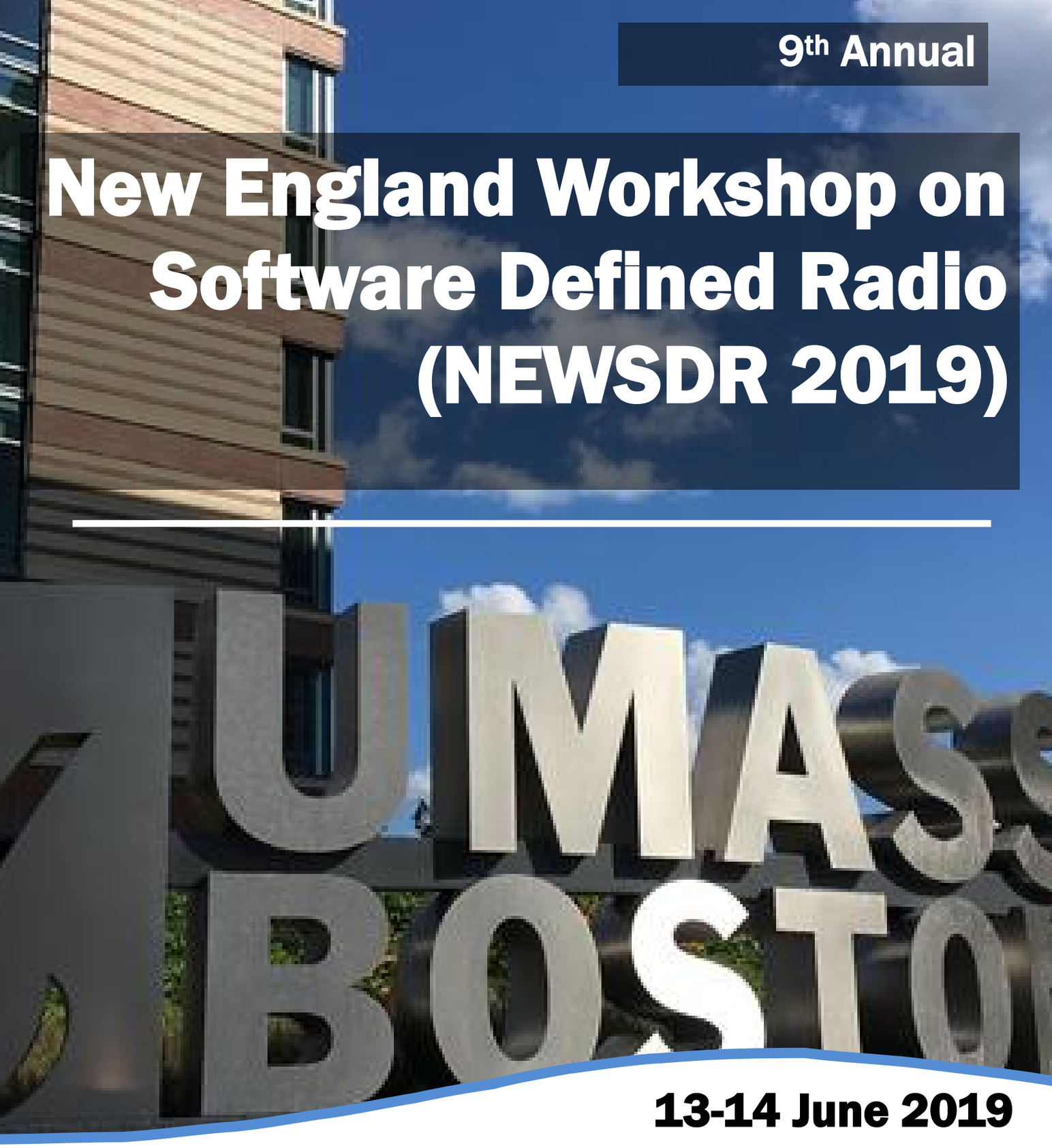

9th Annual

New England Workshop on Software Defined Radio (NEWSDR 2019)

13-14 June 2019

University of Massachusetts Boston | Boston, Mass

Sponsored By:

MathWorks · National Instruments · Ettus Research™ A National Instruments Company · MediaTek · Analog Devices · UMass Boston College of Science and Mathematics, University of Massachusetts Boston · SDR-Boston Boston SDR User Group

#NEWSDR

Welcome

ORGANIZING COMMITTEE

Michael Hirsch
Boston University

Yousof Naderi
Northeastern University

Neel Pandeya
Ettus Research

Michael Rahaim
UMass Boston

Alex Wyglinski
Worcester Polytechnic Institute

The 2019 New England Workshop on Software Defined Radio (NEWSDR) is the ninth installment of an annual series of workshops organized by the Boston SDR User Group (SDR-Boston). This year, we are very excited about having the University of Massachusetts Boston generously serve as the host institution for NEWSDR 2019!

The goal of this series of workshops is to provide a forum through which individuals working on SDR-related projects in the New England area can get together in order to collaborate and introduce SDR concepts to those interested in furthering their knowledge of SDR capabilities and available resources.

Following on the success of these workshops, this year's NEWSDR event offers a chance for presenting the latest developments in SDR and Cognitive Radio research by individuals from academia, industry, and government in the New England area, as well as from across the Nation. In addition to providing an opportunity for researchers in this area to network and interact on issues relating to SDR and Cognitive Radios, NEWSDR 2019 will include:

- Invited Presentations on the latest in SDR
- Poster Presentations with Short "Elevator-Pitch" Oral Presentations
- Technology demonstrations
- Hands-On Tutorials
- Breakfast / coffee / lunch included with advanced registration

During this event, we would like to encourage all of you to engage in conversation with your fellow attendees, exchange ideas, and talk about your latest findings with respect to SDR. We hope that you will find NEWSDR 2019 a productive event to expand your knowledge and horizons regarding SDR technology, and we would like to wish you a very positive and rewarding workshop!

Agenda – Thursday 13 June 2019

4:00PM-5:00PM	Pizza/Soda & Attendee Networking
5:00PM-6:00PM	Early Session for Setup
6:00PM-9:00PM	Short Course 1: Analog Devices “Intro to the AD9361 via the PLUTO SDR, Linux’s IIO, and Open-Source Toolchains“
6:00PM-9:00PM	Short Course 2: National Instruments/Ettus Research “FPGA Programming on the USRP with the RFNoC Framework“

Agenda – Friday 14 June 2019

8:30AM-8:45AM	Welcome and Introduction
8:45AM-10:00AM	Sponsor Overview Presentations (20 minutes each, 4 sponsors)
10:00AM-10:30AM	Poster Presenter Elevator Pitches/Oral Presentations (2 minutes each)
10:30AM-11:00AM	Coffee, Attendee Networking, Poster Sessions, Sponsor Exhibits and Demos
11:00AM-11:45AM	Technical Presentation 1: Mathworks “Modulation Classification with Deep Learning“
11:45AM-1:00PM	Lunch, Attendee Networking, Poster Sessions, Sponsor Exhibits/Demos
1:00PM-2:00PM	Invited Presentation 1: Professor Pau Closas (Northeastern University) “Software Defined Radio for Positioning, Navigation, and Timing“
2:00PM-2:45PM	Technical Presentation 2: MediaTek “5G NR-U – ‘Houston, we have a problem here’“
2:45PM-3:15PM	Coffee, Attendee Networking, Poster Sessions, Sponsor Exhibits and Demos
3:15PM-4:15PM	Invited Presentation 2: Professor Vuk Marojevic (Mississippi State University) “4G/5G Radio Access Security Analysis using Software Radios“
4:15PM-4:30PM	Poster Award Announcements
4:30PM-4:45PM	Closing Remarks

Invited Presentations

Software Defined Radio for Positioning, Navigation, and Timing

Professor Pau Closas (Northeastern University)

Global Navigation Satellite Systems (GNSS) is the technology of choice for most position-related applications, when it is available. A GNSS receiver relies on a constellation of satellites to estimate a set of range measures from which to compute its position. These distances are calculated estimating the propagation time that transmitted signals take from each satellite to the receiver. The term GNSS encompasses GPS, Galileo, GLONASS, or Beidou systems among others. The main challenges of GNSS technology arise when operating in complex environments which are either naturally impaired by multipath, shadowing, high dynamics, or ionospheric scintillation; or intentionally/unintentionally interfered. Ushered by an ever increasing demand for availability, accuracy, and reliability, the mitigation of these challenges has steered intense research on advanced receiver design. Remarkably, the progress in this area is tightly coupled with the increased adoption of the software defined radio (SDR) paradigm within the GNSS community, which allowed for faster transitioning from algorithmic development to real-world testing. This talk will provide a brief introduction to GNSS technology, with focus on the signal processing challenges of receiver design, as well as a discussion of sample research projects where the use of SDR is at the core. The talk will touch upon the GNSS-SDR project (gnss-sdr.org), a free and open source software implementing an end-to-end GNSS receiver. GNSS-SDR has been used in a multitude of projects, some of which will be discussed in this talk, such as the possibility to transform a TV dongle into a GNSS receiver, or localizing and mitigating inferring signals. The main goal of this talk is to highlight the importance of SDR – and its continuous evolution – to boost research activities and, in particular, in the field of satellite-based navigation.

Biography: Pau Closas received his MS and PhD degrees in electrical engineering from the Universitat Politècnica de Catalunya (UPC), Barcelona, Spain, in 2003 and 2009, respectively, as well as a MS in Advanced Mathematics from UPC in 2014. He is an Assistant Professor in the Electrical and Computer Engineering Department at Northeastern University, Boston, Massachusetts. His primary areas of interest include statistical signal processing, stochastic filtering, and robust statistics with applications to positioning systems, wireless communications, and mathematical biology. Among other distinctions, he is the recipient of the NSF CAREER Award, the 2014 EURASIP Best PhD Thesis Award, the Ninth Duran Farell Award for Technology Research, and the 2016 ION Early Achievements Award in recognition to his contributions to navigation systems and signal processing fields. He has served in the organization of flagship IEEE conferences and journals.

4G/5G Radio Access Security Analysis using Software Radios

Professor Vuk Marojevic (Mississippi State University)

4G/5G security is an emerging problem that can potentially affect us in the next 2-3 years, especially with IoT, V2V, UAV and other applications of advanced wireless technology emerging. Public safety and mission critical networks can largely benefit from commercial 4G/5G technologies and network deployments and their evolution. To understand the vulnerabilities of these networks, we built a software radio-based testbed that models 4G environments and developed a series of different cyber attacks to compromise the 4G radio access network. Motivated by the fact that mobile networks highly rely on control channel signaling, we challenged the system performance and availability by attacking individual LTE control channels and signals. Moreover, since user equipment (UEs) implicitly trust networks before the mutual authentication handshake is completed, we tested the effect that fake base stations and fake signaling, which we coined control channel spoofing, have on the behavior UEs. By running numerous tests in controlled radio environments with standard compliant and mission critical LTE networks and commercial UEs we found that a number of radio frequency attacks can cause serious damage to the network performance and availability. One of the simplest, yet most severe attacks that can cause denial of service is to transmit the LTE synchronization signals asynchronously to those of legitimate networks. Fortunately, there is a simple solution to this threat that all LTE UEs face. It consists of the UE correlating received signals, messages and authentication results. An important lesson learned is that standards need to consider operational edge cases for which simple solutions may exist, such as the one that we proposed to mitigate denial of service attacks from control channel spoofing.

Biography: Vuk Marojevic is an associate professor of electrical and computer engineering at Mississippi State University. He graduated from the University of Hannover (M.S.), Germany, and Barcelona Tech-UPC (Ph.D.), both in electrical engineering. Prior to joining Mississippi State, he was with Wireless@Virginia Tech, where he developed various cognitive radio and LTE testbeds and conducted several wireless protocol measurement campaigns. He led Virginia Tech's LTE vulnerability analysis research and proposed several ways to harden LTE. His pioneering work on LTE control channel spoofing was picked up by industry and made it into 3GPP Release 13. His research interests are in software-defined radio, spectrum sharing, 4G/5G cellular technology, wireless network security, and resource management with application to mission-critical networks and unmanned aircraft systems.

Short Courses & Technical Presentations

Intro to the AD9361 via the PLUTO SDR, Linux's IIO, and Open-Source Toolchains

Robin Getz (Analog Devices)

This workshop will provide a thorough and practical introduction to the AD9361, the ADALM-PLUTO SDR, and other IIO based hardware and the open-source software toolchain (IIO utils and IIO-Scope). We will examine the hardware and architecture of the PLUTO software-defined radio in addition to discussing topics such as how to get started using a new PLUTOSDR device, how to install and configure the open-source software toolchain, programming the PLUTO using the libIIO API from Python, C or C++, and other tools using PLUTO SDR. Other hardware capable of running the IIO framework will be discussed, such as the Ettus E310, the Epiq SideKiq Z2, and Analog Device's RF SOM. Several exercises will be performed on the ADALM-PLUTO SDR, such as implementing an FM transmitter and receiver. Various demonstrations of other wireless systems will be shown. Several open-source tools will be discussed, such as SDRangle, GQRX, Fosphor, Inspectrum, and several Out-of-Tree (OOT) modules. For those interested in MATLAB or Simulink the Pluto Hardware support package will be shown. Attendees should come away with a solid foundation and practical understanding of how to configure, program, and use the Pluto SDR and other IIO based hardware to implement a wide range of wireless systems.

FPGA Programming on the USRP with the RFNoC Framework

Neel Pandeya (Ettus Research)

The RFNoC (RF Network-on-Chip) software framework from Ettus Research is meant to decrease the development time for experienced FPGA engineers seeking to integrate IP into the USRP signal processing chain. RFNoC is the architecture for USRP devices that use Xilinx 7-series FPGAs (E310, E312, E320, X300, X310, N310, N320). RFNoC is built around a packetized network infrastructure in the FPGA that handles the transport of control and sample data between the host CPU and the radio. Users target their custom algorithms to the FPGA in the form of Computation Engines (CE), which are processing blocks that attach to this network. CEs act as independent nodes on the network that can receive and transmit data to any other node (e.g., another CE, the radio block, or the host CPU). Users can create modular, FPGA-accelerated SDR applications by chaining CEs into a flow graph. RFNoC is supported in UHD and GNU Radio. In this workshop, we will present an interactive hands-on tutorial on RFNoC, including a discussion on its design and capabilities, demonstrations of several existing examples, and a walk-through on implementing a user-defined CE and integrating the CE into both UHD and GNU Radio.

Modulation Classification with Deep Learning

Ethem Sozer (Mathworks)

Modulation classification is an important part of applications such as operator regulation, communications anti-jamming, user identification and cognitive radio. You can use deep learning algorithms to classify channel impaired signals. This example shows how to train a deep learning algorithm with synthetically generated channel-impaired waveforms for modulation classification. The example also uses two ADALM-PLUTO radios to test the trained network with real world signals.

5G NR-U – 'Houston, we have a problem here'

Timothy Fisher-Jeffes (MediaTek)

3GPP is in the throes of finalizing R16 of their standards, which for the first time will include NR-U, that is 5G in the unlicensed 5GHz band. At this same time, regulatory bodies around the world are actively opening up debate for extending unlicensed access into spectrum above 6GHz, notably as much as 1.2GHz starting at 5.9GHz. The economic importance of this additional spectrum cannot be understated. It does, however, also have some concerning pitfalls, that if not addressed, will result in inefficient use of this valuable resource. We show here theoretical analysis of the 5GHz ETSI regulations as written today with some surprising findings regarding coexistence. The hope is to navigate the regulatory and standardization process to ensure the same mistakes are not made in 6GHz.

Poster Presentations

Adversary UAV Localization with Software Defined Radio

Ian Gelman (WPI), Abdul Hassan, John Loftus, Brian Mahan

Unmanned Aerial Vehicles continue to pose an immediate threat to personal privacy and national security. In an effort to detect and mitigate the threat of unwanted drones, our team designed a RSS-based 3D localization system using software-defined radio. This paper focused on localization of hobbyist drones by detecting the video streaming waveform transmitted by the drone, and measuring its received signal strength. The system's architecture consists of five Ettus software defined radio recievers, and processing of raw samples was performed in GNURadio. Additionally, channel modeling was performed in order to determine the mapping function which relates received signal strength to the 1-dimensional distance from each software-defined radio. Recursive least squares adaptive filtering was used to numerically estimate the drone's 3D position. The precision and accuracy of the system was quantified by distance measurement error and validated against the Cramer-Rao lower bound for an unbiased estimator.

Comparison of Coherent and Noncoherent Receivers for IEEE 802.15.4 OQPSK Modulation Based on SDR Platforms

Evan Faulkner (UConn), Shengli Zhou, Song Han

Since the IEEE 802.15.4 standard was defined in 2003, the performance of microcontroller technology has improved drastically while cost has come down significantly. As a result, wireless communication systems implemented on modern hardware may be capable of performing more complex tasks than those specified in the standard. The accessibility of software defined radio (SDR) technology makes it feasible to investigate the implementation of more complex receiver designs so that we may evaluate the performance of the physical layer with several improvements over the original. In this research, we have worked to implement several improvements on the 2.4GHz OQPSK physical layer design given in the IEEE 802.15.4 standard. The implementation of coherent decoding along with equalization of varying complexity at the receiver results in theoretical improvement in packet delivery ratio to SNR of several dB, and comparable real-world improvements were verified by SDR implementation. Following the conclusion of this investigation, GNU radio blocks for this improved receiver will be developed and released for use by other SDR researchers.

Scientific Measurements of Near-Earth Space: Effective RF Data Strategies Using Software-Defined Radio Architectures

John Swoboda (MIT Haystack Laboratory), Frank D. Lind, Philip J. Erickson, William Rideout, Ryan Volz, Juha Vierinen

Since the 1990s, MIT Haystack Observatory has leveraged software-defined radio architectures for scientific measurements of near-Earth space. Effective execution of these scientific measurements requires precision measurements of very weak received signals that are in some cases at or below the thermal noise floor, along with effective and complete metadata recording in order to provide proper interpretation and extraction of physical information contained in the signals. In some cases, analysis of these signals along with their metadata may take place years or even decades after their collection, requiring long-term stable knowledge of their characteristics. To achieve these scientific goals, it is useful to have a common software toolkit efficiently implementing quick, time-tagged access to RF voltage–level data with accompanying metadata. MIT Haystack has created an open source product, Digital RF, that addresses these needs. Digital RF allows for the recording and storage of RF voltage data with O(1) retrieval speed. With a companion Digital Metadata format and applications program interface (API), use of this highly configurable software stack considerably speeds the software development process for radio science applications.

Visible Light Communication System and Open Source GNU Radio Toolkit

Jason Nguyen (University of Massachusetts Boston)

We present an internet-connected Visible Light Communication (VLC) system as well as an open-source library that integrates with GNURadio (a signal processing toolkit that is widely used in communication) in order to assist researchers who are new to the field. The VLC system utilizes LED and photosensor for downlink and Wi-Fi connection for uplink. Signal processing, network routing and LED characterization will be aspects of the project. The open-source library includes modulators, demodulators and model channels functioning as blocks that we have integrated with the GNU Radio library. Students and engineers can use our open-source library

for simulation of their optical system or for physical system deployment with software-defined radio hardware.

A Compact Design on FPGA SDR Platform with the Same RF Front End

Suranga Handagala (Northeastern University), Jieming Xu, Mohamed Mohamed, Miriam Leeser, Marvin Onabajo

Field Programmable Gate Arrays (FPGAs) are widely used in wireless networking transceivers, however they typically are designed to process one specific wireless protocol at a time. We present an FPGA design that can receive either Wi-Fi or LTE signals by determining which signal is being received, and then applying the appropriate processing. We use the 5 GHz ISM band for both protocols, and demonstrate our method by performing over the air experiments that involve receiving signals using a software configurable radio front end, and performing subsequent processing such as signal detection, synchronization, demodulation and channel estimation etc. using an FPGA in real time. Our goal is to accommodate multiple wireless protocols within the same software-defined radio by efficiently utilizing available resources on the device.

Development of a PAWS (protocol to access white spaces) compliant GNU Radio Block

Hector Reyes-Moncayo (Universidad de los Llanos-Villavicencio-Colombia)

The purpose of this poster is to present the development of a GNU Radio block that is compliant with the protocol PAWS (Protocol to access white spaces). PAWS allows white-space devices to query databases about available spectrum. PAWS is specified by the IETF (Internet Engineering Task Force) through the RFC 6953 y RFC 7545. The block connect a master device with a white space database server to obtain information about the availability of specific portions of the spectrum at specific locations and time slots. The block also connects a slave device with a master device. Through the public Internet or a private IP network, the master device queries the database server on behalf of its associated slave devices to get spectrum availability information, which includes frequency, maximum power allowed, operative schedule, and other parameters. The block can be integrated into GNU Rradio flow graphs along with off the shelf blocks to implement TVWS SDR radios.

Tracking Anonymized Bluetooth Devices

Johannes Becker (Boston University), David Li, David Starobinski

Numerous mobile and wearable devices support communication using the Bluetooth Low Energy (BLE) protocol. BLE devices frequently broadcast on public (non-encrypted) advertising channels to announce their presence to other devices. To prevent tracking on these public channels, devices may use a periodically changing, randomized address instead of their static (permanent) Media Access Control (MAC) address. Thus, many state-of-the-art devices, such as Windows 10 computers and macOS and iOS devices implement address randomization for BLE advertising. We demonstrate that in several instances these address randomization schemes can be circumvented. Specifically, using a software-defined radio, we show that passive adversaries can extract “identifying tokens” from advertising payloads and use them as secondary identifiers. We present an on-line algorithm that updates these identifying tokens in real time to successfully track popular types of devices over longer time periods than their address randomization cycles (sometimes indefinitely longer). We further identify an attack that captures the static MAC address of a device by passively observing interactions between the device and an accessory (i.e., a pen). This attack allows for permanent device tracking. Finally, we propose countermeasures against the presented algorithm and other privacy flaws in BLE advertising.

Dynamic FOV receiver for VLC indoor dense networks

Iman Abdalla (Boston University), Michael Rahaim, Thomas D.C. Little

We propose a dynamic field of view (D-FOV) receiver in a dense network of overhead optical access points. We then show how the FOV of a Visible Light Communications (VLC) receiver can be manipulated to achieve the best Signal to Noise Ratio (SNR) while supporting device mobility and optimal access point (AP) selection. The D-FOV technique is evaluated through modeling, analysis, and experimentation in an indoor environment comprised of 15 VLC access points (APs). The receiver is connected to an N210 USRP attached to a computer running Gnu Radio software and is automated to collect measured data. Each luminiare is using one of 15 USRP channels with a unique frequency, each luminiaire converts electrical power to optical, then optical power is converted to electrical at the receiver. Finally, we calculate the electrical power corresponding to each received sinusoid through an FFT operation using the USRP/Gnuradio framework. Results of this work

indicate the efficacy of the approach including a 3X increase in predicted SNR over static FOV approaches based on measured Received Signal Strength (RSS) in the testbed.

Localization with the PlutoSDR

Lauren Getz (WPI), William Schwartz, Katherine Smith

Implementation of a system which localizes indoor sub-1GHz transmission signals, and provides a low cost and effective alternative to traditional signal sensing and localization. The system uses a pre-existing Wi-Fi network, PlutoSDRs and a server to visualize the estimated origins of the transmitted signals. The results of the system were accurate and precise enough to comply with the goals and standards established.

Wireless Attacks on Aircraft Instrument Landing Systems

Harshad Sathaye (Northeastern University), Domien Schepers, Aanjhan Ranganathan, and Guevara Noubir

Modern aircraft heavily rely on several wireless technologies for communications, control, and navigation. Despite the criticality and the increasing availability of low-cost software-defined radio (SDR) platforms, the resilience of landing systems has not been tested. We investigate and demonstrate the vulnerability of the instrument landing system, a primary nav-aid used by aircraft for safe approaches by providing lateral and vertical guidance in poor-visibility conditions. We analyze the ILS waveforms' and show the feasibility of spoofing using commercially-available SDR, causing last-minute go-arounds, and even missing the runway. We demonstrate that we can control the course deviation indicator in real-time on aviation-grade ILS receivers. We introduce and evaluate an overshadow attack and a low-power single-tone attack. For evaluation, we develop a tightly controlled and closed-loop ILS spoofer. Adversary's signals are adjusted as a function of aircraft's location thus causing an un-detected off-runway landing. We demonstrate the attack on an FAA certified flight-simulator (X-Plane). A spoofing region detector is integrated into our attacks for timely triggering the spoofing which reduces detectability. We systematically evaluate the performance of the attack against X-Plane's autoland feature and demonstrate touchdown offsets of 18 to 50 meters. Finally, we discuss approaches toward secure and efficient aircraft landing systems.

Cosmos Testbed Introduction

Michael Sherman (Rutgers University), Ivan Seskar

The COSMOS testbed enables researchers to explore the technology "sweet spot" of ultra-high bandwidth and ultra-low latency in the demanding real-world environment of NYC. We describe COSMOS's design, compute and network architectures, and critical building blocks. These building blocks include Software Defined Radios for sub-6Ghz, 28Ghz mmWave phased array modules, the optical transport network, core and edge clouds, and control and management software.

NOTES:

NOTES:

NEWSDR 2019 was made possible by generous contributions from our sponsors.

MathWorks is the leading developer of mathematical computing software. Engineers and scientists worldwide rely on its products to accelerate the pace of discovery, innovation, and development.

NI accelerates productivity, innovation, and discovery through an open, software-defined platform. This approach helps you develop and increase the performance of automated test and automated measurement systems. For more than 40 years, NI has developed high-performance automated test and automated measurement systems to help you solve your engineering challenges now and into the future. Our open, software-defined platform uses modular hardware and an expansive ecosystem to help you turn powerful possibilities into real solutions.

Ettus Research™, a National Instruments (NI) company since 2010, is the world's leading supplier of software defined radio platforms, including the Universal Software Radio Peripheral (USRP™) family of products. With a low overall system price, expansive capabilities, and software availability, USRP products are used by thousands of engineers worldwide and remain the top choice in software defined radio hardware for algorithm development, exploration, and prototyping.

MediaTek is a pioneering fabless semiconductor company, and a market leader in cutting-edge systems on a chip for wireless communications, HDTV, DVD and Blu-ray. MediaTek created the world's first octa-core smartphone platform with LTE and our CorePilot technology released the full power of multi-core mobile processors. MediaTek [TSE:2454] is headquartered in Taiwan and has offices worldwide.

Analog Devices is a world leader in the design, manufacture, and marketing of a broad portfolio of high performance analog, mixed-signal, and digital signal processing (DSP) integrated circuits (ICs) used in virtually all types of electronic equipment. Used by over 60,000 customers worldwide, our signal processing products play a fundamental role in converting, conditioning, and processing real-world phenomena such as temperature, pressure, sound, light, speed, and motion into electrical signals to be used in a wide array of electronic devices.

The College of Science and Mathematics is strongly committed to providing the best educational opportunities and resources for our undergraduate and graduate students. This includes an active research faculty to provide a proper background in experimental research for students and the scientific community. A spirit of collaboration exists across departments because modern science requires interdisciplinary approaches. In research labs, undergraduate students work with graduate students and faculty, and the practices that undergraduates learn in the research lab are carried over into their work in the public and private sector.

A community within the New England area that possesses members from academia, industry, and government who are involved in the design and implementation of software-defined radio (SDR) technology in order to advance the current state-of-the-art in wireless communication systems and networks.