Commonwealth Cyber Initiative

Communications with GenAI

CCI @ VT Technical Capabilities

Drs. Jacek Kibilda (*presenting*), Yi Shi, and Jeffrey Reed
Commonwealth Cyber Initiative (CCI)
Dept. of Electrical and Computer Engineering
Virginia Tech

IARPA End-Gen PROPOSERS' DAY
Arlington, VA, 27 February 2025

Overview

Our team combines world-class academic expertise and implementation know-how of advanced wireless communications systems, software-defined radio, generative AI, and wireless security with unique infrastructure and lab capabilities to prototype AI-based communications solutions.

We aim to contribute to the use #2 - *generating waveform protocols in a lab and then transferring to the wild*.

Keywords: Machine Learning, Communications, Software Defined Radios, Wireless Security

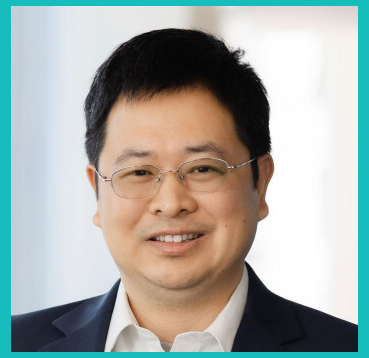
Complementary expertise: Large X Models, Software Engineering, Systems Integration

Core Team

Jacek Kibilda

Research Associate Professor

Expertize in modeling, optimization, and software-defined radio for wireless communications, networks, and security. Experience in research project leadership in the US and EU. Presently, Site Director on the NSF IUCRC for 6G. Recipient of the Fulbright TechImpact Award, IEEE Globecom 2023 Best Paper Award, and IEEE MILCOM 2023 Best Demo.



Yi Shi

Research Associate Professor

Expertize in machine learning, algorithm design, and optimization for wireless communications, networking and security. He received a number of awards, including the Test of Time Paper Award at IEEE INFOCOM 2023 and the Best Paper Award at IEEE INFOCOM 2008. He is an IEEE Fellow.

Jeffrey Reed

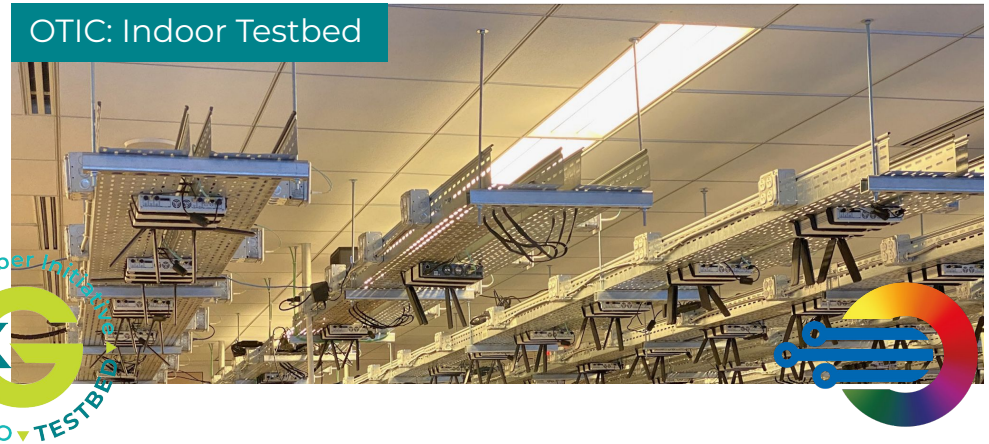
Willis G. Worcester Professor

IEEE Fellow for software radio, communications signal processing and engineering education. Co-founder Federated Wireless, PFP Cybersecurity, and Cirrus360. Interest in SDR, cognitive radio, and wireless security. Elected to National Academies of Inventors.

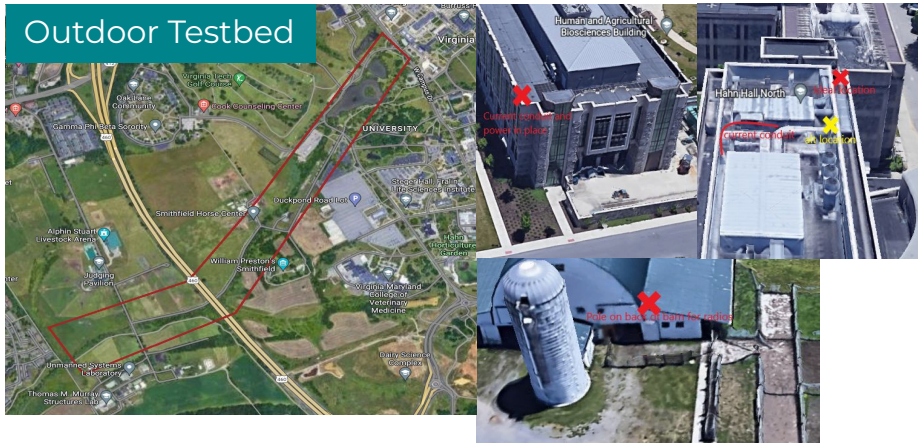
Research Infrastructure Capabilities

Advanced Radio Software Testbed Facilities to Support Lab to Wild Transfer

OTIC: Indoor Testbed



Outdoor Testbed

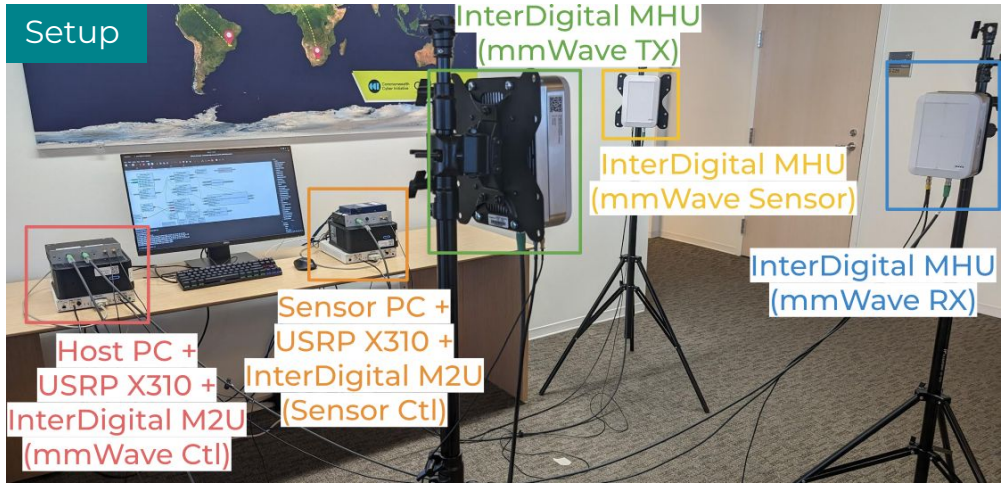


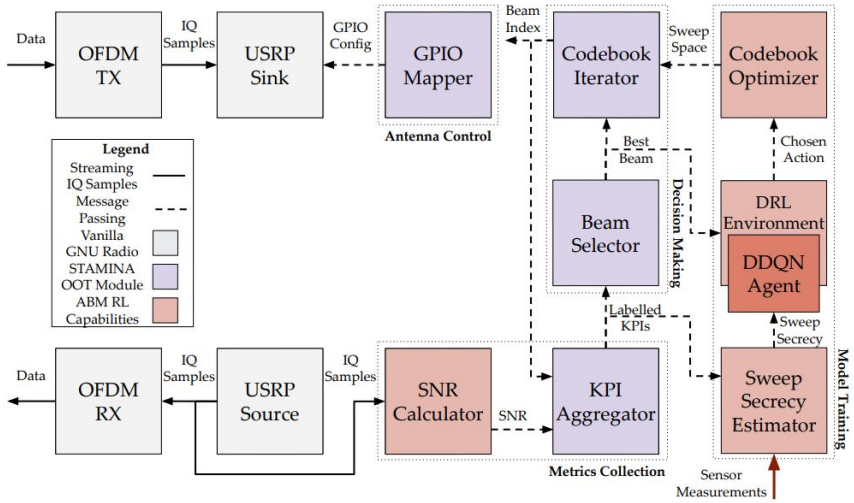
- **Large-scale**, open and programmable wireless testbed
- **FCC experimental license**
- **70+ USRPs**, **4+ GPU-accelerated MEC** nodes, and **10+ HPC servers** with a **10Gbps fiber fronthaul**
- Open-source, **end-to-end O-RAN** environment, including Near- and Non-RT RICs, SMO, and radio stack

- Ongoing deployment of a **private 5G** network in **shared spectrum** (CBRS, 3.5 GHz band) covering 1.5 square miles
- VT holds **Priority Access License** to 4 x 10 MHz CBRS channels
- Deployment of 3 SDR-based, **AI-ready**, edge nodes, with **power metering** capabilities

Sample AI for Comms Lab Prototype

SDR Platform for Secure Beam Sweeping Adaptation in Millimeter-Wave Communications





Real-time Implementation in GNURadio

- **HW Setup:** 3x NI USRP X310 (Tx, Rx, Sensor), 3x InterDigital Mast Head Units (8x8 array, 28 GHz), 2x InterDigital M2U Units (control, sync), Intel NUC
- **SW Setup:** GNURadio-based implementation of data and control plane for beamforming management

- Developed platform natively provides support for training and deployment of machine learning
- Offline and Online Training
- In this implementation, Double Deep Q-Network agent was used for real-time adaptation

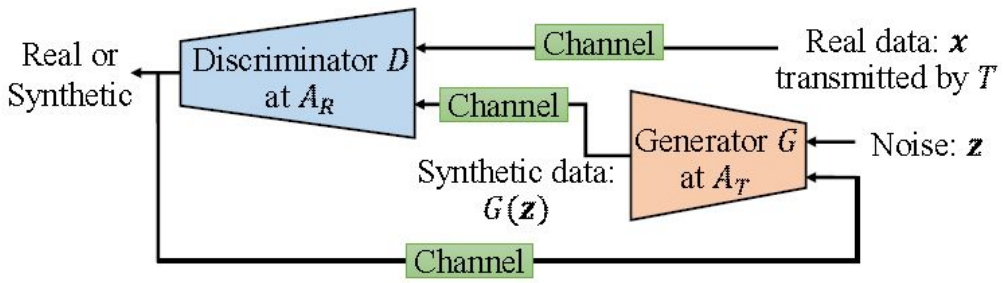
R1. https://github.com/CCI-NextG-Testbed/gr_stamina

R2. A. Baron-Hyppolite, J. F. Santos, L. A. DaSilva, and J. Kibilda, “Eavesdropper Avoidance through Adaptive Beam Management in SDR-Based MmWave Communications”, International Symposium on Wireless Communication Systems, 2024.

R3. A. Baron-Hyppolite, J. V. F. Abreu, J. F. Santos, L. A. DaSilva, and J. Kibilda, “Adaptive Beam Management for Secure mmWave Communications Using Software-Defined Radios,” IEEE MILCOM, 2023. [**BEST DEMO AWARD**]

Gen AI Research Capabilities

Application Areas



- **Wireless signal**, e.g., "Generative adversarial network in the air: Deep adversarial learning for wireless signal spoofing," *IEEE Transactions on Cognitive Communications and Networking*, March 2021.
  Synthetic wireless signal is generated to launch spoofing attack to a DL based signal detection system.

- **Network traffic**, e.g., "Vulnerability analysis for deep learning systems in network security," *IEEE MILCOM 2022*, Restricted Program.
  Synthetic network traffic data is generated to launch evasion attack to a DL based network intrusion detection system.

- **Social media**, e.g., "Systems and means for generating synthetic social media data", US Patent 10,719,779.
  Synthetic social media data is generated to provide input to social media analysis while hiding private information.

R1. Shi, Yi, Kemal Davaslioglu, and Yalin E. Sagduyu. "Generative adversarial network in the air: Deep adversarial learning for wireless signal spoofing." IEEE Transactions on Cognitive Communications and Networking 7.1 (2020): 294-303.

Commonwealth Cyber Initiative

Thank you!

Correspondence: jkibilda@vt.edu, yshi@vt.edu