COGNITIVE RADIO ACCESS MANAGEMENT FOR PUBLIC SAFETY COMMUNICATIONS SYSTEMS

Robert L. Foster, Jr. (Shared Spectrum Company, Vienna, Virginia USA; rfoster [at] sharedspectrum.com); Mark McHenry (Shared Spectrum Company, Vienna, Virginia USA; mmchenry [at] sharedspectrum.com); Thao Nguyen (Shared Spectrum Company, Vienna, Virginia USA; tnguyen [at] sharedspectrum.com); Filip Perich (Shared Spectrum Company, Vienna, Virginia USA; fperich [at] sharedspectrum.com); Peter Tenhula (Shared Spectrum Company, Vienna, Virginia USA; ptenhula [at] sharedspectrum.com)

ABSTRACT

Multi-band, reconfigurable cognitive radio (CR) technology has been identified as offering key solutions to Public Safety spectrum access problems. However, CR technology invokes concerns about the ability to securely control devices with Dynamic Spectrum Access (DSA) capabilities potentially operating autonomously across multiple frequency bands. To alleviate these concerns, an end-to-end, Cognitive Radio Access Management (CRAM) subsystem is presented that focuses on secure, flexible and user-friendly policy-based control mechanisms. On one end of the subsystem, policy conformance enforcement is embedded at the edge of the CR network onto CR devices by leveraging device-understandable, XML-based rules and constraints. On the other end, user-friendly policy authoring and administration tools are available to a wide range of Public Safety stakeholders to create, disseminate, and validate policies before, during and after they are loaded and run on CR devices. Throughout the subsystem, multiple layers of reliable security measures are employed to further ensure trust that the policies are valid and work properly.

1. INTRODUCTION

The Cognitive Radio Access Management (CRAM) subsystem provides Public Safety spectrum managers with transparent, flexible, and adaptable tools to remotely control a large number of cognitive radio (CR) devices in a cost effective, reliable manner. The subsystem's software tools enable the creation, validation and dissemination of spectrum access and priority rules to Public Safety CR devices while allowing incident commanders to monitor, avoid and remedy interference.

Spectrum access conformance enforcement components are embedded directly onto the CR devices at the edge of Public Safety radio networks. These components employ machine-understandable policies indicating when, where, and how the CR devices can transmit on specific sets of frequency bands. The subsystem's security features allow for strong user authentication, policy encryption, secure local and remote policy repositories, configuration management, and logging devise activity.

In this paper, we first describe the policy language-based approach of configuring CR devices. Then, we provide an overview of the CRAM subsystem architecture, tools and modules.

2. POLICY LANGUAGE-BASED APPROACH

There are at least three possible methods to manage CR devices for Public Safety communications. The first and current approach is to use pre-programmed radios that are manually configured to transmit on one or more frequencies. This method is highly inflexible, and is the main cause of Public Safety interoperability and spectrum access problems. In the second method, CR devices are configured (via configuration file). This approach is used to manage newer software defined radios and is more flexible, but it has limits the ability to rapidly reconfigure the radios to adapt to new requirements. If, for example, new radios are brought on the scene of an emergency from another jurisdiction they would require a wholesale change of their pre-programmed configuration files before they are of any use during the incident. Providing this type of reconfiguration and reprogramming support is likely to be highly expensive and time consuming.

A third method that more efficiently and effectively manages and controls public safety radios, including emerging CR devices, is a policy language-based approach. Software policies using machine-understandable language specify authorized frequencies, the time periods they are available, location requirements and other specific spectrum access requirements and constraints. By capturing the spectrum access rules in policies and allowing software components to merge, de-conflict, and enforce policies from multiple stakeholders simultaneously, a wide range of radio types can be managed by Public Safety stakeholders

throughout the incident command structure without extensive reconfiguration and reprogramming support.

Not only does this approach provide significant management and operational flexibility, but it also eliminates the need for absolute conformance among all spectrum access rules (*e.g.*, authorizations and constraints) and combinations of rules from all stakeholders, regulatory bodies and radio manufacturers before CR devices can be fielded at an incident under unplanned circumstances. The representation of rules in a policy language increases flexibility and interoperability while allowing reconfiguration updates to be expressed and disseminated securely. The CRAM subsystem leverages a policy language that built on top of the W3C Ontology Web Language (OWL) and W3C Semantic Web Rule Language (SWRL), which uses XML for its syntax.

The policy language provides for expression of both permissive and prohibitive policies. A permissive policy defines requirements that must be met in order for a CR device to access designated frequencies. A prohibitive policy defines circumstances that, when present, deny a radio from accessing specific spectrum. Prohibitive policies are given priority over permissive policies in the event of a conflict.

3. COGNITIVE RADIO ACCESS MANAGEMENT (CRAM) SUBSYSTEM ARCHITECTURE

High-level functionalities and features of the CRAM subsystem consoles and their respective software tools and modules are described in this section. Figure 1 displays the policy consoles, tools and other components. To limit unauthorized access and minimize potential conflicts among stakeholder roles, the subsystem is separated into three main consoles: Authoring, Administration and User consoles. The User console has some or all of the features as the Administration console and would be used by the Communications Unit Leader (COML) during an incident.

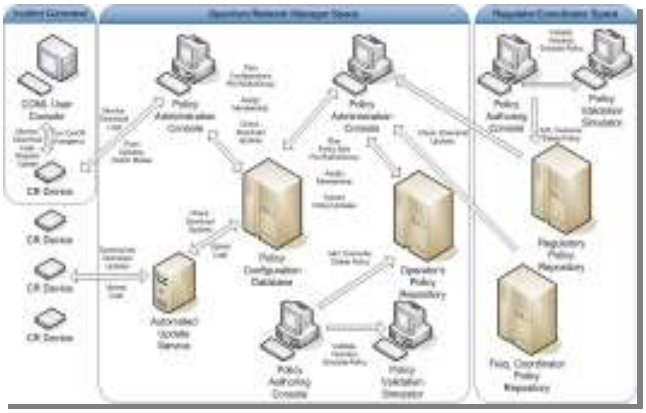

Figure 1 CRAM Subsystem Architecture

The CRAM Policy Authoring Tool allows regulators, frequency coordinators and spectrum/network managers to write spectrum access policies, validate them, and push them to secure data repositories. The Administration and User consoles enable local spectrum/network managers and Incident Commanders (through the COML) to effectively manage policies and CR devices. The Validation Simulator modules enable policy authors and administrators to visualize and validate the correctness of policies with their intended effect and to debug faulty policies. The subsystem uses a standard form of public-key cryptography to ensure secure policy dissemination.

4. POLICY AUTHORING CONSOLE AND TOOLS

The Authoring console's software tools provide a graphical user interface for the creation of new policies and editing existing policies in the OWL/XML format. Using these tools, policy authors do not have to be software engineers and can easily draft, import, copy, edit and upload policies through user-friendly wizards. With the wizards, authors are guided through a set of dialogs to identify CR device operational parameters, describe situational context, and specify restrictions on the parameters and context in terms of constraints and rules. To avoid errors, each form within the application does its own type checking to verify that the policy being generated is well formed in syntax. Thus, the language in each policy generated will be SWRL compliant and recognized by any CR device. More advanced users may also employ a text editor to check the SWRL output or modify the rule.

Permissions Dialog – This dialog appears after the author chooses to create a new policy. The author specifies all of the information requested to generate a policy file, including: (a) the URL for the designated repository and a unique, descriptive name for the policy (*e.g.*, EMS_Unit_1_EMP_v2.0); (b) the policy's relative priority; (c) the legal authority or organization issuing the policy (*e.g.*, City Emergency Management Plan 2.0); and (d) the policy type (*i.e.*, permissive or prohibitive).

Frequency Dialog – This allows the author to specify a list of frequency ranges in which the CR devices may or may not transmit. For example, the CR device may be permitted to transmit only in specified channels or frequencies (f1 to f2) that have been assigned from the Public Safety pool.

Location Selector Dialog – This is used to identify a list of locations at which the CR devices may or may not transmit. Alternatively, specific geography rules can be created based on information relative to the device's potential or authorized locations, which can be specified using shape object identifiers such as points, circles, polylines, and

polygons. With the Location List module, a location consists of a set of latitude and longitude coordinates with corresponding distances/radii.

Because spectrum access rules include geospatial constraints, the authoring tools enable two types of location rules: (1) a generic set of rules based on a list of geo-referenced points for a given latitude, longitude, and altitude; and (2) geography rules based on established or new geographic boundaries. The Geography Rules module (shown in Figure 2) allows the author to specify a boundary by loading a standard shapefile or by creating a new geodata object with the integrated Shape Builder sub-module (shown in Figure 3).

Figure 2 Geography Rule Generators

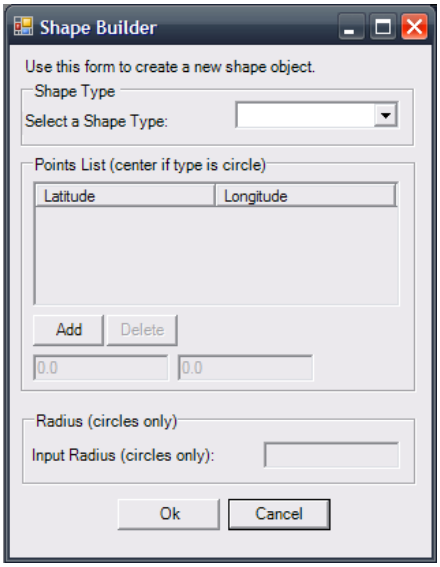

Figure 3 Shape Builder

Transmission Constraints Dialog – This module is used to specify power limits of transmissions as well as the permitted occupied bandwidth for CR devices. This feature also allows for control of other parameters for dynamic transmit power control, signal type, a GPS validation interval (to ensure location accuracy) and maximum time spent transmitting and not transmitting.

Device Dialog – This allows the author to specify a CR device or group of devices to which the policy is applied.

Time Constraints Dialog – This specifies the time(s) of day during which the policy is applicable, allowing for example, temporary policies to expire after an incident concludes.

5. POLICY VALIDATION SIMULATOR

The policy Validation Simulator tool provides a graphical user interface for users to validate policies through the simulation of a CR device running the policies. The tool allows both policy authors and policy administrators to configure the simulated device by adding or removing policies and to adjust the circumstances under which the simulated device is operating. The settings for the simulations are input either from a file, or manually by the user. The following interfaces are available for user input:

Device Identification Dialog – This sub-module allows users to specify the owner, authority, and compatibility version of the device being configured. Because policies can be categorized by owner and authority, providing the device information allows a user to verify that the policy is only applied if the authenticated owner or authority matches those specified in the policy.

Location Dialog – This feature allows users to configure the devices' location in latitude, longitude, and altitude. During a simulation, this location is the default position for the test device, but can be updated during the simulation using the device position visualizer (shown in Figure 4 and described below).

Signal Evidence Dialog – The signal detector feature allows users to specify multiple signal evidence profiles for the device so that policies that respond to changes in the evidence fields can be validated. Signal evidence consists of device state and information about the type of signals detected. Users may configure a device with multiple signal evidence entries based on the time of detection or load evidence from files from actual event measurements.

Transmission Settings Dialog – This configures the simulated devices' transmission capabilities. The dialog accepts frequency range and bandwidth transmission, power constraints, transmission power control (TPC), maximum transmission duration, and minimum wait duration settings.

Frequency & Time Visualizer – Once test policies are loaded, the simulation is initiated by displaying the visualization dialog, which allows users to modify time and geographical settings while displaying the CR devices' responses in real time. The default view of the visualization dialog is the frequency and time view (Figure 4) which allows the user to look closely at the frequencies permitted and denied as the time changes.

Figure 4 Frequency & Time Visualizer

Users input a start and end time for the simulation and specify the frequency values within the range of spectrum regulated by the policies loaded on the device. This will change the policy type/transmit state display of red (prohibitive/do not transmit) and green (permissive/ok to transmit) indicators over the frequency scale indicating where the device would transmit as configured.

Device Position Visualizer – As shown in Figure 5, this screen displays the area in which the simulated device could operate, and a colored point (red or green) representing its current position and policy type/transmit state.

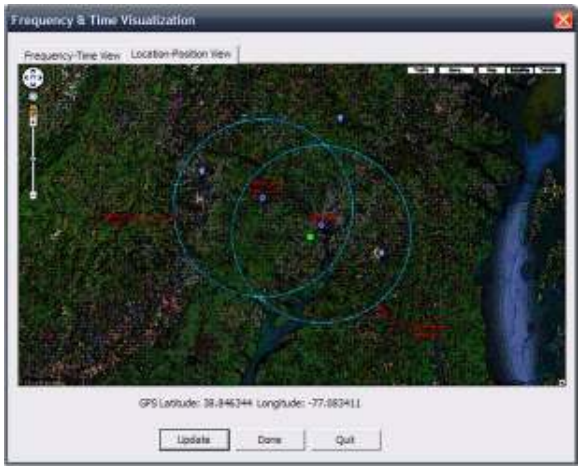

Figure 5 Device Position Visualizer

The point representing the simulated device may be dragged any place on the map and its location and state will update causing the dot to indicate whether the device would be permitted to transmit at the new location.

6. POLICY ADMINISTRATION CONSOLE

The Administration console's software tools provide secure, interactive methods for spectrum managers and incident commanders to remotely modify the operating parameters of one or many CR devices by disseminating policies remotely. Using the dissemination handler (shown in Figure 6), an administrator can add, remove, and query device configuration and policy content. This tool also enables unknown CR devices to interface and connect after secure verification and authorization.

Figure 6 Dissemination Handler & Activity Logger

Security Features – The Administrative console and tools communicate directly with the CR devices in a secure manner. To access the administrative console, only an authenticated user may log in using a secure user name and password, which must correspond to the X.509 private key used to sign the messages transmitted by the console.

The certificate authority for CR devices and administrators is created using OpenSSL. The certificate authority is then used to create a specific certificate for radios and administrators. The messages generated by the administrator will be in XML format. Once the message is generated with the proper values, OpenSSL is used to generate a signature and it is attached to the XML structure as well as the certificate. The user will be notified of security success and failure within the dialog. The Results

text box will log the step-by-step security results of an attempted transmission. In the case of message transmission failure the dialog will display the specific operation causing the failure before aborting the transmission.

Policy Selection Module – This module allows the administrator to execute "Add Policy" or "Delete Policy" commands from a list of predefined policies. The source of each policy on the list may be a local or master repository depending on the administrator's authorization level.

Policy Visualizer – The administrator can monitor the expected behavior of one or many radios from the interface in order to ensure proper functionality or detect functional errors using the tool's visualization capabilities. From the visualization dialog (Figure 7) administrators can look for gaps in spectrum coverage based on the selected policies.

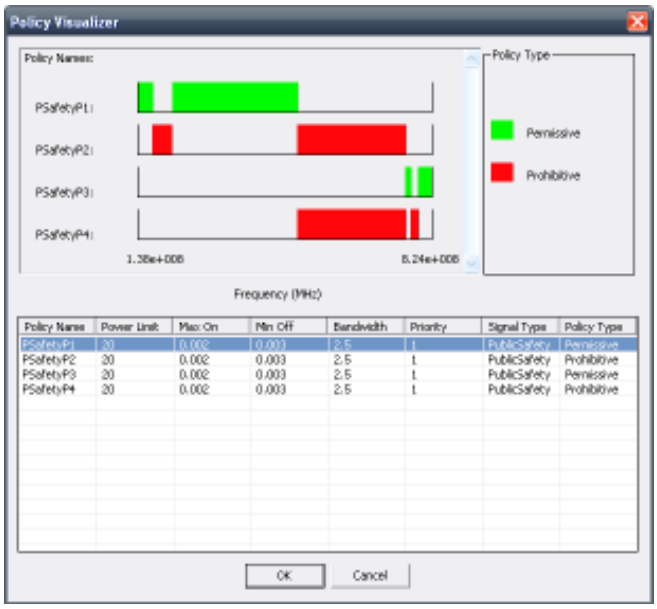

Figure 7 Policy Visualizer

This module allows the administrator to compare and contrast the behavior of known policies as well as view the content and meta-data of a policy to determine configuration settings. The policy visualize shown above in Figure 7 displays four policies, allowing the administrator to observe the frequencies permitted and prohibited by the policy set if they were all loaded on the CR device.

Mode Selection Module – An operational mode consists of one or more policies and a state active/running or inactive. To create an operational mode, the administrator inputs the name of the mode and activates it. Similarly, the administrator may delete an operational mode from a device.

Device Module – The multiple selection list of CR devices allows the administrator to choose which device(s) will receive the outgoing message once the execute command is selected. The list may contain individual devices if the radio tab is selected or groups of devices to contact.

Query Result Table – This module displays the data returned by querying the devices' on-board policy managers, which provides a variety of methods to query, retrieve and modify policies, logs and modes from a single CR device. Query results are constructed into table form based on the query request type and displayed in the multi-tab table (see Figure 6 above).

7. CONCLUSIONS, APPLICATIONS & FUTURE WORK

Multi-band, reconfigurable cognitive radio (CR) technology has been identified as offering key solutions to Public Safety spectrum access problems. However, CR technology invokes concerns about the ability to securely control devices with Dynamic Spectrum Access (DSA) capabilities potentially operating autonomously across multiple frequency bands. To alleviate these concerns, this paper presented an end-to-end, Cognitive Radio Access Management (CRAM) subsystem that provides secure, flexible and user-friendly policy-based control mechanisms for Public Safety stakeholders.

The CRAM subsystem's software tools enable the development of policies for DSA-enabled Public Safety CR devices. It provides a safe and reliable approach to managing multiple CR devices and reduces the time and effort otherwise required to manually reconfigure devices. So far, this initial design and development efforts behind the CRAM subsystem and policy tools provides a proof of concept approach that can demonstrate the following advantages for use of the subsystem in managing Public Safety CR devices: (1) Simplicity – there is no need for spectrum planning since the CR devices will adjust their spectrum usage pursuant to their policy-based rules and as circumstances change throughout the lifecycle of an emergency incident; (2) Speed of deployment – it is easier to copy and paste policies than writing new configurations from scratch.

While each of the tools developed for or used in the CRAM subsystem are being used and tested by Shared Spectrum Company on a variety of CR devices, the subsystem and devices should be tested in live field demonstrations, ideally during Public Safety first responder exercises in an urban environment. SSC's 802.16-based multi-band radio platform can be leveraged for an incident area network (IAN) test and evaluation of broadband

applications. Such demonstrations can show CR device interference avoidance and coexistence with legacy systems while ensuring building penetration and link range/quality.

8. ACKNOWLEDGEMENTS/DISCLAIMER

This project was supported in part by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice, under Award No. 2007-DE-BX-K008 awarded and by the Defense Advanced Research Projects Agency (DARPA) under contract numbers FA8750-05-C-0150 (XG, neXt Generation Communications Phase III) and W31P4Q-06-C-0395/W31P4Q-08-C-0290 (PbWAN, Policy-Based Automated WAN Configuration and Management). The opinions, findings, and conclusions or recommendations expressed in this publication/program/exhibition are those of the author(s) and do not necessarily reflect the views of the Department of Justice or the Department of Defense.

REFERENCES

[1] F. Perich, R. Foster, P. Tenhula, M. McHenry, "Experimental Field Test Results on Feasibility of Declarative Spectrum Management", proceedings of IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DYSPAN), October 2008, available at http://www.sharedspectrum.com/publications/papers/2008-10_SSC_Declarative_Spectrum_Management.pdf.

[2] F. Perich, "Policy-based Network Management for NeXt Generation Spectrum Access Control", proceedings of IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DYSPAN), April 2007, available at http://www.sharedspectrum.com/publications/papers/2007-02_SSC_Policy-based_Network_Mgmt_XG_Spectrum_Access_Control.pdf.

[3] W. Lane, "Cognitive Radio for Public Safety", FCC Public Safety and Homeland Security Bureau Tech Topic No. 8, available at www.fcc.gov/pshs/techtopics/techtopic8.html.

[4] W. Lane, "Cognitive Radio Potential for Public Safety", FCC Public Safety and Homeland Security Bureau Tech Topic No. 9, available at http://www.fcc.gov/pshs/techtopics/techtopic9.html.

[5] P. Cook, S. Hope, "Cognitive Radio Implications for Public Safety Communications", proceedings of the SDR '07 Technical Conference and Product Exposition, Nov. 2007, available at http://www.sdrforum.org/pages/sdr07/Proceedings/Papers/4.2/4.2-5.pdf.

[6] SDR Forum, "Software Defined Radio Technology for Public Safety", Document 2006-A-0001, April 2006, available at http://www.sdrforum.org/pages/documentLibrary/documents/SDRF-06-P-0001-V1_0_0%20_Public_Safety.pdf.

[7] J. Powell, "Cognitive and Software Radio: A Public Safety Regulatory Perspective", report to NPSTC meeting, June 2004, available at http://www.npstc.org/meetings/Powell%20SDR%20Regulatory%20Perspective%20061404.pdf.

[8] SDR Forum, "Utilization of Software Defined Radio Technology for the 700 MHz Public/Private Partnership", SDRF-08-P-0004-V0.8.0 , June 18, 2008, available at http://www.sdrforum.org/pages/documentLibrary/documents/SDRF-08-P-0004-V1_0_0_Technology_for_700_MHz_Spectrum.pdf

[9] SDR Forum, "Comments on Implementing a Public Safety Network in the 700 MHz Band", SDRF-08-R-0005-V1.0.0, June 18, 2008, available at http://www.sdrforum.org/pages/documentLibrary/documents/SDRF-08-R-0005-v1_0_0_700_MHz_NPRM_response.pdf.

[10] SDR Forum, "Use Cases for Cognitive Applications in Public Safety Communications Systems - Volume 1: Review of the 7 July Bombing of the London Underground", SDRF-07-P-0019-V1.0.0, November 2007, available at http://www.sdrforum.org/pages/documentLibrary/documents/SDRF-07-P-0019-V1_0_0.pdf.

[11] N. Jesuale and B.C. Eydt, "A Policy Proposal to Enable Cognitive Radio for Public Safety and Industry in the Land Mobile Radio Bands", proceedings of IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DYSPAN), April 2007, available at http://www.netcityengineering.com/PID354224.pdf.

[12] J.M. Peha, "Protecting Public Safety with Better Communications Systems, IEEE Communications", Vol. 43, No. 3 (March 2005), available at http://www.comsoc.org/ci1/Public/2005/Mar/cireg.html.

[13] SDR Forum, "Comments in Response to Ninth Notice of Proposed Rulemaking", PS Docket No. 06-229 and WT Docket No. 96-86, Feb. 2007, available at http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6518808817.

[14] SDR Forum, "High Level SDR Security Requirements", SDRF-06-I-0001-V1.00, Jan. 2006, available at http://www.sdrforum.org/uploads/pub_31718206_i_0001_v0_00_high_leve_security_rqmts_01_11_06.pdf.

[15] B. Eydt, "A Proposed Regulatory Framework for Facilitating the Inter-Jurisdictional Mobility of Software Defined Radio (SDR) Devices", proceedings of the SDR '05 Technical Conference and Product Exposition, Nov. 2005, available at http://www.sdrforum.org/pages/sdr05/5.1%20Security/5.1-01%20Eydt.pdf.

[16] E. Gallery, "A Policy-Based Framework for the Authorisation of Software Downloads in a Mobile Environment", proceedings of the SDR '03 Technical Conference and Product Exposition, Nov. 2003, available at http://www.sdrforum.org/pages/sdr03/papers/Systems/SY2002-Gallery.pdf.

[17] K. Okuike, K. Umebayashi, R. Kohno, "A Regulatory Framework Using Automatic Certification System for Software Defined Radio", proceedings of the SDR '03 Technical Conference and Product Exposition, Nov. 2003, available at www.sdrforum.org/pages/sdr03/papers/Applications/AP4-002-Okuike.pdf.