WSRD IWG Workshop Report:

Security From A Wireless Spectrum Perspective: Technology Innovation and Policy Research Needs

Prepared by the
Wireless Spectrum Research & Development
Interagency Working Group

September 2019

Table of Contents

Introduction **1**
Key Takeaways **1**
Workshop Topics **2**
Wireless Hardware, Waveforms, and Protocol Security 2
Wireless Access Technologies that Impact Wireless Networks 2
Facets of these Technologies that are Vulnerable to Exploits 3
Opportunities to Mitigate these Vulnerabilities: 3
Spectrum Authentication and Identification 3
Service-Level Agreements 4
Wireless Attack Vectors: From Legacy to Emerging Systems 4
Questions that Need to be Addressed 5
Short-Term Research Goals 5
Long-Term Research Goals 5
Policy Issues 5
Conclusion **5**
Abbreviations 6

Introduction

Communications over the wireless medium pose security threats that are yet to be fully understood. It is currently possible for attackers that are within the wireless range to hijack or intercept an unprotected connection without being detected. With the advent of sophisticated cognitive radios and wireless devices, and applications such as the Internet of Things (IoT), drones, small satellites, driverless cars, and wireless healthcare devices, security threats to wireless mobile communications systems are rapidly increasing. As 5G,[1] low-power wide area networks, and other emerging systems are deployed, innovative protective technologies and policies are needed.

The Networking and Information Technology Research and Development (NITRD) Program's Wireless Spectrum Research and Development (WSRD) Interagency Working Group (IWG), which is co-chaired by the National Science Foundation (NSF) and the National Telecommunications and Information Administration (NTIA), held a workshop, *Security from a Wireless Spectrum Perspective: Technology Innovation and Policy Research Needs*, on September 13, 2018, in Washington, DC. The purpose of the workshop was to share insights and build relationships across Federal agencies and between the public, private, and academic sectors on the topic of wireless mobile device security. The 35 workshop participants represented a balanced cross-section of stakeholders involved in, or impacted by, this area of research. Additional information on the workshop is available at https://www.nitrd.gov/nitrdgroups/index.php?title=WSRD-Workshop-X.

Key Takeaways

The workshop participants discussed the challenges of securing and assuring spectrum availability and performance over wireless links and the need for innovation in the following five key areas:

1. *Improved wireless network system performance*, which depends on understanding the complete range of issues before systems are deployed. Such understanding will need experimentation beyond the laboratory, access to data sets to support new security and privacy mechanisms, and innovative tools and procedures to certify spectrum-sharing devices.
2. *Investigating the impacts of emerging physical layer technologies on the security of the underlying wireless network system*. These technologies include advanced forms of multiple-input multiple-output (MIMO) and beamforming, new antenna designs with higher directivity, and millimeter wave (mmWave)-band systems.
3. *Security overall*. Concerns will increase as 5G and other new systems are leveraged for shared spectrum use. Security mechanisms must support the *availability* of shared spectrum and the *scalable authentication* of devices and their software.
4. *Artificial intelligence and machine learning (AI/ML)*. Such capabilities are likely to be necessary for radio systems to automatically and continually sense, infer, and respond to changing radio frequency (RF) conditions. This requires creation of a multitude of pertinent datasets to train the machine algorithms.
5. *Automatic updating of radio devices* as policy and service agreements evolve. This is particularly true for low-end/low-cost devices.

[1] 5G refers to fifth-generation wireless mobile communication technology; it promises much higher speeds and near real-time connectivity, which is critical for new applications such as sensors and driverless cars.

Workshop Topics

The workshop was organized around the following four topic areas, described below:

- Wireless Hardware, Waveforms, and Protocol Security
- Spectrum Authentication and Identification
- Service-Level Agreements
- Wireless Attack Vectors: From Legacy to Emerging Systems

Wireless Hardware, Waveforms, and Protocol Security

The technologies that support access to wireless networks are rapidly advancing. Waveforms, antenna, and state-of-the art components such as schedulers, policy engines, modulators, demodulators, and frequency selectors all integrate software options internal to the device. The complexity and interdependencies of different hardware and software components require that engineers consider a wide variety of security issues when designing a trustworthy wireless transmitter or receiver. Compounding this challenge is the fact that device and network operations also can be impacted by the operating environment.

Participants examined the design of the entire wireless access system and focused on the security challenges present when users and services interface with wireless networks and network services. Using a three-step process, participants identified: (1) emerging wireless access technologies that impact existing wireless networks; (2) the facets of these technologies that are vulnerable to exploits; and (3) the opportunities to mitigate these vulnerabilities. (Please note that list items are in no particular order.)

Wireless Access Technologies that Impact Wireless Networks

- mmWave technology—the strategic and harmful impact of reflectors
- Massive MIMO and multiuser, distributed MIMO/beamforming
- Carrier aggregation and split-band waveforms
- Full duplex radio design
- Device-to-device communications (such as local communication or device pairing)
- New physical layer waveforms to support delay-sensitive scenarios
- Cross-technology coordination (e.g., WiFi/LTE-U,[2] or communication/radar sharing)
- Flexible framing and intercarrier distances
- Cloud-RAN, edge computing, fog computing[3]
- Low-power wireless technologies, such as wireless personal area networks (WPAN) and IoT
- Drones

[2] LTE (long-term evolution) is a high-speed wireless communication standard for mobile devices and data terminals. LTE-U is an evolving wireless communication system designed to use *unlicensed* spectrum to allow cellular network operators to offload some of their data traffic.

[3] Cloud-RAN, also sometimes referred to as Centralized-RAN (both abbreviated C-RAN), is a proposed cellular network architecture that addresses capacity and coverage issues along with network self-optimization. Edge computing is done at or near the source of the data instead of in a centralized, cloud environment. Fog computing uses edge devices to do computing in spaces between end devices and cloud computing data centers.

Facets of these Technologies that are Vulnerable to Exploits

- *Flexible frame length:* Addressing exploits that take advantage of flexible frame length requires careful implementation of proper timeout and protocol exits, though this weakness may not have serious consequences
- *GPS for synchronization:* There is significant disruption possible for new services that rely on GPS for tight synchronization.
- *mmWave:* Although the inherently smaller radio footprint minimizes harm, it also makes it more difficult to detect and localize attacks. As the quantity of users increases, so do the problems.
- *Combining technologies:* Combining old and new technologies increases the opportunity for security threats. For example, it was found that using LTE-based control planes to support the initial rollout of 5G technologies required the management of two networks; the weakness of the control network was inherited by the new network.
- *Data sharing:* Maintenance and coordination of multiple radio access technologies implies the sharing of data that could reveal private information.
- *Utilizing drone technologies:* Sensors located on drones could monitor spectrum usage over a wide geographic footprint.

Opportunities to Mitigate these Vulnerabilities

- Utilize data analytics and cloud services to process the large volume of wireless network data and detect anomalous activities. This would require the definition of normal and abnormal wireless behaviors (e.g., at the physical or network layers).
- *Improve testbeds to validate and test wireless system configurations prior to deployments and standardization*. For example, the ability to test the integration of old and new wireless technologies in a controlled manner prior to rollout would support the identification of potential attack vectors prior to going live with real users and real threats.
- *Develop ways to test wireless devices over the air* and confirm that their hardware, software, and protocols meet the requirements identified in the standards and/or regulations.

Spectrum Authentication and Identification

As more devices are deployed in shared spectrum bands, authentication and identification become increasingly critical to avoid impersonation and rogue devices. A scalable solution would be one that uses a split approach, where not every device is authenticated. An example is a macro-level authentication that allows an entity to obtain resources, paired with a micro-level authorization between the entity and the different types of devices that would like to use the spectrum. Solutions based on SIM, eSIM, and soft-SIM[4] could be used for small devices and be augmented with additional modalities such as two-factor authentication. Participants noted that this could be part of a global authentication system to support spectrum sharing.

The same two-level approach can apply to the identification of devices. A macro-level entity that handles spectrum authentication in blocks can also be responsible for identifying the devices that use this spectrum.

Other participants suggested that physical layer radio fingerprints (based on their RF emissions) could be used for identification of noncooperative and/or nonresponsive users. This would require a global

[4] SIM (subscriber identification module) is a removeable identity chip that links a mobile device to a network; eSim is an *embedded*, nonremovable SIM; and soft SIM (software SIM) is a reprogrammable chip embedded in a mobile device.

database of fingerprints that presents several challenges, including whether such fingerprints can be accurately measured and whether they change as a function of device age and ambient conditions. Discussion included whether this would be an effective way of monitoring problem users, but it also raised questions of whether measurement data is trustworthy. Could it be used in the courts? If a wrong person is identified, who is responsible?

Policy advancements could support authentication and identification research if there were a certification process that allows devices to behave in a certain way, that can be changed in an authenticated manner, and that allows for identification of misbehaving devices.

Service-Level Agreements

New high-capacity networks promise to provide diverse business services and models as well as operational sustainability (i.e., end-to-end management and deployment, flexibility, scalability, and energy efficiency). To realize these benefits, providers will need service-level agreements (SLAs) that consider latency, throughput, concurrent connections, coverage area, mobility, and network architecture service-level guarantees. These requirements often conflict and make guarantees via SLAs problematic. To begin the discussion, participants identified several different types of SLAs, including location-specific (e.g., hospitals), dynamic and automated, roaming, high-security and privacy, ultra-reliable, and low-latency communications.

Participants then examined these various scenarios and identified the security issues that would be candidates for further research (in no particular order):

- Latency, i.e., time needed to correct network instability
- Denial of Service or use of fake networks (spoofing)
- Cell breathing attacks, i.e., beam patterns that are changed to create self-interference
- Malware attacks, i.e., malicious software that plants a "bug" in a device or network
- mmWave, i.e., antennas that accelerate scanning for waves
- Data analytics and monitoring
- Vulnerability when upgrading wirelessly connected devices' firmware
- Sensing and spectrum awareness
- Network intelligence
- Every software load is different, requiring unique memory layouts, with diversity in positioning, navigation, and timing

Wireless Attack Vectors: From Legacy to Emerging Systems

The requirement to secure wireless networks and the data that rides on them is both critical and difficult to accomplish. Integration of multiple generations of technologies that are often stretched beyond their original purposes creates new attack vectors. Security requirements also differ by use, and establishing the wrong level has consequences. Consider the network navigating a car versus the one carrying a twitter feed, or the case where individuals might not want their movements available through their fitness trackers but might welcome access by a drone hovering over an accident scene to assist first responders.

Participants discussed these and other complex wireless attack vectors, such as insecure 2G and 3G devices connected to the network, inherent challenges of GPS and ADS-B systems,[5] supply chain issues

[5] ADS-B (Automatic dependent surveillance—broadcast) is a surveillance technology in which an aircraft determines its position via satellite navigation and periodically broadcasts it, enabling it to be tracked.

with chip manufacturers, the push to use domestically manufactured parts, and inherent trust in the SIM card manufacturer ecosystem.

The following is a summary of questions that need to be addressed, suggested short-term and long-term research goals, and some policy questions.

Questions that Need to be Addressed

- How do we protect spectrum access in legacy systems?
- What are the implications of new applications to spectrum access security?
- What are the safety implications of spectrum access security for transportation?
- Could resiliency to wireless attack vectors become a competitive advantage?
- Could obfuscation be used as a security tool i.e. promulgation of attack information?
- How do we isolate/separate radio attack vectors from other attack vectors?

Short-Term Research Goals

- Construct a list of widely used systems with legacy security issues.
- Create a list of real world/operational IMSI catcher experiences.[6]
- Define and categorize risk.
- Compile a catalog of vulnerabilities.
- Discover low-cost tools for testing of wireless systems (i.e., some researchers are priced out of participating).
- Develop criteria to understand when an attack will happen, if a user has been attacked, and how to react.
- Explore the capability of user equipment to negatively impact networks.

Long-Term Research Goals

- Find lower-cost security solutions for commercial users.
- Create innovative tools to defend against spectrum terrorism.

Policy Issues

- Develop a realistic risk-definition capability.
- Reduce the impact and costs of mitigation.
- Create a spectrum security access awareness campaign.
- Determine the impact of the domestic availability of inexpensive IMSI catchers.

Conclusion

The workshop participants identified an array of challenges and opportunities surrounding research and innovation to address current and emerging wireless system security threats. The following trends were discussed as challenges that require improved awareness and further study:

- *The increasing diversity of wireless networks*, including the various standards, the wide-range of spectrum bands of operation, and the heterogeneity of wireless devices that operate on them.

[6] IMSI (international mobile subscriber identity) is a unique number associated with mobile telecommunications devices. An IMSI catcher is an eavesdropping device for intercepting mobile phone traffic and tracking location data.

- *The operational complexity of wireless systems* and the subsequent inability to identify points of failure/weakness.
- *The expectation of high service assurance* that wireless users have come to expect even as new applications are developed.
- The ongoing translation of previously hardware-dependent aspects into software services, such as the migration of first-/last-hop wireless operations into the cloud.

Finally, the following were discussed as opportunities that could result from research and innovation in addressing wireless system security threats:

- A more complete end-to-end understanding of wireless systems through the strategic use of AI/ML techniques.
- Improved policy for and management of heterogeneous end-user devices through software-defined operations.
- The potential of emerging technologies, such as massive MIMO and millimeter-wave systems, to help realize secure 5G wireless networking.

Abbreviations

5G	fifth-generation wireless mobile communication technology
AI/ML	artificial intelligence/machine learning
CSIA	Cyber Security and Information Assurance (NITRD IWG)
GPS	Global Positioning System
IMSI	international mobile subscriber identity (chip for mobile devices)
IWG	Interagency Working Group
LTE	long-term evolution (wireless standard)
MIMO	multiple-input multiple-output
NCO	National Coordination Office
NITRD	Networking and Information Technology Research and Development
NSF	National Science Foundation
NTIA	National Telecommunications and Information Administration (Department of Commerce)
R&D	research and development
RF	radio frequency
SIM	subscriber identification module (chip for mobile devices)
WSRD	Wireless Spectrum Research and Development (NITRD IWG)

About this Report and its Authors

The NITRD Program's WSRD IWG organized the workshop, *Security from a Wireless Spectrum Perspective: Technology Innovation and Policy Research Needs*, on September 13, 2018, in Washington, DC, to address the need to include spectrum as a key security design factor for modern communication systems. The workshop included participation from NITRD's Cyber Security and Information Assurance IWG as well as a balanced cross-section of stakeholders involved in, or impacted by, this area of research. This report summarizes the major topics of discussion at the workshop. It is available online at https://www.nitrd.gov/publications/index.aspx.

The NITRD Program is the Nation's primary source of federally funded work on pioneering information technologies (IT) in computing, networking, and software. The NITRD Subcommittee of the National Science and Technology Council's Committee on Science and Technology Enterprise guides the multiagency NITRD Program in its work to provide the R&D foundations for assuring continued U.S. technological leadership and meeting the needs of the Nation for advanced IT. The National Coordination Office (NCO) supports the NITRD Subcommittee and the Interagency Working Groups (IWGs) that report to it. The NITRD Subcommittee's Co-Chairs are Kamie Roberts, NCO Director, and Erwin Gianchandani, Interim Assistant Director of the NSF Directorate for Computer Information Science and Engineering. More information about NITRD is available at https://www.nitrd.gov/about/.

The WSRD IWG consists of Federal agency representatives who work together to coordinate spectrum-related research and development activities both across the Federal Government and with the private sector and academia under the auspices of the NITRD Subcommittee. The WSRD Co-Chairs are Rangam Subramanian of NTIA and Thyaga Nandagopal of NSF. The group's purpose is to facilitate efficient and effective R&D investment in the advancement of spectrum-sharing technologies and systems, consistent with the WSRD IWG's guiding principles, which are transparency, smart investment, and solicitation of opportunities for technology transfer across and beyond the Federal Government. More information is available at https://www.nitrd.gov/groups/wsrd.

Acknowledgments

The National Coordination Office for the NITRD Program gratefully acknowledges the WSRD Co-chairs Rangam Subramanian, NTIA, and Thyaga Nandagopal, NSF, as well as Wade Trappe of Rutgers University, and all the workshop participants and members of the WSRD IWG and CSIA IWG who helped plan and implement the workshop and write and review this report.