# Law Governed Peer-to-Peer Secondary Spectrum Marketplaces

Rishabh Dudheria, Wade Trappe
WINLAB
Rutgers University
North Brunswick, NJ 08902, USA
Email: {rishabh,trappe}@winlab.rutgers.edu

Naftaly Minsky
Department of Computer Science
Rutgers University
Piscataway, NJ 08854, USA
Email: minsky@cs.rutgers.edu

***Abstract*—We describe a decentralized peer-to-peer online secondary spectrum marketplace, where consumers can trade exclusive access rights to a specific portion of the spectrum (designated by geographic location, frequency band and time period) in return for fee payment, under the constraint of obeying the trading rules formulated by the government. The main advantage of such an innovative secondary spectrum marketplace over the current state of the art is that it reduces the complexity of spectrum management by removing governmental agencies from being directly involved in the completion of such transactions. The proposed model allows spectrum consumers to sell, lease or transfer the access rights to a chunk of spectrum by disaggregating, partitioning or time-sharing the corresponding spectrum in their possession. Further, we also outline an architecture in which such exclusive access rights to a portion of the spectrum could be used to regulate radio device transmission to enable proactive enforcement of the spectrum usage policies and to deter unauthorized transmissions. Overall, our secondary spectrum marketplace model has the potential to reduce cost, increase spectrum efficiency, and to simplify the task of spectrum management.**

## I. Introduction

Dynamic spectrum access aims to address the spectrum scarcity myth by providing new and effective ways of accessing spectrum to increase the communication capacity and efficiency of spectrum use. Such methods include the exclusive usage right schemes [1], [2], commons model [3], [4], and opportunistic usage regimes [5]. Much of the research in this area has primarily focused on the problems of maximizing bandwidth efficiency, suitably adjusting power levels of different users, minimizing interference, maximizing profit, providing effective quality of service to secondary spectrum users, etc., using techniques of optimization and game theory. However, very limited prior work exists dealing with the issue of trading of exclusive spectrum usage rights on secondary markets even though the U.S. Federal Communications Commission (FCC) proposed the removal of regulatory barriers to the development of such markets almost a decade ago [6]. Therefore, our focus in this paper is to address this problem of trading of exclusive access rights to a portion of the spectrum (specified by geographic location, frequency band and time period) for the payment of a fee. For simplicity, our discussion principally refers to the U.S. secondary spectrum trading market with the FCC playing the role of the corresponding regulatory authority, although the ideas presented in this work are applicable ubiquitously.

Currently, most spectrum remains idle and hence is underutilized due to the complicated and comprehensive auctioning process followed by the FCC in the primary markets. As a result of the colossal amount of money involved in such transactions only major wireless companies participate in acquiring the spectrum from the FCC. However, the companies that acquire the usage rights to a large portion of spectrum in primary markets are seldom able to utilize it to its full extent. Moreover, there are many applications that can benefit from acquiring the usage rights to a small portion of the spectrum, which is limited by geography, frequency bands, duration of time or their combinations. Thus, there is a need to enable the primary spectrum holders to sell their excess spectrum to interested buyers in order to increase the overall efficiency of spectrum utilization. Additionally, the granularity of such spectrum sales/auctions needs to be flexible so that it can accommodate the requirements of a variety of small scale services, while enabling multiple entities to operate simultaneously.

Many countries support secondary spectrum trading to varying extent—some (such as U.S., UK, Guatemala) require the regulator's prior approval for such trades, whereas others (such as Australia, New Zealand, El Salvador) require the trades to be notified to the regulator in order to maintain a register of spectrum right holders [7]. Effectively, both these systems work in a similar fashion as, even in the case where the trade just needs to be notified to the appropriate authority, the corresponding transaction is not legally valid until it has been verified and entered into the government registers. Such a centralized approach of involving the governmental agencies directly in secondary trading results in considerable cost, overhead and delay for most transactions if not all (one possible exception being the transfer of radio and spectrum licenses in New Zealand, which can be done electronically).

We envision a forward-looking online secondary spectrum marketplace, where spectrum consumers can engage in the trading of exclusive access rights to spectrum in a decentralized peer-to-peer fashion without the direct involvement of the FCC, but under the trading rules formulated by governmental agencies. Such a secondary trading marketplace needs to allow

the spectrum consumers to sell, lease or transfer the exclusive access rights to a portion of the spectrum by disaggregating, partitioning or time-sharing the corresponding access rights to the chunk of spectrum in their possession in order to be effective. Moreover, such a model also needs to support auditing requirements, so that the governmental agencies can use this information for monitoring purposes.

Overall, the requirements of such a marketplace can be met only by a mechanism that is capable of enforcing a common set of rules across all the heterogeneous participants such that the communal properties of the marketplace cannot be violated. Hence, we present a prototype of such a secondary spectrum marketplace using Law Governed Interaction (LGI) [8], which is a decentralized access control and coordination mechanism. Further, we have also outlined an architecture in which such exclusive access rights to a portion of the spectrum could be used to regulate the transmission of radio devices to enable proactive enforcement of the spectrum usage policies and to deter unauthorized transmissions. Moreover, we would also like to point out that we have used the terminology of Argyroudis et al. [9] regarding the buying and selling of spectrum to mean the buying and selling of exclusive spectrum usage rights; and the term *spectrum consumers* to refer to agents (such as cellular network operators, TV companies, wireless broadband providers, end users, etc.) that buy and sell, transfer or lease such exclusive spectrum usage rights. Also, these consumers may divide and sublet the access rights to the spectrum blocks in their possession to others. Additionally, the spectrum blocks are sold without any restrictions or rules about what services can be offered, what blocks can be neighbors, what technologies can be used, etc., i.e., the spectrum is liberalized with constraint only on the maximum level of interference that can be caused to neighboring spectrum consumers.

The remainder of the paper is organized as follows. In Section II, we provide a motivating example of a peer-to-peer secondary spectrum marketplace. Section III presents an overview of LGI, which acts as the basis for our prototype secondary spectrum marketplace. In Section IV, we describe the architecture of our proposed solution to enable the regulation of transmissions made by radio devices based on their exclusive access rights to spectrum. Section V presents a formalization of the peer-to-peer secondary spectrum marketplace policy introduced in Section II. Section VI describes related work. Finally, we conclude and provide directions for future work in Section VII.

## II. A Motivating Example

Consider an innovative online peer-to-peer secondary spectrum marketplace, where spectrum consumers can interact with each other to trade access rights to a specific portion of the spectrum (designated by geographic location, frequency band and time period) in return for monetary payment without the direct involvement of governmental agencies. In order to be practical and effective, such a marketplace needs to operate in compliance with the rules set up by the government of the country, which has jurisdiction over its operation. For example,

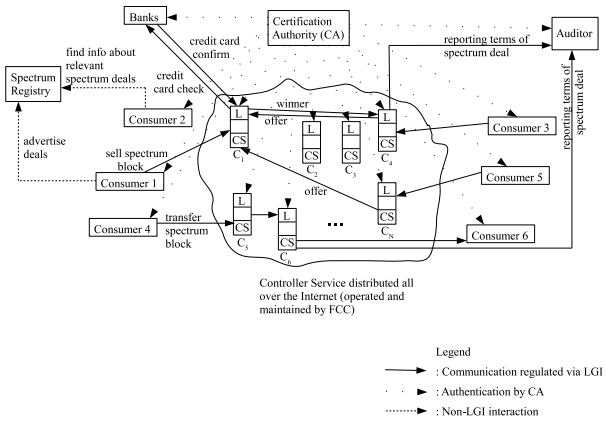


Fig. 1. A snapshot of the interaction taking place in the peer-to-peer Secondary Spectrum Marketplace

the FCC may, on behalf of the U.S. federal government, decide the rules pertaining to the participation; power level of transmissions; selling and buying, transferring and leasing of spectrum blocks; taxes; auditing; monitoring requirements; etc., that needs to be followed by all such online peer-to-peer secondary spectrum marketplaces.

We now present a simplified example of a secondary spectrum marketplace along with the rules that may be imposed by governmental agencies on its operation. Our case study consists of the following entities: (a) *consumers*, who either transfer or buy and sell access rights to spectrum blocks among themselves; (b) the *banks*, that represent the financial infrastructure facilitating the monetary payments for the spectrum blocks (for simplicity, we assume that all the payments are done via credit cards, and the banks provide credit card authorization and money transfer services for the consumers); (c) an *auditor* appointed by the government that keeps a record of the traded spectrum access rights, which can be used later for monitoring purposes and for facilitating the collection of taxes; and (d) a *certification authority* that provides digital credentials to all the participants in the secondary spectrum marketplace. We note that the auditor can easily be replicated to operate in a distributed manner. We assume the presence of a *spectrum registry* that is used by the spectrum consumers to advertise and to search for information about spectrum block sales/auctions. Fig. 1 gives a snapshot of the interaction taking place in such a peer-to-peer online secondary spectrum marketplace.

Our case study adheres to the Government policy ($\mathcal{P}_G$) specified informally below:

- All the participants (consumers, banks, and auditor) are required to authenticate themselves by presenting a digital certificate signed by a specified certification authority (CA).
- The consumers who have initially acquired the access rights to a chunk of spectrum in primary markets via the FCC can authenticate such a possession by providing a digital certificate signed by the FCC.
- Any consumer who possesses the access rights to a par-

ticular portion of the spectrum (specified by geographic location, frequency band and time period) may sell the access rights to it completely or in part (by dividing the spectrum along one of the time/space/frequency dimensions or their combinations) to another consumer for a fixed price or under some kind of auction (e.g., open-cry, Dutch, sealed-bid, etc.); or simply transfer it.
- Monetary payments in this marketplace are handled via credit cards in such a way that the buyer is assured that it would be charged only once for the specified transaction. Moreover, the buyer's credit card information would be revealed only to the designated bank and to no other participating entity (not even the seller).
- The details of the traded spectrum access rights needs to be reported to a special auditor, who has been appointed by the government. Such records can be used later by governmental agencies for monitoring spectrum usage, and to facilitate the collection of taxes.

Note that the participants in such a marketplace are likely to exchange a variety of other information messages pertaining to the advertisement of spectrum goods, negotiations, search and retrieval of information regarding spectrum deals, etc., that need not be regulated by the governmental policy as it is tangential to the concern of the governmental agencies. Therefore, the government policy as such is not concerned with these types of messages.

## III. An Overview of LGI

LGI serves as our mechanism for enabling decentralized secondary spectrum trading over the Internet. LGI is a mode of interaction that allows an *open* group of distributed heterogeneous *agents* to interact with each other with confidence that the explicitly specified policies, called as the *law* of the open group, is complied with by everyone in the group [8]. The most salient aspects of LGI laws are their *strictly local formulation* and the *decentralized nature* of their enforcement. The messages exchanged under a given law $\mathcal{L}$ are called $\mathcal{L}$-messages, and the group of agents interacting via $\mathcal{L}$-messages is called a *community* $\mathcal{C}$, or more specifically, an $\mathcal{L}$-community $\mathcal{C}_{\mathcal{L}}$.

The concept of *open* group has the following semantic: (a) the membership of this group can be very large, and can change *dynamically*; and (b) the members of a given community can be *heterogeneous*. LGI does not assume any knowledge about the structure and behavior of the members of a given $\mathcal{L}$-community. LGI only deals with the interaction between these agents. Members of a community are not prohibited from non-LGI communication, or from participation in other LGI-communities.

For each agent $x$ in a given $\mathcal{L}$-community, LGI maintains the *control state* $\mathcal{CS}_x$ of this agent. These control states, which can change dynamically subject to law $\mathcal{L}$, enable the law to make distinctions between agents, and to be sensitive to the dynamic changes in their states. The semantics of the control state for a given community is defined by its law, and could represent such things as the role of an agent in this community, its identity, its privileges, etc. The $\mathcal{CS}_x$ is viewed as a collection of objects called *Terms*. For instance, under the spectrum marketplace law (to be introduced in Section V), a term of the form *role(auditor)* in the control state of an agent denotes that the agent has the role of an auditor in the community.

We briefly discuss the concepts of LGI in the rest of this section. An inquisitive reader is referred to [10] for a complete understanding of these details.

*The Concept of Law and Its Enforcement:* The law of a community $\mathcal{C}$ is defined over certain types of events occurring at members of $\mathcal{C}$, mandating the effect that any such event should have; this mandate is called the *ruling* of the law for a given event. The events subject to laws, called *regulated events*, include (among others): the *sending* and the *arrival* of an $\mathcal{L}$-message; the *coming due* of an *obligation* previously imposed on a given agent; and the submission of a *digital certificate*. The operations that can be included in the ruling of the law for a given regulated event are called *primitive operations*. They include: operations on the control state of the agent where the event occurred (called, the *home agent*); operations on messages, such as *forward* and *deliver*; and the imposition of an obligation on the home agent. The ruling of the law is not limited to accepting or rejecting a message, but can mandate any number of operations, like the modification of existing messages, and the initiation of new messages and of new events, thus providing the laws with a strong degree of flexibility. More concretely, LGI laws are formulated using an *event-condition-action* pattern. In this paper, we will depict a law using the following pseudo-code notation: **upon** <*event*> **if** <*condition*> **do** <*action*>, where the <*event*> represents one of the regulated events, the <*condition*> is a general expression formulated on the event and control state, and the <*action*> is one or more operations mandated by the law. This definition of the law is abstract in that it is independent of the language used for specifying laws. Thus, a law $\mathcal{L}$ can regulate the exchange of messages between members of an $\mathcal{L}$-community, based on the control state of the participants; and it can mandate various side effects of the message exchange, such as modification of the control states of the sender and/or receiver of a message, and emission of extra messages.

*The Local Nature of Laws:* Although the law $\mathcal{L}$ of a community $\mathcal{C}$ is *global* in that it governs the interaction between *all* the members of $\mathcal{C}$, it is enforced locally at each member of $\mathcal{C}$. This is accomplished by the following properties of LGI laws:

- $\mathcal{L}$ only regulates local events at individual agents.
- The ruling of $\mathcal{L}$ for an event $e$ at agent $x$ depends only on event $e$ and the local control state $\mathcal{CS}_x$ of $x$.

The ruling of $\mathcal{L}$ at $x$ can mandate only local operations to be carried out at $x$, such as an update of $\mathcal{CS}_x$, the forwarding of a message from $x$ to some other agent $y$, and the imposition of an obligation on $x$. The fact that the *same law* is enforced at all the agents of a community gives LGI its necessary global scope, establishing a *common* set of ground rules for the members of $\mathcal{C}$ and providing them with the ability to trust each other, in spite of the heterogeneity of the community.

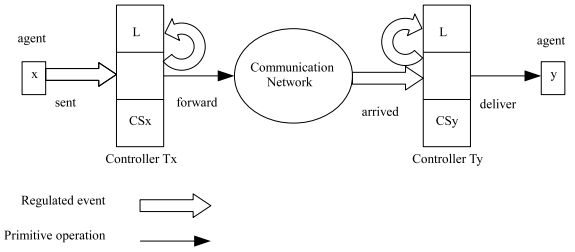


Fig. 2. LGI framework regulates the interaction of agents via controllers

Furthermore, the locality of law enforcement enables LGI to scale with the size of the community.

*Distributed Law-Enforcement:* The law $\mathcal{L}$ of community $\mathcal{C}_{\mathcal{L}}$ is enforced by a set of trusted agents, called controllers that mediate the exchange of $\mathcal{L}$-messages between members of $\mathcal{C}_{\mathcal{L}}$. Every member $x$ of $\mathcal{C}$ has a controller $\mathcal{T}_x$ assigned to it ($\mathcal{T}$ here stands for trusted agent), which maintains the control state $\mathcal{CS}_x$ of its client $x$. All these controllers, which are logically placed between the members of $\mathcal{C}$ and the communication medium as illustrated in Fig. 2 carry the same law $\mathcal{L}$. Every exchange between a pair of agents $x$ and $y$ is thus mediated by their controllers $\mathcal{T}_x$ and $\mathcal{T}_y$, so that this enforcement is inherently decentralized. Controllers are generic, and can interpret and enforce any well-formed law.

*The basis of trust between members of a community:* For an $\mathcal{L}$-agent $x$ to trust its interlocutor $y$ to observe the law $\mathcal{L}$, it is sufficient for $x$ to have the assurance that the following three conditions are satisfied: (a) the exchange between $x$ and $y$ is mediated by correctly implemented private controllers $\mathcal{T}_x$ and $\mathcal{T}_y$, respectively; (b) both controllers operate under law $\mathcal{L}$; and (c) the $\mathcal{L}$-messages exchanged between $x$ and $y$ are transmitted securely over the Internet. The manner and degree to which these conditions are satisfied by the present implementation of LGI is discussed in [10].

*The Controller-Service (CoS) of LGI:* The controller service is responsible for maintaining a reliable and secure set of controllers, which collectively constitute the decentralized trusted computing base (DTCB) of LGI. The LGI implementation supports a prototype of such *CoS* called the *Controller Manager*, which maintains a set of continuously tested, and geographically distributed controllers, and provides the services of these controllers to agents who want to operate under LGI. For an agent $x$ to be able to exchange $\mathcal{L}$-messages with other members of an $\mathcal{L}$-community, it must: (a) procure an LGI controller from a trusted *CoS*; and (b) notify this controller that it wants to use it under law $\mathcal{L}$.

Such a *CoS* for our spectrum marketplace model can be maintained and managed by a governmental organization (such as the FCC) that can serve as a trusted third party, with no financial interest in the computing activities regulated by its controllers. This *CoS* would essentially function as a *public utility*, which could be used by consumers distributed all over the Internet. However, it is essential that the operating organization assumes certain liabilities for various failures of the controllers provided to its customers. Moreover, in case of a dispute, it also needs to provide an audit trail of its controllers' activities, which are secure enough to be accepted in the court of law. The construction of such a public utility of controllers is beyond the scope of our present work.

## IV. Architecture

We broadly outline an architecture that could enable the exclusive spectrum access rights (henceforth, referred to as tokens in this section) traded in our secondary spectrum marketplace to be used to regulate the transmission of radio devices. We assume the existence of a secure clock and a secure GPS on each wireless device that provides the corresponding device with an accurate timing and location information respectively. Further, we also assume the existence of a secure transfer mechanism to enable the tokens originally stored in the controller to be transferred into the corresponding trusted kernel of the user device. Now, if all the transmission requests made by the devices are approved by the kernel such that the corresponding transmission request is permitted *if and only if* it satisfies the frequency, space, timing and other constraints mentioned in the token, then we can ensure that the radio devices transmit in accordance with their spectrum usage rights. Thus, such an architecture would enable proactive enforcement of the spectrum usage policies and deter unauthorized transmissions. But, it should be pointed out that this architecture is limited in that it cannot prevent radio devices from transmitting without complying to the tokens if they have been tampered with, or if they can be operated without such tokens. Unauthorized transmissions resulting from such issues can be dealt with by relying on other techniques such as FCC monitoring, [11], etc.

In this context, our earlier paper [12] had introduced a model of interaction control for the regulation of wireless communication in ad hoc networks to regulate the dynamic behavior of interacting wireless agents. Specifically, we had assumed that each wireless node has a trusted implementation of the controller, which requires the use of Trusted Platform Module (TPM). This implementation allows us to control the application level messaging performed by the wireless nodes and hence can be viewed as an initial proof of concept for the aforementioned architecture.

## V. Implementation of the Case Study

We now show how the motivating example described in Section II can be specified in LGI by formalizing the government policy $\mathcal{P}_G$ into an LGI law $\mathcal{L}_G$. The implementation of the corresponding law written in Java can be found at [13].

As mentioned before, we assume that the sellers advertise their products through a *spectrum registry*, which maintains information about the spectrum block sales/auctions. Once the buyers find out about the relevant sales/auctions (as per their interest) via the spectrum registry, they interact directly with the sellers in a decentralized peer-to-peer manner under the specified government policy (i.e., law in LGI) to participate in the corresponding sales/auctions. The spectrum registry does

not necessarily belong to the community since the interaction with the registry does not need to be governed by LGI.

The *role(R)* term in each agent's control state is used to represent the role played by the agent in the community, for example, the control state of the *auditor* should contain the term *role(auditor)*. Similarly, the presence of the term *name(N)* in the control state of the consumer means that the corresponding agent has the name *N*. Further, the presence of the term *accessible(S)* in the control state of an agent implies that the corresponding agent possesses the access rights to the designated spectrum as mentioned in *S*. For example, *S* could represent the list [frequency(392,396,MHz), time(110000,190000), ...], specifying the details of access rights to a portion of spectrum. Our implementation allows the aforementioned spectrum *S* to be divided along the frequency/space/time dimension as follows:

(a) *Channel Disaggregation:*
$S_1$-[*frequency(392,394,MHz)*, time(110000,190000), ...];
$S_2$-[*frequency(394,396,MHz)*, time(110000,190000), ...].

(b) *Time-sharing:*
$S_1$-[frequency(392,396,MHz), *time(110000,150000)*, ...];
$S_2$-[frequency(392,396,MHz), *time(150000,170000)*, ...];
$S_3$-[frequency(392,396,MHz), *time(170000,190000)*, ...].

Similarly, spectrum blocks can also be formed by the geographic partioning of *S* or by dividing *S* along a combination of the frequency/space/time dimensions such that each of the resultant block is a disjoint subset of *S*.

### A. Establishing the government policy $\mathcal{P}_G$

Law $\mathcal{L}_G$, which implements policy $\mathcal{P}_G$, is shown in Fig. 3. We have assumed for simplicity that the law $\mathcal{L}_G$ permits consumers to sell access rights to spectrum blocks at a fixed price only. Law $\mathcal{L}_G$ itself consists of two parts namely the *preamble* and the *body*. The preamble of $\mathcal{L}_G$ consists of the following clauses. First, the *law clause* identifies the name of this law and the CA that is to be used for certifying the controllers interpreting this law. Second, the *authority clause* specifies the CA and the FCC (represented by the keyed hash of their individual public keys) for certifying the roles played by the different actors in the community and for authenticating the possession of access rights to a specific portion of spectrum purchased by the consumers in the primary market respectively. Third, the *initialCS clause* specifies that the initial control state of everyone who adopts this law would be empty. Fourth, the two *alias clauses* provide shorthand for the identifier (id) of the *bank* and *auditor* respectively. The body of the law is now presented as a set of rules along with their pseudo code, and explained in English.

*1) Agent authentication:* When a participant engages in the system, it does so by sending an adoption message to its LGI controller, a message that can carry its certificate. When the message arrives at the controller, it invokes an *adopted event*. If an actor submits a certificate, then the controller verifies it with the public key of the CA and challenges the actor to prove the possession of the private key of the subject, as shown by rule $\mathcal{R}1$. If the subject is not the one who presented

*$\mathcal{P}$reamble:*

```
law(name(L_G),authority(CA)).
authority(CA,HashOfCAPubKey).
authority(FCC,HashOfFCCPubKey).
initialCS( ).
alias(bank,"bank@rutgers.edu").
alias(auditor,"auditor@rutgers.edu").

R1) upon adopted(Self,Issuer,Subject,Attributes,Args)
      if (Subject!=Self||Issuer!=CA)
        do Quit
      if (Attributes.role==auditor||bank||consumer)
        do Add(role(Attributes.role))
      if (Attributes.role==consumer)
        do Add(name(Attributes.name))

R2) upon certified(Self,Issuer,Subject,Attributes)
      if (Subject==Self && Issuer==FCC)
        do Add(accessible(Attributes))

R3) upon sent(X,start(B,P,T),X)
      if ((CS has role(consumer) && accessible(S)) &&
        (B⊂S))
        do Replace(accessible(S),accessible(S-B))
        do Add(sale(B,P))
        do ImposeObligation(timeout(B,P),T)

R4) upon sent(X,offer(B,P,CreditCard),Y)
      if (CS has role(consumer))
        do Forward

R5) upon arrived(X,offer(B,P,CreditCard),Y)
      if (CS has sale(B,P))
        do Forward(Y,requestCreditCheck(CreditCard,P)
          ,bank)
        do Add(pendingOffer(X,B,P,CreditCard))

R6) upon arrived(Y,requestCreditCheck(CreditCard,P),bank)
      do Forward(bank,creditCheckResponse(CreditCard,
        Ans),Y)

R7) upon arrived(bank,creditCheckResponse(CreditCard,
      Ans),Y)
      if (CS has pendingOffer(X,B,P,CreditCard) &&
        name(N1))
        if (Ans==approved)
          do RepealObligation(timeout(B,P))
          do Remove(sale(B,P))
          do Forward(Y,succeeded(N1,B,P),X)
          do Remove(pendingOffer(X,B,P,CreditCard))
          do Deliver(Self,winner(B,P,X),Self)
        if (Ans==reject)
          do Forward(Y,rejected(B,P),X)
          do Remove(pendingOffer(X,B,P,CreditCard))

R8) upon obligationDue(timeout(B,P))
      do Deliver(Self,dealExpired(B,P),Self)
      do Replace(accessible(S),accessible(S+B))
      do Remove(sale(B,P))

R9) upon arrived(Y,succeeded(N1,B,P),X)
      if (CS has role(consumer) && name(N2))
        do Add(accessible(B))
        do Forward(X,deal(N1,B,P,N2),auditor)
        do Deliver

R10) upon arrived(Y,rejected(B,P),X)
       do Deliver

R11) upon sent(X,transfer(B),Y)
       if ((CS has role(consumer) && accessible(S) &&
         name(N1)) && (B⊂S))
         do Replace(accessible(S),accessible(S-B))
         do Forward(X,transfer(N1,B),Y)

R12) upon arrived(X,transfer(N1,B),Y)
       if (CS has role(consumer) && name(N2))
         do Add(accessible(B))
         do Forward(Y,deal(N1,B,0,N2),auditor)
         do Deliver

R13) upon arrived(X,deal(N1,B,P,N2),auditor)
       do Deliver
```

Fig. 3. Law $\mathcal{L}_G$

the certificate, or if the issuer is not the CA, then the actor is forced to quit. If the attributes of the certificate contain the role of *auditor, bank* or *consumer*, then this role of the actor is extracted from the attributes and saved in the control state maintained by the controller on behalf of the actor. In the case of consumers, the name is also extracted from the attributes and added to the control state. Any consumer can submit a certificate provided by the FCC to authenticate its possession of access rights over a certain portion of spectrum via rule $\mathcal{R}2$. Upon successful verification of such a certificate, the corresponding spectrum access rights gets added to the control state of the consumer.

*2) Regulation over trading activities:* Any consumer can initiate a fixed price sale for the access rights to a block of the spectrum it possesses by specifying its price and the period of time for which the sale is open by rule $\mathcal{R}3$. Consequently, its control state is updated to reflect the corresponding sale and an obligation is imposed on its controller to stop the sale after the specified period of time. According to rule $\mathcal{R}4$, any consumer can make an offer to a spectrum sale by providing its credit card information. The controller of the seller, on receiving an offer for a spectrum block matching its sale price, forwards a credit check request to the specified bank and saves the information about the offer in the control state via rule $\mathcal{R}5$. By rule $\mathcal{R}6$, the bank on receiving a credit check request performs internal checking and then either completes or rejects the corresponding transaction. For simplicity, the law in this case provides an 'approved' or 'reject' reply back to the sender on receiving a credit check request. If the controller of the seller receives an 'approved' reply from the bank, then the sale is ended and a succeeded message is sent to the corresponding buyer via rule $\mathcal{R}7$. Further, the seller's controller removes the information about the buyer's offer from the control state and informs the seller about the consumer who has won the specified spectrum sale. On the other hand, if the controller of the seller receives a 'reject' reply from the bank, then it sends a rejected message to the corresponding buyer and removes the information about the buyer's offer from the control state. It should be noted that the controller of the seller protects the buyer's confidentiality by maintaining its credit card information without disclosing it to the seller. Further, the law ensures that such sensitive information is deleted from the control state of the seller's controller as soon as it receives the corresponding credit check response from the bank. By rule $\mathcal{R}8$, if the sale period ends without a successful offer being received, then the seller is informed that the corresponding deal has expired. Additionally, the spectrum block that was on sale is added back to the control state of the seller. As per rule $\mathcal{R}9$, the controller of the winning consumer adds the specified spectrum block access rights to the control state and reports the details of the transaction to the auditor. Additionally, the succeeded message is also delivered to the corresponding consumer. According to rule $\mathcal{R}10$, if an offer made by a prospective buyer is rejected by the seller, then the rejected message is delivered to the corresponding consumer. As per rule $\mathcal{R}11$, any consumer can transfer the access rights to the spectrum block it possesses to another consumer free of charge. On receiving such a transfer, the corresponding spectrum block access rights are added to the control state of the recipient and the details of the corresponding transaction are reported to the auditor via rule $\mathcal{R}12$. The reports of such transactions get delivered to the auditor by rule $\mathcal{R}13$.

### B. Discussion

Note that the actual transaction of spectrum goods between the buyers and sellers in such a peer-to-peer online secondary spectrum marketplace only involves the bank (which facilitates the credit card transactions). Apart from this aspect of trading, the interaction in this marketplace is decentralized in the sense that the buyers and sellers exchange spectrum blocks without involving any other entity. Moreover, the transfer of spectrum blocks from one consumer to another does not involve any bank. Furthermore, it is also possible to modify the suggested model to incorporate payments through digital cash, which can be easily achieved via the LGI mechanism as has been shown in [14]. This would enable all the interactions taking place in such a secondary spectrum marketplace to be completely decentralized. Additionally, it would also extend the applicability of our scheme by making it suitable for both micropayment and macropayment deals.

The implementation of the spectrum marketplace policy via LGI law has been presented under the assumption of no message failures for simplicity. But, it is possible to extend the law to handle communication faults through the *exception facility* of LGI [10]. Also, the leasing of spectrum blocks between consumers has not directly been addressed in our example, although it is straightforward to extend the policy and the law to include this feature. Further, our case study can additionally be extended to support certificate expiration and revocation as has been shown in [15]. However, we do not address these issues due to lack of space.

## VI. Related Work

Argyroudis et al. [9] have described a policy-driven trading framework for market-based spectrum assignment that allows spectrum consumers to trade exclusive access rights to spectrum blocks (specified by geographic location, frequency band and time period) for electronic payments. They have used the Keynote trust management system [16] to implement a prototype of their policy model and have incorporated real-time hash chain micropayment scheme [17] (via Keynote credentials) to handle monetary exchanges. This framework only deals with the trading of these exclusive access rights, but does not address the crucial question of how these credentials are to be used for policing the spectrum use. Moreover, our model supports delegation by transfer of privileges, allowing a consumer to sell a spectrum block after acquiring it from another consumer, which cannot be achieved by the aforementioned framework since it trades the spectrum access rights in the form of Keynote credentials [14]. Additionally, our mechanism is also capable of enforcing various auditing requirements

(such as reporting of transactions to the specified authorities) that may be essential for monitoring spectrum usage, which cannot be directly supported by the trust management framework as keys do not reveal identity. Trust management systems such as Keynote are intrinsically suitable for server-centric policies, whereas a trading framework for the spectrum marketplace requires communal policies to be enforced such that all the participants obey to a common set of rules. It is this communal aspect of policy enforcement that enables LGI to support delegation by transfer, quotas, and other properties, which cannot be supported in trust management systems.

SpecEx.com [18] provides a centralized online real-time marketplace for secondary spectrum trading in the U.S. It serves as a platform for spectrum holders and buyers to engage in selling, leasing or exchanging spectrum. It allows for disaggregation, partitioning and time-sharing of spectrum along one or any combination of the frequency/space/time dimensions. However, this current state of the art approach involves the FCC in directly approving the transactions once the buyers and sellers agree to some common terms of the sale, resulting in considerable cost, overhead and delay. Besides, such a centralized marketplace can achieve scalability with respect to large number of participants and high transaction volumes only via replication, which tends to be very expensive. It is possible to use a website such as SpecEx.com as a spectrum registry for our model, whereby sellers can advertise about their spectrum goods and buyers can consequently search and find out about the deals they are interested in. Then, the potential buyers can communicate directly with the sellers under the specified secondary spectrum marketplace policy (formulated by the government) by adopting an LGI controller in a decentralized peer-to-peer fashion.

## VII. Conclusion and Future Work

We have proposed an innovative secondary spectrum marketplace, where consumers can trade the exclusive access rights to a portion of spectrum (specified by geographic location, frequency band and time period) for the payment of a fee in a decentralized peer-to-peer fashion without directly involving the governmental agencies. The main benefit of this approach is that it reduces the overhead, delay and cost involved in secondary spectrum transactions, thereby improving the overall spectrum utilization. Our model allows the spectrum consumers to divide and sell, transfer or lease the spectrum access rights they possess along any one of the time/space/frequency dimensions or their combinations. Further, we have also outlined an architecture by which our secondary spectrum trading model can be augmented to regulate the transmissions of the radio devices thus, accomplishing proactive enforcement of the spectrum usage rights. Such an architecture can deter unauthorized transmissions from radio devices and reduce the overall complexity associated with policing schemes used for spectrum management. We have prototyped an example based on a peer-to-peer online secondary spectrum marketplace, where buyers and sellers interact to trade exclusive access rights to a chunk of spectrum in return for fee payment, under the constraint of obeying the trading rules formulated by the government.

We plan to extend the current secondary spectrum marketplace model to support the hierarchical organization of the policies to take into account the hierarchical nature of the authorities (such as federal government, state government, local authorities, etc.) that may be involved in defining its rules, and the volition that may be granted to the spectrum consumers to deal with certain issues (such as negotiations, how access rights to spectrum blocks are to be sold, etc.), which are not directly related to the government regulations.

## References


[1] D. Hatfield and P. Weiser, "Property rights in spectrum: taking the next step," in *New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2005. First IEEE International Symposium on*, Nov. 2005, pp. 43–55.

[2] L. Doyle and T. Forde, "Towards a fluid spectrum market for exclusive usage rights," in *New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2007. 2nd IEEE International Symposium on*, Apr. 2007, pp. 620–632.

[3] W. Lehr and J. Crowcroft, "Managing shared access to a spectrum commons," in *New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2005. First IEEE International Symposium on*, Nov. 2005, pp. 420–444.

[4] M. Cooper, "The economics of collaborative production in the spectrum commons," in *New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2005. First IEEE International Symposium on*, Nov. 2005, pp. 379–400.

[5] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE J.Sel. A. Commun.*, vol. 23, no. 2, pp. 201–220, Sep. 2006.

[6] Secondary markets initiative. Federal Communications Commission. [Online]. Available: http://wireless.fcc.gov/licensing/index.htm?job=secondary_markets

[7] P. Crocioni, "Is allowing trading enough? making secondary markets in spectrum work," *Telecommun. Policy*, vol. 33, no. 8, pp. 451–468, Sep. 2009.

[8] N. H. Minsky and V. Ungureanu, "Law-governed interaction: a coordination and control mechanism for heterogeneous distributed systems," *ACM Trans. Softw. Eng. Methodol.*, vol. 9, no. 3, pp. 273–305, 2000.

[9] P. Argyroudis, T. Forde, L. Doyle, and D. O'Mahony, "A policy-driven trading framework for market-based spectrum assignment," in *Policies for Distributed Systems and Networks, 2007. POLICY '07. Eighth IEEE International Workshop on*, Jun. 2007, pp. 246–250.

[10] N. H. Minsky, "Law governed interaction (LGI): A distributed coordination and control mechanism (an introduction and a reference manual)," Rutgers University, Tech. Rep., Jun. 2005. [Online]. Available: http://www.moses.rutgers.edu/documentation/manual.pdf

[11] S. Liu, L. J. Greenstein, W. Trappe, and Y. Chen, "Detecting anomalous spectrum usage in dynamic spectrum access networks," *Ad Hoc Netw.*, vol. 10, no. 5, pp. 831–844, Jul. 2012.

[12] R. Dudheria, W. Trappe, and N. Minsky, "Coordination and control in mobile ubiquitous computing applications using Law Governed Interaction," in *UBICOMM '10: Proceedings of the Fourth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, Oct. 2010, pp. 247–256.

[13] Secondary spectrum marketplace law. [Online]. Available: http://winlab.rutgers.edu/~rishabh/SecondarySpectrumMarketplaceLaw.java1

[14] X. Ao and N. Minsky, "Regulated delegation in distributed systems," in *Policies for Distributed Systems and Networks, 2006. Policy 2006. Seventh IEEE International Workshop on*, Jun. 2006, pp. 215–226.

[15] X. Ao, N. Minsky, and V. Ungureanu, "Formal treatment of certificate revocation under communal access control," in *Security and Privacy, 2001. Proceedings. 2001 IEEE Symposium on*, 2001, pp. 116–127.

[16] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis, "The keynote trust-management system version 2," IETF RFC 2704, Sep. 1999.

[17] H. Tewari and D. O'Mahony, "Real-time payments for mobile ip," *Comm. Mag.*, vol. 41, no. 2, pp. 126–136, Feb. 2003.

[18] SpecEx, The Online Marketplace for Spectrum. Spectrum Bridge. [Online]. Available: http://spectrumbridge.com/ProductsServices/search.aspx