Misuse Detection in Dynamic Spectrum Sharing Wireless Networks Across Multiple Channels

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

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

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

Abstract - **We propose a spectrum enforcement framework across multiple channels by mobile, crowdsourced agents (also called volunteers), who work in collaboration with a trustworthy infrastructure. The success of spectrum sharing relies on the automated enforcement of spectrum policies. The primary challenge addressed here is to ensure *efficient ex post* spectrum enforcement. In order to achieve this, we focus on attaining maximum coverage of the area of enforcement and of all channels, and on ensuring reliable and accurate detection of spectrum violation. Maximum coverage of the given area of enforcement is ensured by proposing to divide it into smaller regions using the Lloyd's algorithm and solving the enforcement problem by a divide and conquer mechanism over the entire area. We determine the qualification of volunteers based on their likelihood of being in a region, and on their trustworthiness. We define algorithms to select qualified volunteers for every region in an online manner such that every channel is efficiently covered. The enforcement framework is simulated in CSIM19 (C++ version) and extensive analysis of the performance of the proposed methodologies is performed.**

Keywords- volunteer; sentinel; ex post spectrum enforcement; crowdsourced spectrum enforcement; volunteer selection; channel assignment; mobility.

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 Spectrum Access System (SAS). 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). 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 [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. 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]. 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. As we consider *ex post* enforcement approaches, the need to detect enforceable events, gather information about these events and adjudicate claims based on rules and evidence becomes important. In this paper, we focus on designing an efficient framework for 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, this paper proposes an enforcement framework that aims to achieve a) maximum coverage of the entire area of enforcement, b) maximum coverage of all the channels in a region c) an accurate, reliable and feasible detection of an event of violation, d) use of an effective method for hiring and deploying detecting agents. We leverage crowdsourced spectrum enforcement because it is more cost-effective and has the potential for higher accuracy of detection and localization of spectrum access violation when compared to static enforcement [13][28]. 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) *Region Coverage*: We use a clustering algorithm to organize the area into smaller sized "regions" in order to ensure more manageable detection of violation. The enforcement problem can then be solved by a divide and conquer mechanism over all the regions.
b) *Channel Coverage*: We develop an algorithm to ensure efficient coverage of all channels in a region.
c) *Crowdsourced Enforcement*: We explore a mechanism to select crowdsourced agents (also called volunteers) for ensuring that a spectrum access violation is detected with high probability of accuracy and efficiency.
d) *Volunteer Selection*: We develop a framework to assess the *qualification* of a volunteer across two dimensions — location likelihood and trust, which is used to select volunteers such that an "optimal" quality of spectrum enforcement is ensured.

The paper is organized in the following manner. Section II of the paper discusses about the related works, while Section III of the paper discusses about the proposed enforcement framework. Section IV discusses about the crowdsourced monitoring methodology, with a focus on the parameters that qualify a volunteer for selection and the appropriate volunteer selection mechanism. Section V discusses about the experimental setup and the results we obtained from applying the proposed volunteer selection algorithm. Finally, we conclude the paper and discuss about future works in Section VI.

II. Related Works

Jin *et al.* [20] introduce the first crowdsourced spectrum misuse detection framework for DSA systems, where a legitimate transmitter is required to embed a spectrum permit into its physical layer signals, which can be decoded and verified by ubiquitous mobile users. Dutta and Chiang [13] discuss about crowdsourced spectrum enforcement for accurate detection and location of spectrum enforcement. However, they assume that crowdsourced spectrum access enforcers are trustworthy and do not examine the effect of distrust of enforcers. Li *et al.* [23] model 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. However, they assume that the spectrum monitoring agent and the malicious users are always static. 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. Several incentive-based crowdsourced spectrum sensing works have been done over the past few years. 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. Zhu *et al.* [14] propose an incentive-based auction mechanism to improve fairness of bids by taking into consideration the effects of malicious competition behavior and the "free-riding" phenomenon in crowdsourcing services. Lin *et al.* [6] take 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. Contrary to majority of 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 misuse and access rights violations can be effectively prevented by using 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. Moreover, in contrast to the usual methodologies, we explore the use of an online non-incentive-based methodology for selection of mobile volunteers based on their *qualifications* to ensure maximum coverage of enforcement area, efficient coverage of all the channels in an enforcement region and accurate detection of spectrum access violations. This work is an extension of our

previous work [1]. Contrary to our previous work, in this paper, we propose spectrum enforcement over multiple channels. We explore multiple ways to aggregate the different parameters for the calculation of qualification of a volunteer and develop an efficient algorithm for assignment of channels to the selected volunteers for monitoring. In contrary to our work in [27], we explore the effect of different parameters (trust and location likelihood) in the performance of the crowdsourced agents. Finally, in contrast to [1] and [27], we conduct more experiments and analyze the results for a more comprehensive and extensive evaluation of our system.

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

A. System Model

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. To carry out spectrum monitoring practices, volunteers incur transmit power consumption cost and bandwidth consumption cost.

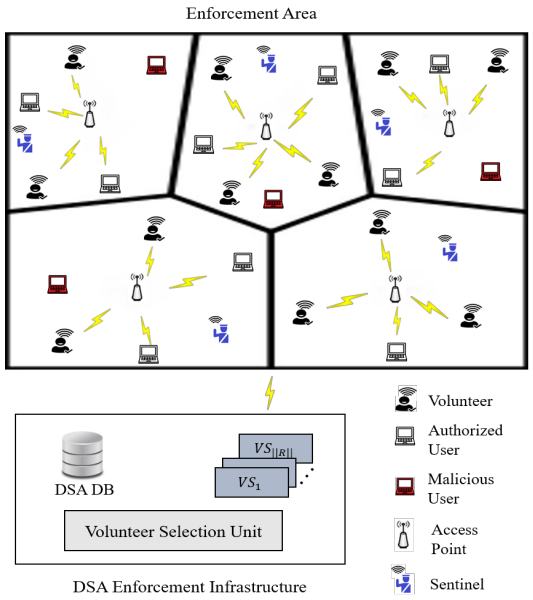

Figure 1. System Model.

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 Database is used to identify the channels and their corresponding authorized users in R. Finally, the system model 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 volunteers who have unreliable behavior.

B. Coverage of Region

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 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 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

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 VS_r of the DSA Enforcement Infrastructure to estimate whether v will be available to monitor a given channel in r in the future.

As shown in Figure 2, 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 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 spectrum access violation or legitimacy. A new set of volunteers is selected in region r at the end of every MI by the Volunteer Selection Unit using the data from Volunteer Service unit VS_r associated with region r. Volunteer selection in r is primarily based on 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 access violation. At the end of every AUI i, a volunteer v reports the observed state $\phi^i_{v,r,c}$ of a channel c that it monitors in region r, over i. The state of a channel c can be either a) violated, when c is being used by a malicious transmitter b) not violated, when c is either idle, i.e., when no user, authorized or malicious, uses c or safe, i.e., when c is used by an authorized transmitter. The necessary ground truth required for calculating accuracy of interference detection by v in r is acquired from the observed state $\phi^j_{s,r,c}$ of c by a sentinel $s \in S'$ that monitors c at a random AUI j in the given MI. 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 in r at a random interval j,which is not known to the volunteers. This helps us to calculate the behavior $b^i_{v,r,c}$ of v in r at AUI i by using (1) given below.

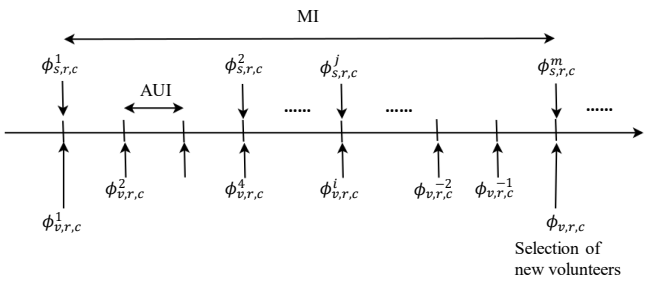

Figure 2. Observations $\phi^i_{v,r,c}$ by volunteer v after every AUI and $\phi^j_{s,r,c}$ by sentinel s after random AUIs, for the 1st MI.

$$b^i_{v,r,c} = \begin{cases} 1, & \phi^i_{v,r,c} = \phi^j_{s,r,c} \\ 0, & \phi^i_{v,r,c} \neq \phi^j_{s,r,c} \end{cases}, \forall i = j \quad (1)$$

As shown in (1), the behavior of a volunteer $b^i_{v,r,c}$ at i in r is assigned to zero when there is a mismatch in the observed state of channel c, 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. 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 is called a matching interval. We aggregate $b^i_{v,r,c}$ over all the matching intervals to find the trust $T_{v,r,c}$ of v to monitor channel c in r, by calculating the arithmetic mean $T_{v,r,c}$, given by (2),

$$T_{v,r,c} = \frac{1}{m}\sum_{p=1}^{m} b^p_{v,r,c} \quad (2)$$

where p is a matching interval and m is the total number of matching intervals over all the monitoring intervals observed so far. After every MI, a volunteer v monitoring a channel c in region r sends the detection results (over all the AUIs in the MI) to the corresponding VS_r in the DSA Enforcement Infrastructure. Similarly, a sentinel s that monitors the spectrum in region r, sends its detection results and the random AUIs in which it monitored to VS_r. Based on the detection results of both the sentinel and the volunteers, the trust $T_{v,r,c}$ of volunteer v is computed in the VS_r. We assume that volunteers can detect spectrum misuse by using any of the methods of misuse detection used in literature [29]-[31]. The impact of choosing any of these methods for misuse detection to the accuracy of detection is out of the scope of this paper.

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, are given preference. The VS_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, $S_v^{j-1}(r)$, 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. Furthermore, we calculate the $(j-1)^{th}$ return time $R_v^{j-1}(r)$ of v in r as the difference between $arr_v^{j}(r)$ and $arr_v^{j-1}(r)$. As given by (4), this enables us to calculate the proportion of time, $P_v^{j-1}(r)$, that v resided in r on its previous $((j-1)^{th})$ visit to r, as the ratio of $S_v^{j-1}(r)$ to $R_v^{j-1}(r)$. 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).

$$P_v^{j-1}(r) = \frac{S_v^{j-1}(r)}{R_v^{j-1}(r)} \quad (3)$$

$$\tilde{P}_v^{j}(r) = \alpha . P_v^{j-1}(r) + (1 - \alpha) . \tilde{P}_v^{j-1}(r) \quad (4)$$

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

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

where $0 < h < 1$, $E_v^{j-1}(r) = P_v^{j-1}(r) - \tilde{P}_v^{j-1}(r)$ is the prediction error, and $\sigma_v^j(r)$ is the average of the past square prediction errors on visit j. $\sigma_v^j(r)$ can be expressed as follows:

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

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 r increases. This is expressed by the separation factor, $\Upsilon_{t,v,r}$, given by (7) as follows:

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

where $0 < \gamma_1, \gamma_2 < 1$, are parameters defined by the system and $d(L_{v,t}, O_r)$ is the displacement between $L_{v,t}$and O_r. Since $\Upsilon_{t,v,r}$ is exponential, so we empirically select values of γ_1 and γ_2 to avoid high variance in the values of $\Upsilon_{t,v,r}$ across all the volunteers.

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 $\Upsilon_{t,v,r}$,. We observe that 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 $d(L_{v,t}, O_r) \geq 0$, so $0 < \Upsilon_{t,v,r} \leq 1$. As

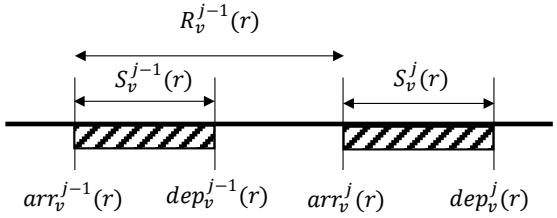

Figure 3. Sojourn time $S_{j,v,r}$ and Return time $R_{j,v,r}$ of volunteer v after its j^{th} visit to region r.

weighting the parameters by linear regression requires large amount of data and preferential weighting is hard to establish because 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 $\Upsilon_{t,v,r}$ as given by (8) below.

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

C. Selection of volunteers

From the set of volunteers, V, in area of enforcement, R, 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.

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

Since $T_{v,r,c}$ and $L_{v,r}(MI)$ represent the measurement of different parameters, we normalize them by using the min-max normalization technique [17] such that $0 \leq T_{v,r,c}, L_{v,r}(MI) \leq 1$. Clearly, both trust and location likelihood are crucial for successful detection of spectrum access violation by crowdsourced volunteers. Therefore, we explore ways to aggregate the two parameters in g in order to assess their impact in measuring the qualification of a volunteer as shown in (10) – (13).

$$g_1 = \frac{w_1}{w_1 + w_2} p_1 + \frac{w_1}{w_1 + w_2} p_2 \quad (10)$$

$$g_2 = e^{\beta_1 . p_2} . \beta_2 . p_1 \quad (11)$$

$$g_3 = e^{\beta_1 . p_2} . \log(1 + \beta_2 . p_1) \quad (12)$$

$$g_4 = \max(p_1, p_2) \quad (13)$$

In the above equations, we assume that $p_1 = T_{v,r,c}$ and $p_2 = L_{v,r}(MI)$. In (10), we aggregate p_1 and p_2 by using weighted addition. The variant g_1 is further divided into g_{1a}, g_{1b} and g_{1c} such that $w_1 < w_2, w_1 = w_2$ and $w_1 > w_2$ respectively. In (11), we make one parameter more dominant (by having it exponentially impact the value of qualification $Q_{v,r,c}(MI)$) than the other parameter which impacts the qualification value linearly. The variant g_2 in (11) is further divided into g_{2a} and g_{2b} where we make parameter p_2 and p_1 exponentially dominating respectively. Similarly, in (12), we make one parameter more dominant by having it exponentially affect the qualification value and by having the other parameter sub-linearly (logarithmically) impact the qualification value. Likewise, we divide g_3 into g_{3a} and g_{3b}

such that p_2 and p_1 are made exponentially dominant respectively. Finally, in (13), we try the variant g_4 where the qualification $Q_{v,r,c}(MI)$ is set as the maximum of the two parameters p_1 and p_2.

This work is an extension of our previous work [1] and focuses on spectrum enforcement over multiple channels in a region. We also assume that a volunteer v can be hired to monitor more than one region over the next MI as v is mobile and can potentially cover multiple regions over a given MI. The Volunteer Selection Unit of the DSA Enforcement Infrastructure builds a centralized $||V||$-by-$||R||$ matrix $\Psi_{V,R}$, using the values of volunteer attributes from the VS_r associated with every region $r \in R$. The matrix $\Psi_{V,R}$ is a volunteer-region qualification matrix that contains the qualification values $Q_{v,r,c}(MI)$ of all $v \in V$ for every channel $c \in C$ in each region $r \in R$. The Volunteer Selection Unit selects k_r volunteers dynamically from V based on the qualification values of all $v \in V$ for every c in r, using Algorithm 1 as shown in Figure 4.

For the volunteer selection Algorithm 1, we use the volunteer-region qualification matrix $\Psi_{V,R}$ to select qualified volunteers for every $r \in R$ (line 1). At the end of a MI (line 3), the Volunteer Selection Unit gains access to the qualification values of all $v \in V$ for r from $\Psi_{V,R}$ and stores

Algorithm 1 Selection of Volunteers

1: Maintain matrix $\Psi_{V,R}$ that stores qualification values $\forall v \in V, \forall r \in R$, list of selected volunteers $V_{S,r}, \forall r \in R$
2: **for** all $r \in R$ **do**
3: **if** $t = MI$ **then**
4: $Q_r \leftarrow \Psi_{V,R}[r]$
5: **if** $k_r = 1$ **then**
6: *Run Classic Secretary Algorithm*
7: **else**
8: $m_r \leftarrow Binom(||Q_r||, 1/2)$
9: **if** $m_r > \lfloor k_r/2 \rfloor$ **then**
10: $l_r \leftarrow \lfloor k_r/2 \rfloor$
11: **else**
12: $l_r \leftarrow m_r$
13: **end if**
14: *Recursively select upto l_r volunteers*
15: $B_r \leftarrow descending\_sort(Q_r[1], ..., Q_r[m_r])$
16: $threshold \leftarrow B_r[l_r]$
17: **for** $i \leftarrow m_r + 1, ..., ||Q_r||$ **do**
18: **if** $Q_r[i] > threshold$ and $||V_{S,r}|| < k_r$ **then**
19: $V_{S,r} \leftarrow V_{S,r} \cup v$
20: **else**
21: *Reject v*
22: **end if**
23: **end for**
24: **end if**
25: **end if**
26: **end for**

Figure 4. Algorithm for selection of volunteers [19].

Algorithm 2 Assignment of Channels to Volunteers

1: Maintain Hash Table $H_{c,V_{S,r}}$ that maps a channel $c \in C$ to a list of selected volunteers $\Lambda_{c,V_{S,r}}$ ordered in descending order by their qualification values to monitor channel c, a list $V_{a,r}$ of volunteers being assigned a channel, a list of selected volunteers $V_{S,r}$
2: **for** all $r \in R$ **do**
3: **if** $t = MI$ **then**
4: **while** $||V_{a,r}|| < ||V_{S,r}||$ **do**
5: *Assign c by Round Robin to the first v in $\Lambda_{c,V_{S,r}}$*
6: $V_{a,r} \leftarrow V_{a,r} \cup v$
7: *Delete v from $\Lambda_{c,V_{S,r}}$ of all c in $H_{c,V_{S,r}}$*
8: **end while**
9: **end if**
10: **end for**

Figure 5. Algorithm for assignment of channels.

them in a list Q_r (line 4). 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, with constant probability. In a classic secretary algorithm, we observe the first $||Q_r||/e$ qualification values to determine a *threshold* and then select the first of the remaining volunteers, whose qualification value is above the threshold [19]. However, if $k_r > 1$, we select volunteers dynamically by using a variant of the 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 8-13). 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 that we observe in the sample of first m_r qualification values. After this, we select every volunteer with qualification value greater than $threshold$, till we select a maximum of k_r volunteers (lines 16-20) [19]. We apply this algorithm for selection of volunteers in every $r \in R$.

However, this algorithm does not ensure that all the channels are covered efficiently. Thus, we develop an algorithm to efficiently assign channels to the selected volunteers as shown in Figure 5. A hash table $H_{c,V_{S,r}}(MI)$ is maintained 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 channel c (line 1). 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 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 $H_{c,V_{S,r}}(MI)$ (lines 5-7). This is continued until all the volunteers are assigned a channel to monitor. 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

In this section, we discuss about the experiments that we conducted and analyze the performance of the proposed spectrum enforcement framework.

A. Simulation Environment

We simulate the enforcement framework by using the C++ version of the CSIM19 simulation engine. For simplicity, we divide the entire area of enforcement R (of total area 500,000 sq. units) into two regions of equal area. This work can, however, be easily extended to deal with more regions. With the assumption that 1 sq. unit is equivalent to 1 sq. meter and by taking the average population density of Pittsburgh (2,140/sq. km) [21], we calculate the total population (1,070 people) in the area of enforcement. A random fraction of people from the total population are chosen as volunteers (equals 183 volunteers). Volunteers are initially placed at random positions within R and they move by following the Random Waypoint Mobility Model [24] with speed ranging from 1m/s to 70m/s. The maximum speed of a volunteer is chosen higher than the usual speed limit of a vehicle in a highway in order to compensate for the limited simulation time. We assume that each region has a set of five channels to monitor. Volunteers are classified as *corrupt* and *honest*. 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. Additionally, we assume that every volunteer uses a sensing device with maximum battery capacity of 7 Wh and that the battery discharges at the rate of 1 J/s for a random time interval drawn from an exponential distribution of the mean active time interval of 100 s. After every active time interval, we assume that the sensing device remains idle for a random time interval drawn from an exponential distribution of the mean idle time interval of 10 s. The simulation runs till the battery of the sensing device used by every volunteer is exhausted, i.e., for 5610 AUIs. Each AUI is equivalent to 5 units of time and one MI is equivalent to 5 AUIs. We select $\gamma_1 = 1$ and $\gamma_2 = 0.01$ for the separation factor $\Upsilon_{t,v,r}$ of v with respect to r. Since $\Upsilon_{t,v,r}$ is exponential, so we empirically decide the value of the γ_2, which is the coefficient of $\mathrm{d}(L_{v,t}, O_r)$ from (7), to avoid high variances in the qualification values of volunteers. Furthermore, we empirically determine the values of $h = 0.03$, $\beta_1 = 10$ and $\beta_2 = 10$ in (5), (11) and (12) respectively. Finally, we assume that $k_r = k$ for every $r \in R$. The essential simulation parameters with their respective values are listed in Table I.

TABLE I. 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
Maximum battery capacity of a volunteer	$7\ Wh$
Number of AUIs	5610
System parameter γ_1	1
System parameter γ_2	0.01
System parameter h	0.03
System parameter β_1	10
System Parameter β_2	10

B. Metrics

We consider two primary metrics for evaluating the performance of our proposed method — the *mean accuracy of detection* and the *mean hit ratio*.

In a monitoring interval MI, if a volunteer v selected for monitoring region r has its current location in r at the beginning of an AUI, then it is a *hit*, otherwise it is a *miss* in the AUI of a MI. This is in accordance with the assumption that a selected volunteer v can successfully monitor a channel c in r over an AUI only if v resides in r over the AUI. The *hit ratio* of a region $r \in R$ over a given MI measures the ratio of the number of *hits* of all the selected volunteers to the sum of the number of *hits* and the number of *misses* of all the selected volunteers in r. A volunteer with high location likelihood will give high hit ratio. The *mean hit ratio* is computed as the average of all the *hit ratios* over all the MIs in a region. The detection of an event conducted by a volunteer is considered accurate if the detection result matches that of a sentinel s in region r at an AUI. The *mean accuracy of detection* of a volunteer is computed as the average of the number of accurate detections in a MI by the selected volunteers over the entire duration of enforcement over all the channels in a region. A volunteer with high location likelihood will give high *mean hit ratio* and a volunteer with high trust value will give high *mean accuracy of detection*.

C. Results

In Figure 6, we compare the mean hit ratio and mean accuracy of volunteers selected by using different variations of the function g that computes qualification $Q_{v,r,c}(MI)$ in (9), such that $k = 1\% - 25\%\ of\ ||V||$ and probability of a volunteer to be *corrupt* is 0.5. In the variant g_{1a}, we observe that the mean hit ratio is higher than the mean accuracy. This is because $w_1 < w_2$ (i.e., the weight associated with location likelihood $L_{v,r}(MI)$ is greater than the weight associated with trust $T_{v,r,c}$). Similarly, in the variant g_{1c}, we observe that the behavior is opposite because $w_1 > w_2$. Interestingly, in variant g_{1b}, we observe that the difference in mean accuracy and mean hit ratio (of values 0.776 and 0.822 respectively) is

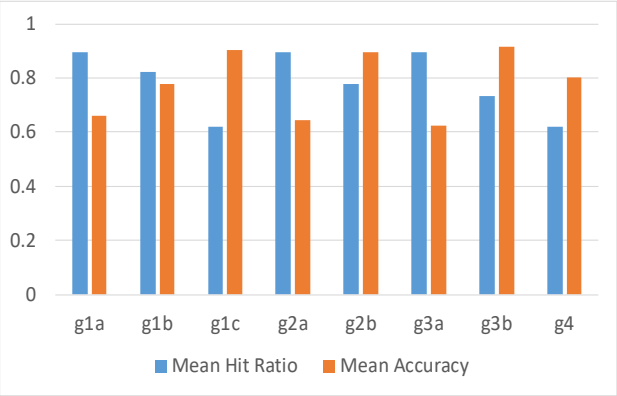

Figure 6. Comparison of the performance of volunteers selected by using different variations of function g in (9)

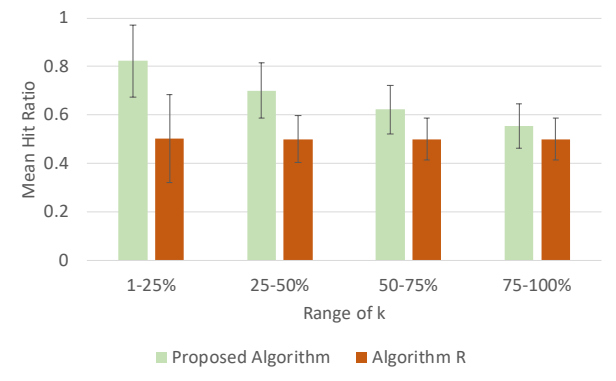

Figure 7. Comparison of the mean hit ratio of volunteers selected by using the Proposed Algorithm and Algorithm R for different values of k.

lower than what we observe in g_{1a} and g_{1c}. This is because $w_1 = w_2$ in g_{1b}. Thus, we conclude that assigning a higher weight to location likelihood results in higher mean hit ratio and assigning higher weight to trust results in higher accuracy. In the variants g_{2a} and g_{2b}, we observe that mean hit ratio is higher than mean accuracy and that mean accuracy is higher than mean hit ratio, respectively. This is because the location likelihood and trust exponentially impact the qualification value $Q_{v,r,c}(MI)$ in g_{2a} and g_{2b} respectively. We observe the same behavior in the variants g_{3a} and g_{3b}. However, we observe that the difference between mean hit ratio and mean accuracy is higher in g_{3a} and g_{3b} (of values 0.268 and 0.181 respectively) than in g_{2a} and g_{2b} (of values 0.25 and 0.119 respectively). This is because the non-dominant factor in g_{2a} and g_{2b} is linear while it is sub-linear (logarithmic) in g_{3a} and g_{3b}. Finally, for variant g_4, we observe that the mean accuracy is higher than the mean hit ratio. This is because we assume that *honest* volunteers detect accurately and hence in such cases mean accuracy is most likely to have a higher value than mean hit ratio. We want to attain both high accuracy of detection and high hit ratio. Therefore, for all the remaining experiments, we use the variant g_{1b} to calculate the qualification $Q_{v,r,c}(MI)$ as it has lowest difference (of value 0.046) between mean accuracy and mean hit ratio among all the variants of function g.

Figure 7 compares the mean *hit ratio* of all the regions over the entire duration of simulation, by using the proposed algorithm and Algorithm R for different ranges of k. Algorithm R selects k volunteers randomly from the total set of volunteers V for a region r, irrespective of their qualification. We observe that the proposed algorithm has a better mean *hit ratio* than Algorithm R for all the ranges of k. However, the mean *hit ratio* by applying the proposed algorithm decreases consistently (from 0.822 for k =1-25% of $||V||$ to 0.554 for k = 75-100% of $||V||$) with the increase in k because the proportion of highly *qualified* selected volunteers reduces as the value of k increases. The error bars in Figure 7 represent the mean standard deviation of the mean *hit ratio* across all regions, which decreases from 0.148 for k =1-25% of $||V||$ to 0.091 for k = 75-100% of $||V||$, using the proposed algorithm and decreases from 0.183 for k =1-25% of $||V||$ to 0.085 for k = 75-100% of $||V||$, using Algorithm R. This type of behavior is attributed to the fact that a balance is approached between the proportions of *qualified* and *unqualified* selected volunteers as the value of k increases.

Figure 8 compares the mean accuracy of detection of the selected volunteers over all the MIs between the proposed algorithm and the Algorithm R for varying ranges of k. We observe that the proposed algorithm performs better than the Algorithm R for all the ranges of k. The mean accuracy of detection decreases consistently (from 0.776 for k = 1-25% of $||V||$ to 0.639 for k = 75-100% of $||V||$) with the increase in k because of the decrease in the fraction of *qualified* volunteers in r as k increases. The mean standard deviation in accuracy of detection across all regions decreases from 0.124 for k =1-25% of $||V||$ to 0.049 for k = 75-100% of $||V||$, using the proposed algorithm and decreases from 0.147

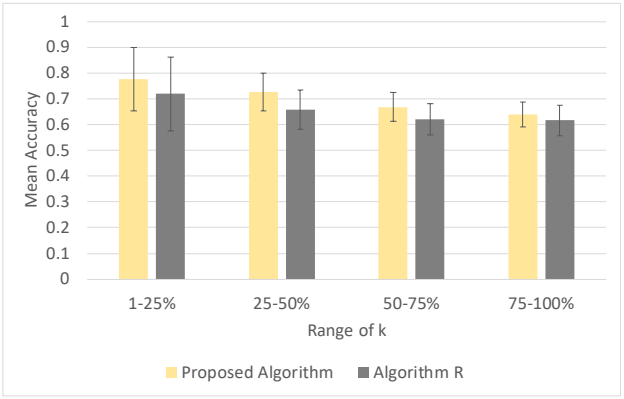

Figure 8. Comparison of the mean accuracy of volunteers selected by using the Proposed Algorithm and Algorithm R for different values of k

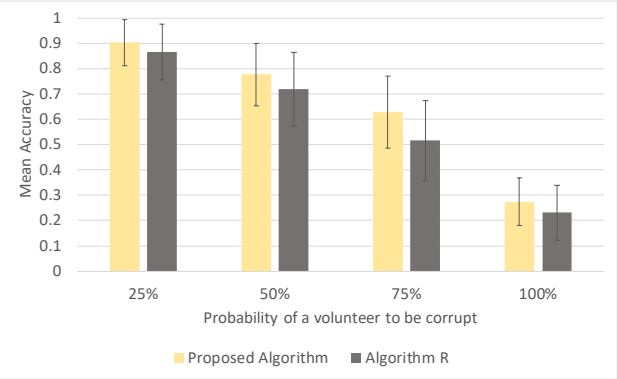

Figure 9. Comparison of the mean accuracy of detection for different probabilities of corruption of volunteers.

for k =1-25% of $||V||$ to 0.062 for k = 75-100% of $||V||$, using the Algorithm R. This is because as more volunteers are selected, a balance is approached between proportions of *corrupt* and *honest* volunteers. An interesting observation here is that the mean accuracy of selecting volunteers by using the proposed algorithm is not significantly higher than the mean accuracy attained by using Algorithm R. However, we can expect better mean accuracy by using the proposed algorithm if we use variations of g that give higher accuracy (like g_{1c}, g_{2b}, g_{3b} and g_4).

In Figure 9, we compare the mean accuracy of detection by using our proposed algorithm and Algorithm R for different probabilities of a volunteer to be corrupt. We observe that the accuracy in misuse detection decreases as the probability of a volunteer to be *corrupt* increases for $k = 1$ to 25% of $||V||$. Using our proposed algorithm, the mean accuracy decreases from 0.902 to 0.275 and by using Algorithm R, the mean accuracy decreases from 0.866 to 0.231 as the probability of a volunteer to be corrupt increases from 0.25 to 1. This is intuitive because more corrupt volunteers are selected with the increase in probability of corruption of a volunteer. Interestingly, for both the algorithms, the accuracy decreases at a faster rate than in Figure 8, proving that the probability of corruption of a volunteer has a greater impact in the overall accuracy of detection than k. Also, we observe that by using the proposed algorithm, the standard deviation increases with the increase in probability of corruption 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 (as all the volunteers are corrupt in this case).

In Figure 10, we study the mean detection accuracy across the five channels in all the regions. We observe that for $k =$ 1 to 25% of $||V||$ and the probability of corruption of a volunteer set to 0.5, the mean accuracy of detection of volunteers selected by our proposed algorithm across all channel is similar, with the highest mean accuracy of 0.833 in channel 1 and the lowest mean accuracy of 0.723 in channel 5. The standard deviation in mean accuracy across all the channels is 0.037, which is impressive. This is attributed to the efficiency of Algorithm 2 (as shown in Figure 5) that is used for the assignment of channels. However, we notice that the mean accuracy of detection decreases from channel 1 to channel 5. This is because by using Algorithm 2, the channels are assigned to volunteers in a round robin manner and hence it is more likely that a channel c_i will be assigned a more qualified volunteer than channel c_{i+1}. This discrepancy can be effectively mitigated by changing the order in which channels are assigned to volunteers after every MI. For example, if channel c_i gets assigned first to a volunteer in a MI, then channel c_{i+1} gets assigned first in the next MI. So, sequentially changing the priority of a channel to be assigned first would solve the problem.

Finally, we explore the impact of mobility pattern in the performance of volunteers for crowdsourced spectrum enforcement. We classify volunteers into three types based on their type of mobility. Volunteers of type 1 move by following the Random Waypoint Mobility model [24]. Using this model, a volunteer chooses a random destination in the area of enforcement and a random speed below the maximum speed limit to travel to the chosen destination. After reaching the destination, the volunteer pauses for a random time interval before choosing the next destination and speed. These volunteers are destination-oriented and can have speeds ranging from the speed of walking to the speed of moving in a car. The maximum speed limit is chosen to be twice the maximum speed limit of cars in USA [25], i.e., approximately 76 m/s for this type of users. The pause time of a volunteer is chosen randomly between 1 and 21 seconds. The maximum speed of a volunteer is chosen higher than the usual speed limit of a car in order to compensate for the limited simulation time. Volunteers of type 2 move in a pattern which resembles *roaming*. Type 2 volunteers choose a random direction (between 0 and 360 degrees) and move in that direction at a random speed below the maximum speed limit for a fixed interval of time. Such volunteers are assumed

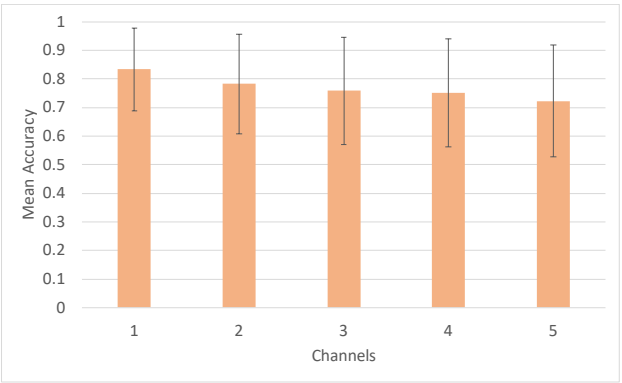

Figure 10. Comparison of the mean accuracy of detection by using the proposed algorithm across the five channels in every region.

to be walking or moving in low speed vehicles, like a skateboard and not in high speed vehicles like cars. The maximum speed limit of such volunteers is chosen as twice the average speed of a skateboarder [26], and is approximately 7 m/s. Again, the maximum speed limit of type 2 users is chosen higher than the usual speed of skateboarding in order to compensate for the limited simulation time. Type 3 volunteers are the ones whose mobility pattern is a hybrid of the mobility patterns of type 1 and type 2 volunteers. Such volunteers make a random decision to either move in a roaming pattern or by following the Random Waypoint Mobility model. After a volunteer completes its journey by using either of the mobility patterns, it will make a new random decision to again choose either of the mobility patterns for traversal.

In Figure 11, we observe the variation of mean hit ratio and mean accuracy for different mobility patterns of users for $k = 1$ to 25% of $||V||$ such that the qualification $Q_{v,r,c}(MI)$ of volunteers is calculated by using the variant g_{1b} (from (10) when w_1=w_2). We study six cases that may arise for the three types of volunteers (based on their mobility patterns). The first case arises when all the volunteers are of type 1, i.e., they follow the Random Waypoint Mobility Model (RWP). Similarly, the second and third cases are the ones where all the volunteers are of type 2 (Roaming) and type 3 (Hybrid) respectively. We observe that among the three cases when all the volunteers are either of Type 1, Type 2 or Type 3, the second case gives the highest mean hit ratio (of value 0.85) when compared to the first and third cases (of values 0.82 and 0.83 respectively). This is because the type 2 users roam at relatively lower speed ranges and hence tend to remain within the same region. Therefore, they have higher location likelihood when compared to type 1 and type 3 users. However, we observe that the mean accuracy of detection in case 2 is the lowest. This is because their location likelihood parameter dominates over their trust parameter for the calculation of their qualification values due to their high

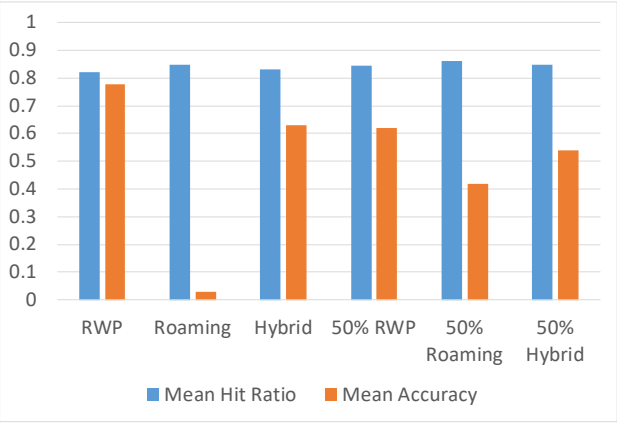

Figure 11. Variation of the mean accuracy of detection and mean hit ratio for different mobility patterns of users.

tendency to stay within the same region. Hence, even though they have high location likelihood, they are not guaranteed to give high accuracy of misuse detection. In comparison, the first and the third cases provide better accuracy of detection (of values 0.78 and 0.63 respectively). The first case provides the least difference (of value 0.043) between mean hit ratio and mean accuracy, which is desirable. Among the next three cases, the fourth case is where 50% of the volunteers follow Random Waypoint Mobility model (RWP) and the remaining volunteers are equally classified (25% each) as type 2 (Roaming) and type 3 (Hybrid) respectively. Similarly, the fifth and sixth cases are where 50% of the volunteers are of type 2 (Roaming) and type 3 (Hybrid) respectively. As expected, among these three cases, the fifth case (50% Roaming volunteers) show the highest mean hit ratio but the lowest mean accuracy. Also, we see that the fourth case (50% RWP) provide higher accuracy when compared to the sixth case (50% Hybrid). This is because hybrid volunteers do move in roaming pattern in some instances (which has previously shown lower mean accuracy). Hence, we can conclude that volunteers who move using the Random Waypoint Mobility Model with speeds ranging from the speed of walking to maximum speed limit of cars, give better performance than the other two mobility patterns because it causes least deviation between mean hit ratio and mean accuracy.

VI. CONCLUSION

In this paper, we discussed about a spectrum enforcement framework over multiple channels based on a crowdsourced spectrum monitoring infrastructure, supported by sentinel-based monitoring and a central DSA Enforcement Infrastructure. The objective was to maximize coverage of the area of enforcement, maximize coverage of channels and to ensure reliable detection of spectrum access violation by selecting highly *qualified* volunteers. We proposed to maximize the coverage of the region of enforcement by following a divide-and-conquer mechanism wherein we divide the area of enforcement into smaller regions, by applying the Lloyd's algorithm, which is a relaxation to the Voronoi algorithm. Every small region in the enforcement area is responsible for its own spectrum enforcement, which in turn ensures enforcement of the entire area. The qualification of a volunteer for the upcoming time interval is decided by its likelihood to stay in the region over the next monitoring interval and by its trust. We explored different ways to aggregate the two parameters of location likelihood and trust to find the best combination for calculating 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. We also developed a mechanism to efficiently assign channels to the selected volunteers for monitoring. We observed the efficacy of the proposed algorithm for assignment of channels and proposed a methodology by which it can be further improved. Finally, we studied the variations in mean accuracy of detection and mean hit ratio as the probability of a volunteer

to be corrupt changes and the mobility pattern of a volunteer changes.

We plan to extend this work to explore different mechanisms to select volunteers for multi-channel spectrum enforcement. We further plan to explore machine learning based methodologies to determine the trust 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] D. Das, T. Znati, M. Weiss, P. Bustamante, M. Gomez and S. Rose, "Crowdsourced Misuse Detection in Dynamic Spectrum Sharing Wireless Networks," International Conference on Networks (ICN), 2019, pp. 74-81.

[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: 30 Aug. 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] S. Shavell, "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] X. Zhu, J. An, M. Yang, L. Xiang, Q. Yang, and X. Gui, "A Fair Incentive Mechanism for Crowdsourcing in Crowd Sensing," IEEE Internet Things J., vol. 3, no. 6, Dec. 2016, pp. 1364–1372.

[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] G. Kamath. *Advanced Algorithms, Matroid Secretary Problems.* [Online]. Available from: http://www.gautamkamath.com/writings/matroidsec.pdf. [Accessed 30 Aug. 2019].

[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/. [Accessed 30 Nov. 2018].

[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] C. Bettstetter, H. Hartenstein, and X. Pérez-Costa, "Stochastic Properties of the Random Waypoint Mobility Model," Wirel. Networks, vol. 10, no. 5, pp. 555–567, Sep. 2004.

[25] CNBC. *Fastest Road in America: 85 MPH and We May Be Going Even Faster.* [Online]. Available from: https://www.cnbc.com/id/49520151. [Accessed 30 Aug. 2019].

[26] RidingBoards. *Average Skateboard Speed: How Fast Do We Ride?* [Online]. Available from: https://www.ridingboards.com/average-skateboard-speed/. [Accessed 30 Aug. 2019].

[27] D. Das, T. Znati, M. Weiss, S. Rose, P. Bustamante and M. Gomez, "Spectrum Misuse Detection in Cooperative Wireless Networks," 17th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2020, in press.

[28] M. Khaledi, M. Khaledi, S. Sarkar, S. Kasera, N. Patwari, K. Derr, and S. Ramirez, "Simultaneous Power-Based Localization of Transmitters for Crowdsourced Spectrum Monitoring," 2017, pp. 235–247.

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

[30] J. Tang and Y. Cheng, "Selfish misbehavior detection in 802.11 based wireless networks: An adaptive approach based on Markov decision process," 2013 Proceedings IEEE INFOCOM, Turin, 2013, pp. 1357-1365.

[31] G. Atia, A. Sahai and V. Saligrama, "Spectrum Enforcement and Liability Assignment in Cognitive Radio Systems," 2008 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, Chicago, IL, 2008, pp. 1-12.