Grouping Abstraction and Authority Control in Policy-based Spectrum Management

Kevin Feeney, David Lewis, Patroklos Argyroudis, Keith Nolan, Declan O'Sullivan

Abstract—**The management of dynamic spectrum access requires the coordination of administrative functions across multiple organizations, from regulators to secondary market operators and commons cooperatives. Policy-based management approaches to dynamic spectrum access must therefore support a wide range of organizational types and handle the relationships between policies authored separately within those organizations. A policy language for administering dynamic access to spectrum resources has been proposed by the DARPA XG initiative. This defines an expressive and extensible language for specifying policies that determine the correct behavior of RF transceivers as spectrum usage opportunities occur. However, this language does not yet address the mapping of policies onto the complex organizational settings that are likely to emerge in the dynamic spectrum access domain. This paper defines how the DARPA XG policy language can be integrated with a meta-policy management scheme that provides the powerful organizational modeling and policy authoring authority control needed to manage the evolution of policies in these complex organizational settings. The benefits of this integration are illustrated through a case study based on the potential use of dynamic spectrum access licenses granted in Ireland for the DySpan 2007 conference, and the organizational conflicts that even this simple scenario can yield. The practical issues of administering a multi-organizational policy management system are examined through an analysis of the interactions between existing components that are being assembled to demonstrate sophisticated policy management of a cognitive radio system.**

I. Introduction

Dynamic spectrum access (DSA) systems require close integration of technological solutions for cognitive radio with the means for managing access to radio resources that accurately reflects legal, economic and public policy goals.

Policy based management is widely seen in the dynamic spectrum access community as the means for providing this integration [1][2]. Policy Based Management (PBM) has been widely researched for its potential application to IT system access control and network management. Based on the definition supplied in [3], we define a policy as: a persistent declarative specification, derived from management goals, of a rule defining decisions about choices in the behavior of a system.

The potential scenarios for the management of dynamic spectrum access present several new challenges for the application of PBM. Primarily these challenges arise from the spectrum being a publicly owned resource access to which is granted to organizations and individuals for a number of purposes. This differs from many existing applications of PBM, which focus on controlling access to resources within a single organization. In contrast, DSA requires policy rules to apply across organizations. No one organization owns or possesses the resource, but instead they are involved in controlling the propagation of the authority to use spectrum under defined conditions. In addition, the resource is potentially accessible to anyone in possession of an RF-enabled device, so assumptions of the existing PBM approach about the existence of a well-defined population of users, e.g. employees of a network operator, or subscribers of a service provider, must be critically assessed.

A proposal has been made for a policy-based management framework for cognitive radio by the U.S DARPA Next Generation Communication (XG) initiative [4]. Previously, we have demonstrated that this proposal is lacking in support for defining the exchange of radio access authority between organizations and for defining the multi-organization structure across which such exchanges take place [5]. In this paper we propose a specific extension to the DAPRA XG policy language (XGPL) based on abstractions from a scheme called Community Based Policy Management (CBPM). We then illustrate how these extensions could be applied using as a case study of the spectrum allocations planned for the DySpan 2007 conference. We then describe how an implementation of CBPM is being used to provide multi-organizational policy management for a plastic radio testbed, included how policy decisions are securely communicated to an RF terminal.

II. Background

A. DARPA XG Policy Language

The DARPA XG Policy Language (XGPL) Framework

Manuscript received November 22, 2006. This material is based upon work partially supported by Science Foundation Ireland under Grant No. 03/CE3/I405 as part of the Centre for Telecommunications Value-Chain Research (CTVR) at Trinity College Dublin (TCD), Ireland.

K. Feeney is with the Knowledge and Data Engineering Group (KDEG) , Department of Computer Science and Statistics at TCD and is participating in the CTVR (kevin.feeney@cs.tcd.ie)

D. Lewis is with the Knowledge and Data Engineering Group, Department of Computer Science and Statistics and is participating in the CTVR. (corresponding author phone +353 1 896 2158, fax +353 1 6772204, dave.lewis@cs.tcd.ie)

P. Argyroudis is a member of the CTVR (argp@cs.tcd.ie)

K. Nolan is a member of CTVR at TCD (keithnolan@mee.tcd.ie_

D. O'Sullivan is with the Knowledge and Data Engineering Group, Department of Computer Science and Statistics and is participating in the CTVR

1-4244-0663-3/07/$20.00 ©2007 IEEE

aims to provide a means by which machine understandable policies can be defined in a highly flexible and traceable manner [2]. The design of the language aims to support the frequent changes to policies that apply to a particular radio system. The policies applicable to an RF system may change in response to: to changes in a wireless operator's business policy; to changes in the spectrum usage context of the RF systems or its mobility between administrative domains with different policies. In addition, the language aims to support consistency checking of policies and the easy introduction of new language concepts.

The XG policy language uses a description logic approach for describing facts, as standardized by the World Wide Web Consortium in the Web Ontology Language (OWL) [6] as part of its Semantic Web initiative. Such facts define concepts for use in policies that can be inherited from multiple existing concepts, simplifying the modeling of spectral resources and the extension of such models over time. Such facts can also be used to define constraints over the concepts used in policies. The use of OWL-based facts allows existing description logic reasoners to be employed in checking the consistency of policies and inferring new constraints on the application of policies.

XG policies consist of:

- a selector descriptor, which allows for easy filtering of relevant policies. This defines:
    - the authority that is establishing and enforcing the policy;
    - the frequency range or frequency group;
    - the region and time over which the policy applies;
    - the capabilities required of a device able to enforce the policy.
- an opportunity descriptor, which defines whether a valid opportunity exists
- a usage constraint descriptor which defines constraints on the device and environment under which the opportunity can be exploited, e.g. maximum transmit power in the available band.

Given an RF system that has detected an opportunity and requested a policy decision, by default all policy rules that satisfy the selector for the device and can conform to the opportunity constraints are applied. However, in common with other policy languages, the XG language allows the definition of meta-policies that specify rules about how other policy rules are enforced. More specifically the XGPL proposal offers the following meta-policy features:

- Grouping: This simply allows policies to be grouped together.
- Precedence: This list policies or policy groups in order of preferences so that a selection can be made when two or more policies match a given selector.
- Disjunction: This allows a set of policies to be tagged so that if more than one is applicable, the policy decision requestor can decide which to choose (rather than rely on a precedence mechanism)
- Delegation: This is only mentioned in outline currently, but it states that the delegation of policy authoring authority from one policy administrator requires that policies defined by the delegator be tagged to indicate whether or not it has precedence over potentially matching policies authored by the delegatee.

These mechanisms all present problems for policy authors. Maintaining a precedence ordering over a large set of policies can quickly become an onerous task, as every addition or change to a policy may require a re-analysis and re-ordering of policies. Grouping policies may ease this task by localizing such re-analysis, but this is largely dependent on how the groups are formed. Furthermore, relying on grouping to ease precedence may conflict with the need to group policies for other administrative reasons. As currently stated, the proposal for delegation also place a burden of additional precedence management on the policy author, while not addressing the need potentially revoke a delegation or to control of the forward delegation of authority by its recipient.

Resolving these issues is complex, and often dependent on the organizational and business context in which policies are being encoded. However, the current meta-policy semantics of XGPL are insufficient to express, and therefore to reason, about these issues. The work presented in this paper is motivated by the need to improve the current meta-policy handling scheme currently defined for XGPL to address several deficiencies that we observe.

Broadly the current XGPL meta-policy scheme offers no mechanism for representing organizational structuring. We envisage, however, that many of the challenges faced in successfully implementing policy-based management of dynamic spectrum access will derive more from the complex and fluid organizational structures involved rather than the complexity of the underlying resource being managed, i.e. access to the RF spectrum. This complexity and fluidity will arise from the proposals for fine-grained trading of spectral resources, supporting secondary markets and commons applications, with a level of openness that supports rapid innovation in technology, applications and business models.

Here, we propose integrating the existing XGPL language with the Community Based Policy Management (CBPM) scheme. CBPM is a powerful meta-policy mechanism designed to accurately reflect and respond to the decision making structure of complex, changing organizations, including federated organizations. The integration of DARPA XG and CBPM is made possible by two important factors:

- DARPA XG has been designed as an extensible language, with a knowledge-based language specification grounded in OWL, making it easily extendible by adding new facts and rules specified in OWL.
- CBPM is designed to be policy language neutral, so that it can provide organization-aware meta-policy handling mechanisms to any policy language with

well-defined applicability semantics.

In the following section we give a brief description of CBPM before detailing the CBPM extension to XGPL.

B. Community-Based Policy Management

The benefits brought by integrating CBPM with XGPL stem from the organizational modeling that CBPM uses as a basis for enforcing policies. CBPM uses the notion of *community* as the primary grouping abstraction with the aim of allowing groups within the organization itself to define communities to naturally reflect the changing nature of decision making (i.e. policy setting) authority. This contrasts with modern role-based access control systems [7][8], such as that used in IBM's Workplace, which typically require the services of external consultants to define roles and their policies. This approach is both expensive and brittle in handling frequent organizational change [9], as will inevitably be the case of a multi-organizational setting such as DSA. Communities towards the top of the hierarchy have the wider membership and more general function, while those toward the bottom have more narrow membership and more specific function. The hierarchy is designed to support organizational change, allowing new sub-communities to be formed and encouraging the delegation of decision making authority as far down the hierarchy as possible.

In CBPM, policies are associated with communities and communities are related to each other according to their relative authority over resources. Communities can form federations with other communities to share resources in controlled ways. Authority over resources is distributed through delegation and escalation, which are ongoing processes which allow the organization to re-organize itself to cope with changing requirements. The CBPM allows administrators to dynamically form a community hierarchy to represent a particular alignment of organizational units in such a way that any conflicts are resolved according to the hierarchy. Thus, for example, a national telecommunications regulator would be positioned in the community hierarchy in such a way that their decisions would over-ride those decisions made by commercial operators. The CBPM community hierarchy can be dynamically modeled in a decentralized way, allowing each organizational unit to define it's own structure and allowing them to operate autonomously of more senior communities and to establish their own policies, only constrained by the policies established by higher-level communities. These features make the CBPM well-suited to the problem of providing policy-based management of DSA, where multiple autonomous organizations, with overlapping spheres of responsibility, are responsible for establishing usage policy. The conceptual basis of CBPM is described in greater detail in the policy paper, by the same authors, also presented at DySPAN 2007.

The implementation of a CBPM System (CBPMS) is structured as in figure 1. At the highest level, the workings of the CBPMS can be divided into two different functions. Firstly, it serves as what is termed a Policy Decision Point (PDP) in the IETF architecture. In the most general terms, this function can be described as responding to events by evaluating the appropriate policies and returning the result of those policy evaluations if required. Secondly, it serves as a policy management system, corresponding with the Policy Management Tool of the IETF architecture, the function of which can be described, again in the most general terms, as responding to management requests by updating the state of the system in accordance with the rules for the operational semantics of the community based model and returning the result of that management request if desired.

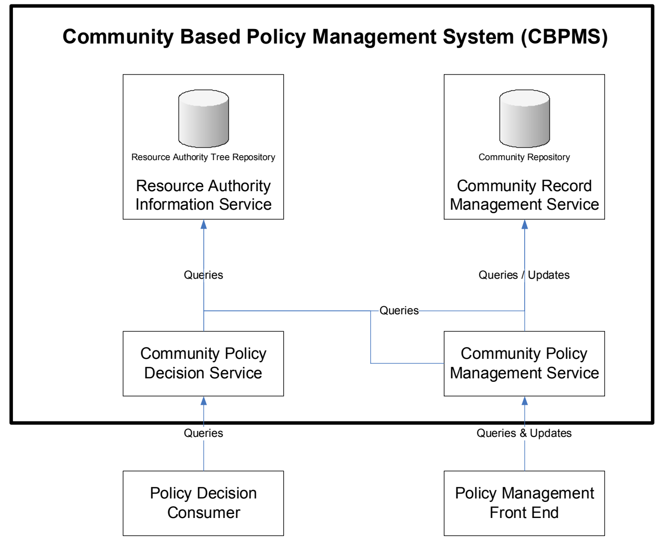

Figure 1: CBPM System Overview

In terms of the conceptual architecture, a service oriented paradigm is adopted. That is to say that the system is divided into a number of discrete providers of well-defined and stateless services and these services are orchestrated in order to provide the required functionality of the system. A service-oriented architecture eases the integration of the CBPMS with existing policy systems and network architectures, as well as allowing other systems to gain selective access to information about the state of the policy system. A top down approach to the definition of the services that make up the system is adopted, defining each component in the system in terms of simple services that it provides and the functions that it provides to the consumers of the service. The first level of analysis of the functioning of the CBPMS - as a service which acts as a PDP - is known as the Community Policy Decision Service (CPDS) and behaves as follows. An event occurs somewhere in the domain covered by the CBPMS, causing the service consumer to issue an appropriate policy decision request to the policy decision service provider. The policy decision service provider evaluates the appropriate policies for the request and returns the result of the evaluation to the consumer in a form that is understood by that consumer. The consumer may then convey these results to another entity in the universe if so required.

The primitives offered by the Community Record Management Service (see Table A) can be used by policy authors to provide meta-policy management for DSA. This involves interaction with the system from the Policy Management Tool, a front end consisting of web-based forms in our current implementation. It also involves the Policy Reasoning Service (PRS) which operates within the Community Policy Decision Service, evaluating policy decision requests from the policy decision consumer, in this case an RF terminal seeking access to a spectrum opportunity.

CBPM Primitive	Effect
genesis / expel	Create a new organizational model or remove an existing one
spawn / cull	create or destroy a sub-community
delegate / recall	Delegate authority from a community to a sub-community
policy / revoke	Define a policy for a community or remove one.
merge / liberate	Merge two organizations together or split an organization in two
federate / withdraw	Join a federation or leave one

Table A: Community Management Primitives

By making it easy to continuously change the organizational structure represented in the CBPM system to reflect changes in the real organization, the CBPM system can be used to document the structure and reason about potential changes. A potentially powerful benefit of this use of the CBPM system is that it enables conflicts that are detected between separately authored access control policies to be mapped to the point in the organization where the divestiture of the authority that was sanctioned. In this way the CBPM system can be used to resolve problems in the organizations authority structure as they are encountered through the detection of conflicting policies.

In CBPM, communities and the actions that can be performed upon them, are included as a hierarchical resource model, normally consisting of a hierarchical tree of targets and a hierarchical tree of actions. Delegation involves the allocation of a pair of nodes from these two trees from one community to another. This provides fine grain management of the delegation of authority to make both structural and policy changes in an organization.

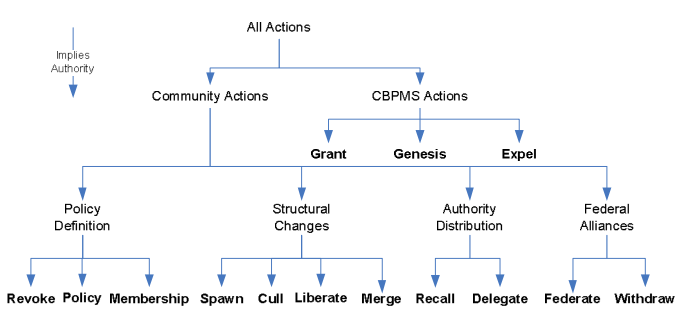

Figure 2: Action tree for the community resource

Figure 2 shows the built in action tree related to the community resource. The structure of the resource target tree in this case, is the structure of communities forming the hierarchy of authority in the organization concerned. This therefore provide inherent manageability of whom can write policies about what by controlling access to the community management primitives (see Table A) offered by the web service implementation of community Policy Management Interface and which map the leave of the community action tree.

Figure 3a give an example of such a resource tree of communities. This represents a simplified view of the hierarchy of authority involved in the administration of the cognitive radio license provide in Ireland to the Centre for Telecommunications Value Chain Research by the Irish regulators, COMREG. Figure 3b shows a refinement of this model where the root community is of all RF users in Ireland. COMREG is a sub-community of the root, but one which has been given authority over the ability to define new user groups (modeled as sub-communities) as well as to specify what other resources owned by the root community, namely the spectrum. COMREG are given wide power in regulating the spectrum, but must do so in response to various interest form the body of spectrum users. The Irish government plays a role in delegating this regulatory authority to COMREG, and the body of spectrum users has a role in influencing the policy of government in this regards through the usual mechanisms of democratic and representative government. Though we do not attempt to model the impact of everyday politics in our example of spectrum management using CBPM, this is feasible (we have already developed a rudimentary CBPM model of the Irish constitution). Similarly, spectrum management authority within CTVR is delegated to the CTVR board. Figure 3c, shows how spectrum management at a temporary event such as the DySpan conference could be managed. The organizing committee obtains the permission to use certain bands in the spectrum from COMREG. It forms in a federal community with companies such as the fictional DSA Inc in order to perform demonstrations at the event. This federal community delegates authority over authoring spectrum usage policies to the demonstration sub-community, but within the constraints, e.g. to ensure all demonstrators have fair access to a usable band. These examples serve to demonstrate the ability to progressively model a wide range of organizational influences on any particular management domain as those influences emerge as deserving of analysis in understanding, analyzing and managing change in that domain. These issues are examined in more depth in the spectrum management case study presented in the section IV.

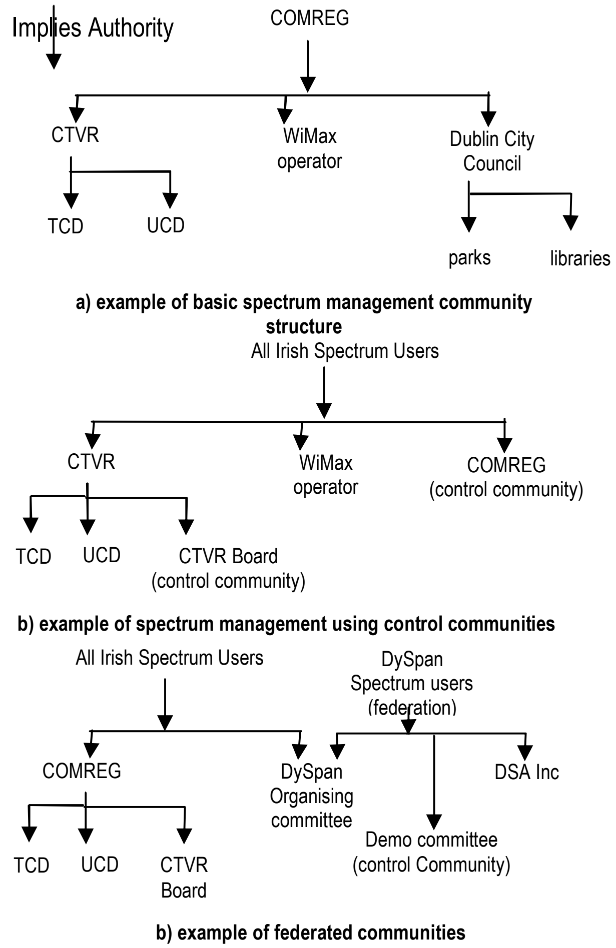

Figure 3: Example communities structures

Whenever a policy aware device requests a policy decision for a particular context from the CPDS, the community hierarchy is used to identify the communities that have authority to define policies for the context and to resolve any policy conflicts - in favor of policies defined in the community higher up the hierarchy. Thus, although each community can be managed autonomously, policy decisions respect the hierarchy of authority and any policies defined in the top-level community will always be enforced, regardless of the policies established by other communities.

III. LANGUAGE EXTENSION

In this section we define the CPBM scheme in terms of OWL extension to XGPL, using the short-hand syntax adopted in [2] for presenting new concept definition, new process definitions and new processing rules. To make clear the distinction between existing XGPL specification and the proposed extension we will use the naming prefix '`xgpl:`' for the existing XGPL definitions and '`cbpm:`' for the extensions.

The core concept of a community (Table B, definition 1) requires a reference to a parent community as well as to any federal community of which this is a sub-community. It contains a list of delegated resource authorities (Table B, definition 4) that it has received from these higher communities plus a list of membership policies and a list of community policies, defining the behavior that the community wishes to impose on the resources over which it has authority.# A Resource Authorities (Table B, definition 2) defines a parcel of authority specifying which target object and which action on that target a community can author policies about. A resource authority references a specific resource model (Table B, definition 3) when defining targets and actions. Within a resource model targets and actions are structured in separate trees, where the edge relationship has the semantics that permission to use a node implies permission to use all its child nodes. A delegation of a parcel of authority

No.	definition
1	`deftemplate cbpm:Cmty (slot id) (slot parent) (multislot federates) (multislot delegatedAuthorities) (multislot membershipPolicies) (multislot communityPolicies) )`
2	`(deftemplate cbpm:RsrcAuth (slot id) (slot resourceModel) (slot target) (slot action) )`
3	`(deftemplate cbpm:RsrcMdl (slot id) (slot resourceTree) (slot actionTree) )`
4	`(deftemplate cbpm:DlgtAuth (slot id) (slot delegatingCommunity) (slot resourceAuthority) )`
5	`(deftemplate cbpm:PlcyDcsnReq (slot id) (slot resourceAuthority) (slot communityId) (multislot context) )`
6	`(deftemplate xgpl:SelInst (slot id) (slot freqDesc) (slot regnDesc) (slot timeDesc) (slot devcDesc) )`

Table B: CBPM extensions to XGPL

In our general purpose implementation of the CBPMS a policy decision request (Table B, definition 4) contains the resource authority to which access is sought; the community, membership of which the requestor claims in making the request; and a series of contexts describing the state within which the request is made.

In integrating with XGPL, the community in the policy decision request should map to a Policy Administrator as identified in [1], however, the meta-policy processing related to this definition is replaced by the CBPM meta-policy processes. This still leaves the issue of how an entity requesting a policy decision request and that providing it, authenticate themselves to each other. This is addressed in more detail in section V.

The particular model of the resource authority in the request has a simple action, i.e. '`access`'. The target model however consists of an element of four dimensions, these being frequency, region, time and device, descriptors for which are already defined in XGPL. The target model for the requested resource authority could therefore correspond to a Selector Instance definition from XGPL (Table B, definition 4).

The context element of the policy decision request corresponds to the environment and device state that are mentioned in the XGPL specification, e.g. current weather conditions. This context does not form part of the resource authority, though in settings where not all the four element of the resource target are used, the remaining elements could instead be used as part of the context. This is the approach used in the case study below, where only the frequency element is used to form the resource model. This is consistent with current command and control approaches to spectrum access management, so we envisage frequency will form the basis of resource models as we move from static to dynamic spectrum access.

IV. CASE STUDY

As a case study familiar to the reader, we address the allocation of bandwidth to demonstrators at the DySpan 2007 conference in Dublin. This case study illustrates how the CBPM system can be used to model the management of dynamic access to wireless communications.

The Centre for Telecommunications Value-Chain Research (CTVR), Trinity College Dublin, Ireland has acquired dedicated spectrum from the Commission for Communications Regulation (COMREG) in Ireland for the duration of this conference. The frequencies are 'provisionally booked' for tests and demonstrations of software-defined radio, cognitive radio and dynamic spectrum access technology under the COMREG Wireless Test License Scheme from 16 April through 22 April 2007 (inclusive),.All current spectrum allocations are in the 230-440 MHz and 2-3 GHz band and are as in Table C

Channel	**Centre Freq. (MHz)**	**Max ERP**	**BW (MHz)**	**Mobile**
1	231.2250	1 W (0dBW)	1.75	Yes
2	233.0250	1 W (0dBW)	1.75	Yes
3	234.8250	1 W (0dBW)	1.75	Yes
4	236.6250	1 W (0dBW)	1.75	Yes
5	238.4250	1 W (0dBW)	1.75	Yes
6	386.8750	1 W (0dBW)	1.75	Yes
7	396.8750	10 W (10dBW)	1.75	Yes
8	406.9750	1 W (0dBW)	1.75	Yes
9	408.7750	10 W (10dBW)	1.75	Yes
10	436.8750	1 W (0dBW)	1.75	Yes
11	2056.0000	1 W (0dBW)	50.0	No
12	2231.0000	1 W (0dBW)	50.0	No

Table C: Dyspan DSA demonstration channel allocations

These frequencies are the centre carrier frequencies, with a channel bandwidth of 1.75MHz in the 230-440 MHz band and 50 MHz in the 2-3 GHz band. The booking specifies that the maximum Effective Radiated Power (ERP) permitted is 1W (0dBW) apart from Channel 7 and Channel 9 where a maximum power of 10W (10dBW) is permitted. Mobile operation is permitted in Dublin city using channels 1-10, but use of channels 11 and 12 are only permitted at the conference centre and at University of Dublin, Trinity College. One particular requirement to note is that there is a legacy assignment of the 436.875 MHz band (channel 10 above) to amateur radio (satellite/ATV), therefore, the management of this band must be included in the organizational model, in order to enable automatic policy conflict resolution.

In order to capture the requirements and model the organizational requirements of the domain, a community hierarchy is constructed using the *genesis* and *spawn* primitives offered by the CBPM system. Figure 5 shows the resulting community structure. The communities that are underlined are *"control communities"*, which means that they dictate the policies of their parent community. Thus, for example, the ITU dictates policies for global radio users, while COMREG dictates policies for radio users in Ireland.

Figure 5 Screenshot of CBPM community structure for spectrum management

Having created the community structure, authority for resources is distributed throughout the hierarchy using the CBPM *delegate* primitive. In this case study, there are two relevant resources; one representing the community structure itself and one representing the radio spectrum. In the above hierarchy all of the communities are self-managed with the exception of those that have control communities beneath them – this is implemented by delegating authority for these community resources to their control communities, while self-managed communities are simply given ultimate authority over their own communities using the CBPM *grant* primitive.

The spectrum is modeled as a simple hierarchical tree where the root represents the entire spectrum and each level beneath it represents a narrower band. Resource authorities representing nodes on this tree are delegated to the appropriate communities. Thus, for example, the entire spectrum, minus any bands that are exclusively reserved for international use, is delegated from the global radio users to the national radio users and to each of the nations. From there, each of the states, under the control of their respective governments or regulators, which act as their control communities, can delegate the nodes in line with their telecommunications assignment plan. Thus, for example, figure 6 shows a segment of the resource tree as seen by the CTVR, containing the first 5 channels that have been allocated to it.

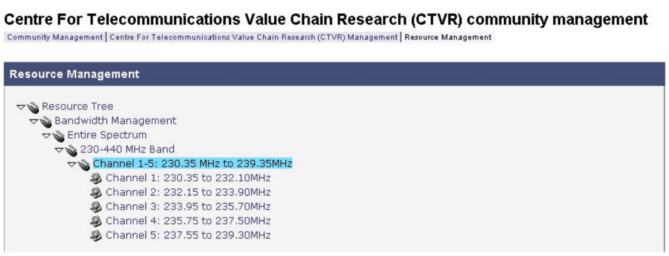

Figure 6: Screenshot of CTVR's spectrum resource

Having carried out the delegations, policies are defined in the various communities, using the CBPM *policy* primitive, in order to enact the various restrictions on the various bands. As COMREG is the control community of the community representing all Irish Radio users, it can define policies which apply to that group. Therefore, COMREG defines policies for its parent community to enforce the power-related restrictions on the various channels that it has delegated to the CTVR. These restrictions are specified as conditions which must evaluate to true using the CBPM built-in policy condition authoring tool for this domain. This tool, shown in figure 7, provides a convenient interface for the authoring of conditions related to spectrum assignment it works by mapping conditions to an underlying policy format which specifies which actions are permitted or denied in which conditions.

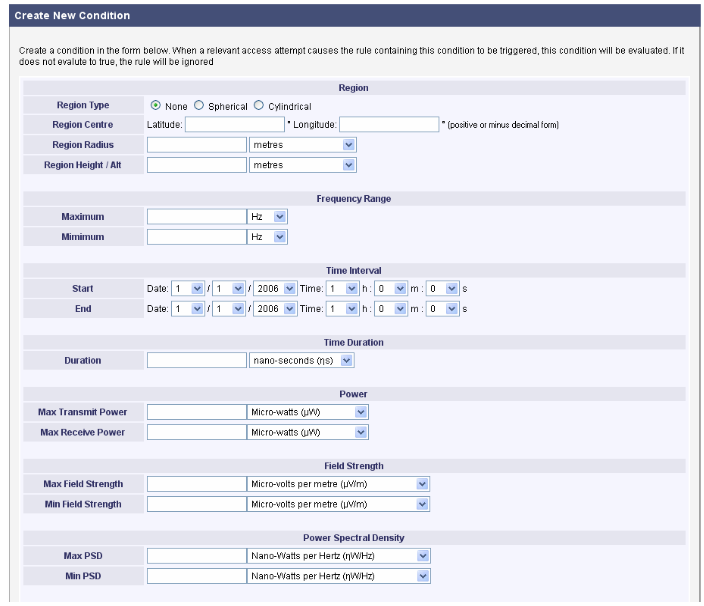

Figure 7: Screenshot of policy condition editing screen

COMREG specifies further policies which enforce the geographical restrictions that it wishes to impose upon users of the delegated bands. To achieve this, it specifies policy conditions, again using the tool, which limit permission to use the various bands to the relevant regions. Thus, a geographical region is defined, with coordinates and area corresponding to Dublin and another region is defined with a region corresponding to Trinity College Dublin. These restrictions are associated with the relevant channels as *"permit conditions"* and if they are not true, the permit policy will not be invoked and the policy decision will not permit usage of the band.

Having specified these policies, COMREG can allow the CTVR to self-manage and to author whatever policies it chooses to, and to define its own internal structure, without any risk that COMREG's policies will not be respected. The CBPM places a priority on policies which mirrors the organizational hierarchy. COMREG's policies have been defined in the community representing all radio users in Ireland and this community is higher in the hierarchy than the CTVR community, so its policies will have precedence over any defined within the CTVR community. This also means that the CTVR does not have to author policies to implement the restrictions mandated by COMREG – they are automatically enforced according to the CBPM policy search algorithm before any policies of the CTVR are evaluated.

It is this policy precedence algorithm which enables policy conflicts to be resolved by the CBPM. All policy conflicts between communities which have a direct hierarchical relationship are resolved in favor of the higher community. In cases where there is no direct hierarchical relationship, policy conflicts must be addressed at the nearest common ancestor of the conflicting communities.

To take an example of this approach to conflict analysis and detection in action, consider the management of conflicts between the amateur radio operators and users of channel 10 of the bandwidth dynamically allocated by the CTVR. In general, since legacy hardware generally won't have the capacity to dynamically alter its behavior, in such cases of conflict, the policy should be that when there is conflict, the device which has the capacity to dynamically alter its frequency should do so to avoid interference with the legacy device. According to our simplified community model, the nearest common ancestor of the two conflicting communities is the community of *Global Radio Users* and thus it is its control community, the ITU, which must define this policy. It simply uses the policy primitive to define a general-purpose rule which gives priority to all legacy applications in cases of conflict, thus resolving all such classes of conflict.

V. TESTBED IMPLEMENTATION

The CBPM DSA implementation provides several features which are not present in the XG architectural vision. In XG, there is an assumption that each device will include a policy reasoner. This is problematic for two reasons. Firstly, devices manufactured by third parties will have to be accredited to ensure that they operate correctly before they can be deployed in practice. Secondly, the requirement for an embedded inference engine dramatically increases the minimum complexity of the devices that use the system. In order to deal with this problem, the CBPM implementation allows policy rules to be specified in such a way so that they are evaluated and enforced on the policy server, rather than on the device.

The basic interaction between the policy-aware device and the policy management system in the CBPM implementation sees the device transmit a *context* to the CBPM service. This context is composed of an XG *selector description* and whatever other contextual information is available to the device's sensors, which is identical to an extended version of the XG *opportunity description*. The CBPM can respond with either

1. A *permit* decision, indicating that the device is permitted to access the spectrum in that context.
2. A *deny* decision, indicating that the device is not permitted to access the spectrum in that context.
3. A permit or deny decision accompanied by a *usage constraint* description, indicating that the device is permitted or denied access to the spectrum in that context as long as the usage constraints are upheld.

```
comment: COMREG is the root of DSA rights for
DySPAN'07
authorizer: "POLICY"
local-constants: COMREG = "rsa-
hex:3048024100a9c77a9be17f0da24316b973457cd412
be147fd026d2946500d61a436377161068cc4f15c089c5
7cf867285ad738ca1ac085a6407d0dcaab84ba3ee82d62
442d0203010001"
authorizer: "POLICY"
licensees: COMREG
conditions:
    app_domain == "IEEE DySPAN 2007" ->
"true";
```

```
comment: CTVR delegates authority over
DySPAN'07 to TCD
local-constants: CTVR = "rsa-
hex:3048024100bf787850c6bf4db379cec2a3d5548140
63a82e1aab9153a536ab52759be4a719e385450fe24d2a
8f153160eba4362613dc2ddf27cd1883f4e1294ae2a44a
c98f0203010001"
     TCD = "rsa-
hex:3048024100bb1ad7d33d2d46e4c81fc79dd8e7fdc9
1d6e524066fbc47cb1efff36e34b29ca76902781838636
d4e52080020162387f2e8c6e9866609cf25feef7e282f8
68e70203010001"
authorizer: CTVR
licensees: TCD
conditions:
    app_domain == "IEEE DySPAN 2007" &&
    region == "tcd.ie" ->
    {
     # in TCD after 18:30 radios are not
     allowed to operate
     @time >= 183000 -> "false";
    };
signature: "sig-rsa-sha1-
hex:5ea43b6d26cd95c9cf8687a348f261b95bca9001f5
128e79d96325883eb1abbc715623da80a15cd7fa4148a3
be79b98a204d6271fb80e336f22b733e4692e270"
```

Figure 8: Example policies encoded by Keynote

Thus, rather than transmitting all policies to the device, and requiring the device to contain an embedded policy reasoner, the CBPM implementation allows policies to be specified in such a way that they can be evaluated and enforced on the CBPM server, allowing the accredited kernels on the devices to be significantly simpler. However, it recognizes that certain constraints are better suited to run-time evaluation and enforcement by the device itself. For example, certain environmental parameters such as Power Spectral Density (PSD) may vary widely as a user moves about – rather than requiring the device to transmit a new context to the CBPM server every time this contextual information changes, it is much more efficient to transmit constraints regarding this parameter and trusting the device to enforce these constraints. On the other hand, other environmental factors may not even be available to the device – for example, most devices will not be able to access the current weather conditions in their location, whereas the CBPM server can use web-services to translate the device's coordinates into weather conditions. Thus, policy conditions which depend upon this parameter will have to be evaluated on the server. The CBPM DSA implementation allows managers to define whether each individual policy condition must be evaluated on the server, must be evaluated on the device, or whether it should be evaluated on the server if possible (i.e. if sufficient information is transmitted in the context).

In the CBPM DSA application, all policy rules are mapped to KeyNote policies, which are then evaluated by IBM's KeyNote security **policy** and trust management system. The CBPM community structure and the delegation of authority throughout it maps simply to KeyNote's delegation chains. KeyNote also takes care of the security of policy specifications, by managing policy certificates and checking policy signatures. Two examples of KeyNote policies, produced by the CBPM implementation for DSA are reproduced below. The first example encodes the community hierarchy in a way that can be verified by KeyNote. The second encodes the delegation of specific access rights from one community to another.

Finally, an example of a user's certificate is presented in figure 9.

```
comment: user is authorized to participate in
DySPAN'07
local-constants:
TCD =
"rsahex:3048024100bb1ad7d33d2d46e4c81fc79dd8e7
fdc91d6e524066fbc47cb1efff36e34b29ca7690278183
8636d4e52080020162387f2e8c6e9866609cf25feef7e2
82f868e70203010001"
user = "rsa-
hex:3048024100aca70bcec849d36eb78b82af668f9
8c61177d528073fb8f19c408c63f7558ea94c29f2f7a86
cf2bdbd22945e82c2890fcbbe7bde3eac3368cef89b1c2
fcbcde9 0203010001"
authorizer: TCDlicensees:
userconditions:
   app_domain == "IEEE DySPAN 2007" && region
==
    "tcd.ie"
     &&  # the following forbids user to
           further delegate authority
_ACTION_AUTHORIZERS ==
     user;signature: "sig-rsa-sha1-
hex:3fb7b9a56a2ed655b94dfeb0913c08ba8a5bfacee6
050ed14
a65adabcfdb7037732bced90672d47d57d36667bbb0855
f856c
8b23cfb31eaa7a0a663eef97e302"
```

Figure 9: Delegation of access rights encoded by KeyNote

VI. Conclusion and Future Work

In this paper we have proposed a sophisticated meta-policy extension to the DARPA XG policy language. This extension is an instance of an existing scheme based on the fine-grained control of delegation of authority between communities of users. The flexibility of cognitive radio and the resulting myriad of structure that can be employed in dynamic spectrum access means that the industry, including regulators, operators and users, may be entering a period of experimentation and one that may well result in multiple management schemes operating in parallel. DARPA XG has recognized this and supports it to an extent by specifying XGPL in OWL, thereby facilitating it extension. The meta-policy extension based on the CBPM scheme goes further in attempting to support changes in organizational structure as a natural part of the policy engineering process. This can involve creating new sub communities, federating communities and changing the distribution of decision making authority across a multi-domain DSA management organization.

Our further work will involve the full integration of the CBPM-based implementation of XGPL with the plastic radio testbed being developed by the CTVR project [10], as indicated by the schematic in figure 10.

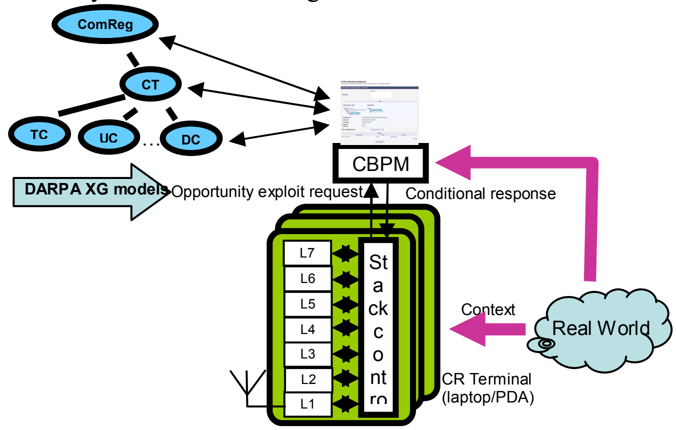

Figure 10: Integration of the CTVR cognitive radio with CBPMS

In addition an Eclipse-based rich client is being developed for DSA management using the CBPMS. This will include support for importing and reasoning about new policy terms expressed in OWL. The CBPMS is itself being developed to support runtime federation between CBPMS servers operated by differing organizations.

Acknowledgment

We would like to thanks Linda Doyle and the rest of the team involved in the CTVR plastic radio testbed in their support and assistance in developing this testbed.

References

[1] DARPA XG Working Group "DARPA XG Policy Language Framework, Request for Comments", version 1.0, prepared by BBN Technologies, Cambridge MA, USA, April 16 2004

[2] Berlemann, L. Mangold, S. Walke, B.H., Policy-based reasoning for spectrum sharing in radio networks, First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.

[3] Damianou,, N. C., A Policy Framework for Management of Distributed Systems, PhD Thesis, Department of Computing, Imperial College. London, U. K. 2002

[4] DAPRA XG Working Group, "The XG Vision Request for Comments". Version 2.0, prepared by BBN Technologies, Cambridge MA, USA, January 2004

[5] D. Lewis, K. Feeney, K. Foley, L. Doyle, T. Forde, P. Argyroudis, J. Keeney, D. O'Sullivan, Managing Policies for Dynamic Spectrum Access, 1st International IFIP TC6 Conference on Autonomic Networking (AN2006), Paris, France, September, 2006, LNCS 4195, Springer, 2006, pp285 - 297

[6] OWL Web Ontology Language Reference, available at: http://www.w3.org/TR/owl-ref/.

[7] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, Charles E. Youman, "Role-Based Access Control Models," Computer, vol. 29, no. 2, pp. 38-47, Feb., 1996.

[8] Lupu, E. C.. A Role-Based Framework for Distributed Systems Management. PhD Thesis, Department of Computing, Imperial College. London, U. K., July 1998.

[9] Jude, M., Policy-based Management: Beyond the Hype. In Business Communications Review, available from http://www.bcr.com/bcrmag/2001/03/p52.asp, March 2001. pp 52-56

[10] Doyle, L.E., Forde T.K. et al., " A Platform for Dynamic Spectrum EXperimentation ", under review for the First International Workshop on Technology and Policy for Accessing Spectrum (TAPAS), Boston, August 1-5 2006.