CSMAC:

Spectrum Management via Databases Working Group

Interim Report

Dec 13, 2013

Version 1.0

Overview

Question:

"How can sensitive and government classified operations be included and protected using a database-driven sharing approach, particularly one that strives toward real-time responses?"

The group agreed to address this question in general to the extent possible but also look at this in context specifically of the 3.5GHz band.

Progress to date

- Level set
  - Goal was to get a common understanding of what spectrum management via a database is. Generated a 1 page overview which as attached as last slide of this presentation and short doc on timing
- Discussed how sensitive and classified information is currently handled.
  - Agreed that our role is to provide a tool kit for how to handle sensitive information and not make recommendations on what should be sensitive information.
- Reviewed background in other bands include 70-90GHz.
- Developed a document with some insights and preliminary ideas for how to do spectrum management when sensitive of classified information maybe involved.

In order to better address the issues surrounding handling of classified and sensitive information, the working group would like to request that we work with the NTIA on a case study of sharing focusing on the 3.5GHz band with ship born SPY radar.

Insights

- **Information required to protect federal primary users is likely substantially less than that required to protect secondary users.** Specifically, Protecting Federal users via a database system likely means we only need receive (Rx) information not information on transit (Tx) characteristics. Rx information is often less sensitive then Tx information.
- **Information needed for effective sharing and how to handle it will be more difficult in some cases then others.** There is no one size fits all solution for what information needs to be shared. In fact for some systems, it will be difficult to share at all due to nature of systems (see 1755 MHz WG 2 Video Surveillance). We should focus on the most solvable scenarios first
  - Such solvable scenarios could include ship borne radar and fixed satellite Rx.
- **For many cases, sharing and protection can be achieved without need for federal users to make available operational information about their systems**. Only information needed to determine their protection needs to be provided to the database or spectrum access system (SAS) not detailed operational parameters.
  - For example no disclosure of modulation, radar waive forms, hopping patterns may be needed

Areas of Study

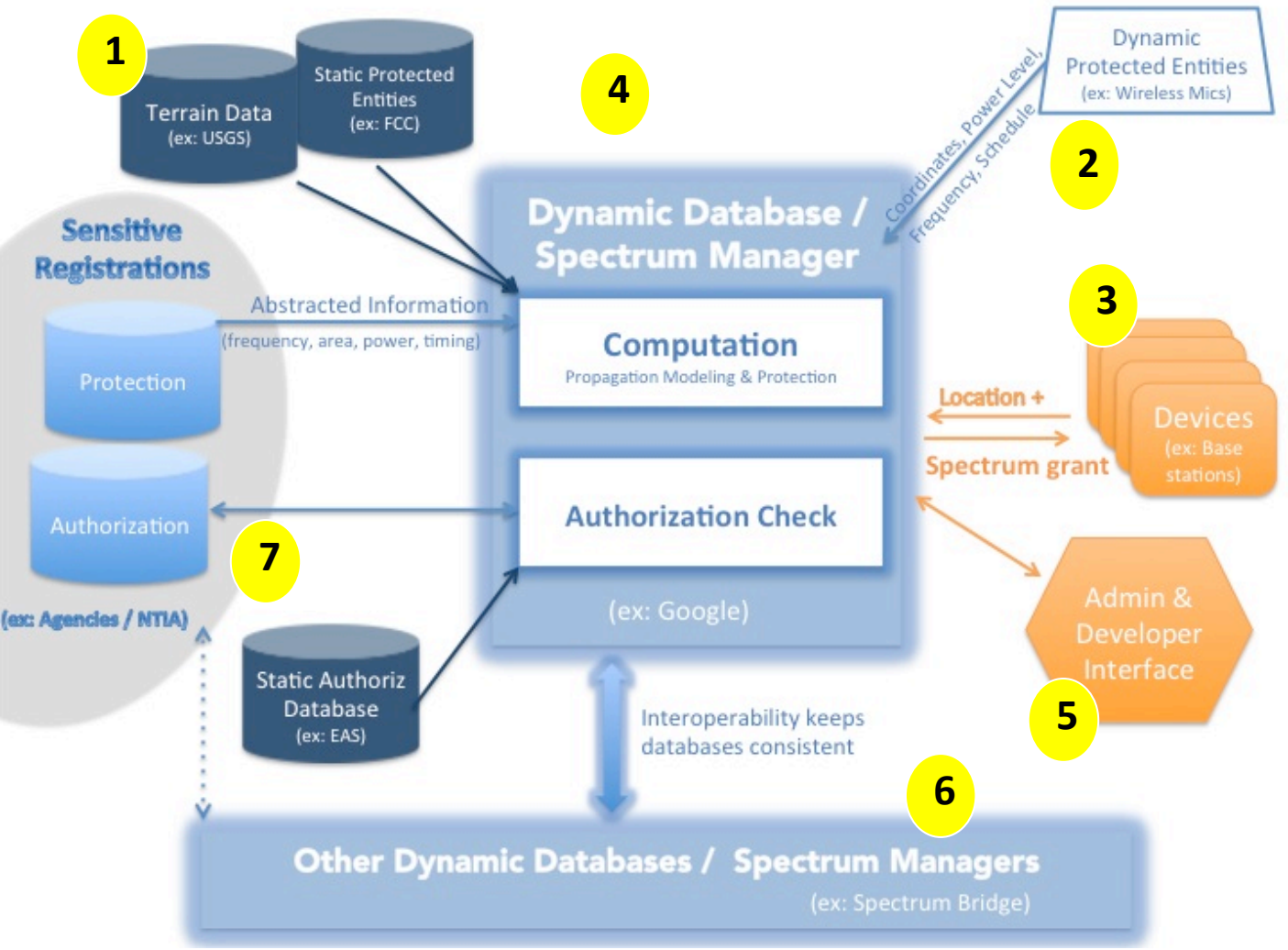
- Focus on minimum information needed for protection. Black box model approach.
  - What information is ***minimal essential information*** needed to enable any effective sharing. First step
  - What information would be ***desirable information*** for more effective/efficient sharing. Second step
- Example approaches being looked at
  - For in-band protection, consider a “Power Flux” specification across geographic boundry with a tolerated dBm/channel specification.
  - For Co-channel consider antenna/filter response curves with maximum post filter tolerated energy.
  - Trusted third party

Next Steps

- Schedule an NITA briefing or interaction to kick of case study on 3.5GHz ship borne radar
- Consider a briefing with OSTP on how they plan to balance need for confidentiality and ability to share.
- Refine work and develop recommendations

Spectrum Management via Database

- Functions as a Dynamic Spectrum Manager: Uses static and near real-time data to identify and allocate available spectrum to devices
- Able to add Classified Registrations without viewing or exposing sensitive data



1 Static data, such as terrain and licensed entities, is sent to the database.

2 Authorized entities can submit Dynamic Registrations to be protected.

3 Devices send location plus supplemental information and query the database for spectrum to use in that location.

4 The Database / Spectrum Manager checks access authorizations and calculate dynamic spectrum availability based on near real-time data from multiple sources.

5 Admin and Developer Interface could be developed if needed.

6 All spectrum databases constantly communicate to keep Dynamic Registrations synchronized.

7 **[Possible method for confidential information]** Sensitive registrations could be included securely.