SAS: Modeling and Analysis of Spectrum Activity Surveillance in Wireless Overlay Networks

Jie Wang Wenye Wang
Department of Electrical and Computer Engineering
North Carolina State University, Raleigh, NC 27606
Email: {jwang50,wwang}@ncsu.edu

Cliff Wang
Army Research Office
Research Triangle Park, NC 27709
Email: cliff.wang@us.army.mil

Abstract*—Spectrum monitoring, run-time usage acquisition, and regulation enforcement, in general can be referred to as spectrum activity surveillance (SAS). It is essential to dynamic spectrum access with a two-fold impact: it is a primitive mechanism to continuously scan spectrum usage for system optimization purposes; it is also a prime widget to obtain spectrum footprints of legitimate users, and record misuse by unauthorized or malicious users. Seemingly trivial, large-scale SAS in wireless overlay networks is actually an open yet challenging problem. This is because on one hand, such a system is time and energy-sensitive and hence unlikely (or not necessary) to implement in practice, due to constraints of radio spectrum license and system deployment. On the other hand, it is not clear how to characterize the efficacy and performance of spectrum monitoring strategies in surveillance over a large geographical region, and detection of *spectrum culprits*, that is, unauthorized spectrum occupants. To address such a challenge, we consider SAS in a 3-dimensional space that is composed of spectrum, time, and geographical region, and then formulate monitoring strategies as graph walks by accounting for the *locality* of spectrum activities. In particular, our approach transforms the SAS problem from a globally collective activity to a set of localized, distributed actions, and strategy objectives from qualitative attributes to quantitative measures. We find that randomized strategies with m monitors can achieve a sweep-coverage over a space of n assignment points in $\Theta(\frac{n}{m}\ln n)$ time, and detect an oblivious or adversarial spectrum culprit in $\Theta(\frac{n}{m})$ time for SAS systems.

I. Introduction

Dynamic spectrum access (DSA) has been envisioned as a key technology for future high-speed wireless overlay systems [1], *e.g.*, 5G networks, that enables various radio access technologies (RAT) to co-exist over a geographical region. By allowing wireless devices to temporally operate beyond their designated spectrum bands, DSA is expected to mitigate the gap between the increasing spectrum demand and the already crowded wireless spectrum, boosting the spectrum efficiency of such overlay systems. Despite its potential, the open nature of DSA-enabled systems bears an intrinsic demand for spectrum activity surveillance (SAS), as both a prerequisite and a supplement to such spectrum-agile systems.

SAS refers to a continuous scan of spectrum activities on the frequencies of interest, which serves two roles in an DSA-enabled system. As the spectrum-police, it determines the legitimacy of instanueous spectrum usages, so that *spectrum culprits*, which refers to overly-aggressive or malicious users that obstruct the 'right-of-way' of legitimate users, can be identified, and spectrum policies can be enforced. This is especially meaningful since application of machine learning in cognitive radio [2] permits 'smart' culprits to exploit the system in an adversarial way [3], which strengthens the need for SAS to guard the right of legitimate users. On the other hand, SAS also serves as a data-collector in the long term, collecting spectrum occupancy statuses, such that a variety of usage data can be collected, including temporal and spatial patterns of spectrum occupancy, user mobility, as well as traffic patterns. On a systematic level, surveillance logs reflect spectrum usage for wireless communications, and can hence be used for system management purposes, *e.g.*, in the construction of the *radio environment map* (REM) [4]; on an individual level, real-time spectrum occupancy measurements can serve as a crude input to reveal and predict the spectrum sensing range [5] for opportunistic access. Therefore, SAS becomes both a premise to leverage spectrum efficiency in compliance to policy enforcement, and a proactive approach to detect spectrum culprits in wireless overlay networks.

Unlike spectrum sensing, which is a quick, individual, and passive action carried out by every wireless device to access spectrum opportunistically, SAS is a system-level, large-scale, and active process by dedicated/crowdsource monitors in a commercial DSA-enabled system. On the avenue of SAS, existing literature can be broadly summarized into two categories: single-monitor technique and multiple-monitor orchestration. The former develops prototypes [5], [6] and algorithms for single monitors, that can differentiate spectrum misuse from legitimate occupancy, *e.g.*, statistical significance testing [7], and spectrum permit mechanism [8]. In contrast, the latter focuses on efficient deployment of *multiple* monitors for the purpose of better surveillance coverage (space/spectrum scanned by monitors) [9], lower cost [10], and faster detection of culprits [3]. To this end, interference map construction from measurement data is studied [4] with dedicated monitors, while a crowdsource paradigm is also proposed for cost and flexibility improvement, taking advantage of collaboration [10] and distributed data decoding [11].

In prior studies of multiple-monitor deployment strategies [3], [9], [10], an implicit assumption is that spectrum monitors are sufficiently powerful, such that they can watch over the

This work is partially supported by NSF CNS-1527696, NSF CNS-1824518 and ARO W911NF-15-2-0102.

entire geographical region of interest and tune/move without any limit. The fact, however, is that most spectrum activities, including communications, attacks/jamming and monitoring/sniffing, are *local* in space/time/frequency, *i.e.*, as noted in spectrum occupancy measurements [4]. This discrepancy is especially pronounced in wide-band wide-area surveillance, *e.g.,* REM construction in wireless overlay networks, which leads to an open question: *how to model, design and analyze Spectrum Activity Surveillance (SAS) processes*?

Seemingly intuitive and trivial, the above question is actually a challenge to SAS systems. First and foremost, high deployment expenses prevent studying of this problem via field tests, especially at the early stage when prototypes [6] are still being developed. Second, objectives of SAS, *i.e.*, occupancy measurement and culprits detection, are by-and-large global and collective, lacking a consolidated measure, through which a monitoring strategy can be evaluated. Third, if spectrum is considered as a 1-D domain, the surveillance problem over a geographical region is naturally extended to a 3-D space, in which tracking surveillance coverage and dynamically deploying monitors are both non-trivial questions.

To address these challenges, we introduce a system model in a 3-D space that incorporates spectra, temporal and geographical domains, and then formulates an SAS process as graph walks, while the underlying graph captures *locality* of spectrum activities, *e.g.*, monitoring power, band-switching and moving capabilities. By this model, design and analysis of SAS strategies become viable, since: (i) the collective surveillance activity of multiple monitors is transformed into localized (even distributed) actions of single monitors; and (ii) the qualitative SAS objectives are translated to clear quantitative metrics in the time domain, *i.e.*, the coverage time and detection time. Our model is also versatile to illustrate dedicated and crowd-source monitors with various capability settings, so that performance of a certain strategy with specific monitors can be analyzed before implementation. As an application of the proposed model, we present randomized strategies to effectively detect adversarial spectrum culprits. Our analysis and simulations show that, despite the switching capacity limit, randomized strategies of m monitors can achieve a full sweep-coverage over a space of n assignment points in $\Theta(\frac{n}{m}\ln n)$ time, and detect a persistent/adversarial culprit in $\Theta(\frac{n}{m})$ time.

Our work focuses on modeling and analyzing the *efficacy* of spectrum monitoring strategies from the perspectives of *coverage* and *detection*. The rest of this paper is organized as follows. We introduce the system model, define performance metrics, and formulate the SAS problem in Sec. II. Then we transform the surveillance process into a tractable graph walk problem in Sec. III. Based on this model, randomized monitor deployment strategies without and with switching capacity limit are examined in Sec. IV and Sec. V respectively. Finally, this paper is concluded in Sec. VI.

II. Problem Formulation

In this section, we formally define the monitoring and exploiting model in the 3-dimensional spectra-location space, and propose metrics to formulate the SAS problem.

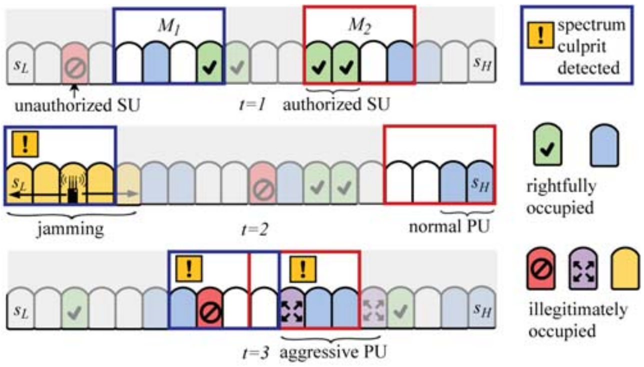


Fig. 1. Two spectrum monitors M_1 and M_2 (blue and red boxs) watch over spectrum block $\mathcal{S} = [s_L, s_H]$. Each spectrum slice can be in *idle* (in white), or *occupied* (in color) state, as a result of different spectrum activities.

A. System Model

Let $\mathcal{S} = [s_L\Delta_f, s_H\Delta_f] \subset \mathbb{R}$ denote a spectra block in a DSA-enabled wireless overlay network. Block $\mathcal{S}$ can be divided into $s_H - s_L$ spectrum slices of width Δ_f, which is the resolution bandwidth[1] of monitors, as shown in Fig.1. Since spectra block $\mathcal{S}$ is accessed through a variety of RAT's, that may not comply to the same channel assignment scheme, a channel in RAT scheme i contains $k_i \in \mathbb{N}^+$ spectrum slices. Considering that the width of spectrum block $\mathcal{S}$ is much larger than the resolution bandwidth Δ_f in a wireless overlay system, Δ_f is omitted for the ease of notation, and spectra block $\mathcal{S}$ is denoted as a continuous interval $[s_L, s_H]$.

To spectrum monitors, the observable *status* of a spectrum slice at a time instant can be: *idle*, *rightfully occupied*, or *illegitimately occupied*, as a result of spectrum activities illustrated in Fig.1. Slice s_i is *rightfully occupied* if it is (i) accessed by an authenticated and authorized primary user (PU), *e.g.*, the blue slices close to s_H at time $t = 2$, or (ii) opportunistically accessed by an authorized secondary user (SU) abiding DSA regulations, *e.g.*, green slices with ✔ markers. Slice s_j is *illegitimately occupied* when (i) the occupant is unauthorized to access s_j, *e.g.*, purple slices at $t = 3$ occupied by an aggressive PU, and red slices (with restriction sign) used by an unauthorized SU; or (ii) the occupant is transmitting in a prohibited manner, *e.g.*, emitting high-power jamming signal (yellow slices at $t = 2$). Such entities that conduct illegitimate occupancy are called *spectrum culprits*.

Rightful or illegitimate, all spectrum activities take place in a *space* that spans over both the 1-D spectrum domain $\mathcal{S}$ and the 2-D geographical space domain $\mathcal{A}$, *i.e.*, a 3-D product space $\mathcal{S}\times\mathcal{A}$, referred to as the *spectra-location space* X in our prior work [12]. As a product space, X is equipped with metric *spectra-location distance* d_{SA}, that is, the product metric of Euclidean distance metrics d_S and d_A in domain $\mathcal{S}$ and $\mathcal{A}$

[1] The recommended resolution is typically 1% to 3% the channel bandwidth [4]. An overly high resolution will consume significantly more resources [4], while a low resolution will obtain inaccurate occupancy measurements. So commercial devices generally set resolution bandwidth to be greater than 1 KHz, *e.g.*, the R&S FSH spectrum analyzer and the SDR prototype in [6].

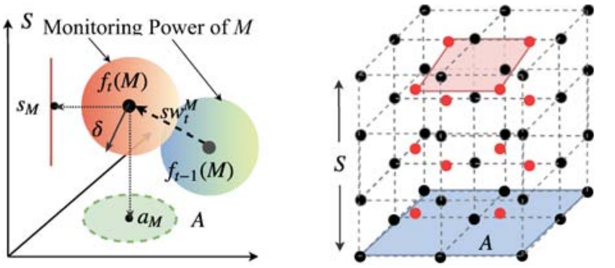


Fig. 2. $q(\delta)$-Monitoring power of a monitor is described as a δ-ball in space $X = \mathcal{S} \times \mathcal{A}$. Based on the monitoring power, space X can be divided into disjoint cells (see Sec. III) whose centers are shown on the right.

respectively. In this sense, the example illustrated in Fig. 1 is a special case when region $\mathcal{A}$ shrinks to a point, *i.e.*, $\mathcal{A} = \{a\}$.

Consider a set $\mathcal{M} = \{M_1, M_2, \cdots, M_m\}$ of m monitors. Let time t proceed in discrete steps $\mathcal{T} = \{1, 2, \cdots\}$.

1) Monitoring Model: At time step t, every monitor is assigned to tune to a center frequency in $\mathcal{S}$, and relocate to a spot in $\mathcal{A}$. During one time step, any monitor can scan, examine and/or record 'nearby' spectrum activities, *e.g.*, the 'box' of adjacent slices in Fig. 1, formally define as follows.

DEFINITION 1. *For a monitor $M \in \mathcal{M}$ assigned at $f_t^m(M) = s_M^t \times a_M^t \in X$ at time t, the $q(\delta)$-**monitoring power** of monitor M is defined as a δ-ball centered at $s_M^t \times a_M^t$, i.e.,*

$$Ball_\delta(s_M^t \times a_M^t) := \{x \in X | d_{SA}(s_M^t \times a_M^t, x) \le \delta\}, \quad (1)$$

inside which any spectrum activity can be identified and recorded by monitor M with probability q.

The ball-shaped monitoring power[2], as shown in Fig. 2 (left), captures *local* and *probabilistic* monitoring actions, as a result of the limited sampling rates of hardwares [6], [13]. Probability function $q : \mathbb{R} \to [0, 1]$ captures reliability of monitoring results with respective to distance d_{SA}. For instance, $\delta_* = \inf_{\delta>0}\{q(\delta) = 1\}$ corresponds to the surveillance range for fully reliable detections, *i.e.*, the $q(\delta_*)|_{q=1}$-monitoring power. If a point $x \in X$ is covered by two or more (*e.g.*, n) monitors, illegitimate occupancy at x can be detected with a higher probability, that is, $1 - [1 - q(\delta)]^n$. If not explicitly specified, we consider $q(\delta) = 1$ hereafter.

The surveillance *coverage* of all monitors in $\mathcal{M}$ at time t is the union of the m monitoring power, *i.e.*, $C(f_t^m) = \bigcup_{M_i \in \mathcal{M}} Ball_\delta(f_t^m(M_i))$. Allowing time t to proceed in $\mathcal{T}$, assignments construct a *strategy*[3] $\{f_t^m\}_t$, and the *sweep-coverage* of the strategy is then $\mathcal{C}_T(f^m) = \bigcup_{t \in [1,T]} C(f_t^m)$.

2) Exploiting Model: Illegitimate spectrum activities come in various forms, ranging from spectrum misuse by unauthorized or aggressive users to malicious jamming by attackers. Despite the form, a spectrum culprit $R \in \mathcal{R}$ located at $a_R \in \mathcal{A}$, illegitimately occupies a portion[4] S_R of the spectrum block $\mathcal{S}$ at time t, and is *detectable*, if $R_t = a_R \times S_R$ overlaps with the monitoring power of some monitor, *i.e.*, $\exists M_i \in \mathcal{M}$ such that $R_t \cap Ball_\delta(f_t(M_i)) \ne \phi$. Over a period of time, the *exploit sequence* $\{R_t\}_{t \in \mathcal{T}}$ captures spectrum exploit activities of culprit R. The exploit *pattern* of spectrum culprits, *i.e.*, how a spectrum culprit $R \in \mathcal{R}$ assigns its exploit sequence, can be either oblivious or adversarial, depending on its learning capability, and will be discussed in Sec. III. A.

3) Switching Model: A *switching* sw_t^Y of a wireless device $Y \in \mathcal{M} \cup \mathcal{R}$ is defined as a relocation of Y from point $Y_{t-1} \in X$ to point $Y_t \in X$, *e.g.*, switching action sw_2^M of monitor M in Fig. 2 left. Considering the fixed-length time steps, this common action of monitors and culprits is also *local*, as it is constrained by time, energy or other kind of cost. A *switching capacities* metric is introduced and discussed in Sec. III. B to address this locality from both range and rate perspectives.

B. Spectrum Activity Surveillance Problem

Recall SAS aims for occupancy measurements and culprit detection. So efficacy of a monitoring strategy can be quantitatively evaluated and fairly compared through temporal metrics with respective to the coverage and detection goals.

DEFINITION 2. *Under strategy $\{f_t^m\}_{t \in T}$, the **coverage time** T_f^m is defined as the first time that its sweep-coverage $\mathcal{C}_T(f^m)$ contains every point in space $X = \mathcal{S} \times \mathcal{A}$, that is,*

$$T_f^m := \min\{T \in \mathcal{T} \mid x \in \mathcal{C}_T(f^m), \ \forall x \in X\}. \quad (2)$$

*The **detection time** $\tau_R(f^m)$ of a culprit R with exploit sequence $\{R(t)\}_{t \in T}$, is defined as the first time that culprit R can be identified by any of the m monitors, that is,*

$$\tau_R(f^m) := \min\{t \in \mathcal{T} \mid \sum_{i=1}^{m} \mathbb{1}_{R_t \in Ball_\delta(f_t^m(M_i))} D_i \ge 1\}, \quad (3)$$

where detection outcome D_i is a Bernoulli r.v. with mean q.

For $\delta = \delta_*$ such that monitoring result is fully reliable, *i.e.*, $q(\delta_*) = 1$, the detection time can be further simplified to

$$\tau_R(f^m) := \min\{t \in \mathcal{T} \mid R(t) \in C(f_t^m)\}. \quad (4)$$

From perspectives of coverage and detection, this paper studies the SAS process of space $X = \mathcal{S} \times \mathcal{A}$ with a set of m monitors. Specifically, we intend to design monitor deployment strategies $\{f_t^m\}_{t \in \mathcal{T}} \in \{X^m\}^{\mathcal{T}}$, and examine their *efficacy* by answering the following questions:

1) What is the the coverage time T_f of the designed strategy f^m, by which time spectra-location space X is sweep-covered, *i.e.*, $X \subset \mathcal{C}_T(f^m)$?
2) Under the monitor deployment strategy f^m, what is the detection time $\tau_R(f^m)$ of a spectrum culprit $R \in \mathcal{R}$ with exploit sequence $\{R_t\}_{t \in [1,\mathcal{T}]}$?

[2] For a commercial monitor, parameters δ and q can be determined by the sensitivity, noise floor, and input range of the hardware.

[3] Superscript m in f_t^m denotes the number of monitors. A second subscript may be added to differentiate strategy types. Any of the three denotations (number of monitors, time and type) may be omitted if no confusion is raised.

[4] Without loss of generality, we consider culprits with a narrow S_R, such that S_R can be viewed as a point $s_R \in \mathcal{S}$, because they are the most difficult to detect. In addition, letting $S_R = \{s_R\}$ is also a reasonable simplification when $\mathcal{S}$ is wide. Then R_t shrinks to one point, and we write $R_t \in X$.

III. From Monitoring Strategy To Graph Walk

Given the limited power (closed δ-balls) of monitors, designing an efficient monitoring strategy to watch over the entire spectra-location space X is a challenging problem, due to the infinite size of the *strategy space* $\{X^m\}^{\mathcal{T}}$. To make the strategy design tractable, we reduce the continuous strategy space $\{X^m\}^{\mathcal{T}}$ to a discrete space through space-tessellation in our prior work [12]. By considering cells of radius δ_c, sweep-coverage can be guaranteed as long as the assignment maps $\{f_t^m\}_t$ are jointly surjective on the finite *assignment space* V composed of cell centers illustrated in Fig. 2 right. For culprit detection, we first identify different exploiting patterns in terms of assignment space V. Then impact of limited *switching capacity* is discussed from both range and rate aspects. Consequently, any monitoring strategy is then mapped to a *walk* on a composite graph (G_M, G_R). Through this process, SAS as a global activity is transformed into a chain of individual actions, *i.e.*, switching (walking) of monitors and culprits, enabling design of distributed strategy.

A. Persistent and Adversarial Spectrum Culprits

We consider persistent culprits (R_p) and adversarial culprits (R_a), whose exploit sequence $\{R_t\}_{t\in\mathcal{T}}$ takes value[5] in $V^{\mathcal{T}}$.

DEFINITION 3. *A* ***persistent culprit*** $R_p \in \mathcal{R}$ *refers to a spectrum culprit whose exploit sequence* $\{R_t\}_t$ *does not change over time, that is,* $\{R_t\}_t$ *is composed of i.i.d. r.v.'s* R_t^p*, all distributed with PMF* $g_{R_p}(v)$*, where* $v \in V$.

Persistent culprit R_p can represent a variety of simple exploiting strategies with different PMF $g_{R_p}(v)$. In contrast, applying machine learning techniques in radio access technology [2] enables sophisticated culprits to steer the game toward their benefit [3]. For example, they can actively dodge monitors by switching to points that are less probable to be monitored, after knowing the monitoring strategy[6].

DEFINITION 4. *An* ***adversarial culprit*** $R_a \in \mathcal{R}$ *is a spectrum culprit with prior knowledge of current strategy* $\{f_t^m\}_{t\in\mathcal{T}}$*, that is,* R_a *knows the set of probabilities* $\{v \in \cup_{M_i} f_t^m(M_i)\}_{v\in V}$ *ahead, and determines its current exploit point* R_t^a *with PMF* $g_{R_a}^t(v) = \frac{1}{|\text{Void}(t)|}$ *for point* $v \in \text{Void}(t)$*, where* $\text{Void}(t) = \arg\min_{v\in V} \mathbb{P}\Big(v \in \bigcup_{M_i\in\mathcal{M}} f_t(M_i)\Big)$.

B. Limited Switching Actions

Recall that a switching is a relocation of a device (monitor or culprit) in X (or equivalently V). For monitors, while switching was assumed to incur no cost (and is hence not constrained) in prior works [3], [6], switching cost is indeed a design concern in both dedicated and crowd-source SAS scenarios, especially when region $\mathcal{A}$ is large. For a dedicated monitor, switching is composed of physical movement and/or tuning, and is restricted by the induced switching cost constraints, including time, energy, budget *etc*. For instance, it is recommended to wait for 1 s for the local oscillator to stabilize after tuning the central frequency of a monitor. In contrast, switching by participants in crowd-source SAS is merely a change of surrogate devices. If immediate communication among all participants is guaranteed, or there exists a central control capable of timely coordination, switching will not be limited; otherwise for distributed crowd-source SAS that relies on local communication, switching is constrained by the communication range of surrogate monitors. In addition, any spectrum culprit is also subject to its own hardware constraint. So in this subsection, we discuss switching actions from the range (how far) and the time (how fast) aspect.

1) Range Aspect (Switching Capacity): Switching range refers to the distance in both spectrum domain $\mathcal{A}$ and space domain $\mathcal{S}$. It is constrained by the following capacity limit, capturing another aspect of *locality* of spectrum activities.

DEFINITION 5. *Suppose* $Y_t = x_Y \in X$ *denote the location (in X) of device* Y *at time t, the* ***switching capacity*** α_Y *of* Y *is defined as the maximum distance in X, that device* Y *can switch over by one action in a time step, that is,*

$$\alpha_Y := \sup_{Y_{t+1}\in X} \{d_{SA}(x_Y, Y_{t+1})\}. \tag{5}$$

Device Y *is referred to as an* α_Y*-monitor or* α_Y*-culprit.*

2) Time Aspect (Switching Rates): In addition to switching range, the rate of switching, that is, how many switching actions can be done in one time step, is also limited by hardware constraints. It seems problematic in culprit detection when monitors and culprits switch at different rates. Counter-intuitively, a more 'capable' culprit that switches faster than the monitors will be detected in an even shorter period of time.

Consider monitors with $q(\delta)$-monitoring power, that is, when a culprit shows up where a monitor is assigned (referred to as *co-location* in the assignment space V), the probability that it is detected by that monitor during one time step is q. Let $qp(s)$ ($s \in [0,1]$) denote the detecting probability when the co-location time s is less than one full time slot, where the non-decreasing function $0 \le p(s) \le 1$ captures the attenuated detection probability due to a reduced transmission time of culprits, and has the property of $p(0) = 0$, $p(1) = 1$.

LEMMA 1. *Suppose culprit* R_1 *differs from* R_2 *only in switching rates:* R_1 *can switch* $k \in \mathbb{N}^+$ *times during one time step, while* R_2 *and the monitors can switch once. The detection time of* R_1 *is stochastically dominated by that of* R_2*, that is,* $\tau_{R_1}(f) \overset{d}{\le} \tau_{R_2}(f)$ *for any* f*, when the following criterion is satisfied:*

$$p(\frac{1}{k}) \ge \frac{1 - [1 - q\mathbb{P}\big(R^2(t) \in C(f_t^m)\big)]^{\frac{1}{k}}}{q\mathbb{P}\big(R^2(t) \in C(f_t^m)\big)}. \tag{6}$$

Proof. Without loss of generality, assume the strategy f is carried out by one monitor M. Lemma 1 holds trivially for

[5] Actually any exploit point R_t takes value in the continuous space X. But when $R_t \in Ball_\delta(f_t(M_i))$, the detection probability $q(\delta)$ is the same in this cell (δ-ball centered at $f_t(M_i)$), so we write $R_t = f_t(M_i) \in V$ instead.

[6] We consider the most powerful culprit (with full knowledge of a strategy) as an extreme case to illustrate the robustness of a system against compromised strategies. A weaker culprit can at least observe the long-term visiting probability of any point $v \in V$ as knowledge. In some cases, SAS strategies are required to be disclosed, *e.g.*, crowd-source SAS systems.

a deterministic strategy f_S, when both R_1 and R_2 are adversarial. In fact, the detection time $\tau_{R_1}(f_S) = \tau_{R_2}(f_S) = \infty$, which is the 'wandering hole' problem analyzed in Sec. IV.A.

If f is a randomized strategy, or R_1 and R_2 are persistent culprits, during a time step t, R_1 generates an exploit sequence $\{R_1^1(t), R_2^1(t), \cdots, R_k^1(t)\}$, and R_2 switches to $R^2(t)$, while monitor M stays at a fixed assignment point $f_t(M) \in V$. The probability that R_2 is identified during t can be written as $Q_2 = q\left(1 - \mathbb{P}\big(R^2(t) \neq f_t(m)\big)\right)$, while for R_1, the probability of being identified by monitor M is

$$Q_1 = 1 - \Pi_{i=1}^k \left(1 - qp(\frac{1}{k})\mathbb{P}\big(R_i^1(t) = f_t(m)\big)\right). \quad (7)$$

Given that R_1 and R_2 only differ in switching rates, that is, $\mathbb{P}\big(R_i^1(t) = v\big) = \mathbb{P}\big(R^2(t) = v\big)$, for any $v \in V$ and $i \in \{1, 2, \cdots, k\}$, the probability $Q_1 = 1 - (1 - p(\frac{1}{k})Q_2)^k$. When criterion Eq. (6) holds, we have $Q_1 \geq Q_2$, which means that R_1 is more probable to be detected during any given time step t. Equivalently, the CCDF of detection time $R_1(f)$ and $R_2(f)$ satisfy $\mathbb{P}(\tau_{R_1(f)} > l) \leq \mathbb{P}(\tau_{R_2(f)} > l)$, for any integer $l \geq 1$. □

Even if Eq. (6) is not satisfied, quantity $|Q_2 - Q_1|$ will be very small, since $\mathbb{P}\big(R^2(t) \in C(f_t^m)\big)$ is small. Based on this observation, we assume both the culprit and monitors switch once every time step hereafter. Then for a persistent culprit R_p with PMF $g_{R_p}(v)$, the probability that it is detected by strategy f in time step k is $p_k = q\sum_{v \in f_k(\mathcal{M})} g_{R_p}(v)$. Denote $p_0 = 0$, and the expected detection time can be calculated by

$$\mathbb{E}\big(\tau_p(f)\big) = \sum_{k=1}^{\infty} k \prod_{i=1}^{k-1} (1 - p_i)p_k. \quad (8)$$

C. Graph Walk on (G_M, G_R): A Chain of Switching Actions

Accounting the switching capacity in deployment strategy design, the assignment space V is a subspace that inherits d_{SA} metric from X. This gives rise to a structure that incorporates possibility of switching actions for monitors, that is, a *graph* $G_M = (V, E_M)$, where an edge $(u, v) \in E_M$ exists, if and only if $d_{SA}(u, v) \leq \alpha_M$. Consequently, an arbitrary strategy $\{f_t^m\}_{t \in [1, \mathcal{T}]}$ can be seen as a *walk* by $m = |\mathcal{M}|$ walkers on the monitoring (sub)graph G_M, and coverage time T_f becomes the time that every assignment point in V is visited.

Meanwhile, spectrum culprit R is also subject to its own switching capacity limit α_R, so the exploiting activity of R is also a walk, but on the exploiting (sub)graph $G_R = (V, E_R)$. Note that the two sub-graph G_R and G_M have the same vertex set V, and are both sub-graphs of the complete graph K_n, which corresponds to $\alpha_M = \alpha_R = \infty$. Consequently, any culprit detection is a composite walk $\{f_t^m, R_t\}_{t \in \mathcal{T}}$ on the composite graph $G = (G_M, G_R)$, as illustrated in Fig. 3.

Formulating a monitoring process into a graph walk makes the strategy design more tractable. However, mathematical results on graph walks (*e.g.* [14]–[16]) will not directly apply to the SAS problem, that incorporates different scenarios and design concerns. For these purposes, adaptation, solution and analysis are discussed for the unlimited ($\alpha_M = \infty$) and limited ($\alpha_M < \infty$) capacity cases, in Sec. IV and Sec. V respectively.

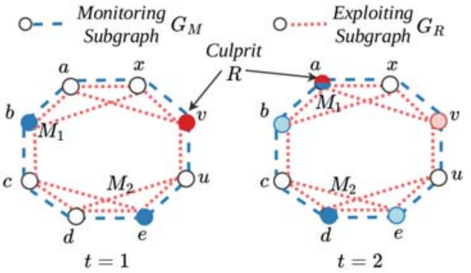


Fig. 3. An example of culprit detection: Two monitors (blue dots) and one culprit (red dot) walk on overlapping graphs. The monitoring subgraph $G_M = (V, E_M)$ (blue dashed edges) is sparser than the exploiting subgraph $G_R = (V, E_M)$ (red dotted edges) due to monitors' weaker switching capacity.

IV. Overcoming the 'Wandering Hole' Problem: Randomized Strategies

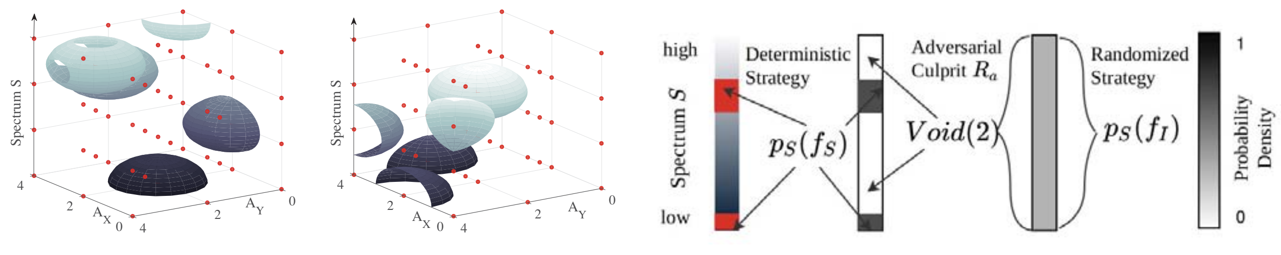
We start from the easier SAS scenario with powerful monitors that are not constrained in switching, and focus on tackling adversarial spectrum culprits. Such culprits pose as great challenges to monitoring strategy design, because they can exploit deterministic strategies in which every monitor's assignments are pre-determined, creating a *'wandering hole'* problem. This motivates us to propose independent and distributed randomized strategies, that are easy to implement, and can achieve a guaranteed coverage and detection performance.

A. The 'Wandering Hole' Problem and Its Root Cause

Deterministic strategy f_S, *e.g.*, the one proposed in [12], usually repeats after $T_S = \lceil \frac{n}{m} \rceil$ time, to maintain a low switching cost. Consequently it is possible for adversarial culprit R_a to observe visiting probabilities, and predict where monitors will most likely not be in the next time step. Then culprit R_a can continue chasing the void, as if hiding in a 'wandering hole' of the dynamically changing coverage.

An example of 'wandering hole' is shown in Fig. 4, where spectrum activities over region $\mathcal{A} = [0, 4]^2$ are monitored by $m = 5$ monitors. Red dots indicate the assignment points in V, while space enclosed by shaded spheres corresponds to the monitoring power of monitors. The white space outside of these spheres corresponds to space that a culprit can exploit without being detected, *i.e.* a spectrum *hole* in the coverage.

The root cause of this problem is that, culprit R_a is able to take advantage of the *difference* among visiting probabilities of assignment points, and determines the spectrum 'hole', *i.e.*, Void(t). The sharper the difference, the clearer the boundary of the 'hole', and the larger the chance to dodge monitors. For instance, under the deterministic strategy shown in Fig. 4(a-b), a culprit R_a located at $(3, 2)$ can easily identify Void$(2) \subset \mathcal{S} \times \{a\}$ (Fig. 4 (c) left) due to the prominent difference in probability density. A targeting counter-measure is to nullify the prior knowledge by eliminating the difference among visiting probabilities. In other words, fully *randomize* the deployment, such that every assignment point is visited with the same probability during any time step. Then the whole



(a) $t = 1$

(b) $t = 2$

(c) Root cause of the *'wandering hole'* problem

Fig. 4. Illustration of a *wandering hole*: 5 monitors are deployed in region $\mathcal{A} = [0,4]^2$ with $\delta = \frac{\sqrt{5}}{2}$. Their coverage C_t at each time step t, is the union of the enclosed space of the blue (partial) balls and the boundary, while the outter space corresponds to the spectrum 'hole', that is 'wandering' in X over time. Root cause of the *wandering hole* problem is the difference in probability density across X. For example, an adversarial culprit located at $(3,2)$ in (a) can infer the spectrum hole Void(2) with clear boundary, due to the sharp probability density difference, which is not the case for randomized strategies.

spectrum $\mathcal{S}$ at location $(3,2)$ will be included in Void(2) in culprit R_a's view (Fig. 4(c) right). Consequently, probability that R_a is not detected during $t+1$ becomes much smaller.

As we will show in this section, both the coverage and detection time of such randomized strategies (i) are bounded, indicating the efficacy for both the sweep-coverage and the detection goals; and (ii) scale as $O(\frac{1}{m})$ with respect to the number of monitors m, revealing their efficiency.

B. Randomized Monitor Deployment Strategies

We consider two randomized strategies that require different levels of coordination and switching capacities: the independent I-strategy f_I and the distributed D-strategy f_D.

Under the I-strategy f_I, during each time step, each monitor $M_i \in \mathcal{M}$ switches to an assignment point $v_i \in V$ uniformly at random, and independently of others. This strategy requires the switching capacity of monitors to include the entire assignment space V. The monitoring process is then equivalent to a composite random walk of $m = |\mathcal{M}|$ walkers, each independently generating a sequence $\{f_{t,I}^m(M)\}_{t\in\mathcal{T}}$, on the monitoring subgraph $G_M = K_n$. The uniform transition probability leads to a convergence-guaranteed stationary visiting probability distribution $\pi_v = \frac{1}{n}$, $\forall v \in V$.

Under the D-strategy f_D, assignment space V is evenly divided into m disjoint subsets $\{V_i\}_{M_i\in\mathcal{M}}$, that composes a partition of V. During time step t, each monitor $M_i \in \mathcal{M}$ switches to point $f_{t,D}^m(M_i)$, chosen uniformly at random from its own subset V_i, that contains $n_m = \lceil \frac{n}{m} \rceil$ assignment points. Thus, the D-strategy is equivalent to m independent single-walker random walks, each on a smaller complete graph K_{n_m}. Note that D-strategy only requires the monitoring power to include a subset V_i of the entire assignment space V, and the resulting stationary distribution is also uniform.

C. Coverage Time T_I^m and T_D^m

By our model that maps the randomized I- and D-strategy to random walks, the coverage time become well-defined r.v.'s taking value in $[1,\infty)$, and their expected value $\mathbb{E}(T_*)$ are referred to as the *cover time* in [14]. For the single monitor case, the I- and D-strategy are exactly the same. For this special case, the expected coverage time can be calculated as $\mathbb{E}(T_I^1) = \sum_{i=1}^{n} \frac{n}{n-i+1} = n\mathcal{H}_n$. For the case of multiple (m) monitors, both expected coverage times can be upper-bounded.

THEOREM 1. *For a set of $m = |\mathcal{M}|$ monitors that follow the I-strategy $\{T_{I,t}^m\}_{t\in\mathcal{T}}$ in an assignment space V of size n,*

$$\mathbb{E}(T_I^m) \le e(n-1)\left[0.562 + 0.768\frac{\mathcal{H}_n}{m}\right]. \tag{9}$$

If monitors in $\mathcal{M}$ follow the D-strategy $\{f_{D,t}^m\}_{t\in\mathcal{T}}$,

$$\mathbb{E}(T_D^m) \le n_m\left[\mathcal{H}_{n_m} + \frac{\sqrt{m-1}\,\left[7(n_m)^2 - 11n_m + 2\right]^{\frac{1}{2}}}{2(n_m-1)}\right], \tag{10}$$

where $n_m = \lceil \frac{n}{m} \rceil$.

Proof. First we prove the bound for $\mathbb{E}(T_I^m)$. Let $T_{I,i}^1$ denote the coverage time of a single monitor $M_i \in \mathcal{M}$. Then $\{T_{I,i}^1\}_{i=1}^m$ is a set of i.i.d. random variables with $T_{I,i}^1 \overset{d}{=} T_I^1$ for any monitor $M_i \in \mathcal{M}$. So

$$\mathbb{E}(T_I^m) \le \mathbb{E}(\min_{1\le i\le m} T_{I,i}^1) \le \mathbb{E}(T_{I,i}^1) = \mathbb{E}(T_I^1). \tag{11}$$

Let $H(x,y) := \min_{t>0}\{f_t^m(M_i) = y \mid f_0^m(M_i) = x\}$ denote the hitting time of monitor $M_i \in \mathcal{M}$ on point $y \in V$, given that M_i started its monitoring from $x \in V$. Note that M_i is inter-changeable with M_j, so the notation of monitor can be suppressed. Each monitor walks/switches independently, so $\mathbb{E}(H(x,y)) = n-1$, for any $x, y \in V$. With the construction technique in [14], we have the probability that the m random walkers have not covered every assignment points in V by time $er(n-1)$, or equivalently the coverage time T_I^m is greater than $er(n-1)$, as $\mathbb{P}\big(T_I^m > er(n-1)\big) \le e^{-mr} \le e^{-\gamma}$, where integer $r = \lceil \frac{\ln n + \gamma}{m} \rceil$, and $\gamma = \lim_{n\to\infty}(\mathcal{H}_n - \ln n)$ is the Euler-Mascheroni constant.

Also, notice that $\mathbb{E}(T_I^m) \le \mathbb{E}(T_I^1) = n\mathcal{H}_n$ from Eq. (11). Therefore, the expected coverage time

$$\begin{aligned}\mathbb{E}(T_I^m) &\le er(n-1)\cdot(1-e^{-\gamma}) + \mathbb{E}(T_I^1)\cdot e^{-\gamma} \qquad (12)\\ &\le \frac{e(n-1)}{m}\left[(\mathcal{H}_n + m)(1-e^{-\gamma}) + \mathcal{H}_n e^{-(1+\gamma)}\right],\end{aligned}$$

and plugging in values of γ and e yields the result.

Now we prove Eq. (10) for the D-strategy.

Let r.v. T_{M_i} denote the coverage time of monitor M_i on its own subset $V_i \subset V$, where $|V_i| = n_m = \lceil \frac{n}{m} \rceil$. Under the D-strategy f_D^m, monitoring sequence of each monitor is a random walk on a separate complete graph K_{n_m}, so $\mathbb{E}(T_{M_i}) = n_m\mathcal{H}_{n_m}$ for all $M_i \in \mathcal{M}$. Further, r.v. $T_{M_i} =$

$\sum_{k=1}^{n_m-1} T_k$, where each T_k is geometrically distributed with parameter $\frac{n_m-k+1}{n_m}$. Hence $\mathbb{E}(T_k) = \frac{n_m}{n_m-k+1}$ and $Var(T_k) = \frac{n_m(k-1)}{(n_m-k+1)^2}$. Then the variance of r.v. T_{M_i} can be obtained as

$$Var(T_{M_i}) = \sum_{k=1}^{n_m} Var(T_k) \leq (n_m)^2 \left(\frac{7}{4} - \frac{2n_m+1}{2(n_m-1)n_m} \right). \tag{13}$$

The coverage time of strategy f_D^m is the maximum of m i.i.d. r.v.s, that is, $T_D^m = \max_{M_i \in \mathcal{M}} \{T_{M_i}\}$, so it can be upper-bounded through a an inequality in [17, Eq.(3)], that is,

$$\mathbb{E}(T_D) \leq \mathbb{E}(T_{M_i}) + \sqrt{(m-1)Var(T_{M_i})}. \tag{14}$$

Plugging Eq. (13) into Eq. (14) yields the upper-bound. □

Theorem 1 upper-bounds the coverage time under the two proposed randomized strategies, and it is validated by numerical simulations. Fig. 5(a) and (b) illustrate the expected coverage time of I-strategy ($\mathbb{E}(T_I^m)$, blue '○' markers) and D-strategy ($\mathbb{E}(T_D^m)$, red '×' markers),and their scaling behavior over $m = \mathcal{M}$ and $n = |V|$ respectively. Zooming in, the case of four monitors ($m = 4$) is shown in the inner box of Fig. 5 (a), from which it can be seen that even the sliding average of coverage time ('○' and '×' markers) are upper bounded. We have the following observations by comparing simulation and bounds. (i) Eq. (10) (red dashed line) is a tight bound on the coverage time of D-strategy. (ii) Eq (9) (blue dotted line), though not tight, accurately describes its $O(\frac{n}{m} \ln n)$ scaling behavior. (iii) I-strategy and D-strategy have very close coverage time performances, not only in the mean sense, but also in distribution, as shown in the inner boxes of Fig. 5 (b). An implication is the more demanding I-strategy (in terms of level of coordination and switching capability of monitors) can be safely substituted by the distributed D-strategy, with the same coverage performance. (iv) Both expected coverage times are $O(\frac{n}{m} \ln n)$ (blue dotted line in (b)), which can be used to predict the number of monitors needed to reach the coverage goal of a given space with a certain resolution.

D. Bounded Detection Time of Adversarial Culprits

As can be seen from the example shown in Fig. 4 (c) (right), the advantage of prior knowledge to adversarial culprits is compromised, as evidenced by the bounded detection time. This is possible due to the uniform visiting probability distribution of both randomized strategies.

THEOREM 2. *Under strategy f_I^m and f_D^m, the expected detection time $\mathbb{E}(\tau_R(f_*))$ of an adversarial culprit R_a is upper-bounded, if the detection probability q is lower-bounded.*

Proof. Consider m monitors over V, each has $q(\delta)$-monitoring power. To I-strategy f_I^m and D-strategy f_D^m, an adversarial culprit R_a is equivalent to a persistent culprit R_{md} with uniform PMF, in terms of detection time, because both strategies achieve a uniform visiting probability over V.

First we consider the I-strategy f_I^m. The detection time $\tau_R(f_I)$ is the meeting time between the culprit and any of the m monitors on the complete graph K_n. By Eq. (8), $\tau_R(f_I^m)$ is geometrically distributed with parameter $p_I = 1 - (1 - \frac{q}{n})^m$, the probability that the culprit is caught by at least one of the m monitors in a single time step. Therefore, given that the detecting probability q is lower-bounded by a positive constant $q_* > 0$, $\mathbb{E}\big(\tau_a(f_I^m)\big)$ can be upper-bounded as

$$\mathbb{E}\big(\tau_a(f_I^m)\big) = \frac{1}{p_I} = \Big[1 - (1 - \frac{q}{n})^m\Big]^{-1} \tag{15}$$
$$\leq \left\{1 - \Big[(1 - \frac{q_*}{n})^{\frac{n}{q_*}}\Big]^{\frac{q_* m}{n}}\right\}^{-1} \overset{\frac{n}{q_*}>1}{\leq} \frac{1}{1 - e^{-\frac{q_* m}{n}}}.$$

Under the D-strategy f_D^m, each monitor walks independently, and occupies a different point in V during each time step t. Therefore, the probability that culprit R_a is identified by any of the m monitors is $p_D = q\frac{m}{n}$, and the corresponding expected detection time is also upper-bounded:

$$\mathbb{E}(\tau_a(f_D^m)) = \frac{1}{p_D} = \frac{n}{qm} \leq \frac{n}{q_* m}, \tag{16}$$

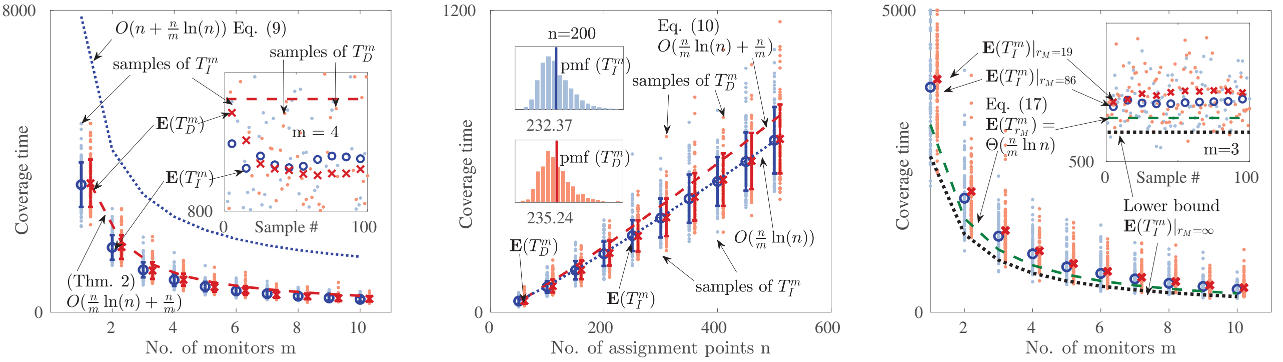
where $q_* > 0$ is a positive constant such that $q \geq q_*$. □

Theoretically, the detection probability q can be very small ($<< 1$) and consequently $\mathbb{E}(\tau_a(f_I^m))$ and $\mathbb{E}(\tau_a(f_D^m))$ go to infinity. But it is highly unlikely in practice, because in that case, parameter δ can be adjusted in the space-tessellation step (discussed in [12]), so that q is boosted to an acceptable level.

Theorem 2 reveals a compelling advantage of randomized strategies other than simpleness, that is, resistance to adversarial culprits. To validate these analysis, numerical simulation is conducted in an assignment space of size $n \leq 500$ and detection probability q is set to 1, as shown in light-blue (I-strategy) and light-red (D-strategy) dots of Fig. 6 (a) and (b). From the bounds and simulation results, we can see first and foremost, not only are the detection time of I-strategy and D-strategy bounded, they can be calculated with Eq. (15) and (16). Moreover, even when the detection is imperfect, that is, the reliability of surveillance result $q < 1$, Eq. (15) and (16) are still valid, so result is not shown due to space limit. This predictability gives random strategies extra edge in the design stage. Secondly, similarly as the coverage time, D-strategy proves to be a good distributed alternative to I-strategy. For both the coverage time and detection time, we can observe a linear 'speed-up' when multiple monitors are employed, that is, $O(\frac{1}{m})$. An implication is that increasing the number of monitors is an efficient performance-boosting measure.

V. SAS WITH LIMITED SWITCHING CAPACITIES

Recall in Sec. III.B, the *switching capacity* α_Y is defined as the maximum distance that a device (monitor or culprit) Y can switch over in one time step. Consider the SAS problem of m independent α_M-monitors (with full reliability $q = 1$) and an α_R-culprit on the assignment space V. Let $r_{\alpha_M}(v)$ denote the degree of point $v \in V$ in the monitoring subgraph G_M, under the switching constraint α_M, and $r_{\alpha_R}(v)$ denote the degree of v in the exploiting subgraph G_R, under the the switching constraint α_R. Then G_M and G_R are both subgraphs of the complete graph K_n, which corresponds to the unlimited case discussed in Sec. IV. Further, if monitors are more 'powerful' than the culprit ($\alpha_M > \alpha_R$), then $E_R \subset E_M$, and vise versa.

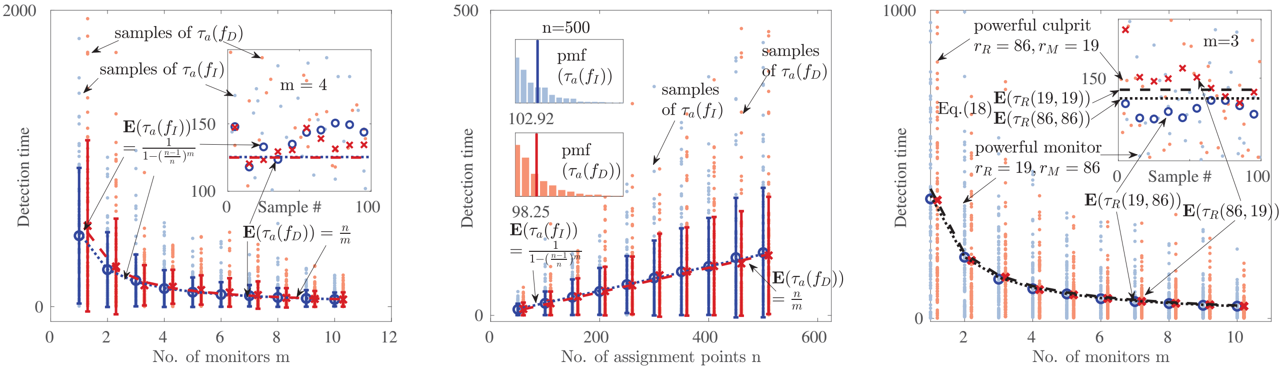


(a) Unlimited switching capacity $O(\frac{1}{m})$.

(b) Unlimited switching capacity $O(n\ln n)$.

(c) Limited switching capacity $\Theta(\frac{n}{m}\ln n)$.

Fig. 5. The expected coverage time of both the I- ($\mathbb{E}(T_I)$) and D-strategy ($\mathbb{E}(T_D)$) is $O(\frac{n}{m}\ln n)$, with or without limited switching capacity.



(a) Unlimited switching capacity $O(\frac{1}{m})$.

(b) Unlimited switching capacity $O(n)$.

(c) Limited switching capacity $\Theta(\frac{n}{m})$.

Fig. 6. The expected detection time of an adversarial culprit is $O(\frac{n}{m})$, under both the I and the D-strategy with unlimited or limited switching capacities.

A. *Regular Graph Approximation*

Observe that assignment points (cell centers) in V are quite 'structured', as shown in Fig. 2 (right). So most vertices in G_M and G_R have similar degrees, except for the few around the boundary. Therefore, we first approximate G_M and G_R as r_M- and r_R-regular graphs (G_{r_M} and G_{r_R}) respectively, on which mathematical tools [14], [15], [18] come in handy. Here $r_M=\frac{1}{n}\sum_{i=1}^{n}r_{\alpha_M}(v_i)$ is the average degree of monitoring subgraph G_M, and r_R is that of exploiting subgraph G_R.

1) Coverage Time: Let $T_{r_M}^m$ denote the coverage time of m independent monitors on r_M-regular graph G_{r_M}, to differentiate from T_I^m on the monitoring subgraph G_M. Asymptotic bounds for $\mathbb{E}(T_{r_M}^m)$ have been studied by multiple researchers, *e.g.*, Alon *et.al.* [14] proved the cover time to be $\Theta(\frac{n\ln n}{m})$. It is shown in [16] that a randomly chosen $r-$regular ($r\geq 3$) graph G_r is "nice" with high probability, so the expected coverage time $\mathbb{E}(T_{r_M}^m)$ follows from [18, Theorem 2],

$$\mathbb{E}(T_{r_M}^m)\sim\frac{r_M-1}{r_M-2}\frac{n\ln n}{m}. \tag{17}$$

2) Detection Time: Let $\tau_R(r_R,r_M)$ denote the detection time of a culprit R (walking on the r_R-regular graph G_{r_R}), by m-monitors (walking on the r_M-regular graph G_{r_M}).

Case 1. $r_R=r_M=r$ such that both monitors and culprit R walk on the r-regular graph G_r. Applying the predictor-and-prey model [18, Theorem 3] we can asymptotically bound the expected detection time of culprit R, that is,

$$\mathbb{E}(\tau_R(r,r))\sim\frac{r-1}{r-2}\cdot\frac{n}{m}. \tag{18}$$

Case 2. $r_R\neq r_M$. An upper-bound of $\mathbb{E}\left(\tau_R(r_R,r_M)\right)$ can be obtained by considering a composite random walk and then follow an inequality in [15, Proposition 6.16].

PROPOSITION 1. *Let* $q=\frac{(n-1)!}{(n-m-1)!}$*, then,*

$$\mathbb{E}\left(\tau_R(r_R,r_M)\right)\leq 1+\frac{q}{n^m}(4q^2-1). \tag{19}$$

Unlike Eq. (17) and Eq. (18), Proposition 1 holds for finite n. When n is large, asymptotic results in [14] and [16] apply, except that in the SAS problem, monitors and the culprit walk on *different* subgraphs ($G_{r_M}\neq G_{r_R}$). Addressing this issue, we have a corollary by considering $\min\{r_R,r_M\}$.

COROLLARY 1. *The expected detection time of a monitoring process on* (G_{r_R},G_{r_M}) *is* $\mathbb{E}\left(\tau_R(r_R,r_M)\right)=\Theta(\frac{n}{m})$.

Note that compared to performance of unlimited switching capacity, the scaling law provided by the average-degree approximate (Eq. (17) and Eq. (18)) differs only by a degree-determined constant, which is no larger than 2. This indicates that the scaling law of both coverage and detection time on regular graph (G_{r_M},G_{r_R}) remains unchanged over m and n.

B. Gap between (G_M, G_R) and (G_{r_M}, G_{r_R})

For Eq. (17) and Eq. (18) to hold, a regular graph needs to be "nice" [16, pp. 733]. It is also shown [16] that a large (n large) r-regular graph G_r randomly selected from all r-regular graphs $\mathcal{G}_r$, is *almost-Ramanujan* with high probability, that is, the largest eigenvalue $\lambda_0(G_r)$ and the second largest eigenvalue $\lambda_1(G_r)$ of graph G_r's adjacency matrix satisfy

$$\lambda_1(G_r) \leq 2\sqrt{\lambda_0(G_r) - 1} + \epsilon, \tag{20}$$

where $\lambda_0(G_r) = r$, as G_r is r-regular. However, this is not necessarily true for the real exploiting and monitoring subgraphs (G_R, G_M). This gap in graph expansion properties does not allow direct application of the scaling law (Eq. (17) and Eq. (18)) to the composite graph (G_M, G_R), induced by switching capacity limit α_M and α_R. Nonetheless, with extensive simulation, we found that $\mathbb{E}(T_I^m)$ and $\mathbb{E}(\tau_R(f_I^m))$ on the real composite graph (G_M, G_R) actually follow the $\Theta(\frac{n \ln n}{m})$ and $\Theta(\frac{n}{m})$ scaling law described in Eq. (17) and Eq. (18), as shown in Fig. 5 (c) and 6 (c). Simulations (dots) and bounds (dashed and dotted lines) are compared in an assignment space V that has $n = 394$ points.

As anticipated, the expected coverage time of a weaker monitor set (red '$\times$' markers, with switching capacity limit $r_M = 19$) is slightly longer than that of a more powerful monitor set (blue '$\bigcirc$' markers) in Fig. 5 (c). The lower bound (black dotted line) is obtained by setting $r_M = \infty$, while the regular graph approximation $\mathbb{E}(T_{r_M}^m)|r_M = 86$ is shown in green dashed line. From both cases the scaling of the expected coverage time $\mathbb{E}(T_I^m)$ over m is well-captured.

For the expected coverage time in Fig. 6 (c), both the upper and lower bound (black dashed and dotted lines respectively) are tight, if not precise, for $m \in [1, 10]$, *i.e.*, $\mathbb{E}(\tau_R(f_I^M)) \simeq \mathbb{E}(\tau_R(r_R, r_M))$. Similar results are also observed for different n settings and are omitted due to space limit.

Comparing the unlimited switching capacity (Fig. 5 (a) and 6 (a)) with the limited case (Fig. 5 (c) and 6 (c)), we observe that the capability limit α_M (or r_M) becomes less influential as m increases, and does not change the scaling behavior, because α_M is sufficiently large so that the quantity $\frac{r_M - 1}{r_M - 2}$ in Eq. (17) comes close to 1. Another interesting observation is that, even though the switching capacity of the monitors and that of the culprit differ considerably in value for the two simulation cases, the mean coverage and detection time ('$\bigcirc$' and '$\times$' markers in Fig. 5 (c) and 6 (c)) are close. The reason behind this is similar to that stated in Lemma 1, *i.e.*, the more 'mobile' (either monitors or culprits), the more 'visible'.

VI. Conclusion

In this paper, we study the spectrum activity surveillance problem, particularly deployment strategies of multiple monitors, for the purpose of sweep-coverage and spectrum culprits detection. We introduce a model that captures the locality of spectrum activities, based on which any deployment strategy can be formulated as a graph walk, and evaluated with coverage and detection metrics. As an application of the proposed model, we present randomized strategies against adversarial spectrum culprits, whose efficacy is theoretically analyzed and validated through simulations. We hope these results could contribute to the knowledge of SAS, and benefit the design and management of dynamic spectrum access systems.

References

[1] O. Holland, H. Bogucka, and A. Medeisis, *Practical Mechanisms Supporting Spectrum Sharing*, pp. 450–. Wiley Telecom, 2015.

[2] M. J. L. Pan, T. C. Clancy, and R. W. McGwier, "A machine learning approach for dynamic spectrum access radio identification," in *2014 IEEE Global Communications Conference*, pp. 1041–1046, Dec 2014.

[3] M. Li, D. Yang, J. Lin, M. Li, and J. Tang, "Specwatch: Adversarial spectrum usage monitoring in crns with unknown statistics," in *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*, pp. 1–9, April 2016.

[4] M. Höyhtyä, A. Mämmelä, M. Eskola, M. Matinmikko, J. Kalliovaara, J. Ojaniemi, J. Suutala, R. Ekman, R. Bacchus, and D. Roberson, "Spectrum occupancy measurements: A survey and use of interference maps," *IEEE Communications Surveys Tutorials*, vol. 18, pp. 2386–2414, Fourthquarter 2016.

[5] A. Nika, Z. Zhang, X. Zhou, B. Y. Zhao, and H. Zheng, "Towards commoditized real-time spectrum monitoring," in *Proceedings of the 1st ACM Workshop on Hot Topics in Wireless*, HotWireless '14, (New York, NY, USA), pp. 25–30, ACM, 2014.

[6] D. Pfammatter, D. Giustiniano, and V. Lenders, "A software-defined sensor architecture for large-scale wideband spectrum monitoring," in *Proceedings of the 14th International Conference on Information Processing in Sensor Networks*, IPSN '15, (New York, NY, USA), pp. 71–82, ACM, 2015.

[7] 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. Special Issue on Cognitive Radio Ad Hoc Networks.

[8] L. Yang, Z. Zhang, B. Y. Zhao, C. Kruegel, and H. Zheng, "Enforcing dynamic spectrum access with spectrum permits," in *Proceedings of the Thirteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '12, (New York, NY, USA), pp. 195–204, ACM, 2012.

[9] D.-H. Shin and S. Bagchi, "An optimization framework for monitoring multi-channel multi-radio wireless mesh networks," *Ad Hoc Networks*, vol. 11, no. 3, pp. 926 – 943, 2013.

[10] X. Jin, J. Sun, R. Zhang, Y. Zhang, and C. Zhang, "Specguard: Spectrum misuse detection in dynamic spectrum access systems," in *2015 IEEE Conference on Computer Communications (INFOCOM)*, pp. 172–180, April 2015.

[11] B. V. den Bergh, D. Giustiniano, H. Cordobés, M. Fuchs, R. Calvo-Palomino, S. Pollin, S. Rajendran, and V. Lenders, "Electrosense: Crowdsourcing spectrum monitoring," in *2017 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pp. 1–2, March 2017.

[12] J. Wang, W. Wang, and C. Wang, "Modeling and strategy design for spectrum monitoring over a geographical region," in *2017 IEEE Global Communications Conference: Cognitive Radio and Networks (Globecom2017 CRN)*, (Singapore, Singapore), Dec. 2017.

[13] S. Yoon, L. E. Li, S. C. Liew, R. R. Choudhury, I. Rhee, and K. Tan, "Quicksense: Fast and energy-efficient channel sensing for dynamic spectrum access networks," in *2013 Proceedings IEEE INFOCOM*, pp. 2247–2255, April 2013.

[14] N. Alon, C. Avin, M. Koucky, G. Kozma, Z. Lotker, and M. R. Tuttle, "Many random walks are faster than one," *Combinatorics, Probability and Computing*, vol. 20, no. 4, pp. 481–502, 2011.

[15] D. Aldous and J. A. Fill, *Reversible Markov Chains and Random Walks on Graphs*. 2002. Unfinished monograph, recompiled 2014, available at http://www.stat.berkeley.edu/$\sim$aldous/RWG/book.html.

[16] C. Cooper and A. Frieze, "The cover time of random regular graphs," *SIAM Journal on Discrete Mathematics*, vol. 18, no. 4, pp. 728–740, 2005.

[17] D. Bertsimas, K. Natarajan, and C.-P. Teo, "Tight bounds on expected order statistics," *Probab. Eng. Inf. Sci.*, vol. 20, pp. 667–686, Oct. 2006.

[18] C. Cooper, A. Frieze, and T. Radzik, *Multiple Random Walks and Interacting Particle Systems*, pp. 399–410. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009.