Wireless Spectrum Sharing: Enforcement Frameworks, Technology, and R&D

Networking and Information Technology Research and Development Subcommittee: Wireless Spectrum Interagency Working Group Report

January 9, 2017

About the Networking and Information Technology Research and Development Subcommittee

The Subcommittee on Networking and Information Technology Research and Development (NITRD) is a body under the Committee on Technology (CoT) of the National Science and Technology Council (NSTC). The NITRD Subcommittee coordinates multiagency research and development programs to help assure continued U.S. leadership in networking and information technology, satisfy the needs of the Federal Government for advanced networking and information technology, and accelerate development and deployment of advanced networking and information technology. It also implements relevant provisions of the High-Performance Computing Act of 1991 (P.L. 102-194), as amended by the Next Generation Internet Research Act of 1998 (P. L. 105-305), and the America Creating Opportunities to Meaningfully Promote Excellence in Technology, Education and Science (COMPETES) Act of 2007 (P.L. 110-69). For more information, see www.nitrd.gov

About the Wireless Spectrum Research and Development Interagency Working Group

The Wireless Spectrum R&D (WSRD) Interagency Working Group (IWG) was formed in late 2010 to coordinate spectrum-related research and development activities both across the Federal government and with academia and the private sector. The purpose is to help coordinate and inform ongoing activities across Federal agencies and to facilitate efficient and effective investment in spectrum sharing technologies and systems. These activities are consistent with the guiding principles of WSRD, which are transparency, smart investment, and the solicitation of opportunities for technology transfer across and beyond the Federal government.

Copyright Information

Wireless Spectrum R&D Interagency Working Group

Co-Chairs:
Rangam Subramanian, NTIA
Thyaga Nandagopal, NSF

Participating Agencies:

Defense Advanced Research Projects Agency (DARPA)
Department of Defense Service Agencies: Air Force, Army, Navy
Department of Homeland Security (DHS)
Department of Energy (DOE)
Department of Justice (DOJ)
Federal Aviation Administration (FAA)
Federal Communications Commission (FCC)
National Aeronautics and Space Administration (NASA)
National Institute of Standards and Technology (NIST)
National Oceanographic and Atmospheric Administration (NOAA)
National Security Administration (NSA)
National Science Foundation (NSF)
National Telecommunications and Information Administration (NTIA)
Office of the Secretary of Defense (OSD)
Office of Science and Technology Policy (OSTP)

Wireless Spectrum Sharing: Enforcement Frameworks, Technology, and R&D

On June 14, 2013, the President issued "Expanding America's Leadership in Wireless Innovation."[1] This memorandum proposed making more wireless spectrum available for commercial use by encouraging shared access by non-Federal and Federal users. In 2015 the National Coordination Office for Networking and Information Technology (NITRD) Wireless Spectrum R&D Interagency Working Group (WSRD IWG) issued a report, "Federal-Commercial Spectrum Sharing Workshop: Models, Applications, and Impacts of Incentives for Sharing"[2], in which it described timely and effective enforcement as a critical component to incentivizing the adoption of spectrum sharing systems and methodologies by spectrum users in both communities.

Enforcement, while critical for the success of spectrum sharing, is also the element of spectrum sharing that is least developed. The simultaneous use of spectrum by multiple users makes enforcement more complex and will require innovation in several areas, including an Environmental Sensing Capability (ESC), Spectrum Access Systems (SAS) and data forensics capabilities. Automating enforcement can address the "timely resolution" factor that is critical in a shared environment, but it raises many other questions. What elements of enforcement *can* be automated; can we automate attribution of responsibility; can we differentiate between intentional and unintentional interference; can we enforce cybersecurity and privacy; and finally, can we leverage work done in other domains such as the NIST Cybersecurity Framework[3] or the Trusted Platform Module (TPM)[4]? Further, to make these systems both effective and trustworthy, enforcement requirements must be prioritized in the technology design process.

After studying the issues and receiving input from additional government, academic, and private sector stakeholders at a workshop on May 15, 2016, the WSRD IWG concluded that the current enforcement system is not dealing well with the challenges of spectrum sharing, particularly in the areas of institutional rules, capacity and technological support. It has also determined that effective automation of interference detection and mediation requires additional research, infrastructure deployment, and testing. WSRD provides the following recommendations for research investment, organized into four categories:

---

[1] "Expanding America's Leadership in Wireless Innovation: Presidential Memorandum." White House. https://www.whitehouse.gov/the-press-office/2013/06/14/presidential-memorandum-expanding-americas-leadership-wireless-innovatio

[2] Lehr, Kahn, Kutsche. "Federal-Commercial Spectrum Sharing Workshop: Models, Applications, and Impacts of Incentives for Sharing." NITRD, March 19, 2015, Page 9. https://www.nitrd.gov/nitrdgroups/images/d/dc/WSRD_Workshop_VII_Report.pdf

[3] NIST Cybersecurity Framework http://www.nist.gov/cyberframework/

[4] TPM (Trusted Platform Module) is a computer chip (microcontroller) that can securely store artifacts used to authenticate the platform (your PC or laptop). These artifacts can include passwords, certificates, or encryption keys. A TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy. Authentication (ensuring that the platform can prove that it is what it claims to be) and attestation (a process helping to prove that a platform is trustworthy and has not been breached) are necessary steps to ensure safer computing in all environment s. Trusted modules can be used in computing devices other than PCs, such as mobile phones or network equipment. See http://www.trustedcomputinggroup.org/trusted-platform-module-tpm-summary/ .

1. ***Information gathering:***
    - Conduct a study to determine the scope of the interference problem
    - Collect case studies on existing enforcement systems, and generalize their key elements
    - Research how to connect a system-of-systems enforcement architecture into a single framework
    - Determine what information needs to be stored in database controlled spectrum management systems to assist in identifying sources of interference
    - Create an interference incident database accessible for researchers

2. ***Measurement and sensing:***
    - Understand what can be learned from crowd-sourced internet measurement that would apply to spectrum measurement efforts
    - Develop methods to fuse end-user, edge-based measurement data (i.e., crowd-sourced) with government systems
    - Design a spectrum-sensing mechanism that creates an affordable nationwide spectrum monitoring capability
    - Develop methods for identifying and locating a malicious device in the midst of cooperative (but occasionally misbehaving) devices
    - Determine how to balance emitter identification needs with privacy needs when investigating interference

3. ***Identification, forensics and adjudication:***
    - Consider how trusted platform module technology can be applied to radio systems
    - Develop enforcement systems that account for multi-band systems that dynamically hop bands (e.g., single 5G covering multiple standard LTE bands)
    - Explore options for interference resolution when parties are complying with the rules
    - Understand the possibilities and incentives behind citizen “interference trackers”

4. ***Policy***
    - Determine if radio design should address enforcement as a first order issue
    - Incorporate risk management into the design of enforcement systems
    - Study the legal options and possible policy changes necessary as current “usage rights” move to “collective action rights” e.g. database auditing
    - Incorporate different models of enforcement (e.g., third party, self-enforcement, and mutual enforcement) into a broad enforcement framework