Policy-based Cognitive Radios for
Unmanned Aircraft Systems Command and Control

by

Suppapol Jaroovanichkul

B.Eng., Chulalongkorn University, 2007

A thesis submitted to the
Faculty of the Graduate School of the
University of Colorado in partial fulfillment of the requirement for the degree of
Master of Science
Interdisciplinary Telecommunications Program
2012
This thesis entitled:
Policy-based Cognitive Radios for Unmanned Aircraft Systems Command and Control
written by Suppapol Jaroonvanichkul
has been approved for the Interdisciplinary Telecommunications Program

__________________________
Prof. Timothy X Brown

__________________________
Prof. Douglas C. Sicker

__________________________
Prof. Harvey M. Gates

Date _____________

The final copy of this thesis has been examined by the signatories, and we find that both the content and the form meet acceptable presentation standards of scholarly work in the above mentioned discipline.
Abstract

Suppapol Jaroonvanichkul (M.S., Telecommunications)
Policy-based Cognitive Radios for Unmanned Aircraft Systems Command and Control
Thesis directed by Professor Timothy X Brown

There is increasing interest in Unmanned Aircraft Systems (UAS) as they can be used for various applications, such as border patrol and real estate photography. However, currently the widespread integration of UAS into the U.S. National Airspace System (NAS) is prevented by several problems. One such problem relates to the radio spectrum for Command and Control (C2), which is the communication link between the Ground Control Station and the Unmanned Aircraft for controlling the aircraft remotely. There are two aspects of the UAS spectrum problem: spectrum scarcity and static spectrum management. First, there is currently no dedicated spectrum for civilian UAS C2. Second, the static approach to spectrum management, where spectrum is assigned for long periods of time over large regions, makes spectrum underutilized for most of the times although it is fully allocated.

The UAS spectrum problem could be solved by the use of Policy-based Cognitive Radios. Policy-based cognitive radios could introduce innovative ways to acquire spectrum: using frequency bands otherwise neglected by UAS, spectrum leasing, and utilizing underused spectrum. Policy-based radios will also be an automatic tool to manage spectrum.

This thesis deals with the conceptual design of a policy-based cognitive radio system that could support UAS C2. The aim of this thesis is to explore the use of cognitive radios as a tool for spectrum management for UAS C2. We design a policy-based cognitive radio system to flexibly manage spectrum for UAS C2 while satisfying stakeholder requirements to support the operations of UAS. We identify requirements from the stakeholders’ perspective. We design
policies’ content to flexibly define rights to use spectrum and support UAS operations. We design mechanisms to distribute policies reliably and securely. The results of this thesis could be useful to the Federal Aviation Administration (FAA) and the UAS industry in enabling more integration of UAS in the NAS. Additionally, the results of this thesis could motivate possible cognitive radio solutions in other areas such as vehicular communications or public safety.
Dedication

To my parents.
Acknowledgements

I would like to thank my thesis adviser, Prof. Tim Brown, for all his guidance, encouragement, and support. He introduced me to the world of research in the Research Method class and gave me an opportunity to work on this project. I would like to thank Prof. Doug Sicker and Prof. Harvey Gates for contributing their time to serve on my committee and providing feedback on the thesis.

I also would like to thank David Jones and Filip Perich of the Shared Spectrum Company for useful discussion during the research.

I appreciate the funding for this project from the Federal Aviation Administration. I also appreciate the National Broadcasting and Telecommunications Commission of Thailand, which provided a scholarship for my Master’s study.

Last but not least, I would like to thank my family for their endless love and support. I also would like to thank my friends for their friendship and all the memorable moments we had together.
# Contents

1. Introduction................................................................................................................... 1  
   1.1 Unmanned Aircraft Systems (UAS) ................................................................. 1  
   1.2 UAS Spectrum Problem....................................................................................... 1  
      1.2.1 Spectrum scarcity....................................................................................... 1  
      1.2.2 Static spectrum management .................................................................... 2  
   1.3 Policy-based Cognitive Radios........................................................................... 2  
   1.4 Why policy-based cognitive radios for UAS C2?............................................. 3  
      1.4.1 Policy-based radios could resolve spectrum scarcity............................... 3  
      1.4.2 A Policy-based radio system will be an automatic tool to manage spectrum 5  
   1.5 Research Question............................................................................................... 6  
   1.6 Scope................................................................................................................... 7  
   1.7 Importance......................................................................................................... 7  
   1.8 Methodology....................................................................................................... 7  
   1.9 Thesis Outline.................................................................................................... 8  

2. Background and Related Work ............................................................................. 9  
   2.1 UA Classes........................................................................................................ 9  
   2.2 UAS C2 Architecture....................................................................................... 10  
   2.3 UAS Phases of Flight.................................................................................... 12  
   2.4 Airspace Classes............................................................................................ 13  
   2.5 Cognitive Radio Functionalities ..................................................................... 14  
   2.6 Related Work.................................................................................................. 15  

3. Requirements Analysis.......................................................................................... 17  
   3.1 Stakeholder Analysis....................................................................................... 17  
   3.2 Stakeholder Requirements............................................................................... 19  
   3.3 UAS Use Cases and Radio Functionalities..................................................... 22  

4. Policy Authoring.................................................................................................... 28  
   4.1 Models of Spectrum Access........................................................................... 28  
   4.2 Background on Policies.................................................................................. 30  
      4.2.1 Implications of policy-based cognitive radios for spectrum management 32  
   4.3 Hierarchy of Policy Authors........................................................................... 34  
   4.4 Policy Parameters............................................................................................ 35  
      4.4.1 Policy Author............................................................................................. 35  
      4.4.2 Policy Receiver......................................................................................... 36  
      4.4.3 Time.......................................................................................................... 36  
      4.4.4 Frequency.................................................................................................. 37  
      4.4.5 Locations.................................................................................................... 37  
      4.4.6 Sublease Eligibility.................................................................................. 38  
      4.4.7 Phase of Flight ......................................................................................... 39  
      4.4.8 Technical Rules......................................................................................... 39  
   4.5 Spectrum Awareness....................................................................................... 40  
      4.5.1 Spectrum Sensing..................................................................................... 40  
      4.5.2 Geolocation and Databases..................................................................... 41  
      4.5.3 Beacon...................................................................................................... 42  
      4.5.4 Analysis..................................................................................................... 42
List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Direct control architecture</td>
<td>10</td>
</tr>
<tr>
<td>2.2</td>
<td>Control via satellite architecture</td>
<td>11</td>
</tr>
<tr>
<td>2.3</td>
<td>Control via cellular-like network architecture</td>
<td>11</td>
</tr>
<tr>
<td>2.4</td>
<td>UAS phases of flight</td>
<td>13</td>
</tr>
<tr>
<td>2.5</td>
<td>Airspace classification</td>
<td>14</td>
</tr>
<tr>
<td>3.1</td>
<td>Cognitive Radio Architecture for Direct Control</td>
<td>23</td>
</tr>
<tr>
<td>3.2</td>
<td>Cognitive Radio Architecture for Control via Satellite</td>
<td>24</td>
</tr>
<tr>
<td>3.3</td>
<td>Cognitive Radio Architecture for Control via Cellular-like Network</td>
<td>24</td>
</tr>
<tr>
<td>4.1</td>
<td>Models of Spectrum Access</td>
<td>29</td>
</tr>
<tr>
<td>4.2</td>
<td>An “upside down wedding cake” shape for defining locations</td>
<td>38</td>
</tr>
<tr>
<td>4.3</td>
<td>Radio Horizon Geometry</td>
<td>44</td>
</tr>
<tr>
<td>4.4</td>
<td>Curve of UA Altitude and Separation Distance</td>
<td>44</td>
</tr>
<tr>
<td>4.5</td>
<td>Curve of Availability and UA Altitude</td>
<td>44</td>
</tr>
<tr>
<td>4.6</td>
<td>Hierarchy of Policy Authors Example</td>
<td>48</td>
</tr>
<tr>
<td>5.1</td>
<td>Web Architecture</td>
<td>54</td>
</tr>
<tr>
<td>5.2</td>
<td>Chain Architecture</td>
<td>55</td>
</tr>
</tbody>
</table>
List of Tables

Table 1.1 - Throughput Requirements of a UAS ................................................................. 6
Table 2.1 – UA Classification .......................................................................................... 9
Table 3.1 - System’s Stakeholders .................................................................................. 18
Table 3.2 - Stakeholder Requirements ......................................................................... 20
Table 3.3 - UAS Use Cases and Associated Functionalities ........................................... 27
Table 4.1 - Policies of Operator X ................................................................................. 51
Table 5.1 - Subset Examples ......................................................................................... 62
Chapter 1

Introduction

1.1 Unmanned Aircraft Systems (UAS)

An unmanned aircraft system (UAS) consists of an aircraft and the relevant “associated elements—the control station and communications links” [1]. Traditionally, UAS have been used primarily in military operations [9]. There is also increasing interest in UAS for civilian operations, as they can be used for various applications, such as border patrol, firefighting, and real estate photography [1]. RTCA, Inc., an organization that provides recommendations to the Federal Aviation Administration, estimated that by 2030, the demand for UA operating in the United States National Airspace System (NAS) will be more than 10,000 UA [13]. However, currently the widespread integration of UAS into the NAS is prevented by several problems. One such problem relates to the radio spectrum for Command and Control (C2) Communications, which is the communication link between the Ground Control Station and the Unmanned Aircraft for controlling the aircraft remotely.

1.2 UAS Spectrum Problem

There are two aspects of the UAS spectrum problem: spectrum scarcity and static spectrum management.

1.2.1 Spectrum scarcity

RTCA has estimated that the spectrum requirement for UAS C2 is at least 13 MHz [14]. However, there is currently no dedicated spectrum for civilian UAS C2. While the military has spectrum allocations for UAS, they are limited and not sufficient for operations [18]. All useful bands for radio communications have been allocated. Allocation of spectrum on a global basis is controlled by international agreements, which are handled by the World Radio Conference [18].
In Agenda 1.3 of the World Radio Conference (WRC) 2012, there will be a discussion of possible allocation of spectrum for UAS [17]. However, in general, spectrum allocation agreements are difficult and slow to be changed [18]. As of the time this thesis is written, it is unclear as to whether there will be spectrum bands allocated for UAS operation. Even if there are bands dedicated to UAS use, there could be years of delay in spectrum refarming - waiting for the existing spectrum users to vacate the bands.

1.2.2. Static spectrum management

While spectrum is fully allocated, paradoxically, studies show that spectrum is underutilized for most of the times. This results from the currently static approach to spectrum management, where a large amount of spectrum is assigned for long periods of time over large regions [6]. Additionally, with “manual” spectrum management, deployment of systems is troublesome. If there are conflicts in frequencies assigned, the time needed to resolve such conflicts can be substantial. For example, Griswold [18] has illustrated that “In Iraqi Freedom, the Army’s Hunter [UAS] did not operate for the first 30 days in-theater because it was awaiting frequency deconfliction in order to obtain operational frequencies to use.”

The UAS spectrum problem could be solved by the use of Policy-based Cognitive Radios described in the next section.

1.3 Policy-based Cognitive Radios

A cognitive radio is “a radio that can change its transmitter parameters based on interaction with its environment” [6]. This implies two characteristics: Cognitive capability and Reconfigurability. Cognitive capability refers to the radio’s ability to “learn” its environment, such as spectrum awareness. Reconfigurability refers to the radio’s ability to “change” its transmitter parameters, such as transmitted frequency [6].
A policy-based radio is, according to the SDR Forum [5], a “radio in which the behavior of communications systems is governed by machine-interpretable policies that are modifiable.” Policies are “set of rules imposed by stakeholders’ preferences intended to accomplish some goals” [23] and “determine the radio behavior in the network” [24]. Conventional radios’ policies are hard-wired in the radio firmware and cannot be changed easily. However, policy-based radios separate policies from the radio firmware [23]. This allows policies to change dynamically and enables more flexible spectrum management [25]. Policies are written in a policy language, which is a machine readable format. We describe policy authoring in Chapter 4.

1.4 Why policy-based cognitive radios for UAS C2?

We discuss why policy-based cognitive radios could help solve the UAS C2 spectrum problem as follows.

1.4.1 Policy-based radios could resolve spectrum scarcity.

Policy-Based Cognitive Radios could help solve the spectrum scarcity problem because they can introduce innovative ways to acquire spectrum. As Griswold [18] pointed out, “[s]ome future challenges can be alleviated by several possible alterations in the way spectrum-dependent systems are acquired.” Such innovative ways to acquire spectrum are described as follows:

1. Frequency agility could allow the use of frequency bands otherwise neglected by UAS in some situations.

With an ability to operate in several frequency bands subject to the policies given, policy-based cognitive radios can flexibly switch the operating frequency depending on different conditions e.g. different phases of flight or location. For example, some bands that are not specifically designated for aeronautical use (e.g. the 2.4 GHz ISM band) may be allowed for UAS operations for some phases of flight (e.g. preflight) where some packet loss would still be
tolerable and interference with other users is limited. This will be useful, for example, when high-quality spectrum bands might be able to accommodate only a limited number of UAS. This limited high-quality band can be avoided by some UAS in certain phases of flight where they use other bands instead. Then they can switch to those high-quality bands later in more critical phases of flight e.g. takeoff and landing.

In fact, some researchers in the UAS community have recognized the benefits of frequency agility. For example, Carney [46] suggested that “UAS should have the ability to reprogram to a wide range of frequencies as required.” Additionally, Weiger [37] argued that “A critical technology enabling capability for unmanned systems is agile frequency spectrum management. As UAS proliferate within a given theater of operations, agile management of the frequency spectrum would maximize operations within the limits of any frequency band.”

2. The policy-based approach could encourage spectrum leasing as a way to acquire spectrum.

Spectrum leasing [38] is an agreement where a spectrum holder leases its spectrum to another spectrum user. Machine readable policies can be used to define lease terms in a spectrum leasing agreement. Machine readable policies allow lease terms to be defined precisely and be followed strictly. So, the policy-based approach could encourage spectrum holders’ willingness to lease their spectrum.

Additionally, the policy-based approach reduces transaction costs as spectrum leasing can be set up automatically and quickly. This could also encourage more leasing transactions.

Policies can be used to define a time limited lease, which is “a set of rights” to use spectrum that is valid for a specified period [22]. The time limited nature limits the risk even if
the lease terms are later found to be unfavorable to either the lessor or the leasee. Time limited leases will be described in Chapter 4.

3. Spectrum awareness could enable the utilization of underused spectrum.

While all useful bands for radio communications have been allocated, research shows that there is much underused spectrum, also referred to as “white spaces” [12]. Cognitive radios have spectrum awareness capabilities, allowing the radios to find white spaces and utilize them. Therefore, this new spectrum access approach could help solve spectrum scarcity.

1.4.2 A Policy-based radio system will be an automatic tool to manage spectrum.

Policy-based radios will enable automatic spectrum management. For example, if there is any policy conflict, the radio will automatically resolve it. Additionally, with little human intervention needed, human error or dishonesty can be mitigated.

We have argued that policy-based cognitive radios are a solution to the UAS spectrum problem. However, unlike other cognitive radios, UAS cognitive radios will have unique challenges. For example, UAS require higher reliability for communication links as the flight safety is of the utmost importance. UAS communication availability requirements exceed 99.8% [4]. In order to meet these stringent requirements, innovative allocations of multiple spectrum bands may be required to have the required redundancy. The RTCA is already proposing multiple radios to meet these needs. Multiple radios that are able to adaptively choose different bands could provide reliability above what is required at lower costs. UAS can also fly at high altitudes so that the third dimension, altitude, should be considered, for example, when specifying UAS locations and cognitive radio policies. Additionally, UAS have bandwidth needs that change with the operational phase. Bandwidth requirements for telecommand and telemetry for different operational phases are shown in Table 1.1 [14].
Table 1.1 - Throughput Requirements (bps) of a UAS

<table>
<thead>
<tr>
<th>Operational Phase</th>
<th>Mode</th>
<th>Throughput (bps)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Telecommand Uplink</td>
</tr>
<tr>
<td>Pre-Flight</td>
<td>Manual</td>
<td>183</td>
</tr>
<tr>
<td>Terminal (Departure)</td>
<td>Manual</td>
<td>2386</td>
</tr>
<tr>
<td></td>
<td>Auto</td>
<td>775</td>
</tr>
<tr>
<td>En Route</td>
<td>Manual</td>
<td>1201</td>
</tr>
<tr>
<td></td>
<td>Auto</td>
<td>289</td>
</tr>
<tr>
<td>Terminal (Arrival)</td>
<td>Manual</td>
<td>4606</td>
</tr>
<tr>
<td></td>
<td>Auto</td>
<td>1246</td>
</tr>
<tr>
<td>Post-Flight</td>
<td>Manual</td>
<td>1</td>
</tr>
</tbody>
</table>

1.5 Research Question

This thesis deals with the conceptual design of a policy-based cognitive radio system that could support UAS C2. The aim of this thesis is to explore the possibility of using cognitive radios as a tool for spectrum management for UAS C2. The research question in this thesis is: *How do we design a policy-based cognitive radio system to flexibly manage spectrum while satisfying stakeholder requirements in order to support the operations of UAS C2 and ultimately solve the UAS spectrum problem?*

There are a number of sub-problems as follows:

1. *What are the system’s requirements?* We identify requirements from the stakeholders’ perspective.

2. *How should the policies be defined?* We identify policies’ content to define rights to use spectrum and support UAS operations.

3. *How should policy distribution work?* We identify mechanisms to distribute policies efficiently, robustly, and securely.
1.6 Scope

The scope of this thesis deals with the architecture of a policy-based cognitive radio system supporting civilian UAS C2 in the United States, including: requirements analysis, policy authoring, and policy distribution. Some problems that are related to but out of scope of this thesis include:

- Optimization of communications performance by cognitive radios;
- The frequency bands that should be used for UAS C2; and
- Implementation of a prototype of the system.
- Military systems and non-US-based systems (although some ideas in this thesis may apply).

1.7 Importance

This thesis has importance to two main groups of audience: the UAS community and the cognitive radio community. For the UAS community, this thesis could provide recommendations to the Federal Aviation Administration (FAA), RTCA, and the UAS industry to enable more integration of UAS in the NAS.

For the cognitive radio community, this thesis shows how cognitive radios could be implemented for a specific application like UAS C2. Currently, little of the cognitive radio research in the literature deals with applications of cognitive radios in particular domains. The results of this thesis could motivate possible cognitive radio solutions in other areas such as vehicular communications or public safety.

1.8 Methodology

The methodology for this research is as follows:
- Identify the system’s stakeholders and their requirements. For example, an UA operator is one of the stakeholders and one of its requirements is that the system ensures flight safety.

- Identify operational scenarios of UAS and the operational spectrum requirements. For example, one of the scenarios is that an UAS is in its preflight phase. Identify functionalities of radios to support these scenarios.

- Based on the stakeholder and operational requirements, develop a policy definition framework.

- Identify the requirements for policy distribution and study mechanisms to handle them.

- If there are several design alternatives, evaluate each of the alternatives, and suggest the scenarios where each is most appropriate.

1.9 Thesis Outline

- Chapter 2 discusses background knowledge and related work.

- Chapter 3 describes requirements analysis. We identify stakeholders, their requirements, operational scenarios, and policy functionalities.

- Chapter 4 describes policy authoring, including important policy parameters.

- Chapter 5 describes policy distribution, including policy integrity and policy authority.

- Chapter 6 concludes the thesis and provides some directions for future work.
Chapter 2

Background and Related Work

In this chapter, we provide a brief background. We describe UA classes, UAS C2 architecture, phases of flight, airspace classes, and cognitive radio functionalities. We also survey some related work.

2.1 UA Classes

UA can be classified as shown in Table 2.1. They range from handheld, toy-like aircraft to large, long range aircraft such as Global Hawk.

<table>
<thead>
<tr>
<th>Categories</th>
<th>Maximum Takeoff Weight (kg)</th>
<th>Range (km)</th>
<th>Altitude (m)</th>
<th>Endurance (hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nano</td>
<td>&lt; 0.025</td>
<td>&lt; 1</td>
<td>100</td>
<td>&lt; 1</td>
</tr>
<tr>
<td>Micro</td>
<td>&lt; 5</td>
<td>&lt; 10</td>
<td>250</td>
<td>1</td>
</tr>
<tr>
<td>Mini</td>
<td>&lt; 30</td>
<td>&lt; 10</td>
<td>150-300</td>
<td>&lt; 2</td>
</tr>
<tr>
<td>Close Range</td>
<td>150</td>
<td>10-30</td>
<td>3,000</td>
<td>2-4</td>
</tr>
<tr>
<td>Short Range</td>
<td>200</td>
<td>30-70</td>
<td>3,000</td>
<td>3-6</td>
</tr>
<tr>
<td>Medium Range</td>
<td>1,250</td>
<td>70-200</td>
<td>5,000</td>
<td>6-10</td>
</tr>
<tr>
<td>Medium Range Endurance</td>
<td>1,250</td>
<td>&gt; 500</td>
<td>8,000</td>
<td>10-18</td>
</tr>
<tr>
<td>Low Altitude Deep Penetration</td>
<td>350</td>
<td>&gt; 250</td>
<td>50-9,000</td>
<td>0.5-1</td>
</tr>
<tr>
<td>Low Altitude Long Endurance</td>
<td>&lt; 30</td>
<td>&gt; 500</td>
<td>3,000</td>
<td>&gt; 24</td>
</tr>
<tr>
<td>Medium Altitude Long Endurance</td>
<td>1,500</td>
<td>&gt; 500</td>
<td>14,000</td>
<td>24-48</td>
</tr>
<tr>
<td>High Altitude Long Endurance</td>
<td>12,000</td>
<td>&gt; 2000</td>
<td>20,000</td>
<td>24-48</td>
</tr>
</tbody>
</table>

The classes of UA have implications for communications in two aspects. First, the size and weight of the UA determines how large a transceiver can be installed on it. Second, the range of the UA determines the appropriate architecture for C2 communications. UAS C2 Architecture is discussed in detail in Section 2.2. Smaller aircraft fly within limited distance from the ground control station, so direct control architecture can be used. Larger aircraft can fly far
away from the ground control station, so control via satellite architecture or control via cellular-like network architecture should be used.

2.2 UAS C2 Architecture

UAS includes more than just an aircraft. It also includes the control station (CS) and intervening communication links. RTCA-SC 203 [20] has proposed three types of possible UAS C2 architecture as follows.

1. **Direct control architecture.** The UA is within line of sight (LOS) of the control station or is in close proximity. These can range up to tens of miles for larger aircraft and more capable radio systems or less than a mile for smaller or simpler systems. The architecture is shown in Figure 2.1. The dotted line indicates a wireless link.

![Figure 2.1 - Direct control architecture](image)

2. **Control via satellite architecture.** The UA is able to operate beyond line of sight (BLOS) of the control station. The control station communicates with the UA via a satellite system, consisting of a satellite earth station and a satellite. Generally, these are on larger aircraft but Iridium phone-based satellite links have been used for aircraft as small as the Aerosonde [21].
The architecture is shown in Figure 2.2. The solid line indicates a ground-based network such as a telephone line, dedicated data link, or other network.

![Figure 2.2 - Control via satellite architecture](image1)

3. **Control via cellular-like network architecture.** There is a nationwide network of base stations. The control station communicates with the UA via a base station. Operationally, this may require radios that require the capability to handoff from one base station to another. The specific handoff mechanism is outside the scope of this thesis although we consider the spectrum and policy impact. The system is not yet in existence although there is a nationwide cellular for aircraft passenger voice and data [27].

![Figure 2.3 - Control via cellular-like network architecture](image2)
Different architectures may be used at different portions of flight. For example, Predator uses a direct control architecture for takeoff and landing and a control via satellite architecture for en route. Another aircraft might use a control via cellular-like network architecture over the continental United States and a control via satellite architecture over the ocean.

2.3 UAS Phases of Flight

A UAS flight can be categorized into several phases. UAS phases of flight are as follows [29]:

**Flight Planning**: This phase “begins when flight tasking is received, and ends with…uploading of the Flight Plan” [29].

**Start & Taxi**: In this phase, the C2 link is established. The UA engine is started. Pre-taxi activities, such as taxi checklists, are performed. The UA rolls down the runway to the takeoff location.

**Takeoff & Departure**: This phase begins when the UA leaves the ground from the departure location. The flight altitude is increasing. The phase concludes when the ATC communications is transferred from departure control to regional or en route ATC authority.

**En route**: This is the phase after takeoff and before approach. Compared to aerial work, en route travel is more direct.

**Aerial Work**: This “is a preplanned or unplanned operation…that may require special flight plan filing and handling” [29]. Aerial work could involve loitering, back and forth search patterns, target following, etc.

**Descent & Approach**: “The UA…commences an approach in anticipation of landing” [29]. The flight altitude is lowering until a “final approach point” [29].
Terminal & Landing: This phase starts when the UA “arrives in the airfield area” [29]. The UA “lands, reduces its speed, and exits the runway” [29].

Post Landing: The UA clears the active runway and is parked.

In addition, there could be an emergency or unexpected operation if the UAS has a failure preventing normal operation [28], [29].

These phases of flight can be illustrated in Figure 2.4.

![Figure 2.4 - UAS phases of flight (from Figure ES-1 in [29])](image)

The phases of flight are related to the bandwidth, delay, and reliability requirements [14]. So, different policies should be assigned to accommodate these various requirements.

2.4 Airspace Classes

The US airspace is categorized into several classes: class A, B, C, D, E, and G [33, 34]. These are used to organize and manage flight operations in the national airspace system by imposing restrictions on which aircraft can enter each class and under what conditions.

Class A: Controlled airspace from 18,000 feet mean sea level (MSL) to flight level (FL) 600 (i.e. 60,000 feet above sea level).

Class B: Controlled airspace from the surface to 10,000 feet MSL around the busiest airports.
**Class C**: Controlled airspace from the surface to 4,000 feet above ground level (AGL) over the airport elevation around airports

**Class D**: Controlled airspace from the surface to 2,500 feet AGL over the airport elevation around smaller airports

**Class E**: Controlled airspace that is not class A, B, C, or D

**Class G**: Airspace that is not class A, B, C, D, or E. This class is normally uncontrolled.

These classes are illustrated in Figure 2.5.

![Figure 2.5 – Airspace classification](image)

The classes of airspace are relevant to policies because the policies might be defined in terms of geographic regions using airspace around airports (class B, C, and D) or for different elevations (e.g. class A).

### 2.5 Cognitive Radio Functionalities

According to Akyildiz et al [6], there are four main functionalities of cognitive radios as follows:

1. **Spectrum Awareness**. Cognitive radios identify available white space spectrum.
2. **Spectrum Decision.** Cognitive radios select a channel for communications based on the available spectrum and policies.

3. **Spectrum Sharing.** As there may be multiple cognitive radio users trying to access the same spectrum band at the same time, there is a protocol to prevent multiple users from interfering with each other.

4. **Spectrum Mobility.** As spectrum availability could change, cognitive radios will vacate the portion of spectrum that is no longer available and will switch to another portion of spectrum so that the communications can continue.

In Chapter 3, we describe how these functionalities relate to UAS operational scenarios. We discuss spectrum awareness in Section 4.4. We do not describe specific protocols to implement spectrum decision, spectrum sharing, and spectrum mobility.

### 2.6 Related Work

RTCA, Inc. is an organization that provides "recommendations regarding communications, navigation, surveillance, and air traffic management" to the Federal Aviation Administration (FAA) for “policy, program, and regulatory decisions.” SC-203 is an RTCA special committee responsible for recommendations about UAS. SC-203 has developed various documents about UAS communications requirements. For example, in “RTCA SC-203 UAS Airspace Integration Architecture Description” [29], the UAS phases of flight and the various types of information exchange in each phase are described.

Cognitive radios are an emerging area of research in wireless communications. A comprehensive survey of the area was provided by Akyildiz et al [25]. The concept of cognitive radios was pioneered by Mitola [35] in the late 90s. The problem of underutilization of the radio spectrum, reported in the FCC’s spectrum policy task force [36] has spurred interests in the area.
The FCC has created regulations allowing cognitive radio to access unlicensed TV white space [12].

There are several directions of cognitive radio objectives. Much research has focused on utilizing white spaces by developing spectrum awareness techniques: sensing [6], geolocation and databases, and beacons [32]. Some research has studied to develop the “intelligence” of radios using machine learning approaches so as to automatically optimize communications performance [10]. Some research has explored cognitive radio applications [45], such as railway communications [8] and public safety [16].

There has been some research on a policy-based approach for cognitive radios. In this aspect, it focuses on using policies as a way to efficiently control radio behavior. Perich [3] has described an architecture of policy-based cognitive radios “as part of the DARPA NeXt Generation communications program.” Wilkins et al. [7] also described an architecture of policy-based cognitive radios but used a different policy language. These are related to our work as they solve a problem of defining policies to specify spectrum to use. But their work are for general applications and do not consider issues specific to UAS e.g. phases of flights, in defining policies.

Some research has explored issues related to cognitive radio policy distribution. In geolocation and databases [32], a query containing the location information of a cognitive radio is sent to the database. The database returns information about available channels at the location, which is similar to a policy containing information about available spectrum. Recently, the FCC has designated database managers for TV white space access [19]. Traditional security concepts such as digital signatures and encryptions are well established in the literature [41] and can be applied toward our research.
Chapter 3

Requirements Analysis

In this chapter, we provide a requirements analysis for the proposed policy-based radio system. We identify the system’s stakeholders and their requirements. We also consider use cases to obtain radio functionalities.

3.1 Stakeholder Analysis

In this section, we identify the stakeholders of the system. Traditionally, many stakeholder analyses in the literature focus on stakeholders within an organization. However, for our proposed system, stakeholders should be considered in terms of several organizations. According to [11], a stakeholder is “any individual, group, organization or institution that can affect or be affected (in a positive or negative way) by the system under study and that has direct or indirect influence on the requirements.” There are often conflicting interests among stakeholders [11].

Stakeholder Analysis is a tool widely used in system engineering as stakeholders are the source of a project’s requirements [11]. Stakeholders can influence the success of the project. For example, if any of their requirements are not met, they might oppose the project. Therefore, it is important that we identify the project’s stakeholders and their requirements so that the project will be likely to succeed.

We identify stakeholders in terms of two aspects: roles and domains. The first aspect is the role of the stakeholder. We can identify three main roles in policy-based radios for UAS: New entrants, Incumbents, and Regulators. The second aspect is the domain of the stakeholder. We can identify two domains: Aviation and Spectrum. Based on these two aspects, we show the stakeholders in Table 3.1.
We describe the stakeholders as follows:

**Unmanned Aircraft System Operators** are considered new entrants in terms of aviation and spectrum as they want to employ new UASs in the NAS and use spectrum for C2.

**Manned Aircraft Operators** are considered incumbents in the aviation domain.

**Other Spectrum Users** are incumbents in the spectrum domain.

The Federal Aviation Administration (FAA) regulates UA flights in the national airspace system. It also oversees the Air Traffic Organization, which provides air traffic control services.

Air Traffic Controllers (ATC) control the traffic of aircraft, including UA, that operate in controlled airspace (class A to E).

The Federal Communications Commission (FCC) assigns and regulates non-federal use of spectrum. This includes spectrum for commercial use, such as the TV bands. The FCC has allowed secondary access to unused TV spectrum [12]. If UAS used the TV white space spectrum, for example, the FCC would play an important role in C2 communications.

The National Telecommunications and Information Administration (NTIA) regulates federal use of spectrum. This includes the spectrum assigned to the Federal Aviation Administration (FAA).

We note that there might be new entities emerging after the design of the system, such as spectrum managers and spectrum brokers (discussed in Chapter 4). As such entities do not exist yet, they do not have demand to be satisfied or concerns to be addressed. We assume that such...
entities do not possess requirements to the system, so we do not include them in the stakeholder analysis.

3.2 Stakeholder Requirements

In this section, we identify the system requirements of each stakeholder. Due to the difficulty of getting all multiple stakeholders involved to collect their requirements, we hypothesize their requirements by inferring from the literature. We will show these requirements to the various stakeholders to get their feedback in future work. Combining these requirements together, we obtain the overall system requirements. We show the stakeholder requirements in Table 3.2.
## Table 3.2 Stakeholder Requirements

<table>
<thead>
<tr>
<th>Stakeholder groups</th>
<th>Stakeholders</th>
<th>Issues</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Entrants</td>
<td>UAS operator</td>
<td>Availability of Spectrum</td>
<td>UAS have enough spectrum to operate safely.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supporting Operations</td>
<td>UAS Radios have functionalities supporting operations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>UAS Radios have appropriate policies supporting operations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Safety of UAS flights</td>
<td>Policies are trustworthy.</td>
</tr>
<tr>
<td>Incumbents</td>
<td>Other Spectrum Users</td>
<td>Protection of their spectrum</td>
<td>There is no harmful interference to other spectrum users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Protection of their economic interest</td>
<td>Other spectrum users have incentive to share spectrum.</td>
</tr>
<tr>
<td></td>
<td>Manned Aircraft Operators</td>
<td>Safety of their flights</td>
<td>Manned aircraft are protected from potential collisions.</td>
</tr>
<tr>
<td>Regulators</td>
<td>FCC/NTIA</td>
<td>Spectrum Management</td>
<td>There is no harmful interference between spectrum users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Rights to use spectrum can be flexibly assigned.</td>
</tr>
<tr>
<td></td>
<td>FAA</td>
<td>Safety of NAS</td>
<td>There are minimal potential collisions between aircraft.</td>
</tr>
</tbody>
</table>

We describe each of these requirements as follows:

*UAS have enough spectrum to operate safely.* Given the nature of limited spectrum for UAS, UAS operators will want to know whether there is enough spectrum for their flight operations.

*UAS Radios have functionalities supporting operations.* Radios should have certain functionalities in order for the UAS to operate in various operational scenarios. We discuss the radio functionalities in Section 3.3.
UAS Radios have appropriate policies supporting operations. Policies should take account of various operational considerations, such as phases of flight. We discuss this in Chapter 4.

Policies are trustworthy. As policies determine UAS radios’ behavior, it is important to ensure their trustworthiness so that UAS flights are safe. We address these in policy distribution in Chapter 5.

There is no harmful interference to other spectrum users. If spectrum for UAS has to be shared with other users, those users will want to be certain that UAS radios do not cause harmful interference to them. For example, if a UAS accesses white spaces spectrum that primary users are not using, the UAS will need spectrum awareness that will be able to find available spectrum without causing harmful interference to the primary users. We discuss this in Chapter 4. Additionally, the FCC and NTIA, as they are responsible for spectrum regulation, will have the requirement that there is no harmful interference between spectrum users. The spectrum regulators can include conditions to prevent harmful interference with which radios must comply. The conditions can be defined in policies, e.g. by limiting locations where radios can use spectrum. We discuss this in Chapter 4.

Other spectrum users have incentive to share spectrum. If spectrum for UAS has to be shared with other users, those users will be likely to share their spectrum, e.g. by leasing, if appropriate incentive exists. As we discussed in Section 1.4, policy-based radios could encourage spectrum leasing because they can enable precise policy definition, strict radio compliance, reduced transaction costs, and limited contractual risk.

Manned aircraft are protected from potential collisions. Manned aircraft operators will be likely to be concerned that UAS, without on-board pilots, would collide with manned aircraft.
Similarly, the FAA, being responsible for ensuring the safety of the NAS, will also have the requirement that there are minimal potential collisions between aircraft. To address this, UAS should be controlled accurately to prevent collision via a reliable C2 link. Spectrum for C2 should be available with high reliability and be able to be planned over a flight plan. Additionally, UAS should be equipped with a Detect Sense and Avoid capability, although we do not address it in this research.

*Rights to use spectrum can be flexibly assigned.* Rights to use spectrum can vary with several possible parameters, such as time, frequency, and locations. Policy definition should take account of such varieties. Additionally, there may be multiple spectrum management models for UAS C2. Policy definition should support such various models. We discuss these issues in Chapter 4.

In this section, we have discussed the overall system requirements. From the requirement that UAS radios have functionalities supporting operations, we further describe radio functionalities in the next section.

### 3.3 UAS use cases and associated radio functionalities

In this section, we identify some UAS operational scenarios and the associated radio functionalities. These functionalities are what the radios should be able to do to support UAS operations.

**UAS Cognitive Radio Architecture**

In direct control architecture, cognitive radios are at the Control Station and the UA as shown in Figure 3.1. In control via satellite architecture, cognitive radios are at the satellite transceivers – the earth station and the satellite – and the UA as shown in Figure 3.2. In control via cellular-like network architecture, cognitive radios are at the base station and the UA as
shown in Figure 3.3. Note that in satellite architecture and cellular-like network architecture, the control station does not control a radio but sends command data to the earth station or the base station, which handles the radio. The earth station and base station are considered a radio proxy for the control station.

To transmit, a policy-based radio must have a policy and a physical radio that can tune to the bands in the policy. To receive, the radio must be able to tune to the bands that the other side (either the UA or control station) transmitted.

---

**Figure 3.1 Cognitive Radio Architecture for Direct Control**
Scenario: Flight planning

We assume that the flight path is planned and known in advance. For safety, before the UA takes off, we should ensure that the radio will be able to find spectrum along the planned flight path. Information about available spectrum can be captured in policies.

**Required Functionality:** Spectrum Awareness and Policy Definition. These issues will be discussed in detail in Chapter 4.
After policies are created, there should be a process to transfer policies from policy servers to the radio.

**Required Functionality:** Policy Distribution - getting policies from policy authors to radios. This will be discussed in detail in Chapter 5.

Note that in flight planning, the radio should know that it will be able to find transmission opportunities, but it does not need to decide its transmission parameters *until* it actually starts C2 communications.

**Scenario: Taking off**

As the UA is taking off, the radio should be able to be guaranteed a channel for communications between the UA and the control station. The control station can send the flight path to the entity that controls the radio e.g. the base station operator. Then the entity that controls the radio can look at the policies to see whether there is spectrum along the flight path. If not, the entity that controls the radio could inform the control station to change the flight path, e.g. making a detour, so that there is sufficient spectrum along the new path.

A policy can include more than one available channel, and the radio selects a channel to use. Or, the policy can state a specific channel to use, and the radio simply follows that.

**Required Functionality:** Channel Selection.

**Scenario: UA comes to a new location.**

After the UA takes off, while the UA is in the En Route phase, the availability of spectrum at a new location could be different from that at the current location. Therefore, the radio should be able to switch to a new channel when appropriate.

**Required Functionality:** Spectrum Mobility.

**Scenario: Radio is interfered.**
Even if the radio carefully complies with policies, the channel could become unavailable unexpectedly due to some reasons, such as an appearance of a primary user, jamming by a malicious user, etc. Therefore, the radio should be able to switch to a new channel if interfered.

Required Functionality: Spectrum Mobility.

**Scenario: Changing phase of flight**

The bandwidth requirements depend on the traffic types that the radio needs to communicate, which usually vary with the phase of flight [14]. Therefore, in different phases of flight, the radio should have different policies to accommodate different bandwidth requirements.

Required Functionality: Having policies specific to different phases of flight. This will be discussed in Chapter 4.

**Scenario: Emergency**

The UA could be in an emergency situation where it needs urgent attention because of some reasons, such as bad weather, low fuel, mechanical failure, etc. The UA demands a very reliable C3 link, e.g. more spectrum. Therefore, the radio should be allowed to use a special channel or extra bandwidth, etc. This will be done with policies for emergency.

Required Functionality: Having policies for emergency. This will be discussed in Chapter 4.

**Scenario: Time elapses.**

The UA could spend a long time flying. Some UAS can stay aloft for more than 24 hours. Spectrum availability could change as time goes by. Therefore, policies should be time limited. This implies two aspects. First, policies could be valid periodically for only certain time of the day. Second, policies could be valid for only a specified time period and later expires.
**Required Functionality:** Defining time in policies – stating when and for how long policies are valid. This will be discussed in Chapter 4.

Note that although we have mentioned channel selection and spectrum mobility as important radio functionalities, specific protocols for these are beyond the scope of this research.

In this section, we have identified essential radio functionalities associated with UAS scenarios. We summarize them in Table 3.3.

**Table 3.3  UAS Use Cases and Associated Functionalities**

<table>
<thead>
<tr>
<th>Scenarios</th>
<th>Radio Functionalities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flight planning</td>
<td>Spectrum Awareness and Policy Definition</td>
</tr>
<tr>
<td></td>
<td>Policy Distribution</td>
</tr>
<tr>
<td>Taking off</td>
<td>Channel Selection</td>
</tr>
<tr>
<td>UA comes to a new location</td>
<td>Spectrum Mobility</td>
</tr>
<tr>
<td>Radio is interfered</td>
<td>Spectrum Mobility</td>
</tr>
<tr>
<td>Changing phase of flight</td>
<td>Having policies supporting different phases of flight</td>
</tr>
<tr>
<td>Emergency</td>
<td>Having policies for emergency</td>
</tr>
<tr>
<td>Time elapses</td>
<td>Defining time in policies</td>
</tr>
</tbody>
</table>
Chapter 4

Policy Authoring

Policy authoring is the writing of policies, which state what spectrum a user can use. In this chapter, we discuss models of spectrum access, implications of policies for spectrum management, possible policy authors, what parameters can be configured in policies, and spectrum awareness.

4.1 Models of Spectrum Access

Before discussing policy definition, we should identify possible models of spectrum access of UASs because they influence how policies are specified. We can define spectrum access in two dimensions. In one dimension, spectrum access can be licensed or unlicensed. Licensed refers to an access where UASs have to ask for a permission before they can use spectrum. Unlicensed refers to an access where UASs can use spectrum without having to ask for any permission. But they may still have to follow certain rules.

In another dimension, spectrum access can be interruptible or uninterruptible. Interruptible refers to an access where UASs access the idle spectrum of other spectrum holders on the condition that UASs do not interfere with the spectrum holders. UASs have to vacate the spectrum if the spectrum holders start to transmit. In other words, spectrum holders, considered primary users, have priority over UASs, considered secondary users.

Uninterruptible, in contrast with interruptible, refers to an access where UASs do not have to avoid any other primary users but may have to avoid interfering with other UASs via the use of some etiquette protocol. There are no other spectrum users having priority over UASs. In other words, no users are referred to as primary or secondary users.
Combing the two dimensions, we obtain four models of spectrum access as shown in the matrix in Figure 4.1.

<table>
<thead>
<tr>
<th></th>
<th>Uninterruptible</th>
<th>Interruptible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensed</td>
<td>e.g. cellular</td>
<td>e.g. Secondary spectrum leasing</td>
</tr>
<tr>
<td>Unlicensed</td>
<td>e.g. WiFi</td>
<td>e.g. TV white space</td>
</tr>
</tbody>
</table>

Figure 4.1 Models of Spectrum Access

We describe each model as follows:

1. **Licensed, uninterruptible**: There are two further sub-models. The first one resembles the traditional approach for licensed spectrum use. UASs are licensed primary users and have exclusive rights to use spectrum granted by the spectrum regulator. But the spectrum assignment in this model could be more dynamic - the spectrum rights could be changed frequently and assigned quickly. The second sub-model is a spectrum leasing model, where UASs lease spectrum from other spectrum holders and temporarily have the rights to use the leased spectrum for a specified period. During the lease period, the spectrum holders cannot interrupt the UASs.

2. **Unlicensed, uninterruptible**: UASs use designated unlicensed bands like the 2.4 GHz ISM band.

3. **Unlicensed, interruptible**: UASs are unlicensed secondary users accessing white spaces. Certain bands that are normally used by primary users are available to UASs for unlicensed operation when and where the primary users are not using channels. UAS radios have to be capable to avoid interfering with primary users and vacate channels if primary users appear. Although unlicensed, UASs still have to comply with the regulator’s rules to access the spectrum. For example, one rule is that UASs, as secondary users, must not cause harmful interference to the primary users. This model is similar to the approach in which the FCC has allowed TV band devices accessing TV white spaces [12].
4. Licensed, interruptible: This is a secondary spectrum leasing model, where UASs lease spectrum from other primary spectrum holders but must avoid interfering with these primary spectrum holders. This model is similar to the licensed, uninterruptible spectrum leasing, but the difference is that the spectrum holders can interrupt the UASs anytime as they wish. If the spectrum holders interrupt, UASs have to vacate the spectrum. This model is also similar to unlicensed, interruptible model, but the number of secondary users is limited by licensing.

We note that each model could be further divided into: fixed assignment and dynamic assignment. In fixed assignment, users take control of spectrum for a long time e.g. 10 years, while in dynamic assignment, users use spectrum for a relatively short time e.g. a few hours or a few days.

The licensed, uninterruptible model and the licensed, interruptible model can be implemented by using time-limited leases as discussed by Chapin and Lehr [22]. “A time-limited lease is a set of rights” to use spectrum that is valid for a specified period [22]. In the licensed, uninterruptible model, the regulator grants such a “lease”, whereas in the spectrum leasing model, a spectrum holder does so.

Which model UASs should or will use is beyond the scope of this research. We envision that the UAS could use spectrum under more than one of these models. Policy authoring can be applied to each of these models.

4.2 Background on Policies

Policies are “rules imposed by stakeholders’ preferences intended to accomplish some goals” [23] and “determine the radio behavior in the network” [24].

Traditional spectrum management functions are as follows [40]:
1. Allocation: Dividing spectrum into frequency bands and determining use in each band.

2. Allotment: Dividing a frequency band into blocks. Each block is for an individual spectrum user.

3. Service and Technical rules: Defining certain rules that spectrum users have to follow e.g. power limit, build-out requirement, etc.

4. Assignment: Giving the rights to use spectrum to spectrum users.

5. Enforcement: Ensuring that spectrum users follow the rules.

Traditionally, these functions are performed manually and statically. For example, technical rules are codified in written rules, such as FCC technical rules in Title 47 CFR. Then radio manufacturers implement the rules by making hard-wired policies in the radio firmware e.g. setting a transmit power limit. Assignment is done by, for example, telling a spectrum user what frequency band it has rights to access.

Policy-based radios allow some of the spectrum management functions to be implemented by using machine readable policies. Specifically, rights in assignment and technical rules can be coded in machine readable policies. For example, instead of telling a spectrum user what frequency band it has rights to access and certain technical rules, the regulator can encode information about that frequency band and the technical rules in a machine readable policy. Then the regulator can send the policy to the spectrum user. In this way, policies can be updated dynamically, making spectrum management flexible. Machine readable policies are written in a policy language. In the literature, there are a few policy languages available, such as SWRL [26],
OWL [39], and CoRAL [7]. In this project, we use the SWRL language since we have cooperated with the Shared Spectrum Company [3] and this is the language that they use.

4.2.1 Implications of policy-based cognitive radios for spectrum management

1. Implications for Allocation and Allotment. The frequency agility of policy-based cognitive radios will allow more flexibility in allocation. Several bands could be designated for use by a single UAS in different phases of flight. For example, if a frequency band to be used during take-off can be used for only a limited number of UASs. There may be many UASs in the pre-flight phase, but only a few UASs might actually take off at a time, so total required bandwidth for the pre-flight phase will be more than for the take-off phase. High quality frequency bands may be much more limited than low quality bands. Radios could use the low quality bands during the pre-flight phase when simply gathering weather data and uploading flight plans and could use the high quality bands during the take-off phase when critical real-time command and control is exchanged between the aircraft and the pilot. Only Radios with frequency agility will be able to do so.

2. Implications for Technical rules. With the policy-based approach, technical rules can be encoded in the policies and changed more flexibly, without having to re-certify radios or change new firmware or hardware.

3. Implications for Assignment. The policy-based approach makes assignment more dynamic. Rights to use spectrum can be quickly assigned, changed, and efficiently managed. Regulators and spectrum holders will be more confident in giving out spectrum [22], e.g. for a trial, as they know that radio transmission is time-limited and will certainly end as agreed.

4. Implications for Enforcement. With policy-based radios, enforcement can be made simpler [22]. First, enforcement is done by focusing on certifying radios and getting correct
policies to them, rather than continuously monitoring their behavior. Assuming that a radio that is certified always behaves according to the policies it holds, we can be sure that it will always behave as desired if given “correct” policies. In other words, once the radio is certified, we ensure its compliance by just making sure that it gets correct policies, rather than having to continuously monitor its behavior.

Second, there is no need to re-certify radios if policies are changed as long as the hardware was already certified. For a traditional radio, it is certified to ensure that it behaves in accordance with a particular policy. If a policy is changed e.g. power limit is lowered, the radio needs to be re-certified to ensure that it complies with the new policy. For a policy-based radio, it is certified to make sure that it behaves in accordance with any policy given, not a particular policy. So, once the radio is certified, we can be sure that the radio will comply with any new policy. We do not need to certify the radio again.

Finally, Interference or misbehavior resulting from poor technical rules can be resolved efficiently by quickly changing policies and updating them to the radios.

4.3 Hierarchy of Policy Authors

There are three abstract categories of policy authors.

1. Spectrum Regulator – This is the entity that regulates spectrum access. In the United States, the FCC and the NTIA are spectrum regulators.

   2. Intermediary – This is the entity that acts as an intermediary between the spectrum regulator and the end user. There can be various possible intermediaries depending on the business model of spectrum acquisition. The following are some examples.

      ATC – like approach This is a licensed, uninterruptible model. The FAA controls the aviation spectrum. There are regional entities resembling regional ATC facilities. Each regional
entity controls the aviation spectrum in its local geographic area. The chain of policy authors in this case is:

NTIA – FAA – Regional managers – End User

**Spectrum leasing approach** This is either a licensed, uninterruptible model or licensed, interruptible model. A private spectrum licensee, User A, obtains spectrum from the FCC. User A leases its spectrum to the end user with the help of a spectrum broker. The chain of policy authors is:

FCC – User A – Spectrum Broker – End User

**TV white space – like approach** This is an unlicensed, interruptible model. Another example similar to the TV white space spectrum access, there is a spectrum manager who maintains the primary users’ activities. The manager provides policies for end users who want secondary access on a non-interference basis. The chain of policy authors is:

FCC – Spectrum Managers – End User

These examples are just illustrations; it is beyond the scope of this project to determine which of these models will be most suitable.

3. End User – This is the entity that operates cognitive radios. This depends on the architecture as discussed in Chapter 3. In direct control architecture, the entity is the control station operator. In satellite architecture, it is the earth station operator. In cellular-like network architecture, it is the base station operator. The entity that operates the radio, e.g. the base station operator, obtains policies from a higher level policy author, e.g. a regional manager, and gives the policies to the radio.
4.4 Policy Parameters

Policies should identify a set of transmission opportunities that the radio could exploit.

The parameters that a policy should address include:

1. Policy author: Identify the policy author and support verification of the policy author
   and their authority to write this policy.

2. Policy receiver: Identify to whom the policy applies.

3. Time: Specify when the policy is valid.

4. Frequency: Identify the spectrum band or bands where it applies.

5. Geographic Locations: Identify the locations where the policy applies.

6. Sublease eligibility: Identify whether the spectrum can be subleased and certain
   conditions to do so.

7. Phase of Flight

8. Technical Rules

We elaborate each of the issues as follows.

4.4.1 Policy’s author

As mentioned in the previous section, there are various types of policy authors. Regulators can define policies. Traditionally, these are in the form of codified rules. For example, NTIA rules are in the “Manual of Regulations and Procedures for Federal Radio Frequency Management” (“Redbook”) [30]. FCC rules for TV band devices are in Title 47 CFR Part 15, subpart H [31]. In the context of policy-based radios, such rules for spectrum access can be transformed into machine readable policies. Regulators could directly author machine readable
policies on their own. Alternatively, they could appoint a policy manager to do so on behalf of them.

In a spectrum leasing model, spectrum holders are additional policy authors. They define policies related to spectrum rights: what frequency band is allowed for leasing, by whom, when, and where.

Policies should support two issues related to policy authors: integrity and authority. First, integrity refers to verifying whether a policy claimed to be authored by an entity is actually authored by that entity. Second, authority refers to ensuring that the policy author has an authority to author that policy. We will discuss these issues in Chapter 5.

4.4.2 Policy receiver: Identify to whom the policy applies.

Policies should specify who the intended policy receiver is. This entity may or may not be an end user. For example, a non-end user includes a regional manager. If the policy receiver is an end user, the policy receiver indicates radio ownership - to whose radio the policies apply. Ownership could be defined broadly, like any UAS that operates in a region in the case of unlicensed operation. Or, ownership could be defined specifically, like a particular base station operator in the case of licensed operation.

4.4.3 Time: Specifying when the policy is valid.

Policies should be valid for only certain times. This refers to two aspects: period of validity and time of the day. First, policies can be defined to become valid and expire at certain times. Expiration could come shortly (e.g. after a few hours) when a UAS operates for a single flight. Or, it could come after a while (e.g. a few months) for longer term policies. They could become valid immediately or sometime in the future.
Second, policies can be defined to be valid for certain times of the day. For example, a primary user could author a policy to be valid nightly from 2-4 am, when the primary user is not using the spectrum.

4.4.4 Frequency: Identifying information about available spectrum.

Policies should provide information that enables radios to know what bandwidth is available to use. In uninterruptible models, certain dedicated channels are given to UASs. Therefore, defining frequency information in this case is simple because the channels are known. The available frequency can be either a specific interval or intervals of spectrum.

In interruptible models, however, there are no dedicate channels for UASs. Frequency identifies the potential range of channels. UASs need spectrum awareness - the capability to determine a list of available channels. A channel is considered available if its use by UAS will not cause interference to primary spectrum users. We will discuss this in Section 4.5.

4.4.5 Geographic Locations: Identifying the locations where the policy applies.

We can define locations as an arbitrary shape depending on operational preference. The simplest are geographic regions. However, because they are used for aircraft, the third dimension, altitude, is important. As an example, a policy might only apply above 18,000 ft to correspond with Class A airspace.

Or, we can define locations using more complex shapes such as an “upside down wedding cake” shape as in Figure 4.2. This resembles a shape of airspace as shown in Figure 2.5. Such a shape has several advantages:

1. It resembles regions to protect primary users (discussed in Section 4.5).
2. It can be designed to closely match the actual airspace shapes.
3. It may be familiar to people in the aviation industry.

![Figure 4.2 An “upside down wedding cake” shape for defining locations](image)

Other shapes may be driven more by radio propagation. For example, in a TV white space – like approach, where UAS try to use the same spectrum as a primary user does, we could define an exclusion zone around the primary user such that the UA will not be allowed to use that spectrum inside the zone to prevent interfering with the primary user. We describe exclusion zones in detail in Section 4.6.

### 4.4.6 Sublease eligibility

Some entities should be allowed to sublease spectrum, while some other should not. For example, the FAA should be allowed to sublease spectrum to regional managers. But an individual UAS may not be allowed to sublease spectrum. Policies should indicate whether the recipient can sublease the spectrum and if so, on what condition it can sublease. Conditions can be related to the type of the subleasee. For example, regional managers may be allowed to sublease spectrum to only UASs, but not cell phone operators.
4.4.7 Phase of flight

Policies can be defined to support preferences for operations in each phase of flight. For example, in different phases of flight, UASs require different types of traffic. This also results in different bandwidth and delay requirements for different phases of flight [14].

Moreover, we could have different channels for different phases of flight. For example, when the UA is in the pre-flight phase when the transmission of the flight plan occurs, poor quality channels with high delays are still acceptable. In contrast, in the landing phase, the channels have to be reliable.

There should be some policies reserved for use only in emergency situations. Emergency includes engine failure, etc. In such events, radios should be given additional spectrum for high reliability of communications. There could be dedicated channels for communications in an emergency.

We can specify the phase of flight in two ways:

1. Use a string to specify the phase of flight. In this way, the flight avionics system provides the phase of flight information to the radio.

2. Use sensor data to imply the phase of flight. UA’s speed and location can imply the phase of flight. For example, in the pre-flight phase, the UA’s speed is zero, and its location is at the airport. But in the en route phase, the UA is moving with a certain speed at a certain altitude.

4.4.8 Technical Rules

Technical rules can be imposed to limit interference. For example, regulators may specify maximum allowable transmit power. If one spectrum user leases spectrum to another, the leaser can also impose stricter requirement, for example, to limit its possible liability if the lessee tends to use higher transmit power than allowed.
4.5 **Spectrum awareness**

There are three design alternatives of the method in which cognitive radios can use to find available spectrum [32].

1. Spectrum Sensing

2. Geolocation and Database

3. Beacon

We evaluate each of the alternatives below:

### 4.5.1 Spectrum Sensing

In this method, the secondary user detects the transmitted signal of the primary transmitter directly to know the presence of the primary user. There are three approaches to do so: matched filter detection, energy detection, and feature detection [6].

**Advantages**

- There is no need to build centralized infrastructure because spectrum sensing is performed by each node. Therefore, the system could start incrementally with minimal initial investment.

- High flexibility – UA could detect primary users in any frequency band of interest.

**Disadvantages**

- Spectrum sensing can result in high errors in primary user detection due to a hidden node problem [32] and detector errors.
Spectrum sensing cannot guarantee spectrum availability along the planned flight path locations in advance as cognitive radios would have to be physically present at such locations in order to detect primary users.

Cognitive radios would be more complicated as the hardware has to be equipped with a sensing capability. Time is also divided between communications and sensing overhead.

### 4.5.2 Geolocation and Databases

In this method, there is a database containing the information about primary users’ transmission activities, including channels being used and primary users’ locations [32]. The secondary user determines its location and uses the database information to identify channels available to use. Alternatively, the secondary user submits its location and desired transmission characteristics to a database. Then a set of allowed frequency bands is returned to the secondary user.

**Advantages**

- This method allows accurate detection of primary users because primary users have to register their transmission parameters and activities with a centralized database.

- We can be certain that there will be spectrum available along the planned flight path and those can be captured in policies.

- UASs are often already equipped with positioning systems to find their own locations.

- Cognitive radios would be less complicated as they do not need to be able to sense primary users.

**Disadvantages**
• A centralized infrastructure of databases is needed. Therefore, the system would be likely to have higher initial costs.

• Less flexibility - UA would be allowed to use only the spectrum bands in which the primary users registered their transmission parameters and activities with centralized databases.

4.5.3 Beacon

In this method, the primary transmitter, primary receiver, or independent set of transmitters broadcasts a beacon signal containing information about local spectrum usage. The secondary user detects the beacon signal to know the presence of the primary user [32].

Advantages

• UASs do not need geolocation capabilities.

• Beacons can be implemented locally.

Disadvantages

• A network of beacons is required.

• Receivers have to work in the frequency bands of beacon signals.

• The coverage of a beacon signal may not match the coverage of a policy.

4.5.4 Analysis

In this research, information about available channels is contained in policies, which are stored in databases, i.e. finding available spectrum is achieved by geolocation and databases because of a number of reasons:
- For safety, UA should be guaranteed in advance that there is available spectrum at the planned flight path locations.

- Cognitive radios should detect primary users with high accuracy to avoid harmful interference.

- Databases allow better management of spectrum over time. As new spectrum becomes available, or existing spectrum becomes reallocated, radios can learn of these changes.

- Databases can enable secondary spectrum markets.

### 4.6 Exclusion Zone

In an interruptible model, where UA access spectrum of primary users, policies can be created to specify exclusion regions around the primary users. We provide a simple calculation of an exclusion zone around a primary receiver in this section.

#### 4.6.1 Size of Exclusion Zone

Consider a UA flying in an airspace at some distance from the primary receiver. We consider when the radio horizon of the primary receiver and that of the UA are at the same position as shown in Figure 4.3.

![Figure 4.3 Radio Horizon Geometry](image)

The distance to the radio horizon of the primary receiver is

\[ d_p = \sqrt{2h_p} \]  (1)
where \( d_p \) is the distance to radio horizon of the primary receiver in miles and \( h_p \) is the primary receiver antenna height above the ground in feet [47].

The distance to the radio horizon of the UA is:

\[
d_{UA} = \sqrt{2h_{UA}}
\]  

(2)

where \( d_{UA} \) is the distance to radio horizon of the UA in miles and \( h_{UA} \) is the UA antenna height above the ground in feet, assumed to be the same as the UA altitude.

Combining equation (1) and (2), we obtain the separation distance between the primary receiver and the UA:

\[
d = d_p + d_{UA} = \sqrt{2h_p} + \sqrt{2h_{UA}}
\]  

(3)

Rewriting the equation, we obtain:

\[
h_{UA} = 0.5(d - \sqrt{2h_p})^2
\]  

(4)

We plot a curve of equation (4) in Figure 4.4 when \( h_p = 10 \) feet.

![Figure 4.4 Curve of UA Altitude and Separation Distance](image-url)
The curve is a parabola. We can interpret the curve as follows.

If the UA is in the space to the right of the curve, the primary receiver is beyond line of sight of the UA. In such a case, we assume that the interference power from the UA to the primary receiver is negligible. In other words, the UA in the space to the right of the curve can transmit without causing interference to the primary receiver. From Chapter 2, we have learned that UA altitudes are typically a few thousand meters. For example, medium range UA altitude is 5,000 m or about 16,000 feet. Given that altitude, the horizontal distance that UA has to be separated from the primary receiver is about 180 miles.

If the UA is in the space to the left of the curve, the primary receiver is within line of sight of the UA. And the interference power from the UA to the primary receiver has to be considered. We assume that the free space propagation model applies:

\[
\frac{P_r}{P_t} = \left(\frac{\lambda}{4\pi d}\right)^2
\]

(5)

Where:

- \(P_r\) is the interference power received by the primary receiver in Watts
- \(P_t\) is the interference power transmitted by the UA in Watts
- \(\lambda\) is the wavelength of electromagnetic waves in meters
- \(d\) is the distance between the primary receiver and the UA in meters.

We provide a numerical example to see a possible value of \(d\).

Suppose that:

- Maximum tolerable interference \(Max\ P_r = -109 \text{ dBm} = 1.259 \times 10^{-14} \text{ W}\)
- \(P_t = 40 \text{ dBm} = 10 \text{ W}\)
- \(\lambda = 0.3 \text{ m (Frequency = 1 GHz)}\)
Substituting the numerical values into equation (5), we obtain:

\[
\frac{1.259 \times 10^{-14}}{10} = \left( \frac{0.3}{4\pi d} \right)^2
\]

\[d = 672,839 \text{ m} = 673 \text{ km}\]

That is, to avoid interfering with the primary receiver, the UA would have to be at least 673 km from the primary receiver. At that distance, the UA would have to be greater than about 200 miles above the ground to be above the horizon.

In conclusion, the space to the left of the horizon curve can be considered an exclusion zone, where the UA should not transmit to avoid interfering with the primary receiver. The curve in the figure, having two dimensions, is a parabola. The actual curve, however, has three dimensions and is a paraboloid. Therefore, an exclusion zone with a paraboloid shape can be defined around a primary user such that UA can transmit outside of the exclusion zone, but not inside of it. The horizontal distance that UA has to be separated from a primary receiver is in the range of a few hundred miles, which is reasonable. Additionally, the advantage of using the horizon is that it depends only on the UA and primary receiver radio geometry and does not depend on radio parameters such as antenna gain, transmit power, receiver sensitivity, etc., which may be difficult to assume.

**4.6.2 Impact of Exclusion Zone on Channel's Availability**

We consider how the exclusion zone affects the availability of a channel. Brown and Balasubramanya [48] derived the relationship between the availability of a channel and the exclusion distance as:

\[Availability = e^{-1_{x,2}^2} \quad \text{(6)}\]

Where
\( \lambda \) is the density of the poisson point process for primary users – the number of primary users per 1 km\(^2\).

\( d_{km} \) is the separation distance around a primary user in km. It can be found by rewriting equation (3) in SI units as follows:

\[
d_{km} = 2.9 \sqrt{2h_{r,meters} + 2h_{UAmeters}}
\]  

(7)

Substituting equation (7) into (6), we obtain:

\[
\text{Availability} = e^{-16.82 \lambda \pi (\sqrt{h_{p}} + \sqrt{h_{UA}})^2}
\]  

(8)

For a numerical example, consider cases in which a channel has 20, 50, 100, and 200 primary receivers across the continental United States, which has an area of 7.7x10\(^6\) km\(^2\). The primary receiver antenna height \( h_{p} = 10 \) m. We plot curves of equation (8) in Figure 4.5.

![Figure 4.5 Curve of Availability and UA Altitude](image)

As can be seen from Figure 4.4, as the UA altitude increases, availability decreases. Overall, the availability of the channel is relatively low. However, we could allow cognitive radios to access multiple channels to improve availability. For example, when the UA altitude is...
5,000 m, and there are 50 primary users, availability is 0.154. Using 38 similar but independent channels will yield \(1-(1-0.154)^{38} = 99.8\%\) availability, which is appropriate for UAS communications.

4.7 Examples of Policies

We now illustrate a simplified scenario. Suppose a UAS is used for a mission from Denver, CO to Salt Lake City, UT. The C2 architecture is control via nationwide cellular-like network architecture operated by base station operator X. The related spectrum authors are:

NTIA – FAA – regional managers – base station operator X.

The hierarchy is shown in Figure 4.6.

![Figure 4.6 Hierarchy of Policy Authors Example](image)

The NTIA gives Policy#1, which defines 100 MHz spectrum for the whole continental U.S. for 10 years, to the FAA.
The FAA gives Policy#2, which defines 50 MHz spectrum in Colorado for a year, to the Colorado Manager.

**Policy #2**
Higher Policy: Policy #1
Policy Author: FAA. Policy Receiver: Colorado regional manager
Allow transmission if:
- Frequency: 1000 – 1050 MHz
- Locations: The state of Colorado
- Sublease Eligibility: Yes, to only aviation
- Power Limit = 50 dBm

The FAA gives Policy#3, which defines another 50 MHz spectrum band in Utah for a year, to the Utah Manager.
The Colorado Manager gives Policy#4, which defines 20 MHz spectrum in Colorado to Operator X.

<table>
<thead>
<tr>
<th>Policy #4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Higher Policy: Policy #1, Policy#2</td>
</tr>
<tr>
<td>Allow transmission if:</td>
</tr>
<tr>
<td>Time: January 1-31, 2012</td>
</tr>
<tr>
<td>Frequency: 1000 – 1020 MHz</td>
</tr>
<tr>
<td>Locations: The state of Colorado</td>
</tr>
<tr>
<td>Sublease Eligibility: Yes, to only aviation</td>
</tr>
<tr>
<td>Power Limit = 40 dBm</td>
</tr>
</tbody>
</table>

The Utah Manager gives Policy#5, which defines another 20 MHz spectrum in Utah to Operator X.
Operator X further suballocate more policies, taking account of each base station and phases of flight as shown in Table 4.1.

**Table 4.1 Policies of Operator X**

<table>
<thead>
<tr>
<th>State</th>
<th>Base station</th>
<th>Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Colorado</td>
<td>A</td>
<td>Policy#6 Flight planning, Policy#7 taxi,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Policy#8 takeoff, Policy#9 en route</td>
</tr>
<tr>
<td>Colorado</td>
<td>B</td>
<td>Policy#10 en route</td>
</tr>
<tr>
<td>Utah</td>
<td>C</td>
<td>Policy #11 en route</td>
</tr>
<tr>
<td>Utah</td>
<td>D</td>
<td>Policy#12 en route, Policy#13 approach,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Policy#14 landing, Policy#15 post landing</td>
</tr>
<tr>
<td>Colorado</td>
<td>A, B</td>
<td>Policy#911 emergency</td>
</tr>
<tr>
<td>Utah</td>
<td>C, D</td>
<td>Policy#912 emergency</td>
</tr>
</tbody>
</table>

Along the flight path of the UAS, there are base stations A and B in Colorado and base stations C and D in Utah. The UAS takes off from an airport in the service area of base station A, flies past base station B and C, and lands at an airport in the service area of base station D. There are different policies for different phases of flight. There are policies for emergency. Policy#911 is valid anywhere in Colorado. Policy#912 is valid anywhere in Utah. For example, Policy#10 is as follows.
Policy #10

Higher Policy: Policy #1, Policy#2, Policy#4
Policy Author: Base station operator X. Policy Receiver: Base station B.
Allow transmission if:
- Time: January 1, 2012, 5 am – 11.30 pm
- Frequency: 1000 – 1002 MHz
- Locations: Cell of Base station B
- Sublease Eligibility: No
- Power Limit = 30 dBm

We can see that with several levels of policy authors, lower level policies can be finer grain.

4.8 Dealing with conflicting requirements between policies

Policies from different policy authors, e.g. regulators and operators, could possibly conflict with each other. For example, an operator could author policies to allow transmission in
a channel that was disallowed by a regulator. This could be either intentional or unintentional.

An example of intentional conflicts is that a dishonest operator wants to take advantage and avoid payment for a license. An example for unintentional conflicts is that an operator could carelessly author policies. In either case, there should be a mechanism to detect and resolve conflicts. We discuss this topic in detail in Chapter 5.

4.9 Policy Creation and Storage

Each policy author creates policies, initially in natural language. From the policies in natural language, machine readable policies are created, possibly by a policy visualization tool (PVT), which has Graphic User Interface (GUI) [3]. The machine readable policies are then stored in a local database in a policy server.

4.10 Summary

In this chapter, we have described how policies can be authored. Varieties of policy parameters have been considered. We have analyzed spectrum awareness techniques and concluded that the Geolocation and database technique is most appropriate for UAS. We show some examples of policies and illustrate how policies can be fine-grained.
Chapter 5
Policy Distribution

In Chapter 4, we have discussed how policies should be specified. In this chapter, we turn our discussion to the processes to deal with policies: how policies are distributed.

5.1 Architecture of Policy Distribution

Policy distribution is the transfer of policies from one entity to another. When an entity wants a policy, it sends a request to an appropriate policy author. That policy author replies with a policy. Two possible arrangements of policy distribution architecture are as follows:

1. Web Architecture. In this architecture, the radio has access to the policy servers of all policy authors in the hierarchy. The radio can request higher level policies directly from the higher level policy authors for the purpose of policy authority validation, which will be discussed in detail in Section 5.6. A lower level policy does not have to include information about higher level policies. The advantage of this architecture is that policy updating is simple. For example, if a lower level policy is changed, the higher level policy does not have to be resent. The disadvantage is that many connections are needed.

![Figure 5.1 Web Architecture](image-url)
2. Chain Architecture In this architecture, the radio connects to only the last policy author. A lower level policy has to include information about the related higher level policy giving the authority. This will be discussed in detail in Section 5.6. The advantage of this architecture is that a small number of connections are needed. The disadvantage is that policy updating is somewhat complicated. For example, if a lower level policy is updated but the related higher level one is not, the information about that higher level policy has to be resent anyway.

![Chain Architecture Diagram](attachment:chain_architecture.png)

**Figure 5.2 Chain Architecture**

### 5.2 Requirements of Policy Distribution

As we discussed in Chapter 4, the system should support the verification of policies in two aspects: policy integrity and policy authority.

#### 5.2.1. Policy Integrity

We need to consider the security of the transmission of policies from one policy author to another in a network. This is done according to traditional network security approaches. Note
that we are focusing on the security of the communications links for policy distribution, not the communications link between the unmanned aircraft and the control station. We discuss policy integrity in Section 5.4 and Section 5.5.

5.2.2. Policy Authority

We need to be certain that the policy author has the authority to create a policy with particular specifications. For example, a policy author can only sublease spectrum that it has rights to use. We discuss policy authority in Section 5.6.

5.3 Security Services

To begin with, we consider what security services the system should provide.

According to [41], there are six security services as follows: Confidentiality, Integrity, Authentication, Non-repudiation, Access Control, and, Availability.

Confidentiality “is the process of keeping information private and secret so that only the intended recipient is able to understand the information” [42]. An attack on confidentiality is interception.

Integrity is the process of “prevent[ing] unauthorized modification of systems and information” [43]. An attack on integrity is modification.

Authentication “is the process of providing proof of identity of the sender to the recipient, so that the recipient can be assured that the person sending the information is who and what he or she claims to be” [42]. An attack on authentication is fabrication.

Non-repudiation “prevents either sender or receiver from denying a transmitted message” [41].
Access Control “is the ability to limit and control the access to host systems and applications via communications links.” An attack on access control is unauthorized access.

Availability The system has availability when the communications link and hosts can function properly with sufficient performance. An attack on availability is denial of service.

In this research, we do not consider non-repudiation, access control, and availability. We focus on confidentiality, integrity, and authentication. We design security mechanisms to provide these security services to the system.

5.4 Security Mechanisms

Suppose a policy author wants to send a message containing a policy to another policy author or policy user, which we denote the policy receiver. We describe security mechanisms to provide security services as follows.

5.4.1 Digital signatures

We need to provide integrity and authentication – to ensure that the policy is not modified maliciously and can be proved that it is from the expected policy author. The mechanism to deal with these is to use digital signatures [41], described below.

The sending policy author uses a hash function to compute a message digest or hash value from the plain text. The hash function is designed in such a way that if the plaintext is altered, the computed hash value will change too. Then the sending policy author digitally signs by use its own private key to encrypt the message digest. The resulting encrypted message digest is the sending policy author’s digital signature and is added in the message along with the plain text. The policy author then sends the message to the policy receiver.

On the policy receiver’s side, the policy receiver needs to check whether the alleged sending policy author is the expected sending policy author. The policy receiver does so by
verifying the digital signature of the alleged sending policy author. For now, we assume that the policy receiver knows the public key of the expected sending policy author. We will discuss how it knows in Section 5.6. The policy receiver uses this public key to decrypt the digital signature in the message. This yields a message digest. The policy receiver also computes the hash value from the plaintext. Then the policy receiver compares the computed hash value with the message digest from the signature decryption. If both match, the alleged sending policy author must have signed with the private key associated with the public key of the expected sending policy author. Assuming that the private key is not compromised, the policy receiver concludes that the alleged sending policy author is the same entity as the expected sending policy author. Additionally, the policy receiver concludes that there is no modification to the message.

5.4.2 Message encryption

We need to provide confidentiality – to ensure that no one other than the intended recipient can read the message. The mechanism to deal with this is message encryption, described below.

The sender uses a key to encrypt the message. Only an entity that has the proper key to decrypt it can read and understand the message’s content. Two types of encryption are available: secret key encryption and public key encryption. In secret key encryption, the key used in the encryption and in the decryption is the same and is known to only the sender and the recipient – the key is “secret.” In public key encryption, the keys used in the encryption and in the decryption are different. The key used in the encryption is a public key of the recipient and is widely known so that anyone wanting to send a message to the recipient can encrypt and send the message to the recipient. In contrast, the key used in the decryption is a private key and is known to only the recipient so that only the recipient can decrypt and read the message.
Comparing the two encryption schemes, one can see that public key encryption is more scalable but slower, whereas secret key encryption is faster but needs higher number of keys. For a detailed discussion of this, see [42] or any standard security textbooks. In practice, public key encryption is used to distribute a secret key, and then secret key encryption is used with the actual message to be sent. First, a secret key is transferred between the sender and the recipient using public key encryption – the sender uses the public key of the recipient to encrypt the message containing the secret key, and the recipient uses its private key to decrypt the message containing the secret key. Then the sender can encrypt the actual message to be sent using the secret key (which was arranged earlier) and the recipient can decrypt the message, also using the secret key.

5.5 Policy Authority

In section 5.4, we have discussed how to ensure that the message is not maliciously modified and that no malicious entity claims to be the expected sending policy author. But even if the message is genuine, we still have to verify whether the sending policy author has the authority to create the policy. Who determines such authority? It is the higher level policy author.

Suppose that A gives A’s policy to B. B then wants to give a policy to another entity. In order for B’s policy to be valid, B can only give a policy on the condition that itself has authority to use and create such policy. The authority is authorized by A’s policy. So, we define that B’s policy is valid if and only if it is within the restrictions of A’s policy i.e. B’s policy is a subset of A’s policy. If that is not the case, e.g. A’s policy allows frequency 1000 – 1100 MHz, but B’s policy allows 900 – 1100 MHz, then B’s policy is not valid.
To validate authority, the policy from the higher level policy author should be examined. There are two architectures of policy distribution to accomplish this as described in Section 5.2: Web Architecture and Chain Architecture

In the web architecture, for the purpose of policy authority validation, the radio can request higher level policies directly from the higher level policy authors. A lower level policy does not have to include information about higher level policies.

In the chain architecture, for the purpose of policy validation, a lower level policy has to include information about the related higher level policy giving the authority. In other words, to show that it has authority to create a policy, the sending policy author also “includes” the policy from the higher level policy author in the message sent to the policy receiver. To illustrate this, suppose A is the highest level policy author. Policy author B wants a policy from policy author A. B sends a request to A. A replies with a message containing A’s policy and A’s signature. We will call this message “A’s message.”

Then policy author C wants a policy from B. C sends a request to B. We can require B to include the policy of A in the message sent to C. So, B replies with a message containing A’s message, B’s policy, and B’s signature. We will call this message “B’s message.”

At C, C first checks the integrity of B’s message - whether alleged B’s message is actually from B and whether it has been altered. This is done as described in Section 5.4. C computes the hash value from B’s message and decrypts B’s signature using B’s public key. C compares the computed hash value and the message digest from the signature decryption. If both match, C knows that the alleged B’s message is actually from B and it has not been altered.

Then, C checks whether B’s authority to create the policy is valid, i.e. whether B’s policy is within the restrictions of A’s policy. To accomplish this, C does two steps:
1. C checks the integrity of the A’s message part in B’s message - whether alleged A’s message is actually from A and whether it has been altered. Again, this is done as described in Section 5.4. C computes the hash value from A’s message and decrypts A’s signature using A’s public key. C compares the computed hash value and the message digest from the signature decryption. If both match, C knows that the alleged A’s message is actually from A and it has not been altered. From this step, now C knows what the policy that A gave to B is.

2. C checks whether B’s authority to create the policy is valid - whether B’s policy is within the restrictions of A’s policy. B’s setting has to be a subset of A’s policy in order to be considered valid. The value of a setting can be either continuous or discrete. Continuous values include frequency and time. For example, A’s policy specifies that the frequency allowed is 500-600 MHz. B’s policy has to specify the frequency within that range, such as 550-600 MHz, but not 550-610 MHz. For another example, A’s policy specifies that the time allowed is 8 am – 5 pm Monday to Friday. B’s policy has to specify the time allowed within that range, such as 9 am – 4 pm, Monday to Friday. Values like 7.59 am – 5 pm, Monday to Friday, and 9 am – 4 pm, Monday to Saturday, would not be valid. Discrete values include radio’s ownership and phase of flight. For example, A’s policy specifies that the allowed radio belongs to either any of the following operators: Operator X, Operator Y, and Operator Z. We can consider this as a set: \{Operator X, Operator Y, Operator Z\}. B’s policy has to specify the radio’s owner accordingly, such as \{Operator X, Operator Y\} or \{Operator X, Operator Z\}, but not, say, \{Operator W, Operator X\}. We show examples of subsets in Table 5.1.
Table 5.1 Subset Examples

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Type of Value</th>
<th>Subset Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Receiver</td>
<td>Discrete</td>
<td>{Operator X, Y} is a subset of {Operator X, Y, Z}</td>
</tr>
<tr>
<td>Time</td>
<td>Continuous</td>
<td>{9 am - 4 pm} is a subset of {8 am - 5 pm}</td>
</tr>
<tr>
<td>Frequency</td>
<td>Continuous</td>
<td>{550 - 600 MHz} is a subset of {500 - 600 MHz}</td>
</tr>
<tr>
<td>Locations</td>
<td>Continuous</td>
<td>{Colorado} is a subset of {Continental U.S.}</td>
</tr>
<tr>
<td>Sublease eligibility</td>
<td>Discrete</td>
<td>{Sublease to aviation} is a subset of {sublease to anyone}</td>
</tr>
<tr>
<td>Phase of flight</td>
<td>Discrete</td>
<td>{en route} is a subset of {any phase}</td>
</tr>
<tr>
<td>Transmit power</td>
<td>Continuous</td>
<td>{less than -30 dBm} is a subset of {less than -10 dBm}</td>
</tr>
</tbody>
</table>

5.6 Public Key Infrastructure (PKI) – A system for distributing public keys

In section 5.4, we have assumed that the receiving policy author knows the public key of the expected sending policy author. Moreover, in section 5.5, we have assumed that C knows the public key of both A and B.

Assume that the public keys of government entities, such as the FCC, are widely known. Then the problem of knowing public keys occurs when there are private entities involved in spectrum assignment. How do we know the public keys of policy authors that are not well known? There must be a mechanism for key distribution. We use Public key infrastructure (PKI) to deal with this issue.

PKI is “[a] complete scheme for certifying bindings between public keys and identities – what key belongs to who” [44]. A certificate, issued and signed by a certificate authority (CA) contains the binding between the public key and an entity. Before issuing a certificate, the CA verifies the identity of that entity to make sure that the alleged public key actually associates with that entity. If one trusts a CA, one then can be certain that the public key in a certificate signed by that CA actually belongs to the claimed entity.

We illustrate how PKI works as follows.
In Section 5.5, we have assumed that C knows both A’s and B’s public keys. To know those, C requests a certificate from Certificate authority Y. Y creates a certificate containing the binding between A’s identity and A’s public key. Y signs the certificate and gives it to C.

Assume that C knows Y’s public key. C uses Y’s public key to verify Y’s signature in the certificate. Then C knows what A’s public key is from the information in the certificate.

C knows Y’s public key because either:

Case 1

Y is a root certificate authority, so Y’s public key is well-known.

Case 2

Y is not a root certificate authority. Another certificate authority X is a root certificate authority - X’s public key is well-known. X creates a certificate for Y containing the binding between Y’s identity and Y’s public key. X signs Y’s certificate and gives it to C. C knows X’s public key (as X is a root certificate authority). C uses X’s public key to verify X’s signature in Y’s certificate. C then knows Y’s public key from the information in the certificate. In this case, we can see that there is a certificate chain from X to Y. We could extend such a chain with more certificate authorities.

5.6.1 PKI Architecture vs. Policy Authoring Architecture

Policy authors and certificate authorities have different roles. Policy authors create and send policies. Certificate authorities create and send certificates certifying policy authors or other certificate authorities. Therefore, policy authors do not have to be the same entities as certificate authorities.
We could have policy authors also acting as certificate authorities for simple architecture – no extra entities needed. It is assumed that there is some form of clock to synchronize policy handling with certificate handling.

Or, we could have separate entities acting as dedicated certificate authorities for administration reasons, e.g. dividing the responsibility to certify policy authors from the responsibility to create policies. Additionally, the periods of validity of policies are usually different from those of certificates. The periods of validity of policies vary from policy to policy, whereas the periods of validity of certificates are relatively static. Certificates do not have to be updated often as long as the public keys remain the same and the associated private keys are not compromised. However, it is important that the architecture does not assume indefinite periods of validity since good security practice will periodically retire keys.

5.7 Summary

In this chapter, we have discussed the architecture of policy distribution. Important requirements of policy distribution are integrity and authority. We have described security services for policy distribution. We have described how policy authority should be validated by examining whether a given policy is a subset of the higher level policy.
Chapter 6

Conclusion and Future Work

6.1 Revisiting Requirements

In Chapter 3, we have described the system’ requirements from the stakeholders’ perspectives. We restate them and summarize how we satisfy them in this section.

_UAS have enough spectrum to operate safely_. In Chapter 3, we have discussed that spectrum can be planned during flight planning to guarantee enough spectrum before taking off.

_UAS Radios have functionalities supporting operations_. In Chapter 3, we have discussed cognitive radio functionalities required for various UAS use cases.

_UAS Radios have appropriate policies supporting operations_. In Chapter 4, we have discussed that phases of flight can be used to define policies to take account of UAS operations.

_Policies are trustworthy_. In Chapter 5, we have described security mechanisms to provide policy integrity. We also discussed how policy authority can be validated.

_There is no harmful interference to other spectrum users_. In Chapter 4, we have described spectrum awareness to allow radios to find spectrum without causing harmful interference to other users. We also discussed exclusion zones, which can be defined around primary users to prevent UA from transmitting within the zones.

_There is no harmful interference between spectrum users_. In Chapter 4, we discussed that technical rules (e.g. power limit) can be included in policies to prevent interferences between users.

_Other spectrum users have incentive to share spectrum_. In Chapter 1, we discussed how policy-based radios could encourage spectrum leasing: defining policy precisely, ensuring compliance, reducing transaction costs, and limiting contractual risk.
Manned aircraft are protected from potential collisions, and there are minimal potential collisions between aircraft. To achieve these, C2 links should be reliable. In Chapter 3, we have described that spectrum for C2 links can be planned over the flight path. In Chapter 4, we discussed the relationship between availability, exclusion distance, and UA altitude. We also described the use of multiple channels to increase availability.

Rights to use spectrum can be flexibly assigned. In Chapter 4, we have described multiple policy parameters and their various possible values to accommodate the flexibility in assigning spectrum rights.

6.2 Summary

Policy-based cognitive radios could resolve spectrum scarcity by introducing innovative ways to acquire spectrum: using frequency bands otherwise neglected by UAS, spectrum leasing, and utilizing underused white spaces. A policy-based radio system will also be a tool for automatic spectrum management. Policy-based cognitive radios will have beneficial implications for spectrum management.

To guide system design, we have identified the overall system requirements of the stakeholders. We have considered use cases and have identified radio functionalities appropriate to each use case.

We discussed a framework for policy authoring by considering various possible spectrum access models, policy authors, and policy parameters. The varieties of these aspects will allow spectrum assignment to be fine-grained, flexible, and efficient.

There can be a hierarchy of possible policy authors, where policies from higher policy authors have higher priority. There should be policy distribution, which transfers policies from a higher level author to a lower level one. Important requirements of policy distribution are
integrity and authority. Security services should be implemented to provide integrity in policy
distribution. Information about higher level policies can help us validate policy authority.

6.3 Future Work

Possible future work could be done in several aspects as follows.

Engineering Aspect

Getting feedback from the stakeholders. As we analyzed their requirements, these should
be verified with the stakeholders to ensure that our assumptions are correct and complete.

Implementing a prototype of the proposed architecture as a proof of concept. A working
prototype will help build acceptance of the proposed system from the stakeholders and the public.

Doing a detailed design of the architecture. A detailed design, which would enable actual
implementation, could be built upon our research.

Economic and Business Aspect

Doing an economic and financial feasibility study. An economic analysis could be done
so that the economic costs and benefits would be known to aid policy making. Financial
feasibility study could be done to aid private entities’ business decision.

Policy and Regulation Aspect

Studying a detailed regulatory framework for the architecture. Existing regulations could be revised or new regulations could be adopted to accommodate our architecture.
References


