Mancuso, Ed.
Probasco
Patil
January 29, 2013

Protocol to Access White Space (PAWS) Database: Use Cases and Requirements

draft-ietf-paws-problem-stmt-usecases-rqmts-12

Abstract

Portions of the radio spectrum that are assigned to a particular use but are unused or unoccupied at specific locations and times are defined as "white space." The concept of allowing additional transmissions (which may or may not be licensed) in white space is a technique to "unlock" existing spectrum for new use. An obvious requirement is that these additional transmissions do not interfere with the assigned use of the spectrum. One approach to using white space spectrum at a given time and location is to verify spectrum availability with a database that manages spectrum sharing and provides spectrum-availability information. The IETF has undertaken to develop a Protocol to Access Spectrum Database [1] for such a management database.

This document describes a number of possible use cases of white space spectrum and technology as well as a set of requirements for the database query protocol. The concept of white spaces is described along with the problems that need to be addressed to enable white space spectrum for additional uses without causing interference to currently assigned use. Use of white space is enabled by querying a database that stores information about spectrum availability at any given location and time.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-

Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 2, 2013.

Copyright Notice

Table of Contents

1. Introduction

1.1. Introduction to white space

Wireless spectrum is a commodity that is regulated by governments. The spectrum is used for various purposes, which include, but are not limited to, entertainment (e.g., radio and television), communication (e.g., telephony and Internet access), military (e.g., radars etc.), and navigation (e.g., satellite communication, GPS). Portions of the radio spectrum that are assigned to a licensed (primary) user but are unused or unoccupied at specific locations and times are defined as "white space." The concept of allowing additional (secondary) transmissions (which may or may not be licensed) in white space is a technique to "unlock" existing spectrum for new use. An obvious requirement is that these secondary transmissions do not interfere with the assigned use of the spectrum. One interesting observation is that often, in a given physical location, the primary user(s) may not be using the entire band assigned to them. The available spectrum for secondary transmissions would then depend on the location of the secondary user. The fundamental issue is how to determine, for a specific location and specific time, if any of the assigned spectrum is available for secondary use. Academia and Industry have studied multiple cognitive radio [2] mechanisms for use in such a scenario. One simple mechanism is to use a geospatial database that contains the spatial and temporal profile of all primary licensees' spectrum usage, and require secondary users to query the database for available spectrum that they can use at their location. Such databases can be accessible and queryable by secondary users on the Internet.

Any entity that is assigned spectrum that is not densely used may be asked by a governmental regulatory agency to share it to allow for more intensive use of the spectrum. Providing a mechanism by which secondary users share the spectrum with the primary user is attractive in many bands in many countries.

This document includes the problem statement followed by use cases and requirements associated with the use of white space spectrum by secondary users via a database query protocol. Note that the IETF has undertaken to develop a white space database query protocol (see Protocol to Access Spectrum Database [1].

1.2. Scope

1.2.1. In Scope

This document covers the requirements for a protocol to allow a device to access a database to obtain spectrum availability

information. Such a protocol should allow a device to perform the following actions:

1. Determine the relevant white space database to query.

2. Connect to and optionally register with the database using a well-defined protocol.

3. Provide its geolocation and perhaps other data to the database using a well-defined format for querying the database.

4. Receive in response to the query a list of available white space frequencies using a well-defined format for the information.

5. Send an acknowledgment to the database with information containing channels selected for use by the device.

1.2.2. Out of Scope

The following topics are out of scope for this specification:

1. Co-existence and interference avoidance of white space devices within the same spectrum.

2. Provisioning (releasing new spectrum for white space use).

2. Conventions and Terminology

2.1. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2.2. Terminology

Database A database is an entity that contains current information about available spectrum at a given location and time as well as other types of information related to spectrum availability and usage.

Device Class Identifies classes of devices including fixed, mobile, portable, etc... May also indicate if the device is indoor or outdoor.

Device ID An identifier for each master device.

Master Device A device that queries the database, on its own behalf and/or on behalf of a slave device, to obtain available spectrum information.

Slave Device A device that queries the database through a master device.

White Space (WS) Radio spectrum that is available for secondary use at a specific location and time.

White Space Device (WSD) A device that uses white space spectrum as a secondary user. A white space device can be a fixed or portable device such as an access point, base station, or cell phone.

3. Protocol Services

A protocol solution must enable many different potential white space services. This section describes the features required of the protocol.

3.1. White space database discovery

A white space radio network is created by a master device. Before the master device can transmit in white space spectrum, it MUST obtain the address of a trusted white space database, which it will query for available white space spectrum. If the master device uses a discovery service to locate a trusted white space database, it performs the following steps:

1. The master device connects to the Internet.

2. The master device constructs and sends a request over the Internet to a trusted discovery service.

3. If no acceptable response is received within a pre-configured time limit, the master device concludes that no trusted database is available. If at least one response is received, the master device evaluates the response(s) to determine if a trusted database can be identified where the master device is able to receive service from the database. If so, it establishes contact with the trusted database, and establishes a white space network (as described in the following use cases).

Optionally, and in place of steps 1 - 3 above, the master device can be pre-programmed with the Internet address of one or more one

trusted databases. The master device can establish contact with one of these trusted databases and establish a white space network (as described in the following use cases).

3.2. Device registration with trusted database

In some regulatory domains, the master device must register with the trusted database before it queries the database for available spectrum. Different regulatory domains may have different device registration requirements.

Figure 1 (Figure 1) shows an example deployment of this scenario.

```
                                               ----------
         \|/                                 |Database|
          |                  .---.    / ---------
       |--|--------|        (     )  /
       |  Master   |       /       \
       |           |========( Internet)
       |-----------|       \       /
                            (     )
                             (---)
```

Figure 1: Example illustration of registration requirement in white space use-case

A simplified operational scenario showing registration consists of the following steps:

1. If required by the regulatory domain, the master device registers with its most current and up-to-date information. If subject to registration, typically the master device will register after power up, after changing location by a predetermined distance, and after prescribed time intervals.

2. To register with the database, the master device sends registration information to the database. This information may include the Device ID, serial number assigned by the manufacturer, device location, device antenna height above ground, name of the individual or business that owns the device, and the name, street and email address, and telephone number of a contact person responsible for the device's operation.

3. The database responds to the registration request with an acknowledgement to indicate the success of the registration request or with an error if the registration was unsuccessful. Additional information may be provided by the database in its response according to regulatory requirements.

4. Use Cases

There are many potential use cases for white space spectrum - for example, providing broadband Internet access in urban and densely-populated hotspots as well as rural and remote, underserved areas. Available white space spectrum may also be used to provide Internet 'backhaul' for traditional Wi-Fi hotspots or for use by towns and cities to monitor/control traffic lights, read utility meters, and the like. Still other use cases include the ability to offload data traffic from another Internet access network (e.g., 3G cellular network) or to deliver data, information, or a service to a user based on the user's location. Some of these use cases are described in the following sections.

4.1. Master-slave white space networks

There are a number of common scenarios in which a master white space device will act as proxy or mediator for one or more slave devices using its connection to the Internet to query the database for available spectrum for itself and for one or more slave devices. These slave devices may be fixed or mobile, in close proximity with each other (indoor network or urban hotspot), or at a distance (rural or remote WAN). Once slave devices switch to white space spectrum for their communications, they may connect through the master to the Internet or use white space spectrum for intra-network communications only. The master device can continue to arbitrate and control white space communications by slave devices, and may notify them when they are required to change white space frequencies or cease white space communications.

Figure 2 (Figure 2) depicts the general architecture such a simple master-slave network, in which the master device communicates on its own behalf and on behalf of slave devices with a white space database.

```
 --------
|Slave |
|Device| \             \|/                         ----------
|  1   |  (Air)         |                          |Database|
--------       \        |                (----)   /|--------|
   |            \ ------|------         (      ) /
   |             \|  Master   |        /        \
 --------        /|           |======= ( Internet )
 |Slave |       / |  Device   |        \        /
 |Device|  (Air)  |           |         (      )
 |  2   | /       |-----------|          (----)
 |-------        /
   o    |       /
   o    |     (Air)
   o    |      /
 --------     /
 |Slave |    /
 |Device|   /
 |  n   |
 --------
```

Figure 2: Master-Slave White Space Network

The protocol requirements for these master-slave device and other similar scenarios is essentially the same: the protocol must support the ability of a master device to make available-spectrum query requests on behalf of slave devices, passing device identification, geolocation, and other slave device parameters to the database as required to obtain a list of white space spectrum available for use by one or more slave devices. Of course, different use cases will use this spectrum information in different ways, and the details of master/slave communications may be different for different use cases.

Common steps may occur in master-slave networks include the following:

1. The master device powers up.

2. Slave devices power up and associate with the master device via Wi-Fi or some other over-the-air non-white space spectrum. Until the slave device is allocated white space spectrum, any master-slave or slave-slave communications occurs over such non-white space spectrum.

3. The master has Internet connectivity, determines (or knows) its location, and establishes a connection to a trusted white space database (see Section 4.1.1).

4. The master optionally registers with the trusted database (see Section 4.1.2).

5. The master sends a query to the trusted database requesting a list of available white space spectrum based upon its geolocation. Query parameters may include the master's location, device identifier, and antenna height. Note that the master may relay available-spectrum requests to the database on behalf of slave devices, then transmit the obtained available-spectrum lists to the slaves (or the master may allocate spectrum to slaves from the obtained spectrum lists).

6. The database responds to the master's query with a list of available white space spectrum, associated maximum power levels,

and a durations of time for spectrum use. If the master made requests on behalf of slave devices, the master may transmit the obtained available-spectrum lists to the slaves (or the master may allocate spectrum to slaves from the obtained spectrum lists).

7. The master may inform the database of the spectrum and power level it selects from the available spectrum list. If a slave device has been allocated available white space spectrum, the slave may inform the master of the spectrum and power level it has chosen, and the master may, in turn, relay such slave device usage to the database.

8. Further communication among masters and slaves over the white space network may occur via the selected/allocated white space spectrum frequencies.

4.2. Offloading: moving traffic to a white space network

This scenario is a variant of the master-slave network described in the previous use case. In this scenario, an Internet connectivity service is provided over white space as a supplemental or alternative datapath to a more costly Internet connection (metered wire service, metered wireless service, metered satellite service). In a typical deployment scenario, an end user has a primary Internet connection, but may prefer to use a connection to the Internet provided by a local white space master device that is connected to the Internet.

Figure 3 (Figure 3) shows an example deployment of this scenario.

```
                      \|/
                       |
                       |
                    |------------|
                   /|   Master   | \
            (Air)-/ |------------|  \
---------  /                         \              -----------
|Slave   |/                           \     (----)  | Database|
|Device  |                             \   (      ) /----------
|--------|\                             \ /        \
           \                             X( Internet )
            \                           / \        /
             (Air)                     /   (      )
                \                     /     (----)
                 \                   /
                  \|---------------|/
                   |    Metered    |
                   |    Service    |
                   |---------------|
```

Figure 3: Offloading Traffic to a White Space Network

A simplified operation scenario of offloading content, such as video stream, from the a metered Internet connection to the a WS connection consists of the following steps:

1. The slave device connects to a metered Internet service, and selects a video for streaming.

2. The slave device switches mode and associates with a master white space device.*

3. The master queries the database for available white space spectrum and relays it to the slave device as described in Section 4.1.*

4. The slave uses available white space spectrum to communicate with the master and connect to the Internet to stream the selected video.

* Note that the slave device can act as a master device to query the database directly for available white space spectrum through its metered connection to the Internet, thus eliminating steps 2 and 3.

4.3. White space serving as backhaul

In this use case, an Internet connectivity service is provided to users over a common wireless standard, such as Wi-Fi, with a white

space master/slave network providing backhaul connectivity to the Internet. Note that Wi-Fi is referenced in Figure 4 (Figure 4) and the following discussion, but any other technology can be substituted in its place.

Figure 4 (Figure 4) shows an example deployment of this scenario.

```
                          \|/   White      \|/    \|/     Wi-Fi \|/
                           |   Space        |      |             |
                           |                |      |           |-|----|
            (----)       |-|----|         |-|------|-|         | Wi-Fi|
           (      )      |Master|         | Slave    |--(Air)--| Dev  |
          /         \    |      |--(Air)--| Bridge   |         |------|
          ( Internet )---|      |         | to Wi-Fi |
          \         /    |------|         |----------|          \|/
           (      )                                   \          |
            (----)                                     \(Air)   |-|----|
                                                             \--| Wi-Fi|
                                                                | Dev  |
                                                                |------|
```

Figure 4: White Space Network Used for Backhaul

Once the bridged device (WS + Wi-Fi) is connected to a master and WS network, a simplified operation scenario of backhaul for Wi-Fi consists of the following steps:

1. A bridged slave device (WS + Wi-Fi) is connected to a master device operating in the WS spectrum (the master obtains available white space spectrum as described in Section 4.1).

2. Once the slave device is connected to the master, the Wi-Fi access point has Internet connectivity as well.

3. End users attach to the Wi-Fi network via their Wi-Fi enabled devices and receive Internet connectivity.

4.4. Rapid network deployment during emergency scenario

Organizations involved in handling emergency operations maintain an infrastructure that relies on dedicated spectrum for their operations. However, such infrastructures are often affected by the disasters they handle. To set up a replacement network, spectrum needs to be quickly cleared and reallocated to the crisis response organization. Automation of the this allocation and assignment is often the best solution. A preferred option is to make use of a robust protocol that has been adopted and implemented by radio manufacturers. A typical network topology solution might include wireless access links to the public Internet or private network,

wireless ad-hoc network radios working independent of a fixed infrastructure, and satellite links for backup where lack of coverage, overload, or outage of wireless access links can occur.

Figure 5 (Figure 5) shows an example deployment of this scenario.

```
                        \|/
                         | ad hoc
                         |
                       |-|-------------|
                       | Master node   |     |------------|
  \|/                  | with          |     | Whitespace |
   | ad hoc           /| backhaul link |     | Database   |
   |             /---/ |---------------|     |------------|
---|------------/                 |      \           /
| Master node   |                 |       |      (--/--)
| without       |                 |        -----(      )
| backhaul link |                 | Wireless  / Private \
----------------\                 |   Access (   net or  )
                 \                 |          \ Internet )
                  \    \|/         |      ------(       /
                   \    | ad hoc   |      |      (------)
                    \   |          |      /          \
                     \--|-------------   /Satellite   ----------
                     | Master node   | / Link        | Other  |
                     | with          |/              | nodes  |
                     | backhaul link |               ----------
                     -----------------
```

Figure 5: Rapid-deployed Network with Partly-connected Nodes

In the ad-hoc network, all nodes are master nodes that allocate RF channels from the white space database (as described in Section 4.1). However, the backhaul link may not be available to all nodes, such as depicted for the left node in the above figure. To handle RF channel allocation for such nodes, a master node with a backhaul link relays or proxies the database query for them. So master nodes without a backhaul link follow the procedure as defined for clients. The ad-hoc network radios utilize the provided RF channels. Details on forming and maintenance of the ad-hoc network, including repair of segmented networks caused by segments operating on different RF channels, is out of scope of spectrum allocation.

4.5. White space used for local TV broadcaster

Available white space spectrum can be deployed in novel ways to leverage the public use of hand-held and portable devices. One such use is white space spectrum used for local TV transmission of audio-video content to portable devices used by individuals in attendance at an event. In this use case, audience members at a seminar, entertainment event, or other venue plug a miniature TV receiver fob into their laptop, computer tablet, cell phone, or other portable device. A master device obtains a list of available white space spectrum (as described in , (Section 4.1), then broadcasts audio-video content locally to the audience over one of the available frequencies. Audience members receive the content through their miniature TV receivers tuned to the appropriate white space band for display on their portable device monitors.

Figure 6 (Figure 6) shows an example deployment of this scenario.

```
                                                |------------|
                                               |White Space |
                                               | Database   |
                                   .---.   /  |------------|
        |-----------|           (     )  /
        |  Master   |         /        \
        |           |========( Internet)
        |-----------|         \        /
             |                 (     )
            /|\                 (---)

        (White Space
         Broadcast)

   \|/   \|/   \|/   \|/   \|/   \|/   \|/
    |     |     |     |     |     |     |      .................
  ----- ----- ----- ----- ----- ----- -----
  |   | |   | |   | |   | |   | |   | |   |
  |   | |   | |   | |   | |   | |   | |   |
  ----- ----- ----- ----- ----- ----- -----
```

USB TV receivers connected to laptops, cellphone, tablets ....

Figure 6: White Space Used for Local TV Broadcast

5. Problem Statement

The use of white space spectrum is enabled via the capability of a device to query a database and obtain information about the availability of spectrum for use at a given location. The databases are reachable via the Internet and the devices querying these databases are expected to have some form of Internet connectivity, directly or indirectly. The databases may be regulatory specific since the available spectrum and regulations may vary, but the fundamental operation of the protocol should be regulatory independent.

An example high-level architecture of the devices and white space databases is shown in Figure 7 (Figure 7).

```
 -----------
|  Master |
|WS Device|                              ------------
|Lat: X   |\           .---.    /--------|Database X|
|Long: Y  | \         (     )  /         ------------
-----------  \-------/       \/                o
                    ( Internet)                o
-----------  /------(        )\                o
|  Master | /        (       ) \
|WS Device|/          (_____)   \         ------------
|Lat: X   |                      \--------|Database Y|
|Long: Y  |                               ------------
-----------
```

Figure 7: High-level View of White Space Database Architecture

In Figure 11, note that there could be multiple databases serving white space devices. The databases are locale specific since the regulations and available spectrum may vary. In some countries, for example, the U.S., the regulator has determined that multiple databases may provide service to White Space Devices.

A messaging interface between the white space devices and the database is required for operating a network using the white space spectrum. The following sections discuss various aspects of such an interface and the need for a standard.

5.1. Global applicability

The use of white space spectrum is currently approved or being considered in multiple regulatory domains, whose rules may differ. However, the need for devices that intend to use the spectrum to communicate with a database remains a common feature. The database implements rules that protect all primary users, independent of the characteristics of the white space devices. It also provides a way to specify a schedule of use, since some primary users (for example, wireless microphones) only operate in limited time slots.

Devices need to be able to query a database, directly or indirectly, over the public Internet and/or private IP networks prior to operating in available spectrum. Information about available spectrum, schedule, power, etc., are provided by the database as a response to the query from a device. The messaging interface needs to be:

1. Radio/air interface agnostic - Any radio/air interface technology used by a white space device can be IEEE 802.11af, IEEE 802.15.4m, IEEE 802.16, IEEE 802.22, LTE etc. However, the messaging interface between a master white space device and the database should be agnostic to any air interface used for such messaging while being cognizant of the characteristics of various air-interface technologies and the need to include any relevant attributes in the query to the database.

2. Spectrum agnostic - the spectrum used by primary and secondary users varies by country. Some spectrum has an explicit notion of a "channel": a defined swath of spectrum within a band that has some assigned identifier. Other spectrum bands may be subject to white space sharing, but only have actual frequency low/high

parameters to define primary and secondary use. The protocol should be able to be used in any spectrum band where white space sharing is permitted.

3. Globally applicable - A common messaging interface between white space devices and databases will enable the use of such spectrum for various purposes on a global basis. Devices can operate in any locale where such spectrum is available and a common interface ensures uniformity in implementations and deployment. Since the White Space Device must know its geospatial location to do a query, it is possible to determine which database, and which rules, are applicable, even though they are locale specific. Note that although a device may know its geolocation, it may not know the country or regulatory domain that it is in. Further, even if the device knows this information, it may not be sufficient for the device to know its expected behaviour in its domain of operation since one domain may adopt a rule set for white space device operation from another regulatory domain (Brazil may adopt the "FccWhitespace2010" US rule set). To allow the global use of white space devices in different countries (whatever the regulatory domain), the protocol should support the Database communicating applicable rule set information to the white space device.

4. Flexible and extensible data structures - Different databases are likely to have different requirements for the kinds of data required for registration (different rule sets that apply to the registration of devices) and other messages sent by the device to the database. For instance, different regulators might require different device-characteristic information to be passed to the database.

5.2. Database discovery

Another aspect of the problem space is the need to discover the database. A white space device needs to find the relevant database to query, based on its current location or for another location. Since the spectrum and databases are domain specific, the device will need to discover the relevant database. The device needs to determine the location of the specific database to which it can send queries in addition to registering itself for operation and using the available spectrum.

5.3. Protocol

A protocol that enables a white space device to query a database to obtain information about available spectrum is needed. A device may be required to register with the database with some credentials prior to being allowed to query. The requirements for such a protocol are specified in this document.

5.4. Data model definition

The contents of the queries and response need to be specified. A data model is required which enables the white space device to query the database while including all the relevant information such as geolocation, radio technology, power characteristics, etc., which may be country and spectrum and regulatory dependent. All databases are able to interpret the data model and respond to the queries using the same data model that is understood by all devices.

6. Requirements

6.1. Data Model Requirements

D.1 The Data Model MUST support specifying the geolocation of the WSD, the uncertainty in meters, the height & its uncertainty, and confidence in percentage of the location determination. The Data Model MUST support WGS84 (see NGA: DoD World Geodetic System 1984 [3]).

D.2 The Data Model MUST support specifying the data and other applicable requirements of the rule set that applies to the white space device at its current location.

D.3 The Data Model MUST support device description data that identifies a device (serial number, certification IDs, etc.) and describes device characteristics, such as or device class (fixed, mobile, portable, indoor, outdoor, etc.), Radio Access Technology (RAT), etc.

D.4 The Data Model MUST support specifying a manufacturer's serial number for a white space device.

D.5 The Data Model MUST support specifying the antenna and radiation related parameters of the subject, such as:

antenna height

antenna gain

maximum output power, EIRP (dBm)

antenna radiation pattern (directional dependence of the strength of the radio signal from the antenna)

spectrum mask with lowest and highest possible frequency

spectrum mask in dBr from peak transmit power in EIRP, with specific power limit at any frequency linearly interpolated between adjacent points of the spectrum mask

measurement resolution bandwidth for EIRP measurements

D.6 The Data Model MUST support specifying owner and operator contact information for a transmitter. This includes the name of the transmitter owner, name of transmitter operator, postal address, email address and phone number of the transmitter operator.

D.7 The Data Model MUST support specifying spectrum availability. Spectrum units are specified by low and high frequencies and may have an optional channel identifier. The Data Model MUST support a schedule including start time and stop time for spectrum unit availability. The Data Model MUST support maximum power level for each spectrum unit.

D.8 The Data Model MUST support specifying spectrum availability information for a single location and an area (e.g., a polygon defined by multiple location points or a geometric shape such as a circle).

D.9 The Data Model MUST support specifying the frequencies and power levels selected for use by a device in the acknowledgement message.

6.2. Protocol Requirements

P.1 The master device MUST identify a database to which it can register, make spectrum availability requests, etc. The master device MAY select a database by discovery at run time or by means of a pre-programmed URI address. The master device MAY validate discovered or configured database addresses against a list of approved databases maintained by a regulatory body.

P.2 The protocol must support the database informing the master of the regulatory rules (rule set) that applies to the master device (or any slave devices on whose behalf the master is contacting the database) at the current location or the master (or slave) device(s).

P.3 The protocol MUST provide the ability for the database to authenticate the master device.

P.4 The protocol MUST provide the ability for the master device to verify the authenticity of the database with which it is interacting.

P.5 The messages sent by the master device to the database and the messages sent by the database to the master device MUST support integrity protection.

P.6 The protocol MUST provide the capability for messages sent by the master device and database to be encrypted.

P.7 The protocol MUST support the master device registering with the database (see Device Registration (Section 3.2)).

P.8 The protocol MUST support a registration acknowledgement indicating the success of failure of the master device registration.

P.9 The protocol MUST support an available spectrum request from the master device to the database. These parameters MAY include any of the parameters and attributes required to be supported in the Data Model Requirements.

P.10 The protocol MUST support an available spectrum response from the database to the master device. These parameters MAY include any of the parameters and attributes required to be supported in the Data Model Requirements.

P.11 The protocol MUST support a spectrum usage message from the master device to the database. These parameters MAY include any of the parameters and attributes required to be supported in the Data Model Requirements.

P.12 The protocol MUST support a spectrum usage message acknowledgement.

P.13 The protocol MUST support a validation request from the master to the database to validate a slave device. The validation request MUST include the slave device ID.

P.14 The protocol MUST support a validation response from the database to the master to indicate if the slave device is validated by the WSDB. The validation response MUST indicate the success or failure of the validation request.

P.15 The protocol MUST support the capability for the database to inform master devices of changes to spectrum availability information in a timely manner.

6.3. Operational Requirements

This section contains operational requirements of a white space database-device system, independent of the requirements of the protocol for communication between the white space database and devices.

O.1 The database and the master device MUST be connected to the Internet.

O.2 A master device MUST be able to determine its location including uncertainty and confidence level. A fixed master device MAY use a location programmed at installation or have the capability to determine its location. A mobile master device MUST have the capability to determine its location. Locations MUST be determined to the accuracy required by the applicable regulatory domain.

O.3 The master device MAY contact a database directly for service or the master device MAY contact a database listing server first, followed by contact to a database.

O.4 The master device MUST obtain information on the rule set of the regulatory body that applies to the master device at its current location (and/or the location of any slave devices on whose behalf the master device is operating).

O.5 The master device MAY register with the database according to local regulatory policy. Not all master devices will be required to register. Specific events will initiate registration, these events are determined by regulator policy (e.g., at power up, after movement, etc...). When local regulatory policy requires registration, the master device MUST register with its most current and up-to-date information, and MUST include all variables mandated by local regulator policy.

O.6 A master device MUST query the database for the available spectrum based on its current location before starting radio transmission in white space. Parameters provided to the database MAY include device location, accuracy of the location, antenna characteristic information, device identifier of any slave device requesting spectrum information, etc.

O.7 The database MUST respond to an available spectrum list request from an authenticated and authorized device and MAY also provide time constraints, maximum output power, start and stop frequencies for each band in the list and any additional requirements for sensing.

O.8 According to local regulator policy, a master device MAY inform the database of the actual frequency usage of the master and its slaves. The master MUST include parameters required by local regulatory policy, e.g., device ID, manufacturer's serial number, spectrum usage and power level information of the master and its slaves.

O.9 After connecting to a master device's radio network a slave device MUST query the master device for a list of available spectrum. The slave MUST include parameters required by local regulatory policy, e.g., device ID, device location.

O.10 According to local regulatory policy, the master device MAY query the database with parameters received from the slave device.

O.11 The database MUST respond to a query from the master device containing parameters from a slave device.

O.12 A master device MUST repeat the query to the database for the available spectrum as often as required by the regulation (e.g., FCC requires once per day) to verify that the operating channels continue to remain available.

O.13 A master device which changes its location more than a threshold distance (specified by local regulatory policy) during its operation, MUST query the database for available operating spectrum each time it moves more than the threshold distance (e.g., FCC specifies 100m) from the location it previously made the query.

O.14 According to local regulator policy, a master device may contact a database via proxy service of another master device.

O.15 A master device MUST be able to query the whitespace database for spectrum availability information for a specific expected coverage area around its current location.

O.16 A Master device MUST include its unique identity in all message exchanges with the database.

O.17 In the case of a natural disaster,emergency services may need to use distributed white space databases on short notice. The database should support any emergency regulations adopted by regulators to provide priority allocation of white space spectrum to emergency services.

6.4. Guidelines

The current scope of the working group is limited and is reflected in the requirements captured in Section 6.1. However white space technology itself is expected to evolve and address other aspects such as co-existence and interference avoidance, spectrum brokering, alternative spectrum bands, etc. The design of the data model and protocol should be cognizant of the evolving nature of white space technology and consider the following set of guidelines in the development of the data model and protocol:

1. The data model SHOULD provide a modular design separating out messaging specific, administrative specific, and spectrum specific parts into separate modules.

2. The protocol SHOULD support determination of which administrative specific and spectrum specific modules are used.

7. IANA Considerations

This document makes no request of IANA.

8. Security Considerations

PAWS is a protocol whereby a Master Device requests a schedule of available spectrum at its location (or location of its Slave Devices) before it (they) can operate using those frequencies. Whereas the information provided by the Database must be accurate and conform to applicable regulatory rules, the Database cannot enforce, through the protocol, that a client device uses only the spectrum it provided. In other words, devices can put energy in the air and cause interference without asking the Database. Hence, PAWS security considerations do not include protection against malicious use of the White Space spectrum.

Threat model for the PAWS protocol:

Assumptions:

It is assumed that an attacker has full access to the network medium between the master device and the white space database. The attacker may be able to eavesdrop on any communications between these entities. The link between the master device and the white space database can be wired or wireless and provides IP connectivity.

It is assumed that both the master device and the white space database have NOT been compromised from a security standpoint.

Threat 1: User modifies a device to masquerade as another valid certified device

Regulatory environments require that devices be certified and register in ways that accurately reflect their certification. Without suitable protection mechanisms, devices could simply listen to registration exchanges, and later registering claiming to be those other devices. Such replays would allow false registration, violating regulatory regimes. A white space database may be operated by a commercial entity which restricts access only to authorized users. A master device MAY need to identify itself to the database and be authorized to obtain information about available spectrum.

Threat 2: Spoofed white space database

A master device discovers a white space database(s) through which it can query for available spectrum information. The master device needs to ensure that the white space database with which it communicates with is an authentic entity. The white space database needs to provide its identity to the master device which can confirm the validity/authenticity of the database. An attacker may attempt to spoof a white space database and provide responses to a master device which are malicious and result in the master device causing interference to the primary user of the spectrum.

Threat 3: Modifying a query request

An attacker may modify the query request sent by a master device to a white space database. The attacker may change the location of the device or the capabilities in terms of its transmit power or antenna height etc., which could result in the database responding with incorrect information about available spectrum or max transmit power allowed. The result of such an attack is that the master device would cause interference to the primary user of the spectrum. It could also result in a denial of service to the master device by indicating that no channels are available.

Threat 4: Modifying a query response

An attacker could modify the query response sent by the white space database to a master device. The available spectrum information or transmit power allowed type of parameters carried in the response could be modified by the attacker resulting in the master device using spectrum that is not available at a location or transmitting at a greater power level than allowed resulting in interference to the primary user of that spectrum. Alternatively the attacker may indicate no spectrum availability at a location resulting in a denial of service to the master device.

Threat 5: Third party tracking of white space device location and identity

A white space database in a regulatory domain may require a master device to provide its identity in addition to its location in the query request. Such location/identity information can be gleaned by an eavesdropper and used for tracking purposes. A master device may prefer to keep the location/identity information hidden from eavesdroppers, hence

the protocol should provide a means to protect the location and identity information of the master device and prevent tracking of locations associated with a white space database query. When the master device sends both its identity and location to the DB, the DB is able to track it. If a regulatory domain does not require the master device to provide its identity to the white space database, the master device may decide not to send its identity, to prevent being tracked by the DB.

Threat 6: Malicious individual acts as a PAWS entity (spoofing DB or as MiM) to terminate or unfairly limit spectrum access of devices for reasons other than incumbent protection

A white space database MAY include a mechanism by which service and spectrum allocated to a master device can be revoked by sending an unsolicited message. A malicious node can pretend to be the white space database with which a master device has registered or obtained spectrum information from and send a revoke message to that device. This results in denial of service to the master device.

The security requirements arising from the above threats are captured in the requirements of Section 6.1 (Section 6.1).

9. Summary and Conclusion

Wireless spectrum is a scarce resource. As the demand for spectrum grows, there is a need to more efficiently utilize the available and allocated spectrum. Cognitive radio technologies enable the efficient usage of spectrum via means such as sensing or by querying a database to determine available spectrum at a given location for opportunistic use. "White space" is the general term used to refer to the bands within the spectrum which are available for secondary use at a given location. In order to use this spectrum, a device needs to query a database that maintains information about the available spectrum within a band. A protocol is necessary for communication between the devices and databases that is globally applicable.

The document describes some examples of the role of the white space database in the operation of a radio network, and also provides examples of services provided to the user of a white space device. From these use cases, requirements are determined. These requirements are to be used as input for the development of a Protocol to Access White Space database (PAWS).

10. Acknowledgements

The authors acknowledge Gabor Bajko, Teco Boot, Nancy Bravin, Rex Buddenberg, Vincent Chen, Gerald Chouinard, Stephen Farrell, Michael Fitch, Joel M. Halpern, Jussi Kahtava, Paul Lambert, Pete Resnick, Brian Rosen, Andy Sago, Peter Stanforth, John Stine and, Juan Carlos Zuniga for their contributions to this document.

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

11.2. Informational References

URIs

[1] <https://datatracker.ietf.org/doc/draft-ietf-paws-protocol/>

[2] <http://en.wikipedia.org/wiki/Cognitive_radio>

[3] <http://earth-info.nga.mil/GandG/publications/tr8350.2/tr8350_2.html>

Authors' Addresses

Anthony Mancuso (editor)

Scott Probasco

Phone:
Fax:
Email: scott@probasco.me
URI:

Basavaraj Patil

Phone:
Fax:
Email: bpatil@ovi.com
URI: