Toward Automated Enforcement of Radio Interference

Pedro J. Bustamante
School of Computing and Information
University of Pittsburgh
Pittsburgh, PA
Email: pjb63@pitt.edu

Debarun Das
School of Computing and Information
University of Pittsburgh
Pittsburgh, PA
Email: ded59@pitt.edu

J. Stephanie Rose
School of Computing and Information
University of Pittsburgh
Pittsburgh, PA
Email: jsr67@pitt.edu

Marcela M. Gomez
University of Pittsburgh
Pittsburgh, PA
Email: mmg62@pitt.edu

Martin Weiss
School of Computing and Information
University of Pittsburgh
Pittsburgh, PA
Email: mbw@pitt.edu

Jung-Min (Jerry) Park
Department of Electrical and Computing Engineering
Virginia Polytechnic Institute
Arlington, VA
Email:jungmin@vt.edu

Taieb Znati
School of Computing and Information
University of Pittsburgh
Pittsburgh, PA
Email: znati@pitt.edu

***Abstract*—In many countries, sharing has become a significant approach to problems of spectrum allocation and assignment. As this approach moves from concept to reality, it is reasonable to expect an increase in interference or usage conflict events between sharing parties.**

Scholars such as Coase, Demsetz, Stigler and others have argued that appropriate enforcement is critical to successful contracts (such as spectrum sharing agreements) and Polinsky, Shavell and others have analyzed enforcement mechanisms in general. While many ex ante measures may be used, reducing social costs of ex ante enforcement means shifting the balance more toward ex post measures. Ex post enforcement requires detection, data collection, and adjudication methods. At present, these methods are ad hoc (operating in a decentralized way between parties) or fairly costly (e.g., relying on the FCC Enforcement Bureau). The research presented in this paper is the culmination of an NSF-funded inquiry into how and what enforcement functions can be automated.

***Keywords*—Spectrum sharing, spectrum regulation, spectrum policy governance, spectrum enforcement, spectrum dispute resolution, crowd-sourced applications, ex-ante enforcement, ex-post enforcement.**

I. Introduction

As the sharing of radio spectrum becomes more intensive, it is reasonable to expect that the number and rate of interference events will increase. Besides, in spectrum sharing scenarios and other allocation and assignation mechanisms, the spectrum access rights granted by the Federal Government to spectrum users come with the "expectation" of protection against conflict situations such as harmful interference. A key element of any framework for managing harmful interference is the mechanism for enforcement of those rights [1].

It is well known in the economics literature that enforcement is important to viable contracts and the definition of property rights [2]. It is also well known that the cost of enforcement plays an important role in whether or not contracts can be written (here, "contracts" are spectrum sharing agreements). Finally, it has been noted that rights enforcement occurs through a combination of *ex ante* and *ex post* techniques [3]. Where a particular enforcement strategy lies on this continuum depends on the relative cost of *ex ante* and *ex post* enforcement. If *ex post* enforcement can be made more inexpensive and efficient, then *ex ante* approaches, which incur social costs and are often less flexible, can be eschewed in favor of more flexible *ex post* approaches. One way to reduce *ex post* enforcement is to automate the detection, forensics, adjudication, and settlement of interference events.

II. Background

As spectrum sharing becomes more intensive and more granular with more stakeholders, we can expect an increasing number of potentially enforceable interference events[1]. Thus, we assert that the success of spectrum sharing systems is dependent to a significant extent on our ability to automate their enforcement.

To date, most of the attention has been on automating *ex ante* enforcement of usage rights. The most visible practical examples of automatic *ex ante* methods are found in the database-driven methods, such at TV White Spaces or Spectrum Access System (SAS) systems. These database-oriented or Geo-location Database (GDB) systems essentially work by preventing users with subordinate rights from using spectrum

[1]An interference event occurs when electromagnetic energy inappropriately enters the electrospace of a user who has currently has the rights to use it. Note that this energy may originate with the license holder who has temporarily transferred rights to use the spectrum to another user or with an entrant who has obtained these rights.

when and where other users with superior rights are operating [4].

At a high level, the goal of this paper is to summarize a research effort to explore how the *ex post* enforcement of radio rights might be automated. The end state of an automated process would be implementing *ex ante* agreements and also *ex post* adjudication of interference events algorithmically[2]. Given our focus on *ex post* enforcement, this means that information about interference events must be detected, then defined, gathered and analyzed (forensics), users identified, and attribution and remuneration inferred (adjudication).

To provide some focus, we begin by framing interference events according to Table I. This particular classification is useful for this research because it distinguishes motives for different events, which simplifies the forensics and user identification process. Since Type 1 events assume that the incumbents and entrants are both cooperative, it is possible to assume that no attempt is made to obfuscate transmissions or to evade compliance. Thus, we assert, Type 1 events are more amenable to automated enforcement. In contrast, non-cooperative actors (who produce Type 2 events) can be assumed to evade detection, evade compliance and engage in a technological "arms race" with incumbents, regulators and other enforcement actors. As a result, Type 2 events are likely to be highly unique on a case by case basis, a situation that is not easily amenable to automation. Type 3 is perhaps a subset of Type 1, except that the potential liability may rest elsewhere. These may also be sufficiently unique to not be easily automated. Finally Type 4 events are also rather unique, with a liability that rests outside of the interfering and interfered parties.

We do not mean to imply that Type 1 events are the most important or most serious. Indeed, it may be the case that Type 2 events have more serious social consequences. Examples of this could include mobile phone jamming, GPS spoofing and other events that are meant to disrupt the operations of socially important wireless systems. Type 2 events also include actors such as "radio pirates" who broadcast license free in licensed broadcast bands. It is also true that different types of interference may have varying consequences for different users or use cases. For example, emissions from LED lighting (Type 3 interference) have been shown to interfere with scientific uses of radio spectrum. The main point we wish to make is that Type 1 events are most likely amenable to automated enforcement of communications-related spectrum uses that employ spectrum sharing strategies and technologies.

Type	Description
1	Sharing parties are making best efforts to comply but interference occurs due to factors that are generally unavoidable
2	Rogue actors making no attempts to comply
3	Technical hardware and software faults
4	Errors in regulatory design – both sharing parties in technical compliance

TABLE I
A TYPOLOGY OF INTERFERENCE EVENTS

III. EX-ANTE ENFORCEMENT

Regulators in the United States (and internationally) have selected the use of Exclusion Zones (EZs)[3] as a common primary *ex-ante* spectrum enforcement method to protect Primary Users in spectrum sharing scenarios.

Defining the EZ boundary, inside which a PU enjoys exclusive spectrum access rights, is considered to be a challenging problem in spectrum sharing. The difficulty of the problem arises because of two conflicting requirements. First, the area defined by the EZ must be sufficiently large to protect the PU from SU-induced interference. Second, the EZ should not be overly large to unnecessarily limit SUs' spectrum access opportunities and, consequently, reduce the new entrants' incentives [7].

In general, the computation of EZ boundaries is based on the interference likely to be experienced by a PU. This interference is not just caused by a single SU, but the *aggregate interference* from all co-existing new entrants. Due to variations in SU dynamics the statistics of aggregate interference change rapidly in a Dynamic Spectrum Sharing (DSS) system[4]. Furthermore, when computing the EZ boundary, the effect of irregular terrain must also be considered in the path loss computations [8], which significantly increases the complexity of the already difficult problem.

Most of the existing methods for defining EZs, such as $F-curves$ [9], consider the worst-case interference scenario and define a conservative static protection boundary for the PU[5]. In other words, they overly emphasize the protection of PUs from harmful interference [11], [12].

To address these problems, Bhattarai *et.al.* propose a novel and systematic framework, named *Multi-Tiered dynamic Incumbent Protection Zones (MIPZ)* [13]. This framework can be used by geolocation database (GDB) systems for prescribing the protection boundaries of PUs in real time. MIPZ ensures that PUs are protected from harmful interference by providing a probabilistic guarantee of interference protection. Unlike legacy approaches that prescribe static and overly conservative EZ boundaries, MIPZ facilitates dynamic adjustment of the PU protection boundary based on the changing radio interference environment.

A. Multi-Tiered Dynamic Incumbent Protection Zones

The FCC in its Notice of Proposed Rulemaking (NPRM) [14] acknowledges that the size of an EZ could be significantly reduced if there were a mechanism for controlling the number

[2]In general, algorithmic enforcement can present significant challenges. For example, [5], [6] examine enforcement of highway speeds.

[3]In this paper, we refer to "Exclusion Zones" as the spatial separation regions defined for protecting Primary Users (PUs) from interference generated by Secondary Users (SUs).

[4]Adding complexity to the design of an EZ boundary.

[5]The notion of a static EZ implies that it has to protect PUs from the union of all likely interference scenarios [10].

of SU transmissions outside the EZ. The introduction of GDB-driven spectrum sharing, such as advanced Spectrum Access Systems (SAS) in the 3.5 GHz band, is an initiative towards this direction. The SAS framework allows regulators to tightly control access to the spectrum by modeling the statistics of aggregate interference at the PU in real-time. Motivated by this initiative, we propose MIPZ for prescribing EZs in GDB-driven spectrum sharing. MIPZ allows the spectrum controller to adjust the size of the EZ dynamically based on instantaneous interference conditions, and hence, allows SUs to exploit more spectrum opportunities than the legacy EZs [13].

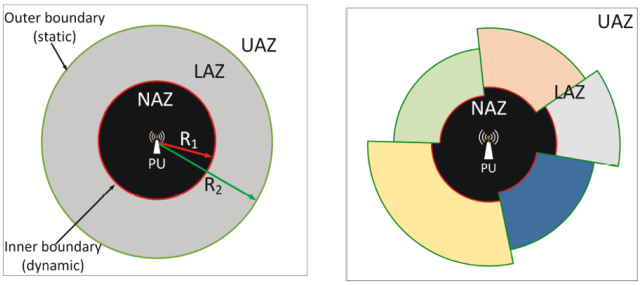
*1) **Conceptual design**:* MIPZ is composed of three access zones around the Incumbent as detailed in the following section.

1) No Access Zone (NAZ): Is the spatial region defined in the immediate vicinity of the PU. Due to its proximity to the PU, even a single SU transmission in this region might produce harmful interference. Therefore, SUs located in the NAZ are not granted spectrum access rights.
2) Limited Access Zone (LAZ): Is the spatial region that lies just outside the NAZ. It is relatively far from the PU, and hence, it is safe to allow a few SUs to transmit in this region without causing harmful interference to the PU. However, it is not far enough for allowing any number of SUs to transmit. Therefore, MIPZ allows only a limited number of co-channel SUs, N, to transmit simultaneously in the LAZ.
3) Unlimited Access Zone (UAZ): Is the region that lies outside the LAZ. Essentially, this region is similar to the area outside conventional EZs where any number of co-channel SUs are allowed to transmit.

The conceptual design of MIPZ is illustrated in Figure 1(a). The PU is located at the center and SUs are spread around the PU in the different access zones. Notice that the two zones boundaries: i) inner boundary, R_1, and ii) outer boundary, R_2, are key elements in defining the NAZ, LAZ and UAZ areas. The outer boundary is defined to be static while the inner boundary is made to be dynamically adjustable based on changes in radio interference statistics, spectrum demand and/or SU transmission parameters.

*2) **Assumptions and design constraints**:* In practice, the zone boundaries will not always be perfect circular coverage areas as shown in Figure 1(a). Terrain variations, environmental effects, antenna radiation patterns, time-constraint conditions, etc. cause the radio signal to attenuate differently in different directions resulting in irregular zone boundaries. To account for these irregularities, in MIPZ we adopt a sectorized model (see Figure 1(b)). We assume that the area within an annular sector exhibits similar propagation characteristics.

We assume that SUs in each LAZ sector are uniformly



(a) Concept of NAZ, LAZ and UAZ (b) Realizing irregular PZs using annular sectors

Fig. 1. MIPZ conceptual design

distributed[6]. We also assume that a PU can operate without significant performance degradation, if it is ensured a probabilistic guarantee of aggregated interference protection. More precisely, a PU achieves its quality of service (QoS), if the aggregate interference, I_{agg}, from SUs is less than-or-equal-to a threshold, I_{th}, for at least fraction, $(1-\epsilon)$, of the time, where ϵ is a pre-defined probabilistic threshold.

$$P(I_{agg} \leq I_{th}) \geq 1 - \epsilon \tag{1}$$

Since SUs are prohibited inside the NAZ, users in this region do not contribute to interference at the PU. Also, SUs in the UAZ have negligible contribution to the aggregate interference because of large path losses. Thus, the aggregate interference power experienced by the PU is the summation of interference caused by N SUs in the LAZ region.

*3) **Determining the MIPZ boundaries**:* In the MIPZ framework it is necessary to determine two boundaries that define the size of the Limited Access Zone (LAZ), namely the outer boundary and the inner boundary.

*a) **Static outer boundary**:* We define the outer boundary, R_2 (see Figure 1), of our framework in the same way most regulators define conventional EZ boundaries. It is based on the maximum distance at which the PU can not longer be impacted by the SUs' operations. The maximum distance depends on several factors such as SU transmit power, type of modulation and coding, antenna gain, PU's interference protection, QoS requirements, etc. We assume that the outer boundary is static and fixed because it is already computed based on the worst-case interference scenario.

*b) **Dynamic inner boundary**:* In our framework, only a limited number of SUs are allowed to operate in the LAZ region. Usually, wireless network conditions are dynamic. Consequently, to maximize the overall spectrum utilization efficiency, the size of the LAZ needs to be adjusted dynamically "on the fly" based mainly on spectrum demand, network dynamics, and aggregate-interference statistics. For

[6]This assumption might seem impractical as several studies have shown that mobile users tend to be clustered due to geographical factors, social gatherings, etc. [15], [16]. However, although SUs are assumed to be distributed uniformly in a LAZ sector, they do not need to be distributed uniformly around the PU.

Fig. 2. Geographical area considered for our Case Study

additional details about the aggregate interference calculations, the optimization formulation, and the technical assumptions used to determine these boundaries, please refer to [10], [13], [17]

*4) **MIPZ case study**:* To make the MIPZ framwork more complete we conducted a case stude of the AWS-3 band. The PU of the band is a Meteorological Satellite (MetSat) and is located near the Petuxant River in Maryland, USA. To protect this Earth station from harmful interference, the NTIA has defined a circular EZ of radius 126km [18]. Note that the area outside this circular EZ corresponds to the UAZ region of MIPZ, and hence, we set R_2 to 126 km (see Figure 2). It is worth noticing that the EZ definition prohibits highly-populated regions such as Washington DC, Baltimore, and Richmond from getting access to the shared resources. Therefore, in this study, we aim to answer the following question: *Given the operational parameters of the PU and SUs, is it possible to allow a limited number of SUs to co-exist inside the EZ boundary without compromising the normal operations of the PU?*

Our specific goal is to find the maximum number of co-channel SUs, N, that can be allowed to operate in Washington and Baltimore (see the green annular sector of Figure 2). For this purpose, we predefined the size of the LAZ by fixing R_1 and compute the optimum value of N. To validate our results we compare them against actual solutions obtained by using the Irregular Terrain Model (ITM) in point-to-point (PTP) communications mode.

From our analysis, we can first observe the path loss map generated by computing the IMP-PTP[7] from the center of each grid to the PU (see Figure 3(a)). As it is shown the EZ and the LAZ from Figure 2 are also overlaid on top of the path loss map to compare both results. The black oval and yellowish annular sector represent the EZ boundary and the LAZ region, respectively.

[7]The required terrain details were extracted from the Global Land One-km Base Elevation (GLOBE) database [19].

We also study the effectiveness of the MIPZ framework in enabling spatial sharing opportunities for new entrants (see Figure 3(b)). MIPZ identifies spatial sharing opportunities by estimating the number of possible co-channel SUs, N, and their corresponding ASC. We can observe that the MIPZ framework identifies these opportunities almost as effectively as the ITM-PTP model. The slight "under-performance" is attributed to the fact that MIPZ uses statistics of radio path loss, whereas ITM-PTP considers the actual conditions in the link for computing the path loss.

Figure 3(c) compares the probability distribution of I_{SU} and I_{agg}. For the MIPZ framework, the parameters of the path loss model (σ and γ) are estimated by fitting a least-squares curve to some samples obtained from ITM-PTP path loss models. Using these parameters we compute the optimum value of N. When comparing I_{agg} from both the MIPZ framework and the ITM-PTP methods, we can observe that the results overlap. This result indicates that when proper values of σ and γ are used, MIPZ provides the same level of interference protection guarantee to the PU as the one provided by the ITM-PTP model.

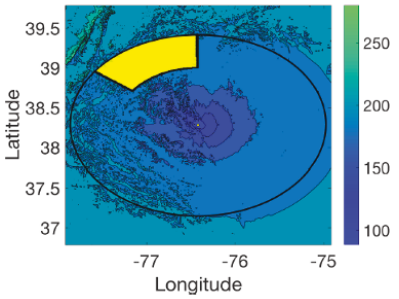
Although the ITM-PTP sligthly outperforms the MIPZ framework[8], it is necessary to point out that the ITM-PTP is computationally expensive while MIPZ is computationally efficient (see Figure 3(d)). ITM-PTP requires us to compute the path loss values from each SU to the PU. On the other hand, MIPZ approximates I_{agg} using closed-form analytical expressions. In addition, MIPZ is easily scalable since its computation time is constant, unlike ITM-PTP, whose computational complexity grows proportionally with N.

Another advantage of the MIPZ framework over the ITM-PTP model is the fact that it does not require the precise geographical location of SUs. MIPZ only needs to know whether the SU lies inside a LAZ sector. On the other hand, the ITM-PTP based method requires the precise locations of the SUs. However, these locations are not always known up-to-date.

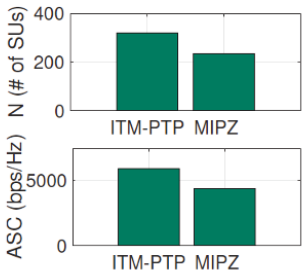
IV. Ex-post enforcement

Ex post enforcement is necessarily composed of several distinct phases. First, it is necessary to *detect* an interference event. When an interference event is detected, information must be gathered and analyzed (*forensics*). This information must be sufficient to the next phase, *adjudication*, in which liability is determined. Finally, there is the *settlement* phase, in which the interference claim is resolved. The detection phase may require independent sensors or may be claims from the "injured" party. Information supporting a claim of interference can include the time and location of the infraction, information about the signal (power, modulatution, type), and information about the offender (identifier, if available). In the adjudication phase, the claim is compared to the terms of the sharing agreement. The outcome of this process is a finding of liability,

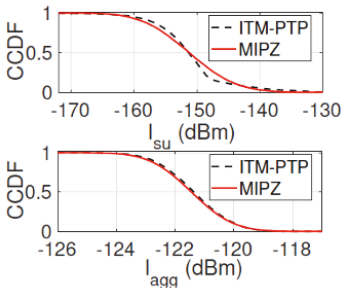
[8]When talking about identifying sharing opportunities.



(a) Path loss map in dB.



(b) Spectrum utilization.



(c) Distribution of interference.

Method	Computation time
ITM-PTP	32.5 sec.
MIPZ	1 sec.

(d) Computation time.

Fig. 3. Summary of Results of our Case Study

which leads to settlement. Note that the settlement need not be monetary.

In many spectrum sharing approaches, Secondary Users employ Software-Define Radios (SDRs) to harmoniously coexist with the Incumbents. A SDR enables a user to readily reconfigure its transmission parameters to avoid usage conflict situations with the PU. Nonetheless, this "programmability" increases the possibility of malfunctioning SU radios [20].

One approach to identify Type 1 interference events is to enable the regulator (e.g., the Federal Communications Commission (FCC) in the U.S.) to uniquely identify transmitters by authenticating their waveforms. This *ex-post* enforcement mechanism would allow the entity in charge to identify an interference source and collect the necessary evidence for the enforcement process [21].

Commonly, there exist three common challenges in carrying out transmitter identification in Dynamic Spectrum Sharing (DSS) systems. First, the enforcement entity is considered a *blind receiver* since it is not the intended receiver of the transmitted signals[9] [22]. Second, the received signals have poor-quality due to multipath fading and very low Message Signal to Noise Ratio (MSNR). Finally, multiple simultaneous signals from multiple transmitters, operating in the same frequency band, could be received by the enforcement entity.

One approach to overcome the challenges of transmitter authentication by a single enforcement entity is to deploy a network of "enforcement nodes". However, deploying and maintaining such a network of dedicated enforcement nodes is prohibitively expensive [23]. A more viable approach is to use a limited number of dedicated enforcement nodes and the employment of a much higher number of SUs' radios[10] that could act as "non-dedicated" enforcement nodes. We refer to this network of dedicated and non-dedicated enforcement nodes as a *Crowd-Sourced Enforcement Network (CEN)* [24].

[9]In addition, the enforcer might have little, if any, knowledge of the physical (PHY) layer parameters that are necessary to demodulate and decode the received signals.

[10]SUs user their "spare" resources to act as enforcement nodes in exchange of well-defined incentives.

A. *Frequency Offset Embedding for CBAT*

In our approach, we apply the concept of *Crow-sourced Blind Authentication of Co-channel Transmitters (CBAT)*. This concept refers to the mechanism of the CEN authenticating multiple co-channel signals by extracting the transmitters' unique identifiable information at the physical (PHY) layer. In this approach, we consider CBAT in a scenario where a CEN consists of a data fusion station (DFS) and a number of dedicated and non-dedicated enforcement nodes. We called this first instantiation of CBAT *FREEquency offset Embedding for CBAT (FREE)* [25].

The main goal of FREE is to address the following challenges: i) authenticate received signals with minimal knowledge of the physical (PHY) layer transmission parameters, ii) authenticate signals with multipath fading and very low Message Signal to Noise Ratio (MSNR), and iii) authenticate signals emitted simultaneously from multiple co-channel transmitters[11].

*1) **Transmitter operations**:* Let there be an authentic SU transmitter that is allotted a particular channel as per the rules stipulated in the corresponding DSS. The transmitter transmits the message signal continuously to communicate with its intended receiver. It utilizes the cyclic prefix (CP) based orthogonal frequency division multiplexing (OFDM) for its message signal. The message signal is transmitted in frames, where each frame contains two parts, namely a preamble, and a message data. The preamble in each frame is utilized to perform time and frequency synchronization. The message data contains user's information along with information regarding the modulation and the encoding of the message data.

In FREE, the transmitter or signal originator carries out four major operations:

- Generate a sequence of frames of the message signal using conventional OFDM procedures.
- Generate the authentication signal which contains the transmitter's authentication data. This data enables the enforcement entity to determine the regulator-assigned

[11]We consider a network scenario where the transmitters, intended receivers, and blind receivers share the same wireless network and are uniformly distributed in a hexagonal cell.

identity and the regulator-imposed spectrum access constraints[12].

- Embed the authentication signal into the message signal by modifying the frequency offset (FO) of each frame of the message signal. The frequency offset is induced in such a way that the authentication signal does not interfere with the decoding process of the message signal at the intended receivers.
- Transmit the embedded signal using the Radio Frequency (RF) front-end procedures.

*2) **Blind receiver operations**:* The blind receivers are aware of the fact that OFDM is employed by the transmitters to modulate and transmit the message signals in frames. The blind receivers also know the sampling frequency, the length of the Fast Fourier Transform (FFT), and the length of CP. These parameters are typically predefined as part of the air-interface standard (e.g., IEEE 802.11g). The received signals are characterized by possessing multipath Rayleigh fading and a very low MSNR.

In FREE, the blind receiver is in charge of four main tasks:

- Down-convert and sample the received signal originated in the transmitter. Then, the blind receiver computes a *decision variable* by calculating the auto-correlation induced due to the repetition of the training samples in the preamble.
- The blind receiver utilizes the heuristic algorithm by Kumar et al. in [25] to determine the number of transmitters and the location of the start of the received frames. This is a critical step since it enables FREE to address the challenge of detecting multiple co-channel signals.
- For each detected transmitter, the blind receiver estimates the frequency offset embedded into the frames of the message signal by utilizing the correlation between the CP samples and the corresponding data samples of the OFDM symbols. In addition, the receiver estimates the time of arrival and the signal to interference and noise ratio of the received frames.
- Communicate the estimated values to the Data Fusion Station (DFS)

*3) **Data Fusion Station (DFS) operations**:* The DFS utilizes a polling-based protocol on a secondary channel (with good MSNR) with the blind receivers to obtain the results of the authentication information extraction procedures.

In FREE, the Data Fusion Station is in charge of four main operations:

- From the reports gathered from the blind receivers, the DFS synchronizes the reported time of arrival and estimates the total number of transmitters in a frequency channel.
- For each transmitter, the DFS aggregates the values of the estimated frequency offsets. In this step, the DFS utilizes the "trustworthiness" weights of the blind receivers to differentiate between an honest blind receiver and a rogue blind receiver.
- Utilizes the aggregated frequency offsets to estimate the authentication signal and verify the validity of the authentication data. It is necessary to point out that the collaboration enabled by the DFS significantly improves the error performance of the estimated authentication signals to address the challenge of very low MSNR.
- After each successful verification, the DFS utilizes the heuristic algorithm by Kumar et al. in [25] to update the "trustworhiness" weights for each blind receiver. This is done by comparing their reported frequency offsets to the true frequency offsets generated from the verified authentication signal.

For additional technical details and performance measurements of FREE, please refer to [25], [26].

V. Governance of Spectrum Sharing Schemes

As part of the automation of enforcement solutions, we also explore the development of "alternative" governance mechanisms. These new governance structures allow for more flexible definitions of both *ex-ante* and *ex-post* enforcement mechanisms.

The exploitation of radio-electric spectrum bands for wireless transmission purposes has some features of the commons: it is subject to congestion and conflict without rules governing its use. The Coasean approach is to assign private property rights to overcome the tragedy of the spectrum commons. The process of assigning these rights is still centralized, with governments assigning property rights through agencies such as the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA) in the United States.

The commons is a general term used to refer to a shared resource in which each competing stakeholder has an equal interest in a given resource [27]. Since the term is often conflated with "open access commons", researchers typically refer to Common Pool Resource (CPR) analysis that can have a variety of access permissions [28]. CPRs are natural or man-made resources shared among different users. These resources are defined by two main features: i) they are sufficiently large so that it is costly to exclude potential beneficiaries from using them, and ii) they are characterized by a high degree of subtractability or rivalry of consumption [29], [30]. We can find a wide range of examples of goods defined as commons, which have been widely explored in the CPR literature: fisheries, forests, innovations, online communities, hacker communities, etc [31]–[36]. A less widely-known example of a CPR system is the exploitation of electromagnetic spectrum bands for wireless communications [37]–[40].

In contrast with the case of CPRs, which situates enforcement as part of the governance structure and incorporates it into the definition of rules, the most common governance mechanism for regulating the exploitation of spectrum bands in the United States has been centralized specification and enforcement of property rights. Usually, a government agency such as the FCC or the NTIA requires or prohibits specific actions or technologies. Rule-breakers are subject to fines,

[12]In terms of frequency, spatial, and temporal domains.

sanctions, and/or imprisonment, depending on the seriousness of the infraction. This system has been the *de facto* approach for spectrum allocation and enforcement in the US since the Radio Act of 1927 [35]. The main mechanism for spectrum assignment and allocation used by the FCC (and most regulators internationally) has been spectrum licensing. Licenses provide incumbents with exclusive property rights to use the corresponding frequency bands, if they remain consistent with the underlying license conditions [41].

In recent years, telecommunications regulators in the U.S. (i.e., the FCC and NTIA) have been working towards shifting from an exclusive licensing scheme to more technically and economically efficient methods for the use and allocation of spectrum bands. One of the most recent approaches has been spectrum sharing between Federal and Commercial entities [42]. This "non-traditional" allocation approach aims to change the current exclusive licensing methods to allow for more flexible resource allocation that addresses many of the challenges stemming from centralized, property-rights approaches.

Our comparative institutional analysis considers self-policing frameworks in spectrum sharing scenarios. In this case, government controllers or community structures (e.g., third-party agencies) are not required (at least as principal actors). This government-less environment constitutes a distributed enforcement approach. It is an "anarchy," which is defined by a lack of formal government intervention, where norms, rules, and enforcement mechanisms are solely the product of repeated interactions among the intervening agents in a given environment [43], [44].

We use Agent-Based Modeling (ABM) to study this "alternative" governance structure in spectrum sharing. By designing and developing an ABM for specific sharing schemes, we are able to analyze the suitability of the proposed self-governance and centralized mechanisms in greater detail. ABM simulations allow us to observe how macro phenomena can emerge from micro-level interactions among independent agents. In this regard, this approach provides insight into the emergence of what Hayek referred to as spontaneous order: order which arises without a conscious design of enforcement [45], [46].

To analyze both the this distributed governance approach in spectrum sharing, we rely on the well-defined framework of the 1695-1710MHz band in the United States. For this work, we focus on the definitions of the restricted zones around the Primary User. For our work, we also use the notation introduced by Bhattarai et al. [10]. This framework allows the PU to adjust the size of the coordination and exclusion zones "on the fly." As a result, three zones (or areas) are defined around the PUs' transmitters (see Section III-A).

A. *The 1695-1710MHz Agent-Based Model*

In this work, our model simulates the interaction of two main types of agents: 1) a single primary user or incumbent (i.e., a meteorological satellite), and 2) several secondary users or new entrants (i.e., LTE handsets). All the agents are placed on a simulation environment that captures the transmission zones NAZ, LAZ, and UAZ (see Section III-A) defined for the sharing scheme in the 1695-1710MHz band. The model considers that conflict situations may arise, and these represent circumstances where the normal operations of the incumbent are impacted by unauthorized actions by one or more new entrants (or SUs). These conflict situations (i.e., interference or enforceable events) arise in the restricted areas of the sharing scheme (i.e., LAZ and NAZ).

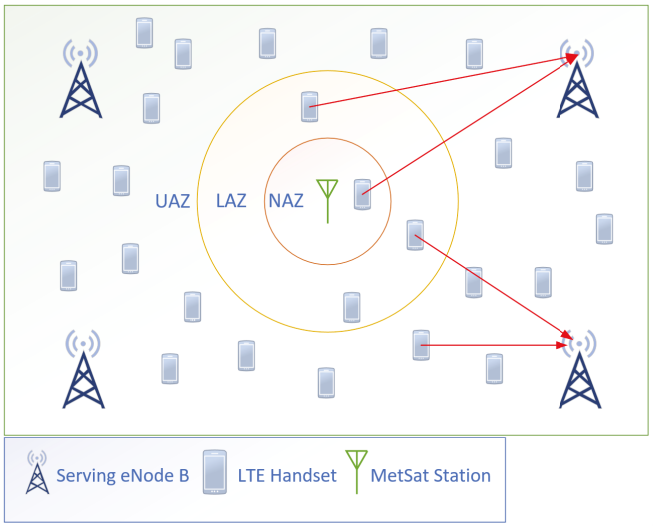


Fig. 4. 1695-1710MHz Spectrum sharing model - Agents, environment, and interactions setup.

*1) **The agents**:* Our model is comprised of three types of participants: meteorological stations (i.e., MetSat), mobile handsets (i.e., LTE Handset), and base stations (i.e., eNodeBs). These entities are represented as independent agents in our model (see Figure 4). First, the NOAA Meteorological Satellite. A single, static agent located in the middle of the protection zones. Second, LTE Mobile Stations. Multiple agents that move around the zones while communicating to their corresponding eNodeBs. Finally, Base Stations. Static agents that serve as coordination and communication points between the PU and SUs.

*2) **Environment**:* The model environment is based on the sharing definitions of the band. In this way, the "world"[13] is divided into three zones: No Access Zone (NAZ), Limited Access Zone (LAZ), and Unlimited Access Zone (UAZ) (see Figure 4).

*3) **Rules, norms, and strategies**:* As defined by North [48], institutions are "[t]he set of rules actually used by a set of individuals to organize repetitive activities that produce outcomes affecting those individuals and potentially affecting others." Based on this definition, we can see that the 1695-1710MHz sharing framework can be categorized as an institution: the actions of the incumbents have an impact on the new entrants and vice versa. This new definition is key to

[13]Defined as the logical or physical plane where the agents are located and interact with each other [47].

	MetSat Definitions				
Agent	MetSat	MetSat	MetSat	MetSat	MetSat
Deontic	Obligated	Obligated	Obligated	Permitted	Permitted
aIm	Communicate LAZ size	Communicate NAZ Size	Communicate LAZ Threshold	Increase LAZ & NAZ size	Decrease LAZ & NAZ size
Condition	All the time	All the time	All the time	Interference Happen	No Interference
Or Else	None	None	None	None	None

TABLE II
RULES, NORMS AND STRATEGIES FOR THE PU (METSAT)

leverage the benefits of the ADICO Grammar of Institutions, which is a framework that permits the definition of shared strategies, norms, and rules as simple statements using five components (see Table III). We leverage the simplicity of the ADICO model to define the rules for both, the primary and secondary users in our system.

*a) **Definitions for the Primary User**:* We explore both "extremes" of governing a spectrum sharing framework. Hence, our agents possess two sets of definitions, one for the centralized approach and one for the distributed perspective. In Table II, we can see the rules that are defined for the the incumbents of the band. The actions with the white background apply in all enforcement situations (government-centric and self-enforcement), while the actions with the blue background apply only in decentralized enforcement scenarios.

First, we discuss the strategy definitions in the centralized approach. In this scenario, the MetSat has little control over the sharing parameters; particularly, the size of the protection areas LAZ and NAZ. Most sharing criteria are defined by a central entity (i.e., the "government") and cannot be updated by the PU. Consequently, the MetSat's only strategy in this scenario is to communicate the sharing parameters to the network's coordination points.

To detect unauthorized transmissions by the SUs, a detection system is assumed to be deployed. In our scheme, this system is given by the detection rate, d. This rate simulates the effectiveness of detection imposed by the government enforcer (or its network of enforcement nodes). The detection rate is a constant given to the system during the initialization phase and it is fixed during the complete simulation process to emulate the governance structure in place.

When talking about the strategy definitions in the distributed (i.e., self-governing) approach, the PU has greater control over the sharing parameters. The main task of the PU is to update the boundaries or size of its surrounding exclusion and protection zones. This update process is based on the behavior of the SU agents and the continuous dealing process. The MetSat can reduce the size of the LAZ and NAZ areas if it receives a "good" signal from the SUs (i.e., no interference has occurred). It can also increase the size of both zones to achieve greater protection against interference events. In any case, the variation in the size of these zones has a direct impact on the ability to detect enforceable events (i.e, the detection rate decreases when the monitoring area increases). For our model, we have selected a linear relationship to capture this problem, which is described in expression 2.

$$d = \frac{MxE}{S} \tag{2}$$

Expression 2 captures the relation between increasing the size of the protection zones, S, and the ability of the system to detect interference situations, d. This detection rate of interference events is also the product of M, which represents the minimum size of the zone to avoid interference, and E, which is the detection effectiveness of the equipment being used (i.e., a probabilistic variable of whether an interfering agent is "caught").

The size of the restricted areas are dynamically adjusted in the system as the simulation progresses. However, the PU still has to "decide" the initial boundary of the restricted areas, and the number of policing equipment units that simulate the "effectiveness", E, of such system. In self-enforcement, this is considered as an "initial gesture of trust" to start a dealing process [49]. Whether an interference event is detected or not by the system in place, the PU is responsible for updating the size of the restricted zones. This is given by the strategy for the PU to modify the boundaries defined according to expression 3.

$$S = \begin{cases} Increase, & Interference \geq 1 \text{ and } S < 1 \\ Decrease, & Interference = 0 \text{ and } S > 0 \end{cases} \tag{3}$$

*b) **Definitions for the Secondary User**:* In Table III, we can observe the rules defined for the secondary users. One important thing to notice here is that the defined rules do not vary with the type of governance system in place. The reason behind this assumption is that the SU always follows the same rule, that is, only transmit when authorized.

The new entrants in the band start by obtaining information on the size of the restriction zones from the LTE eNodeBs. At the same time, SUs are moving around the environment while transmitting using the available spectrum space. To model the behavioral strategies of SUs, we rely on tax evasion literature, particularly on the works by Bloomquist [50], Mittone and Patelli [51], and Davids et al. [52]. Such a well-known modeling strategy allows us to capture user perception of enforcement when complying with the assigned rules. In this manner, although all SU agents have a set of rules to follow (see Table III), they might break them from time to time based on their own enforcement perception and

	Handset Definitions				
Attributes	Handset	Handset	Handset	Handset	Handset
Deontic	Obligated	Forbidden	Permitted	Permitted	Permitted
aIm	Associate with eNodeB	Transmit in NAZ	Transmit in LAZ	Transmit in UAZ	Move around
Condition	All the time	All the time	TXs <Threshold	All the time	All the time
Or Else	None	Sanction	Sanction	None	None

TABLE III
RULES, NORMS, AND STRATEGIES FOR THE SUS (LTE HANDSETS)

associated risk profiles. In other words, they might choose to transmit in the NAZ or the LAZ (when the maximum threshold has already been reached), even though this would cause a spectrum usage conflict. To account for this perception-based decision-making process, our model is based on the standard microeconomic theory of Allinghman and Sandmo [53]. This economics theorem states that a given user will break the rules whenever the perceived caught rate, p, and penalty rate (i.e., sanction), f (where $f \geq 0$), take on values that make expression (4) true.

$$p < \frac{1}{1+f} \tag{4}$$

The problem with Equation (4) is that it does not capture other factors that affect the decision-making process of a given agent. Bloomquist [50] argues that rule-breakers with high compliance opportunity costs (i.e, high discount rates) are more likely to break the rules than other agents. Nonetheless, this is not the only factor that influences the decisions of a given agent. For instance, the time lag between breaking-the-rule and the sanction, or the perceived detection ability of the system should also be taken into account. Consequently, we can use the alternative decision-making expression shown in equation (5).

$$p < \frac{1}{1+cr} \tag{5}$$

$$cr = \frac{fxd}{(1+r_i)^t} \tag{6}$$

With our new parameters, a given user will break the rules if, and only if, expression (5) is true. The cr factor is the product of the interaction of the most important factors affecting the decisions of a given agent, and it is defined by Equation 6. In the expression 6, t, is the average number of time periods between the infraction and the detection; d, is the detection rate of the enforcer, where $0 \leq d \leq 1$; and r_i is the discount rate for the agent i [50]. Based on expressions (5) and (6), an SU agent will break the rules whenever the perceived caught rate, p, and the agent perception, cr, take on values that make expression (7) true.

$$T_x = \begin{cases} No, & \text{if } p \geq \dfrac{1}{1+cr} \\ Yes, & \text{Otherwise} \end{cases} \tag{7}$$

The factors described in expressions (5), (6), and (7) can take on multiple levels. Further, different combinations of these factors can result in distinct decision-making processes for the agents, as depicted in Figure 5. For example, if the detection is immediate, the decision to transmit depends only on the detection rate, d. If only one time period passes between the infraction and the sanction, an agent's transmission decision is based only on its discount rate, r_i. We also observe that the discount rate, detection time, and detection rate of the system affect the different features of the decision-making process, hence providing different outcomes. This shows that the Bloomquist expression captures all the factors involved in the decisions of an independent agent, in a very concrete manner. In our agent-based model, we capture all the aforementioned parameters (see Table IV).

B. *Reaching agreements in self-enforcement*

The main premise of the distributed governance model is that the size or boundaries of the restricted zones are not static. Instead, zone boundaries are the result of the continuous interactions and communication efforts among the PU and SUs. The main intent of this negotiation process is for the agents, and only the agents, to agree on optimal boundaries for the restricted zones (LAZ and NAZ) that protect the incumbent and provide enough incentives for the new entrants. This captures a key aspect of self-governance, the "discipline of continuous dealing". To avoid future conflict situations, the PU increases the size of the restricted areas to obtain additional interference protection against unauthorized SUs' transmissions. Nonetheless, an increase in the size of the restricted areas reduces the available spectrum space for new entrants. In absence of conflict (i.e., when SUs are complying with the transmission requirements in the band), the PU reduces the size of its protection zones, hence increasing participation incentives and resource value for the SUs.

The ideal scenario in this continuous dealing framework is to find the "optimal" boundaries for the different sharing zones, which would lead to a scenario where the system is in a "stable" state. In the context of our work, stable means that there are no future drastic changes in the size of the restricted zones. In other words, a stable system would represent a well self-governed band where agents agree on a restricted zone size that guarantees that conflict situations would not impact the normal operations of the PU while giving enough incentives to the SUs (i.e., higher opportunities to access the available resources).

In our model, a well self-governed 1695-1710MHz band is one where the system reaches a "stable" state. Stability represents a condition in which the incumbent and the new

ABM Variable	Name	Levels
PerceptionFunction	Agent Perception: p	Actual, Perceived, Actual+Random, Perceived+Random
DetectionRateNAZ	Detection Rate in NAZ: d	From 0 to 100%
DetectionRateLAZ	Detection Rate in LAZ: d	From 0 to 100%
AverageDiscountRate	Discount Rate: r_i	From 0 to 100%
AdjudicationTime	Time to be sanctioned: t	From 0 to 10 Time Periods
PenaltyRate	Penalty: f	From 0 to 10 Units

TABLE IV
FACTORS INCLUDED IN THE 1695-1710MHZ ABM MODEL

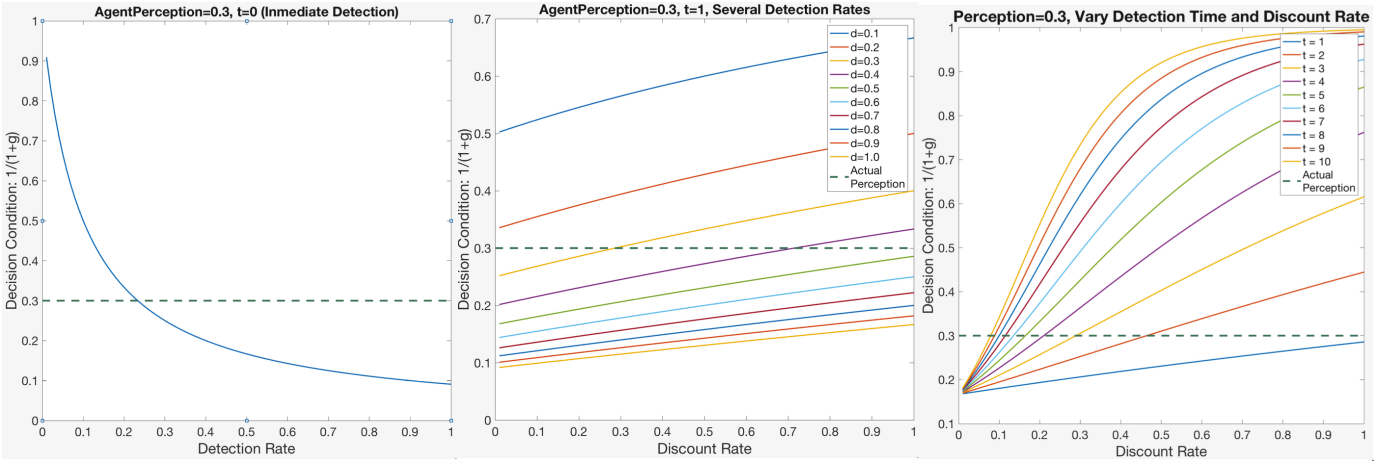


Fig. 5. Effects of the different parameters in the decision-making process of a given SU agent

entrants of the band reach an agreement on the size of the restricted zones without a government, in any principal form, intervening in the negotiation process. Further, when the system is in a stable state, the number of conflict situations (i.e., interference events) due to SUs' unauthorized transmissions is minimal, hence limiting the impact on the normal operations of the PU.[14] In this regard, we can observe in Figure 6 that the proposed negotiation for the size of restricted areas takes place in almost all scenarios regardless of their initial configurations. All simulations representing a case where there is a change in the initial boundaries of the restricted zones (left graph) converge to a stable state in which we reach an agreement on a proper area size. Additionally, we notice that when initial sizes are over 50% of the maximum allowed, they are reduced to more manageable boundaries. When analyzing the detection effectiveness of the system (right graph), we observe that this factor has an impact on the negotiation process. This is due to the fact that when a higher number of agents are caught or their neighbors have been sanctioned, their perception of the enforcement mechanisms changes. Consequently, the number of interference events is reduced, and negotiations take place to adjust the size of the restricted areas. In the particular case of detection effectiveness, when it is very low, we can expect only an increase in the LAZ and NAZ. However, for values over 50%, we can see a reduction in the areas, which is even more evident at very high effectiveness rates. When considering the effectiveness of the system alone (i.e., the equipment capabilities to detect interference events), we can observe that the entire system also reaches a stable state. In other words, there are no further changes in the boundaries of the restricted zones.

As previously mentioned, another key element when evaluating the stability of the system is the number of conflict events occurring in the system. In this context, it is important to observe how the amount of interference events (i.e., enforceable events) correlates to factors such as the initial signals provided by the PU and SUs. In Figure 7, we describe the relationship between the initial gestures and the total number of events in the system. In this figure, the x-axis represents the size of the restricted zones, the y-axis shows the effectiveness of the detection method, and the proportion and color of the "bubble" represent the total number of events in the simulation. These results show that the combination of a very high detection rate and the smallest initial size results in the lowest total number of enforceable events in the system. Further, we find the lowest total number of events in all cases representing smaller restriction areas. For larger area sizes, we observe an interesting phenomenon: even when the detection effectiveness increases, the number of events is not reduced in the same proportion. This demonstrates again that in self-enforcement scenarios, signaling between users has a greater impact than the solely effectiveness to catch "bad" agents.

These results lead us to conclude that a self-enforcement mechanism could be a successful alternative to govern the spectrum sharing framework of the 1695-1710MHz band. Nevertheless, it is necessary to point out some of the caveats of the system. First of all, the band has well defined and identifiable

[14]A poorly governed spectrum sharing scheme is one where the size of the restricted zones keeps changing or the PU is "forced" to maintain the biggest restricted areas for its protection against harmful interference.

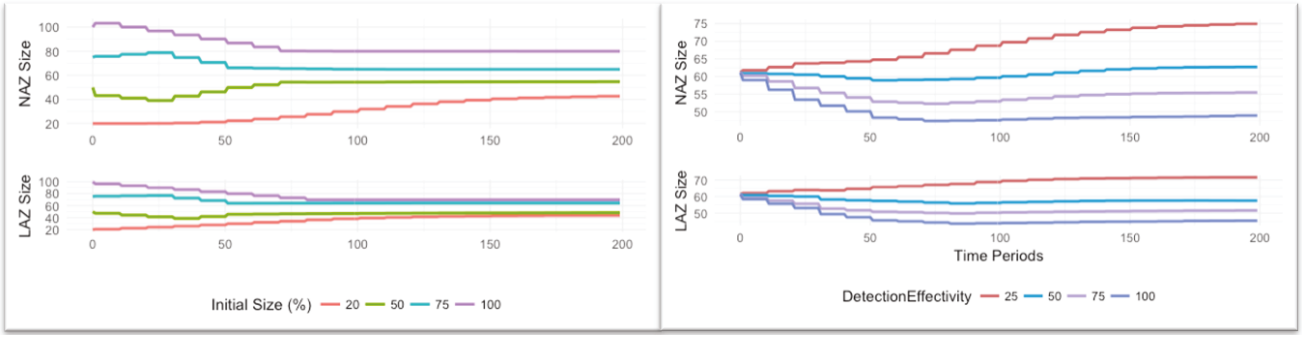


Fig. 6. Self-governance 1695-1710MHz model: Evolution of the SU/PU negotiation process of updating the LAZ and NAZ size

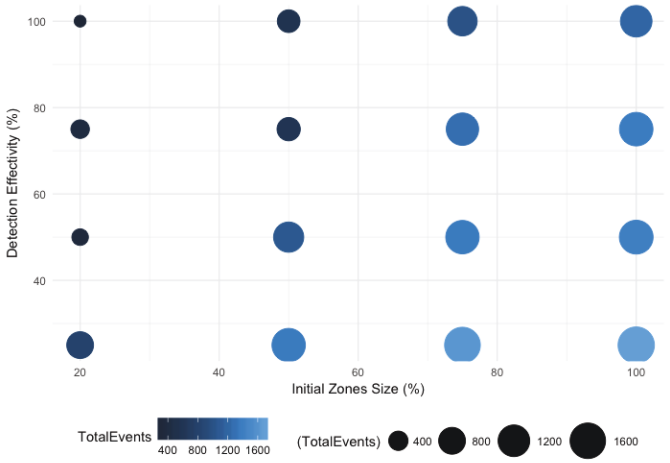


Fig. 7. Self-governance 1695-1710MHz model-Initial Size vs. Detection Rate

participants, which makes it easier to assign the norms and rules for each participant. Second, as in many other self-governing scenarios, the system reaches a stable state where the PU and SUs can agree on the parameters of the system; however, this requires a continuous process where enforceable events are still happening in many situations. Finally, the outcome of the system is highly correlated with the initial signaling process. In this light, gestures of higher trust generate better scenarios for future dealings. This is especially true in cases where the initial size of the coordination and exclusion zones are smaller. Further, initial gestures in self-governing scenarios were a more successful path to reduce the number of enforceable events than increasing the system's ability to catch bad agents (i.e., detection effectiveness, E), which is usually the premise of private property rights schemes.

VI. Adjudication Analysis

Observing the amount of enforceable events is imperative as there is limited research in this area that can serve as a baseline for how the FCC adjudicates violators - those who readily and willingly violate the code of federal regulations (C.F.R), as well as, FCC rules. As the market prepares for the emergence of new innovative technologies such as autonomous vehicles (self-driving cars) and 5G LTE cellular services, more research is being conducted to gain a better understanding of the existing spectrum landscape. Moreover, additional investigation is occurring regarding whether current regulatory practices will be sufficient enough to maintain oversight and enforcement for violators in the event that interference is caused between the vast amount spectrum users. The primary question the research conducted in this section strives to answer is, what is the current state of enforcement for radio spectrum? Secondarily, we posit what current technologies can be utilized to update infrastructure to enhance spectrum regulation by using automated means. The overall goal of this research area is to assess the current state of affairs of spectrum policy and regulation and eventually develop an adaptable automated policy infrastructure that can withstand the next wave of emerging innovative technologies.

To better understand the current state of FCC adjudication of spectrum interference, we analyzed a subset of the FCC enforcement bureau (EB) database.

In most cases, spectrum management, allocation, and the overarching logistics of how regulation is conducted within the United States consistently focuses on mechanisms such as licensing, intensive spectrum sharing techniques, and how to best utilize spectrum in order to ensure competition within the market – however, enforcement and the violations that occur are continuously being discounted. This research investigates the Federal Communication Commission's Enforcement Bureaus' adjudication decisions with the primary focal point being spectrum violations. The primary methods utilized for this research are qualitative. Through data collection and archival research of the Federal Communications Commission's Enforcement Bureau, over 8000 records were reviewed and the subset regarding spectrum interference has been examined further using qualitative analysis in order to better ascertain the existing enforcement processes of the FCC.

Attributes selected included the name of the person and/or business receiving the violation (entity type), the case number – linked the corresponding html document, date of violation – and if not specified the date of the violation notice/enforcement action, city, state, frequency/ explanation of violation – for spectrum implicit cases, penalty – if there was a financial penalty imposed, enforcement type – the publication

the violation was filed under (e.g. NOUO, Forfeiture Order, etc.), type of entity (such as a business (BUS), individual (IND), or religious establishment (REG)), enforcement bureau department location, and lastly, whether the violator was licensed/unlicensed. Preliminary results for this research indicate that although spectrum interference between 2017-2010 account for 15 percent of the records from the Federal Communications Commission's Enforcement Bureau, close readings of these events show that the process in which the FCC EB is using in order to regulate spectrum in this manner may not withstand the forecast of innovative technologies expected to enter the market in the near future. This is to mean, that several documents discuss the mailing and correspondence regarding these matters instead of a system being utilized for regulatory persons, licensees, and the general public which would not only provide ease of responding to a letter of inquiry or submitting a complaint to the FCC, but also allow the transmission of updates (e.g. new policies, erratum, and receiving information from licensees and the general public) in a prompter manner. Moreover, when thinking of policy as a service (PaaS) and the impending arrival of the internet of things (IoT), autonomous vehicles –especially level four automation, embeddable technologies, and 5G services, it becomes ever more critical to investigate the state in which regulation and enforcement are being implemented and begin strategizing on more innovative measures to deploy policy measures and enforcement mechanisms.

The dataset is now a corpus of records ranging from 2017-1999. This that there are now 8040 records pertaining to violations adjudication actions and policies. Out of this dataset, 1250 cases are spectrum violations, which account for 11.8 percent of the cases. In figure 8, it shows which entities are the main violators regarding spectrum according to the FCC data.

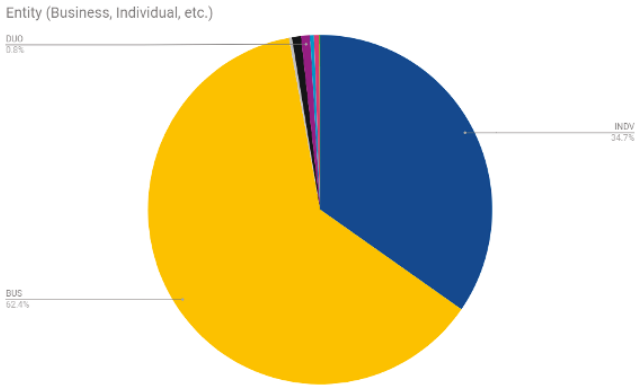


Fig. 8. Violation Entities

when spectrum violations are compared to the other violations (such as not registering antenna structures, marketing/importing unauthorized devices, and/or defrauding the E-Rate program). Even more so, spectrum explicit violations only make up 4.5 percent of the overall dataset which causes me to infer that spectrum interference is a low hanging fruit in the grand scheme of violations where the FCC needs to take enforcement action. The working hypothesis on this phenomenon is that this increase in business entities as violators is due to their infractions being more nuanced and not necessarily spectrum explicit violations. Through the data, we found that some of the businesses (e.g. hotels) jammed/blocked service in order to promote the use of their own Wi-Fi. Additionally, there are circumstances where businesses may be operating with an expired license, or they are not abiding by their FCC license.

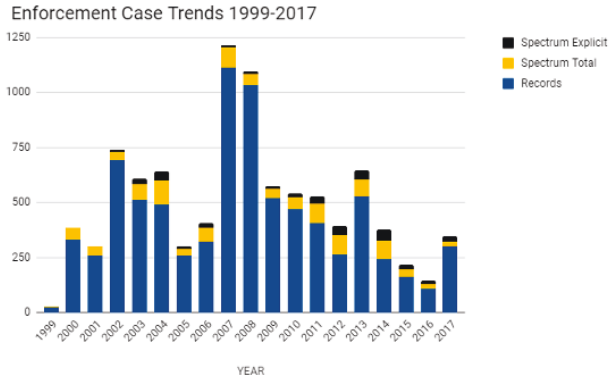


Fig. 9. Enforcement Case Trends

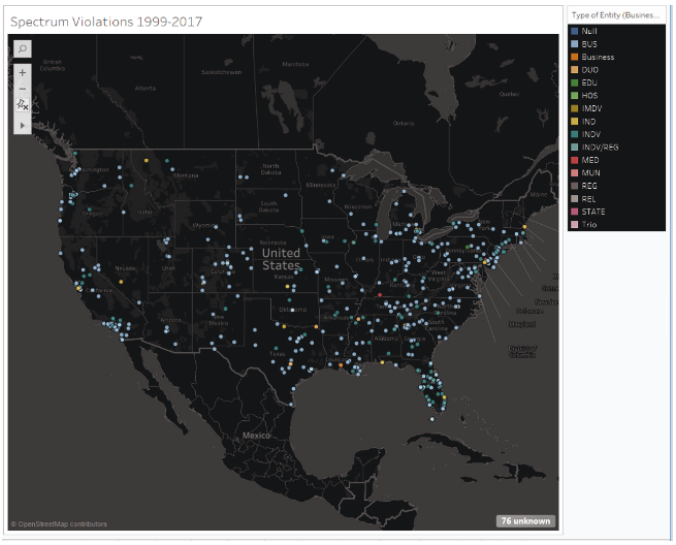


Fig. 10. Spatial Distribution

VII. Crowdsourced Detection

Traditional methods of deploying dedicated physical spectrum monitoring infrastructure [54] do not necessarily ensure a high coverage of channels in the area of spectrum enforcement and is not cost effective [23], [55]. Therefore, a crowdsourced approach is utilized for spectrum enforcement.

A. System model

A "divide and conquer" approach is utilized to ensure maximum coverage of the area of enforcement. To this end, we propose division of the entire area of enforcement R into smaller regions by using Lloyd's algorithm (as shown in Figure 11) [55]–[59] and then focus on solving the enforcement problem for every region $r \in R$. Authorized transmitters, who are legitimate Secondary Users gain access to an available channel through the local access point AP_r in $r \in R$. Conversely, malicious transmitters intrude on spectrum by the illicit use spectrum frequencies in r that they have not been authorized to use by the local AP_r [55]–[58]. A fraction of authorized, mobile users volunteer to monitor a channel for detecting such spectrum access misuse. Such volunteers are assumed to be *honest* (who report truthfully every time) or corrupt (who give a false report probabilistically). In addition, there is a set of mobile sentinels $\mathcal{S}'$ who monitor channels at random time intervals to verify the detection results reported by volunteers [55]–[58]. Finally, there is a central DSA Enforcement Infrastructure to select volunteers for spectrum monitoring. It consists of Volunteer Service units Ω_r for storing and updating volunteer attributes in all $r \in R$, a Volunteer Selection Unit for selecting volunteers based on the information in Ω_r and a DSA Database that maintains the list of channels and their authorized occupants in R [55]–[58].

Total enforcement time is divided into smaller intervals called Monitoring Intervals or MIs. Each MI is further divided into sub-intervals called Access Unit Intervals or AUIs. An AUI is defined as the smallest time interval over which useful work can be accomplished by a user [55]–[58]. We further divide an AUI into Sampling Intervals (SIs), over which a sentinel and a volunteer senses a channel to determine its access type over the AUI. A new set of volunteers is selected by the Volunteer Selection Unit of the centralized DSA infrastructure at the beginning of every MI [55]–[58]. Volunteer selection in r is primarily based on its qualification and is determined by the parameters discussed below [55], [56].

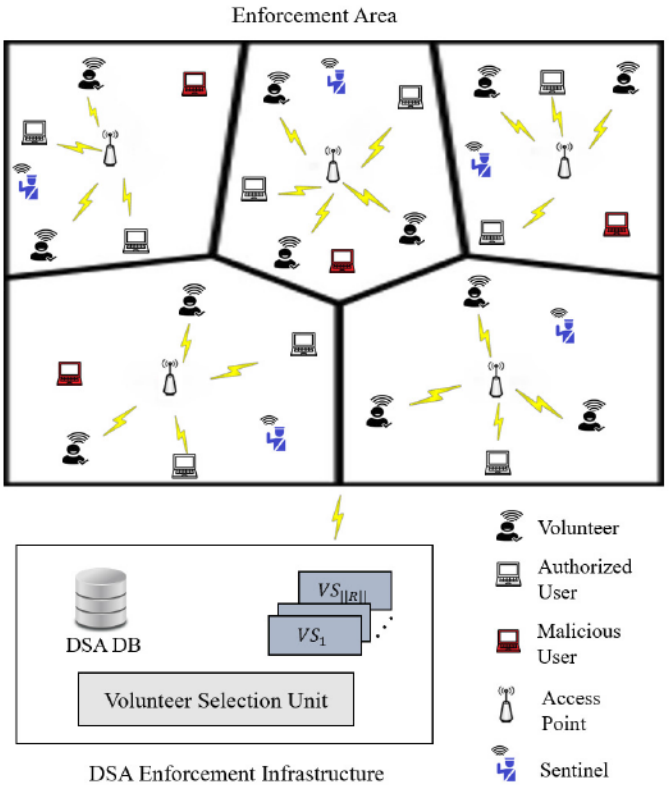


Fig. 11. System Model

*1) **Reputation**:* As discussed in [55], [56] and as shown in Fig. 8, during enforcement, a volunteer v in region r makes an observation $O^{i,j}_{v,r,c}$ of the access state of channel c in every SI j and a sentinel s makes an observation $O^{i,k}_{s,r,c}$ at a random SI k of an AUI i. On the basis of these observations, both v and s arrive at a decision on the spectrum access state of channel c in region r over an AUI i [55], [56]. It is assumed that a volunteer v's decision $\theta^i_{v,r,c}$ is accurate if it is similar to the decision $\theta^i_{s,r,c}$ of sentinel s [55], [56]. We determine trustworthiness $T_{v,r,c}$ of a volunteer by its accuracy in detection of spectrum access violation, where a volunteer v's detection result is accurate if it matches the detection result of a sentinel s [55]–[58]. A sentinel s decides to monitor channel c only at random AUIs to verify the decisions made by the volunteers. The minimum number of observations that are needed by a sentinel in an AUI to determine the ground truth of spectrum access state with a margin of error φ at $X\%$ confidence level is at least $0.25(z^*/\varphi)^2$, where z^* is the critical value [55], [56].

As discussed in [55], [56], the reputation $\Gamma_{v,r,c}$ of a volunteer v in r for channel c is established based on the volunteer's trustworthiness over an extended duration. The primary principle of our approach is to increase reputation slowly after success and decrease it rapidly after it drops below

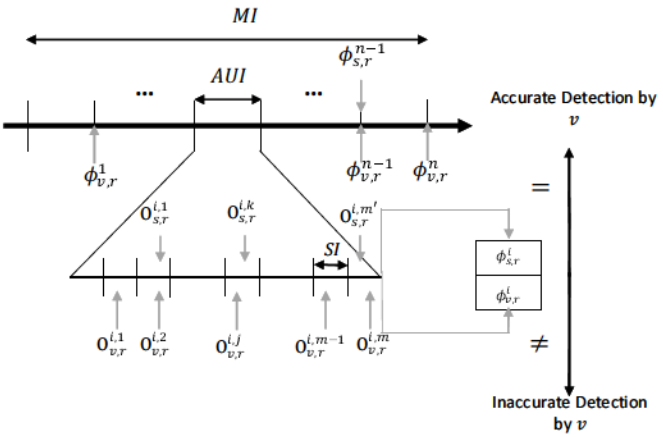


Fig. 12. Decisions by volunteer v after every AUI and by sentinel s after random AUIs, for a given MI.

a threshold [55], [56]. Reputation $\Gamma_{v,r,c}^{z,i+1}$ of a volunteer v at the beginning of AUI $i+1$ of MI z for monitoring channel c in r is given by (8).

$$\Gamma_{v,r,c}^{z,i+1} = \begin{cases} \Gamma_{v,r,c}^{z,i} + f(T_{v,r,c}^{z,i}), & \text{if accurate} \\ \Gamma_{v,r,c}^{z,i} - g(T_{v,r,c}^{z,i}), & \text{otherwise} \end{cases} \tag{8}$$

where $T_{v,r,c}^{z,i}$ is the trustworthiness of v for monitoring c in r after it makes a decision in AUI i of MI z, $f(T_{v,r,c}^{z,i}) = \kappa.T_{v,r,c}^{z,i}$ (where κ is a system parameter) and $g(T_{v,r,c}^{z,i}) = e^{\lambda.(1-T_{v,r,c}^{z,i})}$, such that λ increases if $\Gamma_{v,r,c}^{z,i} < \zeta$, where ζ is the threshold below which reputation is penalized more rapidly. Thus, the reputation is increased linearly when an accurate decision is made by v and decreased exponentially otherwise [55], [56].

*2) **Proportion of Residence Time**:* Volunteers who are likely to reside for a higher proportion of time in region r compared to other regions are preferred to monitor r. The proportion of residence time $\rho_v(r)$ of a volunteer v in r is given by (9).

$$\rho_v(r) = \frac{\tau_v(r)}{\sum_{r \in R} \tau_v(r)} \tag{9}$$

where $\tau_v(r)$ is the total time spent by v in r [55], [56].

*3) **Duration to Destination**:* Volunteers who are likely to reach a region r in shorter duration are preferred for monitoring channels in r. At time t, the location L_v^t of volunteer v enables us to estimate the shortest duration $\Upsilon_v^t(r)$ needed by v to reach a region r, as shown in (10).

$$\Upsilon_v^t(r) = \frac{\gamma.d(L_v^t, \mathcal{O}_r)}{\tilde{\mu_v}} \tag{10}$$

where $\gamma > 0$ is a system parameter, $\tilde{\mu_v}$ is v's average velocity, $\mathcal{O}_r$ is the centroid of region r and $d(L_v^t, \mathcal{O}_r)$ is the shortest distance between L_v^t and $\mathcal{O}_r$ [55], [56].

*4) **Sojourn Time**:* Volunteers who are estimated to have a higher sojourn time in region r after a visit to r are preferred to monitor channels in r. To this end, the sojourn time of a volunteer v in r after every visit of v to r is estimated [55]–[58]. After the j^{th} visit of v to r, we measure its $(j-1)^{th}$ sojourn time, $S_v^{j-1}(r)$ as the difference between its $(j-1)^{th}$ departure time, $dep_v^{(j-1)}(r)$ from r and its $(j-1)^{th}$ arrival time, $arr_v^{(j-1)}(r)$ in r [55]–[58]. Based on this information, the proportion of time that v is likely to stay in r before its j^{th} departure from r is estimated as an exponentially smoothed average [55], [56], given by (11).

$$\tilde{S}_v^j(r) = \alpha.S_v^{j-1}(r) + (1-\alpha).\tilde{S}_v^{j-1}(r) \tag{11}$$

$$\alpha = h.(E_v^{j-1}(r))^2 / \sigma_v^j(r) \tag{12}$$

where $0 < h < 1$, $E_v^{j-1}(r) = S_v^{j-1}(r) - \tilde{S}_v^{j-1}(r)$ is the prediction error on visit j, and $\sigma_v^j(r)$ is the average of the past square prediction errors [55], [56], as shown in (13).

$$\sigma_v^j(r) = h.(E_v^{j-1}(r))^2 + (1-h).\sigma_v^{j-1}(r) \tag{13}$$

B. Volunteer Qualification

The Volunteer Selection Unit selects up to k *qualified* volunteers to monitor R at the beginning of every MI. This is determined by the Qualification $Q_{v,r,c}(MI)$ of a volunteer v to monitor a channel c in $r \in R$ over the next MI, given by (14), defined below [55], [56].

$$Q_{v,r,c}(MI) = f(\Gamma_{v,r,c}, \tilde{S}_v^j(r), \Upsilon_v^t(r), \rho_v(r)) \tag{14}$$

The parameters $\Gamma_{v,r,c}, \tilde{S}_v^j(r), \Upsilon_v^t(r), \rho_v(r)$ are normalized by using the min-max normalization technique [60] such that $0 \leq \Gamma_{v,r,c}, \tilde{S}_v^j(r), \Upsilon_v^t(r), \rho_v(r) \leq 1$. As discussed in [55], [56], we define function f by (15) because it gives the best result among all variants of f that are tested.

$$f = p_0.(\frac{w_1}{w_1+w_2}.p_1 + \frac{w_2}{w_1+w_2}.p_2) \tag{15}$$

We assume that reputation is the most significant component of the selection metric because we strive to get rid of unreliable volunteers, irrespective of their likelihood to be in a region [55], [56]. Furthermore, a volunteer who is likely to have high residence time in a region r is preferred for selection. Hence, the proportion of residence time $\rho_v(r)$ is considered to be next in priority. The parameters Sojourn time and Duration to Destination are next in priority. To this end, we define $p_0 = \rho_v(r).e^{\beta.\Gamma_{v,r,c}}$, where $\beta > 0$, $p_1 = 1 - \Upsilon_v^t(r)$ and $p_2 = \tilde{S}_v^j(r)$, w_1 and w_2 are the weights associated with p_1 and p_2 respectively, such that $w_1 > w_2$ [55], [56] in (15).

C. Volunteer Selection Algorithms

We discuss the design and application of a Secretary-based algorithm and two variants of the stable matching algorithm for volunteer selection. Stable matching is essential to ensure that both the preferences of volunteers and the channel attributes are taken into consideration, which in turn helps in ensuring lesser overhead of switching channels and better volunteer satisfaction [55]. In addition, we combine these vanilla algorithms to develop two hybrid algorithms. Finally, we discuss about a random algorithm which acts as a baseline algorithm.

*1) **Secretary-Based Algorithm**:* As discussed in [55], we use a variant of the Multiple-Choice Secretary (*MC-Secretary*) algorithm as the first volunteer selection algorithm. This algorithm employs a threshold-based methodology and attempts to optimize the probability of selecting the most qualified volunteers [55]–[58], [61], [62]. Using this methodology, at most k_r volunteers are selected for every region $r \in R$. Since this is a threshold-based methodology, we initially select up to $k_r/2$ volunteers recursively [55]–[58], [61] to determine a threshold. Among the remaining volunteers, we select only those volunteers whose qualification value surpasses this threshold. While this methodology helps us to select a set of volunteers $V_{S,r}$ in region r based on their qualification to monitor spectrum in r, it does not assign channels to volunteers for monitoring [55]–[58], [61]. Therefore, as discussed in [55], [56], [58], a modified Round Robin channel assignment scheme (executed by function *Assign_Channels()*) is developed for assigning

channels to volunteers based on their qualification (given by (14) and (15)) to monitor a channel in a region of enforcement.

*2) **Volunteer Matching**:* As discussed in [55], the Volunteer Matching algorithm (*VM*) selects volunteers to monitor spectrum by using a variation of the stable matching algorithm that is proposed by Gale and Shapley [63] for college admissions. For this purpose, a Priority list P_v^r is maintained by every volunteer such that it contains the list of channels (ordered by the volunteer's preferences [55]) that a volunteer v can monitor in a region $r \in R$. Similarly, a Candidate list χ_c^r is maintained by the Volunteer Service Unit Ω_r of the centralized DSA Enforcement Infrastructure for every $c \in C$ in every $r \in R$. A Candidate List is used to maintain the list of volunteers (sorted in descending order by their qualification) who apply to monitor channel c in region r [55].

In this algorithm (executed by function *Volunteer_Match()*), the Candidate list χ_c^r associated with channel c in region r is initially filled with volunteers who have this channel c as their first preference to monitor in their Priority Lists [55]. Out of all the volunteers in the Candidate List of a channel c in region r, only the top q_c^r (such that $q_c^r = k/(||R||.||C_r||)$, where k is the maximum number of volunteers to be selected in R, $||R||$ is the number of regions and $||C_r||$ is the number of channels in r) candidates are stored in the waiting list W_c^r (ranked by their qualification) and the remaining candidates are rejected and stored in a reject list Θ_c^r [55]. This process is repeated for all the channels in the area of enforcement [55]. A volunteer v who is rejected to monitor a channel c will apply to monitor their next choice of channel in their Priority list and the process continues till every volunteer is either in the reject list of all channels or is in the waiting list W_c^r of a channel c in region r [55] . Finally, all the volunteers who are in waiting list W_c^r of a channel c in region r are selected and assigned to monitor c in r (for every $c \in C$ in every $r \in R$) [55].

*3) **Reverse Volunteer Matching**:* As we discussed in [55], it is assumed that for the Reverse Volunteer Matching algorithm (*RVM*), each volunteer $v \in V$ maintains a Priority list P_v^r of channels ordered by its preferences to monitor channels in the area of enforcement (similar to what was maintained in Algorithm *VM*). However, contrary to Algorithm *VM*, where volunteers propose to the centralized DSA infrastructure to be matched to a channel of their choice for monitoring, by using this algorithm *RVM*, the centralized DSA infrastructure first collects all the proposals from volunteers in V and then *proposes back* to volunteers (based on their qualification) with offers to match them to channels in the area of enforcement [55], [63]. The volunteers then choose to either accept or reject this offer based on their availability and/or preferences.

In this algorithm (executed by function *Reverse_Volunteer_Match()*), the Volunteer Service unit Ω_r of region r is responsible for constructing a Candidate list χ_c^r for every channel c in region r such that it contains the list of all volunteers who applied to monitor c in r [55]. This candidate list of volunteers is sorted in descending order by the qualification of volunteers and transmitted to the Volunteer Selection Unit of the centralized DSA infrastructure [55]. The Volunteer Selection Unit gives an offer to monitor a channel c in region r to the first volunteer (i.e., the most qualified volunteer) v_{top} in the Candidate List χ_c^r. If this volunteer v_{top} is not yet assigned to monitor any other channel, then v_{top} and c are matched and the matched channel-volunteer pair is stored in the Match List M_c^r that is maintained by the Volunteer Service Unit Ω_r for every channel c in every region r of the spectrum enforcement area [55]. Conversely, if volunteer v_{top} has already been assigned a channel c' to monitor in region r', and if v_{top} prefers to monitor channel c in r compared to its currently matched channel c' in region r', then v is matched to c instead and removed from the match list $M_{c'}^{r'}$ that is maintained for c' in region r' [55]. This process continues till every channel $c \in C$ in every region $r \in R$ has at most q_c^r matched volunteers or there are no more volunteer left in Candidate List χ_c^r to propose an offer to by the Volunteer Selection Unit [55]. Ultimately, every volunteer in the Match List M_c^r of c in r is selected and assigned to monitor channel c in region r (for every $c \in C$ in $r \in R$) [55].

*4) **Hybrid Algorithms**:* As discussed in [55], the algorithm *MC-Secretary* is combined with the matching algorithms *VM* and *RVM* to develop two hybrid algorithms named *HYBRID-VM* and *HYBRID-RVM* respectively. This helps us to combine the benefits of the individual vanilla algorithms and thereby get an improvement in performance [55]. In both *HYBRID-VM* and *HYBRID-RVM*, we feed the volunteers who are selected by using the algorithm *MC-Secretary* to functions *Volunteer_Match()* and *Reverse_Volunteer_Match()* respectively [55]. This is done to establish a threshold above which volunteers are selected for being matched to channels [55].

*5) **Random Algorithm**:* This algorithm represents the baseline with which every other volunteer selection algorithm is compared [55]–[58]. Using this algorithm, volunteers are selected in random irrespective of their qualification to monitor a channel in a region [55]–[58]. Channels are assigned to volunteers in a simple Round Robin manner, irrespective of their qualification or preferences [55].

D. Experimental Setup

As discussed in [55], for the purpose of our experiments, it is assumed that one MI consists of five AUIs and that volunteers are selected at the beginning of every MI (starting from the second MI). The values that we choose for the Simulation parameters are shown in Table V [55]. It is assumed that a volunteer $v \in V$ uses a sensing device that has a maximum battery capacity of $7Wh$ and that the discharge rate of the battery is $1J/s$ for a random time interval which is drawn from an exponential distribution of the mean active time interval of 100 s [55]–[58]. At the end of every active time interval, it is assumed that the sensing device remains idle for a random time interval that is drawn from an exponential distribution of the mean idle time interval of 10 s [55]–[58]. Simulation is run till battery of the sensing device used by every volunteer

is exhausted [55]–[58]. We measure the performance of the volunteer selection algorithms using the following metrics:

1) *Average Rank of Match*: This represents the average rank of channel (that a selected volunteer v is assigned to monitor) in v's Priority List P_v^r, for all $v \in V$ who are selected to monitor spectrum over the entire duration of simulation [55]. A lower value indicates higher *volunteer happiness* [55].
2) *Mean Hit Ratio*: This represents the mean ratio of the number of hits to the total number of hits and misses. If a volunteer v selected for monitoring region r is present in r at the beginning of an AUI of a MI that v is selected for, then it is considered a *hit*, otherwise it is considered a *miss* [55]–[58]. A higher hit ratio will indicate higher coverage of the area of enforcement R by volunteers over the period of enforcement [55]–[58].
3) *Mean Accuracy of Detection*: We assume that all of the volunteers detect spectrum misuse with probability δ (such that $\delta = 0.5$ for corrupt volunteers and $\delta = 1$ for honest volunteers) times the potential quality of spectrum misuse detection $\psi_v^{c,r}$ (which depends on characteristics of the spectrum sensing device used by a volunteer) [55]. We consider the misuse detection result by a volunteer accurate if it is above a threshold (i.e., matches that of a sentinel s in region r at an AUI in which s monitors) [55].

E. Results

We evaluate and analyze the performance of the volunteer selection algorithms by using the three performance metrics. As discussed in [55], in the first analysis, we measure and compare the average rank of match for the volunteer selection algorithms. It is to be noted that in Fig. 13 and 15, *MC-Secretary-RR* refers to the Multiple Choice Secretary algorithm with simple Round Robin channel assignment (irrespective of volunteer qualification) unlike *MC-Secretary* which uses *Assign_Channels()* [55]. As expected, the baseline Random algorithm performs the worst in all the experiments because it selects volunteers randomly without considering their qualification [55]. In Fig. 13, we observe that both the vanilla matching algorithms (*VM* and *RVM*) and the hybrid algorithms (*HYBRID-VM* and *HYBRID-RVM*) have lower Average Rank of Match (which implies higher *Volunteer Happiness*) than the remaining algorithms because they utilize volunteer preferences for selection and channel assignment [55]. Additionally, we observe that *VM* (or *HYBRID-VM*) performs better than *RVM*(or *HYBRID-RVM*) because stable matching algorithms are biased towards the party who proposes [55], [63]. In the algorithms *VM* and *HYBRID-VM*, volunteers propose to the DSA infrastructure to get matched to a channel. However, in *RVM* and *HYBRID-RVM*, the DSA infrastructure first collects the applications from the volunteers and then makes the final proposal or offer to the volunteers [55]. In the next analysis, we compare the mean hit ratio of the volunteer selection algorithms. In Fig. 14, a clairvoyant *Optimal* algorithm is included which calculates in hindsight the optimal mean hit ratio after selecting k_r volunteers for every region $r \in R$ [55]. The mean hit ratio of this clairvoyant algorithm goes below 1 when k increases because the proportion of k_r volunteers staying in r decreases [55]. It is interesting to note that *VM* and *RVM* give better hit ratio than *MC-Secretary* as k increases because unlike *MC-Secretary*, the vanilla matching algorithms consider volunteer preference to monitor channels in their region of residence [55]. The hybrid algorithms utilize this benefit of the vanilla matching algorithms and in turn give higher hit ratio than MC-Secretary as k increases [55]. We observe that *HYBRID-VM* gives the best mean hit ratio across all ranges of k and performs better on average than *VM* (by 4.1%), *MC-Secretary* (by 19.2%), *RVM* (by 10.1%) and *HYBRID-RVM* (by 9.5%) [55]. In the next analysis, we compare the mean accuracy of detection obtained by the different volunteer selection algorithms. In Fig. 15, we observe that application of *MC-Secretary* to select volunteers gives higher detection accuracy than *MC-Secretary-RR* because it uses *Assign_Channels()* instead of simple Round Robin [55]. It is interesting to note that *MC-Secretary* performs better than *VM* and *RVM* in terms of detection accuracy than in terms of mean hit ratio. This is because *MC-Secretary* attempts to optimize the probability of selecting the most qualified volunteers and in volunteer qualification, the volunteer reputation (being combined exponentially) dominates [55]. We further observe that *VM* and *RVM* perform poorly as the range of k increases because volunteer preferences of channels do not always necessarily align with the best interests of the DSA infrastructure [55]. In this case, the hybrid algorithms utilize this benefit of MC-Secretary and perform better in terms of detection accuracy than *VM* and *RVM* (with *HYBRID-VM* giving the best mean accuracy for all ranges of k).

TABLE V
SIMULATION PARAMETERS

Parameter	Value
Area of Enforcement	$500m \times 1000m$
Population	1070
Number of Volunteers	183
Number of channels per region	5
Number of Regions	2
Mobility Model	Random Waypoint
Maximum Battery Capacity of Volunteer	$7Wh$
System Parameter h	0.03
System Parameter κ	1
Reputation Threshold ζ	-10
Number of AUIs	5580

VIII. DISCUSSION AND CONCLUSIONS

A. Novel enforcement mechanisms

The definition of Exclusion and Coordination Zones is a common ex-ante enforcement mechanism in spectrum sharing scenarios. The main idea is to define geographical regions where usage conflict situations do not alter the normal operations of the PU due to the lack or limited access rights of Secondary Users. Unfortunately, these areas are usually

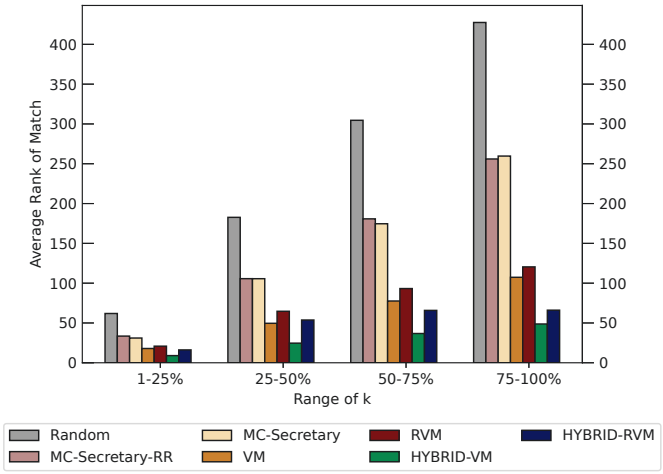


Fig. 13. Comparison of Average Rank of Match with change in k.

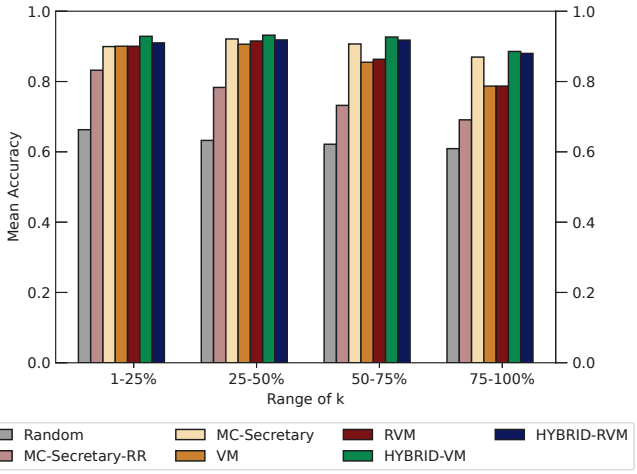


Fig. 15. Comparison of Mean Accuracy of detection with change in k.

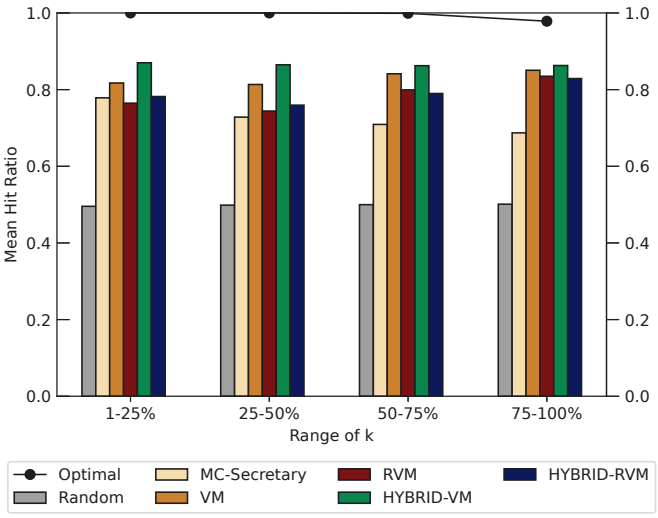


Fig. 14. Comparison of Mean Hit Ratio with change in k.

overly conservative and static. The notion of a static EZ implies that it has to protect the PU from the union of all likely interference scenarios, resulting in a worst-case and very conservative solution. In this light, we propose the MIPZ framework as a means to create multi-tiered dynamic Exclusion and Coordinatuion Zones.

Our MIPZ framework introduces the concept of multi-tiered dynamic EZs for prescribing interference protection to PUs in GDB-driven spectrum sharing. The proposed framework allows a limited number of SUs to operate closer to the PU, and improves the overall spectrum utilization while ensuring a probabilistic guarantee of interference protection. By making some reasonable assumptions, we derived a closed form expression of the aggregate interference power received by the PU, and used it to dynamically adjust the size of the EZ boundary. Using results from extensive simulations and a real world case study, we showed that our framework defines more effective and dynamic EZs that not only protect PUs from harmful interference, but also improve the overall spectrum utilization efficiency for SUs.

A common approach in spectrum sharing scenarios is the development of Software Defined Radios (SDRs). The use of these devices allows for configurable transmission parameters which goal is to protect the incumbent against unauthorized or harmful signals. Nonetheless, conflict usage situations (e.g., harmful interference) caused by "rogue" radios still poses a serious threat to many spectrum sharing schemes. A common approach to mitigate this problem is to adopt *ex-post* enforcement mechanisms of identifying such sources of interference. Usually, the burden of identifying transmitters, by authenticating their waveforms, is solely assigned to regulators such as the Federal Communications Commission (FCC) or the National Telecommunications and Information Agency (NTIA). Nevertheless, this approach faces many challenges. First, the enforcement entity that is in charge of authenticating signals is not the intended receiver of such signals. Hence, it has to decode the signal "blidnly" with little or none knowledge of the transmission parameters. In addition, a single enforcement entity may need to cope with poor signal strength and multiple simultaneous co-channel transmitters.

Our approach to mitigate the problem of authenticating signals from valid sources is the creation of dedicated and non-dedicated enforcement networks. We refer to this network as a Crowd-Sourced Enforcement Network (CEN). For this purpose, we propose a novel concept that effectively addresses some of these challenges, which we refer to as Crowd-Sourced Blind Authentication of Co-channel Transmitters (CBAT). Further, we present a concrete instantiation of this concept called FREquency Offset Embedding for CBAT (FREE). We showed that FREE can reliably authenticate multiple co-channel transmitters that are transmitting simultaneously in a channel with shadowing fading and low MSNR.

B. Alternative governance structures

The most important aspect of self-governing is the successful interaction of primary and secondary users. We showed that the size of the boundaries around the incumbent users, and hence the ability to detect "bad guys" within the system, could stem only from the negotiation process of independent agents. Further, the system could successfully allocate the shared resources according to the band's predefined set of rules. Thus, spectrum sharing through a self-governing arrangement is possible under a wide variety of realistic circumstances.

Regarding the process of self-governance, we showed that once the initial boundaries assigned into the categories of limited and unlimited use, the trust signal of reducing the size for the starting point has the biggest impact on the governance of the spectrum. When starting with the smallest size, we can expect little or no interference with the system, which is consistent with the continuous dealing principle, that is good gestures by primary users are "paid" by the secondary users, and vice versa. Our analysis also shows that perception characteristics, as represented by differences in perception functions of the secondary users, have a great impact on self-governance. When users know the rate of detection, more "infractions" are committed when the detection rate is relatively low. On the other hand, when the agents only have a perception of this rate, the number of events is considerably reduced. Nonetheless, the sole perception of a rate leads to the occurrence of interference events whereas in full knowledge scenarios, especially with higher detection rates, this is not the case. In this regard, one of the main benefits of adopting self-governance frameworks is that sharing schemes can switch from static and centralized definitions to local and dynamic agreements. Such agreements would reflect the local conditions of the sharing process, provide enough protection to the incumbent, and add significant value and incentives to the new entrants.

These results show that a self-governance structure is possible in spectrum sharing scenarios under the right circumstances. For our the band of our analysis these circumstances include a set of well-defined participants, communication channels, sharing conditions, and, most importantly, a common goal of defining optimal protection zones (i.e., avoid conflict situations for the PU while providing incentives and value for the SU). Additionally, the band provides a clear definition of the different interactions between agents and the associated rewards for a "good" behavior. As aforementioned, self-governance is not a "one-fits-all" solution. In this light, other spectrum sharing scenarios might not benefit from a self-governing approach. For instance, if there is no common incentive between the agents to reach a continuous and stable dealing process, there is a lack of clear definitions for the different agents, or there is an absence of clear communication channels between agents.

C. Crowdsourced detection

In light of automating ex post spectrum enforcement, we discuss about a crowdsourced enforcement framework across multiple channels to detect access violation. In order to achieve efficient ex post spectrum enforcement, we focus on attaining maximum coverage of the area of enforcement and of all channels, on ensuring reliable and accurate detection of spectrum violation, and on designing an efficient algorithm for selecting crowdsourced monitoring agents (or volunteers). Attaining maximum coverage of the area of enforcement is addressed by proposing to divide it into smaller regions by using the Lloyd's algorithm which is a relaxation of the Voronoi algorithm) and solving the enforcement problem by a divide and conquer mechanism over the entire area. The crowdsourced infrastructure consists of volunteers (who monitor spectrum) and sentinels (who monitor the activity of volunteers). In addition, there is a centralized DSA infrastructure which is responsible for selecting the volunteers. Volunteers are selected based on their *qualification* to monitor spectrum in an enforcement region. The qualification of a volunteer primarily depends on its reputation and likelihood to be in a region.

We further discuss about three vanilla algorithms for volunteer selection. The first algorithm, *MC-Secretary* is a variant of the Multiple-choice Secretary algorithm which attempts to optimize the probability of selecting volunteers who are most qualified to monitor a channel in a region of enforcement. Since this algorithm cannot assign channels to volunteers, a modified round robin scheme is discussed for assignment of channels to volunteers. The other two algorithms (namely *VM* and *RVM*) are variants of the stable matching algorithm that is proposed by Gale and Shapley in their seminal work. We utilize stable matching to ensure that both the preferences of volunteers and the channel attributes are taken into consideration. This helps in ensuring lesser overhead (of channel switching) and better volunteer satisfaction. We utilize the three vanilla algorithms to combine them and develop two hybrid algorithms (*HYBRID-VM* and *HYBRID-RVM*) that can take advantage of the individual vanilla algorithms. Experimental analysis is done to compare the performance of the selection algorithms over the metrics of mean hit ratio, accuracy of detection and average rank of match. We observe that the *HYBRID-VM* algorithm gives the best performance across all the metrics.

D. Adjudication analysis

With such a projected influx of technologies that will be dependent upon electromagnetic spectrum (such as fully autonomous vehicles, fifth generation cellular services, embeddable technologies, and alike), an increased interest in the regulation – and by extension enforcement – of spectrum has come into the forefront regarding present-day discussion and concern of future spectrum management. This portion of our research specifically focused on identifying the potential problems, reviewed sentiments within the field, investigated and analyzed administrative data, and provided an intervention based on available public data. We entrust and rely on regulatory institutions to create, implement, and enforce policies that can best safeguard various environments – such as radio spectrum resources. This means that there should be a system in place to carry out this task.

ACKNOWLEDGMENT

This work was sponsored in part by the National Science Foundation through grants 1265886, 1547241, 1563832, 1642949, and 1642928.

REFERENCES

[1] M. Altamimi, M. B. Weiss, and M. McHenry, "Enforcement and spectrum sharing: Case studies of federal-commercial sharing," *Available at SSRN 2310883*, 2013.

[2] T. W. Hazlett, "Spectrum tragedies," *Yale J. on Reg.*, vol. 22, p. 242, 2005.

[3] M. B. Weiss, W. Lehr, M. Altamimi, and L. Cui, "Enforcement in dynamic spectrum access systems," 2012.

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

[5] L. Shay, W. Hartzog, J. Nelson, and G. Conti, "Do robots dream of electric laws: An experiment in the law as algorithm," in *Stanford Law Conferences: We Robot, Getting Down to Business*.

[6] W. Hartzog, G. Conti, J. Nelson, and L. A. Shay, "Inefficiently automated law enforcement," *Michigan State Law Review*, vol. 2015, no. 5, p. 1763, 2016.

[7] M. Altamimi and M. B. Weiss, "Enforcement and network capacity in spectrum sharing: Quantifying the benefits of different enforcement scenarios," *Available at SSRN 2481082*, 2014.

[8] R. Murty, R. Chandra, T. Moscibroda, and P. Bahl, "Senseless: A database-driven white spaces network," *IEEE Transactions on Mobile Computing*, vol. 11, no. 2, pp. 189–203, 2011.

[9] R. A. O'Connor, "Understanding television's grade a and grade b service contours," *IEEE transactions on broadcasting*, vol. 47, no. 3, pp. 309–314, 2001.

[10] S. Bhattarai, A. Ullah, J.-M. J. Park, J. H. Reed, D. Gurney, and B. Gao, "Defining incumbent protection zones on the fly: Dynamic boundaries for spectrum sharing," in *Dynamic Spectrum Access Networks (DySPAN), 2015 IEEE International Symposium on*, pp. 251–262, IEEE, 2015.

[11] M. Vu, N. Devroye, and V. Tarokh, "On the primary exclusive region of cognitive networks," *IEEE transactions on wireless communications*, vol. 8, no. 7, pp. 3380–3385, 2009.

[12] S. Kusaladharma and C. Tellambura, "Aggregate interference analysis for underlay cognitive radio networks," *IEEE Wireless communications letters*, vol. 1, no. 6, pp. 641–644, 2012.

[13] S. Bhattarai, J.-M. Park, and W. Lehr, "Dynamic exclusion zones for protecting primary users in database-driven spectrum sharing," *IEEE/ACM Transactions on Networking*, 2020.

[14] F. C. C. (FCC), "Report and order and second further notice of proposed rule-making, gn docket no. 12-354."

[15] V. D. Blondel, A. Decuyper, and G. Krings, "A survey of results on mobile phone datasets analysis," *EPJ data science*, vol. 4, no. 1, p. 10, 2015.

[16] M. Haenggi and R. K. Ganti, *Interference in large wireless networks*. Now Publishers Inc, 2009.

[17] S. Bhattarai, J.-M. J. Park, W. Lehr, and B. Gao, "Tesso: An analytical tool for characterizing aggregate interference and enabling spatial spectrum sharing," in *Dynamic Spectrum Access Networks (DySPAN), 2017 IEEE International Symposium on*, pp. 1–10, IEEE, 2017.

[18] R. Blank and L. E. Strickling, "Report to the president," 2013.

[19] D. Hastings, "The global land one-km base elevation (globe) digital elevation model," *IGBP Newsletter*, pp. 11–12, 1996.

[20] J.-M. Park, J. H. Reed, A. Beex, T. C. Clancy, V. Kumar, and B. Bahrak, "Security and enforcement in spectrum sharing," *Proceedings of the IEEE*, vol. 102, no. 3, pp. 270–281, 2014.

[21] A. Malki and M. B. Weiss, "Ex-post enforcement in spectrum sharing," in *2014 TPRC Conference Paper*, 2014.

[22] V. Kumar, J.-M. Park, and K. Bian, "Blind transmitter authentication for spectrum security and enforcement," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pp. 787–798, 2014.

[23] A. Dutta and M. Chiang, ""see something, say something" crowdsourced enforcement of spectrum policies," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 67–80, 2015.

[24] N. Kaufmann, T. Schulze, and D. Veit, "More than fun and money. worker motivation in crowdsourcing-a study on mechanical turk.," in *Amcis*, vol. 11, pp. 1–11, Detroit, Michigan, USA, 2011.

[25] V. Kumar, H. Li, J.-M. J. Park, and K. Bian, "Crowd-sourced authentication for enforcement in dynamic spectrum sharing," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 3, pp. 625–636, 2019.

[26] V. Kumar, H. Li, J.-M. J. Park, and K. Bian, "Enforcement in spectrum sharing: Crowd-sourced blind authentication of co-channel transmitters," in *2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pp. 1–10, IEEE, 2018.

[27] G. Hardin, "The tragedy of the commons," *science*, vol. 162, no. 3859, pp. 1243–1248, 1968.

[28] B. M. Frischmann, A. Marciano, and G. B. Ramello, "Retrospectives: Tragedy of the commons after 50 years," *Journal of Economic Perspectives*, vol. 33, no. 4, pp. 211–28, 2019.

[29] E. Ostrom, "Governing the commons: the evolution of institutions for collective action," 1990.

[30] E. Ostrom, *Understanding institutional diversity*. Princeton university press, 2009.

[31] M. Cox, G. Arnold, and S. V. Tomás, "A review of design principles for community-based natural resource management," *Ecology and Society*, vol. 15, no. 4, 2010.

[32] J. Potts, "Governing the innovation commons," *Journal of Institutional Economics*, vol. 14, no. 6, pp. 1025–1047, 2018.

[33] C. Harris, "Institutional solutions to free-riding in peer-to-peer networks: a case study of online pirate communities," *Journal of Institutional Economics*, vol. 14, no. 5, pp. 901–924, 2018.

[34] M. R. Williams and J. C. Hall, "Hackerspaces: a case study in the creation and management of a common pool resource," *Journal of Institutional Economics*, vol. 11, no. 4, pp. 769–781, 2015.

[35] T. Dietz, E. Ostrom, and P. C. Stern, "The struggle to govern the commons," *science*, vol. 302, no. 5652, pp. 1907–1912, 2003.

[36] R. Safner, "Institutional entrepreneurship, wikipedia, and the opportunity of the commons," *Journal of Institutional Economics*, vol. 12, no. 4, pp. 743–771, 2016.

[37] P. Bustamante, M. Gomez, M. B. Weiss, T. Znati, J.-M. J. Park, D. Das, and J. S. Rose, "Agent-based modelling approach for developing enforcement mechanisms in spectrum sharing scenarios: An application for the 1695-1710mhz band," *Telecommunications and Policy Research Conference*, 2018.

[38] M. B. Weiss, W. H. Lehr, A. Acker, and M. M. Gomez, "Socio-technical considerations for spectrum access system (sas) design," in *Dynamic Spectrum Access Networks (DySPAN), 2015 IEEE International Symposium on*, pp. 35–46, IEEE, 2015.

[39] C. Henrich-Franke, "Property rights on a cold war battlefield: managing broadcasting transmissions through the iron curtain," *International Journal of the Commons*, vol. 5, no. 1, 2011.

[40] C. A. Herter, "The electromagnetic spectrum: A critical natural resource," *Natural Resources Journal*, vol. 25, no. 3, pp. 651–663, 1985.

[41] D. L. Bazelon, "Fcc regulation of the telecommunications press," *Duke LJ*, p. 213, 1975.

[42] M. Matinmikko, M. Mustonen, D. Roberson, J. Paavola, M. Höyhtyä, S. Yrjölä, and J. Röning, "Overview and comparison of recent spectrum sharing approaches in regulation and research: From opportunistic unlicensed access towards licensed shared access," in *2014 IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN)*, pp. 92–102, IEEE, 2014.

[43] P. T. Leeson, "Efficient anarchy," *Public Choice*, vol. 130, no. 1-2, 2006.

[44] P. T. Leeson, "Anarchy, monopoly, and predation," *Journal of Institutional and Theoretical Economics (JITE)/Zeitschrift für die gesamte Staatswissenschaft*, pp. 467–482, 2007.

[45] P. J. Boettke and C. J. Coyne, "Methodological individualism, spontaneous order and the research program of the workshop in political theory and policy analysis," *Journal of Economic Behavior & Organization*, vol. 57, no. 2, pp. 145–158, 2005.

[46] F. A. Hayek, *Law, legislation and liberty: a new statement of the liberal principles of justice and political economy*. Routledge, 2012.

[47] A. Borshchev and A. Filippov, "From system dynamics and discrete event to practical agent based modeling: reasons, techniques, tools," in *Proceedings of the 22nd international conference of the system dynamics society*, vol. 22, Citeseer, 2004.

[48] D. C. North, "Institutions," *Journal of economic perspectives*, vol. 5, no. 1, pp. 97–112, 1991.

[49] P. T. Leeson, "Pirates, prisoners, and preliterates: anarchic context and the private enforcement of law," *European Journal of Law and Economics*, vol. 37, no. 3, pp. 365–379, 2014.
[50] K. M. Bloomquist, "Multi-agent based simulation of the deterrent effects of taxpayer audits," in *Proceedings. Annual Conference on Taxation and Minutes of the Annual Meeting of the National Tax Association*, vol. 97, pp. 159–173, JSTOR, 2004.
[51] L. Mittone and P. Patelli, "Imitative behaviour in tax evasion," in *Economic simulations in swarm: Agent-based modelling and object oriented programming*, pp. 133–158, Springer, 2000.
[52] J. S. Davis, G. Hecht, and J. D. Perkins, "Social behaviors, enforcement, and tax compliance dynamics," *The Accounting Review*, vol. 78, no. 1, pp. 39–69, 2003.
[53] M. G. Allingham and A. Sandmo, "Income tax evasion: A," 1972.
[54] M. B. Weiss, M. Altamimi, and M. McHenry, "Enforcement and spectrum sharing: A case study of the 1695–1710 mhz band," in *8th International Conference on Cognitive Radio Oriented Wireless Networks*, pp. 7–12, IEEE, 2013.
[55] D. Das, T. Znati, M. B. H. Weiss, M. M. Gomez, P. Bustamante, and J. S. Rose, "Matchmaking of volunteers and channels for dynamic spectrum access enforcement," in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, pp. 1–6, 2020.
[56] D. Das, J. S. Rose, T. Znati, P. Bustamante, M. Weiss, and M. M. Gomez, "Spectrum misuse detection in cooperative wireless networks," in *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1–6, IEEE, 2020.
[57] D. Das, T. Znati, M. Weiss, P. Bustamante, M. M. Gomez, and J. S. Rose, "Crowdsourced misuse detection in dynamic spectrum sharing wireless networks," in *International Conference on Networks (ICN)*, pp. 74–81, 2019.
[58] D. Das, T. Znati, M. Weiss, P. Bustamante, M. M. Gomez, and J. S. Rose, "Misuse detection in dynamic spectrum sharing wireless networks across multiple channels," *International Journal on Advances in Networks and Services, issn 1942-2644, Volume 12, Number 3 & 4,*, pp. 58–68, 2019. http://www.iariajournals.org/networks_and_services/.
[59] Q. Du, M. Emelianenko, and L. Ju, "Convergence of the lloyd algorithm for computing centroidal voronoi tessellations," *SIAM journal on numerical analysis*, vol. 44, no. 1, pp. 102–119, 2006.
[60] B. Talukder, K. W Hipel, G. W vanLoon, *et al.*, "Developing composite indicators for agricultural sustainability assessment: Effect of normalization and aggregation techniques," *Resources*, vol. 6, no. 4, p. 66, 2017.
[61] R. Kleinberg, "A multiple-choice secretary algorithm with applications to online auctions," in *Proceedings of the Sixteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '05, (USA), p. 630–631, Society for Industrial and Applied Mathematics, 2005.
[62] M. Babaioff, N. Immorlica, D. Kempe, and R. Kleinberg, "Online auctions and generalized secretary problems," *SIGecom Exch.*, vol. 7, June 2008.
[63] D. Gale and L. Shapley, "College admissions and the stability of marriage.," *The American Mathematical Monthly 69, no. 1*, pp. 9–15, 1962.