Crowdsourced Misuse Detection in Dynamic Spectrum Sharing Wireless Networks

Debarun Das
School of Computing and Information
University of Pittsburgh
Pittsburgh, USA
ded59@pitt.edu

Taieb Znati
School of Computing and Information
University of Pittsburgh
Pittsburgh, USA
znati@pitt.edu

Martin Weiss
School of Computing and Information
University of Pittsburgh
Pittsburgh, USA
mbw@pitt.edu

Pedro Bustamante
School of Computing and Information
University of Pittsburgh
Pittsburgh, USA
pjb63@pitt.edu

Marcela M. Gomez
School of Computing and Information
University of Pittsburgh
Pittsburgh, USA
mmg62@pitt.edu

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

***Abstract*— To address the scarcity of spectrum, FCC mandated the dynamic sharing of spectrum among the different tiers of users. The success of spectrum sharing, however, relies on the automated enforcement of spectrum policies. We focus on ex post spectrum enforcement during/after the occurrence of a potentially harmful event, but before/after an actual harm has occurred. The major challenges addressed by us are to ensure maximum channel coverage in a given region of enforcement, accurate and reliable detection of enforcement, and selection of an efficient algorithm to select entities for detection of violation. We adopt a crowdsourced methodology to monitor spectrum usage. We ensure maximum coverage of the given area by dividing it into equal-sized regions and solve the enforcement problem by a divide and conquer mechanism over the entire region. We use a variant of the Multiple Choice Secretary algorithm to select volunteers. We finally simulate the enforcement framework and analyze the results. [Will modify the abstract at the end]**

Keywords- volunteers; sentinels; ex post enforcement; crowdsourced monitoring; volunteer selection

I. INTRODUCTION

With the exponential increase in use of wireless services, the demand for additional spectrum is steadily on the rise. In order to address this potential spectrum scarcity problem, the Federal Communications Commission (FCC) proposed dynamic spectrum access (DSA), wherein licensed frequency bands when idle, are utilized by unlicensed users. In April 2015, the FCC adopted a three-tiered spectrum sharing infrastructure that is administered and enforced by SAS [1]. This architecture consists of Incumbents in tier 1, Priority Access Licensed (PAL) devices in tier 2 and General Authorized Access (GAA) devices in tier 3. Incumbents, in general, include military radars, fixed satellite service Earth stations and several of the Wireless Broadband Services (3650 – 3700 MHz) [2]. The SAS ensures that the spectrum is always available to the incumbent users when and where needed. The next level of access is provided to the users who buy PAL for a given location and period of time (usually for a three-year term). Some example use-cases of PAL include QoS-Managed enterprise networks and utility networks. The remaining spectrum can then be used by devices having GAA. These devices have no protection from interference. They must, however, protect incumbents and PALs, while accessing spectrum. Some example use-cases of GAA include personal and business hotspots, and Campus Hotspots [2].

As spectrum sharing becomes more intense and more granular with more stakeholders, we can expect an increasing number of potentially enforceable events. Thus, the success of spectrum sharing systems is dependent on our ability to automate their enforcement. The three key aspects of any enforcement regime are: the timing of enforcement action, the form of enforcement sanction and whether the enforcement action is private or public [3]. This paper focuses on detection of spectrum misuse. Thus, the key aspect of enforcement action for our consideration, is the timing of enforcement. Timing of an enforcement can be either ex ante (before a potentially "harmful" action has occurred) or ex post (after a potentially "harmful" action has occurred, but potentially before or after an actual "harm" has been done) [4]. The *ex ante* and *ex post* enforcement effects are inextricably linked. For example, if the *ex ante* rules and processes are sufficiently strong then *ex post* harms may be prevented before they occur. Also, certain types of *ex ante* rules may be easier to monitor and hence lower the cost of enforcement. Even strong *ex ante* rules may require *ex post* enforcement; for example, licensing approval for equipment is usually based on a prototype or pre-production unit, but compliance of production units may require some kind of policing to ensure compliance. Till date, more significance has been given on automating *ex ante* enforcement of usage rights. As an example, the TV White Spaces database systems essentially work by preventing users with subordinate rights from using spectrum when and where other users with superior rights are operating [5, 6]. This concept has been extended in the new Citizens Broadband Radio Service (CBRS) to a Spectrum Access System (SAS) that is designed

to distinguish the three classes of user types discussed previously [7].

We observe that both SAS and CBRS have well-developed mechanisms to avoid interference but provide no support for addressing interference when it occurs. We also note that these systems require that radios have an access channel available to them. This may artificially limit the granularity of control as well as their ability to function in circumstances where access to the central database is limited. As we consider *ex post* enforcement approaches, the need to detect enforceable events, gather information about these events (i.e. forensic information about the event such as who, where, when and what) and adjudicate claims based on rules and evidence becomes important. Broadly, enforceable interference events might be subdivided into Type 1 events due to the routine operation of participants in a sharing ecosystem; Type 2 events due to "rogue" or malicious users; and Type 3 events due to faulty equipment of authorized spectrum users.

In this paper, we focus on Type 2 events, i.e. on the detection of an interference event, or RF signal energy that is caused by a malicious user. The primary challenge is to ensure efficient *ex post* spectrum enforcement. In order to address this challenge, this paper proposes an enforcement framework that aims to achieve a) maximum coverage of the entire region of enforcement, b) that the detection of an event of violation is accurate, reliable and feasible, c) use of an effective method for hiring and deploying detecting agents. Contrary to formerly proposed spectrum monitoring approaches, which rely exclusively either on large deployment of physical monitoring infrastructure [4, 8, 9, 10] or on crowdsourcing, we believe that spectrum misuse and access rights violations can be effectively prevented using a trusted infrastructure, composed of a minimal number dedicated devices with advanced trust and authentication capabilities, augmented with an opportunistic infrastructure of peer wireless devices with various software and hardware capabilities [11, 12, 13]. Thus, by employing a hybrid infrastructure of crowdsourced and fixed, stationary resources, we aim to ensure "optimal" detection of spectrum access violation in Dynamic Spectrum Sharing Wireless networks. The major contributions of this paper are:

a) *Region Coverage*: We explore algorithms to organize the area into smaller sized "regions" in order to ensure more manageable detection of violation.
b) *Crowdsourced Detection*: We explore a mechanism to select crowdsourced detecting agents (called volunteers) for ensuring that a spectrum violation is detected with high probability of accuracy and efficiency.
c) *Volunteer Selection*: We develop a framework to assess the "utility" of a volunteer across multiple dimensions, including device capability, location likelihood, and reliability to ensure "optimal" Quality of Enforcement (QoE). In addition, we explore ways to select volunteers such that there is maximum coverage of channels in a given region.

The paper is organized in the following manner. Section 2 of the paper discusses the relevant works that have been done in this area. Section 3 discusses about the enforcement framework that we utilize for our work. Section 4 discusses about the experimental setup and the methods to analyze the results. We finally discuss the results of the experiments in Section 5.

II. ENFORCEMENT FRAMEWORK

The main challenge in the design of a hybrid infrastructure stems from the fact that it is not easy to determine where and how these resources are to be mobilized, given the non-deterministic nature of mobile devices' behavior. It is equally difficult to determine how collaboration between these devices must take place to ensure swift detection and response to spectrum misuse and access rights violation. To address this, we broadly follow a sentinel-based monitoring infrastructure.

Considerations of spectrum monitoring in heterogeneous networks suggest that dealing effectively with spectrum monitoring requires the strategic deployment of a hierarchical, dynamically-evolving infrastructure of nodes, with various capabilities, to detect spectrum misuse and access violation, causing sudden decrease of an authorized user's throughput. Nodes in this architecture can be classified into three categories, namely primary sentinels (PSs), secondary sentinels (SSs), and peer sentinels (PeSs, also known as volunteers). PSs and SSs are usually fixed monitoring nodes, deployed by governmental and law enforcement agencies. The dynamic, hierarchical nature of the proposed infrastructure allows it to evolve in response to an increase in the likelihood of non-compliance and access rights violation. When no excessive misuse is detected, the sentinels' network is reduced to a set of active PSs, whose role is to monitor continuously the spectrum for misuse. SSs roles in this scenario is to probabilistically monitor the spectrum over specific intervals of time. The volunteers remain passive and dedicated entirely to supporting their main functions and application. When the likelihood of a misuse is detected, PSs use, potentially secure and authenticated communication channels, to seek reinforcement by asking SSs to increase their SSs' monitoring frequency and possibly activating additional volunteers within the location where misuse is suspected.

Since PSs and SSs are generally static in nature, it requires deployment of these entities in higher numbers, to avoid false positive detection results. The cost of deployment and maintenance of additional static infrastructures can be too high for practical purposes. Moreover, the communication overhead between these coordinating static entities for localizing would be higher than desired [13]. Therefore, in this paper, we focus on the selection of volunteers to collaboratively monitor radio access behavior within their neighborhood and detect anomalous use of spectrum.

A. Primary Infrastructure

The trustworthy, stationary infrastructure, consisting of PSs and SSs is referred to as Primary Infrastructure entity, PI_r, associated with region $r \in R$. A PI_r maintains a database DB_r of all volunteers registered in r, a unit S_r for selection of volunteers and a unit that acts as a Master Node M_r for taking requests from transmitters to access any free channel in r. The volunteers of a region r reports a spectrum access violation to its PI_r. The PI_r also communicates with a Central Database DB_R, which maintains a channel-user occupancy list for the entire set of regions R. The PI_r verifies the veracity of a violation report by communicating and verifying with DB_R if the assumed violator is authorized to use the violated channel or not.

B. Crowdsourced Infrastructure

The crowdsourced infrastructure consists of mobile entities that can monitor radio access behavior within their neighborhood and detect anomalous use of spectrum. Monitoring is used to obtain detailed information on the technical and operational characteristics of the radio systems, including frequency, power and transmitter emission spectrum. To carry out spectrum monitoring practices, volunteers incur transmit power consumption cost and bandwidth consumption cost. A volunteer $v \epsilon V$ registers in the local DB_r of the region r that it currently monitors. The volunteer v reports its location and detection result to the PI_r after a fixed interval of time. Based on the received parameters from v, the PI_r calculates the volunteer's qualification, which it uses to select a future set of volunteers for coverage in r.

C. Transmitters

We broadly classify the users of spectrum frequencies into authorized and malicious transmitters. Authorized transmitters consist of incumbents and legitimate secondary users (SUs). Authorized SUs send a spectrum access request to the local PI_r, whenever they need access to a channel. The Master Node unit M_r of PI_r receives the spectrum access request and refers to the central database DB_R to allocate an unoccupied channel to the requesting user. The malicious transmitters use spectrum frequencies without permission from the local PI_r. They intend to illegitimately use channels for communication that have not been officially allocated to them by a PI_r.

The System model consisting of the Primary Infrastructure, the crowdsourced infrastructure, transmitters and the centralized DB_R, is shown in Figure 1. The volunteers of the crowdsourced infrastructure are selected by the local PI_r to detect spectrum usage by malicious users. The detection results are reported back to the PI_r, who verifies it with the help of the data contained in DB_R.

D. Coverage of Region

To ensure maximum coverage of an area R for enforcement, we follow a divide and conquer method to solve

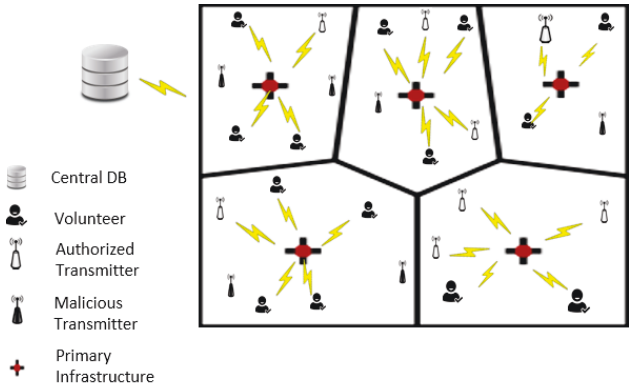

Figure 1: System Model

this. We propose to divide the entire area R into smaller regions. We then focus on solving the enforcement problem for a single region $r \in R$, which in turn can be used for solving the problem for the whole R. For division of R into regions, we employ the Voronoi algorithm [15]. Initially, we assume that the volunteers in V are randomly distributed over R and the primary infrastructures are spread uniformly over R. For each volunteer $v \in V$, its corresponding Voronoi region r consists of every volunteer in the Euclidean plane whose distance to the local PI_r is less than or equal to its distance to any other PI_r[15]. However, the Voronoi algorithm may not produce regions that are of equal size. This is a disadvantage because it may result in some of the regions to have an undersupply of volunteers over time, which in turn may result in possible loss in detection of spectrum violation. Thus, we apply the Lloyd's Algorithm, which is a relaxation of the Voronoi algorithm [16]. This produces uniformly sized convex regions, and thus improves the probability of a fair distribution of volunteers over all regions. The number of regions in R is equal to the number of primary infrastructures in R. We associate a PI_r to every $r \in R$, which in turn is responsible for selecting qualified volunteers in r.

III. CROWDSOURCED DETECTION

As discussed previously, the volunteers in a region r are responsible for detecting violation of spectrum policies. A volunteer $v \in V$ is associated with the following parameters: Serial Number of the sensing device S_v used by v and its location $L_{v,t}$ at time t. While S_v can be used to uniquely identify a volunteer, the location $L_{v,t}$ allows the selection unit S_r of a PI_r to estimate whether v will be available to monitor the channel c_r in r in the future.

As shown in Figure 2, we divide the total enforcement time into a set of intervals called the monitoring interval, MI. Each MI is further divided into a set of n sub-intervals called the Access Unit Intervals (AUIs). One AUI is defined as the smallest interval over which a user, intruder or legitimate, can accomplish *useful* work. It is used as the interference monitoring interval by the selected volunteers to determine

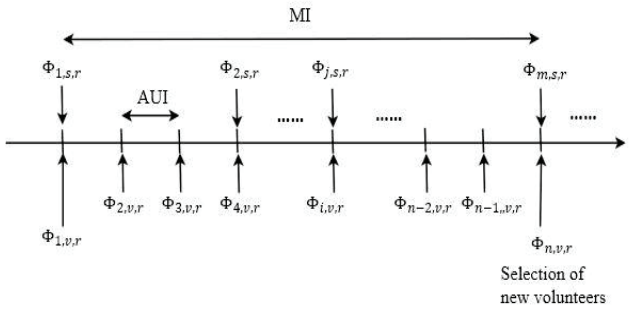

Figure 2: Observations $\Phi_{i,v,r}$ by volunteer v after every AUI and $\Phi_{j,s,r}$ by sentinel s after random AUIs, for the 1st MI

access violation or legitimacy. A new set of volunteers is selected at the end of every MI by the selection unit S_r of the PI_r of region r. Volunteer selection in r is based upon twofold parameters of trust and location likelihood of a v in r.

A. Trust

The trust of a volunteer v is determined by its past *behavior*. The *behavior* of a volunteer v is chiefly determined by its accuracy in detection of spectrum violation. At the end of every AUI i, a volunteer v reports the observed state $\Phi_{i,v,r}$ of a channel c_r that it monitors, over i. The state of a channel can be either a) *idle*, when no user, authorized or malicious, uses c_r, b) *safe*, when $c_r$is used by an authorized transmitter, or c) *violated*, when c_r is used by a malicious transmitter. The necessary ground truth required for calculating accuracy of interference detection by v in r is acquired from the observed state $\Phi_{j,s,r}$ of c_r by a sentinel s that monitors c_r at an AUI j. A sentinel s is a trustworthy agent who helps in verifying volunteer detection result and helps to identify unreliable volunteers. As shown in Figure 2, a sentinel s monitors c_r in r at a random interval j,which is known only to the PI_r. This helps us to calculate the *behavior* $b_{i,v,r}$ of v in r at AUI i by using equation (1) given below.

$$b_{i,v,r} = \begin{cases} 1, & \Phi_{i,v,r} = \Phi_{j,s,r} \\ 0, & \Phi_{i,v,r} \neq \Phi_{j,s,r} \end{cases}, \forall i = j \qquad (1)$$

As shown in equation (1), the behavior of a volunteer $b_{i,v,r}$ at i in r is assigned to zero when there is a mismatch in the observed state of c_r, between v and s.This can be because a) v makes a false detection, b) v lies about the true result, or c) s makes a false detection, d) s lies about the true result. However, for this paper, we assume that s is trustworthy and never makes a false detection or lies about a true result. An AUI when both v and s monitor channel c_r is called a matching interval. So, we aggregate $b_{i,v,r}$ over all the matching AUIs when both v and s monitor c_r to find the trust $T_{v,r}$ of v in r, by calculating the arithmetic mean $T_{v,r}$, given by equation (2),

$$T_{v,r} = \frac{1}{m}\sum_{p=1}^{m} b_{p,v,r} \qquad (2)$$

where p is a matching interval and m is the total number of matching intervals over all the monitoring intervals.

B. Location Likelihood

In order to efficiently support detection of channel violation in a region r, volunteers who are most likely to reside a major proportion of time in r after a visit to r, must be given preference. For this purpose, the PI_r estimates the fraction of time that a volunteer v stays in r after its current visit to r. As shown in Figure 3, after the $(j)^{th}$ visit of v to r, we measure its $(j-1)^{th}$ *sojourn time*, $S_{j-1,v,r}$, in r as the difference between its $(j-1)^{th}$ departure time, $dep_{j-1,v,r}$ from r and its $(j-1)^{th}$ arrival time, $arr_{j-1,v,r}$ in r. Furthermore, we calculate the $(j-1)^{th}$ *return time* of v in r, $R_{j-1,v,r}$, as the difference between $arr_{j,v,r}$ and $arr_{j-1,v,r}$. As given by equation (3), this enables us to calculate the proportion of time, $P_{j-1,v,r}$, that v resided in r on its previous $((j-1)^{th})$ visit to r, as the ratio of $S_{j-1,v,r}$ and $R_{j-1,v,r}$. Based on this information, the PI_r estimates the proportion of time that v is likely to stay in r before its j^{th} departure from r, as an exponentially smoothed average, given by equation (4).

$$P_{j-1,v,r} = \frac{S_{j-1,v,r}}{R_{j-1,v,r}} \qquad (3)$$

$$\tilde{P}_{j,v,r} = \alpha.P_{j-1,v,r} + (1-\alpha).\tilde{P}_{j-1,v,r}. \qquad (4)$$

In order to estimate the smoothed average, $\tilde{P}_{j,v,r}$ more accurately, smoothing factor α is computed as:

$$\alpha = c\frac{E_{j-1,v,r}^2}{\sigma_{j,v,r}}. \qquad (5)$$

where $0 < c < 1$, $E_{j-1,v,r} = P_{j-1,v,r} - \tilde{P}_{j-1,v,r}$ is the prediction error, and $\sigma_{j,v,r}$ is the average of the past square prediction errors on visit j. $\sigma_{j,v,r}$ can be expressed as follows:

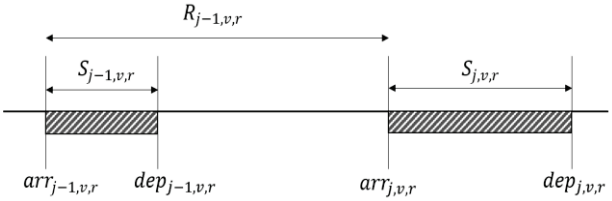

Figure 3: Sojourn time $S_{j,v,r}$ and Return time $R_{j,v,r}$ of volunteer v after its j^{th} visit to region r

$$\sigma_{j,v,r} = \mathrm{c}.E^2_{j-1,v,r} + (1 - \mathrm{c}).\sigma_{j-1,v,r}. \quad (6)$$

Moreover, at any given time t, the location $L_{v,t}$ of volunteer v enables us to estimate the likelihood of v to stay in r over the next monitoring interval, MI, based on the assumption that the likelihood of v to stay in r decreases as the displacement between $L_{v,t}$ and the centroid O_r of region r increases. This is expressed by the *separation factor*, $\Upsilon_{j,v,r}$, given by equation (7) as follows:

$$\Upsilon_{t,v,r} = \gamma_1 \mathrm{e}^{-\gamma_2 \mathrm{d}(L_{v,t}, O_r)}. \quad (7)$$

where $0 < \gamma_1, \gamma_2 < 1$, are parameters defined by the system and $\mathrm{d}(L_{v,t}, O_r)$ is the displacement between $L_{v,t}$and O_r.

Hence, the location likelihood, $L_{v,r}(MI)$ of v in r at time t over the next MI, is given by a function f of the parameters, $\tilde{P}_{j,v,r}$ of the latest (j^{th}) visit of v in r and $\Upsilon_{t,v,r}$,. Since $R_{j-1,v,r} > S_{j-1,v,r}$ and $0 < \alpha < 1$, so $0 < \tilde{P}_{j,v,r} < 1$. Similarly, since $\mathrm{d}(L_{v,t}, O_r) \geq 0$, so $0 < \Upsilon_{t,v,r} \leq 1$. Therefore, we do not require to normalize the two parameters $\tilde{P}_{j,v,r}$ and $\Upsilon_{j,v,r}$. Since weighting the parameters by linear regression requires large amount of data and preferential weighting is hard to establish as it usually requires an expert opinion on the importance of an individual parameter relative to the overall composite parameter [17], so we assign equal weights to the parameters $\tilde{P}_{j,v,r}$ and $\Upsilon_{t,v,r}$. Finally, we define function f as the product of parameters $\tilde{P}_{j,v,r}$ and $\Upsilon_{j,v,r}$ as given by equation (8) below.

$$L_{v,r}(MI) = \tilde{P}_{j,v,r} \times \Upsilon_{j,v,r} \quad (8)$$

C. Selection of volunteers

From the set of volunteers, V, in total area of enforcement, R, a PI_r in region r selects k_r qualified volunteers to monitor r at the beginning of every MI. This is determined by the estimated *Qualification* $Q_{v,r}(MI)$ of a volunteer v to monitor the associated channel in r over the next MI, given by equation (9), defined below.

$$Q_{v,r}(MI) = g(T_{v,r}, L_{v,r}(MI)) \quad (9)$$

As shown in equation (9), $Qualification\ Q_{v,r}(MI)$ of a v in r is given as a function g of its location likelihood $L_{v,r}(MI)$, over the next MI, and trust $T_{v,r}$. Since both $0 < L_{v,r}(MI) \leq 1$ and $0 < T_{v,r} \leq 1$, so we do not normalize $L_{v,r}(MI)$ and $T_{v,r}$. We apply equal weighting to the two parameters since the other two widely used weighting methods [17] of linear regression and preferential weighting are cumbersome due to the requirement of large amount of data and of expert opinion on preference, respectively. We aggregate $L_{v,r}(MI)$ and $T_{v,r}$ in function g, using a) multiplication, b) addition and c) geometric mean.

For this paper, we assume that every region $r \epsilon R$ has a single channel c_r associated with it. So, a v monitoring r will detect spectrum access violation in c_r associated with r. Furthermore, we assume that more than one region can hire a volunteer v over the next MI as v is mobile and can potentially cover multiple regions over a given MI. The PI_r associated with r has access to a centralized $||V||$-by-$||R||$ matrix $\Psi_{V,R}$, which is a volunteer-region qualification matrix that contains the qualification values $Q_{v,r}(MI)$ of all $v \in V$ for all $r \in R$. A PI_r selects k_r volunteers from V based on the qualification values of $v \in V$ for r, using Algorithm S.

For the volunteer selection algorithm S, we use the volunteer-region qualification matrix $\Psi_{V,R}$ to select qualified volunteers for every $r \in R$. At the end of a MI (line 3), a region r gains access to the qualification values of all $v \in V$ for r from $\Psi_{V,R}$ and stores them in a list Q_r. If the number of volunteers to be selected in r, k_r is 1, then we use the classic secretary algorithm [18] to select the most qualified volunteer dynamically. In a classic secretary algorithm, we observe the first $||Q_r||/2$ qualification values to determine a threshold and then select the first of the next $||Q_r||/2$ volunteers, whose qualification value is above the threshold [19]. However, if $k_r > 1$, we select volunteers dynamically using a multiple-choice secretary algorithm, which proceeds as follows. We draw a random sample m_r from a binomial distribution $Binomial(||Q_r||, \frac{1}{2})$, from which we select up to $\lfloor k_r/2 \rfloor$ volunteers recursively (lines 8-10). We keep appending the selected volunteers in set $V_{S,r}$. If m_r is greater than $\lfloor k_r/2 \rfloor$, then we set l_r to $\lfloor k_r/2 \rfloor$, otherwise we set l_r to m_r. Next, we set a $threshold$, which is the l_r^{th} largest qualification value in the sample of m_r qualification values. After this, we select every volunteer with qualification values greater than $threshold$, till we select a maximum of k_r volunteers (lines 13-17) [19]. We apply this algorithm for selection of volunteers in every $r \in R$.

```
Algorithm S: Volunteer Selection
 1: Maintain matrix Ψ_{V,R} that stores
 qualification values ∀v ∈ V,∀r ∈ R, List of
 selected volunteers V_{S,r} ∀r ∈ R
 2: for all r ∈ R do
 3:  if t = MI then
 4:   Q_r ← Ψ_{V,R}[r]
 5:   if k_r = 1 then
 6:    Run Classic Secretary Algorithm
 7:   else
 8:    m_r ← Binom(||Q_r||, 1/2)
 9:    l_r ← ⌊k_r/2⌋
10:   Recursively select up to l_r volunteers
11:   B_r ← descending_sort(Q_r[1], …, Q_r[m_r])
12:   threshold ← B_r[l_r]
13:   for i = m_r + 1, … , ||Q_r|| do
14:    if Q_r[i] > threshold and ||V_{S,r}|| < k_r then
```

```
15:      V_{S,r} ← V_{S,r} ∪ v
16:    else
17:     Reject v
18:    end if
19:   end for
20:  end if
21: end if
22:end for
```

IV. Results

V. Conclusion

Acknowledgment

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g”. Avoid the stilted expression, “One of us (R.B.G.) thanks . . .” Instead, try “R.B.G. thanks”. Put applicable sponsor acknowledgments here; DO NOT place them on the first page of your paper or as a footnote.

References

[1] Federated Wireless. Citizens Broadband Radio Service (CBRS) Shared Spectrum: An Overview. [ONLINE]. Available from http://federatedwireless.com/wp-content/uploads/2017/03/CBRS-Spectrum-Sharing-Overview-v3.pdf

[2] Manuel Uhm, “Paving The Path To Three Tier Spectrum Sharing”, IEEE International Symposium on Dynamic Spectrum Access Networks, March 2017.

[3] Edella Schlager and Elinor Ostrom. “Property-rights regimes and natural resources: A conceptual analysis. Land Economics”, 68(3):249–262, August 1992.

[4] Steven Shavell, “The optimal structure of law enforcement”, Journal of Law and Economics, vol. XXXVI: 255-87, April 1993

[5] Ajay Gopinathan and Zongpeng Li. “Strategyproof auctions for balancing social welfare and fairness in secondary spectrum markets”. In INFOCOM, 2011 Proceedings IEEE, pages 3020–3028. IEEE, 2011

[6] R. Motik and I. Horrocks. HermiT: “A highly-efficient OWL reasoner”. In 5th International Workshop on OWL: Experiences and Directions, 2008.

[7] Joseph Farrell and Matthew Rabin. “The exchange and enforcement of property rights”. 1996

[8] Martin B.H. Weiss, Mohammed Altamaimi, and Mark McHenry. “Enforcement and spectrum sharing: A case study of the 1695-1710 mhz band”. In 8th International Conference on Cognitive Radio Oriented Wireless Networks (CrownCom), July 2013

[9] Dejun Yang, Xiang Zhang, and Guoliang Xue. “Promise: A framework for truthful and profit maximizing spectrum double auctions”. In INFOCOM, 2014 Proceedings IEEE, pages 109–117. IEEE, 2014.

[10] R. Chen, J. M. Park, and J. H. Reed. “Defense against primary user emulation attacks in cognitive radio networks”. IEEE Journal on Selected Areas in Communications (JSAC), 26(1):25– 37, 2008.

[11] Ajay Gopinathan and Zongpeng Li. A prior-free revenue maximizing auction for secondary spectrum access. In INFOCOM, 2011 Proceedings IEEE, pages 86–90. IEEE, 2011.

[12] N. Goergen, S. Lin, K-J-R. Liu, and T.C. Clancy. Extrinsic channel-like fingerprint embedding for authenticating MIMO systems. IEEE Trans. on Wireless Communications, 10(12), 2011.

[13] Aveek Dutta, Mung Chiang, ““See Something, Say Something” Crowdsourced Enforcement of Spectrum Policies”, IEEE Trans. on Wireless Communications, 15(1), 2016

[14] Christian A. Herter. The electromagnetic spectrum: A critical natural resource. Natural Resources Journal, 25:651–663, July 1985.

[15] F. Aurenhammer and R. Klein. Voronoi diagrams. In J.-R. Sack and J. Urrutia, editors, Handbook of Computational Geometry, page ?? Elsevier Science Publishers B.V. North-Holland, Amsterdam, 1998.

[16] Qiang Du, Maria Emelianenko, Lili Ju, “Convergence of the Lloyd Algorithm for Computing Centroidal Voronoi Tessellations”, Siam J. Numer. Anal., 44(1), pages 102-119, 2006

[17] Byomkesh Talukder, Keith W. Hipel, Gary W. vanLoon, “Developing Composite Indicators for Agricultural Sustainability Assessment: Effect of Normalization and Aggregation Techniques”, Resources, 6(4), 2017

[18] Gautam Kamath, “Advanced Algorithms, Matroid Secretary Problems”.[ONLINE]. Available from: http://www.gautamkamath.com/writings/matroidsec.pdf

[19] Robert Kleinberg, “A Multiple-Choice Secretary Algorithm with Applications to Online Auctions”, Proceedings of the Sixteenth Annual ACM-SIAM Symposium on Discrete Algorithms, pages 630-631, 2005

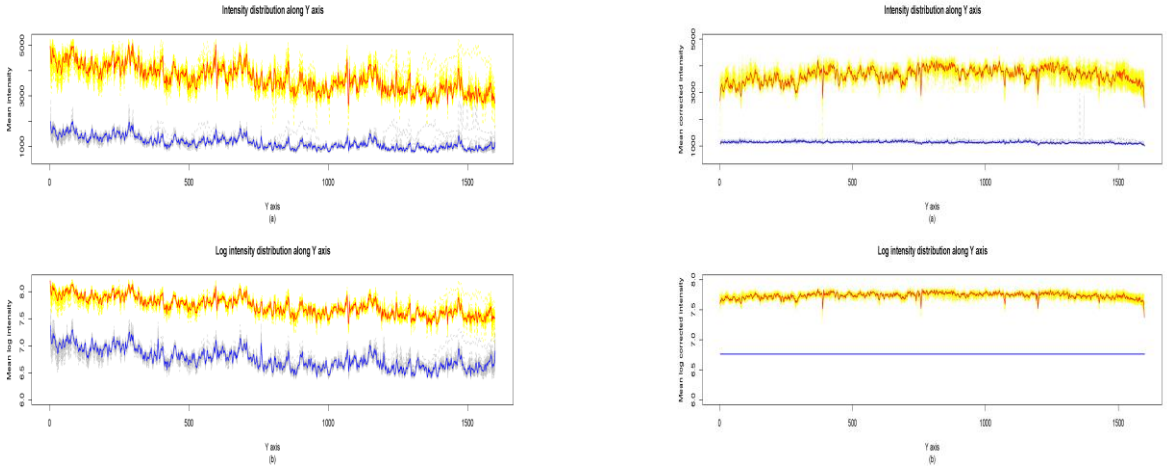

Figure 1. Example of a TWO-COLUMN figure caption: (a) this is the format for referencing parts of a figure.