Internet Engineering Task Force (IETF)
Request for Comments: 6953
Category: Informational
ISSN: 2070-1721

A. Mancuso, Ed.
Google
S. Probasco

B. Patil
Cisco Systems

May 2013

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

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. This document includes the problem statement for the development of a protocol to access a database of white-space information followed by use cases and requirements for that protocol. Finally, requirements associated with the protocol are presented.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6953.

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 [CRADIO] 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. The final sections include the requirements associated with such a protocol. Note that the IETF has undertaken to develop a database query protocol (see [PAWS]).

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 database to query.

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

3. Provide 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 at the specified geolocation 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 and other device operation parameters.

Note: The above protocol actions should explicitly or implicitly support the ability of devices to re-register and/or re-query the database when they change their locations or operating parameters. This will allow them to receive permission to operate in their new locations and/or with their new operating parameters, and to send acknowledgments to the database that include information on their new operating parameters.

1.2.2. Out of Scope

The following topics are out of scope for this specification:

1. It is the device’s responsibility to query the database for new spectrum when the device moves, changes operating parameters, loses connectivity, etc. Other synchronization mechanisms are out of scope.

2. A rogue device may operate without contacting the database to obtain available spectrum. Hence, enforcement of spectrum usage by devices is out of scope.

3. The protocol defines communications between the database and devices. The protocol for communications between devices is out of scope.

4. Coexistence and interference avoidance of white-space devices within the same spectrum are out of scope.

5. Provisioning (releasing new spectrum for white-space use) is out of scope.

2. Conventions Used in This Document

2.1. 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 a 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.

Trusted Database: A database that is trusted by a device or provides data objects that are trusted by a 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.

2.2. 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].

3. 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. While databases are expected to support the rule set(s) of one or more regulatory domains, and the regulations and available spectrum associated with each rule set may vary, the fundamental operation of the protocol must be independent of any particular regulatory environment.

An example of the high-level architecture of the devices and databases is shown in Figure 1.

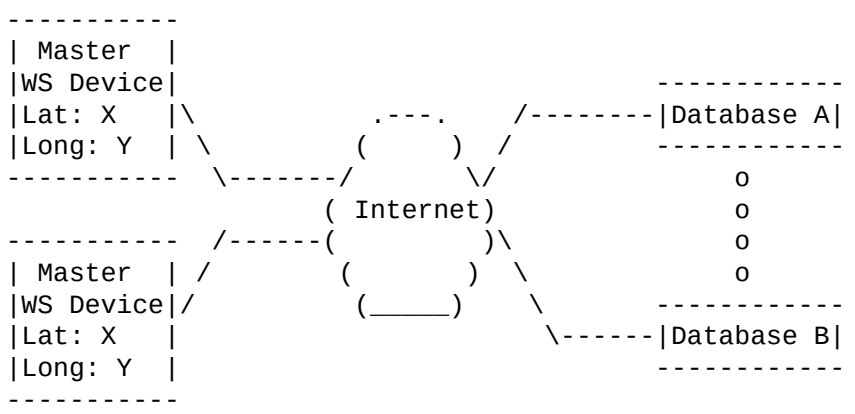

Figure 1: High-Level View of White-Space Database Architecture

Note that there could be multiple databases serving white-space devices. In some countries, such as 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.

3.1. 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. Interface agnostic - An interface between a master white-space device and database can be wired or unwired (e.g., a radio/air interface technology such as 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 the interface used for such messaging while being cognizant of the characteristics of the interface technology 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 bands have 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 location where such spectrum is available and a common interface ensures uniformity in implementations and deployment. To allow the global use of white-space devices in different countries (whatever the regulatory domain), the protocol should support the database that communicates the applicable regulatory rule-set information to the white-space device.

4. Built on flexible and extensible data structures - Different databases are likely to have different requirements for the kinds of data required for registration (different regulatory 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.

3.2. Database Discovery

The master device must obtain the address of a trusted database, which it will query for available white-space spectrum. If the master device uses a discovery service to locate a trusted database, it may perform the following steps (this description is intended as descriptive, not prescriptive):

1. The master device constructs and sends a request (e.g., over the Internet) to a trusted discovery service.

2. 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.

3. The master device establishes a white-space network as described in Section 4.

Optionally, and in place of steps 1-2 above, the master device can be pre-configured with the address (e.g., URI) of one or more trusted databases. The master device can establish contact with one of these trusted databases.

3.3. Device Registration

The master device may register with the database before it queries the database for available spectrum. A registration process may consist of the following steps:

1. 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, postal address, email address, and phone number of a contact person responsible for the device's operation.

2. The database responds to the registration request with an acknowledgment 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 to the master device.

3.4. 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.

3.5. Data Model Definition

The contents of the queries and response need to be specified. A data model is required; it must enable 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, 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.

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 it may notify them when they are required to change white-space frequencies or cease white-space communications.

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

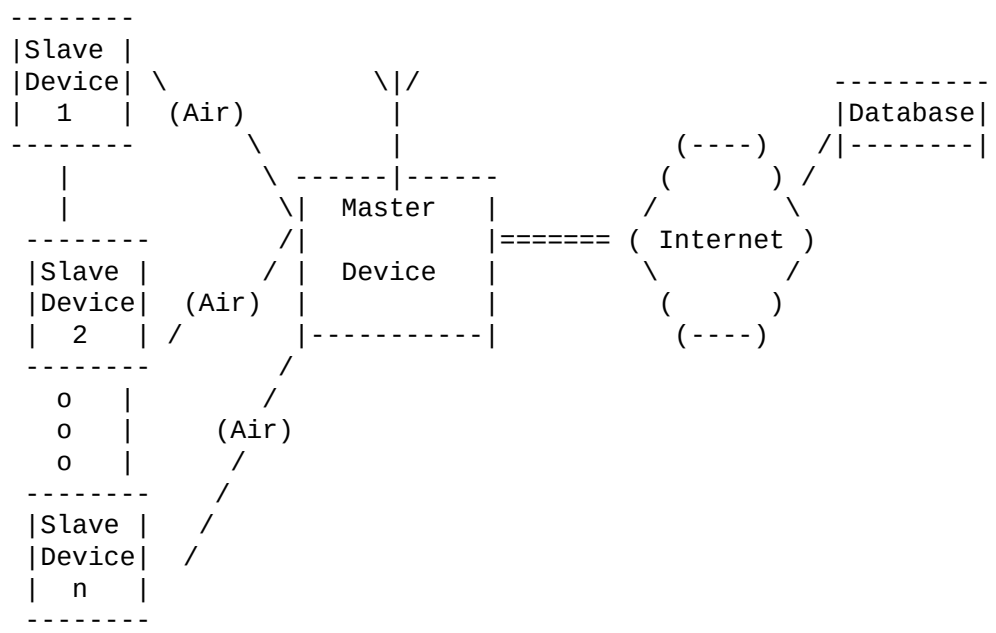

Figure 2: Master-Slave White-Space Network

The protocol requirements for these master-slave devices 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 that may occur in master-slave networks include the following:

1. The master device powers up.

2. Slave devices may 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 database (see Section 3.2).

4. The master may register with the trusted database (see Section 3.3).

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. The master may send available-spectrum requests to the database on behalf of slave devices.

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

Note: Steps 5 through 7 may be repeated by the master device when it (or a slave device that uses the master as a proxy to communicate with the database) changes its location or operating parameters -- for example, after a master changes location, it may query the database for available spectrum at its new location, then acknowledge the subsequent response received from the database with information on the spectrum and power levels it is using at the new location.

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 access point (AP) offers a white-space service that offloads Internet traffic as an alternative data path to a more congested or costly Internet wire, wireless, or satellite service.

Figure 3 shows an example of deployment of this scenario.

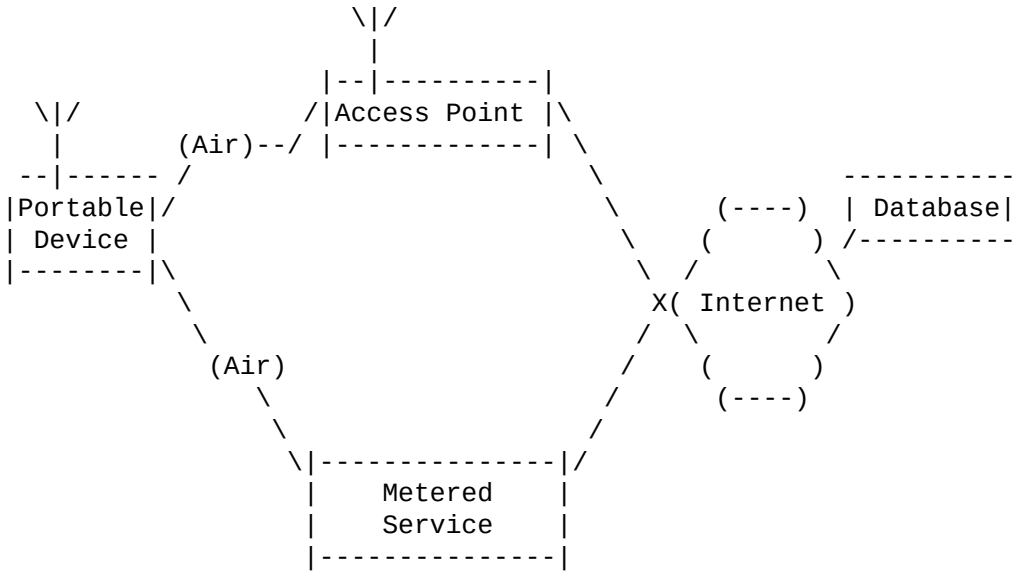

Figure 3: Offloading Traffic to a White-Space Network

A simplified operation scenario of offloading content, such as video stream, from a congested or costly Internet connection to a white-space service provided by an AP consists of the following steps:

1. The AP contacts the database to determine channels it can use.

2. The portable device connects to a paid Internet service and selects a video for streaming.

3. The portable device determines if it can offload to a white-space AP:

   A. If the portable device knows its location, it

      1. asks the database (using the paid service) for available white-space spectrum;

      2. listens for and connects to the AP over the permitted white-space spectrum.

   B. If the portable device does not have GPS or other means to determine its position, it

      1. uses non-white-space spectrum to listen for and connect to the AP;

2. asks the AP to query the database for permitted white-space spectrum on its behalf;

3. uses the permitted white-space spectrum to connect to the AP.

4. The portable device accesses the Internet through the AP to stream the selected video.

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 and the following discussion, but any other technology can be substituted in its place.

Figure 4 shows an example of deployment of this scenario.

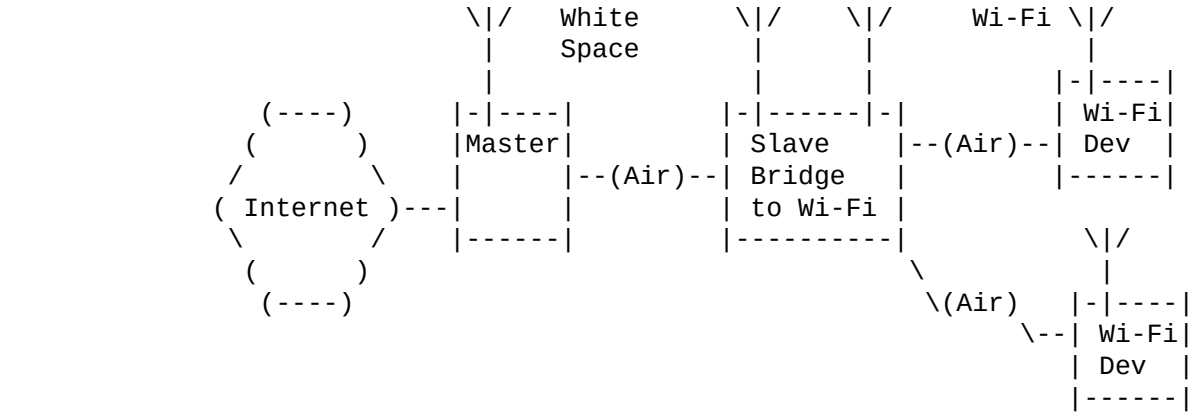

Figure 4: White-Space Network Used for Backhaul

Once the bridged device (Slave Bridge + 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 (Slave Bridge + 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 Emergencies

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 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 independently of a fixed infrastructure, and satellite links for backup where lack of coverage, overload, or outage of wireless access links can occur.

Figure 5 shows an example of deployment of this scenario.

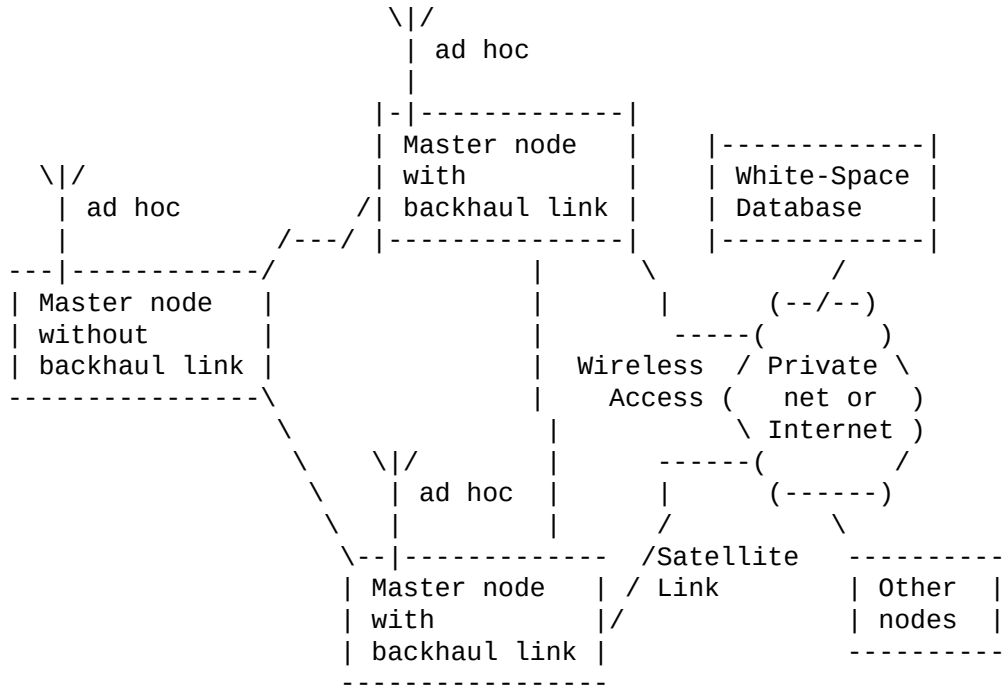

Figure 5: Rapidly Deployed Network with Partly Connected Nodes

In the ad hoc network, all nodes are master nodes that allocate radio frequency (RF) channels from the 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 the monitors of their portable devices.

Figure 6 shows an example of deployment of this scenario.

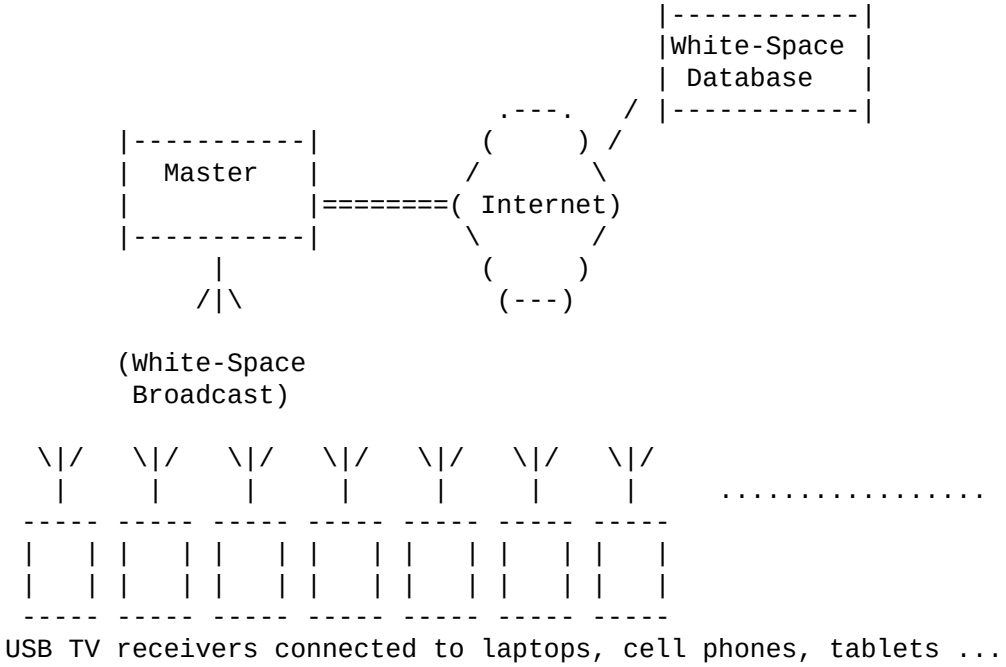

Figure 6: White Space Used for Local TV Broadcast

5. Requirements

5.1. Data Model Requirements

D.1 The data model MUST support specifying the geolocation of the white-space device, the uncertainty in meters, the height and its uncertainty, and the percentage of confidence in the location determination. The data model MUST support [WGS84].

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 a specified location.

D.3 The data model MUST support device description data that identifies a white-space device (serial number, certification IDs, etc.) and describes device characteristics, such as 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 white-space device, such as:

- antenna height
- antenna gain
- maximum output power, Equivalent Isotropic Radiated Power (EIRP) in dBm (decibels referenced to 1 milliwatt)
- 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 (decibels referenced to an arbitrary reference level) 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 and the name, 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 white-space device in the acknowledgment message.

5.2. Protocol Requirements

P.1 The master device identifies a database to which it can register, make spectrum availability requests, etc. The protocol MUST support the discovery of an appropriate database given a location provided by the master device. The master device MAY select a database by discovery at run time or by means of a pre-programmed URI. The master device MAY validate discovered or configured database addresses against a list of known databases (e.g., a list of databases approved 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 a specified location.

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 Tracking of master or slave device uses of white-space spectrum by database administrators, regulatory agencies, and others who have access to a white-space database could be considered invasive of privacy, including privacy regulations in specific environments. The PAWS protocol SHOULD support privacy-sensitive handling of device-provided data where such protection is feasible, allowed, and desired.

P.8 The protocol MUST support the master device registering with the database; see Device Registration (Section 3.3).

P.9 The protocol MUST support a registration acknowledgment indicating the success or failure of the master device registration.

P.10 The protocol MUST support an available spectrum request from the master device to the database, which may include one or more of the data items listed in Data Model Requirements (Section 5.1). The request may include data that the master device sends on its own behalf and/or on behalf of one or more slave devices.

P.11 The protocol MUST support an available spectrum response from the database to the master device, which may include one or more of the data items listed in Data Model Requirements (Section 5.1). The response may include data related to master and/or slave device operation.

P.12 The protocol MUST support a spectrum usage message from the master device to the database, which may include one or more of the data items listed in Data Model Requirements (Section 5.1). The message may include data that the master device sends on its own behalf and/or on behalf of one or more slave devices.

P.13 The protocol MUST support a spectrum usage message acknowledgment.

P.14 The protocol MUST support a validation request from the master device to the database to validate a slave device, which should include information necessary to identify the slave device to the database.

P.15 The protocol MUST support a validation response from the database to the master to indicate if the slave device is validated by the database. The validation response MUST indicate the success or failure of the validation request.

P.16 The protocol MUST support the capability for the database to inform master devices of changes to spectrum availability information.

5.3. Operational Requirements

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

O.1 The master device must be able to connect to the database to send requests to the database and receive responses to, and acknowledgments of, its requests from the database.

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.

O.3 The master device MUST be configured to understand and comply with the requirements of the rule set of the regulatory body that apply to its operation at its location.

O.4 A master device MUST query the database for the available spectrum at a specified location before starting radio transmission in white space at that location.

O.5 A master device MUST be able to query the database for the available spectrum on behalf of a slave device at a specified location before the slave device starts radio transmission in white space at that location.

O.6 The database MUST respond to an available spectrum request.

5.4. Guidelines

White-space technology itself is expected to evolve and include attributes such as coexistence 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 messaging-specific, administrative-specific, and spectrum-specific parts into distinct modules.

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

6. Security Considerations

PAWS is a protocol whereby a master device requests a schedule of available spectrum at its location (or the location of its slave devices) before it (or 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:

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

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

A master device identifies itself to the database in order to obtain information about available spectrum. Without suitable protection mechanisms, devices can listen to registration exchanges and later register with the database by claiming the identity of another device.

Threat 2: Spoofed database

A master device attempts to discover a database (or databases) that it can query for available spectrum information. An attacker may attempt to spoof a database and provide responses to a master device that are malicious and result in the master device causing interference to the primary user of the spectrum.

Threat 3: Modifying or jamming a query request

An attacker may modify or jam the query request sent by a master device to a database. The attacker may change the location of the device or its capabilities (transmit power, antenna height, etc.), and, as a result, the database responds with incorrect information about available spectrum or maximum

transmit power allowed. The result of such an attack is that the master device can cause interference to the primary user of the spectrum. It may also result in a denial of service to the master device if the modified database response indicates that no channels are available to the master device or when a jammed query prevents the request from reaching the database.

Threat 4: Modifying or jamming a query response

An attacker may modify or jam the query response sent by the database to a master device. For example, an attacker may modify the available spectrum or power-level information carried in the database response. As a result, a master device may use spectrum that is not available at a location or may transmit at a greater power level than allowed. Such unauthorized use can result in interference to the primary user of that spectrum. Alternatively, an attacker may modify a database response to indicate that no spectrum is available at a location (or jam the response), resulting in a denial of service to the master device.

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

A master device may 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 unauthorized tracking purposes.

Threat 6: Malicious individual acts as a database to terminate or unfairly limit spectrum access of devices

A database may include a mechanism by which service and spectrum allocated to a master device can be revoked by sending a revoke message to a master device. A malicious user can pretend to be a database 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 5.2.

7. Acknowledgments

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, Barry Leiba, Subramanian Moonesamy, Pete Resnick, Brian Rosen, Andy Sago, Peter Stanforth, John Stine, and Juan Carlos Zuniga for their contributions to this document.

8. References

8.1. Normative References

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

[WGS84] National Imagery and Mapping Agency, "Department of Defense World Geodetic System 1984, Its Definition and Relationships with Local Geodetic Systems", NIMA TR8350.2 Third Edition Amendment 1, January 2000, <http://earth-info.nga.mil/GandG/publications/tr8350.2/wgs84fin.pdf>.

8.2. Informative References

[CRADIO] Cognitive Radio Technologies Proceeding (CRTP), "Federal Communications Commission", ET Docket No. 03-108, August 2010, <http://fcc.gov/oet/cognitiveradio>.

[PAWS] Chen, V., Ed., Das, S., Zhu, L., Malyar, J., and P. McCann, "Protocol to Access Spectrum Database", Work in Progress, May 2013.

Authors' Addresses

Anthony Mancuso (editor)
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043
US

EMail: amancuso@google.com

Scott Probasco

EMail: scott@probasco.me

Basavaraj Patil
Cisco Systems
2250 East President George Bush Highway
Richardson, TX 75082
US

EMail: basavpat@cisco.com