Spectrum Misuse Detection in Cooperative Wireless Networks

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

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

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

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

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

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

Abstract— **Cooperative wireless networks, enabled by Cognitive Radios, facilitate mobile users to dynamically share access to spectrum. However, spectrum bands can be accessed illegitimately by malicious users. Therefore, the success of dynamic spectrum sharing relies on automated enforcement of spectrum policies. While the focus has been on ex ante spectrum enforcement, this work explores new approaches to address efficient ex post spectrum enforcement. The main objective of this work is to ensure maximum coverage of the area of enforcement and accurate detection of spectrum access violation. The first objective is achieved with the help of Lloyd's algorithm to divide the enforcement area into a set of uniformly sized coverage regions. The interference detection accuracy is achieved through crowdsourcing of the spectrum access monitoring to volunteers, based on their computational capabilities, location attributes and reputation. A simulation framework was developed in CSIM19 (C++ version) to analyze the performance of the proposed system over the entire area of enforcement. The results show that the proposed scheme ensures efficient coverage of all the channels and regions in the area of enforcement and a high average accuracy of detection.**

Keywords—cooperative wireless networks, volunteer, sentinel, reputation, ex post enforcement, crowdsourced spectrum monitoring, volunteer selection.

I. Introduction

As the use of wireless services increases exponentially, the demand for additional spectrum is steadily on the rise. In order to address spectrum scarcity, the Federal Communications Commission (FCC) proposed Dynamic Spectrum Access (DSA), wherein unlicensed users use idle licensed frequency bands. FCC adopted a three-tiered spectrum sharing infrastructure that is administered and enforced by Spectrum Access System (SAS) [1]. This architecture consists of Incumbents in tier 1, followed by Priority Access Licensed (PAL) devices in tier 2 and General Authorized Access (GAA) devices in tier 3. While it is ensured that the spectrum is always available to the incumbent users when and where needed, the next level of access is provided opportunistically to PAL and GAA devices. [2].

Cooperative wireless networks that are empowered by cognitive radios, allow users which are on the move with speeds ranging from the speed of walking to the speed of moving in vehicles, to dynamically share access to spectrum. These networks are however plagued by the possibility of malicious users illegitimately accessing spectrum bands. Thus, the success of spectrum sharing systems is dependent on our ability to automate their enforcement. The key aspect of enforcement 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) [3][4]. Ex ante and ex post enforcement effects are inextricably linked. For example, if ex ante rules are sufficiently strong then ex post harms may be prevented before they occur. However, 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. Till date, more significance has been given on automating ex ante enforcement of usage rights. For 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]. This concept has been extended in the new Citizens Broadband Radio Service (CBRS) to a SAS that is designed to distinguish the three classes of user types discussed previously [2].

We observe that both SAS and CBRS have well-developed mechanisms to avoid interference but provide no support for addressing interference when it occurs. In this paper, we focus on the detection of an interference event that is caused by a malicious user. The primary challenge is to ensure efficient ex post spectrum enforcement. In order to address this challenge, the paper proposes an enforcement framework that aims to achieve a) maximum coverage of the entire area of enforcement, b) optimal coverage of the channels in the area of enforcement c) accurate detection of spectrum access violations, d) accurate estimation of the qualification of a crowdsourced detecting agent e) use of an effective method for hiring and deploying detecting agents. By employing a hybrid infrastructure of crowdsourced and trusted, dedicated 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) Coverage: We explore mechanisms to aim for both region and channel coverage in the area of enforcement.

b) Accuracy of Crowdsourced Detection: We explore a mechanism to select crowdsourced detecting agents for ensuring that a spectrum violation is detected with high probability of accuracy and efficiency.

The paper is organized in the following manner. Section II of the paper discusses about the related works. Section III and IV of the paper discusses about the enforcement framework and the crowdsourced monitoring methodology, respectively. Section V discusses about the experiments and results. Section VI underlines the conclusion and future scope of this work.

II. Related Works

Jin et al. [20] introduces the first crowdsourced spectrum misuse detection for DSA systems. Dutta and Chiang [13] discusses about crowdsourced spectrum enforcement for accurate detection and location of spectrum enforcement. Salama et al. [22] proposed an optimal channel assignment framework for crowdsourced spectrum monitoring, where volunteers are assigned to monitor channels based on their availability patterns and are awarded with incentives in return. Li et al. [23] models the spectrum misuse problem as a combinatorial multi armed bandit problem to decide which channels to monitor, how long to monitor each channel, and the order in which channels should be monitored. Yang et al. [7] studied two incentive based crowdsourcing models, where a Stackelberg Equilibrium was computed in the platform-centric model, and a truthful auction mechanism was proposed under the user-centric model. [6] takes the Sybil attack into consideration for incentive based crowdsourced spectrum sensing. The works [11] and [12] propose frameworks for crowdsourced spectrum sensing without violating the location privacy of mobile users. Wang et al. [14] and Benedetto et al. [25] discusses a reputation-based framework where malicious users are identified based on data agreement and by statistics of the consecutively true and false decisions respectively. Contrary to the formerly proposed spectrum monitoring approaches, which rely exclusively either on large deployment of physical monitoring infrastructure [8]-[10] or on crowdsourcing, we believe that spectrum access rights violations can be effectively prevented by using a hybrid of trusted infrastructure, composed of a central DSA Enforcement Infrastructure and a minimal number of mobile, wireless devices with advanced trust and authentication capabilities, augmented with an opportunistic infrastructure of wireless devices with various software and hardware capabilities. In addition, contrary to majority of the previous works which have studied the reputation of a secondary user, we focus on modeling the reputation of agents who monitor the behavior of secondary users. Also, while reputation has been majorly modeled to change in a static manner based on the success/failure of a user, we focus on a strategic approach to build reputation over time for ensuring high accuracy of detection. We further explore ways to combine different attributes to estimate the qualification of a crowdsourced agent to monitor multiple channels in a region and select them using a mechanism that ensures high coverage of enforcement area and of channels. This work is an extension of our previous work [26] which is a much simpler model, with simpler, fewer parameters and experiments for spectrum enforcement in only a single channel per region.

III. 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 the 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. To address this, we broadly follow a crowdsourced monitoring infrastructure, supported by sentinel-based monitoring and a central DSA Enforcement Infrastructure.

The entire area of enforcement R is divided into smaller regions, with an Access Point AP_r, associated with every $r \epsilon R$. Authorized users, who are legitimate Secondary Users (SUs) gain access to an available channel through the local AP_r in r. On the contrary, malicious users are unauthorized transmitters who intrude on spectrum by illegitimately using spectrum frequencies in r that they have not been authorized to use by the local AP_r. Some of the authorized users volunteer to monitor a given channel for access violation, in addition to accessing the spectrum to transmit their own data. Such volunteers are mobile agents who can monitor radio access behavior within their neighborhood and detect anomalous use of spectrum. Volunteers are classified as *honest* and *corrupt*. We assume that *honest* volunteers always tell the truth and *corrupt* volunteers tell the truth probabilistically. The system model further consists of a set of sentinels S' who monitor a given channel in r at random intervals to verify the detection results reported by the volunteers and to prevent selection of *corrupt* volunteers.

As shown in Figure 1, the system model further consists of a central DSA Enforcement Infrastructure, which consists of a set of Volunteer Service units VS_r for every $r \in R$, a Volunteer Selection Unit and a DSA Database. A volunteer $v \epsilon V$ in $r \in R$ registers itself to the VS_r associated with r. A VS_r stores and updates volunteer attributes over the entire period of enforcement. The Volunteer Selection Unit uses the latest attributes of all the volunteers in a VS_r to select volunteers for monitoring a given channel in r over the next epoch of enforcement. The DSA Database maintains a channel-user occupancy list, for the entire area of enforcement R. The information contained in the DSA

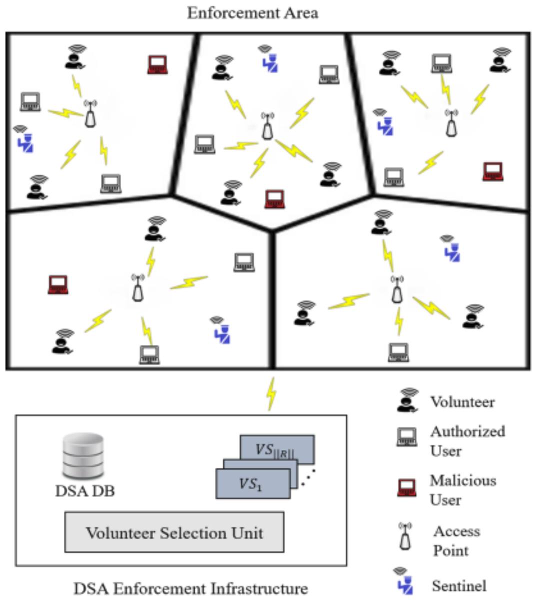

Figure 1. System Model.

Database is used to identify the channels and their respective authorized users in R.

To ensure maximum coverage of an area R for enforcement, we follow a divide and conquer method. We propose to divide the entire area R into smaller regions and then focus on solving the enforcement problem for a single region $r \in R$. This in turn can be used for solving the problem for the whole R. For division of R into regions, we propose the employment of the Voronoi algorithm [15]. Initially, we assume that the volunteers in V are randomly distributed over R and the access points 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 AP_r is less than or equal to its distance to any other AP_r [15]. However, the Voronoi algorithm may not produce regions that are of equal size. This is a disadvantage as it may result in some of the regions to be undersupplied by volunteers over time, which in turn may result in possible loss in detection of spectrum misuse. Thus, we propose to apply a relaxation to the Voronoi algorithm, called the Lloyd's Algorithm [16], which 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 access points in R.

IV. Crowdsourced Spectrum Monitoring

We divide the total enforcement time into a set of intervals called the Monitoring Intervals, MIs. Each MI is further divided into a set of 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 access violation or legitimacy. Each AUI is divided into Sampling Intervals (SIs), over which a sentinel and a volunteer senses a channel to determine its access type. A new set of volunteers is selected at the beginning of every MI by the VS_r of region r. Volunteer selection in r is primarily based upon the parameters of reputation, sojourn time, duration to destination and likelihood of visit, all of which are discussed below.

A. Reputation

As shown in Figure 2, a volunteer v in region r makes an observation $O_{v,r,c}^{i,j}$ of the access state of channel c in every SI j and a sentinel s makes an observation $O_{s,r,c}^{i,k}$ at a random SI k of an AUI i. Based on these observations, both v and s decide the spectrum access state over AUI i. We assume that a volunteer v's decision $\phi_{v,r,c}^{i}$ is accurate if it is the same as the decision $\phi_{s,r,c}^{i}$ of sentinel s. The trustworthiness of a volunteer is determined by its accuracy in detection of spectrum access violation as given by (1).

$$T_{v,r,c} = \sum_{MI} \frac{s_{v,r,c}(MI)}{s_{v,r,c}(MI) + f_{v,r,c}(MI)} \tag{1}$$

where $s_{v,r,c}(MI)$ and $f_{v,r,c}(MI)$ are the number of times that the decisions of v and s matched and didn't match for channel c respectively, over a given MI. A sentinel s decides to monitor c at random AUIs to verify the decisions made by the volunteers. The minimum number of observations η required by a sentinel in an AUI to determine the ground truth of spectrum access state with a margin of error δ at $\beta\%$ confidence level is given by (2).

$$\eta \geq 0.25.\left(\frac{z^*}{\delta}\right)^2 \tag{2}$$

where z^* is the critical value.

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 tenet of our approach is to increase the reputation slowly after success and penalize the reputation rapidly after it falls below a threshold. The 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 region r is given by (3).

$$\Gamma_{v,r,c}^{z,i+1} = \begin{cases} \Gamma_{v,r,c}^{z,i} + f\left(T_{v,r,c}^{z,i}\right), \ if\ accurate \\ \Gamma_{v,r,c}^{z,i} - g\left(T_{v,r,c}^{z,i}\right), \ otherwise \end{cases} \tag{3}$$

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, $f\left(T_{v,r,c}^{z,i}\right) \propto T_{v,r,c}^{z,i}$ and $g\left(T_{v,r,c}^{z,i}\right) \propto e^{\lambda.\,(1-T_{v,r,c}^{z,i})}$, such that λ increases if $\Gamma_{v,r,c}^{z,i} < \theta$, where θ is the threshold below which we decrease reputation more rapidly. So, the reputation is increased linearly when an accurate decision is made by v and decreased exponentially otherwise.

B. Sojourn Time

In order to efficiently support detection of channel access violation in a region r, volunteers who are most likely to reside a major proportion of time in r after a visit to r, are given preference. To this end, we estimate the sojourn time of a volunteer $v \in V$ in $r \in R$ after every visit of v to r. After the $(j)^{th}$ visit of v to r, we measure its $(j-1)^{th}$ sojourn time, $S_v^{j-1}(r)$, in 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. Based on this information, the VS_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 (4).

$$\tilde{S}_v^j(r) = \alpha.S_v^{j-1}(r) + (1-\alpha).\tilde{S}_v^{j-1}(r) \tag{4}$$

In order to estimate the smoothed average, $\tilde{S}_v^j(r)$ more accurately, smoothing factor α is computed as:

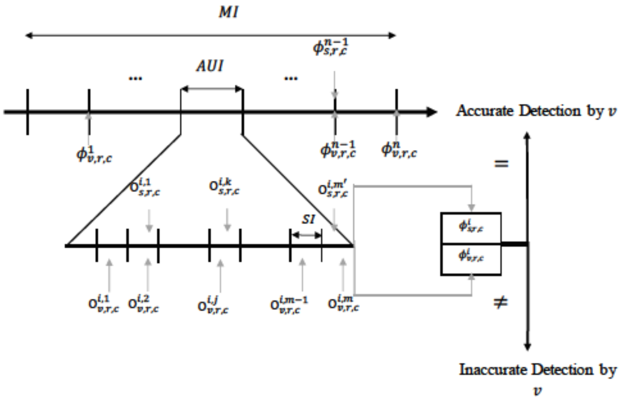

Figure 2. Decisions by volunteer v after every AUI and by sentinel s after random AUIs, for a given MI.

$$\alpha = h.\frac{(E_v^{j-1}(r))^2}{\sigma_v^j(r)} \tag{5}$$

where $0 < h < 1$, $E_v^{j-1}(r) = S_v^{j-1}(r) - \tilde{S}_v^{j-1}(r)$ is the prediction error, and $\sigma_v^j(r)$ is the average of the past square prediction errors on visit j, as shown in (6).

$$\sigma_v^j(r) = h.(E_v^{j-1}(r))^2 + (1 - h).\sigma_v^{j-1}(r) \tag{6}$$

C. Duration To Destination

Volunteers who are likely to reach a region r in shortest time are given preference to monitor r for efficient spectrum access violation detection. At any given 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 (7).

$$\Upsilon_v^t(r) = \frac{\gamma d(L_v^t, O_r)}{\tilde{\mu}_v} \tag{7}$$

where $\gamma > 0$ is a system parameter, $\tilde{\mu}_v$ is average velocity of v, O_r is the centroid of region r and $d(L_v^t, O_r)$ is the shortest distance between L_v^t and O_r.

D. Likelihood of Visit

The Volunteer Selection Unit prefers volunteers who have a high likelihood of visiting and residing in a region r. The likelihood $\rho_v(r)$ of a volunteer v to visit r is given by the fraction of time spent by v in r, as shown in (8).

$$\rho_v(r) = \frac{\tau_v(r)}{\sum_{r \in R} \tau_v(r)} \tag{8}$$

where $\tau_v(r)$ is the time spent by v in region r.

E. Volunteer Selection

The Volunteer Selection Unit selects k_r *qualified* volunteers to monitor region r at the beginning of every MI. This is determined by the estimated Qualification $Q_{v,r,c}(MI)$ of a volunteer v to monitor a channel c in r over the next MI, given by (9), defined below.

$$Q_{v,r,c}(MI) = f(\Gamma_{v,r,c}, \tilde{S}_v^j(r), \Upsilon_v^t(r), \rho_v(r)) \tag{9}$$

Since $\Gamma_{v,r,c}$, $\tilde{S}_v^j(r)$, $\Upsilon_v^t(r)$ and $\rho_v(r)$ represent the measurement of different parameters, we normalize them by using the min-max normalization technique [17] such that $0 \leq \Gamma_{v,r,c}, \tilde{S}_v^j(r), \Upsilon_v^t(r), \rho_v(r) \leq 1$. Clearly, reputation is the most significant component of the selection metric. Untrustworthy volunteers, regardless of their location or likelihood to be in a region, must be eliminated. Furthermore, since a volunteer can only monitor a channel in a region that it resides in over an AUI, the likelihood of visit $\rho_v(r)$ of v in r is next in priority. With this assumption, we explore ways to aggregate the above four parameters in f in order to assess their impact in measuring the qualification of a volunteer as shown in (10)-(13).

$$f_1 = p_0.(\log(1 + p_1).\log(1 + p_2)) \tag{10}$$

$$f_2 = p_0.(\log(1 + p_1) + \log(1 + p_2)) \tag{11}$$

$$f_3 = p_0.(\frac{w_1}{w_1 + w_2}p_1 + \frac{w_2}{w_1 + w_2}p_2) \tag{12}$$

$$f_4 = p_0.(\frac{w_1}{w_1 + w_2}p_1.\frac{w_2}{w_1 + w_2}p_2) \tag{13}$$

In the above equations, we assume that $p_0 = \rho_v(r).e^{\beta.\Gamma_{v,r,c}}$ 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. We define p_1 as such because lower duration to destination $\Upsilon_v^t(r)$ is preferred, unlike the other three parameters. We observe that reputation $\Gamma_{v,r,c}$, being the dominating factor, exponentially impacts the qualification $Q_{v,r,c}(MI)$, while the parameter $\rho_v(r)$ is multiplied linearly to it. In (10) and (11), parameters $\tilde{S}_v^j(r)$ and $\Upsilon_v^t(r)$ are used logarithmically and thus have a sub-linear impact. $\tilde{S}_v^j(r)$ and $\Upsilon_v^t(r)$ are aggregated by addition and multiplication in (10) and (11) respectively. On the contrary, in (12) and (13), parameters $\tilde{S}_v^j(r)$ and $\Upsilon_v^t(r)$ are combined in a weighted linear manner and aggregated by addition and multiplication respectively.

Volunteers are selected by using a variant of the Multiple-Choice Secretary Algorithm [18][26]. Using this algorithm, we select up to $\lfloor k_r/2 \rfloor$ volunteers from the initial m volunteers, where m is a random sample drawn from a Binomial distribution. The observed qualification values are used to determine a threshold such that among the remaining volunteers, only those whose qualification values surpass this threshold are selected. However, this algorithm does not ensure that all the channels are covered efficiently. To address this, we devise a scheme to efficiently assign channels to the selected volunteers. We maintain a hash table $H_{c,V_{S,r}}(MI)$ where a channel c is mapped to the list $\Lambda_{c,V_{S,r}}$ of all $v \in V_{S,r}$ (where $V_{S,r}$ is the set of selected volunteers in region r in a MI), ordered in descending order by their qualification values to monitor c. For every region $r \in R$, a channel c is then assigned in a round robin manner to the topmost v in $\Lambda_{c,V_{S,r}}$, i.e., c is assigned to the volunteer who is most *qualified* to monitor c, after which v is deleted from the list $\Lambda_{c,V_{S,r}}$ of every channel $c \in C$ in $H_{c,V_{S,r}}(MI)$. This ensures that no volunteer monitors more than one channel over a given MI and further helps to ensure effective coverage of all channels

V. Experiments And Results

The enforcement framework is simulated using the C++ version of CSIM19. The total area of enforcement is divided into two regions of equal area and each region is assigned a similar set of five channels. A random fraction of the population is chosen as volunteers (equals 183 volunteers). The mobility of volunteers is based upon the Random Waypoint mobility model. The *corrupt* volunteers detect accurately with probability ranging from 0 to $0 + \delta$ ($\delta = 0.5$) and the *honest* volunteers detect accurately with a probability of 1. Also, we assume that $k_r = k$ for all $r \epsilon R$. Accuracy of spectrum misuse detection and hit ratio are primary metrics used to measure the effectiveness of a given procedure. Hit ratio is the ratio of the number of hits to the total number of hits and misses. If a volunteer v selected for monitoring r is in r at the beginning of an AUI in a MI that v is selected for, then it is a *hit*, otherwise it is a *miss*. Thus, a higher hit ratio signifies higher coverage of regions over the period of enforcement.

In Figure 3, we compare the mean hit ratio and mean accuracy of volunteers selected by using different variations of the function f that computes qualification $Q_{v,r,c}(MI)$ in (9), such that $k = 1\% - 25\%\ of\ ||V||$, probability of a volunteer to be *corrupt* is 0.5, $\beta, \gamma = 1$ and $h = 0.03$. While the variations f_1 and f_2 are as defined in (10) and (11) respectively, the variation f_3 (defined in (12)) is divided into $f_{3a}(s.t.\ w_1 > w_2)$, $f_{3b}(s.t.\ w_1 = w_2)$ and $f_{3c}(s.t.\ w_1 < w_2)$. Similarly, variation f_4 (defined in (13)) is divided into f_{4a}, f_{4b} and f_{4c}. We observe that the variations which aggregate p_1 and p_2 additively (f_2 and all variations of f_3) give higher accuracy than the remaining variations which use multiplicative aggregation. This is because multiplication of the exponential reputation term in p_0 by the product of the other terms (which are fractions between 0 and 1), decreases the overall domination of p_0 in determining $Q_{v,r,c}(MI)$. By using variation f_{3a}, the selected volunteers give the highest mean accuracy (0.92) and hit ratio (0.78). This is better than the mean accuracy (0.89 and 0.83) and hit ratio (0.73 and 0.62) obtained by using f_{3b} and f_{3c} respectively. This proves that having higher weights associated with p_1, results in better overall performance when p_1 and p_2 are used linearly and aggregated additively.

In all the remaining experiments, we use the variation f_{3a} to calculate $Q_{v,r,c}(MI)$ because it gave the best performance (as shown in Figure 3). We assume $k = 25\% - 50\%\ of\ ||V||$ and that the probability of a volunteer to be *corrupt* is 0.5. The proposed algorithm has the potential to be designed as an incentive-based variant, which can then be compared against the incentive-based auction algorithms that have been used in many of the related works. Instead, we compare the performance between volunteers that are selected by using the proposed algorithm and by using an Algorithm R which selects volunteers in a random fashion, irrespective of their qualification. In Figure 4, we observe that the mean hit ratio of volunteers selected by using the proposed algorithm is greater than that of Algorithm R for all values of k. However, by applying the proposed algorithm, the mean *hit ratio* decreases consistently with the increase in k because the proportion of highly *qualified* selected volunteers reduces as the value of k increases. Also, there is an overall decrease in standard deviation for both the algorithms as range of k increases from 1-25% of $||V||$ to 75-100% of $||V||$ because a balance is approached between the proportions of highly *qualified* and less *qualified* selected volunteers as the value of k increases. In Figure 5, we observe that even though the mean accuracy of detection by using the proposed algorithm decreases as k increases, yet it performs better for all ranges of k when compared to Algorithm R. In Figure 6, we observe that the mean accuracy of misuse detection decreases for both the algorithms as the probability of a volunteer to be *corrupt* increases. This is intuitive because more *corrupt* volunteers are selected with the increase in probability of a volunteer to be *corrupt*. Interestingly, for both the algorithms, the accuracy decreases at a faster rate than in Figure 5, proving that the probability of a volunteer to be *corrupt* has greater impact than the range of k in the overall accuracy of detection. Also, we see that using the proposed algorithm, the standard deviation increases with the increase in probability of a volunteer to be *corrupt* because of the increasing disparity of results between *corrupt* and *honest* volunteers. However, it decreases when the probability of a volunteer to be *corrupt* is 1 because of the decrease in disparity between their results. Finally, for probability of a volunteer to be *corrupt* being 0.5, we observe that the standard deviation in mean accuracy of detection across all the five channels is 0.0056 for $k = 25\% - 50\%\ of\ ||V||$ and the average standard deviation in detection accuracy across all the five channels for all the ranges of k is 0.00705, which are significantly low. Thus, our mechanism ensures efficient and uniform channel coverage.

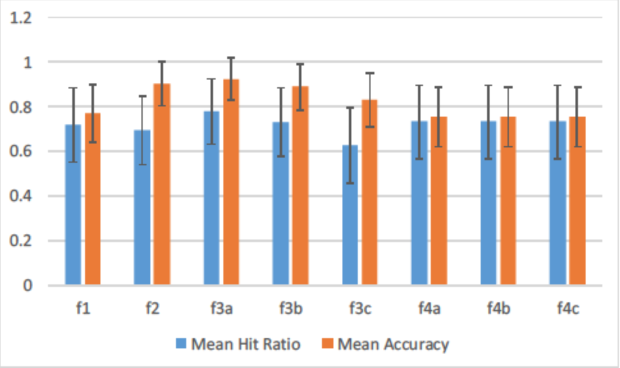

Figure 3. Comparison of the performance of volunteers selected by using different variations of function f in (9)

VI. Conclusion

In this paper, we discussed about a spectrum enforcement framework in cooperative wireless networks, based on crowdsourced infrastructure, supported by sentinel-based

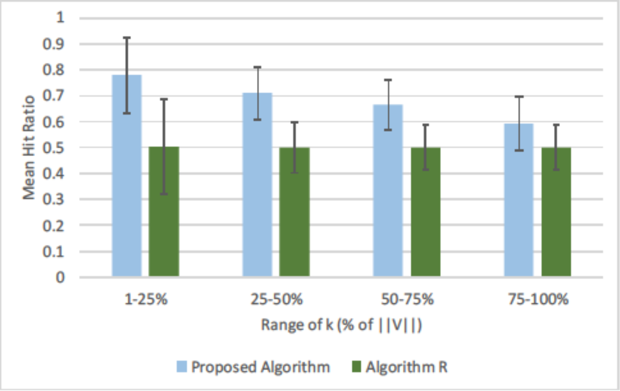

Figure 4. Comparison of the mean hit ratio by selecting volunteers using the proposed algorithm and Algorithm R.

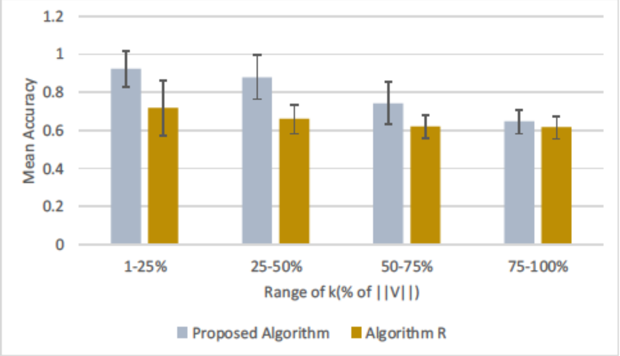

Figure 5. Comparison of the mean accuracy by selecting volunteers using the proposed algorithm and Algorithm R.

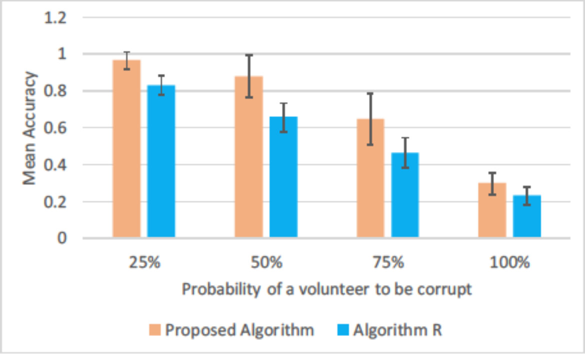

Figure 6. Comparison of the mean accuracy of detection for different probabilities of a volunteer to be *corrupt*.

monitoring and by a central DSA Enforcement Infrastructure. The objective was to maximize coverage of the area of enforcement, the coverage of all the channels in it and to ensure accurate detection of spectrum access violation by selecting *qualified* volunteers. We developed a framework to select volunteers based on their reputation, sojourn time, estimated duration to reach a destination and likelihood of visit to a region. We explored ways to aggregate the above four parameters in order to assess their impact in measuring the qualification of a volunteer. We used a variant of the multiple-choice Secretary algorithm to select volunteers dynamically based on their qualifications to monitor a region and developed a mechanism for optimal assignment of channels to volunteers. The results indicate that our proposed methodology ensures higher accuracy in detection of spectrum access violation and higher coverage of enforcement area when compared to an algorithm that selects volunteers in a random fashion. Efficient coverage of all channels is ensured too.

We plan to extend this work to develop an incentive-based variant of the proposed algorithm and explore more algorithms to select volunteers for multi-channel spectrum enforcement. We further plan to explore different AI based mechanisms to determine the reputation and location likelihood of volunteers in the enforcement area.

Acknowledgment

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

References

[1] Federatedwireless.com. (2019). [online] Available at: http://federatedwireless.com/wp-content/uploads/2017/03/CBRS-Spectrum-Sharing-Overview-v3.pdf [Accessed 25 Jul. 2019].

[2] Federal Communications Commission. *3.5 GHz Band / Citizens Broadband Radio Service.* [Online]. Available from: https://www.fcc.gov/wireless/bureau-divisions/broadband-division/35-ghz-band/35-ghz-band-citizens-broadband-radio#block-menu-block-4 [Accessed 25 Jul. 2019].

[3] E. Schlager and E. Ostrom, "Property-Rights Regimes and Natural Resources: A Conceptual Analysis," Land Econ., vol. 68, no. 3, 1992, pp. 249–262.

[4] Shavell, Steven. "The Optimal Structure of Law Enforcement." The Journal of Law & Economics, vol. 36, no. 1, 1993, pp. 255–287. JSTOR, www.jstor.org/stable/725476.

[5] A. Gopinathan, Z. Li, and C. Wu, "Strategyproof auctions for balancing social welfare and fairness in secondary spectrum markets," 2011 Proc. IEEE INFOCOM, 2011, pp. 3020–3028.

[6] J. Lin, M. Li, D. Yang, G. Xue, and J. Tang, "Sybil-proof incentive mechanisms for crowdsensing," in IEEE INFOCOM 2017, pp. 1–9.

[7] D. Yang, G. Xue, X. Fang, and J. Tang, "Crowdsourcing to Smartphones: Incentive Mechanism Design for Mobile Phone Sensing," in Proceedings of the 18th Annual International Conference on Mobile Computing and Networking, 2012, pp. 173–184.

[8] M. B. H. 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, 2013, pp. 7–12.

[9] D. Yang, X. Zhang, and G. Xue, "PROMISE: A framework for truthful and profit maximizing spectrum double auctions," in Proceedings - IEEE INFOCOM, 2014, pp. 109–117.

[10] R. Chen, J.-M. Park, and J. H. Reed, "Defense Against Primary User Emulation Attacks in Cognitive Radio Networks," IEEE J.Sel. A. Commun., vol. 26, no. 1, Jan. 2008, pp. 25–37.

[11] X. Jin, R. Zhang, Y. Chen, T. Li, and Y. Zhang, "DPSense: Differentially Private Crowdsourced Spectrum Sensing," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 296–307.

[12] X. Jin and Y. Zhang, "Privacy-Preserving Crowdsourced Spectrum Sensing," IEEE/ACM Trans. Netw., vol. 26, no. 3, Jun. 2018, pp. 1236–1249.

[13] A. Dutta and M. Chiang, "“See Something, Say Something" Crowdsourced Enforcement of Spectrum Policies," IEEE Trans. Wirel. Commun., vol. 15, no. 1, Jan. 2016, pp. 67–80.

[14] Wang, T.-H. Tsai, and W.-H. Chung, "The Novel Crowdsourcing Algorithm for Cooperative Spectrum Sensing," 2018 IEEE Int. Symp. Dyn. Spectr. Access Networks, pp. 1–5, 2018.

[15] F. Aurenhammer, "Voronoi diagrams—a survey of a fundamental geometric data structure", ACM Comput. Surv., vol. 23, no. 3, Sep. 1991, pp. 345–405.

[16] Q. Du, M. Emelianenko, and L. Ju, "Convergence of the Lloyd Algorithm for Computing Centroidal Voronoi Tessellations," SIAM J. Numer. Anal., vol. 44, no. 1, Jan. 2006, pp. 102–119.

[17] B. Talukder, K. W. Hipel, and G. W. vanLoon, "Developing Composite Indicators for Agricultural Sustainability Assessment: Effect of Normalization and Aggregation Techniques," Resources, vol. 6, no. 4, 2017.

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

[19] R. Kleinberg, "A Multiple-choice Secretary Algorithm with Applications to Online Auctions," in Proceedings of the Sixteenth Annual ACM-SIAM Symposium on Discrete Algorithms, 2005, pp. 630–631.

[20] X. Jin, J. Sun, R. Zhang, Y. Zhang, and C. Zhang, "SpecGuard: Spectrum misuse detection in dynamic spectrum access systems," 2015 IEEE Conf. Comput. Commun., 2015, pp. 172–180.

[21] Pittsburgh Population. (2018-06-12). [Online]. Available from: http://worldpopulationreview.com/us-cities/pittsburgh/.

[22] A. M. Salama, M. Li, and D. Yang, "Optimal Crowdsourced Channel Monitoring in Cognitive Radio Networks," in IEEE Global Communications Conference, GLOBECOM, Singapore, December 4-8, 2017, pp. 1–6.

[23] M. Li, D. Yang, J. Lin, M. Li, and J. Tang, "SpecWatch: A framework for adversarial spectrum monitoring with unknown statistics," Comput. Networks, vol. 143, 2018, pp. 176–190.

[24] W. Chen, Y. Wang, and Y. Yuan, "Combinatorial Multi-Armed Bandit: General Framework and Applications," in Proceedings of the 30th International Conference on Machine Learning, 2013, vol. 28, no. 1, pp. 151–159.

[25] F. Benedetto, A. Tedeschi, G. Giunta, and P. Coronas, "Performance improvements of reputation-based cooperative spectrum sensing," in 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2016, pp. 1–6.

[26] D. Das, T. Znati, M. Weiss, P. Bustamante, M. Gomez, S. Rose, "Crowdsourced Misuse Detection in Dynamic Spectrum Sharing Wireless Networks", International Conference on Networks (ICN), 2019, pp. 74-81.