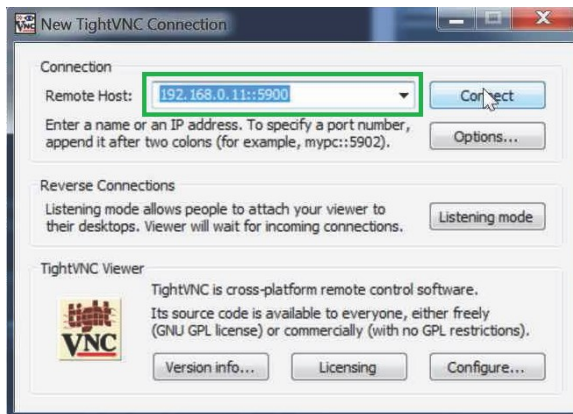


Figure 17: Launching TightVNC Viewer.

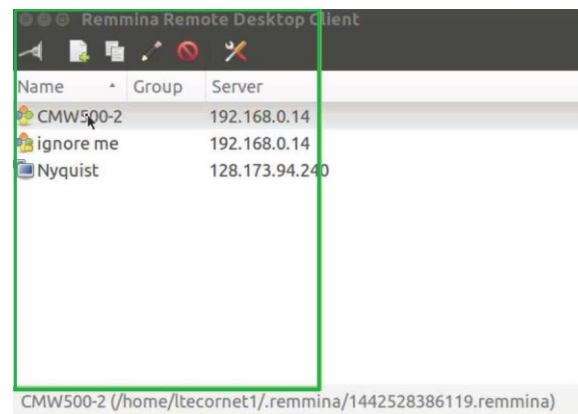


Figure 18: Launching Remmina Client to connect to CMW500.

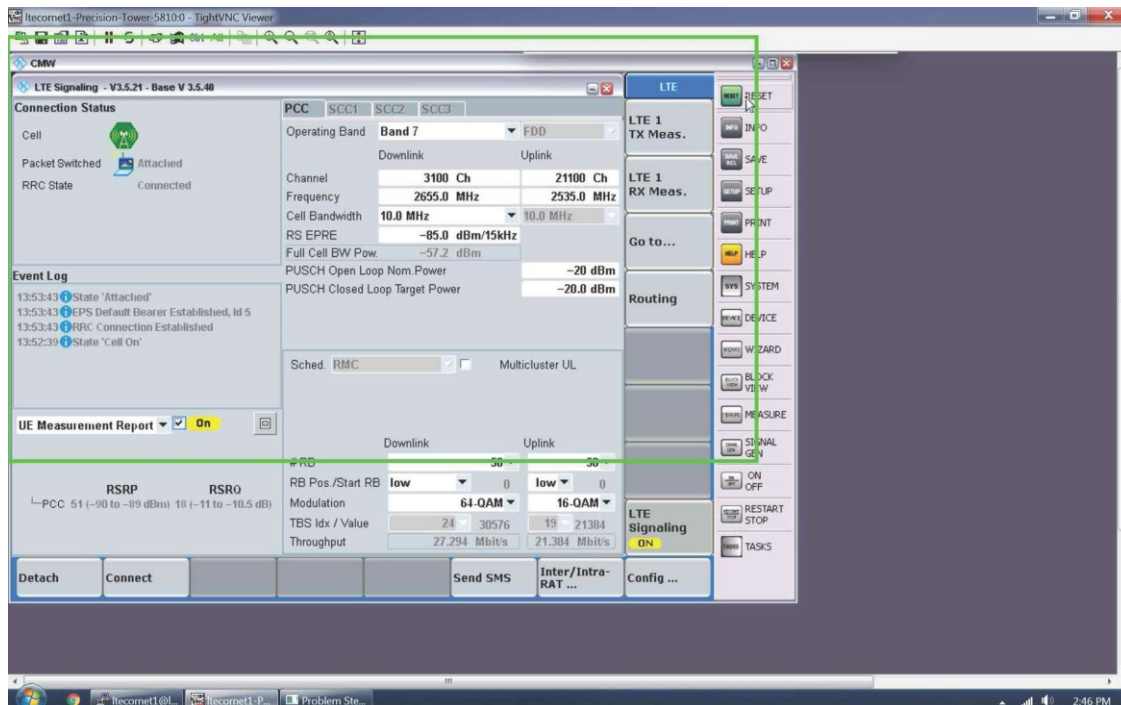


Figure 19: The CMW500 interface.

5.3 Configure the Testbed

This section describes the steps involved in using the various testbed for deploying a LTE base station, core network and channel emulator scenarios. For a more detailed discussion, the user is encouraged to refer to the specific documentation for the particular software or hardware component.

5.3.1 Amarisoft

Amarisoft's Amari LTE 100 is a software eNodeB + Evolved Packet Core Network. It gives a powerful computer interfaced with a USRP, the capability to form its own LTE Evolved Packet Core Network. This section describes the procedure of installing the software package, and on using it.

The two most important modules of Amarisoft that the user needs to be aware of are

1. **LTEENB:** This module implements the radio front-end of the eNodeB on the USRP interfaced to the computer. The USRPs currently in use, in the testbed are B210s and the N210s.
2. **LTEMME:** The module emulates the Mobility Management Entity (MME) + Evolved Packet core of the LTE network.

Installing Amarisoft on an Ubuntu Machine

1. Install dependencies, especially for Stream Control Transmission Protocol (SCTP) as this is how the USRPs communicate with the machine.

```
sudo apt-get install lksctp-tools linux-image-extra-3.13.0-24-generic.
```

Some symbolic links may be necessary due to naming differences between Fedora and Ubuntu:

```
$ls -s /lib/x86_64-linux-gnu/libcrypto.so.1.0.0 /lib/x86_64-linux-gnu/libcrypto.so.10
```



```
$ln -s /lib/x86_64-linux-gnu/libssl.so.1.0.0 /lib/x86_64-linux-  
gnu/libssl.so.10
```

2. Install UHDS (USRP Hardware Driver). To run Amarisoft with
 - a. USRP N210 - UHD version 3.5.4 and above.
 - b. USRP B210 - UHD version 3.7.0 and above.

Advisable to do a source installation of the UHDS. Follow the procedure in http://files.ettus.com/manual/page_build_guide.html under sections “Getting the source code”, “Build Instructions (UNIX)” and “Post-install tasks”.

3. Install Amarisoft by getting the license keys. The license keys are obtained by running

```
$sudo ./ltemme config/mme.cfg
```

or

```
$sudo ./lteenb config/enb.cfg
```

The node-locked license presents a 16-digit hexadecimal code that needs to be sent to support@amarisoft.com. Once the keys are obtained, of names ‘ltemme.key’ and ‘lteenb.key’. Create a folder .amarisoft in the home directory of the root user and copy these keys in the folder:

```
$su  
$cd /root/  
$mkdir ./amarisoft  
$cp {Folder where the keys are present} /root/.amarisoft/
```

4. Set up IP forwarding and masquerading on the PC. The script for doing so is written in ‘lte_init.sh’. Not setting this up would prevent the UEs from being able to access the internet.

Using Amarisoft

The most common applications of Amarisoft involve execution of the LTEENB (eNodeB) and LTEMME (Mobility Management Entity) modules. The most basic configuration for testing Amarisoft is by executing

```
$sudo ./ltemme config/mme.cfg
```

and in another terminal, execute

```
$sudo ./lteenb config/enb.cfg
```

Care must be taken to ensure that the appropriate configuration files are used in ‘enb.cfg’. For USRP B210, it is “rf_driver-lchan-b2x0.cfg” and for N210, it is “rf_driver-lchan.cfg”.

There are a lot of parameters that can be changed in the configuration file. For detailed information, read the Amarisoft documentation on LTEENB.

It is possible to connect multiple USRPs to the same PC running Amarisoft, constrained by the number of Ethernet (for the N210) and the USB (for the B210) ports and the computational power of the PC. This is possible by the following sequence of steps

1. Changing the GTP-U addresses in the specific configuration files,
2. adding the USRP device serial number in the driver configuration file for the USRP, i.e. “rf_driver-lchan-b2x0.cfg” and for N210, it is “rf_driver-lchan.cfg”.

5.3.2 RFnest

The RFnest hardware uses two software modules for executing different scenarios - the Channel Emulator Controller (CEC), and the RFView GUI. The GUI provides a visual environment to define the parameters of the scenario, and the CEC acts as the interface with the hardware. Hence, it is always a good practice to first launch the CEC, followed by the GUI each time the attenuation values between the ports are to be modified. With the CEC running in the background, the RFView GUI should be launched through a separate terminal window. This section describes the steps required to access the RFView GUI and CEC. For specific instructions on creating and modifying scenarios using the GUI, the user should consult the RFnest documentation and examples contained in them.

The procedure for launching CEC and RFView GUI is as follows:

1. Navigate to the CEC installation folder by typing the following command in a terminal window

```
$ cd Desktop  
$ cd cec
```

2. The next step is launching the CEC script. This is done by the command,

```
$ ./run.sh
```

3. Once CEC is running, its version number is displayed in the terminal. Closing the terminal window will exit CEC, and it is recommend to use a separate terminal window for launching other programs.

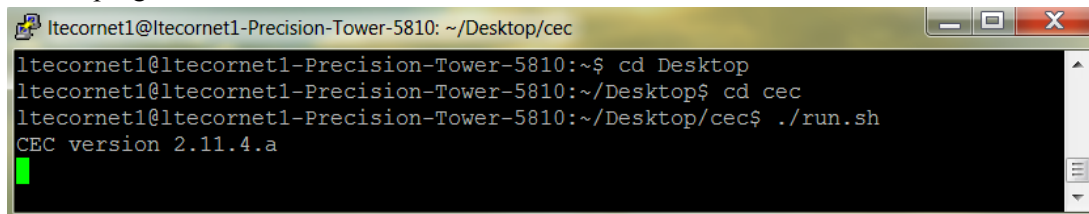


Figure 20: Launching CEC using the terminal.

The procedure for launching RFview GUI is as follows:

1. Navigate to the RFnest installation folder by typing the following command in a terminal window

```
$ cd Desktop  
$ cd rfview
```

2. The next step is launching the RFview script. This is done by the command,

```
$ ./rfview.sh
```

3. Once launched, the terminal window displays a confirmation message and the GUI is launched. Use the RFnest documentation to configure and modify scenarios using the GUI.

```

ltecornet1@ltecornet1-Precision-Tower-5810: ~/Desktop/rfview
ltecornet1@ltecornet1-Precision-Tower-5810:~$ cd Desktop
ltecornet1@ltecornet1-Precision-Tower-5810:~/Desktop$ cd rfview
ltecornet1@ltecornet1-Precision-Tower-5810:~/Desktop/rfview$ ./rfview.sh
The capacity changed from 48 to 24 and the purge size changed from 35 to 15.

```

Figure 21: Launching RFview script using the terminal.

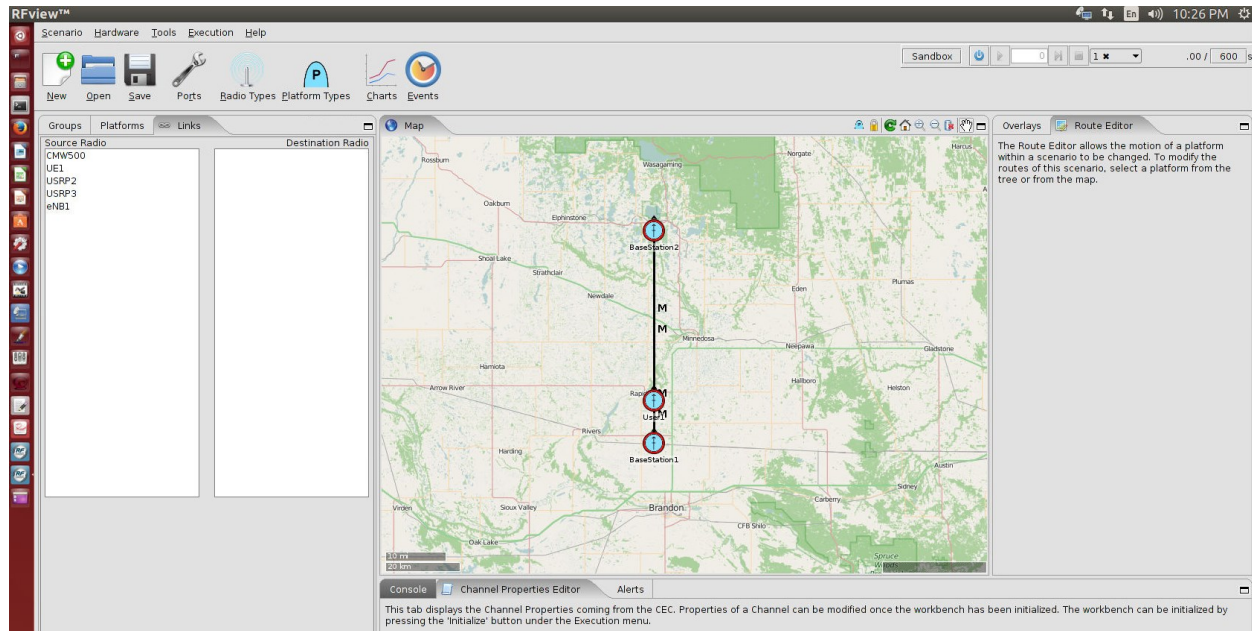


Figure 22: RFview GUI showing a loaded scenario.

4. At any time, pressing the button next to the 'Sandbox' option on the menu bar initializes the system. If at the end of the initialization process, an error is displayed instead of a confirmation message, check if the hardware is powered ON and if CEC is running correctly.

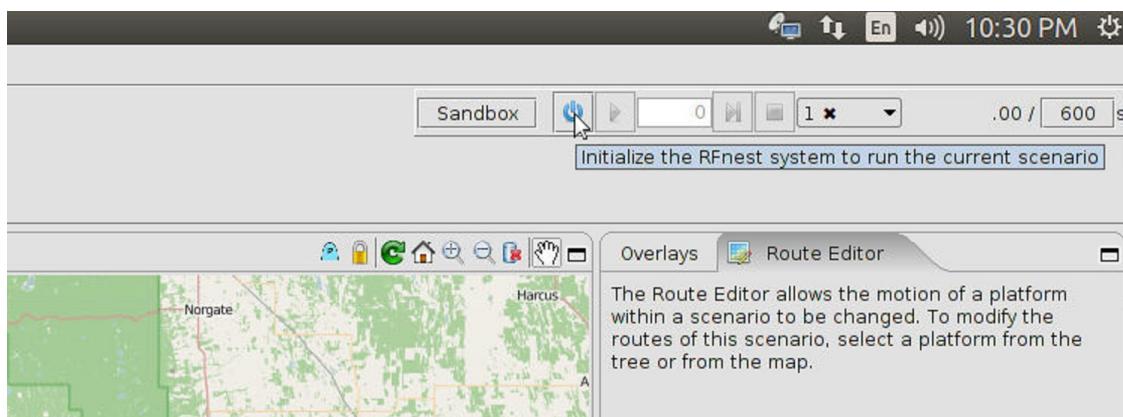


Figure 23: Initializing the RFnest hardware using RFview GUI.

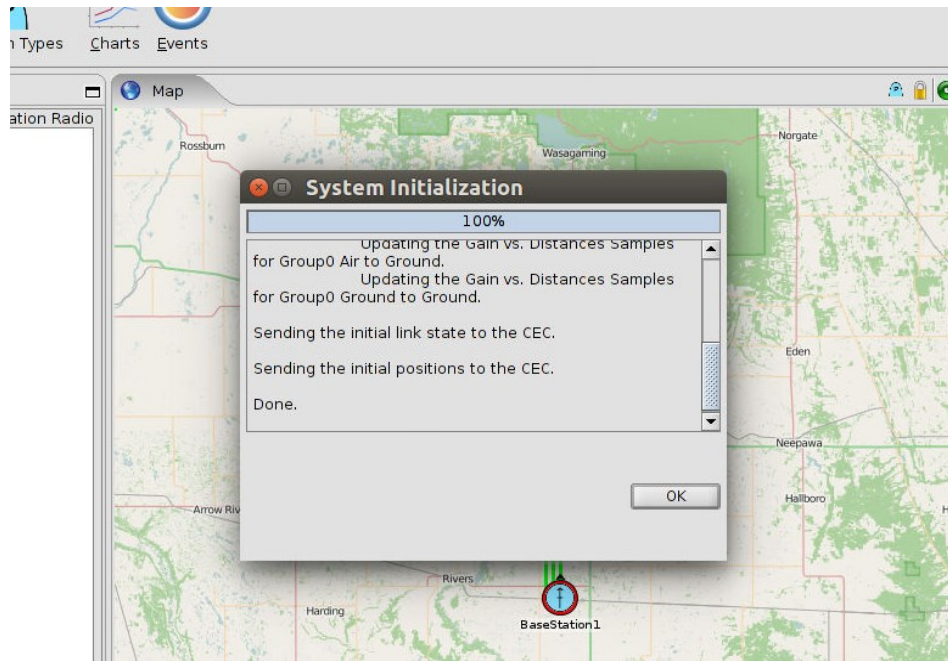


Figure 24: Confirmation message displayed after successful initialization of the RFnest hardware.

5.3.3 CMW500

The procedure for accessing the CMW500 instrument is outlined in an example in the earlier section. For specific instructions on setting up an eNodeB, modifying parameters, accessing performance parameters etc. the user may please refer to the CMW500 User Guide and White Papers available online on the Rohde & Schwarz website.

It is always a good practice to reset the CMW500 at the start of an experiment session. This ensures that all parameters are configured as per the requirements of the current experiment, and eliminates the accidental use of an earlier configuration.

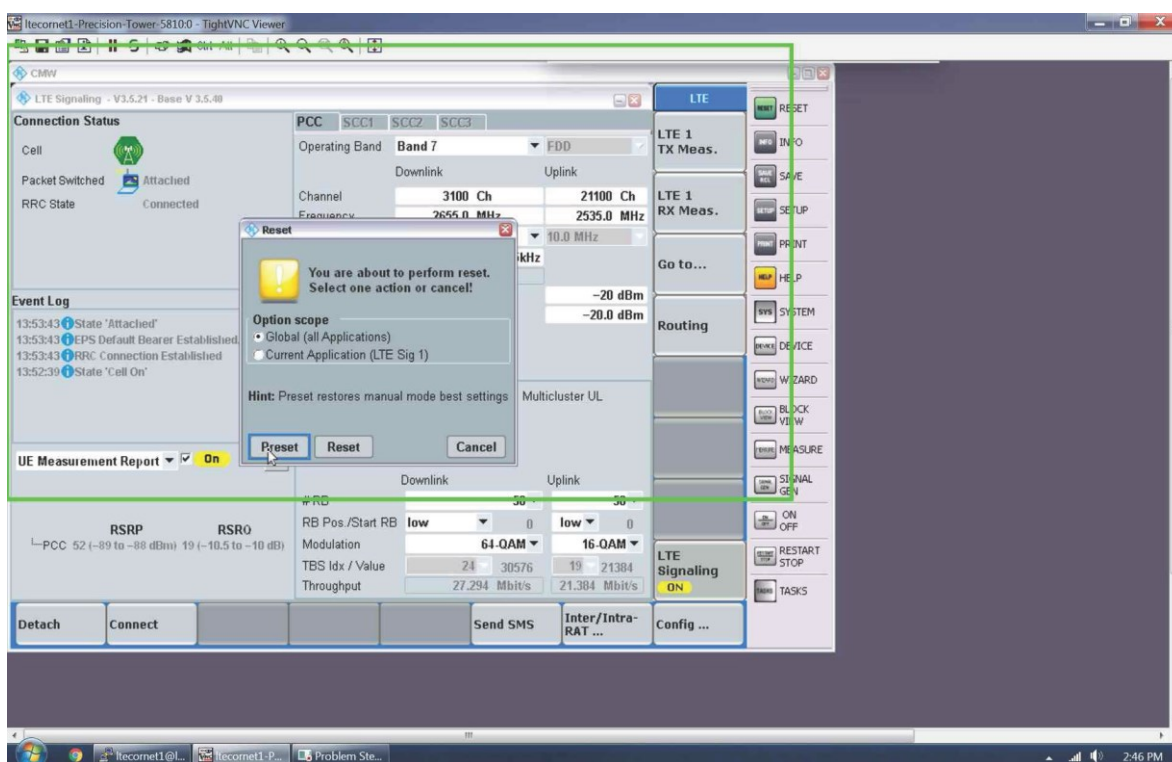


Figure 25: Performing a reset on the CMW500 prior to an experiment.

Also, if not being used for an extended duration of time, it is a good practice to turn off the signal generators on the CMW500. This helps in conserving power and also prolongs the life of the RF hardware.

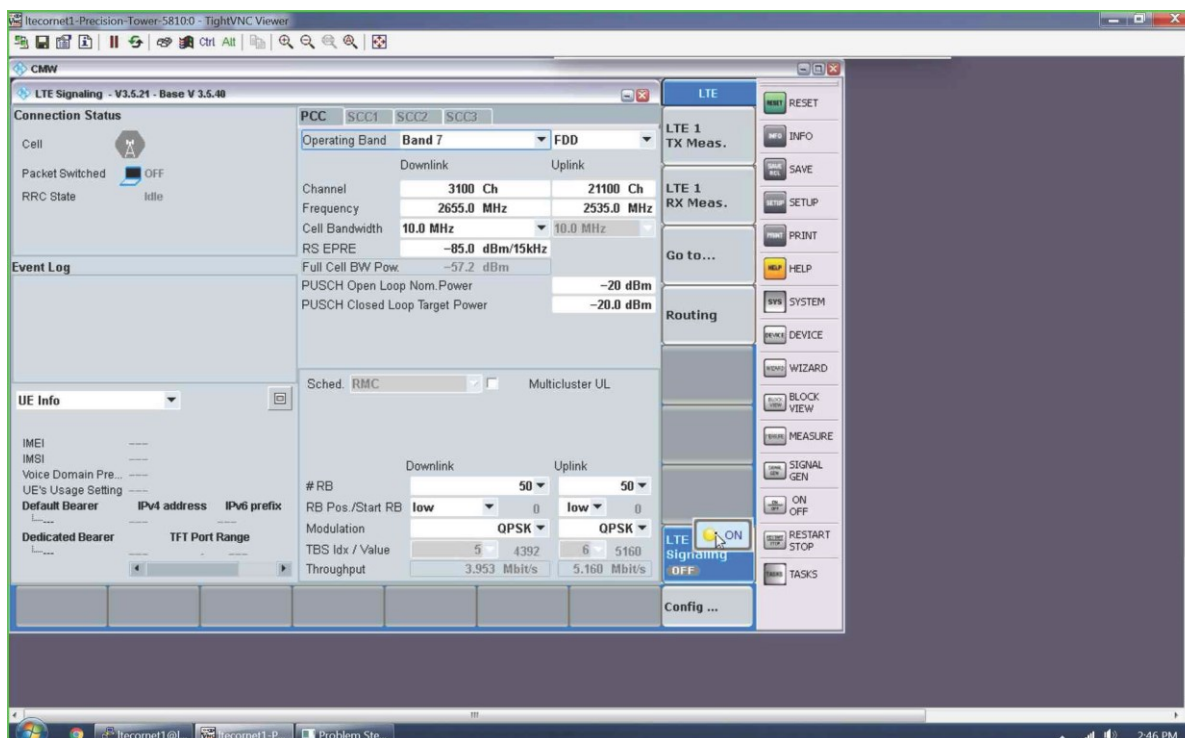


Figure 26: Turning the Signal Generator ON/OFF using the CMW500 interface.

5.3.4 UE

Two UEs have been used extensively for experimentation with the testbed, namely the Rogers AirCard 330U by Sierra Wireless, and the B593s router by Huawei. This section describes the basic operation and configuration of the same for use with the testbed. For more information on specific device, refer to the UE sub-section in the testbed document, and also to the respective devices' documentation.

UE interfaces have a lot of common features, and the points described here could be used for other manufacturer's devices as well. It is always a good idea to check these settings before using a device for the testbed, and resetting it to factory condition and starting configuration over if needed.

Using the Rogers AirCard 330U:

1. Check that a correct test-sim is inserted correctly into the UE. The USIM details would be needed for authentication on the network.
2. The Rogers UE has been tested with Windows machines. When the UE is first plugged into the computer's USB port, the driver installation menu launches automatically. Follow the on-screen instructions and the necessary drivers and the Rogers Connection Manager utility are installed.
3. Follow the path Options -> Network and verify that the all of the LTE frequency bands are selected for use.
4. Follow the path Options -> Profiles -> Rogers LTE -> Advanced -> TCP/IP settings and verify that parameters are configured correctly.

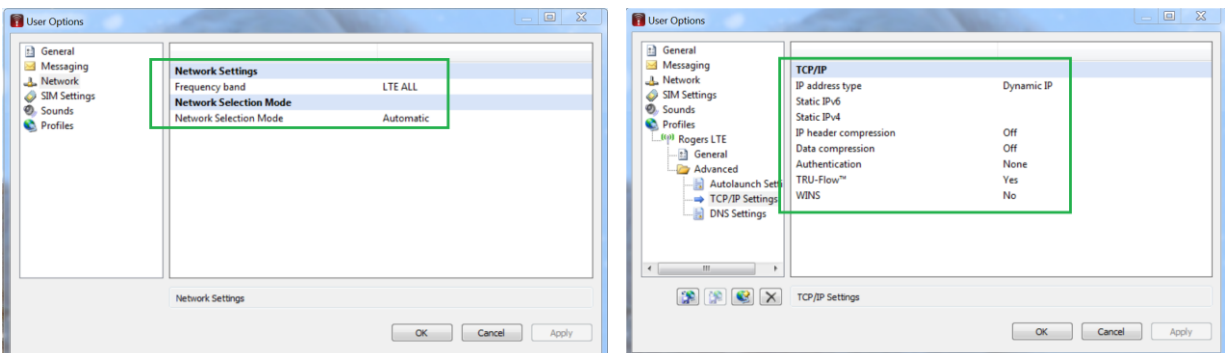


Figure 27: Configuring the Rogers UE.

Using the Huawei B593s:

1. The Huawei B593s router doesn't require any drivers to be installed for its operation. Its internal page can be accessed using any internet browser on any platform by connecting over LAN on any one of the 4 LAN ports.
2. Check the device documentation for the path to the internal page as it may be different across different generations of the same device. For the current devices, it is located at:

`http://192.168.8.1/html/home.html`

3. The default login id is `admin` and the password is `admin` as well. It is a good practice to either leave the default login unchanged, or to make a note of the new login information if modifying the same.

5.3.6 iperf and jperf

iPerf is a measurement tool that creates streams of traffic data and determines the maximum achievable bandwidth on IP networks. It is originally developed by ESnet/Lawrence Berkeley National Laboratory and is available for download from its homepage at [9].

6. System Administration

The LTE-CORNET testbed can be administered remotely. User accounts can be setup for individual or a set of nodes. A few personal accounts have been created as well as generic student accounts that can be used to provide access to attendees of CORNET tutorials, among others. Only the system administrator account has root privileges.

Portable and mobile nodes, additional fixed node mounts, antennas, as well and other support equipment is located in Durham 439 and can be checked out for conducting experiments. The equipment is to be exclusively used for conducting related research or education or for the purpose of advancing the O-CORNET infrastructure and will be locked in drawers while not in use. Wireless@Virginia Tech will manage the equipment and maintain a log file with regular backups to keep track of the equipment as well as the experiments that are being conducted. The CORNET web site will serve as a portal for this.

7. Testbed Use in Research and Education

7.1 Education

The testbed has been used by students of the graduate-level classes *Cellular Communication Systems* (ECE 5664) and *Software Radios* (ECE 5674) at Virginia Tech. Students used the fixed and mobile nodes for experimenting with LTE signals and open-source SDR software libraries and frameworks. An example class project from the 2013 Software Radios class is described in continuation.

Fifth generation (5G) wireless networks are predicted to be optimized at each layer of the protocol stack to meet the necessary $1000\times$ capacity enhancement. At the physical layer, there is widespread research focus on alternate waveforms that have better characteristics than OFDM used in 4G. Some of the waveform contenders include Filter-bank Multicarrier (FBMC), Universal Filtered Multicarrier (UFMC), and Faster than Nyquist (FTN) [12]. We have taken a step forward in this direction by porting a Filtered Multi-Tone FBMC (FMT-FBMC) waveform on a Universal Software Radio Peripheral (USRP) using GNU Radio. This was part of an SDR class project at Virginia Tech in 2015. More precisely, the FMT-FBMC transceiver is implemented in GNU Radio [6] to demonstrate communication using four parallel 16-QAM symbol streams or subchannels. The software runs on PC2 and the RF signal through RFnest with 30 dB attenuation. Figure 28 illustrates the received constellation diagrams for the four symbols streams before equalization. The constellation is rotated with respect to the ideal constellation being the result of uncompensated phase shifts due to propagation delays.

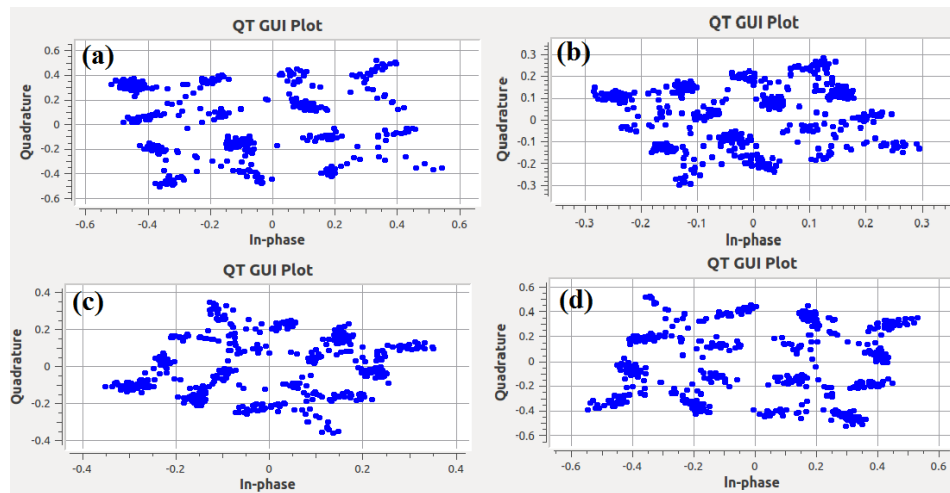


Figure 28: Constellation diagram of the four 16-QAM data streams of the FMT-FBMC waveform.

This implementation can be extended to operate at full capacity using Staggered Multi-tone FBMC (ST-FBMC) at full-capacity [13].

Open source software toolboxes, such as GNURadio [6], srsLTE [4], and liquidDSP [14], can be used on our testbed to design and prototype new signal processing algorithms and protocols for the evolution of 4G LTE or new 5G waveforms.

7.2 Research

7.2.1 LTE Evolution into Shared and Unlicensed Spectrum

Facing the need of $1000\times$ enhancement in capacity by 2020 [21], the wireless research community is on the pursuit of technologies to bridge this gap. One of the ways this has been proposed to be implemented in the near future, is by extending LTE into the unlicensed and shared spectrum. One approach is aggregating bandwidth in shared spectrum as a secondary cell to the primary cell in licensed spectrum through the LTE-A feature *carrier aggregation* [11]. This technology is being termed as LTE-Unlicensed (LTE-U) or Licensed Assisted Access (LAA) and is currently standardized by the 3GPP, although other proposals for LTE-Unlicensed exist. It targets the 5 GHz band, which is used by WiFi and radar systems. LTE is also considered for deployment in the new shared bands, such as the new 3.5 GHz band and the AWS-3 bands in the US.

One of the challenges of operating LTE in unlicensed and shared spectrum is the ability to coexist with legacy systems in that band. Since LTE will be the secondary user system, it will need to back off whenever the primary or incumbent access (IA) user uses the band. There is some timeframe x within which the channel needs to be vacated. Ideally, within this timeframe, the LTE system should find another band and handoff all its users with an active session without disrupting or terminating the service. We define *interfering cell* as the cell that would interfere with the primary or incumbent access users and propose using handover as a mechanism for the secondary users to vacate to another band whenever primary or incumbent access users need access to the band. Here we discuss two mechanisms that we tested for multi-cell handovers using two (primary) cells at different center frequencies (EARFCNs) that are supported by the UEs:

1. Gradually lower the power of the interfering cell upon detection of a primary user such that there is a smooth transition of the UE from one cell to another.
2. Force the user to move out of the interfering cell by turning the cell off upon detection of the presence of primary users. This would result in cell reattachment and disrupts the active session.

In addition to initial cell deployments, we can rapidly deploy a new cell in a different band, and force the user to move into that cell or, handover the UE to the newly deployed cell gradually. Based on initial experiments, we are able to execute the entire process within one minute. Stricter channel vacation and UE handover or reattachment times are needed, which requires more research. We performed experiments on forced handovers, using our testbed. LTE100 was used to set up two FD-LTE cells in adjacent channels with a single B210 USRP: cell 0x01 (DL: 2680 MHz, UL: 2560 MHz) and cell 0x02 (DL: 2674.9 MHz, UL: 2544.9 MHz). Figure 29 shows the stages of forcing a user out of the interfering cell, which in this case is cell 0x01. Even though this experiment is carried out in LTE Band 7, it is representative of the scenarios that would occur in shared or unlicensed bands.

Instead of using two primary cells, we can use one primary cell and one or more secondary cells through the carrier aggregation feature of LTE-A, which is supported by Amarisoft's LTE100 eNB.

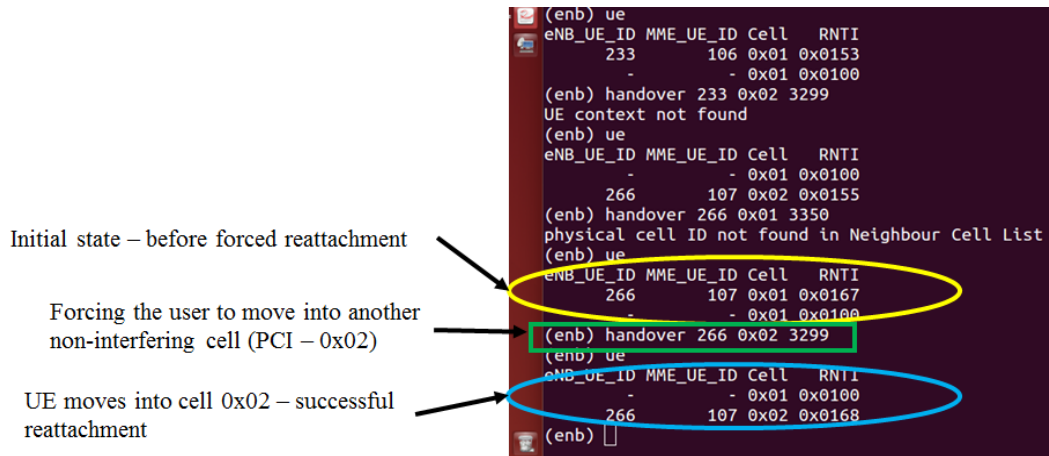


Figure 29: Snapshot showing the stages of forced handover with the forced handover feature of LTE100.

7.2.2 LTE for Mission-critical Networks

LTE has been used in the domain of public safety (FirstNet), and military communication networks in USA. Since commercialization of LTE has resulted in the public availability of standards documentation, adversaries with malicious intent could leverage this to target weak spots in the LTE protocol stack in order to enhance the potency of their attack.

We carried out several experiments to assess the impact of jamming and spoofing on LTE/LTE-A and proposed mitigation strategies to protect against the most efficient adversarial attacks that can cause Denial-of-Service (DoS). Figure 30 shows one of our experiment configurations using a combination of fixed and mobile testbed nodes. See [15], [16], and [23] for more information.

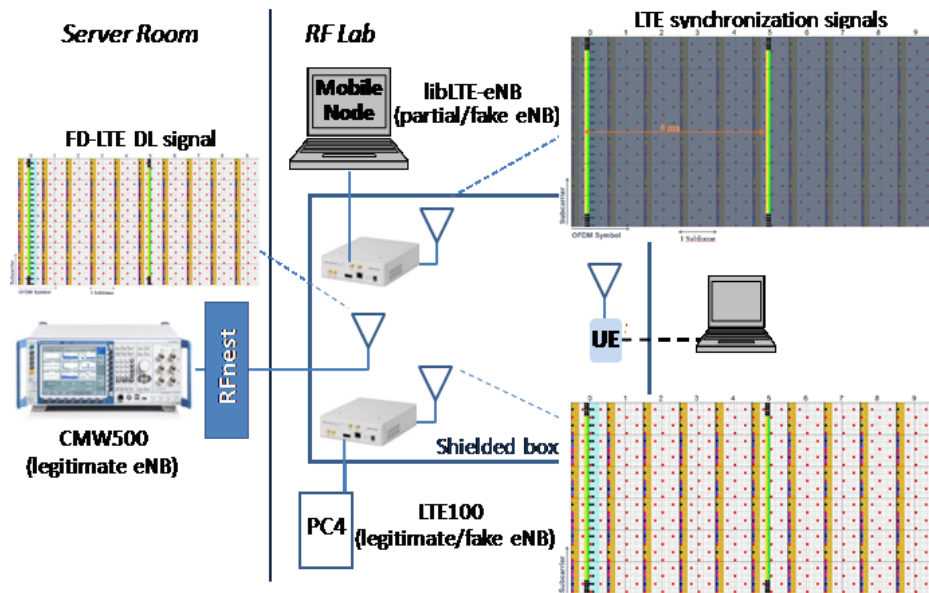


Figure 30: Experiment setup for the LTE vulnerability analyses of [15] [16] [23].

8. Conclusions and Lessons Learned

LTE-CORNET has enabled research and education in 4G LTE and LTE-Advanced. It supports experimental validation of theoretical research results. Students and researchers have used parts of the testbed since 2014. Some of these projects are described in Section 7. Initial research results have been published in peer-reviewed journals and conference proceedings (see Appendix C).

The testbed has already been expanded with more hardware and software, as described in the final report for the Cognitive Medical Wireless Testbed System (COMWITS), supported under Army Research Office DURIP Grant W911NF-14-1-0554. It will continue to enable research and education in emerging areas of communications with applications to commercial (4G, 5G), military, hospitals of the future, IoT, and many other systems. Some of the lessons learned are described below.

A. Computing power

The CPU load at the software eNodeB is proportional to the LTE bandwidth. Using a bandwidth greater than 10 MHz resulted in a large number of underflow/overflow errors when communicating with the USRP device due to not enough CPU time being available. Even at 10 MHz, care had to be taken while running additional software packages like iPerf to prevent these errors.

B. Heating of USRP

Since the USRP was operated at high data rates inside a shielded enclosure, the heat generated by the device would frequently lead to oscillator drift and frequent disconnection of the UE. Hence, it was necessary to stop and restart the eNodeB signalling before each measurement to prevent overheating.

C. UE Disconnection

Occasionally, the UE behaviour was erratic and it would refuse to latch onto the network. On other occasions, it would randomly disconnect from the network. This was initially suspected to be an issue with device authentication, and a number of test USIMs and IMSI combinations were attempted, but there was not much luck. Finally, the only reliable option to shake the UE out of its random behaviour was to do a full factory reset of its internal settings.

D. Throughput measurements

When LTE throughput is measured in uplink or downlink, separate RF paths are needed to provide separate attenuation on uplink and downlink to avoid disconnection of UEs because of weak downlink signals when measuring uplink throughput. Note that the LTE test equipment used has different output powers than regular LTE equipment. In particular, the SDR or CMW500 RF outputs can be significantly lower than the UE output power. Reference signal received power measured at the UE is accurately reported to the eNB. CQI and MCS are tightly correlated with each other. Monitoring MCS helps analyzing results, because there are standard tables that related MCS and transport block sizes [22]

E. MIMO measurements

During MIMO measurements it was observed that increasing the analog gains of the USRPs tend to cause frequent UE disconnections.

F. Performance of Cat. 3 UEs

When referring to 2x2 MIMO operation with Cat. 3 UEs, it is important to understand that they support only two layers of spatial multiplexing on the DL, but not on the UL. This means that with a Cat. 3 UE, the maximum UL data rate that can be achieved is that as of the SISO case. Further, Cat. 3 UEs can achieve a maximum of 64 QAM only in DL (MCS 28) while they are limited to a maximum modulation scheme of 16QAM in the UL (MCS 20).

References

- [1] CORNET Web Site, <http://cornet.wireless.vt.edu>
- [2] Tektronix H500/SA2500 Datasheet, <http://www.tek.com/sites/tek.com/files/media/media/resources/H500-SA2500-Spectrum-Analyzer-Datasheet-1.pdf>
- [3] PEAR™ S4935i Pigtail Broadband In-Building Antenna Datasheet, <http://www.galtronics.com/wp-content/uploads/2015/02/Galtronics-PEAR-S4935i-Pigtail-Datasheet.pdf>
- [4] srsLTE - Open-Source LTE, <https://github.com/srsLTE/srsLTE>
- [5] The OpenAirInterface Software Alliance (OSA), <http://www.openairinterface.org/>
- [6] Install GNU Radio, <http://gnuradio.org/redmine/projects/gnuradio/wiki/InstallingGRFromSource>
- [7] PuTTY homepage, <http://www.putty.org/>
- [8] TightVNC, <http://tightvnc.com/download.php>
- [9] iPerf homepage, <https://iperf.fr/>
- [10] JPerf download page, <https://sourceforge.net/projects/jperf/>
- [11] R. Zhang, M. Wang, L. X. Cai, Z. Zheng, X. Shen and L. L. Xie, "LTE unlicensed: the future of spectrum aggregation for cellular networks," in *IEEE Wireless Communications*, vol. 22, no. 3, pp. 150-159, June 2015.
- [12] P. Banelli, S. Buzzi, G. Colavolpe, A. Modenini, F. Rusek and A. Ugolini, "Modulation Formats and Waveforms for 5G Networks: Who Will Be the Heir of OFDM? – An overview of alternative modulation schemes for improved spectral efficiency," *IEEE Signal Processing Magazine*, vol. 31, no. 6, pp. 80-93, Nov. 2014.
- [13] M. Bellanger, "FBMC Physical Layer: A Primer", PHYSDYAS, 2010, URL: http://www.ict-phydyas.org/teamspace/internal-folder/FBMC-Primer_06-2010.pdf
- [14] liquidsdr.org - Making Software Radio Portable Homepage, <http://liquidsdr.org/>
- [15] M. Lichtman, R. P. Jover, M. Labib, R. M. Rao, V. Marojevic, J. H. Reed, "LTE/LTE-A Jamming, Spoofing and Sniffing: Threat Assessment and Mitigation," *IEEE Commun. Mag.*, vol. 54, no. 4, pp. 2-9, April 2016.
- [16] M. Labib, V. Marojevic, J. Reed, "Analyzing and enhancing the resilience of LTE/LTE-A," *Proc. IEEE Conf. Standards for Communications and Networking (CSCN)*, Tokyo, Japan, 28-30 Oct. 2015.
- [17] Sierra Wireless AirCard 330U, "Quick start guide," <https://www.sierrawireless.com/>
- [18] Huawei E3276 4G LTE Mobile Internet Key, "User guide," Version: V100R001_01 Part Number: 31010NWB.
- [19] Huawei Technologies Co., Ltd, "Welcome to the LTE CPE! - Online help."
- [20] Huawei E8278, "User guide."
- [21] Technical specifications for Sierra Wireless AirCard® 330U LTE Mobile Broadband Modem, <http://www.rogers.com/cms/images/en/Wireless/CellPhoneDetail/Support/Sierra-Wireless-AirCard330Uen.pdf>
- [22] Technical Specification, LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures (3GPP TS 36.213 version 12.4.0 Release 12).
- [23] M. Labib, V. Marojevic, J.H. Reed, A.I. Zaghloul, "Enhancing the robustness of LTE systems: analysis and evolution of the cell selection process," *IEEE Commun. Mag.*, accepted Aug. 2016, to be published.

Appendix A: FCC Experimental License Application Process

Introduction and Background

In order to ensure that the radio frequency spectrum may be shared efficiently by a large number of users the Federal Communications Commission (FCC) was established by Congress. The FCC established regulations that provided for segregated frequency bands which divide the spectrum according to usage. For example, audio broadcasting is allocated frequency bands around 1 MHz (AM) and 100 MHz (FM) while television broadcasting is allocated several frequency bands above 54 MHz but not including the 100 MHz audio broadcast band. Numerous other services compete for the spectrum including Public Safety, land mobile and common carriers (e.g. Cellular telephone)¹. Certain frequency bands are also reserved for Federal Government and Military use. Those frequencies are coordinated by other agencies such as the NTIA. Within the various frequency bands most services are allocated particular frequencies which are coordinated on a geographic basis to prevent interference within a local area. The ideas of frequency and geographic separation of users is the basis for almost all of our radio regulations. In order to regulate radio frequency usage the FCC provides a licensing system where applications are reviewed for compliance with the regulations. If approved, a license is issued for a specific time period. Particular frequencies, locations and modes of operations are specified in the license.

In addition to the usual radio services, the FCC provides for an experimental radio service. An experimental radio license is issued to those who have a specific need to use a portion of the radio spectrum either to conduct radio experiments or where radio is required as a part of an experimental system². Experimental radio is administered through the FCC Office of Engineering Technology (OET). The CAER Cognitive Radio Testbed and CORNET are examples of systems requiring an experimental license.

Obtaining an Experimental License

Experimental radio is administered through the FCC Office of Engineering Technology (OET). Applicants for experimental licenses use an online Experimental Licensing System (ELS)³. (Other online systems are used for Commercial and Amateur radio services.) For experiments lasting 6 months or less an application for a Special Temporary Authorization (STA) should be made. For longer term experiments an Experimental License should be requested. The Experimental license procedure is described below.

Obtain a FRN

Before applying it is necessary to get a FCC Registration Number (FRN) which identifies the applicant. The FRN may be obtained by registering online using the FCC CORES system⁴. The FRN should be recorded as it is used for all future FCC applications Business information, tax ID number and applicant information are required for the FRN application. The FRN is public information. . There is a search

¹ Title 47 Code of Federal Regulations (CFR), http://www.ecfr.gov/cgi-bin/text-idx?SID=a3ca4e7e75b40503be19b91c4a188323&tpl=/ecfrbrowse/Title47/47tab_02.tpl

² Title 47 CFR Chapter 1A subpart 5, http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=a3ca4e7e75b40503be19b91c4a188323&tpl=/ecfrbrowse/Title47/47cfr5_main_02.tpl

³ <https://apps.fcc.gov/oetcf/els/index.cfm>

⁴ <https://apps.fcc.gov/coreWeb/publicHome.do>

engine that allows the FRN to be found is it is lost. A required password should also be recorded as it is required to edit the FRN information.

Application Process

Start at the index page: <https://apps.fcc.gov/oetcf/els/index.cfm>

Under the “Miscellaneous” menu heading select “User Guide” to view a comprehensive manual for the licensing process.

A practice application site is provided to help users to learn the process. Data entered at the practice site will not be processed by the FCC. The practice site can be accessed through the hyperlink on the index page labeled “the Experimental Licensing System test site”.

Select: “Form 442 - New License/Modification of License”. On the new page select new application and enter your FRN then “proceed”.

Administrative Section Entry

On the new page you enter your contact information and answer a few questions on the nature of the experimental program. Additional descriptive information will be required depending on your answers to questions 4 through 7. That information should be placed in a PDF file and inserted at the end of the application process. For a “radio test-bed” the answers to questions 5, 6 and 9 are probably “no”. The FCC may not issue the license for the full term of planned operation. If not you will be able to renew the license. “Proceed” to the next application page.

The following page “question 10” requests information on the transmitting equipment used in the experiment. Enter the Manufacturer, model and number of units. If the equipment is experimental indicate so as “yes”. For example: Manufacturer: Ettus Engineering, Model: E110, Number of units: 10, Experimental: Yes. Select either “enter more equipment” or “proceed”.

The next page contains questions 11 through 18. The answers to questions 11, 13 and 14 will probably be “no”. The answers to questions 15 and 17 will probably be “yes”.

The application is “signed” by typing your name in the appropriate box. The application is far from complete at this point though! “Proceed” to the next section.

File and Confirmation Numbers

At this point you will receive a “File Number” and a “confirmation number” it is very important to record those values as you won’t be able to restart the application process without them. If you close the web browser at this point you will need the numbers to log back in to the application. They are also required to check the application status.

An outline of the technical data entry procedure is also given on this page. The technical data entry can be confusing and redundant. It may require several attempts before getting everything in order. “Proceed” to the next application page.

Antenna Registration Entry

The “Antenna Registration” page specifies the location of the antenna/radio used. There may be other antennas which are added on other application pages. For an indoor SDR test bed (depending on the configuration) it may be possible to treat all units as “mobile”. In that case enter the coordinates of the

building and a radius of operation that includes the entire building. “Directional Antenna” and “Antenna Height” questions are probably “no”. “Proceed” to the Antenna Frequency Registration.

Frequency Registration Entry

At this page it will be necessary to enter frequency bands and power levels that will be used by the transmitters. Frequency tolerance may be left blank if a wide band of frequencies is specified. A typical frequency range would be 3550-3650 MHz. Where possible it is good to use existing frequency band limits and emission types for a particular service as this avoids some coordination questions. If a restricted frequency band (such as an emergency frequency) is included in the frequency range it will probably be rejected. It probably isn't a good idea to include the whole spectrum in one line! Specify reasonable power levels. The antenna gain will probably be zero dBi or less so the ERP can be identical to the transmitter power 1W peak is probably a good value to choose for the test bed. You may use less than the specified amount of power. Continue to add frequencies as necessary by selecting the appropriate button. After all frequencies have been added you can continue by adding emissions to each frequency.

Emissions Entry

The emissions portion of the application requires the applicant to specify the type of modulation and bandwidth that will be used. Multiple emissions may be specified for each frequency band. Each frequency band must have at least one emission specified. This tends to make the application very complex in cases such as a SDR test-bed where many different emissions are to be tested. Fortunately, it is possible to request a modification to the license to add emissions at a later date. Once the emission is determined an emissions designator and bandwidth must be formulated. For example: F3E is a frequency modulated analog sound transmission. A copy of the emissions designator table is included as an Appendix to this report. Some emissions are more difficult to define, however. An accepted designator for a LTE signal is W7W which falls into the “cases not covered above” category. In cases where the emissions designator is not sufficient to describe the signal it may be necessary to attach an explanation to the application. The process is repeated until all frequencies and emissions are complete.

Attachments

Near the end of the application process is the attachment section. Attach any additional information here as appropriate. A PDF document is usually the best format. Some common attachments are listed here.

Experiment description or Government project information (as determined by application questions 4-7).

Stop buzzer page: gives the contact information in case the experiment must be terminated immediately.

Request for fee waiver: Educational and certain other agencies may request a fee waiver. Attach a text document (PDF) that explains the situation.

Fee Payment

Fee payment is required for most applicants. If a fee waiver has been requested the payment may be skipped. Otherwise the details are shown on the Fee Payment page of the application.

Processing the Application

Once the application has been completed the FCC will usually either grant it within a few weeks or ask for additional information. In cases where there are Government users of the frequencies requested the license application will be forwarded to the appropriate government agency for review. This review process takes additional time.

Example Application

The VT O-CORNET license, described below, is an example of what can be obtained through this process. Note that the license is very specific as to location, frequencies and emissions. There are also limitations or “Special Conditions” appended to the license. Typically the Special Conditions contain a statement that the experimental station must cease operation if it causes interference. Another typical statement omits the frequency tolerance requirement. Another typical condition statement is that the experimental user must coordinate with other users before operating on the frequency. These conditions effectively make the experimental license secondary to all other licenses and subject to termination if any interference occurs.

FCC Experimental License

Our experimental FCC license for the campus-wider O-CORNET testbed cover several bands as indicated in the table below.

Table A.1: Frequency bands and transmission parameters for FCC experimental license for fixed, mobile and portable O-CORNET SDR nodes (see also <https://apps.fcc.gov/els/GetAtt.html?id=154653&x=>).

Frequency [MHz]	Data Type	Modulation	Max. channel bandwidth [MHz]
450 - 512	Digital, Analog	BPSK, QPSK, QAM, A0, F2, F3, 1M40W7W (OFDM, LTE)	1.4 (LTE)
764 – 862 (98 MHz)	Digital, Analog	BPSK, QPSK, QAM, A0, F2, F3, 1M40W7W (OFDM, LTE)	1.4 (LTE)
869 - 894	Digital, Analog	BPSK, QPSK, QAM, A0, F2, 1M40W7W (OFDM, LTE)	1.4 (LTE)
902 - 928 (ISM 1)	Digital, Analog	BPSK, QPSK, QAM, A0, A3, F2, F3, 1M40W7W (OFDM, LTE)	1.4 (LTE)
2000 - 2100	Digital, Analog	BPSK, QPSK, QAM, A0, F2, F3, 10M0W7W (OFDM, LTE)	10 (LTE)
3400 - 3550	Digital, Analog	QPSK, 16QAM, 64QAM, A0, F2, F3, 3M00P0N, 40M0W7W (OFDM, LTE)	40 (LTE) 3 (pulse)
3550 - 3650	Digital, Analog	QPSK, 16QAM, 64QAM, 256QAM, A0, F2, F3, 3M00P0N, 40M0W7W (OFDM, LTE)	40 (LTE) 3 (pulse)

F2: FSK

F3: FM

A0: unmodulated (single tone)

A3: AM, including single-sideband voice

3M00P0N: Unmodulated pulse, 3 MHz bandwidth

5M00W7W, 10M0W7W: OFDMA 5 MHz and 10 MHz

Emission types: http://wireless.fcc.gov/services/index.htm?job=licensing_2&id=industrial_business
<http://www.comreg.ie/fileupload/publications/ComReg0834.pdf>

Appendix B: FCC Emissions Table

§ 2.201 Emission, modulation, and transmission characteristics.

The following system of designating emission, modulation, and transmission characteristics shall be employed.

(a) Emissions are designated according to their classification and their necessary bandwidth.

(b) Three symbols are used to describe the basic characteristics of emissions. Emissions are classified and symbolized according to the following characteristics:

(1) First symbol—type of modulation of the main carrier;

(2) Second symbol—nature of signal(s) modulating the main carrier;

(3) Third symbol—type of information to be transmitted.

Note to paragraph (b): Two additional symbols for the classification of emissions may be added for a more complete description of an emission. See Appendix 1, Sub-Section IIB of the ITU *Radio Regulations* for the specifications of these fourth and fifth symbols. Use of these symbols is not required by the Commission.

(c) First Symbol—types of modulation of the main carrier:

(1) Emission of an unmodulated carrier	N
(2) Emission in which the main carrier is amplitude-modulated (including cases where sub-carriers are angle-modulated):	
—Double-sideband	A
—Single-sideband, full carrier	H
—Single-sideband, reduced or variable level carrier	R
—Single-sideband, suppressed carrier	J
—Independent sidebands	B
—Vestigial sideband	C
(3) Emission in which the main carrier is angle-modulated:	
—Frequency modulation	F
—Phase modulation	G
(4) Emission in which the main carrier is amplitude and angle-modulated either simult. or in a pre-established sequence	D
(5) Emission of pulses: ¹	
—Sequence of unmodulated pulses	P
—A sequence of pulses:	
—Modulated in amplitude	K
—Modulated in width/duration	L
—Modulated in position/phase	M

—In which the carrier is angle-modulated during the period of the pulse	Q
—Which is a combination of the foregoing or is produced by other means	V
(6) Cases not covered above, in which an emission consists of the main carrier modulated, either simultaneously or in a pre-established sequence, in a combination of two or more of the following modes: amplitude, angle, pulse	W
(7) Cases not otherwise covered	X

¹ Emissions where the main carrier is directly modulated by a signal which has been coded into quantized form (e.g. pulse code modulation) should be designated under (2) or (3).

Note: Whenever frequency modulation “F” is indicated, Phase modulation “G” is also acceptable.

(d) Second Symbol—nature of signal(s) modulating the main carrier:

(1) No modulating signal	0
(2) A single channel containing quantized or digital information without the use of a modulating sub-carrier, excluding time-division multiplex	1
(3) A single channel containing quantized or digital information with the use of a modulating sub-carrier, excluding time-division multiplex	2
(4) A single channel containing analogue information	3
(5) Two or more channels containing quantized or digital information	7
(6) Two or more channels containing analogue information	8
(7) Composite system with one or more channels containing quantized or digital information, together with one or more channels containing analogue information	9
(8) Cases not otherwise covered	X

(e) Third Symbol—type of information² to be transmitted:

(1) No information transmitted	N
(2) Telegraphy—for aural reception	A
(3) Telegraphy—for automatic reception	B
(4) Facsimile	C
(5) Data transmission, telemetry, telecommand	D
(6) Telephony (including sound broadcasting)	E
(7) Television (video)	F
(8) Combination of the above	W
(9) Cases not otherwise covered	X

² In this context the word “information” does not include information of a constant, unvarying nature such as is provided by standard frequency emissions, continuous wave and pulse radars, etc.

(f) Type *B* emission: As an exception to the above principles, damped waves are symbolized in the Commission's rules and regulations as type *B* emission. The use of type *B* emissions is forbidden.

(g) Whenever the full designation of an emission is necessary, the symbol for that emission, as given above, shall be preceded by the necessary bandwidth of the emission as indicated in § 2.202(b)(1).

[49 FR 48697, Dec. 14, 1984, as amended at 75 FR 63030, Oct. 13, 2010]

Appendix C: Equipment List

Tables C.1 and C.2 list the main and auxiliary LTE-CORNET equipment, source and purchase prices.

Table C.1. Main equipment list.

Product	Source	#	Unit Price ⁵	Total Price
RFnest A208 (1.8-2.8 GHz)	Intelligent Automation Inc.	1	\$22,000	\$22,000
1201.0002K50: CMW500 (Serial # 152659)	Rohde & Schwarz	1		
• CMW-PS503: CMW500 Basic Assembly (mainframe), 70MHz to 3.3GHz		1	\$10,024	\$10,024
• CMW-S100A (includes H100A): Baseband Measurement Unit, with 1GByte digitizer memory		1	\$2,511	\$2,511
• CMW-S550B (includes H550B): Baseband Interconnection, flexible link, for non-signaling, signaling and IQ access		1	\$1,383	\$1,383
• CMW-S570B (includes H570B): RF Converter (TRX)		1	\$7,004	\$7,004
• CMW-S590A (includes H590A): RF Frontend, basic functionality		1	\$1,463	\$1,463
• CMW-S600B (includes H600B): CMW500 frontpanel with display/keypad		1	\$1,422	\$1,422
• CMW-B300B (includes H300B): Signaling Unit Wideband, for WCDMA / LTE		1	\$10,684	\$10,684
• CMW-B620A (includes H620A): Digital Video Interface (DVI)		1	\$253	\$253
• CMW-KB036: Extended frequency range, 3.3 GHz to 6 GHz, per RF converter		1	\$6,496	\$6,496
• CMW-KM010: Spectrum analyzer, resolution bandwidth 100 Hz to 10 MHz		1	\$2,030	\$2,030
• CMW-KM550: LTE TDD (TD-LTE) Release 8, TX measurement, uplink		1	\$5,277	\$5,277
• CMW-KN550: LTE TDD Release 8/9, eNode B TX measurement, Downlink		1	\$4,062	\$4,062
• CMW-KS550: LTE TDD Rel. 8, signaling/network emulation, basic functionality		1	\$9,020	\$9,020
• CMW-KS525: LTE, user defined bands, signaling/network emulation, generic feature		2	\$5,316	\$10,632
Amarisoft LTE 100 eNB Software License	Amarisoft, www.amarisoft.com	1	\$4,947	\$4,947
Amarisoft LTE 100 eNB Software License	Amarisoft, www.amarisoft.com	1	\$5,748	\$5,748
Amarisoft LTE 100-64 UE Software License	Amarisoft, www.amarisoft.com	1	\$7,228	\$7,228
Dell Precision Tower 5810	Dell, Inc. www.dell.com	3	\$2,735	\$8,206

⁵ Including discounts, where available

Product	Source	#	Unit Price ⁶	Total Price
Dell Mobile Workstation M4800	Dell, Inc. www.dell.com	1	\$2,367	\$2,367
Dell Mobile Workstation: Mobile Precision 7510	Dell, Inc. www.dell.com	2	\$2,144	\$4,288
Dell Precision Rack 7910: Rackmount Workstation	Dell, Inc. www.dell.com	1	\$10,618	\$10,618
Ettus Research Octoclock	National Instruments, www.ni.com	1	\$909	\$909
Ettus Research USRP N210 w/ SBX daughterboards	National Instruments, www.ni.com	3	\$2,197	\$6,591
Ettus Research USRP B210	National Instruments, www.ni.com	2	\$1,100	\$2,200
Ettus Research USRP B210 w/ enclosures	National Instruments, www.ni.com	8 ⁷	\$1,194	\$1,958
RF Switch: MiniCircuits RC-2SP4T-A18 (4) + BKT-272-08+ (2)	MiniCircuits, www.minicircuits.com	4	\$2,210	\$8,840
RF Switch: MiniCircuits RC-8SPDT-A18 + BKT-272-08+	MiniCircuits, www.minicircuits.com	1	\$2,625	\$2,625
NEMA4 Aluminum Enclosure with Panel	State Electric Supply Company	1	\$468	\$468

⁶ Including discounts, where available

⁷ Jointly purchased with COWMITS testbed, Army Research Office DURIP Award Number W911NF-14-1-0554

Table C.2. Auxiliary equipment.

Product	Source	#	Unit Price ⁸	Total Price
Intel NUC-i5 Mini PC	B&H	1	\$343	\$343
• Kingston 8 GB RAM	Technology Integration Group	2	\$30	\$60
• Samsung 950 Pro 256 GB SSD	Dell Marketing LP	1	\$86	\$86
Intel NUC-i7 Mini PC	CDW-G	2	\$584	\$584
• Crucial 32 GB RAM	B&H	2	\$114	\$228
• Samsung 950 Pro 256 GB SSD	B&H	2	\$190	\$380
Huawei B593s-22 4G LTE UE	Ebay, www.ebay.com	1	\$215	\$215
Huawei E8278s-602 4G LTE UE	Ebay, www.ebay.com	1	\$199	\$199
Sierra Wireless NETGEAR Aircard 330U LTE	www.amazon.com	1	\$95	\$95
LTE test SIM cards (CMW-Z04)	Rohde & Schwarz	2	\$135	\$270
Samsung 250 GB T3 Portable SSD	Amazon	5	\$104	\$520
RF and Network Cables and Accessories	Various			\$4,430
Indoor Omni Thru Ceiling Mount Antenna	Tessco Inc.	5	\$83	\$414
Directional Coupler: ZHDC-10-63-S+	MiniCircuits, www.minicircuits.com	3	\$85	\$255
Fixed Attenuators: BW-S10W2+	MiniCircuits, www.minicircuits.com	5	\$30	\$150
Fixed Attenuators: BW-S20W2+	MiniCircuits, www.minicircuits.com	6	\$30	\$180
Samsung 1TB 840 Evo-Series SATA III Internal SSD (hard drive)	Newegg.com	1	\$449	\$449
StarTech.com Mini HDMI to DVI-D Cable	WFCF/DALY Computers Inc.	1	\$9	\$9

⁸ Including discounts, where available

Appendix D: Publications

The testbed has enabled relevant research and the initial research results have been published in scholarly articles and presented at conferences of high prestige. The published or to be published papers are listed below; others are still under review.

Journal and Magazine Papers:

- M. Labib, V. Marojevic, J.H. Reed, A.I. Zaghloul, “Enhancing the robustness of LTE systems: analysis and evolution of the cell selection process,” *IEEE Commun. Mag.*, *accepted Aug. 2016, to be published*.
- M. Lichtman, R. Jover, M. Labib, R. Rao, V. Marojevic, J.H. Reed, “LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation,” *IEEE Commun. Mag.*, April 2016.

Peer Reviewed Conference Papers:

- M. Labib, V. Marojevic, J. Reed, A. Zaghloul, “How to enhance the immunity of LTE systems against RF spoofing,” *Proc. Int. Conf. on Computing, Networking and Communications (ICNC 2016)*, Kauai, Hawaii, 15-18 Feb. 2016.
- M. Labib, V. Marojevic, J. Reed, “Analyzing and enhancing the resilience of LTE/LTE-A,” *Proc. 1st IEEE Conf. Standards for Communications and Networking (CSCN)*, Tokyo, Japan, 28-30 Oct. 2015.