Secure Crowdsourced Radio Environment Map Construction

Yidan Hu
Department of Computer and Information Sciences
University of Delaware
Newark, DE 19716
Email: yidanhu@udel.edu

Rui Zhang
Department of Computer and Information Sciences
University of Delaware
Newark, DE 19716
Email: ruizhang@udel.edu

***Abstract*—Database-driven Dynamic Spectrum Sharing (DSS) is the de-facto technical paradigm adopted by Federal Communications Commission (FCC) for increasing spectrum efficiency. In such a system, a geo-location database administrator (DBA) maintains spectrum availability information over its service region whereby to determines whether a secondary user can access a licensed spectrum band at his desired location and time. To maintain spectrum availability in its service region, it is desirable for the DBA to periodically collect spectrum measurements whereby to construct and maintain a Radio Environment Map (REM), where the received signal strength at every location of interest is either directly measured or estimated via proper statistical spatial interpolation techniques. Crowdsourcing-based spectrum sensing is a promising approach for periodically collecting spectrum measurements over a large geographic area, which is, unfortunately, vulnerable to false spectrum measurements. How to construct an accurate REM in the presence of false measurements remains an open challenge. This paper introduces SecREM, a novel scheme for securely constructing a REM in the presence of false spectrum measurements. SecREM relies on a small number of trusted spectrum measurements whereby to evaluate the trustworthiness of the measurements from mobile users and gradually incorporate the most trustworthy ones to construct an accurate REM. Extensive simulation studies based on a real spectrum measurement dataset confirm the efficacy and efficiency of SecREM.**

I. Introduction

Database-driven Dynamic Spectrum Sharing (DSS) [1], [2] is the de-facto technical paradigm adopted by Federal Communications Commission (FCC) for enhancing spectrum efficiency. In such a system, a geo-location database administrator (DBA) maintains the spectrum availability information in its service region, and secondary users (SUs) are required to inquire the DBA about the availability of any interested spectrum before using it. Current DBAs estimate spectrum availability based on the registered locations and transmission schedules of primary users (PUs) in combination with radio propagation modeling, e.g., FCC Curves [3] based on the Longley-Rice model [4]. Recent measurement studies [5]–[8], however, have shown that such estimations are often inaccurate and tend to be overly conservative for ignoring local environmental factors (e.g., trees and high-rise buildings), resulting in a considerable waste of valuable spectrum opportunities.

978-1-5090-6501-1/17/$31.00

Spectrum sensing can effectively improve the spectrum-estimation accuracy in database-driven DSS systems and is demanded in FCC's 2016 call for proposals for the 3.5 GHz band [9]. In this approach, the DBAs explore a network of spectrum sensors to determine spectrum availability by detecting radio activities on licensed spectrum bands. Large-scale sensor networks, however, are notoriously difficult and expensive to deploy, operate, and maintain, especially in urban areas where DSS is expected to have great potential. Therefore, it has been widely advocated that the DBA only needs to deploy a small number of dedicated spectrum sensors at strategic locations [5], [6] and outsource the majority of spectrum-sensing tasks to ubiquitous mobile users [10], [11]. The feasibility of this approach lies in the deep penetration of mobile devices into everyday life and the wide expectation that future mobile devices can perform spectrum sensing via either internal spectrum sensors or external ones acquired from other parties like the DBA [12]–[18]. With real-time spectrum measurements from dedicated sensors and mobile users, the DBA can construct and maintain a Radio Environmental Map (REM) [19], [20] whereby to determine whether SUs can transmit or not on specific bands at given times and locations.

Crowdsourcing-based REM construction is, unfortunately, vulnerable to false spectrum measurements. In particular, mobile users cannot be fully trusted and may submit false spectrum measurements for various reasons such as faulty spectrum sensors and malicious intents. Since most existing techniques for constructing REM to date [10], [21]–[24] rely on statistical interpolation techniques such as Ordinary Kriging (OK) [25] that are known to be sensitive to outliers [26], even a small number of false measurements can heavily distort the REM, leading to either missed spectrum opportunities or interference to PUs.

Despite the large body of work on secure cooperative spectrum sensing against false spectrum measurements [12]–[14], [27]–[32], how to combine possibly forged spectrum measurements to construct an accurate REM poses unique challenges and remains untouched. In particular, cooperative sensing aims to decide whether a PU at a known location is transmitting or not, whereas secure REM construction intends to estimate the received signal strength (RSS) at every location

of interest from possibly forged local spectrum measurements when the PUs' locations and transmission activities are known. The unique challenges brought by REM construction render prior solutions [12]–[14], [27]–[32] inapplicable. These situations call for sound solutions to construct REM with sufficient accuracy in the presence of false spectrum measurements.

This paper introduces the design and evaluation of SecREM, a novel framework for secure crowdsourced REM construction in the presence of false spectrum measurements. Inspired by the self-labeled techniques [33] proposed for semi-supervised learning, SecREM constructs highly accurate REMs from a small number of trusted measurements and many more untrusted measurements via iterative statistical spatial interpolation. Specifically, an initial REM is constructed using only the trusted measurements, and the resulting REM is then used to evaluate the trustworthiness of the untrusted measurements by comparing predicted RSSs and reported RSSs. In each subsequent iteration, a certain number of remaining measurements deemed most trustworthy are incorporated to refine the REM. This process is repeated until certain terminal condition is met, at which point all remaining untrusted measurements are discarded and the final REM is produced. Our contributions in this paper can be summarized as follows.

- To the best of our knowledge, we are the first to study secure crowdsourced REM construction in the presence of false spectrum measurements.
- We propose SecREM, a novel framework for constructing REM from a small number of trusted measurements and many more untrusted spectrum measurements.
- We confirm the efficacy and efficiency of SecREM via extensive simulation studies using a real spectrum measurement dataset. For example, our simulation results show that even when twenty percent of the measurements are false, SecREM can produce an REM with mean absolute error (MAE) of 2.92 dB which is only 3.62% higher than that of the ideal case as if all the false measurements are known in advance and excluded by the DBA. In contrast, using only trusted measurements and blindly using all spectrum measurements result in MAEs of 3.99 dB and 4.85 dB or 41.6% and 72.1% higher than that of the ideal case, respectively.

The rest of this paper is structured as follows. Related work is discussed in Section II. The system and adversary models along with our design goals are introduced in Section III. The detail design of SecREM is presented in Section IV. We evaluate the performance of SecREM in Section V and conclude this paper in Section VI.

II. Related Work

In this section, we discuss the work most germane to the proposed research.

A. Augmenting Geo-location Database with Spectrum Sensing

Several recent studies [5]–[8] have shown that spectrum availability determined by radio propagation modeling are inaccurate and tend to be overly conservative. Several efforts have been made to augment geo-location database with spectrum sensing. The first line of research is to construct Radio Environmental Map or detailed PU coverage map from local spectrum measurements, where received PU signal strength at every location of interest is either directly measured or estimated via spatial interpolation techniques. Various statistical interpolation methods have been proposed to construct REM for which a recent survey can be found at [34]. Commonly used spatial interpolation techniques include Ordinary Kriging [10], [21]–[24], Universal Kriging [35], Delaunay triangulation [36], spatial simulated annealing [37], and their combination [38]. In [24], [39], [40], Kriging is used to determine the coverage of wireless networks. All these work assume that all the measurements are trusted, while it is well known that these statistical spatial interpolation techniques are sensitive to outliers due to the well-known masking and swamping effects. For example, it was shown in [26] that even a small number of false measurements could significantly affect the predictions at unobserved locations.

B. Secure Cooperative Spectrum Sensing

Tremendous efforts have been made to secure cooperative spectrum sensing, which aims at determining PU activity based on potentially forged spectrum measurements. Proposed approaches include identifying false spectrum measurements via statistical anomaly detection [12], [14], [27]–[29], differentiating malicious spectrum sensors from legitimate ones by tracking their long term behaviors using reputation systems [27], [30], or relying on some trusted nodes [13], [31], [32]. As we discussed in Section I, none of these solutions can be applied to the problem of secure REM construction, in which the PU's location and transmission activity are known, but its signal strength needs to be estimated at every location of interest.

III. System and Adversary Models and Designed Goals

In this section, we introduce our system and adversary models as well as our design goals.

A. System Model

We consider a DSS system shown in Fig. 1, in which a DBA provides spectrum service to SUs in its service region $\mathcal{D}$. The service region $\mathcal{D}$ is divided into N non-overlapping *cell*s of equal size. We assume that there is one PU in $\mathcal{D}$ whose location and transmission schedule are known to the DBA.

The DBA estimates spectrum availability through spectrum sensing by constructing and periodically updating an REM over $\mathcal{D}$. As in [13], [32], we assume that the DBA deploys a small number of stationary spectrum sensors at strategic locations, referred to as *anchor sensor*s hereafter. Anchor sensors can be remotely attested by the DBA and excluded if they are detected as compromised. Due to cost constraints, the DBA cannot afford to deploy too many anchor sensors to cover the entire service region and still relies on the spectrum measurements from the majority of mobile users to ensure the

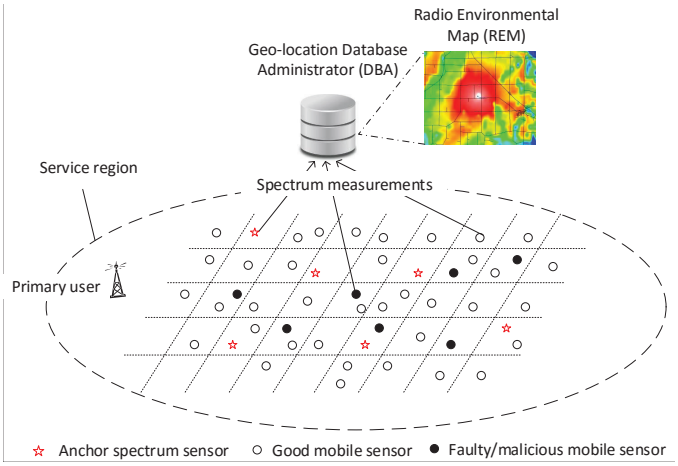


Fig. 1. An exemplary database-driven DSS system.

accuracy of the REM. We hereafter denote by Θ_a the set of anchor sensors and Θ_m the set of mobile sensors.

We assume that the time is divided into epochs of equal length. During each epoch, each sensor $i \in \Theta_a \bigcup \Theta_m$ submits a spectrum measurement $R_i = (Z_i, \mathbf{x}_i)$, where Z_i is the measured RSS (in dBm) at location $\mathbf{x}_i$. Some cells may not have any measurement taken, and some measurements may be taken at locations other than the center of any cell. Given the set of spectrum measurements $\mathcal{R} = \{R_i | i \in \Theta_a \bigcup \Theta_m\}$, the DBA intends to build an REM by estimating the RSS at the center of every cell.

B. Adversary Model

We assume that the DBA is trusted to perform all system operations faithfully and that the spectrum measurements submitted by anchor sensors are trusted. In contrast, mobile sensors may submit false spectrum measurements due to faulty spectrum sensors, intentionally forging spectrum measurements to claim the reward at the DBA without actual sensing, or being hired by the DBA's business competitor to damage its reputation. We assume that false spectrum measurements may be arbitrarily different from the true ones and that the number of false measurements is unknown to the DBA in advance. We do not consider spectrum measurements with forged locations because such measurements are equivalent to the ones with false RSSs at the claimed locations.

Our subsequent discussion focuses on REM construction in the presence of false spectrum measurements. We assume that communications between anchor/mobile sensors and the DBA are properly secured via standard cryptographic techniques such as TLS [41]. Moreover, we do not consider other attacks targeting DSS systems such as primary user emulation attack for which we resort to existing rich literature, e.g., [42].

C. Designed Goals

We design SecREM with the following goals in mind.

- *Resilience to false measurements*: SecREM should produce an REM in the presence of a unknown number of false spectrum measurements with sufficient accuracy. Specifically, SecREM should be able to produce an REM close to the one constructed from all good measurements with an accuracy much higher than either using only trusted spectrum measurements or blindly using all spectrum measurements.
- *Low cost*: SecREM should only need a small number of anchor sensors to achieve high accuracy of the resulting REM.

IV. SecREM Design

In this section, we first give an overview of SecREM and then detail its design.

A. Overview

SecREM is inspired by the self-labeled techniques developed for semi-supervised classification, for which a recent survey can be found at [33]. Self-labeled techniques are proposed to explore a small amount of labeled data with a large amount of unlabeled data for classification. In self-labeled techniques, a classifier is trained based on the labeled data only, which is then applied to the unlabeled data to generate more labeled samples as additional input to refine the classifier. Self-labeled techniques have been shown to surpass the classification performance obtained either by supervised learning with the unlabeled data discarded or by unsupervised learning with the label information discarded.

As an analog to the self-labeled techniques, SecREM constructs an REM by building an initial REM with only trusted measurements. The initial REM is then used to evaluate the trustworthiness of other measurements according to the differences between the estimated RSSs and corresponding reported RSSs. The smaller the difference is, the more trustworthy of the measurement, and vice versa. The DBA then incorporate a fixed number of measurements deemed most trustworthy to refine the initial REM. This process continues until a certain terminal condition is met, and the remaining measurements are discarded. The DBA then uses all the remaining measurements to construct a final REM by predicting the RSS at every other unmeasured location of interest.

SecREM is a general framework that can be integrated with different statistical interpolation techniques. In what follows, we first briefly introduce the background of Ordinary Kriging (OK) [25] and then detail the design of SecREM by taking OK as an example for its overwhelming popularity and satisfactory performance in REM construction [10], [21]–[24], [39], [40].

B. Background on Ordinary Kriging

Kringing [25] refers to a class of geo-statistical spatial interpolation techniques that are originally developed for mining but have been increasingly being used for radio mapping. Under Kringing, the RSS at any location $\mathbf{x}$ is modeled as as a Gaussian random field in the form

$$Z(\mathbf{x}) = \mu(\mathbf{x}) + \delta(\mathbf{x}),$$

where $\mu(\mathbf{x})$ is the mean capturing path loss and shadowing, and $\delta(\mathbf{x})$ represents possible sampling error.

In OK [25], $Z(\mathbf{x})$ is further assumed to be *intrinsic stationary* in the sense that

$$\begin{aligned} &\mathsf{E}[Z(\mathbf{x})] = \mu(\mathbf{x}) = \mu, \\ &\mathsf{E}[(Z(\mathbf{x}_1) - Z(\mathbf{x}_2))^2] = 2\gamma(h) \ , \end{aligned} \tag{1}$$

for all $\mathbf{x} \in \mathcal{D}$, where $\mathsf{E}(\cdot)$ denotes expectation, μ is an unknown constant, $h = ||\mathbf{x}_1 - \mathbf{x}_2||$ is the *distance lag* between two locations, and $\gamma(\cdot)$ is the *semivariogram* function that models the variance between two locations as a function of their distance. This assumption may not hold for original spectrum measurements but has been found acceptable in the literature [10], [21], [22], [24], [39], [40], especially after removing any source of nonlinear trend from measurements through detrending process [23].

C. Detailed Design

On receiving all the measurements $\mathcal{R}$, the DBA first performs detrending on the measurements and then constructs an REM from the detrended measurements in an iterative fashion.

1) Detrending: Detrending original spectrum measurement is usually preferred to make the measurements a better fit for the OK model. SecREM does not rely on any specific detrending procedure but assumes the existence of a suitable one for the received measurements. Below we briefly introduce the detrending procedure proposed in [23] as an example for completeness, which is not our contribution.

In [23], Carrier-to-Interference and Noise Ratio (CINR) measurements are detrended by subtracting the predicted path loss at the measured locations from the original measurements. Specifically, the path loss at any location $\mathbf{x}$ is estimated using the following empirical log-distance model

$$P(\mathbf{x}) = \alpha 10\log_{10}(d) + 20\log_{10}(f) + 32.45 + \epsilon \ , \tag{2}$$

where d is the distance between the $\mathbf{x}$ and the PU, f is the PU's transmitting frequency, 32.45 represents free-space path loss, and α and ϵ are parameters obtained via experimental fitting. For each original measurement $R_i = (Z_i, \mathbf{x}_i)$, the corresponding detrended measurement is then $R'_i = (S_i, \mathbf{x}_i)$, where

$$S_i = Z_i - P(\mathbf{x}_i)$$

is the residue at $\mathbf{x}_i$.

2) Iterative REM Construction Semivariogram: The DBA then constructs an REM in an iterative fashion from $\{S_i | i \in \Theta_t \bigcup \Theta_c\}$ using OK. Specifically, the DBA maintains a trusted sensor set Θ_t and a candidate sensor set Θ_c at all time, where $\Theta_t = \Theta_a$ and $\Theta_c = \Theta_m$ initially. In each iteration, the DBA does the following in sequel.

The DBA first builds an empirical semivariogram $\hat{\gamma}(h)$ from the trusted measurement $\{R'_i | i \in \Theta_t\}$. Specifically, the DBA first computes

$$\hat{\gamma}(h) = \frac{1}{2|\mathcal{P}(h)|} \sum_{(\mathbf{x}_i, \mathbf{x}_j) \in \mathcal{P}(h)} (S_i - S_j)^2,$$

where $\mathcal{P}(h) = \{(\mathbf{x}_i, \mathbf{x}_j) | i, j \in \Theta_t, ||\mathbf{x}_i - \mathbf{x}_j|| = h\}$ is the set of location pairs with distance h. The DBA then fits $\hat{\gamma}(h)$ with a suitable parametric model. For example, the commonly used exponential model is given by

$$\gamma(h; \alpha_1, \alpha_2) = \alpha_1(1 - \exp(\frac{-h}{\alpha_2})) \ ,$$

where α_1 is related to the variance of the signal strength measurements, and α_2 scales the correlation distance of the model. Other popular models include Gaussian, Cauchy, and Spherical models [43]. These parameters can be obtained from the estimated semivariogram through least squares estimator.

The DBA then evaluates the trustworthiness of the measurements based the empirical semivarogram model $\hat{\gamma}(\cdot)$ obtained above to estimate the residues at the locations $\{\mathbf{x}_j | j \in \Theta_c\}$ at which candidate measurements have been submitted. Specifically, given the set of trusted measurements $\{R'_i | i \in \Theta_t\}$, the DBA predicts the residue at each location $\mathbf{x}_j (j \in \Theta_c)$ as

$$\hat{S}(\mathbf{x}_j) = \sum_{i \in \Theta_t} w_i \cdot S(\mathbf{x}_i) = \sum_{i \in \Theta_t} w_i \cdot S_i.$$

where $\sum_{i \in \Theta_t} w_i = 1$ are normalized weights. The estimation error is given by

$$\begin{aligned} \epsilon(\mathbf{x}_j) &= \hat{S}(\mathbf{x}_j) - S(\mathbf{x}_j) \\ &= [w_1, \ldots, w_{|\Theta_t|}, -1] \cdot [S_1, \ldots, S_{|\Theta_t|}, S(\mathbf{x}_j)] \ , \end{aligned}$$

where $S(\mathbf{x}_j)$ is the true residue at $\mathbf{x}_j$ that may be different from the reported residue S_j. It is easy to see that the estimator is unbiased as $\mathsf{E}(\epsilon(\mathbf{x}_j)) = \sum_{i \in \Theta_t} w_i \mu - \mu = 0$. Let $h_{i,j} = ||\mathbf{x}_i - \mathbf{x}_j||$ for all $i, j \in \Theta_t$. Since minimizing the prediction variance of an unbiased predictor is equivalent to minimizing the mean squared error, we have

$$\begin{aligned} \mathsf{Var}(\epsilon(\mathbf{x}_j)) &= \mathsf{E}(\hat{S}(\mathbf{x}_j) - S(\mathbf{x}_j))^2 \\ &= \mathsf{E}(\sum_{i \in \Theta_t} w_i S_i - S(\mathbf{x}_j))^2 \\ &= -\sum_{i \in \Theta_t} \sum_{k \in \Theta_t} w_i w_k \hat{\gamma}(h_{i,k}) + 2 \sum_{i \in \Theta_t} w_i \hat{\gamma}(h_{i,j}) \end{aligned}$$

To find the optimal $\{w_i\}_{i \in \Theta_t}$, the DBA solves the following optimization problem

$$\begin{aligned} \min \quad & -\sum_{i \in \Theta_t} \sum_{k \in \Theta_t} w_i w_k \hat{\gamma}(h_{i,k}) + 2 \sum_{i \in \Theta_t} w_i \hat{\gamma}(h_{i,j}) \\ \text{subject to} \quad & \sum_{i \in \Theta_t} w_i = 1. \end{aligned}$$

The solution to the above optimization problem is given by

$$\begin{pmatrix} w_1 \\ \vdots \\ w_{|\Theta_t|} \\ \nu \end{pmatrix} = \begin{pmatrix} \gamma(h_{1,1}) & \ldots & \gamma(h_{1,|\Theta_t|}) & 1 \\ \vdots & \ddots & \vdots & \vdots \\ \gamma(h_{|\Theta_t|,1}) & \ldots & \gamma(h_{|\Theta_t|,|\Theta_t|}) & 1 \\ 1 & \ldots & 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} \gamma(h_{1,j}) \\ \vdots \\ \gamma(h_{|\Theta_t|,j}) \\ 1 \end{pmatrix}, \tag{3}$$

where ν is a Lagrange multiplier used in the minimization to honor the unbiasedness condition.

The DBA proceeds to evaluate the trustworthiness of each candidate measurement $R'_j (j \in \Theta_c)$ based on the difference between predicted and reported residue values. Specifically,

we define the *inconsistency* of a candidate measurement $R'_j = (S_j, \mathbf{x}_j)$ as

$$I_j = |\sum_{i \in \Theta_t} w_i S_i - S_j| \ , \tag{4}$$

where S_j is the reported residue. The smaller I_j, the more trustworthy measurement R'_j, and vice versa.

The DBA then finds the q candidate sensors whose measurements are deemed most trustworthy, denoted by Θ_q, where q is a system parameter that represents the tradeoff between the computation overhead and accuracy of the final REM. The DBA then moves Θ_q to the trusted sensor set, i.e., $\Theta_t = \Theta_t \bigcup \Theta_q$ and $\Theta_c = \Theta_c \setminus \Theta_q$.

The DBA repeats the above process, i.e., refitting the empirical semivarogram model $\hat{\gamma}(\cdot)$ using the updated trusted measurements $\{R'_i | i \in \Theta_t\}$, predicting the residues at each location $\mathbf{x}_i$ for all $i \in \Theta_c$, evaluating the inconsistency of each measurement R'_i for all $i \in \Theta_c$, and moving the q candidate sensors with the most trustworthy measurements from Θ_c to Θ_t.

The DBA terminates the process upon certain condition is met. In this paper, we investigate three terminal conditions as follows.

- *Condition 1*: The ratio between the number of the trusted sensors and the total number of sensors reaches a predetermined threshold η_1, i.e.,

$$|\Theta_t| / |\Theta_a \bigcup \Theta_m| \geq \eta_1 \ ,$$

  where η_1 is a system parameter.
- *Condition 2*: The number of trusted measurements reaches a predefined threshold, i.e.,

$$|\Theta_t| \geq \eta_2 \ ,$$

  where η_2 is a system parameter.
- *Condition 3*: At least one of the q most trustworthy measurement has inconsistency (i.e., I_j) higher than η_3.

The three terminal conditions correspond to different assumptions about the false spectrum measurements. Specifically, the first terminal condition assumes that the ratio of false measurements is small, and the DBA intends to defend against up to $1 - \eta_1$ ratio of false measurements. The second terminal condition assumes that there are sufficient good measurements, while the ratio of false measurements could be potentially large. Using Terminal Condition 2, the DBA intends to construct a sufficiently accurate REM despite that there might be additional truthful measurements that can be explored. The third terminal condition assumes that false measurements exhibit high inconsistency, i.e., large I_j. Note that the last iteration may add less than q candidate sensors to the trust sensor set. After the above process is terminated, all the measurements from remaining candidate sensors are discarded.

The DBA finally constructs the REM based on the measurements from the trusted sensors. In particular, the DBA refits the empirical semivarogram model using $\{R'_i | i \in \Theta_t\}$. For every cell center $\mathbf{x}_c$, the DBA predicts it residue $\hat{S}(\mathbf{x}_c)$ using Eq. (3) and outputs its estimated RSS as

$$\hat{Z}(\mathbf{x}_c) = \hat{S}(\mathbf{x}_c) + P(\mathbf{x}_c) \ ,$$

where $P(\mathbf{x}_c)$ is the predicted path loss given in Eq. (2).

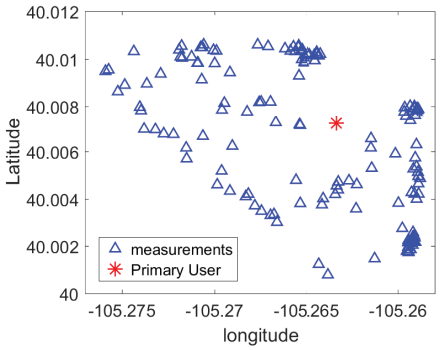


Fig. 2. Measurement/PU locations of `cu/wimax` dataset.

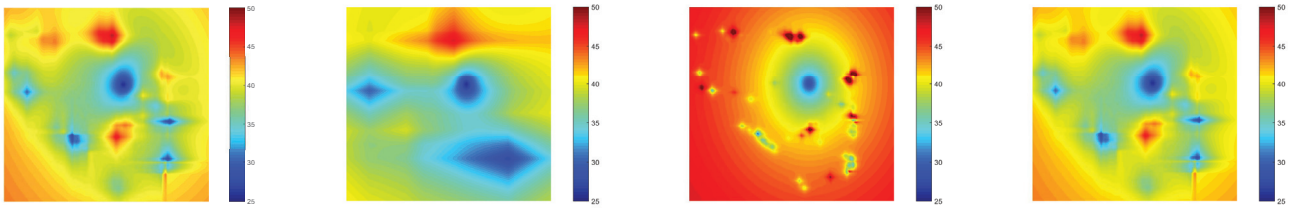
V. Performance Evaluation

In this section, we evaluate the performance of SecREM via simulation using a real spectrum measurement dataset.

A. Dataset

We use the CRAWDAD `cu/wimax` dataset [44] for our simulation studies, which was also used in [23]. The `cu/wimax` dataset was collected at the University of Colorado Boulder (UC) and contains the CINR measurements of the WiMax network consisting of 5 base stations serving the UC campus taken by a portable spectrum analyzer. The measurements were taken on a 100m equilateral triangular lattice and additional measurements taken at random and optimized points. For our purpose, we chose the measurements for channel 308 and BSID 3674210305, which includes 145 measurements at different locations. Fig. 2 shows the locations of the measurements and the PU.

We follow the detrending procedure in [23] to remove the nonlinear trend in the measurements. First, we calculate the distance between the measurement location and the base station at longitude -105.26333 and latitude 40.00722. We then use the predictive model in Eq. 2 to estimate the path loss based on the calculated distance with frequency $f = 2578$ MHz and fitted parameters (path loss exponent $\alpha = 1.22$ and offset $\epsilon = 28.81$). We finally obtain the residue values after deducting the estimated path loss from collected CINR measurements. Since the difference between CINR and actual RSS value is a constant depending on noise floor (e.g., 95 dBm), PU's transmission power, and receiver's antenna gain, we hereafter ignore such constant factors and construct REMs in terms of the CINR values.



(a) ABFM (b) TMO (c) AM (d) SecREM

Fig. 3. Exemplary REMs (in terms of CINR) constructed by SecREM, TMO, AM, and ABFM with 10 trusted and 20 false measurements.

B. Simulation Settings

We divide the 145 measurements into two sets: a testing dataset $\mathcal{R}_t$ with 100 measurements and a validating set $\mathcal{R}_v$ with 45 measurements as the ground truth. For 100 testing measurements, we randomly choose ten measurements as the trusted ones and another 20 measurements as the false ones. Moreover, we call a false measurement R_i with an *attack strength* T (dB) if it reports a $Z_i + T$ where Z_i is the true RSS values [28]. Table 1 summarizes our default simulation settings unless mentioned otherwise.

We mainly use Mean Absolute Error (MAE) to evaluate the performance of RecREM. Specifically, for each measurement $R_i \in \mathcal{R}_v$, let Z_i and $\hat{Z}_i$ be the reported RSSs and estimated RSSs, respectively. The MAE is defined as

$$\text{MAE} = \frac{\sum_{R_i \in \mathcal{R}_v} |Z_i - \hat{Z}_i|}{|\mathcal{R}_v|}.$$

Since SecREM is the first proposal for secure REM construction against false spectrum measurements, we compare the performance of SecREM with three other strategies.

- **Trusted measurements only (TMO)**: the REM constructed using the trusted measurements submitted by anchor sensors only.
- **All measurements (AM)**: the REM constructed using all measurements, including false ones.
- **All but false measurements (ABFM)**: the REM constructed using all but false measurements. Note that since the DBA does not know which measurements are false in advance, the accuracy achieved by all but false measurements is the upper bound of any mechanism that can achieve.

The simulation is done using MATLAB, and every point represents the average of 100 runs each with a distinct seed.

TABLE I
DEFAULT SIMULATION SETTINGS

Para.	Val.	Description.
$\lvert\Theta_t\rvert$	10	The number of trusted measurements
$\lvert\Theta_c\rvert$	90	The number of candidate measurements
	20	The number of false measurements
T	20 dB	Attack strength
q	10	Step length
η_1	80	Terminal condition 1
η_2	80%	Terminal condition 2
η_3	10 dB	Terminal condition 3

C. Simulation Results

We now report our simulation results.

1) Comparison of REMs Constructed by ABFM, TMO, AM, and SecREM: Fig. 3 compares the REMs in terms of CINR constructed by ABFM, TMO, AM, and SecREM, which have a constant offset from the actual RSS values. Fig. 3(a) shows the ideal REM constructed by all good measurements, which can serve as the baseline for other mechanisms. Generally speaking, the closer the REM produced by a mechanism to the ideal REM, the more resilient the mechanism against false spectrum measurements. Fig. 3(b) shows the REM constructed only using ten known trusted measurements from anchor sensors, which is very different from the ideal REM constructed by ABFM and shows that the REM constructed using only a small number of known trusted measurements is highly inaccurate. On the other hand, Fig. 3(c) shows that the REM constructed from all the measurements is highly distorted by the 20 false measurements, which highlights the detrimental impact from even a small number of false measurements. Finally, Fig. 3(d) shows the REM constructing by SecREM. As we can see, the REM is very close to the ideal REM shown in Fig. 3(a), indicating the high resilience of SecREM to false measurements. These exemplary REMs indicate that SecREM outperforms both TMO and AM.

Fig. 4 shows the CDFs of the estimation errors at the locations where validating measurements are taken under ABFM, TMO, AM, and SecREM and the default simulation settings, where SecREM-1, SecREM-2, and SecREM-3 refer to SecREM with terminal condition 1, 2, and 3, respectively. In addition, SecREM-1 and SecREM-2 share the same performance as they are equivalent under the default settings. As we can see, the estimation error is smaller than 4 dB for 70.64% and 70.53% of the measured locations under SecREM-1&2 and SecREM-3, respectively, both of which are very close to 71.82% under ABFM and much superior to 59.03% and 51.91% under TMO and AM, respectively. Moreover, less than 10% of the measured locations have estimation error over 7 dB under both ABFM, SecREM-1&2 and SecREM-3. In contrast, more than 10% of the measured locations have estimation error over 10 dB and 12 dB under TMO and AM, respectively.

Fig. 5 shows the boxplots of the MAEs of ABFM, TMO, AM, SecREM-1&2, and SecREM-3 over 100 runs. The median MAEs under AM, TMO, ABFM, SecREM-1&2, and SecREM-3 are 4.78 dB, 4.03 dB, 2.80 dB, 2.86 dB, and 2.86

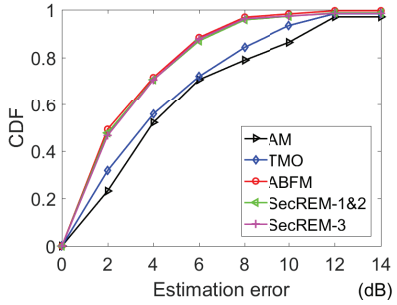


Fig. 4. CDF of estimation errors.

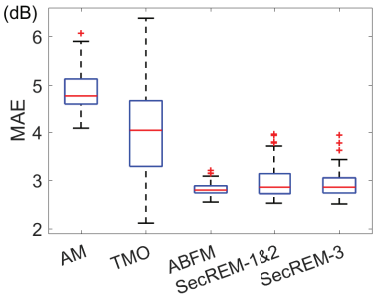


Fig. 5. Boxplot of estimation errors.

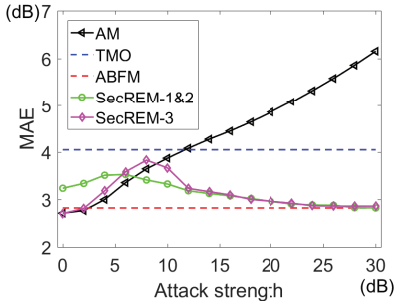


Fig. 6. MAE vs. attack strength.

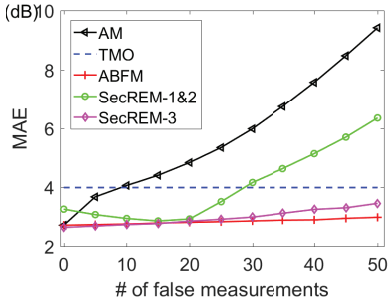


Fig. 7. MAE vs. # of false measurements.

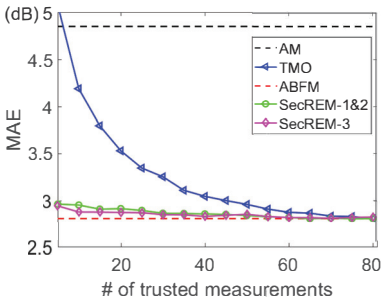


Fig. 8. MAE vs. # of trusted measurements.

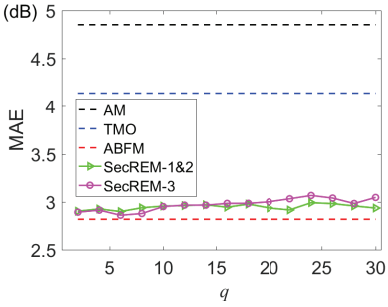
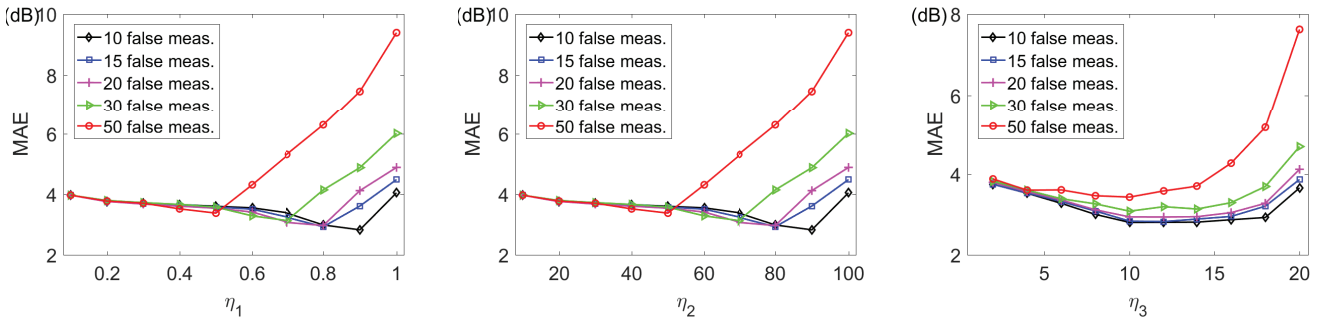


Fig. 9. MAE vs. step length q.

dB, respectively. We can see that overall SecREM achieves smaller MAE than AM and TMO. For the five strategies, the distances between two "whiskers" above and below the box are 1.82 dB, 4.26 dB, 0.53 dB, 1.179 dB, and 0.92 dB, respectively. TMO has the largest distance, indicating that the MAE by TMO highly depends on the locations of the trusted measurements. In contrast, although both SecREM-1&2 and SecREM-3 have several outliers, the distances between first and third quartiles are only 0.41 dB and 0.31 dB, respectively, which are quite small in comparison with 0.56 dB and 1.36 dB in AM and TMO, respectively. These results show that the accuracy of the REMs produced by SecREM is much more stable.

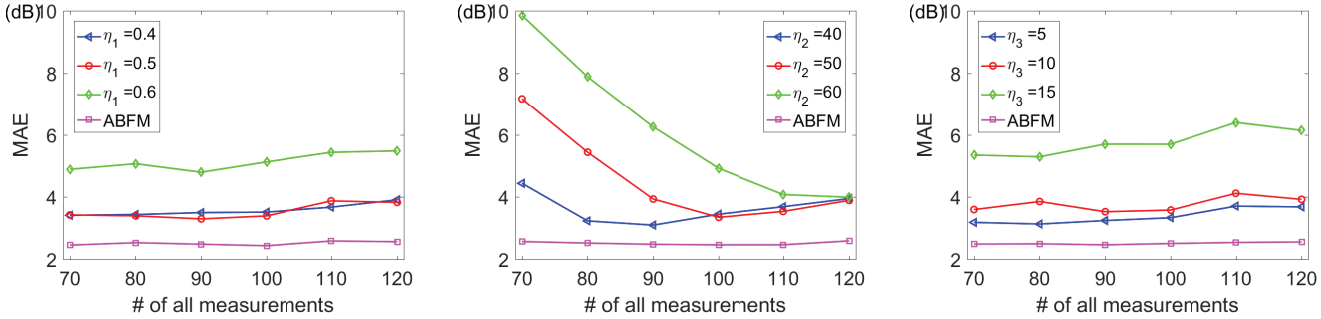
2) Impact of Attack Strength: Fig. 6 shows the MAEs varying with attack strength for ABFM, TMO, AM, and SecREM, where the MAEs of AM and ABFM are not affected by the change in attack strength and are plotted for reference only. As we can see, the MAE of ABFM, i.e., the ideal case, is 2.82 dB, which represents the limit of OK-based REM construction and coincides with the results obtained in the recent measurement study [22]. In addition, the MAE of TMO is larger than 4dB, which again shows that the REM constructed from only a small number of trusted measurements is highly inaccurate. Moreover, the MAE of AM increases close linearly as the attack strength increases and is unbounded. In contrast, as the attack strength increases from 0 to 30 dB, the MAE of SecREM-1 and SecREM-2 initially increases and then gradually decreases until reaches that of ABFM, i.e., the ideal case, and the maximum MAE appears when the attack strength is 6 dB. In addition, SecREM-3 exhibits the similar trend with slightly worse performance than SecREM-1 and SecREM-2 but still outperforms AM and TMO. These trends suggest that SecREM-1, 2 and 3 can effectively bound the impact of false measurements and exclude all the false measurements if the attack strength is too large.

3) Impact of the Number of False Measurements: Fig. 7 shows the MAEs of TMO and SecREM with the number of false measurements varying from 0 to 50, where the MAE of TMO stays at 3.99 dB and is plotted for reference only. We can see that the MAE of AM is the same as that of ABFM when there is no false measurement and increases almost linearly as the number of false measurements increases, which surpasses that of TMO when the number of false measurements exceeds 10. This is anticipated, as the negative impact from false measurements grows as their number increases. On the other hand, the MAE of ABFM slightly increases as the number of false measurements increases, which is due to the corresponding decrease in the number of good measurements. In addition, the MAE of SecREM-1&2 initially declines as the number of false measurements increases. The reason for the initial decline is that SecREM-1&2 may terminate too early when there are only few false measurements, meaning some good measurements are excluded from being used to improve the accuracy of the REM. As the number of false measurements increases, fewer good measurements are discarded, and the MAE of SecREM-1&2 approaches that of ABFM when the number of false measurements reaches 20. As the number of false measurements further increases from 20, the MAE of SecREM-1&2 deteriorates and surpasses that of TMO when the number of false measurements reaches 30. This is



(a) Terminal condition 1 (b) Terminal condition 2 (c) Terminal condition 3

Fig. 10. MAEs of SecREM-1, 2, and 3 with different terminal conditions



(a) SecREM-1 (b) SecREM-2 (c) SecREM-3

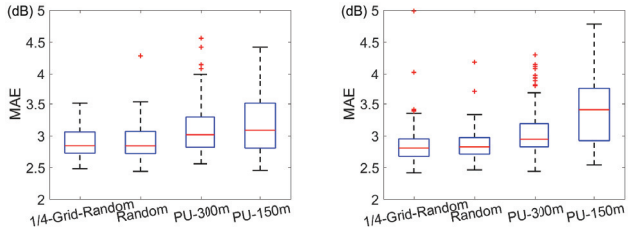
Fig. 11. MAEs of SecREM-1, 2, and 3 vs. the total number of measurements, where half of the measurements are false.

also expected, as SecREM-1&2 always include some false measurements in the final REM under such situations. Finally, the MAE of SecREM-3 increases slowly as the number of false measurements increases and stays below than that of TMO even when half of the measurements are false. The reason is that with the terminal condition parameter properly set, e.g., $\eta_3 = 10$ dB in this case, SecREM-3 can terminate at a more proper time and exclude most of the false measurements, resulting in higher accuracy of the REM even when the false measurements constitute the majority.

4) Impact of the Number of Trusted Measurements: Fig. 8 shows the MAEs of ABFM, AM, and SecREM with the number of trusted measurements, i.e., anchor sensors, varying from 5 to 80, where the total number of good measurements is fixed, and the MAEs of AM and ABFM are not affected and are plotted for reference only. As we can see, the MAEs of AM and ABFM are 4.84 dB and 2.81 dB, respectively. As the number of trusted measurements increases from 5 to 80, the MAE of TMO decreases from 5.07 dB to 2.81 dB, which is anticipated as the more good measurements being used, the higher the accuracy of the resulting REM. Moreover, while we can see that the MAEs of both SecREM-1&2 and SecREM-3 decrease as the number of trusted measurements increases, the gain by having more trusted measurements is relatively small. For example, with only five trusted measurements, the MAEs of SecREM-1&2 and SecREM-3 are 2.96 dB and 2.95 dB, respectively, which decrease to 2.92 dB and 2.88 dB with additional 15 trusted measurements. These results indicate that SecREM-1/2/3 only require a small number of trusted measurements to ensure the high accuracy of resulting REMs.

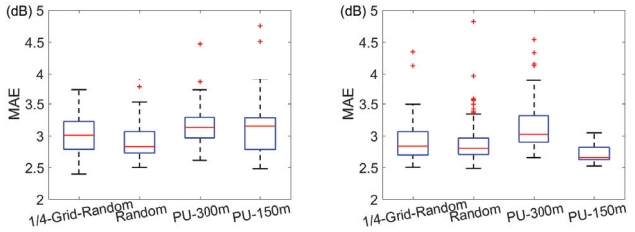
5) Impact of Step Length q: Fig. 9 shows the MAEs of SecREM-1&2 and SecREM-3 varying with step length q, where AM, TMO, and ABFM are not affected by the change in step length and their MAEs are plotted for reference only. As we can see, the MAEs of SecREM-1&2 and SecREM-3 both slightly increase as the step length increases at the beginning. The reason is that the initial REM constructed from the trusted measurements is relatively coarse, and using the initial REM to estimate the trustworthiness of other measurements and select too many at once may have some false measurement included. This will lead to higher MAE for the final REM. As the step length further increases from 20, the MAE of the final REM slightly fluctuate. Overall, the change in step length has limited impact on the accuracy of the resulting REM under our default settings.

6) Impact of Terminal Conditions: We now evaluate the impact of different terminal conditions on the accuracy of the REMs produced by SecREM. We can see from Fig. 10(a) that the MAE of SecREM-1 first decreases as η_1 increases and then increases after $1-\eta_1$ exceeds the ratio of false measurements. This is anticipated, as more good measurements are included with a larger η_1. As long as $1-\eta_1$ is smaller than the ratio



(a) SecREM-1&2 (b) SecREM-3

Fig. 12. MAEs of SecREM-1&2 and 3 vs. anchor sensor placement.



(a) SecREM-1&2 (b) SecREM-3

Fig. 13. MAEs of SecREM-1&2 and 3 vs. locations of false measurements.

of false measurement, SecREM-1 can produce an REM with sufficient accuracy. Similarly, we can see from Fig. 10(b) that the MAE of SecREM-2 first decreases as η_2 increases and then increases after η_2 surpasses the number of good measurements. Finally, Fig. 10(c) shows that the MAE of SecREM-3 first decreases and then increases as η_3 increases. The reason is that when η_3 is set too small, some good measurements would be excluded, leading to higher MAE. On the other hand, if η_3 is set too large, some false measurements will be included into the final REM, leading to higher MAE.

7) Impact of the Total Number of Measurements: We now study the impact of the total number of measurements. Given the limited size of our dataset, we choose 25 measurements as the validating set and randomly choose 70 to 120 measurements as the testing dataset. For each testing dataset, we randomly choose half of the measurements as the false measurements with attack strength 20 dB and then randomly choose another 10 measurements as the trusted measurements. Figs. 11(a) to 11(c) compare the MAEs of SecREM-1, 2, and 3 with ABFM with the total number of measurements varying from 70 to 120.

We can see from Figs. 11(a) to 11(c) that ABFM has the smallest MAE, which is expected. In addition, Fig. 11(a) shows that the MAE of SecREM-1 is relatively insensitive to the change in the total number of measurements. This is expected, as SecREM-1 can produce an REM with sufficient accuracy if the ratio of false measurements is lower than $1-\eta_1$. On the other hand, we can see from Fig. 11(b) that the MAE of the REM produced by SecREM-2 decreases as the total number of measurements increases. This is anticipated, as the number of good measurements increases as the total number of measurements increases, if the ratio of false measurements remains the same. As long as there are more than η_2 good measurements, SecREM-2 can produce an REM with sufficient accuracy. Finally, Fig. 11(c) shows that the MAE of SecREM-3 is relatively insensitive to the change in the total number of measurements. The reason is that when the parameter η_3 is small, SecREM-3 can effectively exclude false measurements.

8) Impact of Anchor Sensor Placement: We now study the impact of the locations of anchor sensors. We consider the following four strategies for placing anchor sensors.

- *1/4-Grid-Random*: Divided the area into four square grids of equal size and randomly select 2 or 3 measurements in each zone to form the 10 trusted measurements.
- *Random*: Randomly select 10 measurements as the trusted measurements.
- *PU-300m*: Randomly select 10 measurements within 300 meters of the PU.
- *PU-150m*: Randomly select 10 measurements within 150 meters of the PU.

Generally speaking, the anchor sensors are distributed most evenly under 1/4-Grid-Random, followed by Random, PU-300m, and PU-150m.

Fig.12 compares the MAEs under the four anchor sensor placement strategies for SecREM-1&2. The median MAEs under 1/4-Grid-Random, Random, PU-300m, and PU-150m over 100 runs are 2.84 dB, 2.84 dB, 3.02 dB, and 3.09 dB, respectively, and the MAEs of PU-300m and PU-150m exhibit larger variance. Generally speaking, the more unevenly distributed the anchor sensors, the higher the MAE, and vice versa, which also holds for SecREM-3 as shown in Fig. 12(b). However, the differences among the MAEs under the four placement strategies are relatively small. Given the limited size of our dataset, we leave the further investigation of the optimal anchor sensor placement as our future work.

9) Impact of the Locations of False Measurements: We consider the same four strategies for the attacker to place false measurements. Fig. 13(a) compares the MAEs under the four strategies for SecREM-1&2. The median MAEs under 1/4-Grid-Random, Random, PU- 300m, and PU-150m over 100 runs are 3.01 dB, 2.83 dB, 3.13 dB, and 3.15 dB, respectively. We can see that placing false measurements close to the PU may result in higher MAE for SecREM-1&2. However, no clear conclusion can be drawn from Fig.13(b) for SecREM-3. We leave further investigation of the optimal placement of false measurements as our future work.

VI. Conclusion

In this paper, we present the design and evaluation of SecREM, a novel framework for secure crowdsourced REM construction in the presence of false spectrum measurements. Inspired by self-labeled techniques developed for semi-supervised learning, SecREM constructs an initial REM from only trusted measurements and gradually refines it by adding more measurements deemed most trustworthy until certain terminal conditions are met. Extensive simulation studies based on a real spectrum measurement dataset confirms that SecREM can produce an REM with sufficient accuracy in the

presence of false measurements. As our future work, we plan to investigate the optimal placement for anchor sensors as well as the optimal attack strategy against SecREM.

ACKNOWLEDGMENT

We would like to thank Dr. Caleb Phillips for answering our questions about CRAWDAD dataset. We are also grateful to the anonymous reviewers for their insightful comments that help improve the quality of this paper. This work was partially supported by the US National Science Foundation under grants CNS-1651954 (CAREER), CNS-1700039, and CNS-1700032.

REFERENCES

[1] D. Gurney, G. Buchwald, L. Ecklund, S. L. Kuffner, and J. Grosspietsch, "Geo-location database techniques for incumbent protection in the tv white space," in *IEEE DySPAN'08*, Oct 2008, pp. 1–9.

[2] R. Murty, R. Chandra, T. Moscibroda, and P. V. Bahl, "Senseless: A database-driven white spaces network," *IEEE Trans. Mobile Comput*, vol. 11, no. 2, pp. 189–203, 2012.

[3] "Second report and order and memorandum opinion and order," FCC, 2008.

[4] A. G. Longley and P. L. Rice, "Prediction of tropospheric radio transmission loss over irregular terrain. a computer method," OTIC Document, Tech. Rep., 1968.

[5] T. Zhang and S. Banerjee, "Inaccurate spectrum databases?: Public transit to its rescue!" in *HotNets'13*, College Park, Maryland, 2013, pp. 6:1–6:7.

[6] T. Zhang, N. Leng, and S. Banerjee, "A vehicle-based measurement framework for enhancing whitespace spectrum databases," in *ACM MobiCom'14*, Maui, Hawaii, USA, 2014, pp. 17–28.

[7] A. Chakraborty and S. R. Das, "Measurement-augmented spectrum databases for white space spectrum," in *ACM CoNEXT'14*, Sydney, Australia, 2014, pp. 67–74.

[8] A. Saeed, K. A. Harras, and M. Youssef, "Towards a characterization of white spaces databases errors: An empirical study," in *WiNTECH'14*, Maui, Hawaii, USA, 2014, pp. 25–32.

[9] "Wireless telecommunications bureau and office of engineering and technology establish procedure and deadline for filing spectrum access system (sas) administrator(s) and environmental sensing capability (esc) operator(s) applications," https://apps.fcc.gov/edocs_public/attachmatch/DA-15-1426A1.pdf.

[10] X. Ying, S. Roy, and R. Poovendran, "Incentivizing crowdsourcing for radio environment mapping with statistical interpolation," in *IEEE DySPAN'15*, Sept 2015, pp. 365–374.

[11] B. Gao, S. Bhattarai, J.-M. J. Park, Y. Yang, M. Liu, K. Zeng, , and Y. Dou, "Incentivizing spectrum sensing in database-driven dynamic spectrum sharing," in *IEEE INFOCOM'16*, San Francisco, CA, April 2016.

[12] O. Fatemieh, R. Chandra, and C. Gunter, "Secure collaborative sensing for crowdsourcing spectrum data in white space networks," in *IEEE DySPAN'10*, Singapore, Apr. 2010.

[13] O. Fatemieh, M. LeMay, and C. Gunter, "Reliable telemetry in white spaces using remote attestation," in *ACSAC'11*, Orlando, FL, 2011.

[14] O. Fatemieh, A. Farhadi, R. Chandra, and C. Gunter, "Using classification to protect the integrity of spectrum measurements in white space networks," in *NDSS'11*, San Diego, CA, Feb. 2011.

[15] A. Min, X. Zhang, and K. Shin, "Detection of small-scale primary users in cognitive radio networks," *IEEE J. Sel. Areas Commun*, vol. 29, no. 2, pp. 349 –361, Feb. 2011.

[16] A. Nika, Z. Zhang, X. Zhou, B. Y. Zhao, and H. Zheng, "Towards commoditized real-time spectrum monitoring," in *HotWireless'14*, Maui, HI, 2014, pp. 25–30.

[17] R. Calvo-Palomino, D. Pfammatter, D. Giustiniano, and V. Lenders, "A low-cost sensor platform for large-scale wideband spectrum monitoring," in *IPSN'15*, Seattle, Washington, 2015, pp. 396–397.

[18] D. Pfammatter, D. Giustiniano, and V. Lenders, "A software-defined sensor architecture for large-scale wideband spectrum monitoring," in *IPSN'15*, Seattle, Washington, 2015, pp. 71–82.

[19] Y. Zhao, L. Morales, J. Gaeddert, K. K. Bae, J. S. Um, and J. H. Reed, "Applying radio environment maps to cognitive wireless regional area networks," in *IEEE DySPAN'07*, April 2007, pp. 115–118.

[20] H. B. Yilmaz, T. Tugcu, F. Alagoz, and S. Bayhan, "Radio environment map as enabler for practical cognitive radio networks," *IEEE Commun. Mag.*, vol. 51, no. 12, pp. 162–169, December 2013.

[21] A. B. H. Alaya-Feki, S. B. Jemaa, B. Sayrac, P. Houze, and E. Moulines, "Informed spectrum usage in cognitive radio networks: Interference cartography," in *PIMRC'08*, Sept 2008, pp. 1–5.

[22] A. Achtzehn, J. Riihijarvi, G. M. Vargas, M. Petrova, and P. Mahonen, "Improving coverage prediction for primary multi-transmitter networks operating in the tv whitespaces," in *IEEE SECON'12*, June 2012, pp. 623–631.

[23] C. Phillips, M. Ton, D. Sicker, and D. Grunwald, "Practical radio environment mapping with geostatistics," in *IEEE DYSPAN'12*, Oct 2012, pp. 422–433.

[24] X. Ying, C. W. Kim, and S. Roy, "Revisiting tv coverage estimation with measurement-based statistical interpolation," in *COMSNETS'15*, Jan 2015, pp. 1–8.

[25] N. A. Cressie and N. A. Cassie, *Statistics for spatial data*. Wiley-Interscience; 2 edition, July 1993.

[26] X. Liu, F. Chen, and C. T. Lu, "Robust prediction and outlier detection for spatial datasets," in *IEEE ICDM'12*, Dec 2012, pp. 469–478.

[27] R. Chen, J. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *IEEE INFOCOM'08*, April 2008, pp. 1876–1884.

[28] A. Min, K. Shin, and X. Hu, "Attack-tolerant distributed sensing for dynamic spectrum access networks," in *IEEE ICNP'09*, Princeton, NJ, oct. 2009, pp. 294–303.

[29] H. Li and Z. Han, "Catch me if you can: An abnormality detection approach for collaborative spectrum sensing in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3554–3565, Nov. 2010.

[30] K. Zeng, P. Paweczak, and D. Cabric, "Reputation-based cooperative spectrum sensing with trusted nodes assistance," *IEEE Commun. Lett.*, vol. 14, no. 3, pp. 226 –228, march 2010.

[31] S. Choi and K. G. Shin, "Secure cooperative spectrum sensing in cognitive radio networks using interference signatures," in *IEEE CNS'13*, Oct 2013, pp. 19–27.

[32] R. Zhang, J. Zhang, Y. Zhang, and C. Zhang, "Secure crowdsourcing-based cooperative spectrum sensing," in *IEEE INFOCOM'13*, Apr. 2013, pp. 2526–2534.

[33] I. Triguero, S. García, and F. Herrera, "Self-labeled techniques for semi-supervised learning: taxonomy, software and empirical study," *Knowledge and Information Systems*, vol. 42, no. 2, pp. 245–284, 2015.

[34] M. Pesko, T. Javornik, A. Kosir, M. Stular, and M. Mohorcic, "Radio environment maps: The survey of construction methods," *KSII T Internet Info*, vol. 8, no. 11, pp. 3789–3809, 2014.

[35] J. Ojaniemi, J. Kalliovaara, A. Alam, J. Poikonen, and R. Wichman, "Optimal field measurement design for radio environment mapping," in *CISS'13*, March 2013, pp. 1–6.

[36] Y. Dai and J. Wu, "Integration of spectrum database and sensing results for hybrid spectrum access systems," in *MASS'15*, Oct 2015, pp. 28–36.

[37] J. Ojaniemi, J. Kalliovaara, J. Poikonen, and R. Wichman, "A practical method for combining multivariate data in radio environment mapping," in *PIMRC'13*, Sept 2013, pp. 729–733.

[38] A. Achtzehn, J. Riihijarvi, and P. Mahonen, "Improving accuracy for tvws geolocation databases: Results from measurement-driven estimation approaches," in *IEEE DySPAN'14*, April 2014, pp. 392–403.

[39] A. Konak, "A kriging approach to predicting coverage in wireless networks," *Int. J. Mob. Netw. Des. Innov.*, vol. 3, no. 2, pp. 65–71, Jan. 2009.

[40] H. Braham, S. B. Jemaa, B. Sayrac, G. Fort, and E. Moulines, "Low complexity spatial interpolation for cellular coverage analysis," in *WiOpt'14*, May 2014, pp. 188–195.

[41] T. Dierks and E. Rescorla, "The transport layer security (TLS) protocol," RFC 4346, Apr. 2006.

[42] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *IEEE S&P'10*, Washington, DC, USA, 2010, pp. 286–301.

[43] N. Cressie, "Fitting variogram models by weighted least squares," *Mathematical Geology*, vol. 17, no. 5, pp. 565–586, 1985.

[44] M. Ton and C. Phillips, "CRAWDAD dataset cu/wimax (v. 2012-06-01)," Downloaded from http://crawdad.org/cu/wimax/20120601, Jun. 2012.