"See Something, Say Something" Crowdsourced Enforcement of Spectrum Policies

Aveek Dutta, *Member, IEEE*, and Mung Chiang, *Fellow, IEEE*

***Abstract*—As sharing agreements are being ratified by the Federal Communications Commission (FCC) for various spectrum bands for commercial broadband use, it also opens up an equally challenging problem of enforcing these policies. The efficacy of an enforcement system greatly depends on the accuracy of evidential information and the speed of adjudication. The inherent unguided and unbounded nature of radio wave propagation allows spectrum infractions to cause widespread damage and makes it hard to locate at the same time. On the other hand, it also lends itself to distributed methods for efficient enforcement of spectrum etiquette. We leverage a crowd of mobile users to implement a paradigm of "eye-witness" for detecting violations of spectrum policies. We design and analyze the crowdsourced enforcement architecture and show three main results: 1) it detects an infraction with a consistent high degree of accuracy (> 90%); 2) it is able to accurately locate the source of infraction and 3) it lowers the frequency of policy infractions over time.**

***Index Terms*—Crowdsourcing, data fusion, distributed fault tolerance, enforcement of spectrum policies, inspection game, localization, mobile systems, signal detection, tiered spectrum sharing.**

I. Introduction

THE MAIN goal of an enforcement system is to maintain a fair and rightful usage of a shared commodity. Wireless spectrum is one such commodity that is shared among various devices, typically owned and operated by either federal, civilian or commercial entities. For licensed bands, owners of a swath of radio frequency are protected from encroachment by granting exclusive rights to communicate within that part of the spectrum. The proposed spectrum sharing architecture in the PCAST report [1] and the subsequent rule-making efforts that followed, is a marked revision from this paradigm of exclusive spectrum rights. The tiered sharing model [2] requires novel rules to support coexistence of licensed as well as unlicensed, opportunistic devices within the same frequency band and, if possible, at the same time. Therefore, it is important that devices with higher access priority (Tier-2) are protected from lower tier (Tier-3) devices, often at fine granularity of time and space. While architecting these rules remain one of the open problems, in this paper, we choose to address the other important half of this novel paradigm, which is enforcement of spectrum rules in an efficient manner, specifically for opportunistic users defined as Tier-3 in the proposed licensing model by the FCC.

We introduce the term *"eye-witness"* in the domain of spectrum enforcement by leveraging the power of the *"crowd"*, defined as devices that are also operating in the same part of the spectrum. The objective of such a method is to observe a frequency band for policy-violations and, if an anomaly is detected, report it to the appropriate law enforcement agency for adjudication. Using these accounts as evidence, the spectrum law enforcement agency is able to detect, identify and establish a chain of custody to bring a violator to justice with high accuracy. However, the credibility of such evidence depend on two key metrics: 1) the *proximity* of the eye-witness to the actual scene of the incident, (especially if it is short-lived like hit-and-run accidents) and 2) the *quality* of the evidence, which depend on the individual's ability and willingness to accurately witness and record the event.

In case of radiowaves, attenuation over free space and other objects in the path of the wavefront alters the signal such that the same event (violation of rules) is observed with different intensity by various detectors in the vicinity. Specifically, the credibility of the eye-witness account is proportional to the signal to noise ratio (SNR) of the received signal.

Figure 1a shows an example of the tiered spectrum sharing. A violation occurs when a Tier-3 client creates harmful interference to the Tier-2 clients. This can be a result of non-compliance to geographical exclusion zones (as shown in Figure 1a) or specific waveform and signal attributes defined for various tiers of networks. Figure 1b shows the dissipation of the signal power from an infraction over a geographical area which is received by other users at different strengths. Processing signals for spectral violation at different SNR translate to specific measures of detection and false positives. Figure 1c shows the functional blocks of an enforcement system. Enforcement involves many steps and this paper focuses on the aggregation and interpretation of the eye-witness accounts. We present an efficient method to aggregate this variety of observations to increase the credibility of the evidence and also locate the source of infraction with high accuracy. Our analysis shows that this form of crowdsourced enforcement is also beneficial over planned and static deployments. This is particularly true because it is almost impossible to have complete coverage due to undesirable high cost of enforcement. Along with high operating and maintenance cost of this infrastructure, an infraction may happen farther away from the static detectors diminishing the overall accuracy of the evidence. As is typical in fog networking, using the crowd of "eye witness" devices, we increase

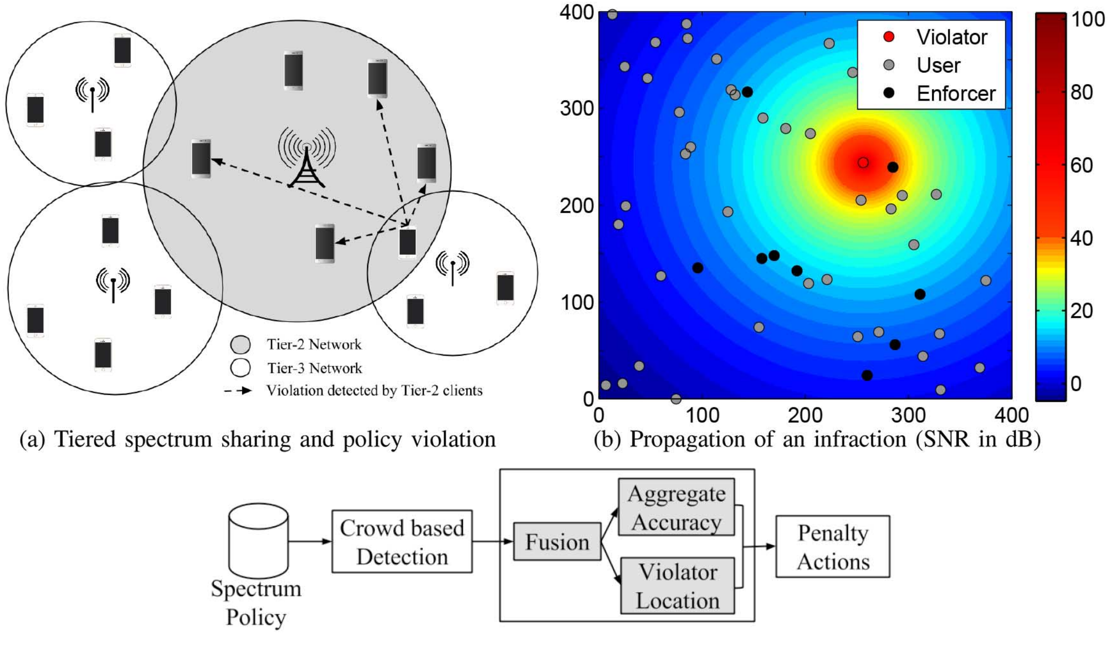
Manuscript received January 8, 2015; revised May 14, 2015 and July 23, 2015; accepted July 23, 2015. Date of publication August 11, 2015; date of current version January 7, 2016. This work was supported in part by NSF NeTS under Grants 1011962, 1318607, and 1456847. The associate editor coordinating the review of this paper and approving it for publication was Dr. Tommaso Melodia.

A. Dutta is with the Department of Electrical Engineering and Computer Science, The University of Kansas, Lawrence, KS 66045 USA (e-mail: aveekd@ku.edu).

M. Chiang is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08540 USA (e-mail: chiangm@princeton.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2015.2466550



(a) Tiered spectrum sharing and policy violation

(b) Propagation of an infraction (SNR in dB)

(c) Functional blocks of crowdsourced enforcement

Fig. 1. Crowdsourced enforcement of spectrum policies: a) Networks coexist in time, space and frequency but are separated based on policies and exclusion zones. b) A signal that violates a spectrum policy (Violator) propagates to the members of the *crowd* (User) and a subset of the users (Enforcer) detect that at different SNR. c) The Enforcers forward these *eye-witness* accounts for aggregation to the law enforcement agency to improve the credibility and localize the source (Violator). The shaded boxes are the modules that this paper focuses on.

the chances of being closer to the violation event and collecting measurements faster, leading to better evidence.

Another dimension to the general problem of enforcement is the cost of enforcement. Although the cost of participating in enforcement by a member of the crowd is best understood by itself, the marginal utility as observed by the enforcement agency is also important for evaluating the efficacy. We model and analyze the cost of enforcement using game theoretic methods to measure the relative payoffs of the participants and the enforcement agencies.The central goal of this paper is to provide a practical, cost-effective solution for enforcing spectrum laws by leveraging the ubiquity and ever-increasing computation resources of mobile devices:

1) We architect and design a crowdsourced enforcement system for improving the accuracy of detection of spectrum infractions in DSA – §II.
2) We present a data-fusion algorithm to improve the probability of detection while reducing the likelihood of false positives for an infraction and compare its performance to static enforcement schemes – §III.
3) We present a computationally efficient method to identify and localize the source of infraction with high accuracy – §IV.
4) We extend the scheme to detect multiple violations and violations caused by mobile users – §V and §VI.
5) Lastly, we measure the cost of enforcement and the reduction in the frequency of infraction over time – §VII.

The rest of the paper is organized as follows: In §II we introduce the concept of eye-witness and present the methodology. §III we aggregate witness reports to improve the accuracy of the detection using practical simulation. enforcement required in practical situation. In §IV we present a technique to locate the source of infraction using crowdsourced information. We further extend the scheme to detect multiple, simultaneous infractions in §V and when violators are mobile in §VI. §VII presents a model to analyze the cost of enforcement using our technique. In §VIII, we discuss steps to further improve the overall performance of this system. Finally, we present prior work in this area in §IX and conclude in §X.

II. Crowdsourced Enforcement

In the realm of spectrum enforcement, there are three entities that are important:

a) The *"Violator"*, whose objective is to act greedy and violate spectrum policies. This may also include harmful acts like denial of service and jamming attacks as well. In this paper, we focus on the violations that leverage the physical layer of the device. Emulating a higher priority user or the incumbent using signatures like cyclostationary features that are embedded in the radio signal is an example of such infraction. Sometimes, these infractions may not be intentional as in the case of faulty hardware that may lead to unwanted spectral leakage. Such actions will alter the signal characteristics causing harmful interference to rightful users of that band.

b) The *"Enforcer"*, who is interested in locating and assigning liability to the Violator. In this paper, we define the rightful users of a frequency band, who are willing to participate in detection and localization of spectrum infractions, as Enforcers. It is assumed that each Enforcer will be provided with a set of rules to check for infraction and are equipped with the corresponding detectors either in hardware or software [3], [4]. The main incentive of participation is in lowering the *hostility* in the radio environment, allowing legitimate users (like themselves) to operate at their peak performance. In that sense, the members of the crowd watch out for each other by protecting the spectrum from encroachment.

c) The *"Policy-maker"*, who has the authority to collect evidential proof from the Enforcers and adjudicate on the infraction and levy monetary or other forms of penalty to the Violator. The FCC and the Department of Justice (DoJ) are examples of such entities.

Why Crowdsourced and not Just Static?: As a part of the rule-making process by the FCC, it has been mandated that mobile nodes under the Tier-3 category will have to share the band with users of higher priority (Tier-2) and certainly the incumbent of that band (Tier-1). This opportunistic mode of access engenders greedy and often rogue behavior, which will cause interference to users of higher priority. These rules may have many dimensions of control like, maximum transmit power, spectral mask, directionality, waveform signatures or even higher layer attributes. In this work, we assume that such rules are already defined and deployed for a frequency band. Our focus is on measuring and quantifying if those rules are being adhered to.

We envision that networks, comprised of Tier-3 users will be relatively short range, in the order of few hundreds of meters. This is a practical assumption as larger distances will induce higher transmit power causing widespread interference to neighboring networks sharing the same frequency band. A typical Tier-3 radio, similar to TV band devices will have no more than $40mW$ [5] of transmit power, which makes a spectrum infraction harder to detect with desired accuracy unless the detector is in the vicinity of the infraction. While deploying static detectors at every Tier-3 Access Points (AP) is a plausible solution, it is highly likely that policy violation events are farther away from static detectors leading to false positives. The cost of deploying such infrastructure and maintaining it for desired coverage can be too high for practical purposes. Also, localizing the violator require multiple static Enforcers to coordinate their actions increasing communication overhead. We discuss such comparisons in §III.

Signal Detection and Accuracy: The capability of the detection depends on many factors, *e.g.*, RF front-end, processing power, processor load, battery constraints, etc. In that sense, the devices are heterogeneous in their detection capabilities and that greatly influence the efficacy of the system. The accuracy of detection also depends on the SNR of the received signal which is equivalent to the proximity of the *eye-witness* to the infraction.

Detecting an infraction can happen at different levels of granularity, and aggregating many observations over a wide geographical area provides better visibility. Signal detection can be represented as a hypothesis test where hypotheses are either confirmed or rejected based on certain pre-determined thresholds. Each threshold corresponds to a unique combination of detection accuracy and false-positives. We define these thresholds as *Operating Points (OP)*, which is chosen by an Enforcer to detect spectrum infractions. These attributes of a detector is collectively captured using the Receiver operating Characteristics (RoC). The RoC contain two key parameters that determine the quality of an eye-witness account: 1] Probability of Detection (P_d): This provides a measure of the fraction of events that are correctly classified as a violation of spectrum policies and 2] Probability of False-positive (P_f). Figure 2 shows the RoC for detecting a deterministic signal in white Gaussian noise using the Neyman-Pearson optimality criterion for various SNRs [6] as an example. In practice, each Enforcer will have the RoC to detect a particular type of infraction. Using RoC as the pivot, we design and evaluate the crowdsourced enforcement system. This also makes this method widely applicable to a variety of infractions as long as the corresponding RoC is available to the Enforcer[1].

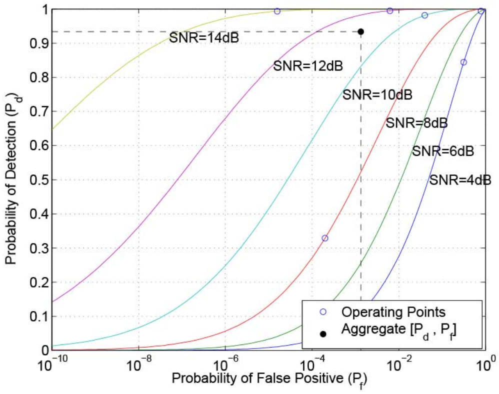


Fig. 2. Receiver operating Characteristics (RoC) for an energy detector. Each Enforcer chooses a different operating point on the RoC curve corresponding to the SNR of the received signal and internal constraints. The Policy-maker aggregates these data points to converge on an accurate estimate of $[P_d, P_f]$.

III. Accuracy of Crowdsourced Enforcement

An Enforcer turns on a specific detector and an infraction event is reported to the Policy-maker using the quadruplet: $[P_d, P_f, SNR, loc]$, for that and the chosen OP will be different for each Enforcer. In this work, we assume that unless specified by the Policy-maker, Enforcers are free to choose any operating point based on constraints that are best understood by itself. Examples of such constraints include, remaining battery, available resources and activity level of the user. Consequently, the detection results from the crowd will vary over a wide range and careful aggregation is important to draw intelligent inference. The participation phase is followed by the data aggregation phase. The purpose of this phase is to improve the accuracy of detection and reduce false positives at the same time. There are three possible ways to aggregate OPs:

1) Pick the best: The OP consists of two metrics, P_d and P_f. Since these points are chosen by the Enforcers based on their internal constraints, the Enforcer providing the best P_d may not provide the best P_f. Therefore, comparing two OPs is difficult.

2) Simple Mean: Averaging is one way to combine the points. But, the heterogeneity of the OPs makes it difficult to improve the aggregate $[P_d, P_f]$ as smaller values adversely affect the mean value.

[1] Policies enforced beyond the radio access network like billing, subscription and usage rights, are beyond the scope of a RoC. In such cases the the crowd can raise *warning flags* to the Policy-maker who performs further policy-checks. Also, with additional information from the Policy-maker, the crowd is to be able to localize the Violator as discussed in §IV.

Algorithm 1. Aggregate $[P_d, P_f]$ at the Policy-maker

```
1  Function calculatePdPf(PdPfSnrLoc)
2      topEnforcers = getRequiredTopEnforcers();
       // sort on $P_d$, followed by $SNR$
3      sorted_on_Pd = sort(PdPfSnrLoc, 1, 3);
4      best_Pd = sorted_on_Pd[0 : ($topEnforcers - 1$)];
       // inverse sort on $P_f$, followed by SNR
5      sorted_on_Pf = inverseSort(PdPfSnrLoc, 2, 3);
6      best_Pf = sorted_on_Pf[0 : ($topEnforcers - 1$)];
7      bestEnforcers = unique(best_Pd ∪ best_Pf);
8      $P_{d_{aggregate}} = \frac{\sum_{i \in bestEnforcers} round(10 * P_{d_i}) \times P_{d_i}}{\sum_{i \in bestEnforcers} round(10 * P_{d_i})}$;
9      $P_{f_{aggregate}} = \frac{\sum_{i \in bestEnforcers} round(\ln(P_{f_i})) \times P_{f_i}}{\sum_{i \in bestEnforcers} round(\ln(P_{f_i}))}$;
10     return $[P_{d_{aggregate}}, P_{f_{aggregate}}]$;
11 end
```

TABLE I
SIMULATION PARAMETERS

Parameters	Value/Model
Area	$400m$ x $400m$
Population Distribution	Uniform
Population	$[50, 100, 150]$
Enforcement Fraction	$[0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7]$
topEnforcer (T)	$[1, 2, 3, 5, 7, 9]$
Propagation	Hata-Urban Model [8]
Transmit Power (P_t)	$40mW$
Carrier Frequency (f)	$600MHz$
Tx/Rx height (h_B/h_M)	$1.5m$ (Handset height)
Detector/RoC	Neyman-Pearson detector [7]

3) Weighted Mean (Algorithm 1): Instead of treating all the OPs equally, we use pre-determined weights for P_d and P_f. By assigning higher weights to higher values of P_d and smaller values of P_f, the accuracy of the system is improved. The weights are generic enough to be applied to a variety of RoCs. Typically false positives are reported in logarithmic scale and hence we use a log-linear function to compute the weights for P_f while the weights of P_d are linear. The weighted mean is computed in lines 8−9 of Algorithm 1. The *rounding* function provides linear weights in discrete steps. These weights are static assignments based on the fact that the Policy-maker has complete trust in the reported OP and analyzing the effect of distrust of Enforcers is out of scope of this paper. This method does not rely on the closest (highest SNR) eye-witnesses because that node may choose to operate at an OP that provides low P_d and high P_f values, which is clearly undesirable. A weighted average over all Enforcers allows the Policy-maker to increase the confidence in P_d and P_f which is more desirable than relying on one observation and leading to either indicting the wrong entity or incurring large cost by pursuing a false positive. The heterogeneity of nodes in SNR and the OPs ensure a wider coverage and aggregating these observations lead to accurate estimate of the presence of an infraction. In the following section we provide a method to further improve the aggregation of OPs.

A. *Too many Enforcers may not be desirable*

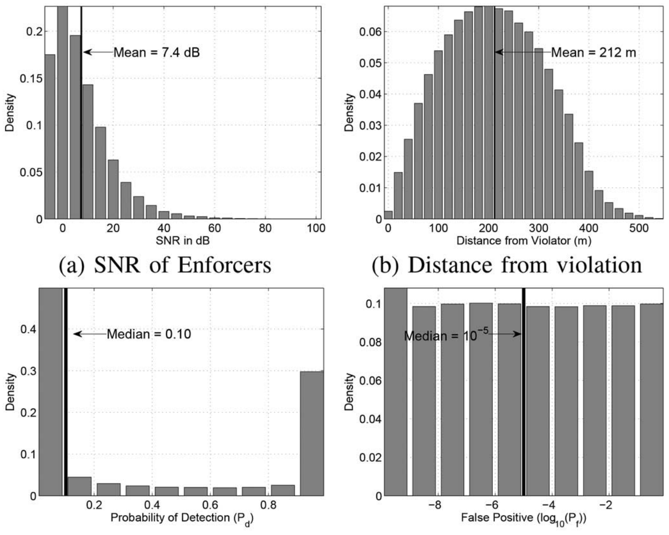
A general perception exists in aggregating crowdsourced information, that more number of unique participants will provide better aggregate result. We show that higher number of Enforcers does not lead to higher aggregate values of $[P_d, P_f]$. Since the reward to the Enforcer is strictly dependent on the chosen OP on the RoC curve, the Policy-maker should make careful decision as to who is to be compensated for the enforcement services. Therefore, we incorporate an additional step before computing the weighted mean outlined in lines 2−7 in Algorithm 1.

We define a decision parameter, topEnforcer (T), which specifies a subset of witness accounts ($[P_d, P_f]$) chosen from the total set of participating Enforcers. We assume that the Policy-maker will provide this value as shown in line 2. In the following step, the OPs obtained from the Enforcers are sorted separately on P_d and P_f. From each of the sorted lists, T number of OPs are selected. Since, some Enforcers may provide good values for both P_d and P_f, only unique Enforcers are chosen from this set. These OPs are used to compute the weighted mean to produce the aggregate values of $[P_d, P_f]$ as shown in lines 8−9. If two Enforcers report the same values of P_d or P_f the Enforcer that operates at a higher SNR is chosen. This is useful for two reasons: from Figure 2 it is evident that for the same value of P_f a higher value of P_d is obtained if signal is detected at a higher SNR. This is also true for P_f as well. Secondly, this increases the likelihood of finding a node with both high P_d and low P_f.

The main purpose of this step is to make sure that the Policy-maker is only taking the relatively better Enforcers among the participants. This also prevents unwanted compensations to Enforcers whose OPs are not useful for improving the detection accuracy. This method has an added incentive for the crowd to participate, because even though an Enforcer operates at a relatively weak SNR, it may be able to detect at a relatively high OP. Therefore, participating in enforcement is always desirable because it might be the best OP among all the participating Enforcers. This is another apparent counter-intuitive feature of this paradigm which makes it a lucrative solution for enforcement. We illustrate the efficacy of the aggregation using practical simulations and highlight the various facets of the technique.

B. *Evaluation of accuracy*

Table I shows the parameters and models used for practical simulations. We assume that there is one Violator in the geographical area at a time. It is also assumed that both the Violator and the Enforcer are using omni-directional antennas. This makes it harder to detect and localize a Violator because from a communication standpoint, beamforming increases spatial reuse and reduces interference, which is beneficial for dense sharing of spectrum. However, if the Violator intentionally beamforms in the direction of the Tier-2 clients, it will not



(a) SNR of Enforcers

(b) Distance from violation

(c) P_d of the chosen OPs

(d) P_f of the chosen OPs

Fig. 3. Distribution of data in simulation: Wide variety of SNR and OP shows heterogeneity of the crowdsourced detection.

be able to communicate with its AP, which is not a desired outcome for a Violator. Hence we use onmi-directional propagation as it models a more realistic violation.

Figure 3 shows the distribution of simulation data for 100 topologies. To analyze the effect of T, we keep the population and the participating Enforcers as constant, which is chosen as a fraction of the population (denoted by Enforcement Fraction in Table I). Figures 3a and 3b shows the distribution of received SNR and distance from the Violator with an average of 7.4 *dB* and 212 *m* respectively for all Enforcers and topologies. Also, Figure 3c and 3d shows the distribution of the OPs chosen by the Enforcers with median P_d and P_f being 0.1 and 10^{-5} respectively. Apparently, the distribution of OPs looks weak to accurately detect the violator. This is where the power of a crowdsourced enforcement and centralized aggregation lies.

Figure 4 shows the data aggregation based on Algorithm 1. Figures 4a and 4b shows the variation of the weighted mean of all the Enforcers (before sorting on OPs) participating in enforcement. The median value for P_d is approximately 0.9, which is encouraging. It is clear that increasing number of Enforcers does not translate to an increase in accuracy of detection after a certain point. It also shows the inter-quartile range, which decreases as the number of Enforcers increases. This is primarily because, with more Enforcers, there is a higher likelihood of good OPs, reducing the dispersion in OPs while the weighted mean maintains the accuracy. Similar trends are visible in false positives, as shown in Figure 4b with median value of 0.004. Both the values for P_d and P_f are convincing in terms of motivating the Policy-maker to take action on the Violator.

Figures 4c and 4d show the detection accuracy, when $T = 5$ is chosen for computing the weighted mean. This is considered as the minimum level of enforcement in our simulations (10% of the minimum population, which is 50). The detection accuracy improves significantly when only the "best 5" Enforcers are chosen. This is because the choice of an OP is an independent decision of an Enforcer and that the Policy-maker will have to make decisions based on what is provided to it. Figure 4e shows the average number of unique Enforcers selected after the sorting phase. We observe that with increase in number of Enforcers, the number of unique participants also increases. This is because the likelihood of finding an Enforcer with both high P_d and low P_f drops with the increase in the number of Enforcers as it induces more heterogeneity in OP. Therefore, from Figure 4, we see that instead of aggregating the results from all the Enforcers, it is desirable to select a subset of those that provides the best combination of P_d and P_f.

C. Desired level of enforcement

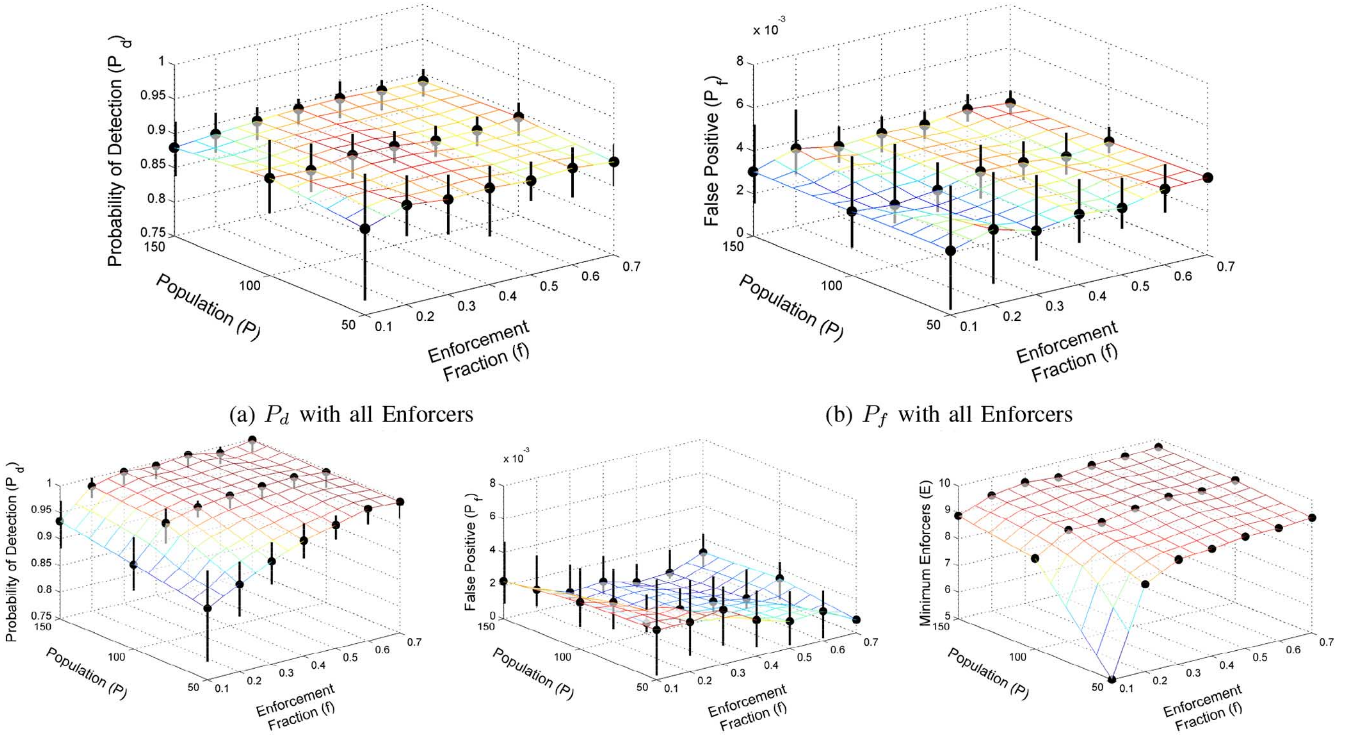
In order to focus on the desired level of enforcement for different population densities, we highlight the results of varying T. It is apparent from Figure 5a that the number of Enforcers is almost always greater than T. This is because the heterogeneity of OP makes it harder to find the same Enforcer with the best P_d as well P_f. Figures 5b and 5c shows the reduction in accuracy with an increasing T. It is also evident that a weighted mean of the $T = 1, 2, 3$ provides the best aggregated values of P_d and P_f. This is desirable if the Policy-maker has complete trust in all the Enforcers selected and that those are truthful. The trends shown in Figure 5 is crucial in determining a desired level of enforcement under varying degree of trust and reputation on part of the Enforcers.

Although trust models are out of scope of this work, we provide a blueprint for a Policy-maker to decide on the level of enforcement if and when such models are available. In other words, under an ideal scenario with complete trust and high reputation picking $T = 1$ is the desired choice. However under lack of trust and reputation, the Policy-maker may employ $T > 1$ as an enforcement strategy. We also find that with increasing density of Enforcers, aggregate value of P_d and P_f improves. Under this scenario we can certainly claim that more number of Enforcers is better for the Policy-maker, because it increases the likelihood of aggregating better OPs. This is also a useful tool to optimize the cost of Enforcement against the accuracy of detection.

D. Comparing with static enforcement

Enforcing spectrum rules using static detectors at fixed locations is also a plausible architecture. Figure 6a shows a topology where static Enforcers are located at the vertexes and at the center of the opposite side of a square block. This architecture provides wide coverage as each can be shared with the neighboring block as well. A static node can be mandated to operate at a certain OP. So, we fix the false positive to the mid-point of the range of P_f values supported by the RoC, which is 8×10^{-6} for the RoC chosen in this work (Figure 2). Using algorithm 1 and the same propagation model we compare the aggregate detection accuracy with the results obtained for $T = 3$ for crowdsourced enforcement.

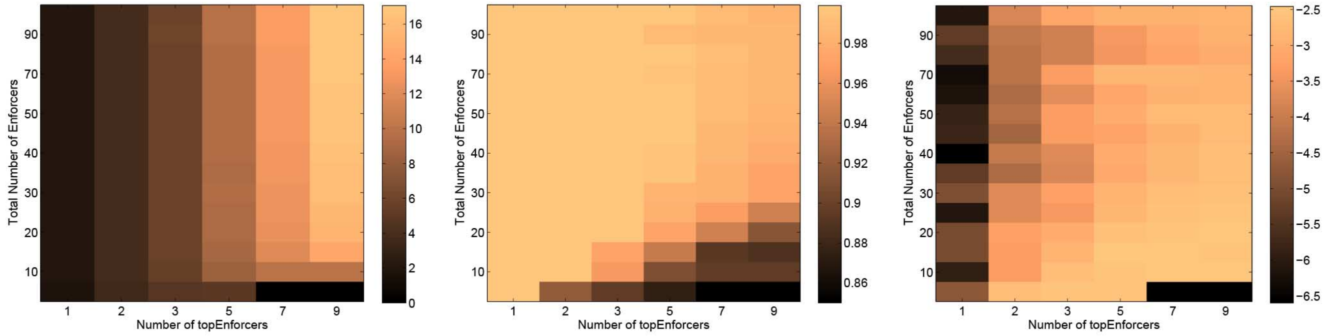
In Figure 6b, we show that the percentage improvement in the median value of P_d for various Enforcer densities. For



(a) P_d with all Enforcers (b) P_f with all Enforcers

(c) P_d for $T = 5$ (d) P_f for $T = 5$ (e) Unique enforcers: $T = 5$

Fig. 4. Aggregate $[Pd, P_f]$ with varying population and enforcement fraction: Aggregating OPs provides better accuracy of detection than individual Enforcers. Accuracy is further improved using topEnforcer (T) instead of all the participants.



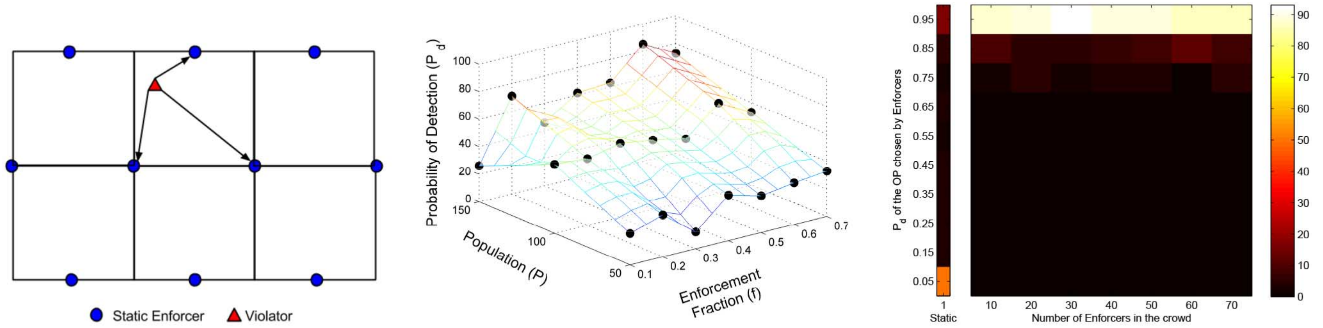
(a) Unique Enforcers (b) Aggregate P_d (c) Aggregate P_f

Fig. 5. Detection accuracy with varying T: Better detection accuracy is achieved with smaller number of T.

higher enforcement densities, the crowd significantly outperforms the static architecture. This is simply because the relative distance from each Enforcer ($mean \approx 285\ m$) is much greater than that in the crowdsourced paradigm, where the possibility of closer (or high received SNR) Enforcer with a good OP is much higher. It is also insightful to compare the best OPs obtained in the two cases. Figure 6c shows the spread of the detection probabilities for $T = 1$ for both the scenarios. For the static enforcement, we find that the best OPs are equally split between very low (< 0.1) and very high (> 0.9) values for P_d. This is strictly attributed to the large distance and much lower received SNR ($mean \approx 1\ dB$). While in the case of the crowd-based enforcement, most of OPs are very high (> 0.9), which guarantees a higher accuracy. To tackle this problem, static enforcement will have to upgrade to low-power detectors, which will incur additional cost. Thus crowdsourced enforcement is not only more accurate, but also cost-effective compared to static scenarios.

IV. Locating the Source of Infraction

Locating the source of infraction is accomplished by utilizing the knowledge of the propagation characteristics for a particular geographical area. The received SNR of the signal being detected depends on the path loss of the channel between the Violator and the Enforcer and also on the mandated transmit power (P_t) for that class of device. The average noise floor (NF) for a short range communication, similar to 802.11a/g,



(a) Static enforcement (b) Improvement in P_d (c) Range of OP for static and crowd

Fig. 6. Comparison with static enforcement: Crowd performs better than static with increasing density of Enforcers.

is approximately −96 *dBm* [8]. Thus the path loss (L_u) experienced by the infraction signal while propagating to the receiver antenna of the various Enforcers is computed using 1.

$$L_u(dBm) = P_t(dBm) - SNR(dB) - NF(-96\ dBm) \tag{1}$$

After estimating the path loss, an inverse mapping, using the path loss model provides an estimate of the distance to the transmitter or the Violator. Based on the parameters chosen for evaluation in Table I, using the Hata-Urban pathloss model [9] and the correction factor (C_h) for large cities the distance to the Violator ($\hat{d}$) in meters is given by 2.

$$C_h = 3.2 \times (log_{10}(11.75 \times h_M))^2 - 4.97 \tag{2a}$$

$$exp = (L_u - 69.55 - 26.16 \times log_{10} f + 13.82 \times log_{10} h_B + C_h)/(44.9 - 6.55 \times log_{10} h_B) \tag{2b}$$

$$\hat{d} = round(10^{exp} \times 1000) \tag{2c}$$

However, there are various sources of error in this method of estimation. The two major sources of error are: 1) Receiver sensitivity, and 2) Accuracy of the path loss model. Receiver sensitivity is largely attributed to the duration of measurement and the dynamic range and linearity of the analog and digital components of the RF front-end. Therefore, it is practical to add measurement error around the SNR reported by the Enforcers which is reflected in the path loss (L_u) in 1 and the estimated distance ($\hat{d}$) computed using the propagation model in 2.

Algorithm 2 shows the various steps in locating the Violator. This is computed at the Policy-maker and utilizes the same data structure obtained as responses from the Enforcers, denoted by *PdPfSnrloc*. Although, the Enforcers are required to report their location to the Policy-maker, it needs to be anonymous for privacy reasons. However, anonymity of Enforcers does not affect the performance of the system. Also, in the absence of positioning systems like GPS, such as indoor locations, AP based localization techniques [9] can be used to map into global coordinate space. Furthermore, if the the Tier-2 network is based on the cellular architecture, anonymous location information is already built into such systems, which can be readily utilized in this method.

The first step is to select "three" Enforcers that are closest to the Violation. In other words, the responses from the participating Enforcers are sorted in descending order of SNR and the top three Enforcers are chosen, as shown in lines 3−4. This is followed by the addition of error to the reported SNR from each Enforcer, to compensate for receiver sensitivity variations and inaccuracy of the path loss model. We model the estimation error as a zero mean Gaussian random variable with a standard deviation of 2 *dB* and is generated using the function call in line 6. The function call returns an upper (s_{max}) and lower limit (s_{min}) of the error, which is added to the reported SNRs. In practice, the SNRs are reported as an average of multiple observations and adding error around this reported value provides a range of SNRs observed, which is useful for estimating the distance to the Violator. The next step is to calculate the distance to the Violator using the path loss model in Table I. This is performed using function calls with the upper and lower limits of the SNR as shown in lines 7−8. This function returns two distances, innerC and outerC. The path loss exponent is computed using (2) before computing the distance within this function as well in lines 7−8. This provides an upper and a lower bound for the distance to the Violator. Since the error is modeled as a random variable, we do not impose additional dependence of the error on the SNR of the received signal. This adjustment in performed for the three Enforcers, providing three annular regions as shown in Figure 7a because of the assumption that both the Violator and the Enforcers use omni-directional antenna. We term this annular regions as Zone of Coverage (ZoC). The coordinates that define the ZoC for each Enforcer is obtained using a function call with radii of the inner and outer circles and the location of that Enforcer as argument, as shown in line 10.

In computing the ZoC, it is always beneficial to choose the Enforcers that are operating at high SNR. Since, the estimated distance to the transmitter depends on the path loss exponent as shown in 2, for the same amount of estimation error (lines 8−9) the ZoCs are bigger for Enforcers receiving at lower SNR. For example: Two Enforcers have detected the same event at 5 *dB* and 15 *dB* respectively. If the same amount of estimation error is added to both the Enforcers, then the ZoC of the Enforcer detecting at 5 *dB* SNR will be larger than the Enforcer detecting at 15 *dB*. This is because the path loss is higher for Enforcers detecting with low SNR and it appears as an exponent for computing the distance ($\hat{d}$), which results in unequal ZoCs for Enforcers detecting at different SNR.

The three ZoCs overlap in space, and Figure 7a shows a two dimensional projection of the overlapped area. Using this

Algorithm 2. Algorithm to determine the ZoE

```
1  Function getZoneOfEnforcement(PdPfSnrLoc)
2      topSNR = 3;
       // sort based on third element, $SNR$
3      sorted_on_SNR = sort(PdPfSnrLoc, 3);
4      topN = sorted_on_SNR[0 : $topSNR - 1$];
5      for $i = 0$ to $topSNR - 1$ do
           // Add error in SNR estimation
6          [$s_{max}, s_{min}$] = chooseError();
           // Calculate distance from pathloss model
7          innerC = getDistance(topN[i][3] $- s_{min}$);
8          outerC = getDistance(topN[i][3] $+ s_{max}$);
           // Store location and Radii of circles
9          circles[i] = [topN[i][4], innerC, outerC];
           // Compute inner and outer circles points
10         circPts[i] = getCircPoints(loc,innerC,outerC);
11     end
12     cmnPts = [];
13     for $i = 0$ to $topSNR - 1$ do
14         j = mod(i + 1, topSNR);
15         k = mod(i + 2, topSNR);
           /* For each point of both circles of node
              i, check if it is inside the annular
              rings of nodes j and k                   */
16         pts = getCmnPts(circPts[i], circles[j], circles[k]);
17         cmnPts = [cmnPts, pts];
18     end
19     return getArea(cmnPts);
20 end
```

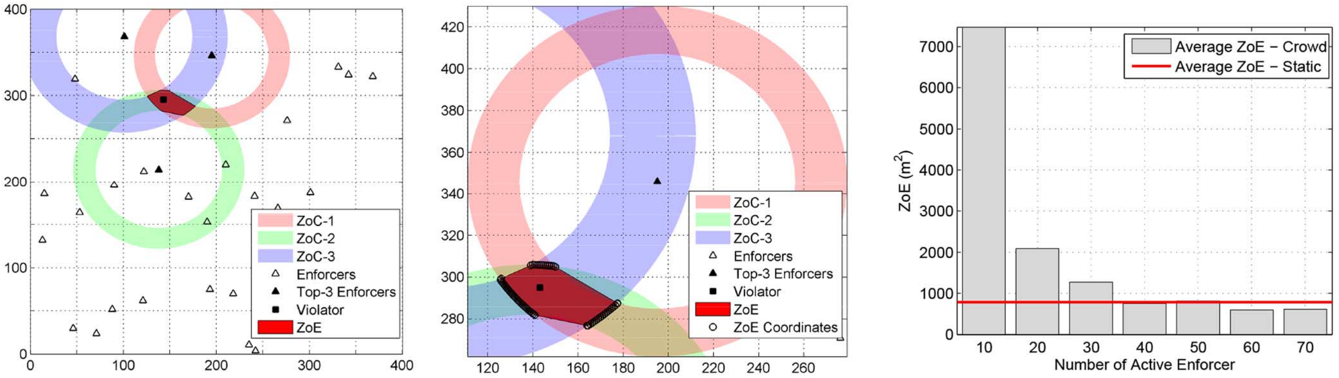
technique, we show that the Violator will always fall within the overlapped ZoCs. The error about the ideal distance is a combination of the inaccuracy in the path loss model, receiver heterogeneity and other noise sources. This makes the ZoC an annular region rather than a circle. We call the overlapping zone of the three ZoCs as the Zone of Enforcement (ZoE). This is the geographical area that needs to be patrolled specifically to look for the source of infraction. The efficacy of this technique depends on the size of the ZoE and a smaller variance in error will result in a smaller ZoE. From an enforcement standpoint, the Policy-maker has to deploy its resources based on the geographical coordinates of the ZoE. This is obtained as follows: *for each inner and outer circle points of the ZoC of an Enforcer, find the points that lie within the ZoC of the other two Enforcers*. Lines 14−20 in Algorithm 2 outlines the steps and Figure 7b shows the ZoE that encompasses the Violator. The common points are obtained via function call at line 16 of Algorithm 2.

This technique requires exactly three Enforcers with the highest SNR instead of all the participants. This is because, if two Enforcers are used, there is a possibility that the ZoCs overlap at more than two locations. This will create ambiguity at the Policy-maker as it creates more than one ZoE, making it harder to locate the Violator. Therefore, adding the third Enforcer, ensures that there is only one ZoE. The randomness of the crowd also has the added advantage that Enforcers are scattered around the source of infraction as shown in figure 7a leading to a small ZoE. The area enclosed by these coordinates is given by the convex hull of the common points and is a measure of localization accuracy (line 19). This method is also computationally efficient and provides a smaller search space compared to other known localization techniques, while utilizing only three Enforcers that are closest to the source of infraction.

The accuracy of this method depends on the accurate estimation of the distance between the Violator and the Enforcers. We argue that since we are utilizing the observations of Enforcers that detects with the highest SNR, it makes the estimation accurate because the possibility of multipath components overwhelming the average time-domain SNR is much lower. In a rich multipath environment, path resolution using multiple antenna is a suitable solution and the SNR of the direct path should be chosen for selecting the Enforcers. Also, the variance of the error term can be increased to make sure that the ZoC encompasses the Violator. This error term can be considered as a system design parameter to balance accuracy versus enforcement cost. The ZoC is computed based on the knowledge of the transmit power (P_t) of the Violator. This is a valid assumption because from a hardware standpoint, power amplifiers and related circuitry of the Tier-3 transmitter can be mandated to operate at fixed power levels in form of secure firmware that may not be accessible from the user space. This is also practical in light of tight policies that will be in place for the sharing scheme to work effectively. However, if a Violator uses a more sophisticated device to operate beyond the mandated power limits, additional steps are required. If it operates at a higher power level, then it results in shorter ZoCs because of the higher SNR of the received signal at the Enforcers, which in turn may lead to non-intersecting ZoC. This is treated as an anomaly by the system and by increasing the radii of the annular zones of the three Enforcers, in equal steps the system will arrive at an overlapped area which will contain the Violator. The step size should correspond to the distance calculated for 1 *dBm* change in path loss. On the other hand, lowering the transmit power is not an issue in this case as it lowers the uplink datarate due to lower SNR at the Tier-3 AP. Hence we do not consider such cases in our analysis.

Figure 7c shows the accuracy of the localization technique with varying density of Enforcers. Compared to static, crowdsourced enforcement technique performs better with increasing density of enforcement. The localization method outlined in Algorithm 2 achieves the same level of accuracy when three Enforcers with highest SNR are chosen among 40 participating Enforcers. Using static Enforcers, we find that there is at least one Enforcer, on either side of the Violator. This helps to reduce the ZoE because of annular zones overlap from three directions. While in crowdsourced paradigm, all the Enforcers chosen may be close to each other and on one side of the Violator thus generating a relatively wider ZoE when the total number of Enforcers is small. This also shows the power of the crowd in providing better enforcement results.

In summary, using propagation models and careful selection of Enforcers, the source of infraction can be located with high accuracy while the cost of Enforcement can be controlled by



(a) ZoC for 3 Enforcers

(b) ZoE with 3 Enforcers

(c) Area of the ZoE

Fig. 7. Zone of Enforcement (ZoE) for 3 Enforcers: Shaded area denotes the area to be patrolled to locate the violator. Crowd achieves the same ZoE accuracy as static enforcement when 3 Enforcers with best SNR are chosen from 40 participants.

encouraging more users to participate such that the ZoE can be minimized.

V. Detecting Multiple Violations

Multiple violations using omni-directional antenna that are not spatially co-located can be detected using directional antenna by the Enforcers. The details of the detection and aggregation scheme is discussed below.

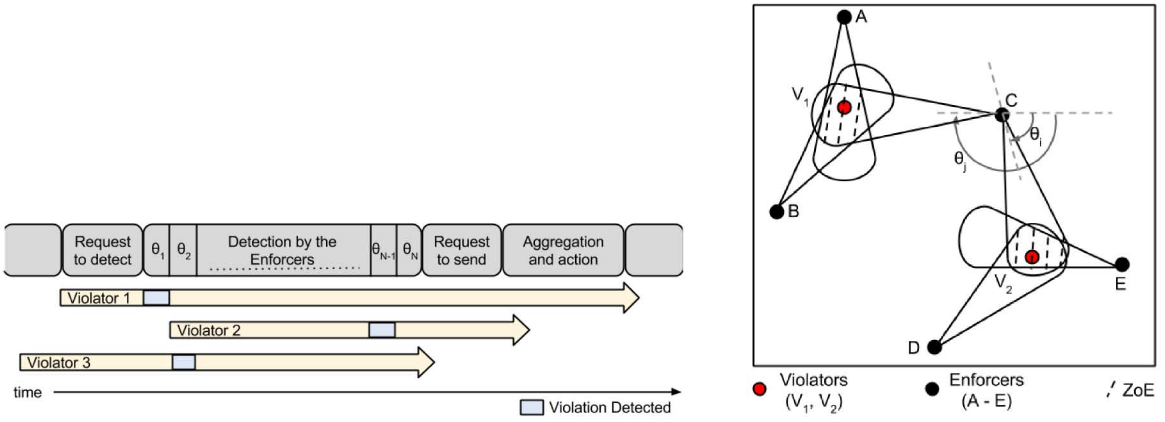
A. Detection

Figure 8a shows the temporal view of the detection and reporting phases of the scheme. All Enforcers willing to participate wait for the "request to detect" message from the Policy-maker to trigger their individual detectors. This applies to detecting single violation using omni-directional antenna as well. During the detection phase, each Enforcer will sweep across the azimuth in discrete steps and process the received signal for detecting possible spectrum infractions. We do not pose any restriction on the sweep speed, step-size, beamwidth (BmW) or the antenna type. We believe that these are design choices for individual Enforcer and the system allows for fair participation of these heterogeneous devices. The length of the detection phase is a design choice for the Policy-maker. As a guideline, it should be long enough to accommodate acquisition of sufficient number of samples required for detection along all antenna directions in one sweep cycle for a commercial directional antenna (typically of the order of tens of milliseconds). This strict protocol is required to maintain coherency of the detection results and also to take actions (after aggregation and inference) based on the crowdsourced information. As the Enforcer sweeps across the azimuth, infractions are detected at different time-steps (or directions denoted by θ), as shown in 8a. It is assumed that the slot times are long enough to process the received signal for violation. Post-processing or pipelined operation is also an architectural choice for slower, less powerful devices. It is to be noted that each participating Enforcer will have internal constraints and processing load that may interfere with the detection process. Hence, a device may choose to sweep across a subset of directions during the detection phase. The detection is followed by all the Enforcers reporting the results as a set of six parameters: $[P_d, P_f, SNR, loc, \theta, BmW]$, for every instance of a particular infraction that has been detected. To maintain uniformity of information, the Enforcers report the direction relative to a mutually agreed reference point, *e.g.*, clockwise relative to the geographic East as shown in figure 8b. Therefore, using these qualitative metrics, we are able to compensate for the variability in device specifications that commonly exist in commercial hardware.

Usually, for practical purposes, a spectrum infraction has to happen continuously for a certain duration for the Violator to benefit from that. From an enforcement standpoint, it is desirable that the Violator is active continuously during the entire detection phase or more. In practice, it may happen that infractions are intermittent during the detection phase or the Violator stops before the Enforcers beamform in that direction. In such cases, the power of the crowd will ensure that other members of the crowd are able to detect this infraction with sufficient accuracy. From §IV, we showed that at least three Enforcer is required to localize the Violator using this scheme. This also holds true for Enforcers using directional antenna, with the added advantage of having the ability to detect multiple infractions.

B. Aggregation and localization

Aggregating detection results using directional antenna starts by recreating the antenna beam patterns (as a 2D projection) from the detection results. Figure 8b shows an example with two Violators (V_1, V_2) and five Enforcers (A through E). Enforcer-C is close enough to both the infractions such that it is able to detect two violations (in different directions) with high accuracy. Based on the angle(s) (θ) and beamwidth (BmW) from the detection set of each Enforcer, the Policy-maker generates two geographic areas where the three beams overlap. From here, the ZoC and the ZoE is calculated based on the SNRs reported, using Algorithm 2 in §IV. The ZoC, in this case, will be an annular sector because of the directionality of



(a) Temporal view of the enforcement scheme

(b) Detection of multiple violations

Fig. 8. Enforcement of multiple violations: a) The detection and aggregation using directional antenna. The detection occurs in steps (θ_i) corresponding to the beam-forming direction. b) A node may detect two violations in two different directions which are aggregated as independent events along with the other detectors.

the antennas. Since the common overlapping area of the three beams is same as that for omni-directional antenna, the ZoE remains unaltered compared to omni-directional beam pattern.

Therefore, we show that using directional antenna and geometric representation of the detection results from the crowd, we are able to detect multiple violations in a given area. Since, neither the location nor the identity of the Violator is known a priori, the first step in aggregation is to isolate independent infraction events. Unlike detecting single violation, improving accuracy of P_d and P_f is done after isolating multiple infraction events. Once the detection results are attributed to independent infractions, corresponding values for P_d and P_f are aggregated using Algorithm 1 as discussed in §III.

VI. Detecting A Mobile Violator

When violations are caused by mobile users, a hierarchical inference is required along with using directional antenna for signal detection. This is illustrated using the example shown in figure 9. The first step towards inferring moving Violators is to observe violation events over multiple detection phases (figure 8a shows one detection phase). Let's consider the enforcement scenario of figure 9a, which consists 8 users, of which 5 are participating as Enforcers with 2 of them having detected violation events (V_1, V_2) in multiple directions. To this point, it is similar to detecting multiple independent violations as discussed in §V. Now, in the subsequent detection phase, represented by figure 9b, a different set of Enforcers participate and detect violations V_1' and V_2'.

The Policy-maker, as discussed previously, will re-create the geometry of the antenna beams as shown in figure 9a and 9b and infer the mobility pattern of the violations. It is to be noted that since the identity of the Violators are unknown, the Policy-maker will have to predict the mobility pattern, if any, from the movement of the ZoE obtained from the two detection phases. From figure 9, we can infer two things:

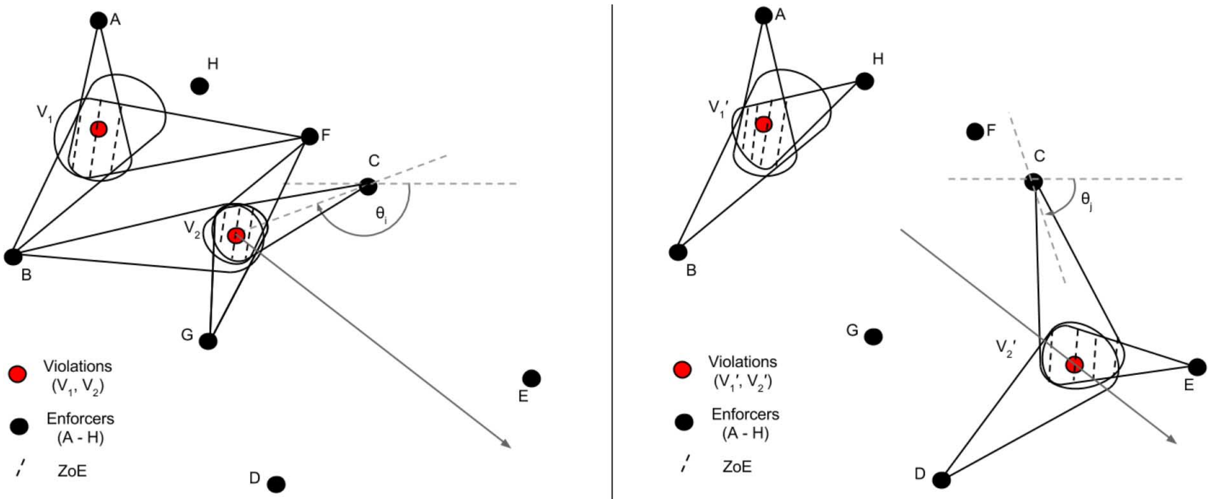
1) V_1 and V_1' have overlapping areas, hence it can be inferred that either it is a static Violator, violating over multiple detection phases or two independent violations separated in time. In either case, the enforcement action involves deploying resources to that ZoE for further investigation. In other words, we can disprove the fact that these two events are from a mobile Violator.
2) On the other hand, the ZoE corresponding to V_2 and V_2' may be correlated if there is consistent movement at a realistic velocity. For example, if the ZoE for V_2 and V_2' are separated by a large distance that is impossible to cover by a mobile user then they are uncorrelated events. Also, if these two ZoE are not along a stretch of road (after overlaying the beam patterns on a street map), then they are independent violation events. However, if there is an observable pattern in the movement of the ZoE of the two violations over multiple decision phases, then the system raises a warning flag that it might be caused by a mobile Violator. The Policy-maker can provide heads-up notification to its resources along the direction of the movement of the ZoE for further investigation. Therefore, using crowdsourced detection, we can detect mobile Violators as well.

VII. Modeling the Cost of Enforcement

A. Existing game-theoretic model

The conflict between the Violator and the Enforcer has been modeled as a simple (one-shot), 2-by-2 inspection game, as proposed by Tsebelis [10]. The general payoff matrix for the game is defined in table II with the following assumptions: 1] $c_1 > a_1$: The Violator will choose to not-violate in presence of enforcement; 2] $b_1 > d_1$: The Violator will always violate if there is no enforcement (no static or crowd-based detectors are deployed); 3] $a_2 > b_2$: Enforcer will always enforce if there is violation of spectrum rules and 4] $d_2 > c_2$: Enforcer will not-enforce if there is no violation in spectrum rules.

This game has a Nash equilibrium in mixed-strategies, where the Violator chooses to violate with probability $P(V) = p$ and



(a) First detection phase

(b) Second detection phase

Fig. 9. Detecting mobile Violators using detection results over multiple phases.

TABLE II
GENERAL PAYOFF MATRIX FOR A 2 × 2 ENFORCEMENT GAME

	Enforce	**Not-Enforce**
Violate	a_1, a_2	b_1, b_2
Not-Violate	c_1, c_2	d_1, d_2

the Enforcer chooses to enforce with a probability, $P(E) = q$, given by the equation below [10],

$$[p^*, q^*] = \left[\frac{d_2 - c_2}{(a_2 - b_2 + d_2 - c_2)}, \frac{b_1 - d_1}{(b_1 - d_1 + c_1 - a_1)}\right] \quad (3)$$

B. Application to crowdsourced enforcement

In order to understand the cost of the crowdsourced spectrum enforcement, we characterize the payoffs of the Enforcer and the Violator in Table III. We identify two payoffs that can be optimized by the Policy-maker to design a cost-effective enforcement system:

1) a_1 - *Penalty imposed on the Violator*: This amount strictly depends on the type of policy violation.
2) a_2 - *Cost of enforcement per infraction*: Since the Enforcer is an agent of the Policy-maker, this is a critical parameter to optimize for a balanced enforcement system.

The remaining payoffs are very specific to a particular type of violation and are assumed to be determined a priori. Rewriting the equilibrium strategies based on the interpretation in Table III,

$$[p^*_{crowd}, q^*_{crowd}] = \left(\frac{a_2}{b_2}, \frac{2b_1}{(b_1 - a_1)}\right) \quad (4)$$

Definition 1: The policy-maker's equilibrium strategy, q^*_{crowd}, is the minimum level of enforcement that can be maintained using the crowd.

Implication 1: In crowdsourced enforcement, given a specific policy infraction (b_1), the penalty levied to the Violator (a_1) is constant, given by (5)

$$a_1 = -\left(\frac{b_1(2 - q^*_{crowd})}{q^*_{crowd}}\right) \quad (5)$$

The minimum level of enforcement is chosen by the Policy-maker and the median aggregate accuracy (P_d) for that level of enforcement is given by Algorithm 1, discussed in § III. Therefore, for a given geographic area and a specific infraction, the equilibrium strategy of the Policy-maker, q^*_{crowd} is a constant and can be pre-determined. Furthermore, the estimated payoff to the Violator per infraction event, in absence of enforcement (b_1) is also deterministic given a specific type of infraction (say B), *e.g.*, number of bytes transmitted by the Violator by violating a particular policy, which is a constant value. Therefore, substituting these in (5) we can compute a constant penalty (a_1) for that infraction.

Example: From our evaluation, the minimum level of enforcement is 5 Enforcers as shown in Figure 4a. The corresponding median aggregate P_d, for the type of infraction defined by the RoC in Figure 2, is 0.875. Similar detection accuracy can be obtained for even smaller number of Enforcer (<5) if the population is sparse using the same procedure. Since the Policy-maker can implement a constant level of enforcement using the crowd, this value of P_d is the equilibrium strategy of the Policy-maker, hence $q^*_{crowd} = 0.875$. Therefore, substituting, q^*_{crowd} and B in (5), the penalty that should be levied to the Violator for this form infraction is $a_1 = -1.29 \times B$, which is a constant value. The negative sign indicates that it is a penalty.

Implication 2: In a crowdsourced enforcement, given a specific policy infraction, the Violator's equilibrium strategy, p^*_{crowd} is determined by the cost of enforcement.

The cost of enforcement (a_2) for the Policy-maker's equilibrium strategy, $q^*_{crowd} = 0.875$, can be derived, if the incentives to the crowd is pre-defined. This amount should be determined by the Policy-maker to design a profitable enforcement system

TABLE III
INTERPRETATION OF PAYOFFS FOR ENFORCER AND VIOLATOR IN THE DOMAIN OF ENFORCEMENT OF SPECTRUM ETIQUETTE. THE UNITS ARE ASSUMED TO BE NORMALIZED BY SUITABLE FACTORS. NOTE: $(a2 - b2) = catch\ premium$

Player	Strategy	Variable (Table II)	Sign	Payoff Definition
Violator	Violate	a_1	-ve	Penalty or fine imposed on the violator if caught.
		b_1	+ve	Amount of data sent/received by violating spectrum rules
	No-Violate	c_1	-ve	Opportunity lost (in bytes) by not-violating. Magnitude same as $b1$
		d_1	-ve	Magnitude same c_1. Payoff for not-violating is independent of the level of enforcement
Enforcer	Enforce	a_2	-ve	Cost of enforcement per infraction
		b_2	-ve	Damage caused by the infraction, *e.g.*, spectrum outage and increased interference.
	Not-Enforce	c_2	-ve	Same as a_2, Unit cost of enforcement is independent of the level of infraction
		d_2	N/A	Assumed to be 'zero'. The enforcer does not incur any cost in absence of infraction

and should be kept at a constant level. Similarly, for a specific policy violation, the damage caused to the Policy-maker (b_2) is also deterministic and known a priori, *e.g.*, revenue lost due to outage in spectrum usage from legitimate Tier-3 users due to the infraction. Therefore, from (4), we find that the frequency of violation, p^*_{crowd} is a constant value since a_2 and b_2 are both fixed and deterministic for a specific violation.

Implication 3: A Crowdsourced enforcement lowers frequency of violation over time by forcing the Violator to play her equilibrium strategy p^*_{crowd}.

From (4), we find that if the Violator, violates with $p > p^*_{crowd}$, with the intent to cause more damage to the Policy-maker (higher b_2), it will violate less frequently for same level of Enforcement (constant a_2). Also, more policy violation means increased payoff to the Violator (b_1) and from (5) we find that it will attract higher penalty and that will force the Violator to Not-Violate over time and resort to its equilibrium strategy. However, if $p < p^*_{crowd}$, it is assumed to be acceptable to the Policy-maker unless additional efforts are made (at higher enforcement cost) to further lower the frequency of infraction.

Therefore, the above analysis suggests that crowdsourced enforcement paradigm is cost effective and maintains a low levels of infraction over time as well.

VIII. DISCUSSIONS

Accuracy and population density: Ideally, only one Enforcer is good enough if the OP and SNR are both very good. In real deployments, this may not be possible, especially if it is far away from the violation or have other computational constraints, forcing it to choose a poor OP. This is precisely where the benefit of aggregating multiple Enforcers comes from as it identifies the "best" set of detectors among the crowd. Even if the crowd is not uniformly distributed, it is ubiquitous and has an incentive to regain rightful access to the spectrum. Detecting at any SNR will map into some detection metric ($[P_d, P_f]$), which allows the Policy-maker to carefully select the good ones to improve the overall accuracy. It pays off to be on the watch for violation because members of the crowd depend on each other to prevent harmful infractions. The system is most useful when there are at least 3 Enforcers. The only constraint on the Enforcer is that the signal has to be received at a minimum SNR that has a corresponding performance curve in the RoC. Figure 2 shows a range of SNR from $4-14$ dB with 2 dB steps. Generating smaller steps and extending the range can be easily done during the construction of the RoC for the detector.

Accuracy and propagation model: The enforcement methodology works with any propagation model, in any terrain. However, the accuracy of the model is crucial for calculating the estimated path loss and the distance to the Violator ($\hat{d}$). The addition of the error around the theoretically calculated distance in §IV, compensates for any model inaccuracies and errors in measuring the SNR. The ZoE obtained using the geometry of the antenna beams provides a coarse but accurate estimate of the origin of the infraction. As in any enforcement scheme, resources will have to be deployed at strategic locations within this area to further improve the location of Violator, using signal measurements and localization techniques. The reliance on propagation model is necessary because spectrum infractions propagate over large distances, which necessitates an accurate initial estimate, as represented by the ZoE, to focus on fine-grain signal analysis to obtain a "fix". Alternatively, either it will require a large number of Enforcers (cost-prohibitive) to decide in a collaborative fashion or computationally intractable (solving large systems of equations).

Comparing with other radio-location techniques: The localization technique is an extension of the 2-dimensional trilateration [11] method commonly used in geolocation and navigation systems. The key difference is that the trilateration for spectrum enforcement is performed over annular regions rather than circles. Positioning systems like GPS rely on trilateration in three dimensions along with accurate measures of time (using atomic clocks), time difference of arrivals (that translates to distance to the satellites) to locate a receiver. However, in this case the challenge is to locate the Violator (transmitter, not the receiver) without any additional timing related information. Unlike positioning systems, which rely on periodic transmission of known sequences, spectrum infractions are often sporadic and aperiodic. This requires constant surveillance of the radio spectrum, which is efficiently implemented by the using evidences from the eye-witnesses in the network.

Other geometry based methods like Multilateration [12], utilizes the time difference of arrival (TDOA) from multiple receivers. In this case, the estimated distance to the transmitter hinges on the accuracy of the measured time of arrival (or detection) of a signal feature. Furthermore, research have shown security vulnerabilities in multilateration based methods [13]. For accurate localization, all Enforcers will have to report the same instance of the violation and extracting absolute measures of time in a distributed system is extremely difficult in absence of added synchronization overhead. When receivers are common mobile devices, this introduces significant error in the estimated distance to the Violator. Firstly, since every receiver operate asynchronously and has different processing loads, the time recorded by the system will vary. Even a difference of 1 μs will lead to a distance error of 300 m. Secondly, each Enforcer may detect different instances (Violator transmits multiple packets) of the violation. In such cases, the calculated TDOA will be largely erroneous. Therefore, the lack of synchrony among the Enforcers, which is commonly seen in a crowdsourced paradigm, along with being insecure, will render TDOA based techniques unusable. Collaborative techniques sometimes are useful at the cost of communication overhead and increased complexity. Collaboration necessitates exchange of signal traces to perform cross-correlation to extract TDOA of certain signal features. The major drawback of such schemes is that mobile devices are power limited and lacks the computational power of centralized aggregation. Therefore, for practical purposes, the architecture splits the detection to eyewitnesses in the crowd while the aggregation is performed at the Policy-maker along with the information of the geometry of the Enforcers' radio propagation characteristics.

IX. Related Work

Crowdsourced enforcement of spectrum policies lies at the intersection of many disparate areas of research. Weiss *et al.* [14], presents a detailed description regarding the general premise of spectrum enforcement stressing on *ex-ante* and *ex-post* paradigms of enforcement.Authors in [15], discuss the requirement and design criterion for specific federal and non-federal frequency bands which are crucial for practical implementation. While this work present many insights into the general problem of enforcement of spectrum policy, it does not have any specific method to realize an efficient enforcement system. A survey of common threats in DSA is outlined in [16] while authors in [17] present a specific form of enforcement that relies on advanced coding theory and detection. In comparison our method is applicable for any form of infraction as long as the RoC is available. We harness the collective power of the "crowd" as opposed to individual capabilities.

Early works [10] have modeled the general conflict in enforcement that has since been extended by others [18], [19], to analyze the the cost of an enforcement system. Our work is an adaptation of the general framework and lends insights from a perspective of radio engineering. Spectrum enforcement also parallels intrusion detection system in wired and wireless networks [20], [21]. While intrusion detection suffers from the drawback that all the detectors are observing the infraction event at the same granularity and thus produce the same detection results and false positives. However, detection of infractions that propagate over radiowaves is harder because of propagation related losses which diminishes the integrity of the signal. This is one of the most important factors in enabling crowdsourced detection and aggregation. Our methodology outperforms static detector by order of magnitude while maintaining an acceptable minimum level of enforcement cost.

Smartphones have made crowdsourcing a reality. Authors in [22] present an analysis on incentives of a general crowdsourced paradigm which can be applicable to analyze crowdsourced spectrum enforcement as well. However, the revenue and cost models are vastly different in this domain as compared to something akin to crowdsourced mobile advertisement. Traffic and civilian law enforcement agencies have long relied on eye-witness accounts have also adopted the ubiquity of mobile devices to aggregate information [23]–[25].

X. Conclusion

In this paper, we measured the efficiency of a crowdsourced paradigm for enforcing spectrum etiquette, especially when applied to the novel, tiered licensing model proposed for DSA. Through simulations and analysis, we draw three firm conclusions: 1) The crowdsourced enforcement outperforms equivalent planned and static enforcement methods. This is largely attributed to the ubiquity of mobile detectors and careful aggregation, 2) Using a very small number of mobile nodes (3 in our work) the Policy-maker is able to locate and identify a Violator with high accuracy and 3) It maintains a constant level of enforcement at a very low cost that results in lowering the frequency of infractions. While many implementation challenges remain, the encouraging results point towards adopting this concept in reality.

References

[1] PCAST—Presidents Council of Advisors on Science and Technology, "Realizing the full potential of government-held spectrum to spur economic growth," Executive Office of the President, Tech. Rep., 2012.

[2] Federal Communications Commision, "NPRM: Ammendment of the commission's rules with regard to commercial operations in 3550-3650 MHz Band," Tech. Rep. FCC 1547, 2013 [Online]. Available: https://apps.fcc.gov/edocs_public/attachmatch/FCC1547A1.pdf

[3] A. Nika, Z. Zhang, X. Zhou, B. Y. Zhao, and H. Zheng, "Towards commoditized real-time spectrum monitoring," in *Proc. 1st ACM Workshop Hot Topics Wireless*, 2014, pp. 25–30.

[4] A. Achtzehn, J. Riihihjärvi, I. A. Barriía Castillo, M. Petrova, and P. Mähönen, "CrowdREM: Harnessing the power of the mobile crowd for flexible wireless network monitoring," in *Proc. 16th Int. Workshop Mobile Comput. Syst. Appl.*, 2015, pp. 63–68.

[5] Federal Communications Commision, "Unlicensed operation in the TV broadcast bands," Tech. Rep. FCC 10-174, 2012 [Online]. Available: https://apps.fcc.gov/edocs_public/attachmatch/FCC10174A1.pdf

[6] B. C. Levy, *Principles of Signal Detection and Parameter Estimation*, 1st ed. New York, NY, USA: Springer, 2008.

[7] J. S. Seybold, *Introduction to RF Propagation*. Hoboken, NJ, USA: Wiley, 2005.

[8] LAN/MAN Standards Committee, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, vol. 2012, IEEE Std 802.112012, 2012.

[9] J. Xiong and K. Jamieson, "ArrayTrack: A fine-grained indoor location system," in *Proc. 10th USENIX Conf. Netw. Syst. Des. Implementation (NSDI'13)*, 2013, pp. 71–84.

[10] G. Tsebelis, "Are sanctions effective? A game-theoretic analysis," *J. Conflict Resolut.*, vol. 34, no. 1, pp. 3–28, 1990.

[11] B. W. Parkinson, J. J. Spilker, Jr., P. Axelrad, and P. Enge, *Global Positioning System, Volume 1—Theory and Applications*. Washington, DC, USA: American Institute of Aeronautics and Astronautics, 1996.

[12] M. Geyer, "Aircraft navigation and surveillance analysis for a spherical Earth—Project memorandum," U.S. Department of Transportation, Tech Rep. DOTVNTSCFAA1501, 2014 [Online]. Available: http://ntl.bts.gov/lib/53000/53100/53123/DOTVNTSCFAA1501.pdf

[13] S. Capkun and J.-P. Hubaux, "Secure positioning in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 221–232, Feb. 2006.

[14] M. B. H. Weiss, W. Lehr, M. Altamaimi, and L. Cui, "Enforcement in dynamic spectrum access systems," *SSRN Electron. J.*, vol. 2012 TRPC, pp. 1–34, 2012.

[15] M. B. H. Weiss, M. Altamimi, and M. Mchenry, "Enforcement and spectrum sharing: Case studies of federal-commercial sharing," *in Proc. 8th Int. Conf. Cognit. Radio Oriented Wireless Netw.*, 2013, pp. 1–6.

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

[17] G. Atia, A. Sahai, and V. Saligrama, "Spectrum enforcement and liability assignment in cognitive radio systems," in *Proc. 3rd IEEE Symp. New Front. Dyn. Spectr. Access Netw.*, Oct. 2008, pp. 1–12.

[18] M. Holler, *Fighting Pollution When Decisions are Strategic*. Norwell, MA, USA: Kluwer, 1993, vol. 76, pp. 347–356.

[19] L. Andreozzi, Rewarding Policemen Increases Crime. Another Surprising Result from the Inspection Game. Norwell, MA, USA: Kluwer, 2004, vol. 121, pp. 69–82.

[20] H. Wei, "Using Bayesian game model for intrusion detection in wireless ad hoc networks," *Int. J. Commun. Netw. Syst. Sci.*, vol. 3, no. 7, pp. 602–607, 2010.

[21] J. Gaffney and J. Ulvila, "Evaluation of intrusion detectors: A decision theory approach," *in Proc. IEEE Symp. Secur. Privacy. (S&P'01)*, 2001, vol. 9, pp. 50–61.

[22] D. Yang, G. Xue, X. Fang, and J. Tang, "Crowdsourcing to smartphones: Incentive mechanism design for mobile phone sensing," in *Proc. 18th Annu. Int. Conf. Mobile Comput. Netw.*, 2012, pp. 173–184.

[23] Los Angeles County Sheriffs Department. *LEEDIR*, 2014 [Online]. Available: http://boingboing.net/2014/04/11/leedir.html

[24] Nextdoor. (2015). *Nextdoor App* [Online]. Available: https://nextdoor.com/

[25] Department of Homeland Security. *If You See Something, Say Something* [Online]. Available: http://www.dhs.gov/if-you-see-something-say-something

Aveek Dutta (M'15) received the M.S. and Ph.D. degrees in electrical engineering from the University of Colorado, Boulder, CO, USA.

He is an Assistant Professor with the Department of Electrical Engineering and Computer Science, The University of Kansas, Lawrence, KS, USA. Prior to his appointment, he was a Postdoctoral Research Associate with the Department of Electrical Engineering, Princeton University, Princeton, NJ, USA. His research has produced fast and efficient MAC layer protocols by utilizing the signal processing subsystems of OFDM-based physical layers. He has also architected flexible radio platforms and has worked on knowledge representation methods for complex physical layers in cognitive radio networks. His research interests include crossroads of communication theory, networked systems, and radio architectures that spans from novel MAC-PHY crosslayer solutions to heterogeneous networks.

Mung Chiang (S'00–M'03–SM'08–F'12) is the Arthur LeGrand Doty Professor of Electrical Engineering with Princeton University, Princeton, NJ, USA. He created the Princeton EDGE Lab in 2009 to bridge the theory-practice divide in networking by spanning from proofs to prototypes, resulting in a few technology transfers to industry, and several startup companies. He serves as the inaugural Chairman of Princeton Entrepreneurship Council and the Director of Keller Center for Innovation in Engineering Education, Princeton, NJ, USA. His Massive Open Online Courses on networking reached over 250 000 students since 2012 and the textbook received the 2013 Terman Award from American Society of Engineering Education. He was named a Guggenheim Fellow in 2014. He was the recipient of the 2012 IEEE Kiyo Tomiyasu Award and the 2013 Alan T. Waterman Award.