Security Issues in Radar-Communications Spectrum Sharing

Dr. John Chapin

VP, Advanced Technologies

jchapin@robersonandassociates.com

WSRD Workshop X

13 September 2018

Roberson and Associates, LLC

Technology and Management Consultants ®

Focus of this briefing

The new security issues that arise in

radar-communications spectrum sharing **between separate organizations**

Radar-radar spectrum sharing:

- is designed into radars already
- raises no new security issues for the spectrum community

Sharing within a single organization:

- will see first deployments soon
- raises no new security issues for the spectrum community

Context of radar-communications spectrum sharing

- Assume a shared band where radar is primary
- Current use cases
  - Weather radars
  - Air search and tracking radars
    - Mobile – Naval
    - Fixed – Civil Air Traffic Control
- Potential use cases
  - Vehicular radars – ground, aerial, altimeters

- Technical issues considered in isolation
  - Mitigation of bidirectional interference is challenging but solvable
  - 15 years of work on this topic starting with FCC 5 GHz DFS proceeding

- Adding security concerns makes the problem much harder

Denial of Service Attacks

- DOS attacks on the radar
  - Direct jamming by communications systems (physical layer attack)
  - Attack that causes radar's spectrum sharing control system to thrash
  - Vectors:
    - Malware in communications devices
    - Cyber attack on spectrum control/support systems (e.g. SAS, ESC, data link from radar)
    - Insider attack on spectrum control/support systems

- DOS attacks on the communication system
  - Vectors:
    - Same 3
    - Spoof transmission of a radar signal
    - Cause radar to trigger hard shutdown of communications system in the band
      - Spoof transmission of comms signal
      - Malware causes misbehavior by (a few) comms devices

Privacy Violation Attacks

- Attacks on radar privacy (issue today)
  - Security concern: reduce cost for adversary to collect information about the radar
    - Location of mobile radars
    - Operating state, waveform shape, pulse timing (military only)
  - Vectors
    - Same 3 as for DOS attacks
    - Harvest observations from a large number of comms devices
    - Harvest history information from spectrum control/support systems

- Attacks on comms system privacy (potential future issue)
  - Load, usage, operating state (business intelligence)
  - Application layer data
  - Vectors
    - Use radar as SIGINT device

Solution Principles – DOS attacks

1. Assume the sharing system will malfunction

   - Requires backup mechanism to protect critical operational capability
   - Backup mechanism must have high reliability, may have low spectrum efficiency
   - See example on Slide 8

2. Graduated responses to violations

   - Force attacker to sustain attack over time, issue it from many locations, to cause big response
   - Simplifies detection of attacks
   - Facilitates collection of information to ID attacker/vector
   - Increases attack cost, thus reducing number of capable attackers and number of attacks

Solution Principles – Privacy Attacks

- Obfuscation is a primary method
  - Must balance privacy gain against loss of spectrum efficiency

3. Share the information yourself or lose control of it

  - Failure to share just forces the other side to build a sensor system to gather the information
  - The sensor system may gather private information
  - Lose the ability to control the obfuscation – raw data now vulnerable to sensor system insiders

4. Agree a spectrum access SLA between the parties

  - Enables all sides to plan
  - Can continually obfuscate up to the SLA level
    - NOT constant spectrum usage
    - Statistical access guarantees – e.g. lose usage of a channel for X days per year
  - Creates a policy challenge about how to evolve SLA over time

Example: Reliable mechanism to mitigate radar DOS in CBRS

- SAS channel access grants are (crypto authenticated) time limited leases
  - Enforce lease timeouts at a low (firmware) level in comms devices
- Radar operator can push a “big red button”
  - Causes SAS in that area tell all comms devices in the area to evacuate the band immediately.
  - SAS then shuts down (!) – handles case there is malware or fault in the SAS
- Correctly operating comms devices evacuate the shared band when:
  - SAS evacuate command
  - Loss of contact with SAS
- Compromised or buggy comms devices cease transmission when the TLL expires.
- Every push of the big red button is treated like an airplane accident.
  - The NTSB equivalent (SSSB?) investigates and prepares a public report.
  - Whoever pushed the button needs to have a defensible reason.

Thank You

"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