Software-Defined LTE Evolution Testbed Enabling Rapid Prototyping and Controlled Experimentation

Vuk Marojevic, Deven Chheda, Raghunandan M. Rao, Randall Nealy, Jung-Min (Jerry) Park, Jeffrey H. Reed
Wireless@Virginia Tech, Bradley Department of Electrical and Computer Engineering
Blacksburg, VA, USA
{maroje|devenjc|raghumr|rnealy|jungmin|reedjh}@vt.edu

***Abstract*—The long-term evolution (LTE) has spread around the globe for deploying 4G cellular networks for commercial use. These days, it is gaining interest for new applications where mobile broadband services can be of benefit to society. Whereas the basic concepts of LTE are well understood, its *long-term evolution* has just started. New areas of R&D look into operation in unlicensed and shared bands, where new versions of LTE need to coexist with other communication systems and radars. Virginia Tech has developed an LTE testbed with unique features to spur LTE research and education. This paper introduces Virginia Tech's LTE testbed, its main features and components, access and configuration mechanisms, and some of the research thrusts that it enables. It is unique in several aspects, including the extensive use of software-defined radio technology, the combination of industry-grade hardware and software-based systems, and the remote access feature for user-defined configurations of experiments and radio frequency paths.**

Keywords—LTE Evolution; Mission-critical communications; Software-defined radio (SDR); Spectrum sharing.

I. INTRODUCTION

A lot of R&D as well as standardization work has gone into the long-term evolution (LTE) since Release 8 of the 3rd Generation Partnership Project (3GPP) specifications was finalized in 2008. New potential avenues for LTE/LTE-Advanced (LTE-A) are public safety and mission-critical networks, IoT, industry 4.0, and many others. New modes of LTE have therefore been defined, including LTE-M or NB-LTE for supporting machine-type communications (MTC) and narrowband systems. On the other extreme, standardization is ongoing to further extend the LTE-A system throughput through use of massive carrier aggregation and advanced MIMO technology [1].

The limited spectrum that is available for cellular communications has motivated researchers, regulators, carriers and manufacturers to look at new spectrum and new ways of spectrum management. The unlicensed spectrum at 5 GHz is currently being considered for LTE, which will need to coexist with WiFi and different types of radars. Regulation has identified several bands for spectrum sharing, such as the new 3.5 GHz band and the AWS-3 band in the US. The Federal Communications Commission (FCC) has proposed a three-tier spectrum access model, where the incumbent users have highest priority to access the spectrum, followed by licensed secondary users, which are expected to deploy LTE networks, and unlicensed opportunistic users [2].

Frequency agility and the extensive use of software-defined radio (SDR) and cognitive radio (CR) technologies drive the evolution of LTE. LTE-Unlicensed is a spectrum-aware variant of LTE that will coexist with other systems in the 5 GHz band by regularly turning its transmission off. Different variants of LTE-Unlicensed have been proposed to adapt to the different regulations in different parts of the world [3]. Standardization of this and other new LTE technologies needs to go along with theoretical and experimental research and testing.

Testbeds play a major role while developing new technologies and systems. They allow rapid prototyping and testing of research results and provide a valuable experience to students when used in education. Whereas 4G/LTE service is now widely available, LTE research and education is far from reaching saturation. This research drives the evolution of 4G cellular technology into new spectrum spaces and use cases on the path towards 5G.

The motivation for this testbed is to enable research on LTE evolution and, in particular:

- Quick prototyping and testing of new protocol features,
- Controlled RF environment with real and customizable channel conditions,
- Implementation of other, co-existing communication waveforms, radars and interferers.

This paper briefly surveys the existing university testbeds that support LTE research and education (Section II) before presenting Virginia Tech's LTE testbed (Section III). Our testbed is unique in several aspects: We make extensive use of SDR technology, combine industry-grade instruments with commercial and free open-source software, provide remote as well as physical access to the entire testbed, and enable flexible, user-defined testbed configuration for supporting a variety of experiments in controlled and repeatable radio environments. The testbed's main components are a variety of LTE systems and over-the-air and emulated channel modes. We also provision for an experimental license, issued by the Federal Communications Commission (FCC), for over-the-air transmission in several frequency bands.

The testbed supports LTE research and education. We illustrate the testbed's capabilities through two use cases that

This is the author's version of the work. For citation purposes, the definitive Version of Record of this work is: V. Marojevic, D. Chheda, R. M. Rao, R. Nealy, J. M. Park and J. H. Reed, "Software-Defined LTE Evolution Testbed Enabling Rapid Prototyping and Controlled Experimentation," 2017 IEEE Wireless Communications and Networking Conference (WCNC), San Francisco, CA, 2017, pp. 1-6. doi: 10.1109/WCNC.2017.7925757

address current research needs (Section IV): LTE vulnerability analysis to targeted radio frequency (RF) interference [4]

TABLE I. UNIVERSITY LTE TESTBEDS

Testbed	Standards	No. of nodes	Frequencies/Channels	Main Characteristics
LTE/LTE-A Testbed, TU Dresden, Germany[1]	LTE Rel. 8	Up to 4 eNBs and 4 UEs	0.5 - 2.57, 2.62 - 2.69, 1.98-2, 2.17-2.19 GHz 20MHz bandwidth (BW)	Focused towards CR and PHY layer aspects of LTE and future 5G systems
UC4G wireless MIMO testbed, Heriott-Watt University, Edinburg UK[2]	LTE	2	10 MHz to 6.6 GHz BW: 50 MHz	Spatial modulation, MIMO LTE, channel emulation, channel measurement
CorteXlab, France[3]	WiFi, Zigbee, LTE, LTE-A	38 SDR nodes 42 wireless sensor nodes	Shielded room allows 300 MHz – 5 GHz 2x2 and 4x4 MIMO	Remotely accessible network of SDR nodes and wireless sensor networks for distributed CR experiments
ORBIT, Rutgers University, USA[4]	LTE , WiFi 802.11a/b/g/n/ ac, Bluetooth, ZigBee	20 x 20 grid plus outdoor network	100 MHz – 6000 MHz in increments greater than 125 MHz	Hardware acceleration for real-world PHY waveforms, hardware virtualization capable of supporting multiple radios on the same platform, open-source software toolkit
PhantomNet, University of Utah, USA[5]	LTE	32 UEs, 16 eNodeB units	LTE Band 4 Matrix with 128 distinct paths and 0 to -95 dB attenuation	Supports mobility and networking experiments, provides RF attenuation matrix for user devices, access points and SDR nodes for realistic RAN conditions and protocols
NITOS, University of Thessaly, Greece[6]	WiFi, WiMax, LTE	50 outdoor and 50 indoor	2.4 and 5 GHz	Supports multiple technologies in outdoor, RF isolated, and office indoor setups
Berlin LTE-A Testbed, Germany[7]	LTE, LTE-A	Two cells, two terminals	2.68 GHz, 2.53 GHz BW: 1, 2, 5, 10 MHz	Offers 2x2 MIMO OFDMA, MU-MIMO in downlink, and 1x2 SC-FDMA in uplink
LabView - based testbed, NYU Poly, USA[8]	LTE	2 base stations, 2 UEs w/ 2x2 MIMO	200 MHz to 4.4 GHz BW: up to 100 MHz	Supports open protocol stack to prototype PHY/MAC cross layer algorithms in a software defined networking (SDN) framework
Testbed for C-RAN Research, Campus Universitario de Santiago, Portugal[9]	LTE, C-RAN	2	70 MHz – 6 GHz BW: up to 56 MHz	Supports up to eight 20 MHz channels, 2x2 MIMO capabilities
Virtualized platform for testing LTE broadcast service, Universidad Politecnica de Madrid, Spain[10]	LTE	N/A	N/A	Supports analysis of multimedia services in a software based simulation environment
Testbed for evaluating LTE in High-Speed Trains, University of A Coruña, Spain[11]	LTE, LTE-A	2 portable nodes	700 – 1050 MHz, 2.4 and 5 GHz BW: 50 MHz	Portable self-contained testbed nodes, supports both TDD and FDD LTE
Testbed for coexistence of DVB-T and LTE systems, Brno University of Technology, Czech Republic[12]	LTE	1	791-821 MHz (Band 10) BW: 1.4, 3, 10 MHz	Supports coexistence of DVB-T and LTE systems
Wireless Network Virtualization, CONTENT Project, Multiple Universities[13]	LTE, Wi-Fi	50 WiFi nodes 2 LTE nodes	2.4 and 5 GHz	Supports end-to-end virtualization for network and infrastructure with heterogeneous, wireless and metro optical networks
Vienna MIMO Testbed, Vienna Institute of Technology, Austria[14]	LTE	3 outdoor nodes, 1 indoor receiver	2.503 GHz BW: 20 MHz 4 antennas on each node	Supports measurements with different antenna positions, interference alignment scenarios over 4x4 channel
MIMO Communications Testbed, University of Newcastle, Australia[15]	LTE	1	2.4-2.5 GHz BW: 40 MHz	Features interchangeable radio modules for different bands, support for 4x4 MIMO, interfacing with a MATLAB model of LTE

[1] M. Danneberg, R. Datta, A. Festag, G. Fettweis, "Experimental testbed for 5G cognitive radio access in 4G LTE cellular systems," *Proc. IEEE Sensor Array and Multichannel Signal Processing Workshop*, A Coruña, Jun. 2014.

[2] P. Chambers, et al., "The UC4G wireless MIMO testbed," *Proc. IEEE Global Telecom. Conf.*, Anaheim, CA, Dec. 2012.

[3] L. S. Cardoso, et al., "CorteXlab: an open FPGA-based facility for testing SDR & cognitive radio networks in a reproducible environment," *IEEE Conference on Computer Communications Workshops,* Toronto, ON, Apr.-May 2014.

[4] Open-Access Research Testbed for Next-Generation Wireless Networks (ORBIT) Homepage, http://www.orbit-lab.org/

[5] A. Banerjee, et al., "PhantomNet: research infrastructure for mobile networking, cloud computing and software-defined networking," *Proc. GetMobile*, vol. 19, no. 2, pp. 28–33, 2015.

[6] N. Makris, C. Zarafetas, S. Kechagias, T. Korakis, I. Seskar, and L. Tassiulas, "Enabling open access to LTE network components: the NITOS testbed paradigm," *Proc. IEEE Conf. Network Softwarization,* London, UK, Apr. 2015.

[7] T. Wirth, V. Venkatkumar, T. Haustein, E. Schulz, R. Halfmann, "LTE-Advanced relaying for outdoor range extension," *Proc. IEEE VTC 2009-Fall*, Anchorage, AK, 20-23 Sept. 2009.

[8] R. Gupta, et al., "LabVIEW based platform for prototyping dense LTE / WiFi networks in CROWD project," *Proc. European Conf. Networks and Communications,* Bologna, Italy, Jun. 2014.

[9] D. Riscado, et al., "A Flexible research testbed for C-RAN," *Proc. Euromicro Conf. Digital System Design*, Fuchas, Madeira, Aug. 2015.

[10] C. M. Lentisco, et al., "A virtualized platform for analyzing LTE broadcast services," *Proc. European Conf. Networks and Communications*, Paris, France, Jun.-Jul. 2015.

[11] J. Rodriguez-Pineiro, J. Garcia-Naya, A. Carro-Lagoa, L. Castedo, "A testbed for evaluating LTE in high-speed trains," *Proc. Euromicro Conference on Digital System Design*, Los Alamitos, CA, Sep. 2013.

[12] J. Kristel, L. Polak, and T. Kratochvil, "Co-Channel coexistence between DVB-T/H and LTE standards in a shared frequency band," *Proc. Conf. Radioelektronika*, Pardubice, Czech Republic, Apr. 2015.

[13] K. Katsalis, et al., "Wireless network virtualization: the CONTENT project approach," *Proc. Int. Workshop Computer Aided Modeling and Design of Comm. Links and Networks*, Athens, Greece, Dec. 2014.

[14] S. Caban, C. Mehlführer, R. Langwieser, A. L. Scholtz, M. Rupp, "Vienna MIMO testbed," *EURASIP J. Appl. Signal Processing*, Vol. 2006, pp. 1–13, 2006.

[15] D. Bates, S. Henriksen, B. Ninness, S. R. Weller, "A 4×4 FPGA-based wireless testbed for LTE applications," *Proc. IEEE PIMRC*, Cannes, France, Sept. 2008.

and channel back-off in shared spectrum. The paper concludes with an outlook on experimental LTE research that lies ahead (Section V).

II. University LTE Testbeds

Several universities and research centers have LTE testbeds. Each testbed supports a particular research thrust. Table I provides an incomprehensive list of popular university LTE testbeds. Whereas most of them are standalone installations in one location (Table I[2,3,4,5,8,12,15]) or spread across multiple sites[1,6,7,13,14], a few portable testbeds have been reported[11]. A large number of testbeds operate in the ISM bands[3,6,11,14,15] to simplify licensing and interoperability with other systems. Several testbeds deploy open-source software, such as Open Air Interface (OAI)[5,6] or GNU Radio[3,11], whereas others use custom routines, developed in LabView[2,8], MATLAB[2,9,15] or C/C++ to implement the LTE protocol stack or part of it. NS-3 network simulator is part of some setups[5,8]. Commercial handsets and USB dongles are commonly used for the user terminals. Only few testbeds are completely networked and fully remotely accessible and configurable[3,5]. The majority of testbeds use commercial-of-the-shelf (COTS) components rather than custom hardware and SDR software or industry-grade LTE test equipment.

III. Virginia Tech's LTE Testbed

A. Design Methodology

Wireless @ Virginia Tech built and manages the cognitive radio network (CORNET) testbed [6]. CORNET is a large-scale university testbed that supports research and education on SDR, CR and dynamic spectrum access since 2009. We decided to leverage our experience in testbed design, deployment, and operation to build an LTE testbed that would support our research and education on modern cellular communication technologies and systems. Our main design objectives were to (a) use software-defined radios, commercial and open-source software along with industry-grade instruments, (b) provide remote and physical access, (c) enable flexible and user-defined configurations and the integration of personal devices, and (d) allow for upgrades without redesign.

B. General Architecture and Capabilities

Figure 1 illustrates the main hardware components of our testbed. The testbed features several LTE systems that run as software on four desktops and one laptop. The CMW500 is an industry-grade communication system tester from Rohde & Schwarz. Two modes of operation are supported, cabled and over-the-air. RFnest (RF network channel emulation and simulation tool) is an RF channel emulator that provides a controlled radio environment. A shielded enclosure provides RF shielding. Users can bring their own equipment and conduct experiments in a research lab space, which creates a typical indoor radio environment (Fig. 1b).

Table II shows the main system capabilities of the testbed, which offers LTE implementations that are compliant with 3GPP Releases 8-12 as well as legacy WiFi systems for coexistence experiments. The hardware supports operation at frequencies up to 6 GHz. FCC experimental licenses cover several bands from 450 MHz to 3.65 GHz. Users can access the testbed remotely or physically, or a combination of both.

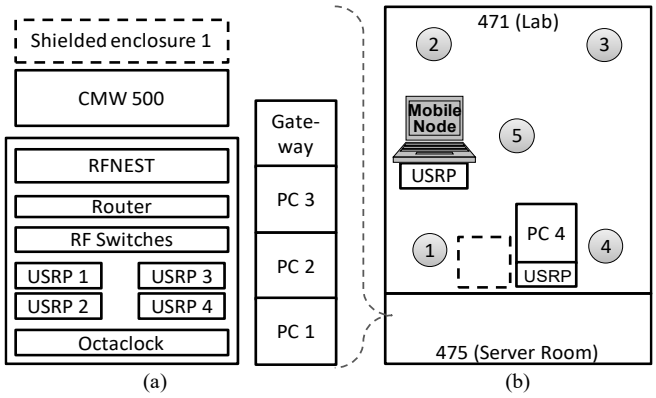

Fig. 1. Virginia Tech's LTE testbed: main components in server room (a) and antenna setup and testbed components in RF lab (b).

TABLE II. Testbed Features

Feature	Support
Standards	3GPP LTE Rel. 8-12 [a] IEEE 802.11a/g/n (CMW500)
Frequencies	Hardware supports up to 6 GHz Lab antennas: 698-960, 1710-2700, 2700-3200 MHz
Licenses	FCC experimental license, several bands in 450–3650 MHz range (FCC Call Sign WH2XLE)
Channels	Channel emulation through cabled mode (RFnest) and over-the-air transmission with or w/o shielded enclosure
Synchroni-zation	Eight 10 MHz and eight pulse per second (PPS) reference signals (Octoclock)
Access	Remote and physical

[a.] Hardware, commercial software, and free open-source software.

TABLE III. LTE System Options

	Product	Characteristic
eNB	Rohde & Schwarz CMW500	Industry-grade UE test system and eNodeB emulator
	Amarisoft LTE100 (PC1, PC4, mobile node)	Commercial software, 3GPP Rel. 12 compliant [a]
	srsLTE (PC2, PC3)	Free open-source software [a]
	libLTE (mobile node)	Free open-source software [a]
	Eurecom Open Air Interface (PC2, PC3)	Free open-source software [a]
UE	USB dongles, multiple vendors	FD-LTE bands 1, 3, 4, 5, 7, 8, 9, 17; TD-LTE band 38
	Huawei B593	FD-LTE bands 1, 5, 7,8, 9; TD-LTE band 38
	srsUE (PC2, PC3)	Free open-source software [a]
	libLTE (mobile node)	Free open-source software [a]

[a] Interfaces with COTS SDR front ends, user-defined UL/DL frequency.

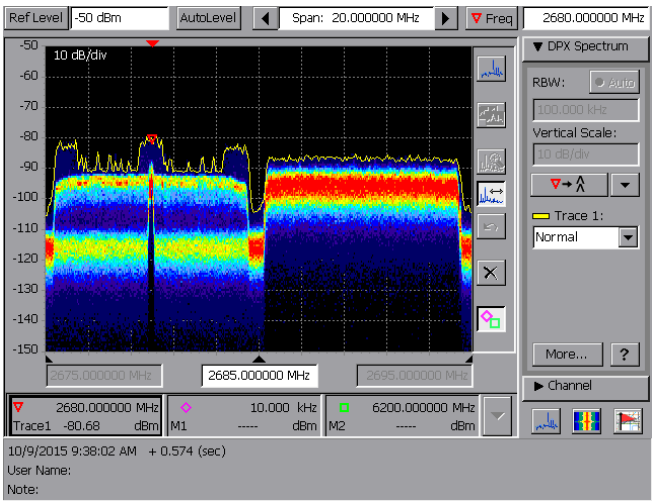

Fig. 2. Spectra of two adjacent 10 MHz LTE cells. The left band shows a TD-LTE signal spectrum (LTE100 eNB); the power level histogram shows peaks at -95 and around -117 dBm because of the different received power levels of the UL and DL signals with the SDR's local oscillator leakage at the carrier frequency at 2680 MHz. The right band shows a clean FD-LTE DL signal spectrum (CMW500 eNB) with full resource allocation.

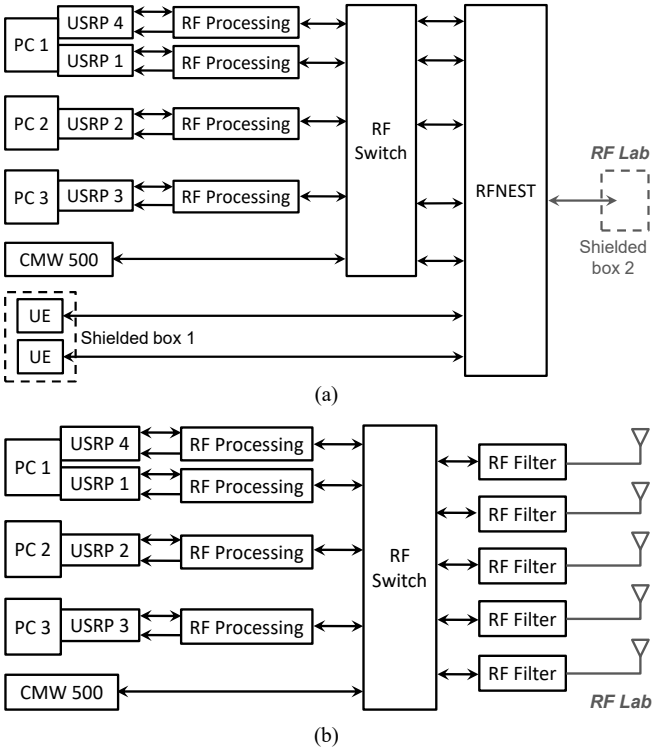

Fig. 3. RF functional diagrams for the channel emulation (a) and over-the-air (b) modes.

C. LTE Systems

The radio access network (RAN) and the core network (CN) define a cellular communication network. The RAN manages the radio resources, initiates handovers and schedules UL and DL resources, among others. The CN is responsible for mobility management, user authentication, charging, security control and so forth and provides access to external networks.

An LTE base station, or evolved NodeB (eNB), is part of the evolved universal terrestrial RAN (eUTRAN) and provides the network access point for user equipment (UE). The evolved packet core (EPC) is the LTE CN. Our testbed features several eNBs, which integrate a simplified EPC.

Table III summarizes our LTE system components. Our CMW500 takes the role of an UE system monitor and eNB emulator, but can also act as a spectrum analyzer. It supports both UL/DL duplexing modes, that is, time division duplex and frequency division duplex, or FD-LTE and TD-LTE. The current support is for Rel. 8/9, but upgrades are possible. The Amarisoft LTE100 is a fully software-defined eNB that is compliant with 3GPP Rel. 12. The open-source alternatives srsLTE, libLTE, and OAI implement part of the LTE protocol stack. All four software libraries compile and run on different PCs that interface with the N210 or B210 Universal Software Radio Peripherals (USRPs) from Ettus Research [7].

LTE100 is installed on PC1, PC4 and the mobile node (laptop), srs_eNB and OAI run on PC2 and PC3, whereas libLTE is installed on the mobile node. The Ubuntu 14.04 operating system runs on PC1, PC2, PC3 and the mobile node, whereas Fedora 20 runs on PC4.

The testbed features several UEs in different form factors. USB dongles are accessed from PCs for control and monitoring. The Huawei router is accessed via Ethernet or WiFi and can be configured or monitored through a browser. srsUE is an SDR UE, which runs on a PC and interfaces a USRP. It allows making modifications to the UE processing and signaling for system evolution or monitoring. The libLTE software library implements the UE PHY layer processing on the mobile node.

Fig. 2 shows the signal spectra of two adjacent LTE cells generated with the LTE100 SDR system (left) and the CMW500 (right). Note the differences in the spectra because of the different implementations and resource scheduling.

D. Channels

Fig. 3 shows two configurations of the testbed, the cabled mode using the channel emulator (Fig. 3a) and the over-the-air mode using antennas (Fig. 3b). The RF processing includes couplers and attenuators to combine the two USRP ports and provide 10 dB of attenuation to the transmitted signal. (The deployed N210 USRP with the SBX daughterboard can source 100 mW.) An additional 10 dB attenuator is provided at the RFnest port to limit the maximum signal power to approximately 0 dBm.

RFnest from Intelligent Automation, Inc. allows generating realistic wireless channel effects. The A208 model supports the integration of up to eight real radios in addition to virtual radios [8]. The hardware carries out the digitization of the incoming RF signals and applies selected channel effects digitally, before converting the resulting signals back to the analog domain in real-time for all connected radios. RFview is a graphical user interface that provides time-synchronized, geospatial displays and allows for scenario modeling, analysis, recording and replay with several built-in channel models.

The RF filters are separate blocks and are used in the over-the-air mode to remove the harmonics that are not filtered by the USRPs. The five antennas are ceiling-

mounted antennas that are deployed in the RF lab as illustrated in Fig. 1b.

The two UEs shown in Fig. 3a have external RF connectors and are connected through RF cables. The shielded box is necessary because UEs and USRPs are not well shielded and direct radiation from the circuit boards would bypass the intended RF signal path through RFnest. In a system like this it is critical to have at least 90 dB of isolation.

E. Networking and User Interface

All testbed components, including RF switches, are networked through Ethernet and can be remotely accessed and configured. The Gateway server provides user authentication and remote access over the Internet. A user who possesses a valid certificate can access the testbed through OpenVPN and then has full control over it and can configure and execute experiments, as illustrated in Fig. 4.

IV. Enabled Research

The reason for building the presented testbed was to support LTE education and research with emphasis on topics of interest to academia, regulators and industry. This section presents two case studies where the testbed provided a useful asset for demonstration purposes or for advancing the state of the art in these research thrusts described in continuation.

A. LTE for Mission-Critical Networks

Security in wireless networks has been of huge interest for across all generations and 4G is not an exception. LTE has been proposed for next generation public safety networks as well as for military communications. LTE is an open standard and all documentation is publicly available. With today's technology and tools, one can easily leverage this to target the weak spots of LTE to disrupt its effective operation.

We carried out other experiments to assess the impact of protocol-aware RF jamming on LTE/LTE-A systems and proposed several improvements to the protocol. Fig. 5 shows one of our experiment setups using a combination of fixed and mobile testbed nodes. The open-source LTE software toolbox srsLTE allows creating custom interference or RF spoofing signals as shown in the top right of Fig. 5. Due to space limitations we refer the interested reader to [4], [5].

B. LTE Evolution into Shared and Unlicensed Spectrum

Facing the need for a 1000× improvement in wireless capacity by 2020, the wireless research community is exploring new architectures, technologies, and frequency bands. LTE will soon operate in new bands and, most likely, in the 5 GHz unlicensed spectrum. One approach is setting up a secondary cell in the unlicensed spectrum through carrier aggregation [3]. The most common technology is the Licensed Assisted Access (LAA), which has been standardized by the 3GPP in Rel. 13. LTE is also considered for deployment in shared bands, such as the 3.5 GHz and the AWS-3 bands in the US.

The main challenge of operating LTE in unlicensed and shared spectrum is to enable co-existence with legacy systems. In shared spectrum, LTE will be the secondary user system and will need to back off whenever the primary or incumbent user transmits. 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. We propose using handover as a mechanism for the secondary users to vacate to another

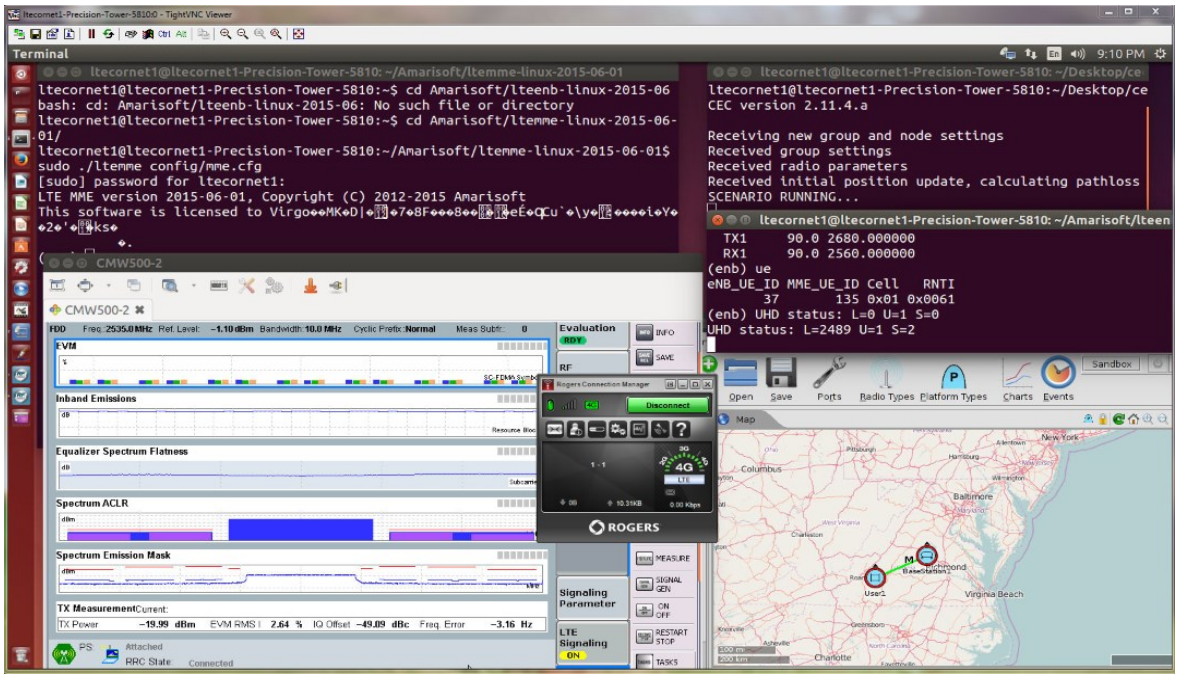

Fig. 4. Remote desktop snapshot showing an experiment with two FD-LTE cells in Band 7, 25 MHz spaced apart, and generated by the CMW500 (bottom left) and LTE100 (top). The Rogers UE (middle) is a USB dongle that is attached to the LTE100 eNB, whereas the Huawei router (not shown) is attached to the CMW500 eNB. The USB dongle communicates over-the-air within the shielded box, whereas the router is fully cabled.

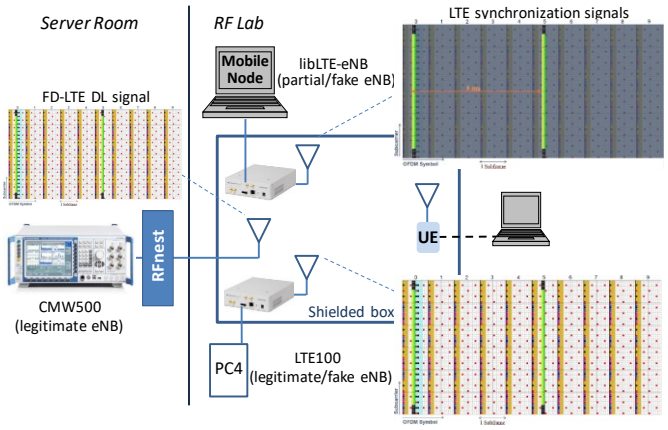

Fig. 5. Experiment setup for the LTE vulnerability analyses of [4] [5].

band whenever a primary user (PU) transmits. Here we discuss two mechanisms that we tested for multi-cell handovers using two (primary) cells at different center frequencies:

1. Gradually lower the power of the interfering cell upon detection of a PU to hand the user over to another cell without disrupting the active session.
2. Force the user to move out of the interfering cell by turning the interfering cell off upon detection of the presence of the PUs.

We performed experiments on forced handovers, using PC1 and USRP4. LTE100 was used to setup 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). Fig. 6 shows the stages of forcing a user out of the interfering cell, which in this case is cell 0x01. These initial experiments have shown that 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. 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.

As opposed to parallel cell deployments, we can rapidly deploy a new cell in a different band when needed and force all users to switch to that cell. Instead of using two primary cells, we can use one primary cell and one or more secondary cells with the carrier aggregation feature of LTE-A, which is supported by the LTE100 eNB.

V. Conclusions

3GPP Rel. 13 has just been finalized. This is the 6th release on LTE. LTE-A now offers even more flexibilities and new features for embracing fairly different communications contexts, from high-bandwidth streams to low-powered IoT and device-to-device communications.

Virginia Tech's LTE testbed provides a flexible architecture with a variety of tools and knobs to leverage experimental LTE research and education and pave the path to 5G. The testbed is remotely accessible and remotely configurable and combines open-source with commercial software and industry-grade test instruments.

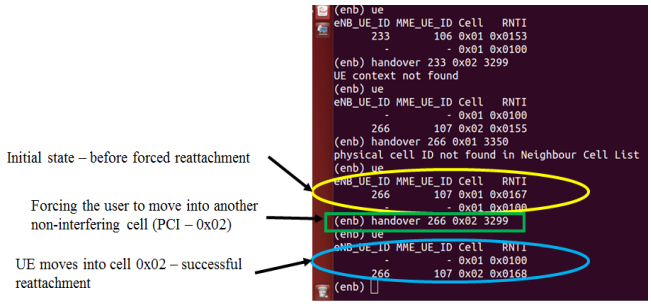

Fig. 6. Snapshot showing the stages of forced handover with the forced handover feature of LTE100.

Research that has been conducted with this testbed includes analysis of LTE for mission-critical systems. Based on our results [4], [5], we proposed improvements to the 3GPP LTE/LTE-A specifications that are backward compatible and provide important protection mechanisms against denial-of-service attacks [9]. We have leveraged these results to design new waveforms for 5G [10]. Our current research focuses on solutions for License Assisted Access (LAA) and other variants of LTE-Unlicensed and coexistence in shared bands. The testbed has been built to support LTE evolution research in a controlled environment; it allows researchers to customize experiments and the testbed for their needs.

Acknowledgements

This research has been supported in part by National Science Foundation grant #1642873, the Army Research Office DURIP grants W911NF-14-1-0553/0554, and the Office of the Secretary of Defense.

References

[1] J. Lee, Y. Kim, Y. Kwak, J. Zhang, A. Papasakellariou, T. Novlan, C. Sun, Y. Lin, "LTE-advanced in 3GPP Rel-13/14: an evolution toward 5G," *IEEE Commun. Mag.*, Vol. 4, Iss. 3, pp. 36-42, March 2016.

[2] M. M. Sohul, M. Yao, T. Yang, J. H. Reed, "Spectrum access system for the citizen broadband radio service," *IEEE Commun. Mag.*, Vol. 53, Iss. 7, pp. 18-25, July 2015.

[3] R. Zhang, et al., "LTE-unlicensed: the future of spectrum aggregation for cellular networks," *IEEE Wireless Communications*, Vol. 22, No. 3, pp. 150-159, June 2015.

[4] M. Lichtman, R. P. Jover, M. Labib, R. M. Rao, V. Marojevic, J. H. Reed, "LTE/LTE-A jamming, spoofing and sniffing: threat assesment and mitigation," *IEEE Commun. Mag.*, Vol.54, No.4, pp. 2-9, Apr. 2016.

[5] M. Labib, V. Marojevic, J.H. Reed, "Analyzing and enhancing the resilience of LTE/LTE-A," *Proc. IEEE Conf. Standards Communications & Networking (CSCN)*, Tokyo, Japan, Oct. 2015.

[6] T. Newman, S.M.S. Hasan, D. Depoy, T.Bose, J.H. Reed, "Designing and deploying a building-wide cognitive radio network testbed," *IEEE Commun. Mag.*, Vol. 48, Iss. 9, Sept. 2010.

[7] Ettus Research Homepage, http://www.ettus.com/

[8] Intelligent Automation, Inc., RFnest data sheet, 2013.

[9] 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.*, Vol. 55, Iss. 2, Feb. 2017.

[10] J. Reed, V. Marojevic, M. Carrick – Virginia Tech, "Method for jointly adapting an OFDM waveform and the demodulator for interference mitigation and harsh channels," Int. Patent Application No: PCT/US2016/026509, File Date: Apr. 07, 2016.