5G Wireless Security

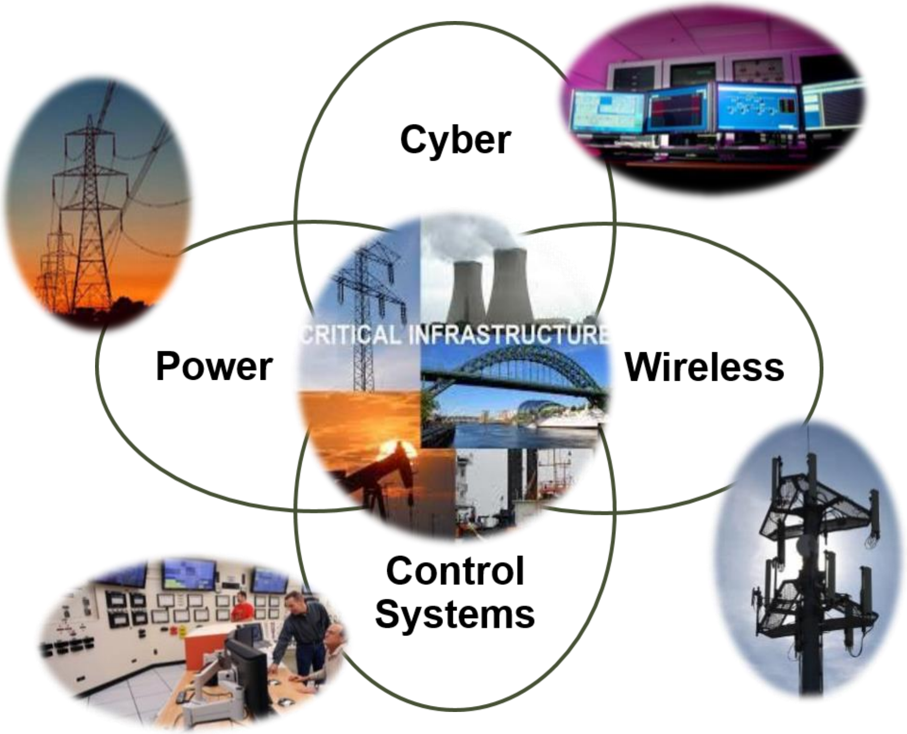
Dr. Arupjyoti (Arup) Bhuyan
Dr. Carl Kutsche

National & Homeland Security
Idaho National Laboratory

September 13, 2018

www.inl.gov

Wireless security is essential to protecting the nation’s critical infrastructure



INL Capabilities Secure Wireless Solutions from Concept through Validation and Deployment

Wireless Research: **Develop solutions to national spectrum and wireless communications security challenges** ***(WSComm[1], WiFIRE[2], mmWave physical layer security, 5G Cellular UAS[3])***

Wireless Modeling & Simulation: **Advanced software engineering, validation and testing of wireless security solution technology design (*IMOM[4]*)**

Wireless Test Bed: **Test and validate full-scale deployment of wireless communications security technology solutions (*JamX 17[5]*)**

[1] Wireless Spectrum Communications, [2] Wireless RF signal Identification and protocol Reverse Engineering, [3] Unmanned Aircraft System, [4] Improved Many on Many, [5] 2017 First Responder Jamming Exercise

Securing Wireless Communications Spectrum

Current challenges:

- Communication disruption from both unintended and deliberate interference.
- Violation of spectrum sharing rules.
- Use of vulnerabilities in wireless spectrum protocols (LTE/WiFi, etc.) to disrupt or degrade services.
- Illegal access of subscriber information for spectrum use, user traffic, and protected spectrum databases.
- Attack on critical information such as location in a sensor network.
- Use of cellular connected UAS/drone to attack critical infrastructure.

Current approaches for mitigation:

- Detection and localization of interference source.
- Transmission of content over a large band with very low power levels comparable to noise.
- Signaling data link with higher reliability.
- Real time spectrum monitoring and RF classification with machine learning.
- Cryptographic methods such as authentication and encryption.
- Security at the lower/physical layer exploiting uniqueness of wireless transmission.
- Detection of unauthorized UAS in sensitive areas.

How will 5G Impact the Spectrum Security Issue

New spectrum capabilities with 5G:

- Additional spectrum with and without spectrum sharing in sub 6 GHz and mmWave bands.
- Use of unlicensed and shared spectrum with 5G NR (New Radio).
- Beam based instead of sector based air interface.
- 5G enabled IoT[1], connected health, vehicles, UAS etc.
- Edge computing with SDN[2] and NFV[3] for applications including industrial IoT, augmented reality (AR), connected health, and connected vehicles (V2X).

Additional challenges:

- Increase in illegal and disruptive use of spectrum sharing.
- Adapting wireless security to beam based directional transmission.
- Secure operation of increasing number of connected UAS and vehicles.
- Secure use of edge connectivity to enable 5G applications.
- Decrease in the size of an antenna array needed to localize RF sources in the GHz bands for malicious purpose.

[1] Internet of Things, [2] Software Defined Networking, [3] Network Function Virtualization

Wireless Research Opportunities

5G Wireless Security Research Areas:

- Security and resiliency improvement using unique physical layer characteristics in the mmWave bands (e.g., device forensics and RF biometrics).
- Attack identification and threat mitigation for the radio frames and channels in NR.
- Secure spectrum sharing with improved and faster detection, localization, and response to spectrum abuse.
- Secure cellular UAS/drone control and communication system, including authentication system for detecting and localizing illegal users.
- Beam propagation and RF coverage models in the air for secure and reliable cellular UAS/drone operation.
- Secure and reliable use of spectrum for V2X wireless communications.

Additional Recommendations:

- Increase nationwide focus on wireless security and resiliency research efforts.
- Advocate “Cyber Informed Engineering” for spectrum control and operations.
- Support Intrusive test set and procedures to certify equipment for secure use of spectrum (e.g., adversarial model based automated test generation).

INL

Idaho National Laboratory

"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development
(NITRD) Program

Mailing Address: NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

Physical Address: 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674,
Fax: 202-459-9673, Email: nco@nitrd.gov, Website: https://www.nitrd.gov