A Spatiotemporal Approach for Secure Crowdsourced Radio Environment Map Construction

Yidan Hu, *Student Member, IEEE*, and Rui Zhang, *Member, IEEE*

***Abstract*— Database-driven Dynamic Spectrum Sharing (DSS) is the de-facto technical paradigm adopted by Federal Communications Commission for increasing spectrum efficiency, which allows licensed spectrum to be opportunistically used by secondary users. In database-driven DSS, a geo-location database administrator (DBA) maintains spectrum availability information over its service region in the form of a Radio Environment Map (REM), where the received signal strength from the primary user at every location is either directly measured via spectrum sensing or estimated via statistical spatial interpolation. Crowdsourcing-based spectrum sensing is a promising approach for periodically collecting spectrum measurements over a large geographic area but is unfortunately vulnerable to false spectrum measurements. Despite a large body of prior work on secure cooperative spectrum sensing, how to construct an accurate REM in the presence of false measurements remains an open challenge. In this paper, we introduce ST-REM, a novel spatiotemporal approach for securely constructing an REM in the presence of false spectrum measurements. Inspired by the self-label techniques developed for semi-supervised learning, ST-REM iteratively constructs an REM from a small number of spectrum measurements from trusted anchor sensors and many more measurements from mobile users. During each iteration, the DBA evaluates the trustworthiness of each measurement by jointly considering its spatial fitness with other trusted measurements and the mobile user's long-term behavior. By gradually incorporating the most trustworthy spectrum measurements, the DBA is able to construct a REM with high accuracy. Extensive simulation studies using a real spectrum measurement dataset confirm the efficacy and efficiency of ST-REM.**

***Index Terms*— Dynamic spectrum sharing, crowdsourcing, spectrum sensing, radio environment map, security.**

I. Introduction

DATABASE-DRIVEN Dynamic Spectrum Sharing (DSS) is the de facto technical paradigm adopted by Federal Communications Commission (FCC) for meeting the ever-growing spectrum demand by allowing secondary users to opportunistically access licensed spectrum bands without causing interference to primary users' transmissions [2], [3]. In a database-driven DSS system, a geo-location database administrator (DBA) maintains the spectrum availability in its service region and manages spectrum access from secondary users. Any secondary user who wants to access a licensed spectrum band is required to inquire the DBA, which may either grant or deny the spectrum-access request based on the spectrum availability at the desired time and location.

Effectively enhancing spectrum utilization requires accurate spectrum availability information, for which a widely advocated approach is to let the DBA construct and maintain a Radio Environmental Map (REM) over its service region. The REM concept [4], [5] was originally proposed as an abstraction of radio environments represented by a distributed database for storing information and knowledge of the radio environment to support a wide range of spectrum-related functionalities. Following the recent work [6], we consider an REM as a map characterizing primary users' radio activities, in which the received signal strength (RSS) from the primary user at every location of interest is either directly measured via spectrum sensing or estimated using proper statistical spatial interpolation techniques.

Maintaining an accurate REM requires the DBA to periodically collect many spectrum measurements over a large geographic region, which can be accomplished in mainly two ways. A straightforward approach is to deploy a network of spectrum sensors for detecting radio activities on licensed spectrum bands. However, it is well known that large-scale sensor networks are expensive to deploy and difficult to operate and maintain. Therefore, it has been widely advocated that the DBA only needs to deploy a small number of dedicated spectrum sensors at strategic locations [7], [8] and outsource the majority of spectrum-sensing tasks to ubiquitous mobile users. 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 [9]–[15].

Crowdsourcing-based REM construction is, unfortunately, vulnerable to false spectrum measurements, which contain RSS values much higher (or lower) than the true RSS measurements. In particular, mobile users cannot be fully trusted and may submit false spectrum measurements due to various

Manuscript received March 23, 2019; revised January 16, 2020; accepted May 2, 2020; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor Y. Chen. This work was supported in part by the National Science Foundation of the United States under Grant CNS-1651954(CAREER), Grant CNS-1700039, Grant CNS-1718078, and Grant CNS-1933047. The preliminary version of this article titled "Secure crowdsourced Radio Environment Map construction" was published in the proceedings of the IEEE ICNP, 2017. *(Corresponding author: Rui Zhang.)*

The authors are with the Computer and Information Sciences Department, University of Delaware, Newark, DE 19716 USA (e-mail: yidanhu@udel.edu; ruizhang@udel.edu).

Digital Object Identifier 10.1109/TNET.2020.2992939

reasons. For example, a good mobile user may submit false spectrum measurements because of faulty spectrum sensor. As another example, a selfish mobile user may submit forged spectrum measurements without actual sensing to save battery. Last but not the least, a malicious mobile user may be hired by the DBA's business competitor to submit false spectrum measurements to damage the DBA's reputation. Since most existing techniques for REM construction [16]–[20] rely on statistical interpolation techniques, eg. Ordinary Kriging, that are known to be sensitive to outliers [21], even a small number of false measurements can heavily distort the REM, leading to either missed spectrum opportunities or harmful interference to primary users' transmissions.

Despite the large body of work on secure cooperative spectrum sensing against false spectrum measurements [9]–[11], [22]–[27], how to construct an accurate REM from possibly false spectrum measurements poses new challenges. In particular, secure cooperative sensing aims to decide whether a primary user at a known location is transmitting or not, whereas REM construction intends to estimate the RSS from the primary user at every location of interest where the primary user's transmission activity is known. The unique challenges brought by REM construction render prior solutions [9]–[11], [22]–[27] inapplicable. These situations call for sound solutions to construct REM with high accuracy in the presence of false spectrum measurements.

To tackle this challenge, we introduce ST-REM, a novel spatiotemporal approach for securely constructing REMs in the presence of false spectrum measurements. Inspired by self-labeled techniques [28] originally developed for semi-supervised learning, ST-REM 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 from dedicated spectrum sensors and then gradually refined by incorporating the most trustworthy measurements from the remaining ones. The key ingredient of ST-REM is a novel mechanism for evaluating of the trustworthiness of every spectrum measurement submitted by mobile users, which jointly considers the measurement's spatial and temporal trustworthiness. The former is evaluated based on the measurement's spatial fitness with other measurements that have already been deemed trustworthy. The latter, on the other hand, is evaluated by tracking the mobile user's long-term behavior, which provides strong indication for the quality of the measurement he/she submits in the current epoch. Using the most trustworthy spectrum measurements, the DBA is able to filter out false ones and construct an REM with high accuracy. 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 introduce ST-REM, a novel approach for constructing REM from a small number of trusted measurements from dedicated spectrum sensors and many more from untrusted mobile users. The accuracy of the resulting REM is achieved by jointly considering the spatial and temporal trustworthiness of the measurements from mobile users and constructing the REM using only the most trustworthy ones.
- The efficacy of ST-REM is confirmed 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, ST-REM can produce an REM with mean absolute error (MAE) of 2.75 dB, which is only 2.83% higher than the case where all false measurements are known in advance and excluded by the DBA.

The rest of this paper is structured as follows. Related work is discussed in Section II. We introduce the system and adversary models along with the design goals in Section III. Section IV presents the design of ST-REM. We evaluate the performance of ST-REM in Section V. Section VI concludes this paper.

II. Related Work

In this section, we discuss prior work in several areas that are most germane to our work.

A. REM Construction via Statistical Spatial Interpolation

There have been a number of attempts to improve the spectrum estimation accuracy at the DBA by constructing an REM or detailed PU coverage map from spectrum measurements through statistical spatial interpolation, for which a recent survey can be found at [29].

Ordinary Kriging is the most popular statistical spatial interpolation technique for radio mapping. Alaya-Feki *et al*. [16] introduced a solution for constructing a map of received signal strength from radio measurements using Ordinary Kriging. In [17], Achtzehn *et al*. conducted a large-scale measurement campaign and demonstrated that spatial interpolation techniques such as Ordinary Kriging outperform well-known propagation models in predicting transmitter's signal strengths in the TV whitespace. Another measurement study was reported in [18], in which Phillips *et al*. used Ordinary Kriging to estimate the coverage of a 2.5 GHz WiMax network in a US university campus. A similar study appeared in [30], which showed that the accuracy of TVWS geo-location database can be improved by predicting the primary user's signal strength with a relatively small number of measurements using Ordinary Kriging. The advantage of Ordinary Kriging over model-based predication such as Longley-Rice model, FCC F-Curves, and k nearest neighbor, is later reconfirmed by another measurement study in Seattle, WA in [19]. Crowdsourcing-based REM construction using Ordinary Kriging was firstly studied in [20], in which Ying *et al*. introduced an incentive mechanism to stimulate mobile users' participation.

Other statistical spatial interpolation techniques have also been used for radio mapping. Ojaniemi *et al*. explored several methods, including Ordinary Kriging, Cokriging, and spatial simulated annealing, for integrating field measurements into radio propagation model [31]. Dai and Wu [32] proposed a framework for integrating spectrum sensing results and

spectrum database via Delaunay triangulation. Delaunay triangulation was also used in [30] to predict the signal strengths at unmeasured locations.

All these works assume that all the measurements are trusted, while it is well known that these statistical spatial interpolation techniques are sensitive to outliers due to masking and swamping effects. For example, it was shown in [21] that even a small number of false measurements can significantly affect the predictions at unobserved locations.

B. Secure Cooperative Spectrum Sensing

Secure cooperative spectrum sensing has been studied extensively in the past decade, for which the goal is to determine whether or not a PU at a known location is transmitting from potentially false spectrum measurements. Existing solutions can be generally classified into three categories.

The first category detects and filters out false spectrum measurements via statistical anomaly detection. In [23], Min *et al*. proposed an attack-tolerant distributed sensing protocol by exploring shadow fading correlation to detecting abnormal spectrum sensing results. A Bayesian-based approach was introduced in [33] to evaluate the suspicious level of spectrum sensing reports whereby to filter out potential false ones. In [34], Wang *et al*. introduced a joint spectrum sensing and access framework based on statistical hypothesis testing to cope with false spectrum sensing reports. A secure cooperative spectrum sensing scheme was introduced in [35] to detect false sensing reports with M-ary quantized sensing data.

The second category uses reputation system to track sensors' long term behaviors to differentiate bad sensors from good ones. Typically, every sensor's reputation score is computed based on the accuracy of their past sensing measurements [22] or whether its local decision matches the global network decision [25]. A sensor is considered misbehaving if its reputation score drops below certain threshold. For example, a reputation-based detection scheme is introduced in [36] in which sensing reports from a sensor would be excluded from the fusion process if its reputation score exceeds certain threshold. More recently, reputation score is incorporated into learning process to determine possible punishment for secondary users with poor sensing performance [37].

The third category relies on machine learning techniques to differentiate false measurements from good ones. In [11], the authors proposed to train a classifier using Support Vector Machines from reliable sensing reports whereby to detect and filter false spectrum measurements. A reinforcement-learning-based user selection method is proposed in [37] to select secondary users according to their past performance.

Finally, it has been shown in [26], [27] that trusted sensors can be used to defend against false measurements. For example, PUET [26] is a technique that explores a trusted transmitter transmitting test signals to detect sensing data falsification attacks. Reputation-based mechanisms have also been integrated with trusted users in [25], [27]. Furthermore, trusted measurements are also used as training data for machine learning solutions [11].

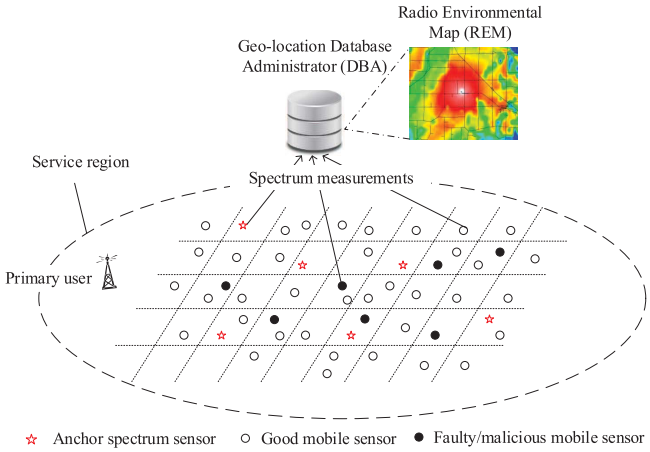


Fig. 1. An exemplary database-driven DSS system.

As 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 need be estimated at every location of interest.

C. False Data Injection Attack in Mobile Crowdsensing

The attack tackled in this paper can be viewed as a special case of the false data injection attack in general crowdsensing systems, which has been studied in other contexts in the past. Yang *et al*. [38] introduced an unsupervised learning approach to filter out anomalous sensing data by evaluating mobile users' sensing qualities and long-term reputations. A similar scheme was introduced in [39] to improve data trustworthiness in crowdsourcing-based positioning systems. More recently, data poisoning attack was studied in [40], [41], where Miao *et al*. introduced several attack strategies to allow malicious workers to maximize attack utility while evading detection. Xie *et al*. [42] detect false sensing data according by exploiting the observation that the matrix formed by real measurements has lower rank than that of the false data. None of these works can be directly applied for secure crowdsourced REM construction.

III. Problem Formulation

In this section, we first introduce the system and adversary models and then our design goals.

A. System Model

Fig. 1 shows an exemplary database-driven DSS system. We consider a DBA that provides spectrum access service to secondary users in its service region $\mathcal{D}$. While there could be multiple PUs in $\mathcal{D}$, we assume that there is one primary user transmitting in every epoch and that the locations and transmission schedules of all primary users are known to the DBA. For simplicity, our subsequent discussion considers a single primary user.

The DBA estimates the spectrum availability through spectrum sensing and constructing and periodically updating an

REM over $\mathcal{D}$. As in [10], [27], 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, referred to as *mobile sensor*s hereafter to ensure the accuracy of the REM. We subsequently 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. At the beginning of each epoch, every 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 $\mathbf{x}_i$. We assume that the service region $\mathcal{D}$ is divided into N non-overlapping *cell*s of equal size. Some cells may not have any measurement taken, and the locations at which measurements are taken may not be the center of any cell. Given the set of spectrum measurements $\mathcal{R} = \{R_i | i \in \Theta_a \bigcup \Theta_m\}$, the DBA's goal is to construct an REM by estimating the RSS at the center of every cell.

B. Adversary Model

The DBA is trusted to faithfully perform all system operations, and the spectrum measurements submitted by anchor sensors are trusted. In contrast, mobile sensors may submit false spectrum measurements due to faulty spectrum sensors, 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 do not differentiate between noisy measurements submitted by users with faulty sensors and forged measurements submitted by malicious users but regard both of them as false measurements, which may contain RSS values arbitrarily different from the true RSS measurements. Similarly, we do not specifically consider spectrum measurements with forged locations because such measurements are equivalent to false measurements at the claimed locations. We assume that the attacker can submit false RSS measurements in different epochs following arbitrary strategy unknown to the DBA. We also assume that the number of false measurements is unknown to the DBA in advance.

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 secured via standard cryptographic techniques such as TLS [43]. Moreover, we do not consider incentive mechanism design for stimulating mobile users' participation or other attacks targeting general DSS systems such as jamming attack, for which resort to existing rich literatures such as [44], [45].

C. Designed Goals

ST-REM is designed with the following goals in mind.

- *Resilience against false spectrum measurements*: ST-REM should produce an REM in the presence of unknown number of false spectrum measurements with high accuracy. In particular, it should produce an REM with much higher accuracy than either using only trusted spectrum measurements from anchor sensors or blindly using all spectrum measurements.
- *Low deployment cost*: ST-REM should only require a small number of anchor sensors to ensure sufficiently high accuracy of the resulting REM.

IV. ST–REM: A Spatiotemporal Approach

In this section, we first give an overview of ST-REM and introduce the background of Ordinary Kriging, the interpolation technique used by ST-REM. We then detail the design of ST-REM.

A. Overview

ST–REM is designed to construct highly accurate REMs using a small number of trusted measurements and many untrusted measurements via iterative statistical spatial interpolation. This approach is inspired by the self-labeled techniques [28] proposed for semi-supervised learning with the goal of exploring a small amount of labeled data and a large amount of unlabeled data for classification [28]. In self-labeled techniques, an initial 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 achieved by either supervised learning where all unlabeled data are discarded or unsupervised learning where all label information is ignored.

As an analogue to self-labeled techniques, ST-REM constructs an REM in an iterative fashion. In each epoch, on receiving all the spectrum measurements, an initial REM is constructed using only the trusted measurements from anchor sensors. In each subsequent iteration, a fixed number of remaining measurements deemed most trustworthy are incorporated to refine the REM. This process continues until certain terminal condition is met, at which point all remaining measurements are discarded and the final REM is produced.

A key component of ST-REM is the evaluation of the trustworthiness of measurements from mobile users. In particular, ST-REM calculates a spatial trust score and a temporal trust score for every measurement. The spatial trust score is computed based on the measurement's spatial fitness with the REM constructed from the measurements that have already been deemed trustworthy. The temporal trust score, on the other hand, is computed from the mobile sensor's past performance, which provides strong indication for the quality of the measurement he/she submits in the current epoch. The overall trust score of the measurement is obtained by combining its spatial and temporal trust scores.

While ST-REM is general in the sense that it can be integrated with different statistical interpolation techniques, we take Ordinary Kriging [46] as an example to illustrate its design for Ordinary Kriging's overwhelming popularity and satisfactory performance in REM construction [16]–[20], [47], [48]. In what follows, we first briefly introduce the background of Ordinary Kriging and then detail the design of ST-REM.

B. Background on Ordinary Kriging

Kriging [46] is a class of geo-statistical spatial interpolation techniques originally developed for mining but have been increasingly being used for radio mapping. Under Kriging, the RSS at any location $\mathbf{x}$ is modeled as a Gaussian random field in the form

$$Z(\mathbf{x}) = \mu(\mathbf{x}) + \delta(\mathbf{x}), \tag{1}$$

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

In Ordinary Kriging [46], $Z(\mathbf{x})$ is further assumed to be *intrinsic stationary* in the sense that

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

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 $\mathbf{x}_1$ and $\mathbf{x}_2$, and $\gamma(\cdot)$ is the *semivariogram* function that models the variance between two locations as a function of their distance. The assumption of intrinsic stationary may not hold for spectrum measurements but has been found acceptable in the literature [16], [17], [19], [20], [47], [48], especially after removing possible source of nonlinear trend from measurements through a proper detrending process [18].

C. Detailed Design of ST-REM

In each epoch, the DBA constructs an REM from the set of measurements $\mathcal{R} = \{R_i | i \in \Theta_a \bigcup \Theta_m\}$ it receives in three steps. First, the DBA performs detrending process to the measurements to remove possible nonlinear trend from the measurements so that the residue measurements fit the Ordinary Kriging model better. Second, the DBA constructs an REM from the detrended measurements in an iterative fashion. Finally, the DBA adds the detrended values back to generate a final REM.

1) Detrending: Detrending is the process of removing any non-linear trend from the original spectrum measurements, which is usually preferred as the resulting detrended measurements would better fit the Ordinary Kriging model [49]. Specifically, given an original spectrum measurement $R_i = (Z_i, \mathbf{x}_i)$ from a mobile or anchor sensor, the corresponding detrended measurement is given by $R'_i = (S_i, \mathbf{x}_i)$, where

$$S_i = Z_i - P(\mathbf{x}_i) \tag{3}$$

is the residue RSS at $\mathbf{x}_i$, and $P(\mathbf{x}_i)$ is the RSS at $\mathbf{x}_i$ predicted by a suitable radio propagation model. ST-REM does not rely on any particular detrending procedure but assumes the existence of a suitable one for the received measurements. For completeness, we will present an exemplary detrending procedure adopted from [18] in Section V-B.

2) Iterative Measurement Selection: Given the set of detrended measurements $\{R'_i | i \in \Theta_t \bigcup \Theta_c\}$, the DBA gradually selects a set of measurements in an iterative fashion for REM construction. 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.

First, for every candidate measurement $R'_j, j \in \Theta_c$, the DBA calculates a trust score T_j. The process of calculating T_j is deferred to Section IV-C.3. Second, the DBA finds the q measurements with the highest trust scores, denoted by Θ_q, where q is a system parameter that represents the tradeoff between computation overhead and accuracy of the final REM. Third, the DBA 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 selection process is terminated if the ratio between the number of trusted measurements and the total number of measurements reaches a predetermined threshold η, i.e.,

$$\frac{|\Theta_t|}{|\Theta_a \bigcup \Theta_m|} \geq \eta \ . \tag{4}$$

All the remaining candidate measurements $\{R'_j | j \in \Theta_c\}$ are then discarded.

3) Spatiotemporal Trustworthiness Evaluation: A key component of ST–REM is a novel method to evaluate the trustworthiness of a candidate measurement by jointly considering its spatial fitness with other trusted measurements and the sensor's past performance. Specifically, for every candidate measurement $R'_j, j \in \Theta_c$, the DBA calculates a spatial trust score and a temporal trust score and then combine the two into an overall trust score.

Spatial Trust Score: The spatial trust score of a measurement $R'_j, j \in \Theta_c$, characterizes its spatial fitness with current trusted measurements $\{R'_i | i \in \Theta_t\}$. The key idea is to construct an REM using the current trusted measurements whereby to predict the RSS value at the candidate measurement's location $\mathbf{x}_j$. The smaller the difference between the reported RSS value and the predicted RSS value, the better R'_j fits the current trusted measurements, the more trustworthy of the candidate measurement, and vice versa. In particular, the spatial trust score of each measurement R'_j is calculated as follows.

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

$$\hat{\gamma}(h) = \frac{1}{2|\mathcal{P}(h)|} \sum_{(\mathbf{x}_i, \mathbf{x}_k) \in \mathcal{P}(h)} (S_i - S_k)^2, \tag{5}$$

where $\mathcal{P}(h) = \{(\mathbf{x}_i, \mathbf{x}_k) | i, k \in \Theta_t, ||\mathbf{x}_i - \mathbf{x}_k|| = h\}$ is the set of location pairs with distance h. The DBA then fits $\hat{\gamma}(h)$ with a suitable parametric model. There are several popular parametric models in Ordinary Kriging, such as Gaussian, Cauchy, and Spherical models [50]. In this paper, we choose the commonly used exponential model, which is given by

$$\gamma(h; \alpha_1, \alpha_2) = \alpha_1 (1 - \exp(\frac{-h}{\alpha_2})), \tag{6}$$

where α_1 is related to the variance of the spectrum measurements, and α_2 scales the correlation distance of the model. These parameters can be obtained from the estimated semivariogram via least squares estimator.

Second, the DBA estimates the residue RSS at location $\mathbf{x}_j$ at which candidate measurement R'_j was taken using the empirical semivarogram model $\hat{\gamma}(\cdot)$. Specifically, the DBA predicts the residue RSS at location $\mathbf{x}_j$ as a linear combination

of the trusted residual measurements $\{R'_i | i \in \Theta_t\}$ given by

$$\hat{S}(\mathbf{x}_j) = \sum_{i \in \Theta_t} w_i \cdot S_i, \tag{7}$$

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

$$\begin{aligned} \epsilon(\mathbf{x}_j) &= \hat{S}(\mathbf{x}_j) - S(\mathbf{x}_j) \\ &= (w_1, \ldots, w_{|\Theta_t|}, -1) \cdot (S_1, \ldots, S_{|\Theta_t|}, S(\mathbf{x}_j)), \end{aligned} \tag{8}$$

where $S(\mathbf{x}_j)$ is the true RSS residue at $\mathbf{x}_j$ that may be different from the reported residue S_j. It is easy to see that the above estimator is unbiased as

$$\begin{aligned} \mathsf{E}[\epsilon(\mathbf{x}_j)] &= \sum_{i \in \Theta_t} w_i \mathsf{E}[S_i] - \mathsf{E}[S(\mathbf{x}_j)] \\ &= \sum_{i \in \Theta_t} w_i \mathsf{E}[S(\mathbf{x}_i)] - \mathsf{E}[S(\mathbf{x}_j)] \\ &= \sum_{i \in \Theta_t} w_i \mu - \mu \\ &= 0. \end{aligned} \tag{9}$$

Let $h_{i,k} = ||\mathbf{x}_i - \mathbf{x}_k||$ for all $i, k \in \Theta_t$ and $h_{i,j} = ||\mathbf{x}_i - \mathbf{x}_j||$ for all $i \in \Theta_t, j \in \Theta_m$. Since minimizing the prediction variance of an unbiased predictor is equivalent to minimizing the mean squared error, we have

$$\begin{aligned} \mathsf{Var}[\epsilon(\mathbf{x}_j)] &= \mathsf{E}[(\hat{S}(\mathbf{x}_j) - S(\mathbf{x}_j))^2] \\ &= \sum_{i \in \Theta_t} \sum_{k \in \Theta_t} w_i w_k \mathsf{E}[S(\mathbf{x}_i) S(\mathbf{x}_k)] \\ &\quad - 2 \sum_{i \in \Theta_t} w_i \mathsf{E}[S(\mathbf{x}_i) S(\mathbf{x}_j)] + \mathsf{E}[(S(\mathbf{x}_j))^2] \\ &= -\frac{1}{2} \sum_{i \in \Theta_t} \sum_{k \in \Theta_t} w_i w_k \mathsf{E}[(S(\mathbf{x}_i) - S(\mathbf{x}_k))^2] \\ &\quad + \sum_{i \in \Theta_t} w_i \mathsf{E}[(S(\mathbf{x}_i) - S(\mathbf{x}_j))^2] \\ &= -\sum_{i \in \Theta_t} \sum_{k \in \Theta_t} w_i w_k \hat{\gamma}(h_{i,k}) + 2 \sum_{i \in \Theta_t} w_i \hat{\gamma}(h_{i,j}) \end{aligned} \tag{10}$$

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

$$\begin{aligned} &\text{mininize } -\sum_{i \in \Theta_t} \sum_{k \in \Theta_t} w_i w_k \hat{\gamma}(h_{i,k}) + 2 \sum_{i \in \Theta_t} w_i \hat{\gamma}(h_{i,j}), \\ &\text{subject to } \sum_{i \in \Theta_t} w_i = 1. \end{aligned} \tag{11}$$

The Lagrangian associated with the optimization problem is given by

$$\begin{aligned} \mathcal{L}(\mathbf{w}, \nu) = &-\sum_{i \in \Theta_t} \sum_{k \in \Theta_t} w_i w_k \hat{\gamma}(h_{i,k}) + 2 \sum_{i \in \Theta_t} w_i \hat{\gamma}(h_{i,j}) \\ &+ \nu \Big(\sum_{i \in \Theta_t} w_i - 1 \Big), \end{aligned} \tag{12}$$

where ν is the Lagrange multiplier. Taking the partial derivatives of $\mathcal{L}(\mathbf{w}, \nu)$ with respect to the $\{w_i\}_{i \in \Theta_t}$ and ν, we can obtain

$$\begin{cases} \dfrac{\partial \mathcal{L}}{\partial w_i} = 0, \quad \forall i \in \Theta_t, \\ \dfrac{\partial \mathcal{L}}{\partial \nu} = 0. \end{cases}$$

The solution to the above optimization problem is given by

$$\begin{pmatrix} w_1 \\ \vdots \\ w_{|\Theta_t|} \\ \nu \end{pmatrix} = \begin{pmatrix} \gamma(h_{1,1}) & \ldots & \gamma(h_{1,|\Theta_t|}) & 1 \\ \vdots & \ddots & \vdots & \vdots \\ \gamma(h_{|\Theta_t|,1}) & \ldots & \gamma(h_{|\Theta_t|,|\Theta_t|}) & 1 \\ 1 & \ldots & 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} \gamma(h_{1,j}) \\ \vdots \\ \gamma(h_{|\Theta_t|,j}) \\ 1 \end{pmatrix}, \tag{13}$$

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

Under the optimized weights given in Eq. (13), the difference between the reported RSS value S_j and predicted RSS value S_j is given by $|\sum_{i \in \Theta_t} w_i S_i - S_j|$. Intuitively, the smaller the difference, the better measurement R'_j fits with other trusted measurements $\{R'_i | i \in \Theta_t\}$, and vice versa. Let $\epsilon_{\max}$ be the maximum estimation error, which we set to be the maximum detrended RSS among all anchor sensors, i.e., $\max\{S_j | j \in \Theta_a\}$. We define the *spatial trust score* of the measurement R_j (or corresponding detrended measurement R'_j) as

$$T_j^s = \frac{|\sum_{i \in \Theta_t} w_i S_i - S_j|}{\epsilon_{\max}}, \tag{14}$$

where $\{w_i\}_{i \in \Theta_t}$ is given in Eq. (13).

Temporal Trust Score: Unlike spatial trust score that considers a measurement's spatial fitness with other trusted measurements, the temporal trust score of a candidate measurement captures the mobile sensor's long-term behavior. As a mobile sensor participates in spectrum sensing in many epochs, its past performance can provide strong indication for the quality of spectrum measurement it submits in the current epoch. Recall that the DBA gradually incorporates candidate spectrum measurements into trusted measurement sets to construct the REM in each epoch. Intuitively, the earlier a measurement is added into the trusted measurement set, the better the measurement fits with existing trusted measurements, the higher quality of the measurement, and vice versa.

Based on the above intuition, the DBA maintains a *temporal trust score* T_j^t for each mobile sensor $j \in \Theta_m$, where $0 \leq T_j^t \leq 1$. When each mobile sensor j first joins the system, the DBA assigns an initial temporal score $T_j^t = \eta$, as the DBA does not know whether or not its first measurement would be added to the trusted measurement set when iterative measurement selection terminates. At the end of each subsequent epoch, the DBA updates T_j^t based on the quality of measurement he submits. Consider epoch l as an example. Assume that measurement R_j from sensor j is the r_jth measurement moved from the candidate measurement set to the trusted measurement set, where we postulate that $r_j = |\Theta_m|$ if measurement R_j is discarded in the end. The DBA updates mobile sensor j's temporal trust score as

$$T_j^t = \alpha T_j^t + (1 - \alpha) \frac{r_j}{|\Theta_m|}, \tag{15}$$

where $\alpha \in [0, 1]$ is a system parameter that controls how fast past performance is forgotten.

Overall Trust Score: The overall trust score of a candidate measurement is a linear combination of the corresponding spatial trust score and temporal trust score. Specifically, we define

the *trust score* T_j of candidate measurement R'_j as

$$T_j = \omega T_j^s + (1-\omega)T_j^t, \tag{16}$$

where $\omega \in [0,1]$ is another system parameter indicating the weight given to the spatial trust score.

4) Final REM Construction: After the above process terminates, the DBA constructs a final REM using the trusted measurements $\{R'_j | j \in \Theta_t\}$. In particular, the DBA refits the empirical semivarogram model using $\{R'_j | j \in \Theta_t\}$ as in the evaluation of spatial trust scores. For every cell center $\mathbf{x}_c, c \in \{1,\ldots,N\}$, the DBA predicts it residue RSS $\hat{S}(\mathbf{x}_c)$ using Eq. (13) and outputs its estimated RSS as

$$\hat{Z}(\mathbf{x}_c) = \hat{S}(\mathbf{x}_c) + P(\mathbf{x}_c), \tag{17}$$

where $P(\mathbf{x}_c)$ is the predicted RSS at location $\mathbf{x}_c$ given in Eq. (3).

D. Discussion

Terminal Condition: As mentioned before, the DBA terminates the process if the ratio between the number of the trusted measurements and the total number of measurements reaches a predetermined threshold η. This terminal condition assumes that the ratio of false measurements is small, and the DBA intends to defend against up to $1-\eta$ ratio of false measurements.

There are another two possible terminal conditions with each corresponding to a different assumption about the attacker. First, the iterative measurement selection process may terminate when the number of trusted measurements reaches a predefined threshold, $i.e. |\Theta_t| \geq \eta_2$, where $\eta_2 \in [|\Theta_a|, |\Theta_a \bigcup \Theta_m|]$ is a system parameter. This terminal condition assumes that there are sufficient good measurements, while the ratio of the number of false measurements over the total number of measurements could be potentially large. Using this terminal condition, the DBA intends to construct an REM with sufficiently high accuracy with just enough trusted measurements even if there are additional good measurements that can be explored. Second, the iterative measurement selection process may terminate when no remaining candidate measurement has a trust score exceeding η_3, where $\eta_3 \in [0,1]$ is a system parameter. This terminal condition assumes that false measurements exhibit high inconsistency in comparison with trusted measurements, i.e., with large T_j. Note that under this terminal condition, the last iteration may add fewer than q candidate sensors to the trust sensor set.

Computation Complexity: We now analyze the computational complexity of the proposed ST-REM. In comparison with constructing an REM using the standard OK, ST-REM involves an additional iterative measurement selection procedure. The computational complexity of each iteration is dominated by computing the estimated RSS at each of the $|\Theta_c|$ candidate measurement locations according to Eq (2). Assuming that the Gauss–Jordan elimination is used for matrix inversion, computing each estimated RSS has a computation complexity of $O(|\Theta_t|^3)$. Since there are at most $|\Theta_c|/q$ iterations with each involving computing $|\Theta_c|$ estimated RSS. Let $\Theta = \Theta_a \bigcup \Theta_m$. Since $|\Theta_t| < |\Theta|$ and $|\Theta_c| < |\Theta|$ for every iteration, the overall computation complexity introduced by ST-REM over the standard OK is upper-bounded by $O(|\Theta|^4/q)$.

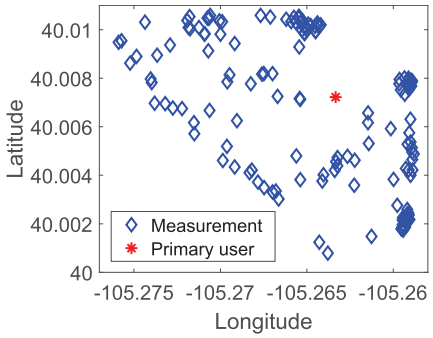


Fig. 2. The locations of measurements and the PU in `cu/wimax` dataset.

V. Performance Evaluation

In this section, we firstly introduce the spectrum measurement dataset used for evaluation and the detrending procedure that we use. We then report our simulation results.

A. Dataset

We use the CRAWDAD `cu/wimax` dataset [51] for the simulation studies, which was also used in [18]. The `cu/wimax` dataset was collected at the University of Colorado Boulder (UC) and contains the Carrier to Interference plus Noise Ratio (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 equalateral triangular lattice and additional measurements taken at random and optimized points. In our simulation studies, we choose 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.

B. Measurement Detrending

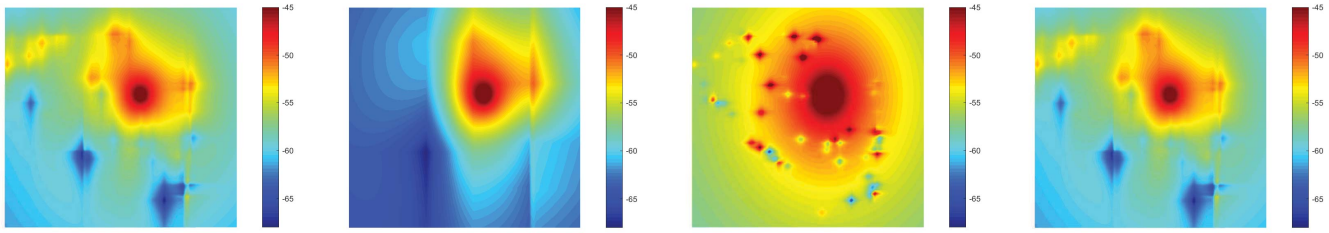
We follow the detrending procedure in [18] to remove the potential source of non-linear trend from the measurements. Specifically, for each CINR measurement $Z_{\text{cinr}}(\mathbf{x})$ at location $\mathbf{x}$, we first convert it into the corresponding path loss value by computing

$$Z_{\text{pl}}(\mathbf{x}) = \mathcal{T} + G_{\text{tx}} - N - Z_{\text{cinr}}(\mathbf{x}), \tag{18}$$

where $\mathcal{T} = 40$ dBm is the PU's transmission power, $G_{\text{tx}} = 10$ dB is the receiver antenna gain, and $N = -95$ dBm is the constant noise floor value. Second, we compute the predicted pass loss using an empirical log-distance path loss model as

$$P(\mathbf{x}) = \alpha 10\log_{10}(d) + 20\log_{10}(f) + 32.45 + \epsilon, \tag{19}$$

where d is the distance between $\mathbf{x}$ and the PU, $f = 2578$ MHz is the PU's transmitting frequency, 32.45 (dB) represents the free-space path loss, $\alpha = 1.22$ and $\epsilon = 28.81$ dB are the path loss exponent and the offset obtained by fitting the



(a) ABFM. (b) TMO. (c) AM. (d) ST–REM.

Fig. 3. Exemplary REMs constructed by TMO, AM, ABFM, and ST–REM with 10 trusted and 20 false measurements.

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
ω	0.5	Weight of spatial trust score
	20	The number of false measurements
T	5 dB	Attack strength
q	10	Step length
η	80	Terminal condition 1
η_1	0.8	Terminal condition 2
η_2	0.8	Terminal condition 3

measurements, respectively. The detrended measurement is then given by

$$S(\mathbf{x}) = Z_{\text{pl}}(\mathbf{x}) - P(\mathbf{x}), \tag{20}$$

where $P(\mathbf{x})$ is given by Eq. (19).

C. Simulation Settings

We divide the 145 measurements into two sets: a testing set $\mathcal{R}_t$ with 100 measurements and a validating set $\mathcal{R}_v$ with 45 measurements as the ground truth. From the 100 testing measurements, we randomly choose 10 measurements as trusted ones and another 20 measurements as the false ones. Moreover, we say a false measurement R_i has an *attack strength* T (dB) if it reports a $Z_i + T$ where Z_i is the true measurement [23]. Table I summarizes our default simulation settings unless mentioned otherwise.

We primarily use Mean Absolute Error (MAE) to evaluate the performance of ST–REM. In particular, for each measurement $R_i \in \mathcal{R}_v$, let Z_i and $\hat{Z}_i$ be the reported RSS and estimated RSS, respectively. The MAE is defined as

$$\text{MAE} = \frac{\sum_{R_i \in \mathcal{R}_v} |Z_i - \hat{Z}_i|}{|\mathcal{R}_v|}. \tag{21}$$

Since ST–REM is the first solution for secure REM construction against false spectrum measurements, we compare its performance with the following three strategies.

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

D. Simulation Results

We now report the simulation results for comparison of TMO, AM, ABFM, and ST–REM.

1) Exemplary REMs Constructed by TMO, AM, ABFM, and ST–REM: Fig. 3 shows four exemplary REMs constructed by ABFM, TMO, AM, and ST–REM, respectively, where attack strength T is 5 dB. For each REM, we first estimate the path loss value at the center of every cell in the region and then convert the predicted path loss value back into RSS by computing

$$\hat{Z}(\mathbf{x}) = \mathcal{T} + G_{\text{tx}} - (\hat{S}(\mathbf{x}) + P(\mathbf{x})).$$

Fig. 3a shows the REM constructed by ABFM using all the good measurements, which can serve as the baseline for the other three mechanisms. Generally speaking, the closer the REM to the one constructed by ABFM, the more resilient the mechanism against false spectrum measurements. Fig. 3b shows the REM constructed by TMO using only the 10 known trusted measurements from anchor sensors, which is very coarse and different from the REM constructed by ABFM. On the other hand, Fig. 3c shows that the REM constructed by AM using all the measurements is highly distorted by the 20 false measurements, which highlights the detrimental impact of even a small number of false measurements. Finally, Fig. 3d shows the REM constructed by ST–REM. As we can see, the REM is very close to the REM constructed by ABFM shown in Fig. 3a, indicating the high resilience of ST–REM to false measurements. These exemplary REMs demonstrate that the significant advantage of ST–REM over TMO and AM.

2) Impact of Attack Strength T: Fig. 4 show the MAEs under ABFM, TMO, AM, and ST–REM with the attack strength T varying from 0 dB to 30 dB. The MAEs under TMO and ABFM are not affected by the change in the attack strength and are plotted for reference only. As we can see, the MAE under ABFM is approximately 2.67 dB, which can

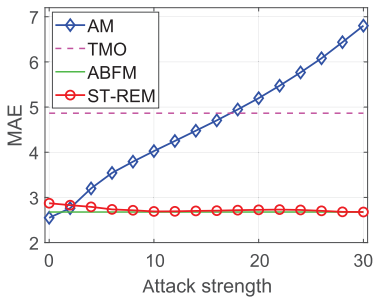


Fig. 4. MAE vs. attack strength.

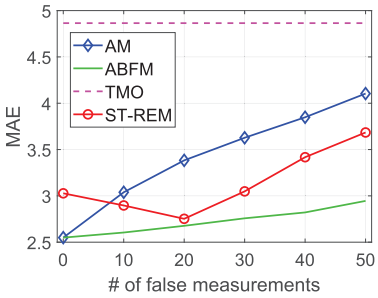


Fig. 5. MAE vs. # of false measurements.

be considered as the lower bound of the MAE of the REM constructed using Ordinary Kriging and coincides with the results obtained in the recent measurement study [17]. In addition, the MAE under TMO is around 4.86 dB, which again shows that the REM constructed from only a small number of trusted measurements is highly inaccurate. Moreover, the MAE under AM increases nearly linearly as the attack strength increases. In contrast, the MAE of ST–REM is very close to that of ABFM, which shows that ST–REM can effectively filter out false measurements and demonstrates its resilience against the change in attack strength.

3) Impact of the Number of False Measurements: Fig. 5 shows the MAEs under ABFM, TMO, AM, and ST–REM with the number of false measurements varying from 0 to 50, where the MAE under TMO stays at 4.86 dB and is plotted for reference only. We can see that the MAE under AM is the same as that under ABFM when there is no false measurement and increases nearly linearly as the number of false measurements increases. This is anticipated, as the adverse impact of false measurements on the MAE grows as the number of false measurements increases. On the other hand, the MAE under ABFM slightly increases as the number of false measurements increases, which is caused by the corresponding decrease in the number of good measurements. In addition, the MAE under ST–REM initially declines as the number of false measurements increases. The reason for the initial decline is that ST–REM may terminate too early when there are only few false measurements, i.e., some good measurements are excluded from being used to improve the accuracy of the REM. As the number of false measurements approaches 20, fewer good measurements are discarded, and the MAE under ST–REM approaches that under ABFM. As the number of false measurements further increases from 20, the MAE under ST–REM deteriorates but is still much lower than that under AM. This is also expected, as ST–REM would include some false measurements in the final REM under such situations.

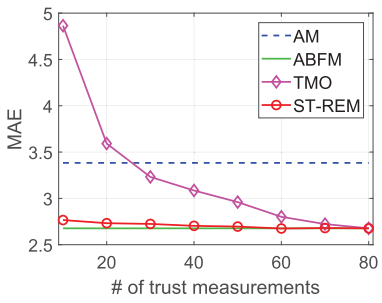


Fig. 6. MAE vs. # of trust measurements.

4) Impact of the Number of Trusted Measurements: Fig. 6 compares the MAEs under ABFM, AM, and ST–REM with the number of trusted measurements, i.e., anchor sensors, varying from 10 to 80, where the MAEs under AM and ABFM are not affected and are plotted for reference only. As we can see, the MAEs under AM and ABFM are 3.38 dB and 2.67 dB, respectively. In addition, the MAE under TMO decreases from 4.86 dB to 2.67 dB as the number of trusted measurements increases from 10 to 80. This is anticipated, as the more good measurements, the higher the accuracy of the resulting REM, and vice versa. Moreover, while we can see that the MAE under ST–REM decreases as the number of trusted measurements increases, the gain resulted from the additional trusted measurements is quite small. For example, the MAE under ST–REM is 2.76 dB with 10 trusted measurements and decreases to 2.73 dB with 10 additional trusted measurements. These results show that ST–REM only requires a small number of trusted measurements to produce an REM with high accuracy.

5) Impact of Step Length q: Fig. 7 shows the MAEs under ST–REM with the step length q varying from 2 to 20, where the MAEs under AM, TMO and ABFM are not affected by the change in the step length and are plotted for reference only. As we can see, the MAE under ST–REM slightly increases as the step length increases. The reason is that the initial REM constructed from the measurements submitted by anchor sensors is quite coarse, and using the initial REM to estimate the trustworthiness of other measurements and add too many other measurements at once may have some false measurement included. This would lead to higher MAE of the final REM. As the step length further increases from 15 to 20, the MAE of the final REM slightly fluctuates. Overall, the change in step length has very limited impact on the accuracy of resulting REMs under the default settings.

6) Impact of Anchor Sensor Placement: We also evaluate the impact of anchor sensors' placement. Specifically, we consider the following four strategies for placing anchor sensors.

- *1/4–Grid–Random*: Divide the whole area into four square grids of equal size and randomly select 2 or 3 measurements in each grid to form the 10 trusted measurements.

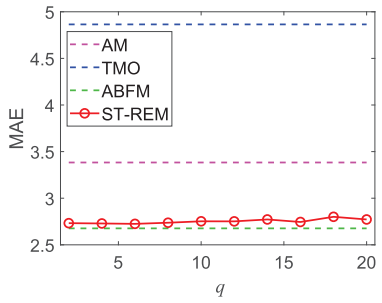


Fig. 7. MAE vs. step length q.

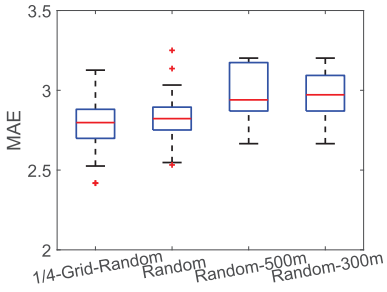


Fig. 8. MAE vs. anchor sensor placement.

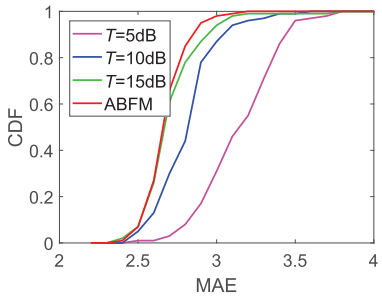


Fig. 9. CDF of MAE under SSO.

- *Random*: Randomly select 10 measurements in the whole area as the trusted measurements.
- *Random-500m*: Randomly select 10 measurements within 500 meters of the PU as the trusted measurements.
- *Random-300m*: Randomly select 10 measurements within 300 meters of the PU as the trusted measurements.

Generally speaking, anchor sensors are distributed most evenly under 1/4-Grid-Random, followed by Random, Random-500m, and Random-300m.

Fig. 8 compares the MAEs under the four anchor sensor placement strategies for ST–REM. The median MAEs under 1/4-Grid-Random, Random, Random-500m, and Random-300m over 100 runs are 2.79 dB, 2.82 dB, 2.94 dB, and 2.97 dB, respectively. Generally speaking, the more unevenly anchor sensors are distributed, the higher the MAE, and vice versa. However, the difference among the four placement strategies are relatively small. Given the limited size of our dataset, we leave further investigation of the optimal anchor sensor placement as our future work.

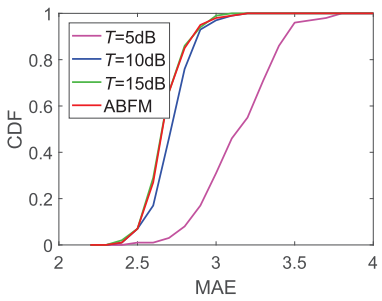


Fig. 10. CDF of MAE under TSO in 5th epoch.

7) Comparison of SSO, TSO, and ST–REM: Since ST–REM relies on both spatial and temporal trust scores to rank and select candidate measurements, we also compare it with the following two variants to better understand their effectiveness.

- *Spatial trust score only (SSO)*: The spatial trust score in ST–REM is given an weight of one, i.e., $\omega = 1$ in Eq. (16).
- *Temporal trust score only (TSO)*: The spatial trust score in ST–REM is given zero weight, i.e., $\omega = 0$ in Eq. (16).

Fig. 9 shows the Cumulative Distribution Functions (CDFs) of the MAEs under SSO under different attack strengths across 100 runs, where the CDF of the MAE under ABFM is plotted for reference. As we can see, the MAE under SSO decreases as the attack strength increases. In particular, when the attack strength is 15 dB, 94% of MAEs are higher than 3 dB. In contrast, when the attack strength is 10 dB and 5 dB, the percentage drops to 87% and 31%, respectively. This is due to the fact that when the attack strength is small, e.g. 5 dB, the differences between false measurements and good measurements are quite small, making it difficult to differentiate them and resulting in a relatively high MAE. It also indicates that SSO is most effective if the attack strength is large.

Fig. 10 shows the CDFs of the MAEs under TSO under different attack strengths, where the CDF under ABFM is plotted for reference only. We can see that when the attack strength keeps 5dB in previous four epochs, the MAE under TSO in the fifth epoch is much higher than that under ABFM. In contrast, when the attack strength is 15dB in previous four epochs, the CDF of the MAEs under TSO matches closely with that of ABFM in the fifth epoch. This is anticipated, because the larger the attack strength, the later a false measurement is added into the trusted measurement set, the higher temporal trust score of the false measurement, and vice versa. It is thus easier for TSO to differentiate false measurements from good ones when the attack strength is high.

8) Impact of Sudden Change in Attack Strength: To evaluate the effectiveness of spatial and temporal trust scores in filtering out false measurements in the presence of sudden change in the attack strength, we further consider the following two exemplary attack strategies.

- *Attack Strategy 1-sudden decrease in the attack strength*: The attacker chooses an attack strength of 15dB in the

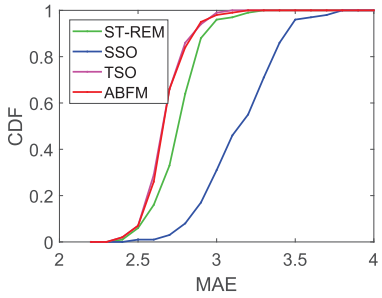


Fig. 11. CDF of MAE under Attack Strategy 1.

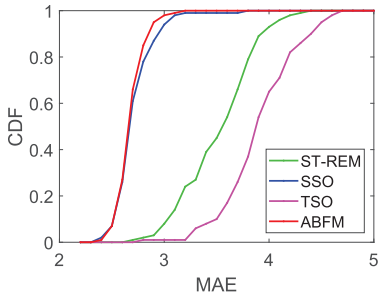


Fig. 12. CDF of MAE under Attack Strategy 2.

first four epochs and changes the attack strength to 5 dB in the fifth epoch.

- *Attack Strategy 2-sudden increase in the attack strength*: The attacker chooses an attack strength of 5dB in the first four epochs and changes the attack strength to 15 dB in the fifth epoch.

Fig. 11 shows the CDFs of MAEs in the fifth epoch under ST-REM, SSO, TSO, and ABFM under Attack Strategy 1, where the CDF of the MAE under ABFM is plotted for reference only. We can see that the MAE under ST-REM is very close to that under TSO and much lower than that under SSO. In particular, the CDF of MAEs under ST-REM and TSO are close to the one under ABFM, while the CDF of the MAEs under of SSO is quite far from that under ABFM. In addition, the CDF of the MAEs under TSO overlaps with the one under ABFM. The reason is that as the attack strength in the previous epoch is relatively high, e.g., 15 dB, false measurements are easier to be filtered out by SSO and ST-REM, which result in lower temporal trust scores for false measurements in the current epoch. In contrast, since the attack strength is relatively small, i.e., 5 dB, in the current epoch, the spatial trust score of false measurements are relatively small, making it difficult to filter out false measurements by SSO, leading to a higher MAE under SSO. Although SSO alone is less effective under Attack Strategy 1, ST-REM is still able to differentiate false measurements from good ones by jointly considering the temporal trust scores of the measurements.

Fig. 12 shows the CDFs of the MAEs under ST-REM, SSO, TSO, and ABFM under Attack Strategy 2, where the CDF of the MAE under ABFM is again plotted for reference. We can see that ST-REM outperforms TSO, but it is less effective than SSO. The reason is that under Attack Strategy 2, the attack strength in each previous epoch is 5dB, which is too small to always assign high temporal trust scores for false measurements. Thus, the CDF of MAEs under TSO is far from the CDF of MAEs under ABFM. In contrast, since the attack strength in current epoch is 15dB, which is large enough to filter out false measurements correctly, the CDF of MAEs under SSO is very close to the ideal case. In this circumstance, although the temporal trust score is not reliable, ST-REM is also powerful to exclude false measurements with the benefit of spatial trust score.

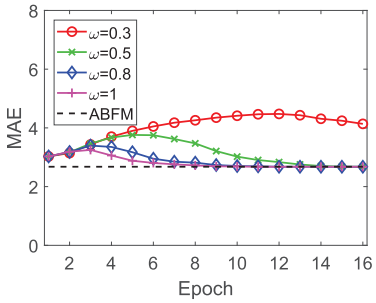


Fig. 13. MAE under gradually ascending attack strength.

These results indicate that SSO is most effective in filtering out false measurements when the attack strength is high in the current epoch, while TSO can differentiate false measurements from good ones as long as the attack strength is high enough in previous epochs. By jointly considering the spatial and temporal trust scores, ST-REM can effectively filter out false measurements as long as the attacker chooses a high attack strength in any epoch.

9) Impact of Dynamic Attack Strength: We also evaluate the impact of dynamic attack strength by considering gradually ascending attack strength, gradually descending attack strength, and static attack strength.

Fig. 13 shows the MAE under ST-TEM with the attack strength gradually increased from 0 by 2 dB in each epoch for 15 epochs and different ωs, where the MAEs under ABFM is plotted for reference. We can see that the MAE under ST-REM initially increases and then gradually decreases until reaching the MAE under ABFM under all weight ωs. In addition, the higher the weight ω, the earlier the MAE under ST-REM starts to decrease and thus the earlier converge to that under ABFM. The reason is that when the attack strength is small, e.g., 2 dB in the second epoch, false measurements are very similar to good ones, and ST-REM is unable to filter out all false measurements. As the attack strength further increases, while false measurements become easier to filter out by ST-REM, some false measurements are still deemed trusted by ST-REM, and their overall impact on the MAE increases due to higher attack strength. As the attack strength keeps increasing, more and more false measurements are detected by ST-REM and excluded from the final REM, resulting in the overall decrease in the MAE under ST-REM. In addition, we can see that the higher the weight ω, the earlier the MAE starts to decrease, and vice versa. This is because spatial trust score is more effective than temporal trust score in filtering out false measurements with increasing attack strength.

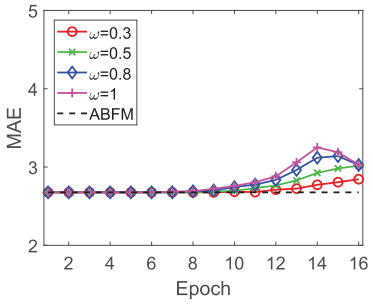


Fig. 14. MAE under gradually descending attack strength.

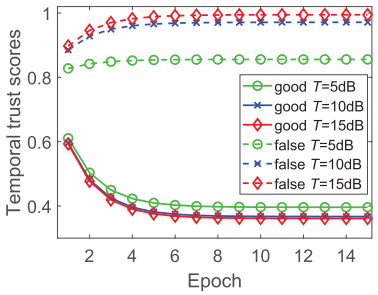


Fig. 15. Temporal trust scores multiple epochs under equal attack strategies.

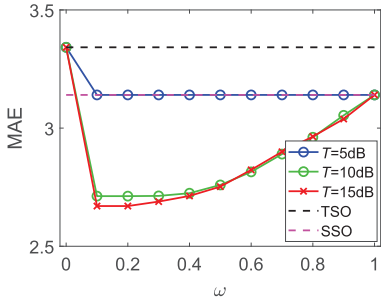


Fig. 16. MAE vs. weight ω.

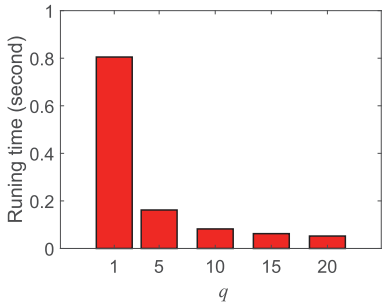


Fig. 17. Running time vs. q.

Fig. 13 shows the MAE under ST-TEM with the attack strength gradually decreased from 30 dB by 2 dB in each epoch for 15 epochs and different ωs, where again the MAEs under ABFM is plotted for reference. We can see that the MAE under ST-REM is the same as that under ABFM for the first eight epochs for all ωs. This is because false measurements with large attack strength, e.g., 16 dB in the eighth epoch, are very different from good ones and can be easily filtered out by ST-REM. As the attack strength further decreases, the MAE under ST-TEM first increases and then decreases under different ωs. The reason is that as the attack strength becomes smaller, some false measurements will be deemed trusted under ST-REM, leading to the increase in the MAE. As the attack strength keeps decreasing, while more false measurements will be added to the trusted measurement set under ST-REM, their accumulative impact on the MAE becomes smaller. Moreover, we can see that the higher the weight ω, the larger the maximum MAE the attacker can achieve over the 16 epochs. This is because the spatial trust score alone is less effective in filtering out false measurements with small attack strengths and the smaller the weight given temporal trust score, the less likely a false measurement can be filtered out by ST-REM.

Fig. 15 shows the average temporal trust score of good and false measurements over 15 epochs, where the attack strength stays at 5 dB, 10 dB, and 15 dB for all epochs. We can see that the average temporal trust score of good measurements decreases rapidly in the first few epochs and then remains stable thereafter. In contrast, the average temporal trust score of false measurements increases in the first few epochs and becomes stable in the following epochs. The reason that the average temporal trust scores of good and false measurements change slower in later epochs is as follows. In the first epoch, all the measurements are assigned the same initial temporal score η, and whether a measurement is added to the trusted measurement set depends solely on its spatial trust score. The order in which the measurements are added to the trusted measurement set results in the update of their temporal trust scores. In each subsequent epoch, false measurements with higher temporal trust scores will have higher overall trust scores and be added to the trusted measurement set even later than in the previous epoch, if ever. This process leads to the continuous decrease in the average temporal trust score of good measurements and the continuous increase in that of false ones. Finally, the larger the attack strength, the larger the gap between the average temporal trust scores of good and false measurements, and vice versa, which is expected.

10) Impact of the Weight ω: Fig. 16 shows the MAE of ST-REM with the weight of spatial score ω varying from 0 to 1, where the MAEs under TSO ($\omega = 0$) and SSO ($\omega = 1$) are plotted for reference. Here we assume that the attack strength in current epoch is 5 dB and that in the previous three epochs is 5 dB, 10 dB and 15 dB, respectively. We can see that as ω increases from 0 to 0.1, the MAE under ST-REM first decreases sharply from 3.34 dB under TSO to 3.14 dB, 2.71 dB and 2.67 dB when attack strength in previous epoch is 5 dB, 10 dB and 15 dB, respectively. As ω further increases from 0.1 to 1, the MAE under ST-RE gradually increases to 3.14 dB achieved by SSO under all three attack strengths in previous epochs. This result shows that there is always an optimal weight ω assignment under which ST-REM outperforms both SSO and TSO.

11) Running Time: Fig. 17 shows the running time of ST-REM with the step length q varying varying from 1 to 20. As we can see, the running time decreases as q increases,

which is anticipated. As discussed in Section IV.D, the computation complexity of the iterative measurement selection is inversely proportional to q. Moreover, the running time is less than 0.2 s when q is above five, which is very practical. In addition, recall from Fig. 7 that the change in step length has limited impact on the accuracy of the final REM, thus a relatively large q can be selected in reality.

VI. Conclusion

In this paper, we have introduced the design and evaluation of ST-REM, a novel spatiotemporal approach for secure crowdsourced REM construction in the presence of false spectrum measurements. Inspired by self-labeled techniques, ST-REM constructs an REM using a small number of trusted measurements and gradually incorporating measurements from mobile sensors that are deemed most trustworthy by jointly considering each measurement's spatial fitness of trusted measurements and the long-term behavior of the mobile sensor. Extensive simulation studies using a real spectrum measurement dataset confirm that ST-REM can produce an REM with sufficient accuracy in the presence of false measurements.

References

[1] Y. Hu and R. Zhang, "Secure crowdsourced radio environment map construction," in *Proc. ICNP*, Oct. 2017, pp. 1–10.

[2] 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 *Proc. 3rd DySPAN*, Oct. 2008, pp. 1–9.

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

[4] Y. Zhao, B. Le, and J. H. Reed, "Network support: The radio environment map," in *Cognitive Radio Technology*, B. A. Fette, Ed. Oxford, U.K.: Newnes, 2006, ch. 11, pp. 337–363. [Online]. Available: https://www.elsevier.com/books/cognitive-radio-technology/fette/978-0-7506-7952-7

[5] 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 *Proc. DySPAN*, Apr. 2007, pp. 115–118.

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

[7] T. Zhang and S. Banerjee, "Inaccurate spectrum databases? Public transit to its rescue!" in *Proc. HotNets*, 2013, pp. 6:1–6:7.

[8] T. Zhang, N. Leng, and S. Banerjee, "A vehicle-based measurement framework for enhancing whitespace spectrum databases," in *Proc. ACM MobiCom*, 2014, pp. 17–28.

[9] O. Fatemieh, R. Chandra, and C. A. Gunter, "Secure collaborative sensing for crowd sourcing spectrum data in white space networks," in *Proc. DySPAN*, Apr. 2010, pp. 1–12.

[10] O. Fatemieh, M. LeMay, and C. A. Gunter, "Reliable telemetry in white spaces using remote attestation," in *Proc. ACSAC*, 2011, pp. 323–332.

[11] O. Fatemieh, A. Farhadi, R. Chandra, and C. A. Gunter, "Using classification to protect the integrity of spectrum measurements in white space networks," in *Proc. NDSS*, 2011. [Online]. Available: https://dblp.org/db/conf/ndss/ndss2012.html

[12] A. W. Min, X. Zhang, and K. G. 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.

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

[14] R. Calvo-Palomino, D. Pfammatter, D. Giustiniano, and V. Lenders, "A low-cost sensor platform for large-scale wideband spectrum monitoring," in *Proc. ACM/IEEE IPSN*, 2015, pp. 396–397.

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

[16] 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 *Proc. PIMRC*, Sep. 2008, pp. 1–5.

[17] 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 *Proc. SECON*, Jun. 2012, pp. 623–631.

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

[19] X. Ying, C. Wook Kim, and S. Roy, "Revisiting TV coverage estimation with measurement-based statistical interpolation," in *Proc. COMSNETS*, Jan. 2015, pp. 1–8.

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

[21] X. Liu, F. Chen, and C.-T. Lu, "Robust prediction and outlier detection for spatial datasets," in *Proc. IEEE ICDM*, Dec. 2012, pp. 469–478.

[22] R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. IEEE INFOCOM*, Apr. 2008, pp. 1876–1884.

[23] A. W. Min, K. G. Shin, and X. Hu, "Attack-tolerant distributed sensing for dynamic spectrum access networks," in *Proc. IEEE ICNP*, Oct. 2009, pp. 294–303.

[24] 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.

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

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

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

[28] I. Triguero, S. García, and F. Herrera, "Self-labeled techniques for semi-supervised learning: Taxonomy, software and empirical study," *Knowl. Inf. Syst.*, vol. 42, no. 2, pp. 245–284, Feb. 2015.

[29] M. Pesko, T. Javornik, A. Košir, M. Štular, and M. Mohorčič, "Radio environment maps: The survey of construction methods," *KSII Trans. Internet Inf. Syst.*, vol. 8, no. 11, pp. 3789–3809, 2014.

[30] A. Achtzehn, J. Riihijarvi, and P. Mahonen, "Improving accuracy for TVWS geolocation databases: Results from measurement-driven estimation approaches," in *Proc. IEEE DySPAN*, Apr. 2014, pp. 392–403.

[31] J. Ojaniemi, J. Kalliovaara, J. Poikonen, and R. Wichman, "A practical method for combining multivariate data in radio environment mapping," in *Proc. IEEE PIMRC*, Sep. 2013, pp. 729–733.

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

[33] W. Wang, H. Li, Y. Sun, and Z. Han, "CatchIt: Detect malicious nodes in collaborative spectrum sensing," in *Proc. IEEE GLOBECOM*, Nov. 2009, pp. 1–6.

[34] W. Wang, L. Chen, K. G. Shin, and L. Duan, "Thwarting intelligent malicious behaviors in cooperative spectrum sensing," *IEEE Trans. Mobile Comput.*, vol. 14, no. 11, pp. 2392–2405, Nov. 2015.

[35] H. Chen, M. Zhou, L. Xie, and J. Li, "Cooperative spectrum sensing with M-Ary quantized data in cognitive radio networks under SSDF attacks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 8, pp. 5244–5257, Aug. 2017.

[36] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *IEEE Trans. Signal Process.*, vol. 59, no. 2, pp. 774–786, Feb. 2011.

[37] H. Chen, M. Zhou, L. Xie, K. Wang, and J. Li, "Joint spectrum sensing and resource allocation scheme in cognitive radio networks with spectrum sensing data falsification attack," *IEEE Trans. Veh. Technol.*, vol. 65, no. 11, pp. 9181–9191, Nov. 2016.

[38] S. Yang, F. Wu, S. Tang, X. Gao, B. Yang, and G. Chen, "On designing data quality-aware truth estimation and surplus sharing method for mobile crowdsensing," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 4, pp. 832–847, Apr. 2017.

[39] J. Hu, H. Lin, X. Guo, and J. Yang, "DTCS: An integrated strategy for enhancing data trustworthiness in mobile crowdsourcing," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4663–4671, Dec. 2018.
[40] C. Miao, Q. Li, H. Xiao, W. Jiang, M. Huai, and L. Su, "Towards data poisoning attacks in crowd sensing systems," in *Proc. ACM MobiHoc*, Jun. 2018, pp. 111–120.
[41] C. Miao, Q. Li, L. Su, M. Huai, W. Jiang, and J. Gao, "Attack under disguise: An intelligent data poisoning attack mechanism in crowdsourcing," in *Proc. WWW*, 2018, pp. 13–22.
[42] K. Xie, X. Li, X. Wang, G. Xie, D. Xie, Z. Li, J. Wen, and Z. Diao, "Quick and accurate false data detection in mobile crowd sensing," in *Proc. IEEE INFOCOM*, Apr./May 2019, pp. 2215–2223.
[43] T. Dierks and E. Rescorla, *The Transport Layer Security (TLS) Protocol*, document RFC 4346, Apr. 2006.
[44] Y. Hu and R. Zhang, "Differentially-private incentive mechanism for crowdsourced radio environment map construction," in *Proc. IEEE INFOCOM*, Apr. 2019, pp. 1594–1602.
[45] D. Hlavacek and J. M. Chang, "A layered approach to cognitive radio network security: A survey," *Comput. Netw.*, vol. 75, pp. 414–436, Dec. 2014.
[46] N. A. Cressie, *Statistics for Spatial Data*, 2nd ed. Hoboken, NJ, USA: Wiley, Jul. 1993.
[47] A. Konak, "A Kriging approach to predicting coverage in wireless networks," *Int. J. Mobile Netw. Design Innov.*, vol. 3, no. 2, p. 65, 2009.
[48] H. Braham, S. B. Jemaa, B. Sayrac, G. Fort, and E. Moulines, "Low complexity spatial interpolation for cellular coverage analysis," in *Proc. WiOpt*, May 2014, pp. 188–195.
[49] R. A. Olea, "A six-step practical approach to semivariogram modeling," *Stochastic Environ. Res. Risk Assessment*, vol. 20, no. 5, pp. 307–318, Jul. 2006.
[50] N. Cressie, "Fitting variogram models by weighted least squares," *J. Int. Assoc. Math. Geol.*, vol. 17, no. 5, pp. 563–586, Jul. 1985.
[51] M. Ton and C. Phillips. (Jun. 2012). *CRAWDAD Dataset cu/wimax (v. 2012-06-01)*. [Online]. Available: http://crawdad.org/cu/wimax/20120601

Yidan Hu (Student Member, IEEE) received the B.E. and M.E. degrees in computer science from Hangzhou Dianzi University in 2013 and 2016, respectively. She is currently pursuing the Ph.D. degree in computer and information science with the University of Delaware. Her primary research interests are security and privacy in networked and distributed systems, wireless networking, and mobile computing.

Rui Zhang (Member, IEEE) received the B.E. degree in communication engineering and the M.E. degree in communication and information system from the Huazhong University of Science and Technology, China, in 2001 and 2005, respectively, and the Ph.D. degree in electrical engineering from Arizona State University, in 2013. He has been an Assistant Professor with the Department of Computer and Information Sciences, University of Delaware, since 2016, and was an Assistant Professor with the Department of Electrical Engineering, University of Hawaii, from 2013 to 2016. His primary research interests are security and privacy issues in wireless networks, mobile crowdsourcing, mobile systems for disabled people, cloud computing, and social networks. He received the U.S. National Science Foundation CAREER Award in 2017.