Developments Towards a More Robust and Dynamic Spectrum Sharing Framework

Working Document WINNF-TR-2016

Version V1.0.0
July 30, 2025

TERMS, CONDITIONS & NOTICES

This document has been prepared by the Wireless Innovation Committee Midband Sharing Work Group to assist The Software Defined Radio Forum Inc. (or its successors or assigns, hereafter "the Forum"). It may be amended or withdrawn at a later time and it is not binding on any member of the Forum or of the Wireless Innovation Committee Midband Sharing Work Group.

Contributors to this document that have submitted copyrighted materials (the Submission) to the Forum for use in this document retain copyright ownership of their original work, while at the same time granting the Forum a non-exclusive, irrevocable, worldwide, perpetual, royalty-free license under the Submitter's copyrights in the Submission to reproduce, distribute, publish, display, perform, and create derivative works of the Submission based on that original work for the purpose of developing this document under the Forum's own copyright.

Permission is granted to the Forum's participants to copy any portion of this document for legitimate purposes of the Forum. Copying for monetary gain or for other non-Forum related purposes is prohibited.

THIS DOCUMENT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS DOCUMENT.

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of the specification set forth in this document, and to provide supporting documentation.

This document was developed following the Forum's policy on restricted or controlled information (Policy 009) to ensure that that the document can be shared openly with other member organizations around the world. Additional Information on this policy can be found here: http://www.wirelessinnovation.org/page/Policies_and_Procedures

Although this document contains no restricted or controlled information, the specific implementation of concepts contain herein may be controlled under the laws of the country of origin for that implementation. Readers are encouraged, therefore, to consult with a cognizant authority prior to any further development.

Wireless Innovation Forum ™ and SDR Forum ™ are trademarks of the Software Defined Radio Forum Inc.

Table of Contents

List of Figures

Contributors

Highly Dynamic Spectrum Sharing Task Group Chair: Andrew Clegg, Baylor University

Other Contributors:

- Virgil Cimpu, Ericsson
- Andrew Clegg, Baylor University
- Farinaz Edalat, RKF Engineering
- Monisha Ghosh, Spectrum X
- Fred Goldstein, WISPA
- Rauf Hafeez, Charter
- Wuri Hapsari, Boost Mobile
- Colby Harper, Pathfinder Wireless
- Ted Kaplan, RKF Engineering
- Minh Le, RED Technologies
- Richard Lee, iPosi
- Meihua Liang, MITRE
- Amit Mukhopadhyay, Nokia
- Masoud Olfat, Federated Wireless
- Pete Young, Comsearch

Developments Towards a More Robust and Dynamic Spectrum Sharing Framework

1 Introduction and Scope

Members of the Wireless Innovation Forum (WInnForum) have extensive expertise in spectrum sharing. They wrote the standards upon which the U.S. Citizens Broadband Radio Service (CBRS) operates and collaborated on the standards upon which the U.S. 6 GHz Automated Frequency Coordination (AFC) architecture operates [5]6]. The members also represent Spectrum Access System (SAS) and AFC system operators, CBRS and 6 GHz equipment manufacturers, and CBRS and 6 GHz network users.

The purpose of this document is to leverage that expertise and provide insight into how some of the aspects of these systems, which operate at a relatively "slow" dynamic spectrum sharing cadence, can be extended to support dynamic sharing on shorter timescales, with more robustness to detection or informing of incumbent activity. This effort is necessary to address more complex sharing environments to be faced in the future. For example, in the lower 3 GHz band, the number of different types of incumbent systems that must be protected is much bigger: >100, compared to about 2-3 in CBRS and 6 GHz. In addition, operations of the protected systems is much more dynamic, including airborne radar systems moving at hundreds of kilometers per hour. In CBRS, the fastest protected systems are shipborne (max speed on the order of 30-40 km/h), while other systems in CBRS, and all protected systems in 6 GHz band, are stationary.

The new application of several concepts relevant to spectrum sharing are discussed in this document. Among them:

- Reducing the time over which secondary users react to changes in incumbent use from 24 hours (6 GHz Band) and 5 minutes (CBRS Band) to potentially seconds
- Various incumbent detection/informing methods and their application of highly-dynamic spectrum sharing (HDSS), including:
    - Portal, including extensions to TARDyS3 to support HDSS
    - Dedicated sensing, RAN-based sensing, and hybrid models
- Improvements to propagation prediction, such as the use of known signals for in-situ clutter loss characterization
- The use of closed-loop interference reporting to reduce dependence on propagation models altogether while ensuring incumbent protection

1.1 Terminology

Before delving into a discussion on spectrum sharing, it is important to understand the different types of spectrum users. In this document, the terms Primary User and Secondary User (defined below) are used to describe relative interference protection rights. They are not referring to allocation status in the band.

Primary User (PU) will be a class of user in a band which has the highest interference protection rights (for example, a federal incumbent in CBRS)

Secondary User (SU) will be a class of user in a band that must protect Primary Users from interference (for example, CBRS users protecting federal incumbents in the CBRS band).

1.2 References

1. WInnForum Coordinated Periodic Activities Policy_All SAS admin https://winnf.memberclicks.net/assets/CBRS/WINNF-SSC-0008.pdf
2. CBRS Operational and Functional Requirements, https://winnf.memberclicks.net/assets/CBRS/WINNF-TS-0112.pdf
3. Post Initial Certification Revision to WINNF-TS-0112-V1.9.1, https://winnf.memberclicks.net/assets/CBRS/WINNF-TS-1020.pdf
4. National Spectrum Research & Development Plan, https://www.nitrd.gov/pubs/National-Spectrum-RD-Plan-2024.pdf
5. WINNF-TS-0112, Version 1.9.2, 1 April 2024, https://winnf.memberclicks.net/assets/CBRS/WINNF-TS-0112.pdf
6. WINNF-TS-1014, Version 1.5.0, 25 April 2025, https://winnf.memberclicks.net/assets/work_products/Specifications/WINNF-TS-1014.pdf
7. WINNF-TR-2017, Version 1.0.0, 30 April 2025, https://winnf.memberclicks.net/assets/work_products/Reports/WINNF-TR-2017.pdf

1.3 Acronyms

1. 3GPP - The 3rd Generation Partnership Project
2. AFC - Automated Frequency Coordination
3. CBRS - Citizens Broadband Radio Service
4. CBSD - Citizens Broadband radio Service Device
5. CONUS - Contiguous United States
6. DPA - Dynamic Protection Area
7. DSS - Dynamic Spectrum Sharing
8. ESC - Environmental Sensing Capability
9. FAR - False Alarm Rate
10. FCC - Federal Communications Commission

11. FS - Fixed Service
12. FSS - Fixed-Satellite Service
13. GAA - General Authorized Access
14. GNSS - Global Navigation Satellite System
15. HDSS - Highly Dynamic Spectrum Sharing
16. IPC - Interference Protection Criterion
17. IPT - Interference Protection Threshold
18. ISAC - Integrated Sensing and Communication
19. ISED - Innovation, Science and Economic Development (Canada)
20. ITM - Irregular Terrain Model
21. ITS - The Institute for Telecommunication Sciences
22. LEO PNT - Low Earth Orbit PNT
23. LiDAR - Light Detection and Ranging
24. NIST - National Institute of Standards & Technology
25. NLCD - National Land Cover Database
26. NTIA - National Telecommunications and Information Administration
27. OBS - Occupancy-Based Sensing
28. PAL - Priority Access License
29. PA - Protection Area
30. PE - Protected Entity
31. PNT - Positioning, Navigation, and Timing
32. PU - Primary User
33. RAN - Radio Access Network
34. RF - Radio Frequency
35. ROC – Receiver Operating Characteristic
36. SAS - Spectrum Access System
37. SNR - Signal-to-Noise Ratio
38. SU - Secondary User
39. TARDyS3 - Telecom Advanced Research and Dynamic Spectrum Sharing System
40. UE - User Equipment
41. UUID - Universally Unique Identifier
42. USGS - United States Geological Survey
43. WInnForum - Wireless Innovation Forum

2 Examples of existing Spectrum Sharing Frameworks between Incumbent and Commercial Systems

2.1 CBRS SAS

The Citizens Broadband Radio Service (CBRS) band (3.55 – 3.7 GHz), is shared by three-tiered access system/users, i.e., Incumbent Access as the first tier, PAL (Priority Access License) as the second tier and GAA (General Authorized Access) as the third tier. There are two categories of incumbent users: the Federal (DoD) radars and the non-Federal FSS (Fixed-Satellite Service) earth stations. The DoD radars are required to be protected on a dynamic basis, while the FSS earth stations only require a static protection. The commercial users providing wireless services utilizing PAL or GAA license are required to power down or use a different frequency to ensure interference protection of a DoD radar system.

The sharing framework for CBRS mainly relies on a Spectrum Access System (SAS) that authorizes and manages use of spectrum for the CBRS PAL and GAA users so as to avoid harmful interference to incumbent users. The sharing framework to protect DoD radar system consists of a network of Environmental Sensing Capability (ESC) sensors and a SAS[1]. The ESC notifies the SAS when it senses/detects a DoD radar signature, and the SAS upon receiving notification from ESC will notify the impacted CBSD (Citizens Broadband radio Service Device) within a certain area/neighborhood to adjust its power or to relocate the transmission to different frequency, based on a pre-calculated aggregated interference of all the CBSDs in that certain area.[1]

The government-defined geographic areas where DoD incumbents could be operating are called Dynamic Protection Areas (DPAs). Areas surrounding each DPA in which CBSDs must be considered in the aggregate interference calculation into the DPA is called the DPA neighborhood. A DPA is “activated” on one or more 10 MHz CBRS channels when incumbent activity is detected to be occurring on those channels. For each DPA, every 24 hours the SASs collaboratively determine a set of CBSDs whose operating frequency range and the power must be reconfigured when incumbent activity is detected on one or more 10 MHz CBRS channels in that DPA, called “DPA Move List”. A DPA Move List is determined based upon the estimated aggregate interference from the CBSDs located inside the DPA neighborhood. CBSDs outside of the DPA Move List are unaffected by incumbent activity in that DPA. The potential for a CBSD to be included in any Move List will become less if it is located far from the DPA boundary, is transmitting at low power, and/or its antenna is pointed away from the DPA.

Reference [2] specifies the detailed requirements for incumbent protection for CBRS. Reference [3] specifies the enhancements to the calculation of the DPA neighborhood distance which drastically improve the usability of CBRS band.

[1] In a few areas, a SAS becomes aware of an incumbent activity by the use of an online portal rather than ESC.

2.2 6 GHz AFC

In the 6 GHz band, standard power 6 GHz unlicensed devices (access points and fixed client devices) are required to operate under the control of an FCC-authorized Automated Frequency Coordination (AFC) system to avoid harmful interference with licensed fixed microwave stations in U-NII-5 (5925 – 6425 MHz) and U-NII-7 (6525 – 7125 MHz), and certain radio astronomy sites in 6650-6675.2 MHz.

Per FCC 47 CFR Part 15.407(k) rules, upon daily inquiry by the unlicensed device, the AFC system provides the maximum permissible power in the inquired frequency range at all points within the unlicensed device's location uncertainty volume. For the fixed service (FS) microwave stations, the AFC system uses the FCC Universal Licensing System database and, to protect cross-border FS in Canada, the daily ISED Spectrum Management System, and computes the maximum power levels that the unlicensed device can transmit at each frequency range while meeting the single-entry I/N threshold at all FS receivers that could be impacted (considering both in-band and adjacent-channel interference). For radio astronomy, AFC systems compute the distance to each radio astronomy site in FCC CFR Part 15.407(m) and eliminates the spectrum between 6650-6675.2 MHz from unlicensed device use if that distance is less than the line-of-sight distance calculation assuming 4/3 Earth curvature. In neither case (FS or radio astronomy) is aggregate interference considered.

Note that unlicensed low power indoor devices (indoors only) and very low power devices (indoors and outdoors) are allowed to operate throughout 5925 to 7125 MHz (U-NII-5,6,7,8) without coordination with an AFC system.

WInnForum TS-1014 provides the Functional Requirements for the U.S. 6 GHz Band under the Control of an AFC system– including both the FCC rules as well as additional implementation details [6].

3 Defining Highly Dynamic Spectrum Sharing

The terminology “Spectrum Sharing” is used in different contexts in the industry and by regulators and it has many different implications. Similarly, “Dynamic Spectrum Sharing” also has multiple interpretations among various users of the terminology. Finally, “Highly Dynamic Spectrum Sharing” is being used for the first time in the industry by WInnForum. As such, it is important to have clear definitions of these terminologies so that there is a common understanding. A detailed discussion of this topic has been captured in WInnForum TR-2017, “Time Scale Interpretations of Different Spectrum Sharing Frameworks, Including Dynamic and Highly Dynamic Spectrum Sharing”[7]. In this section, only a brief summary of the essential contents from that document is presented.

3.1 Spectrum Sharing

The National Institute of Standards & Technology (NIST) uses the following definition for “Spectrum Sharing”: “Spectrum sharing is a way to optimize the use of the airwaves, or wireless communications channels, by enabling multiple categories of users to safely share the same frequency bands.” While the NIST definition was created in the context of CBRS, it is still worth noting the generic nature of its definition.

3.2 Dynamic Spectrum Sharing

In the National Spectrum Research and Development Plan [4], Dynamic Spectrum Sharing (DSS) “means adaptive coexistence using techniques that enable multiple electromagnetic spectrum users to operate on the same frequencies in the same geographic area without causing harmful interference to other users (in cases where such users have an expectation of protection from harmful interference) by using capabilities that can adjust and optimize electromagnetic spectrum usage in real time or near-real time, consistent with defined regulations and policies for a particular spectrum band.” This definition has been developed primarily in the context of lower 3 GHz (3.1-3.45 GHz) but is still very generic in nature

3.3 Highly Dynamic Spectrum Sharing

In general, dynamic spectrum sharing involves temporal apportioning of spectrum resources among various users, but the time scale of apportioning will vary upon the applications. A systematic approach is needed to establish the relative timescales as presented in this section, building from slowest “semi-static” to faster “dynamic” to eventually fastest “highly dynamic”. The three main types are described below.

It is generally assumed that the incumbents in a spectrum band will have to be protected from any harmful interference potentially caused by the use of spectrum by new entrants. The burden of interference avoidance/mitigation will lie, at least initially, on the new entrants.

3.3.1 Semi-static

This form of spectrum sharing is stable over a substantial period of time. Once the operating conditions (location, power, antenna parameters etc.) for new entrants are established, they do not change in 24 hours (e.g., AFC-managed devices in the U.S. 6 GHz band).

3.3.2 Dynamic

This form of spectrum sharing is stable over a relatively short period of time. The new entrant will have to detect operation of incumbent, decide on course of action and execute to reduce interference in a matter of "~5 minutes" (e.g., CBRS for Federal incumbents).

3.3.3 Highly Dynamic

This form of spectrum sharing is executed in a relatively fast timescale. The new entrant will have to detect operation of an incumbent, decide on a course of action (which can be pre-computed) and execute to reduce interference in a matter of "a few seconds" (e.g., to deal with airborne radar for lower 3 GHz). The requirement could be further reduced (e.g., to 1 second or even less) in the future, once more detailed studies and possibly some field trials are carried out. The key is to remember that the time scale is significantly lower than those spectrum management schemes

4 Primary User Protection Concepts

This section summarizes concepts that can be applied when sharing spectrum with an incumbent that is a Primary User in a band and it needs to be protected from interference generated from operations of Secondary Users in the band.

4.1 Planned vs Unplanned Spectrum Sharing

When a Primary User (PU) utilizes spectrum intermittently, it creates opportunities for Secondary Users (SUs) to access the spectrum during idle periods.

4.1.1 Planned Spectrum Sharing

In planned sharing scenarios, the PU can schedule its spectrum usage in advance (e.g., days, hours, or minutes) and communicate this schedule to SUs via a centralized notification system (e.g., a spectrum portal). This approach allows SUs to operate without interfering with PU activities.

Key Components:

- **PU Requirements:**
  - Publish accurate and timely usage schedules to the portal.
- **SU Requirements:**
  - Monitor the portal.
  - Adjust transmissions to comply with PU protection requirements.

Feasibility:
Current technologies support updates with granularity as low as one minute.

4.1.2 Unplanned Spectrum Sharing

When advance scheduling is not feasible, unplanned spectrum sharing relies on real-time sensing of PU activity. This method requires additional investment and coordination.

Implementation Options:

1. **PU Self-Sensing:**
   - The PU detects its own activity and communicates availability in near-real-time.
   - Treated as automated planned sharing.
2. **Third-Party Sensing:**
   - Involves external sensor networks (site acquisition, installation, backhaul, etc.).
   - Sensors must be protected from interference, potentially requiring *whisper zones*—areas where SUs do not operate.

3. **SU-Based Sensing:**
    - Sensing is integrated into SU devices, reducing infrastructure cost.
    - Challenges:
        - Requires knowledge of PU signal characteristics.
        - Must continuously monitor PU activity, which could pose security and compliance concerns.

4.1.3 Unified Framework

A common notification system or portal can be developed to support both planned and unplanned sharing models, improving coordination and spectrum efficiency.

4.2 Protected Entity and Protected Area

A Protected Entity (PE) can be defined as an entity belonging to the Primary User that operates in the band and requires interference protection.

The Protected Entities can be catalogued using different criteria. For example:

- Based on the location of the PE:
    - Fixed Protected Entity, which is a singular entity with a defined fixed location on the map
    - Mobile Protected Entity, which is a PE that can moved either in a predefined mobility area or in an arbitrary mobility area
    - Entity with distributed components that requires protection inside a Protection Area (PA)
- Based on PE activity:
    - Always Active PE – requires protection all the time
    - Intermittently Active PE
- Based on observability of PE activity:
    - Detectable PE – when PE transmits a signal (e.g. radar)
    - Undetectable PE – when PE is operating in receive-only mode (for example, radio astronomy)

The concept of Protection Area can be applied not only for a PE with distributed components, but also to protection of a Mobile PE when it is more practical to avoid tracking the real-time

position of the PE and instead protect the area where the PE is located without knowing the exact PE position. For reference, a Dynamic Protection Area (DPA) can be defined as a Protection Area that is intermittently active.

4.3 Protection Method

A simple Primary User protection approach is to allow Secondary Users to use the spectrum unincumbered while the Primary User is not active. When a Primary User's PE becomes active, Secondary Users will have to apply mitigation features that will guarantee that the interference experienced by the PE is within tolerable range:

1. Determine when the Primary User is active.
2. Estimate the interference level from Secondary Users devices towards the Primary User's active PE/PA.
3. Identify the list of Secondary User's devices that must apply mitigation/coexistence features to reduce their interference towards PE/PA.
4. Activate the mitigation/coexistence features on Secondary User's devices identified in step 3.
5. Determine when the PE is deactivated and no longer needs protection.
6. Deactivate mitigation/coexistence features, allowing the Secondary User to make full use of the spectrum.

4.3.1 Determining Primary User Activity

Accurately identifying when a Primary User (PU) is active is critical for effective spectrum sharing. Several detection methods exist, each with specific trade-offs:

4.3.1.1 Methods for PU Activity Detection

1. **PU Self-Reporting via Notification Portal**
    - Ideal when the PU can plan or report spectrum usage in real time.
    - Allows pre-scheduled ramp-down periods, enabling SUs to prepare for PU activation.
    - Risk: Overreporting or conservative declarations by the PU could reduce spectrum availability unnecessarily.
2. **PU Self-Sensing with Automated Reporting**
    - Sensors deployed by the PU detect its own transmissions and automatically update the portal.

- Minimizes manual input and enhances real-time accuracy.

3. **SU-Based Detection (Passive Sensing)**
    - SUs incorporate sensing capabilities (e.g., "RAN-as-a-sensor") to detect PU activity.
    - Requires knowledge of PU waveform characteristics to identify activity accurately.
    - Could introduce complexity and potential security/privacy concerns.
4. **Third-Party Sensor Networks**
    - Independent sensors monitor PU activity and report to the shared portal.
    - Deployment requires infrastructure (e.g., site acquisition, backhaul).
    - Sensors could need interference protection, possibly creating *whisper zones* where SU operation is limited.

4.3.1.2 Essential Detection Parameters

Regardless of the detection method, the following information must be determined and shared to enable coexistence:

- **Geographic location** of the active **Protected Entity/Protected Area**
- **Frequency range** in use by the PU during active periods

4.3.2 Estimating Interference towards Protected Entity/Protection Neighborhood

The interference level is dependent on the power level transmitted by the Secondary User's device and the signal attenuation due to the path loss between the device and the PE location. One option is using the maximum allowed device power along with a predefined propagation model to estimate the upper bound of the interference level. Using clutter information (meaning buildings and foliage along the line of sight) for the propagation model will help with the accuracy of the predicted path loss.

The following information, if available, would be useful to increase the accuracy of the predicted interference level:

- PE location (longitude, latitude, height)
- PE antenna orientation (azimuth, tilt)
- PE antenna characteristics
- Secondary User device location (longitude, latitude, height)

- Secondary User device antenna orientation (azimuth, tilt)
- Secondary User device antenna characteristics
- Secondary User device transmit power
- Terrain and Clutter information

For a PA/DPA, the interference level can be estimated for a grid of points located inside the area, and the maximum estimated interference level among all the points can be used.

4.3.3 Calculation of the direction from the base station to the Protected Entity

The azimuth and elevation angles (θ_R and φ_R) of the line between the base station main beam and the Protected Entity location relative to the base station antenna boresight direction are calculated by using the following equations:

$$\theta_R = \alpha - az$$

$$\varphi_R = \beta + \cos(\theta_R) \cdot \tau$$

where:

az is the base station antenna main beam pointing azimuth
τ is mechanical downtilt

Figure 1 represents the orientation of the base station relative to the global coordinate system. The azimuth angle az, in the global xz-plane, describes the orientation of the base station antenna boresight (z' axis) and is positive clockwise from True North. The mechanical downtilt τ describes the elevation angle of the antenna boresight direction. Additionally, 2 shows the orientation of a victim receiver (which could be a Protected Entity) in the global coordinate system described by the azimuth angle α to the projection of the Protected Entity into the xz-plane. The azimuth angle α is positive clockwise from True North. The elevation angle β towards the Protected Entity is positive above horizon (towards the sky) and negative below horizon (towards the ground).

The mechanical downtilt τ is explicitly required to be from -15 to 15 degrees due to limitations in the approximations used to calculate antenna gain patterns.

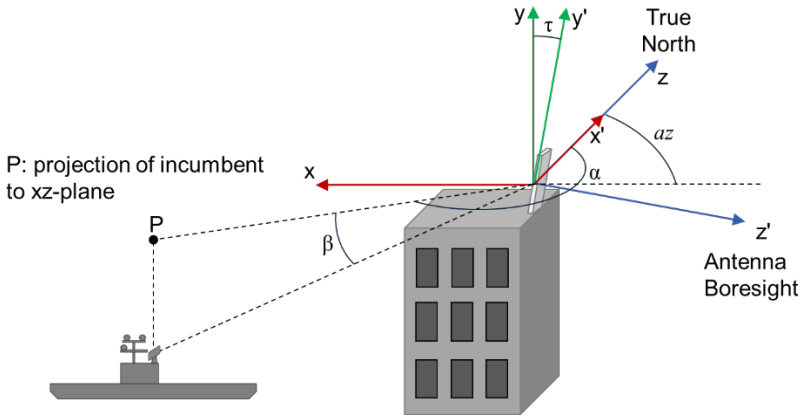

Figure 1 Global coordinate system illustration

The orientation of the base station is described by the azimuth angle az relative to True North and the mechanical downtilt angle τ. The position of the Pprotected Eentity is given by the azimuth angle α, and the elevation angle β.

4.3.4 Identifying the List of Secondary User Devices that Must Apply Mitigation Features

Assuming that the interference level tolerated by a Primary User's PE is known and specified by an Interference Protection Threshold (IPT), one way of protecting the PE would be to estimate the interference level from Secondary Users' devices and make sure that interference is lower than the tolerated interference threshold.

A "Protection Neighborhood/Coordination Area" can be defined as an area around the PE or PA where the deployed Secondary User devices have the potential to cause relevant level of interference towards the PE/PA. For the same PE/PA, there could be several protection neighborhoods defined, depending on the characteristics of Secondary User devices, for example the maximum power level used for transmission.

The following figure provides an illustration of the Protected Entity and the Protection Neighborhood.

Figure 2 Protection Neighborhoods

Protection Neighborhoods are used to limit the number of Secondary User devices that are analyzed when determining the interference impact towards the PE/PA. For example, in the figure above $Radio_1$ and $Radio_2$ are part of the PE Protection Neighborhood and will be part of the list of devices that might have to apply mitigation features when PE becomes active. $Radio_3$ and $Radio_4$, on the other hand, are outside the Protection Neighborhoods for any of the Primary User PE/PA and they will be able to operate unencumbered regardless of the activity of the Primary User.

In general, if a Secondary User device is located inside a Protection Neighborhood, it can operate unencumbered as long as the PE/PA is not active (however, there could be cases when the PE/PA is always active). When the PE/PA becomes active, if a Secondary User device frequency range overlaps with the frequency range of the PE, then, if necessary, it must adapt its behavior by applying mitigation features that will limit the interference generated towards the PE/PA.

4.3.5 Activating the Mitigation/Coexistence Features on Secondary User Devices

Secondary User device can apply different mitigation/coexistence features to limit interference towards the incumbent. Some examples of the mitigation features that can be applied:

- Stop transmitting the entirety of signals that overlap with the frequency range used by PE
- Avoid transmission in the frequency range used by the PE (e.g. PRB blanking), which allows only portions of the signals to be affected
- Reduce transmission power

- Using beamforming, create a null in the direction of the incumbent

4.3.6 Determine when the PE is Deactivated and no longer needs Protection

Similar to step 1, this can be done in multiple ways, including via a portal or using sensing of PE activity.

4.3.7 Deactivate Mitigation/Coexistence Features

For the impacted Secondary User devices, the previously applied mitigation/coexistence feature will be deactivated. It will be up to the Secondary Users to decide if they will return to the original operation mode or if they will choose to avoid frequency ranges with a history of high activation rates that are deemed to be too unstable to be useful.

4.4 Spectrum Usage Timeline for Primary and Secondary User

Figure below shows the timeline for spectrum usage by the Primary and Secondary Users.

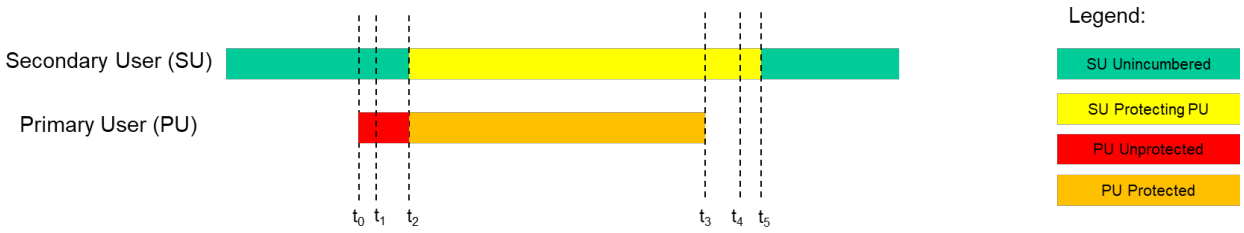

Figure 3 Timeline for shared spectrum usage

The green portion represents the time when the Secondary User has unencumbered access to the spectrum. The yellow portion represents the time when the Secondary User has activated the mitigation/coexistence feature required to protect the Primary User and has limited access to the spectrum. The red portion is when the Primary User has started using the spectrum, but its operation is not protected from interference. The orange portion is when the Primary User is protected against interference from Secondary User.

The following times are marked in the figure above:

t_0 – is the time when the Primary User has started using the spectrum;

t_1– is the time when the Primary User spectrum activity has been detected;

t_2 – is the time when the Secondary User has activated the mitigation/coexistence features;

t_3 – is the time when the Primary User has stopped using the spectrum;

t_4 – is the time, after the cool-off period, when the Primary User is considered no longer active;

t_5 – is the time when the Secondary User has deactivated the mitigation/coexistence features.

The following time periods are relevant:

- Primary User activity detection time (t_1-t_0)
- Activation of Primary User protection (t_2-t_1)
- Cool-off time after Primary User stops using the spectrum (t_4-t_3) to implement obfuscation of incumbent activity and/or to avoid hysteresis effects if the incumbent is inactive for only a brief period of time
- Deactivation of Primary User protection (t_5-t_4)

5 Closed Loop Interference Feedback for More Robust Spectrum Sharing

An adjustable interference threshold can be applied by using a feedback loop on coordination. Figure 4 shows and example of closed loop mechanism for adjustable interference threshold. In the loop, the Federal System is the Primary User and always monitors the interference and updates this information to a portal, and the non-Federal/Secondary Users read the information in that portal. If the Primary User detects harmful interference, the interference threshold will be decreased (more stringent). Otherwise, it can be increased (relaxed). The Secondary Users adjust their operations based on the updated information on the detection of harmful interference.

Some potential benefits of this methodology:

- Maximizes access to the spectrum.
- Feedback reduces reliance on propagation/clutter modeling in coordinating shared access.
- The Primary User is protected from Aggregate Interference without the complexity of aggregate interference calculation.

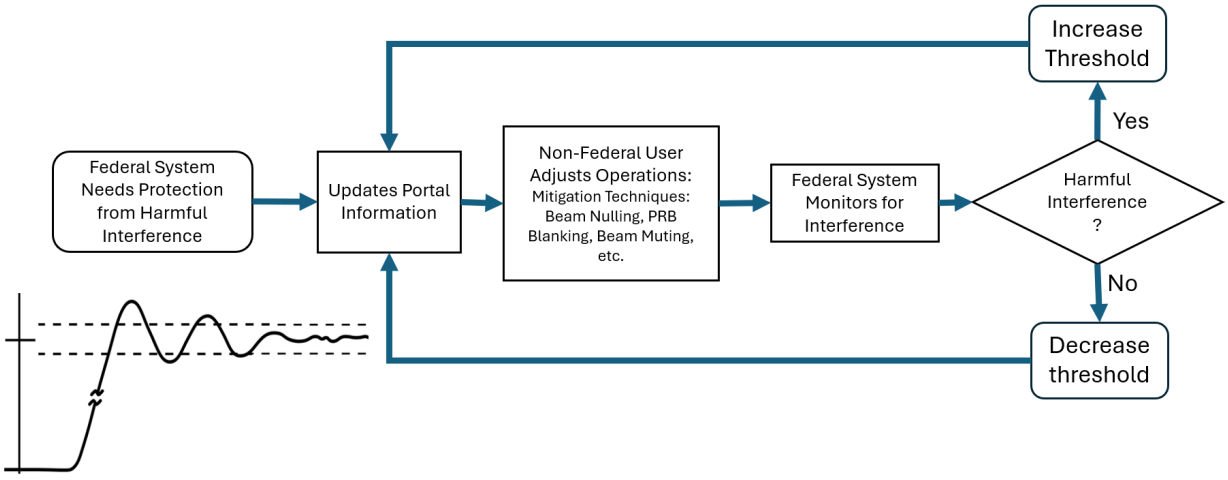

Figure 4 Closed Loop for Adjustable Interference Threshold

In theory, the closed-loop feedback can be implemented in a centralized, decentralized or hybrid system. In a centralized system, the Primary User updates the protection threshold to the portal which is read by a centralized controller which manages Secondary Users:

- If any harmful interference is detected, the Primary User escalates the protection threshold by immediately sending updated value to the portal.
- If no harmful interference is detected in a certain period (e.g., 30 minutes), the Primary User must relax the protection threshold and send that updated value to the portal.

After receiving the updated protection threshold from the portal, the centralized controller recomputes the maximum power that each Secondary User in the neighborhood of the Primary User can transmit and then sends it to the corresponding Secondary Users.

In a decentralized system, Secondary Users (or their domain proxy) interact with the portal directly, and increase or decrease their transmission powers in response to the protection threshold changes. In a hybrid system, some Secondary Users are managed by the centralized controller while others act independently.

5.1 Initialization

When a Secondary User initiates transmission (at deployment or after maintenance) it needs to know the allowable transmit power to protect the Primary User. The Primary User does not provide this information in the portal. If the Secondary User transmits full power according to regulatory limits, it could cause interference to the Primary User located nearby causing the Primary User to increase its protection threshold. This could cause other Secondary Users in the area to reduce their transmit powers unduly, creating an unfair spectrum sharing situation. The transmit power limit can be determined by measurement or modeling interference to the incumbent using its location which is obfuscated to a degree for security, and its protection parameters. This can be done by the Secondary Users directly in a decentralized system or by the centralized controller that manages the Secondary Users. Another solution is to have neighborhood and whisper zones around each Primary User location informing Secondary Users their initial transmit power limits based on their antenna parameters. The latter solution is not as accurate as the first solution as the zones can only approximate the propagation loss between the two systems.

5.2 Discussion

The implementation feasibility and security aspects of de-centralized and hybrid systems need to be studied. Also, the feasibility of centralized systems in controlling access to a system with low latency requirements needs to be studied.

6 Solutions Based on a Notification System

6.1 Example of Airborne Radar Protection using Portal-activated DPAs

The following method is applicable if the Primary User would consider planned spectrum sharing or self-sensing (for example, the portal can start activating a DPA as soon as the plane takes off, and then it can use GPS position to active/deactivate DPAs).

This approach is using existing technology proven to work in CBRS. In the highly-dynamic case, portal-activated DPAs are defined to cover CONUS. The DPA diameter could be approximately 200 km, which means that the plane would take 20 min to traverse the DPA at a cruising speed of 600 km/h. The DPAs can be distributed in a 21 x 14 honeycomb matrix, as shown in the figure below. If the plane is operating at a higher speed than the normal cruising speed, there is an option to activate a cluster of DPAs to reduce the rate of DPA activations/deactivations. The following figure illustrates the DPA matrix, with the red DPA being active, the dotted red line represents the Protection Neighborhood of the DPA and the red arrow represents the plane's travelling direction.

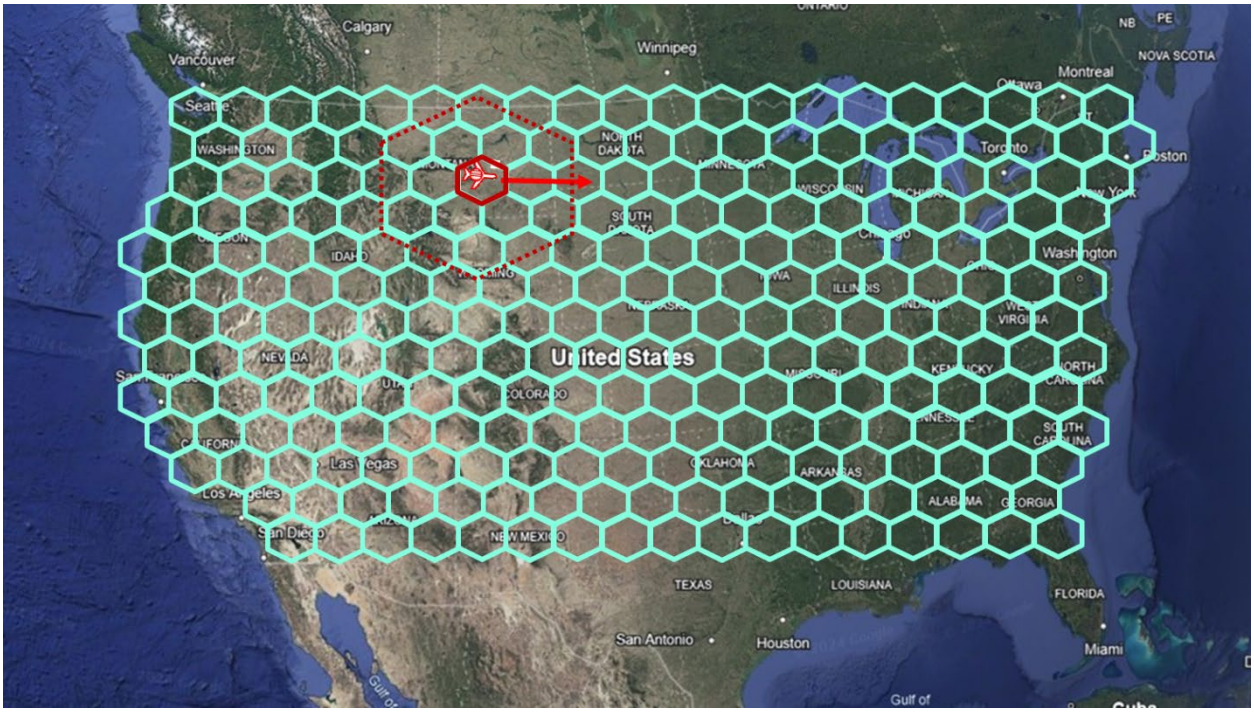

Figure 5 Airborne radar protection using Portal-activated DPAs

DPA Protection Neighborhood size needs to be determined. All radios inside an active DPA could stop transmission or apply other interference mitigation methods in the frequency range(s) identified for protection for the airborne radar. Operation of radios in the DPA's Protection Neighborhood needs to be assessed based on interference contribution.

6.2 TARDyS3

6.2.1 TARDyS3 in CBRS

TARDyS3 (Telecom Advanced Research and Dynamic Spectrum Sharing System) is an example of a portal. It is a DoD calendar-based tool that controls the activation/deactivation of the portal-managed DPAs (P-DPAs). To reference the P-DPAs, a JSON object provides the immutable UUIDs (Universally Unique Identifiers) used by TARDyS3. This JSON object is included in a file which is accessed approximatively every five minutes by all SAS admins.

TARDyS3 and the SASs do not interface directly. Instead, TARDyS3 notifies SASs by sending upcoming events to an HTTP storage proxy (referred to as the proxy), and the SASs retrieve the data from the proxy. Both TARDyS3 and the SASs send or retrieve data autonomously. The proxy is access-controlled and managed by the National Telecommunications and Information Administration (NTIA).

TARDyS3 sends DoD spectrum use events in portal-activated DPAs by pushing the data via an HTTPS PUT request to the proxy server. The SASs connect to the proxy server and pull the data by performing an HTTPS GET request. The data includes the date, start and end times, frequency channel, and location for each event. The payload is sent as a JSON payload.

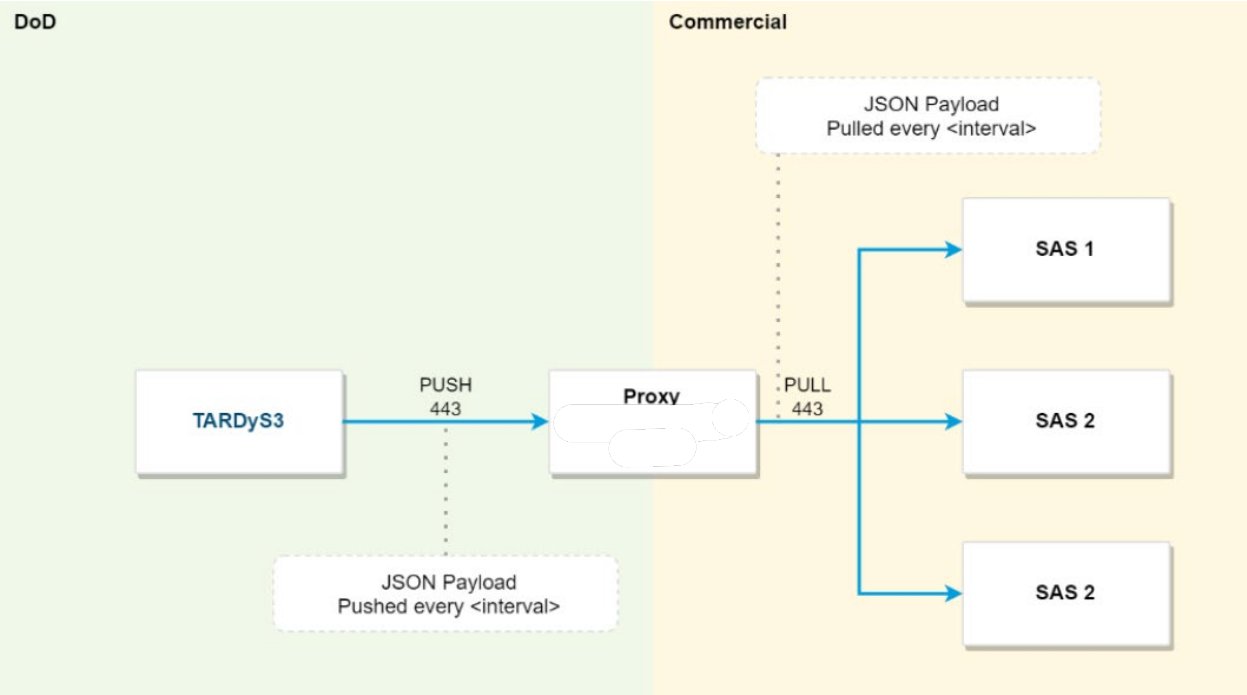

Figure 6: TARDyS3-SAS Interface Architecture

TARDyS3 can read and write to the proxy server. SASs only have read access.

System	Protocol	Method	Access
TARDyS3	HTTPS	GET/PUT	Read/Write
SAS	HTTPS	GET	Read

The SASs can handle the data that they pull from the proxy server multiple ways:

1. Translate the data from the proxy into the SASs' commercial calendar system. This allows SASs to continue to utilize the current API between the SAS and the calendar system, where a data interchange layer pulls from the proxy and pushes it to the calendar system.
2. Read from the proxy directly. SASs can pull data directly from the proxy without using the existing commercial calendar system.

TARDyS3 sends the data package as often as needed to communicate scheduled DoD events:

- Within five minutes of an event being approved if it is within 72 hours of the start date.
- At least once every 24 hours. In cases where the schedule data has not changed, the 24-hour push is used to indicate the system health from TARDyS3 to the proxy.

SASs pull the data package as often as needed:

- Every five minutes to confirm changes in schedule data.
- If there is no new data over a 24 hour period, SASs continue with the most recent data.

Once an updated schedule is received, DoD expects that SAS operations reflect the current status of DoD's scheduled events, and that SASs adjust channel plans accordingly to avoid harmful interference to DoD.

6.2.2 Proposals for TARDyS3 in 3.1 GHz band

the use of the JSON object mentioned in section 6.2.1 can be extended to all kinds of federal incumbents (DPA, FSS, …) that exist in 3.1 GHz band. In addition, this JSON object must contain the protection threshold. Therefore, this parameter can be removed from the kml file (for DPA) or the specification document (for FSS).

```
{
        "AMERICAN_SAMOA": {
        "id": "aaaa,"
        "name": "AMERICAN SAMOA,"
        "protectionThreshold": -144,
        "deprecated": false
            },
        "BARKING_SANDS": {
        "id": "bbbb,"
        "name": " BARKING SANDS ,"
        "protectionThreshold": -144,
```

"deprecated": false
},
…

}

With this mechanism, updating the value to the JSON file, the Primary User can adjust the protection threshold more conveniently and rapidly as discussed in section 5 of this document.

7 Solutions Based on Sensing

RAN or user equipment-based sensing are attractive solutions for which technology and implementation feasibility need to be further studied. Some use cases and frameworks in which the user equipment-based sensing could provide benefits are further discussed in this section.

Sensing to enable spectrum sharing can be performed by either (or both) RAN and UE/Devices designed to sense clutter loss (also called "Clutter Mapping") or presence of incumbent signal(s). Clutter loss sensing could leverage a sense-by-measurement of clutter to determine isolation between incumbent(s) and secondary users (also applicable for dividing access among secondary-to-secondary users). Incumbent signal sensing would be targeted to sense presence of incumbent or secondary signals at sites designed for that purpose to determine, then decide the incumbent's access and derivative secondary user assignments. This section describes these approaches.

7.1 RAN -Assisted Clutter Mapping & Sensing

In CBRS, a Spectrum Access System (SAS) enables spectrum sharing among commercial systems and incumbents while avoiding harmful interference to the latter.

To determine the potential for harmful interference, SAS applies statistical modeling such as the Irregular Terrain Model (ITM) to estimate RF propagation loss between commercial transmitters and incumbent receivers. Commercial systems are often deployed in urban and suburban environments with antennas situated below clutter, such as buildings and vegetation. The signals from these radios undergo additional (clutter) losses before reaching the incumbent. ITM doesn't model clutter loss. ITU-R P.2108 model is used to determine clutter loss for commercial systems with antenna height below 6 m. Although the use of the clutter loss model is helpful in making more spectrum available for commercial systems, it does not address the situation where the antenna height is above 6 m but still much lower than surrounding clutter. A majority of commercial systems fall in this category. In order to account for clutter loss for such systems, clutter height / loss determination has to be done with reasonable accuracy to avoid the risk of harmful interference to incumbents. If good clutter information was not available, then one would have to account for zero clutter loss to avoid the risk of harmful interference. For a band like 3.1 GHz that has a large number and type of incumbent systems, not accounting for clutter loss in a majority of deployment scenarios would severely limit the amount of spectrum available for sharing with commercial systems.

Sensing enables site-specific clutter loss determination with high accuracy which makes spectrum sharing more efficient and robust without the risk of harmful interference. This is performed in two ways: (a) using external ("sounding") reference signals and (b) using the network's own (internal) reference signals. The following section describes each of these two approaches in more detail.

7.2 RAN-Embedded Clutter Sensing Using External Signals

7.2.1 RAN-Embedded Isolation & Spectrum Occupancy-Based Sensing (OBS)

This method utilizes external signals (i.e., signals not transmitted by the network) to provide clutter probe sounding signals used to generate 3D clutter mapping data. These external signals must be globally available, present continuously transmitted ray paths over most horizonal and azimuthal entry angles. Examples include GPS, GNSS, ADS-B, as well as emerging low earth orbit PNT (LEO PNT) signals. These candidate sounding signals are optimal for measuring mid-band, currently regarded by regulatory bodies to fall between 1 GHz and 15.35 GHz[1] propagation through building entry/exit as well as other outdoor morphologies. PNT and GPS signals are particularly well suited for clutter mapping since these have uniform signal intensity over the earth's surface. This characteristic makes these also appropriate for wide area differential-loss measurement, using conventional reference stations to build site-specific maps of clutter within the propagation path(s) of interest. These are then used by spectrum management systems to coordinate and assign spectrum access.

External signal clutter sensing employs a differential-loss method that begins with known non-cluttered ground-reference signal of known intensity. These are compared to site measurements taken by embedded sensors at transmission sites, resulting in a precise site-specific clutter loss value for each azimuth/elevation angle sounding. This method facilitates 3D clutter loss mapping, particularly useful for low power dense, to high power microcell measurements to ascertain, coordinate or adjust each site's directional transmission so as to not interfere with incumbent spectrum operations across air, surface, and maritime domains.

External signal clutter loss data are collected continuously as satellites and/or airborne sources traverse the sky, horizon to horizon. If GPS or GNSS functions are already integrated into the RAN, then RAN-embedded sensing may also support other functionalities such as UTC time synchronization and remote sensing.

External signal clutter mapping leverages electromagnetic reciprocity principles, meaning the loss encountered in-bound is the same as the target transmission's path loss encountered out-bound. The embedded external signal sensor, with cloud-based DSP support, collects 3D loss values reflecting variations due to composite ambient conditions (reflective, diffractive or absorptive losses). These cumulative variations are observed along each inbound path where clutter interacts with and attenuates signal strength. Since path loss is directionally independent, differential-loss clutter maps can be generated—effectively 3D data images representing radio isolation arising from surrounding clutter. These clutter maps can be further processed using 3D polar coordinates to intelligently and proactively manage the incumbent's electrospace to avoid incumbent interference. Appendix B at end of this document contains information regarding implementation and additional propagation measurement features for internal and external signal (OBS) sounding approaches.

[1] Among multiple sources, refer to US FCC DA 23-296 April 12, 2023, OFFICE OF INTERNATIONAL AFFAIRS SEEKS COMMENT ON RECOMMENDATIONS APPROVED BY THE WORLD RADIOCOMMUNICATION CONFERENCE ADVISORY COMMITTEE, IB Docket No. 16-185. "*Op-Ed: Spectrum Sharing: Preparing for WRC-27*", August 12, 2024, Fierce Wireless

7.2.2 OBS Features

Frequency-Dependent Loss Management: Embedded isolation measurements use sounding transmissions at frequencies below the frequency ranges or bands of interest. These signals, such as those at the lower end of the mid-band, are suitable for estimating transmission losses. A substantial body of empirical research reveals that building materials and foliage transmission loss rise modestly following an upward attenuation slope as a function of rising carrier frequency. In a comprehensive peer review 2017 study[1] of many building types, across carrier frequencies between 1GHz to 30 GHz, the measured attenuation presents a loss difference attributable to carrier frequency attributed loss just under 1dB per 1 GHz rise in carrier frequency. Therefore, use of external sounding signals and the loss difference at the lower frequency bound is conservative (since the sounding measurement presents less loss than is estimated for any higher carrier frequency loss). Thus, this method is optimal to protect incumbent operation based on marginally greater loss occurring at higher mid-band frequencies. Exterior clutter field map data also includes near- and far-field losses, such as surrounding urban/suburban and terrain within the field of view.

Capture of clutter dynamics subject to changing field conditions. Clutter characteristics often change, thus propagation loss also changes. Moveable obstructions, reflectors, scattering, and diffractive surfaces can impact propagation and the extent of clutter isolation between co-channel users. A relatively common case in private network are loading docks where raising/lowering dock doors change relevant path loss 15-20 dB or more. Therefore, capturing changes in isolation becomes important, especially for aggregate interference cases.

Waveform and Band Flexibility: OBS sharing is waveform-agnostic and supports clutter mapping and occupancy profiling across any mid-bands. This approach supports both co-channel and adjacent-band protection over a broad mid-band spectrum region.

[1] I. Rodriguez, H. C. Nguyen, I. Z. Kovács, T. B. Sørensen and P. Mogensen, "An Empirical Outdoor-to-Indoor Path Loss Model From Below 6 GHz to cm-Wave Frequency Bands," in *IEEE Antennas and Wireless Propagation Letters*, vol. 16, pp. 1329-1332, 2017, doi: 10.1109/LAWP.2016.2633787

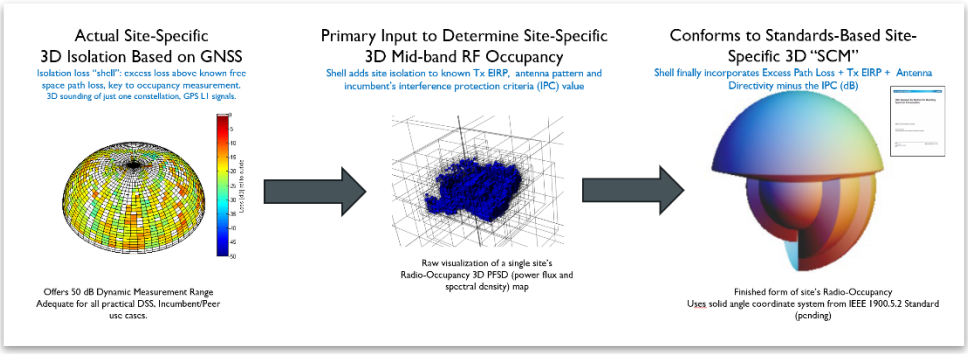

Figure 7 External Signal Clutter Losses combine with Site-Specific Antenna, Transmitter Power Data to Form IEEE 1900.5.2 Occupancy Spheroid

Role of the Spectrum Manager in OBS: Using OBS, central (or distributed) spectrum management intelligence, spectrum management assignment, notification and coordination can be proactive. Calculation of interference margin can be performed in advance of open or classified incumbent spectrum operations. This measure exploits presence of occupancy information in advance of multiple transmissions during peak demand for instance. It also enables the incumbent to optimize their access using tools such as Digital Twins. It also can establish fairness among secondary civil agency, and private sector users. Classified operations are also supported including meeting access obfuscation requirements that avoid detection or prediction of military operating frequencies.

Flexible, Mission-Specific Incumbent Protection Criteria (IPC) Threshold Setting within the Spectrum Manager: IPC, or interference thresholds, can vary by mission or system requirements. The Institute for Telecommunication Sciences (ITS) and NTIA identified a range of IPC thresholds between -1 to -10 dB I/N for "interference protection criteria for realistic channel conditions"[1], the 2025 DoD ADSSD demonstration project will initially set the threshold to a middle value of -6 dB I/N IPC. This builds on previous work by ITS published in 2014[2]. The Spectrum Manager should anticipate supporting flexible IPC thresholds to avoid upset to demanding mission-critical operations while enabling access to the most amount of spectrum.

7.3 RAN-Embedded Clutter Sensing using Internal Signals

Integrated Sensing and Communication (ISAC) is a 3GPP technology candidate with promising potential. ISAC integrates sensing and location of passive (not connected) objects into the mobile communication network, expanding the network's functionality beyond just communication. The integrated sensing and communication capability of a wireless communication system could sense surrounding clutter, e.g. buildings, vegetation, etc. It could determine clutter location, size, shape, etc. using time delay of arrival and reflected signal strength measurements. A scattering

[1] Achatz, R et al, " Interference Protection Criteria for Realistic Channel Conditions, NTIA ITS, 2022 IEEE Symposium on Electromagnetic Compatibility and Signal Power Integrity, 2022. doi: 10.1109/EMCSI39492.2022.9889623

[2] F. Sanders, et al. "EMC Measurements for Spectrum Sharing between LTE Signals and Radar Receivers," NTIA TR-05-507. July 2014. https://www.its.bldrdoc.gov/publications/2760.aspx

cross section of the clutter could be developed to identify scattering losses as a function of incident and scattering angles as shown in the figure below.

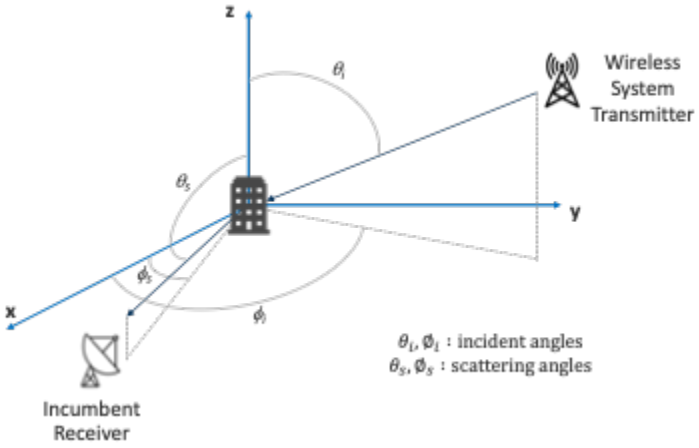

Figure 8 Clutter Mapping via Internal Signal Diagram

7.4 RF propagation via scattering

Information about clutter surrounding a wireless communication system can be used to determine additional RF propagation loss due to clutter (clutter loss) in the direction of another system, such as an incumbent Navy radar system or a higher-tier system requiring protection. RF propagation loss can be used to estimate interference potentially caused by the wireless communication system to other systems. Improved interference estimates which include clutter effects can be used to enhance spectrum sharing between systems. Interference estimation can be done by the wireless communication system itself or a spectrum access system that controls spectrum access for multiple wireless communication systems.

Clutter loss can be calculated as follows.

Lc=LTX-SC+LSC-RX

where LTX-SC is the additional loss between the transmitter of the ISAC capable wireless communication system and the surrounding clutter, and LSC-RX is the additional loss between the surrounding clutter and the incumbent (or higher-tier user) receiver.

If the surrounding clutter is blocking the line-of-sight path between the transmitter and the receiver, the signal undergoes diffraction along the path to the receiver. In this case, LTX-SC can be estimated by using the “height gain loss” formula of the Okumura-Hata model. If the clutter is not in the path between the transmitter and the receiver, the signal undergoes scattering at the clutter to reach the incumbent receiver. In this case, LTX-SC is the scattering loss in the direction of the receiver which is determined from the scattering cross section of the clutter developed using sensing.

The loss between the surrounding clutter and the incumbent receiver LSC-RX can be estimated by using the Okumura-Hata model or the Irregular Terrain Model (ITM). Terrain and clutter heights along the profile between the surrounding clutter and the incumbent receiver can be used for this purpose. Terrain heights can be obtained from the United States Geological Survey (USGS). Clutter heights above terrain can be obtained from Light Detection and Ranging (LiDAR) or National Land Cover Database (NLCD).

7.5 RAN-Augmented Incumbent-Presence Sensing (Hybrid Sensing)

7.5.1 Hybrid Sensing Introduction

In the context of this section, we explicitly define the term “Hybrid Sensing” as meaning the sensing system is a Hybrid of *both* centralized standalone sensors *and* distributed sensors, where the distributed sensors only *augment* the centralized standalone sensor. By “Hybrid RAN-Augmented Incumbent-Presence Sensing” we specifically mean a hybrid where RAN-based incumbent sensing augments standalone dedicated incumbent sensors. That is, one utilizes RAN-based sensing (where RAN Base Station sensing and measurements as well as--when useful--UE-based measurement) creating a multi-sensor fusion capability that improves the overall incumbent detection function beyond that of standalone sensors (that is, those dedicated sensors *not* also augmented with distributed sensors).

7.5.2 Hybrid RAN-Augmented Sensing is just another form of Diversity Combining:

This approach builds on mature, well-understood technology rather than requiring any radical conceptual leaps. Multi-sensor fusion as outlined here is essentially just another form of diversity combining, an already proven design and engineering approach in long-operational systems like MIMO, cellular base stations, WiFi, radar, and GPS.

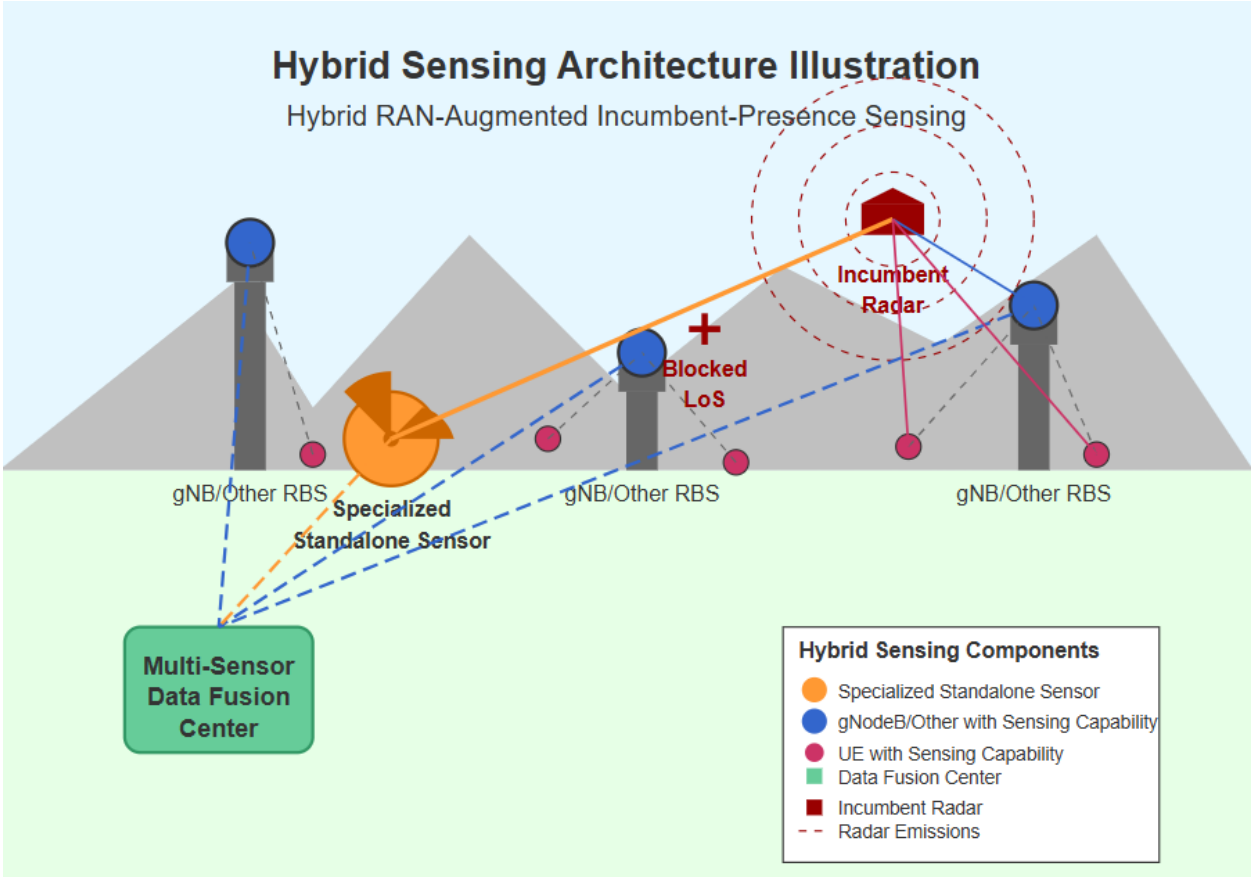

Figure 9 Hybrid Sensing Architecture Illustrative Example

The visualization above illustrates a fundamental advantage inherent in fusion-based Hybrid Sensing systems. The diagram shows how distributed sensing elements (both base stations and UEs) can overcome line-of-sight limitations that challenge standalone-only sensors. When one specialized standalone-only sensor's view is blocked by terrain or obstacles, multiple distributed nodes with lesser per-sensor capability can still actively, mono- or multi-static, as well as derivatively (via measurements perturbation) sense the radar energy emissions and relay this information to a central fusion center to augment the central standalone-only sensor.

A geo-distributed Hybrid Sensing approach provides additional value in tactical environments where radar emissions can be deliberately intermittent, low-power, non-cyclostationary, or utilize various other LPI/LPD (Low Probability of Intercept/Low Probability of Detect) and/or obfuscation techniques.

While Hybrid Sensing approaches have some benefits as outlined in the following sections, to better understand engineering and market-development considerations, further study is still required to understand the impact from:

- RAN requirements for sensing on the RAN network performance, e.g. spectral efficiency impact from required quiet periods

- Whisper zones required to protect the standalone sensors
- RAN deployment aspects such as antenna orientations and beam patterns. They, for example, may not be optimal from sensing capabilities point of view
- Cost, e.g. associated with RAN radio unit receiver level sensitivity requirements or other required enhancements to sense non-mobile communication-based waveforms in asynchronous environments.

7.5.2.1 Diversity Combining & Multi-Sensor Fusion's Information Theory Foundation:

Bottom Line Up Front

- Building on proven diversity combining principles already deployed in operational systems
- Information theory provides mathematical proof multi-sensor fusion works when implemented correctly, Hybrid Sensing could deliver probably superior detection performance over standalone sensors

Hybrid Sensing (i.e.: RAN-Sensing as augmentation to standalone sensor)

- By definition includes everything a standalone sensor offers (+ more sensors)
- Is expected to perform at least as well as a single-instrument standalone sensor

As a superset of a single-instrument sensor, outperforms in overall information extraction, redundancy, and geometric diversity

Core Information Theory Principle

- Information content of multiple independent sources is additive.
  - Note: In the case of RAN-sensing there will be upfront as well as steady-state & smaller-magnitude sensor fusion/learning delays to realizing this additivity.
- Different sensors capture different aspects of reality with uncorrelated errors
- When one sensor makes a mistake, others don't necessarily make the same mistake

How Independence Creates Information Gain

- Independent measurements can resolve ambiguities that single sensors cannot
- Combined measurements provide additional constraints to help eliminate false possibilities
- Entropy reduction through multiple perspectives on same phenomenon

Mathematical Fusion Advantage

- Mathematically optimal way to combine independent noisy measurements
- Fused estimate variance is expected to be always smaller than any individual sensor
- Direct translation from variance reduction to information gain

Complementary Information

- Each RAN base station provides, for instance, unique geometric positioning and multipath signatures
- Different angle-of-arrival measurements and propagation characteristics
- Total information approaches the sum of individual contributions minus overlap

ROC (Receiver Operating Characteristic) Performance Enhancement

- Standalone Sensor: Single ROC curve with classic Pd vs Pfa tradeoff
- Hybrid Sensing:
  - Is expected to shift entire ROC curve outward
  - Could simultaneously achieve higher Pd AND lower Pfa
  - Targets to exploits uncorrelated noise and diverse detection statistics

Proven Diversity Combining in Current Systems

- MIMO systems routinely combine multiple antenna signals for improved performance
- Cellular base stations use antenna diversity to combat fading and multipath
- WiFi access points employ spatial diversity for reliability and throughput
- Radar systems implement diversity across frequency, polarization, and spatial domains
- GPS receivers combine multiple satellite signals with different geometric dilution factors
- These established techniques demonstrate diversity combining is mature, well-understood technology

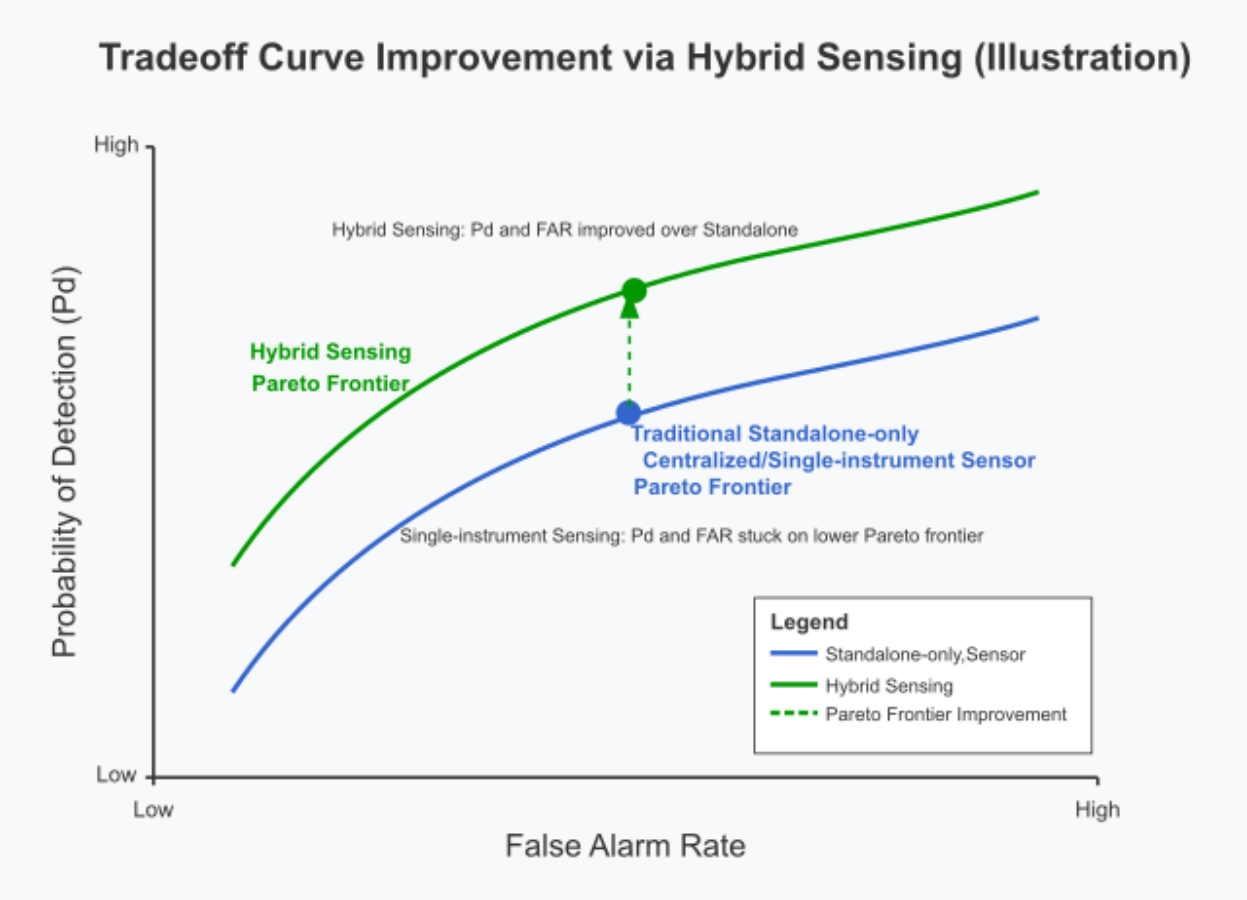

Figure 10 Expected Tradeoff Curve Improvement via Hybrid Sensing

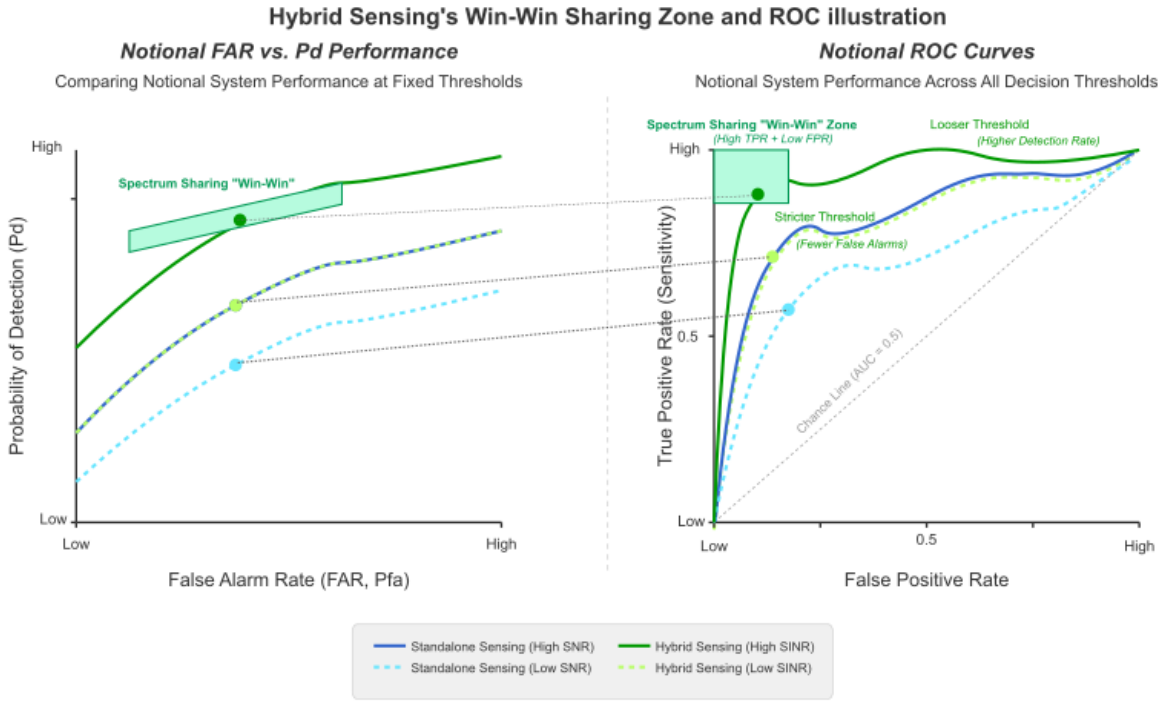

Figure 11 Expected Hybrid Sensing's Win-Win Sharing Zone and ROC Curves illustration

The lower chart demonstrates the potential categorical advantage of a Hybrid Sensing augmentation vs simply a standalone sensor. While as noted a traditional single-instrument standalone-only sensor operates along a *fixed* tradeoff curve between probability of detection and false alarm rate (blue line), the Hybrid Sensing RAN-as-a-Sensor augmentation approach shifts this frontier upward (red line), potentially allowing *simultaneous* improvement in *both* metrics. While multi-sensor fusion is simply another in a long line of diversity combining techniques demonstrating clear benefits over single-instrument sensors, it enjoys its own growing theoretical and practical systems trajectory since the 1950's.[1]

Note the ROC curve represents the fundamental tradeoff every detection system faces. Consider a security system monitoring for threats: setting high sensitivity catches all real threats (high Probability of Detection, Pd) but triggers frequent false alarms from benign events (high

[1a] R. Thompson et al., "False positive analysis in RF-based drone detection systems," in *IEEE International Conference on Acoustics, Speech and Signal Processing*, 2021, pp. 2560-2564.
[1b] Federal Aviation Administration, "UAS Detection Systems—Technical Considerations," Technical Report UAS-TQ-01-UL, 2020.
[1c] F. Hoffmann et al., "Future Countering Unmanned Aerial Systems," *NATO Science and Technology Organization*, STO-TR-SCI-301, 2020.
[1d] NATO Communications and Information Agency, "Class I Unmanned Aircraft Systems (UAS) tracking, classification and identification challenge," JISR Services & Innovation and Data Science, The Hague, Netherlands, Feb. 12, 2021.
[1e] R. Zhang and J. Cao, "Radar-communication integration for UAV detection: Challenges and opportunities," *IEEE Communications Magazine*, vol. 59, no. 5, pp. 112-118, 2021.
[1f] M. Ritchie et al., "Micro-drone RCS analysis," in *IEEE Radar Conference*, 2016, pp. 1-5.
[1g] K. Johnson et al., "Limitations of RSSI-based localization for moving aerial targets," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 56, no. 4, pp. 3458-3471, 2020.
[1h] F. Fioranelli et al., "Optimal combination of radar and optical sensors for humanitarian demining based on information theory," *IET Radar, Sonar & Navigation*, vol. 15, no. 6, pp. 577-587, 2021.
[1i] Defense Advanced Research Projects Agency, "Signal Processing at the Physical Layer (SPPL)," Technical Report DARPA-BAA-21-17, 2021.

Probability of False Alarm, Pfa). Low sensitivity reduces false alarms but risks missing actual threats.

The ROC curve maps this tradeoff by plotting Probability of Detection versus Probability of False Alarm. Each point represents a different detection threshold. A perfect detector would achieve 100% detection with zero false alarms, but real systems require compromise.
A single sensor operates along one specific ROC curve determined by its signal-to-noise ratio and detection algorithm. Adjusting thresholds merely moves along this fixed curve, trading detection probability for false alarm rate.

Multi-sensor fusion fundamentally changes this constraint. Properly combining diverse sensors shifts the entire ROC curve outward. This breaks the traditional single-sensor limitation.
This explains why RAN-based sensors augmenting the specialized sensor is compelling. Rather than incremental improvement, it enables the possibility to operate on a fundamentally superior ROC curve, delivering detection performance the standalone sensor cannot achieve regardless of parameter tuning.

The detection system's performance metrics—probability of detection (Pd) and false alarm rate (FAR/Pfa)—help improve the critical balance between competing stakeholder interests in spectrum sharing frameworks. For new spectrum entrants/secondary users, high false alarm rates translate directly to lost transmission opportunities, unreliable service quality, and poor economics. Each false alarm forces secondary users to vacate or avoid spectrum unnecessarily, potentially rendering spectrum sharing arrangements less viable in high-FAR (Pfa) environments. For incumbent users, low detection probability represents a significant threat to critical systems that often cannot always be easily modified once deployed. Military radar and satellite infrastructure with decades-long lifecycles could experience harmful interference when legitimate signals go undetected, compromising mission-critical functions and potentially putting lives at risk in tactical scenarios.

The Hybrid Sensing approach addresses this fundamental tension by enabling a simultaneous improvement in both metrics. This can create a true "win-win" scenario where incumbents gain better protection against interference while new entrants experience fewer false alarms and more usable spectrum. Rather than forcing regulators into the worst regions of trade-offs between incumbent protection and spectrum utilization, such improved detection performance can expand the regulatory solution space (by exactly how much is for later design and engineering analysis phases), enabling sharing frameworks that more adequately serve both constituencies. The hybrid RAN-as-a-Sensor augmentation of Standalone sensor approach could help unlock greater economic and social value from limited spectrum resources while creating stronger incentives for continued collaboration in spectrum management approaches.

7.5.3 Cost-Efficient Infrastructure Leverage

The system could leverage communication infrastructure that will be deployed , creating cost efficiencies compared to deploying numerous additional specialized standalone sensors blanketing a given area and volume to achieve comparable coverage. By combining the strengths of specialized standalone sensors with the widespread coverage of commercial e.g wireless

infrastructure that shares a band, this approach delivers significant technical advantages while leveraging existing investments in current communication networks as well as emerging Integrated Sensing and Communications (ISAC) networks (both *non-3GPP-based* ISAC networks as well as *3GPP-based* ISAC networks).

7.5.4 Dedicated Single-instrument Sensor versus Hybrid RAN-based detection time scale

To enable bands shared with mobile radar systems, including airborne as well as ground-based and maritime without causing harmful interference, highly responsive Hybrid Dynamic Spectrum Sharing (HDSS) algorithms are required. These algorithms must allow 3GPP-based and other radio access systems to detect radar activity and react within TBD seconds (e.g., under 10 seconds).

HDSS solutions under consideration include both sensor-based systems and Radio Access Network (RAN)-based detection methods. A single sensor, if it receives a radar pulse with sufficient signal-to-noise ratio (SNR), could be able to detect radar presence with high confidence and initiate a rapid response. However, because the exact location and trajectory of the radar could be unknown, the initial commercial wireless system response could need to cover a wide area to ensure protection.

To improve responsiveness and precision, a dense network of environmental sensors could be necessary. These sensors could help not only with rapid detection but also with tracking and predicting radar movement, allowing the commercial system to minimize disruption while maintaining service quality.

In addition, widely deployed commercial networks themselves can contribute to radar detection and prediction. RAN-based detection relies on input from numerous base stations and user devices. While this approach might not be as immediately responsive as dedicated environmental sensors, it can offer valuable data over a longer time scale. Over time, the collective input from RAN elements could refine radio system responses—more accurately determining which commercial devices could reduce or cease transmission and better predict radar behavior and its potential impact.

7.5.5 Hybrid Sensing Performance Advantage vs Standalone-only

Relative to standalone sensors, Hybrid Sensing increases number, angular visibility, diversity, and geographic footprint, allowing the system to break traditional pareto frontier trade-offs and simultaneously improve probability of detection while reducing false alarm rates. This pareto improvement is unavailable to standalone sensors and enables efficient spectrum sharing.

"RAN-as-a-Sensor" implements distributed networked sensing, enjoying inherent benefits of all such systems. It's not inherently superior to other distributed designs, but distributed sensing can augment standalone sensing functions. As RAN-as-a-Sensor follows this architectural pattern, it's generically applicable to other mid-band sensing augmentation.

7.5.6 Complementary Systems

RAN-based sensing could augment dedicated incumbent sensing. These systems operate on complementary time scales: standalone sensors could provide rapid detection but may protect unnecessarily large areas, reducing spectrum sharing opportunities. RAN-based detection could enable progressive protection zone refinement and improved radar behavior prediction for both systems, enabling more precise spectrum sharing.

Distributed sensing elements could overcome line-of-sight limitations challenging standalone sensors. When specialized sensors are blocked by terrain, multiple distributed nodes can actively sense radar emissions and relay information to fusion centers. Even with implementation challenges including sensor correlation, non-uniform distribution, and synchronization errors, Hybrid Sensing could deliver significant improvements.

7.5.7 Augmentation Capabilities

Overcoming Physical Limitations Single-instrument sensors face constraints including line-of-sight limitations, terrain masking, power limitations, and single points of failure. Distributed RAN sensors compensate for these limitations. For example, when mountains block a sensitive standalone sensor's view, base stations and user equipment throughout the area detect signals from blocked regions and relay information to fusion centers.

Signal Verification and False Alarm Reduction When detecting unknown waveforms, standalone sensors may register ambiguous signals. Distributed sensing could provide verification: if multiple geographically dispersed sensors observe similar activity, confidence increases that detection is legitimate. This corroboration is valuable when pattern matching isn't possible with unknown waveforms.

Contextual Environmental Information Distributed sensors could collect RF environment data, creating baseline understanding. When unknown radar begins operating, standalone sensors detect unusual activity but lack broader context. The distributed system provides environmental awareness, helping distinguish between normal variations and suspicious signals.

7.6 UE/Device Embedded Sensing

The 3GPP protocol today incorporates multiple examples of UE-based information being transmitted to the BS for follow-on action. For example, parameters such as RSRP, RSRQ, CSI, PMI, et cetera are routinely estimated by 3GPP UEs, transmitted to the BS and then used by the RAN for optimizing resource allocations in time, frequency and space. Extending these protocols to include sensing of non-3GPP signals such as incumbent radars is to be further studied from a UE capability point of view. A TDD frame configuration that reserves timeslots for such sensing could be required: these “quiet periods” would enable all UEs to perform sensing in a coordinated fashion and the RAN to collate sensing information from multiple UEs and BSs to arrive at robust decisions on incumbent presence. Similar concepts were standardized in IEEE 802.22 in the case of TV White Space spectrum sharing and could be considered for future systems that will coexist with incumbent systems.

8 Conclusions

This document has leveraged the expertise of the Wireless Innovation Forum in the context of dynamic spectrum sharing, and has introduced the new application of several concepts relevant to moving toward highly-dynamic spectrum sharing. Among them:

- Reducing the time over which secondary users react to changes in incumbent use from 24 hours (AFC) and 5 minutes (CBRS) to potentially seconds
- Various incumbent detection/informing methods and their application of highly-dynamic spectrum sharing (HDSS), including:
    - Portal, including extensions to TARDyS3 to support HDSS
    - Dedicated sensing, RAN-based sensing, and hybrid models
- Improvements to propagation prediction, such as the use of known signals for in-situ clutter loss characterization
- The use of closed-loop interference reporting to reduce dependence on propagation models altogether while ensuring incumbent protection

These concepts will be valuable in bands that require much more responsiveness in the protection of incumbent systems from secondary users, such as the lower 3 GHz band in the U.S., but will also be relevant to a large number of future shared spectrum opportunities in the U.S. and elsewhere, as spectrum occupancy increase and sharing becomes more complex.

Appendix A: Revision History

Document History		
V1.0.0	28 July 2025	Initial Release

Appendix B: Implementation and Additional Propagation Measurement Features for Internal and External Signal (OBS) Sounding Approaches

OBS (Occupancy Based Sharing) using External or Internal Signal Sounding Methods

Features that are intended to expand HDSS incumbent sharing applications include: *Atmospheric and Environmental Clutter Loss Measurement:* OBS uses L-band PNT sounding satellite signals. This offers an advantage for capturing or mapping troposcatter propagation events where path loss can drop as much as 50dB sounding (ITS report) which can incite over-the-horizon propagation from surrounding frequency-sharing macro-cell stations to introduce interference not otherwise bounded by terrain. due to their relatively low loss through atmospheric loss variations. However, higher frequency signals in the future are also possible, provided these can be accurately calibrated for clutter mapping purposes.

OBS in HDSS Coordination. Notification and Avoidance of Spectrum Access "Collisions": The term "Electrospace," coined by NTIA/ITS in the 1980s, describes the electromagnetic resource in terms of coordination in spatial, spectral, and temporal dimensions. This multi-dimensional approach provides a framework for standardizing HDSS coordination and proactive spectrum assignment, especially within government bands that must retain sensitive legacy spectrum operations (e.g., missile defense). Development of new standards includes the recent IEEE 1900.5.2 SCM to hasten development of data transfer across multiple vendor platforms or intelligent entities.

*Standardized Data Formats for Spectrum Access Coordination***:** OBS aligns with and conforms to the IEEE 1900.5.2 standard (also known as the Spectrum Consumption Model) which promotes cross-industry, multi-vendor data formats within a HDSS ecosystem. This enables scalable HDSS data management and coordination across diverse incumbent and secondary access use cases and architectures.

Within IEEE 1900.5.2, spectrum occupancy surrounding each node can be visualized as a spheroidal shell encapsulating extent of radiation out to the point where emissions do not exceed continuously managed interference thresholds, also known as the Incumbent Protection Criteria (IPC). This spatial/spectral modeling ensures non-overlapping operations between incumbent and secondary spectrum operations as well as protect, optimally coordinate access among multiple secondary user operations.

Waveform and Band Flexibility: OBS sharing is waveform-agnostic and supports clutter mapping and occupancy profiling across any mid-band candidate (currently defined as between 1 GHz with an upper bound of 13.3 to 15.3 GHz). This approach supports both co-channel and adjacent-band protections, and sounding can be implemented in FR-1 or FR-2 RAN/ORAN front ends, supporting internal ISAC signals or external GNSS sounding signals.

Appendix C: RAN-Augmented Incumbent-Presence Sensing (Hybrid Sensing)

Practical Example of Hybrid Sensing Augmentation

Consider a concrete operational scenario where a sophisticated standalone sensor works in conjunction with a distributed sensor network like a RAN-as-a-Sensor network to detect an adversary's experimental radar using unknown waveform characteristics:

1. **Initial Detection**: The specialized standalone sensor detects faint, unusual emissions somewhere in the S-band. These emissions don't match any known radar signature in its database. The sensor flags this as a "potential unknown signal" but has low confidence since it could be interference or noise.

2. **Distributed Verification**: The system immediately queries all distributed RAN sensors in a, say, 10km radius. Three base stations (for example, gNodeBs or any other suitably equipped access point) and seven UEs also report detecting anomalous signals in the same frequency band. The spatial pattern of these detections forms a clear directional trend pointing toward a specific hillside location.

3. **Environmental Context**: The distributed sensors report that this particular pattern of emissions is highly unusual for this area and time of day, representing a, *say*, 92% deviation from the established baseline RF environment.

4. **Combined Analysis**: The multi-sensor data fusion center integrates the standalone sensor's high-fidelity signal capture with the distributed sensors' spatial awareness and environmental context. This fusion creates a comprehensive detection assessment: "Unknown signal with, *say*, 94% likelihood of being radar-based emissions, originating from coordinates 34.5678°N, 78.9012°W, first appeared at 14:32 local time."

5. **Adaptation and Learning**: As the system continues to monitor the signal, the distributed sensors track its presence across different locations and times. This data teaches the standalone sensor what characteristics to focus on, gradually improving its ability to detect this previously unknown waveform directly.

The key difference in this scenario is that ***neither system alone*** could have achieved this level of detection confidence. The standalone sensor provided superior signal detection capability but lacked spatial awareness and environmental context. The distributed sensors provided verification, localization, and contextual information but might not have initially recognized the signal as significant without the standalone sensor's alert.