REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
27-03-2019	Final Report	12-Sep-2012 - 11-Mar-2016

4. TITLE AND SUBTITLE
Final Report: Secure Detection of Mobile Small-Scale Primary Users in Cognitive Radio Networks

5a. CONTRACT NUMBER
W911NF-12-1-0530

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of Michigan - Ann Arbor
3003 South State Street

Ann Arbor, MI 48109 -1274

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
58400-CS.4

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Kang Shin
UU	UU	UU	UU		19b. TELEPHONE NUMBER 734-763-0391

RPPR Final Report
as of 16-Apr-2019

Agency Code:

Proposal Number: 58400CS **Agreement Number: W911NF-12-1-0530**
INVESTIGATOR(S):

Name: Kang Geun Shin kgshin@umi
Email: kgshin@umich.edu
Phone Number: 7347630391
Principal: Y

Organization: **University of Michigan - Ann Arbor**
Address: 3003 South State Street, Ann Arbor, MI 481091274
Country: USA
DUNS Number: 073133571 EIN: 386006309
Report Date: 11-Jun-2016 Date Received: 27-Mar-2019
Final Report for Period Beginning 12-Sep-2012 and Ending 11-Mar-2016
Title: Secure Detection of Mobile Small-Scale Primary Users in Cognitive Radio Networks
Begin Performance Period: 12-Sep-2012 **End Performance Period:** 11-Mar-2016
Report Term: 0-Other
Submitted By: Kang Shin Email: kgshin@umich.edu
Phone: (734) 763-0391
Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees: **STEM Participants:**

Major Goals: • Model, characterize, and analyze attack-tolerant detection and location tracking for real-time monitoring of mobile primary user activities;
• Establish and analyze governing principles for safe coexistence with small-scale primary users by identifying the key security threats;
• Develop innovative techniques that exploit the PHY-layer signal propagation characteristics to maintain high detection accuracy in hostile CRN environments; and
• Implement the developed techniques and evaluate their performance via simulation and experiments on a heterogeneous and SDR-based wireless network testbed.

Accomplishments: We devloped a novel mobile, small-scale primary user (e.g., wireless microphone) tracking framework, called SOLID, that accurately tracks the location of primary user based solely on the PHY-layer signal propagation characteristics (i.e., measured received primary signal strengths (RSSs)) even in the presence of compromised or faulty spectrum sensors. In essence, SOLID augments the conventional Sequential Monte Carlo (SMC)-based target tracking with shadow-fading estimation, which, in turn, improves both localization accuracy and detection of compromised or faulty sensors, by efficiently exploiting the coupling between them. Our extensive simulation-based evaluation shows that SOLID achieves high-level robustness, while reducing the localization error by up to 77% under no attack, and 55% under attacks, compared to the conventional SMC-based tracking.

Training Opportunities: Under this grant support, one student (Alex Min) trained to become an expert in the area of wireless network security, received the PhD degree, and joined Intel Corporation.

RPPR Final Report
as of 16-Apr-2019

Results Dissemination: The research results have been published in premier journals and at conferences.

1. Alex Min and Kang G. Shin,
``Joint optimal sensor selection and scheduling in dynamic spectrum access networks," {\em IEEE Transactions on Mobile Computing},
vol. 12, no. 8, pp. 1532-1545, August 2013.

2. Jaehyuk Choi, Alex Min, and Kang G. Shin,
``On selfish configuration in Wi-Fi tethering,"
IEEE Communications Letters, vol. 17, no. 5, pp. 841--843, May 2013.

3. Alex Min and Kang G. Shin,
``Robust tracking of small-scale mobile primary users in cognitive radio networks,"
IEEE Transactions on Parallel and Distributed Systems}, vol. 24,
no. 4, pp. 778--788, April 2013.

4. Alex Min, Kang G. Shin, and Xin Hu,
``Secure cooperative sensing in IEEE 802.22 WRANs using shadow fading correlation,"
IEEE Transactions on Mobile Computing, vol. 10, no. 10,
pp. 1434-1447, October 2011.
(This paper was selected as the Spotlight Paper for the October 2011 issue of the IEEE Transactions on Mobile Computing).

5. Alex Min, Xinyu Zhang, and Kang G. Shin,
``Detection of small-scale primary users in cognitive radio networks,"
IEEE Journal of Selected Areas of Communications,
vol. 29, no. 2, pp. 349--361, February 2011.

6. Alex Min, Kyu-Han Kim, and Kang G. Shin,
``Robust cooperative sensing via state estimation in cognitive radio networks,"
IEEE DySPAN 2011, May 2011.

Honors and Awards: Nothing to Report

Protocol Activity Status:

Technology Transfer: Nothing to Report

PARTICIPANTS:

Participant Type: PD/PI
Participant: Kang Geun Shin
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: Alexander Min
Person Months Worked: 6.00 **Funding Support:**
Project Contribution:
International Collaboration:

International Travel:
National Academy Member: N
Other Collaborators:

Robust Tracking of Mobile Small-scale Primary Users in Cognitive Radio Networks

Kang G. Shin

Real-Time Computing Laboratory
Department of Electrical Engineering and Computer Science
The University of Michigan, Ann Arbor, MI 48109-2121, USA
kgshin@umich.edu

ABSTRACT

In cognitive radio networks (CRNs), secondary users must be able to identify the location of primary users to efficiently coexist with them in the same geographical area without causing excessive interference to primary communications. Although various sensing schemes have been proposed for the detection of spectrum opportunities in time and frequency domains left unused by large-scale primary users, identifying spectrum opportunities in space domain—by tracking the location of a primary transmitter—has not been studied efficiently before. Although the target tracking problem has studied extensively in the context of wireless sensor networks, it is challenging to secure primary user tracking due to CR-unique features, such as the absence of primary-secondary cooperation and low sensor density. This project devloped a novel mobile, small-scale primary user (e.g., wireless microphone) tracking framework, called `SOLID`, that accurately tracks the location of primary user based solely on the PHY-layer signal propagation characteristics (i.e., measured received primary signal strengths (RSSs)) even in the presence of compromised or faulty spectrum sensors. In essence, `SOLID` augments the conventional Sequential Monte Carlo (SMC)-based target tracking with shadow-fading estimation, which, in turn, improves both localization accuracy and detection of compromised or faulty sensors, by efficiently exploiting the coupling between them. Our extensive simulation-based evaluation shows that `SOLID` achieves high-level robustness, while reducing the localization error by up to 77 % under no attack, and 55 % under attacks, compared to the conventional SMC-based tracking.

1. INTRODUCTION

Cognitive radio (CR) is a key technology to enhance the spectrum efficiency by allowing secondary (unlicensed) users/devices to reuse spectrum opportunities (a.k.a. spectrum white spaces), thus mitigating the spectrum-scarcity problem that we may soon face due to the explosive growth of wireless/mobile users, services and applications. The main goals of CR technology are efficient detection and reuse of spectrum opportunities, which are found to be abundant in the time, frequency, and space domains [5, 27, 31, 41, 43].

While spectrum sensing has been studied extensively [4, 22, 24, 28, 32], most existing sensing schemes target the detection of large-scale primary signals, such as DTV signals in IEEE 802.22. For such large-scale primary signals, detecting/reusing *spatial* spectrum opportunities, i.e., the area where the licensed spectrum bands are temporarily unused by the primary users (PUs), is relatively easy and is less of concern. This is because large-scale PUs are often stationary and their location is known *a priori* to secondary users (SUs). This make the geo-location database a feasible solution for detecting large-scale PUs. Moreover, a large spatial footprint of primary signals requires most, if not all, of the secondary devices on the spectrum band to promptly vacate the band upon return of PUs, in order to avoid interference to the PUs. For example, all the CR devices (called CPEs) in an 802.22 cell must vacate the current operating channel within 2 seconds upon detection of a TV signal, which has a keep-out radius of 150.3 km [12].

Unlike the detection of large-scale primaries, accurately tracking the physical location of a *mobile* small-scale primary transmitter is crucial in achieving main objectives and functionalities of CRNs, such as spatial spectrum reuse [9], interference management [19, 42], routing decisions [11], and fake primary signal detection [7, 25]. For example, knowing the location of the primary transmitter enables SUs to reuse the licensed spectrum more efficiently without causing excessive interference to the primary by admission and transmit-power controls [9, 19, 37, 42]. Recently, we have shown in [30] that performance of cooperative sensing also highly depends on the accuracy of location information, especially in case of detecting a very weak primary signal like a wireless microphone (WM) signal [30]. Recently, Yang *et al.* [44] studied the problem of detecting the boundary of primary signals. However, they only cosider a large-scale stationary primary transmitter and assume a separate sensor network without addressing any security issues.

The small-scale primary tracking is vulnerable to attacks, since its accuracy depends heavily on the integrity of sensor reports, or the sensors' measured received primary signal strengths (RSSs). The measured RSSs at sensors is often the only available information at the BS since is it not feasible to modify primary system for opportunistic spectrum access, as stated by the FCC. As a result, the tracking process can be easily disrupted by malicious or faulty sensors that

report fake or distorted RSSs. However, it is challenging to secure the tracking mechanism because there does not exist any collaboration or communication between secondary and primary devices in CRNs. This is because the FCC specifies that no modification to the primary system for the opportunistic spectrum access by the unlicensed devices [16]. Moreover, low sensor density in CRNs exacerbates the vulnerability against such attacks, e.g., the average sensor density in 802.22 WRANs is only about 1.25/km^2 [33]. Inaccurate location estimation may ultimately cause SUs to generate excessive interference to the primary system, violating the basic premise of CRNs and unmotivating PUs to share their licensed spectrum bands with SUs. Therefore, there is a clear need for efficient and secure tracking of mobile, small-scale PUs.

In this project, we address the problem of reliably tracking mobile, small-scale PUs in CRNs. Specifically, we design a novel RSS-based tracking scheme, called `SOLID`, which jointly estimates the location of a primary and shadow-fading gains in the RSSs. The shadowing estimation in `SOLID` greatly improves the localization performance. In addition, by monitoring temporally-correlated shadow fading, `SOLID` accurately detects manipulated or erroneous sensor reports. The key motivation behind exploiting temporal correlation in attack detection is based on the observation that malicious sensors cannot control the physical-layer signal-propagation characteristics.

1.1 Contributions

This project makes the following main contributions.

- Identification of a new type of attack in CRNs that disrupts the process of tracking a small-scale PU by manipulating the sensing reports. Despite its importance, the problem of designing robust tracking schemes for mobile PUs has not yet been studied effectively. Most previous work builds on an unrealistic assumption that the location information of small-scale primary transmitters is available to the SUs.
- Development of a novel attack-tolerant tracking scheme, called `SOLID`, that jointly estimates the primary's location and shadow-fading gains using an adaptive filter. `SOLID` exploits the temporal correlation in shadow fading to (i) improve the localization accuracy, and (ii) promptly detect abnormal sensor reports. To the best of our knowledge, this is the first attempt that exploits shadow-fading correlation to securely track mobile nodes, such as small-scale primary transmitters.
- In-depth evaluation of `SOLID` in a realistic shadow-fading environment under various attack scenarios. Our simulation results show that, under no attack, `SOLID` lowers the average localization error by up to 77 % compared to the conventional Sequential Monte Carlo (SMC)-based tracking scheme. When attack exits, `SOLID` lowers the average error more than 55 % in various attack scenarios.
- Investigation of an interesting tradeoff in the performance of localization accuracy, i.e., when the BS filters out sensors or sensing reports too aggressively (conservatively), the localization can suffer from lack of samples (existence of manipulated RSS reports). These observations provide practical guidelines in spatial spectrum reuse in the presence of localization error so that the primary receivers can be protected even under various attacks.

Note that our focus is not on a new localization/tracking algorithm, which has been studied extensively [14, 35, 46]. Rather, we focus on adding robustness to the existing localization and tracking algorithms.

1.2 Organization

The remainder of this report is organized as follows. Section 2 describes the network, signal-propagation, PU tracking models, and introduces the attack models. Section 3 presents our proposed approach for attack detection, and the underlying localization protocol. Section 4 details our approach for the generation of shadow fading, the estimation of shadow fading, and the design of attack detector. Section 5 evaluates the performance of `SOLID`. Section 6 reviews the related work on detection of small-scale primaries, and Section 7 concludes the report.

2. SYSTEM AND ATTACK MODELS

In this section, we describe the network, spectrum sensing, and signal-propagation models. We then overview our primary transmitter tracking model and introduce the attack model.

2.1 Network Model

We consider a CRN consisting of primary and secondary users/devices in the same geographical area. The secondary network is infrastructure-based network, such as IEEE 802.22 WRANs, where each cell consists of a base station (BS) and multiple sensors.[1] We assume that sensors are stationary and the BS has the location information of the sensors within its own cell. For example, sensors in 802.22 WRANs, also called *consumer premise equipments* (CPEs), are stationary and the IEEE 802.22 standard draft requires the BS to have their location information. We assume that the sensors have been deployed in an area A, e.g., an IEEE 802.22 WRAN cell, following a point Poisson process with average density ρ, i.e., $n_A \sim Poi(n; \rho|A|)$. Unlike the typical wireless sensor network environment where sensors are densely distributed, we assume a low sensor density ρ as the typical density of CPEs in rural areas is only 1.25/km^2 [40].[2]

There are different types of PUs in TV white space, such as ATV, DTV, and WM, but here we focus on tracking the location of a WM transmitter. WMs emit very weak signals[3], and they are mobile. While we focus on robust tracking of WMs' location in 802.22 WRANs, for the ease of presentation, the techniques we propose here are *generic* and can be used for detecting other types of small-scale primaries or, in a broader context, target tracking in wireless sensor networks.

The BS estimates the location of WM transmitters based on the received signal strengths measured at sensors. We assume that the initial location of WMs is known to the BS via cooperative sensing [30], and we focus on tracking their location using sensor reports. In each sensing period, the BS

[1]We use the terms *secondary user* and *sensor* interchangeably because secondary devices also functions as sensors.
[2]This differs from the conventional wireless sensor networks where sensors are densely deployed in order to detect events of interest.
[3]For example, the equivalent isotropic radiated power (EIRP) of WMs is around or even below 25 mW, with a corresponding transmission range of 150-200 m [34].

directs a set of sensors S_t within its cell to measure the received primary signal strengths using the well-known energy detection technique [38]. At the end of sensing period, the sensors reports their measurement to the BS for estimating the location of the WM transmitter, as well as for detecting the disappearance of WM signals.

2.2 Spectrum Sensing and Signal-Propagation Models

For spectrum sensing, we assume that sensors use energy detection (ED) [38] at the PHY-layer.[4] The test statistics of ED is an estimate of the sum of received primary signal power and noise power. We assume that the BS uses only the sensors located close to the primary transmitter for location tracking. This is a reasonable assumption because the reports from the sensors located far away from the WM transmitter will be close to the noise level, and thus, do not contribute to the improvement of localization accuracy.

Thus, assuming that the noise power is much smaller than the received primary signal strength, the sensor n's measurement in sensing time slot t can be expressed as (in dB) [15]:

$$P_{t,n} = P_o + \alpha 10\log(d_o) - \alpha 10\log(d_{t,n}) + X_{t,n} + Y_{t,n}, \quad (1)$$

where P_o is the signal strength at the primary transmitter, α the path-loss exponent, d_o the reference distance (e.g., 1 m), and $d_{t,n} = \sqrt{(\hat{x}_t - x_n)^2 + (\hat{y}_t - y_n)^2}$, the distance between the primary transmitter and sensor n in time slot t. Log-normal shadow fading is denoted by $X_{t,n}$, which is often characterized by dB-spread, σ_{dB}, where $X_{t,n} \sim \mathcal{N}(0, \sigma_{dB}^2)$.

It is important to note that a large variation of the multi-path fading can hamper the effectiveness of SOLID significantly.[5] To avoid such detrimental effects, we assume that sensors perform sensing for longer than the channel coherent time, thus making the effects of multi-path fading negligible. We assume non-fading components, such as antenna and device losses, are approximated as an i.i.d. Gaussian random variable with zero mean and variance σ_m^2, denoted as $Y_{t,n} \sim \mathcal{N}(0, \sigma_m^2)\ \forall n$.

The received primary signal strength at cooperating sensors in Eq. (1) can be expressed in a vector form as:

$$\mathbf{P_t} = \mathbf{h(d_t)} + \widehat{\mathbf{X}}_\mathbf{t} + \mathbf{Y_t}, \quad (2)$$

where $\mathbf{h(d_t)} = [\, h(d_{t,1}), \ldots, h(d_{t,|S_t|}) \,]^T$ represents the channel gain due to path-loss, where each element is $h(d_{t,n}) = P_o + \alpha 10\log(d_o) - \alpha 10\log(d_{t,n})$. The set of cooperating sensors in time slot t is denoted as S_t. The shadow fading gain and multi-path fading gain vectors are denoted as $\widehat{\mathbf{X}}_\mathbf{t}$ and $\mathbf{Y_t}$, respectively.

A key feature of SOLID is that it estimates the shadow-fading gain $\widehat{\mathbf{X}}_\mathbf{t}$ in each time slot. So, the randomness in received primary signal strengths $\mathbf{P_t}$ mainly comes from the multi-path fading components $\mathbf{Y_t}$. This allows the BS to achieve better localization accuracy, while providing a shadowing profile for attack detection.

2.3 RSS-based Primary User Tracking Model

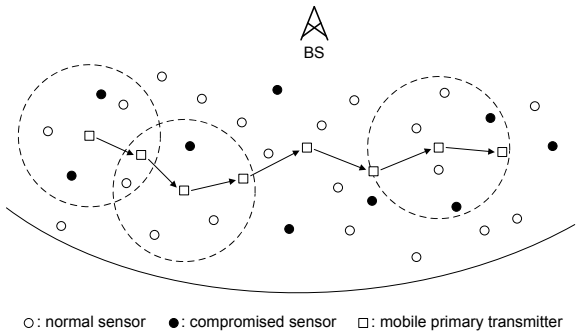


Figure 1: An illustrative example of small-scale primary transmitter (e.g., a WM) tracking via cooperative sensing/localization in a CRN.

Fig. 1 depicts an example scenario of tracking a mobile primary transmitter in a CRN. At each sensing period t, the BS employs a set of sensors S_t located within the sensing range, i.e., a unit disc of radius R_s centered at the estimated location of the primary transmitter for cooperative sensing. Then, the cooperating sensors in the set S_t measure the received signal strength (RSS) on the target channel in a scheduled sensing period using the ED and report them to the BS. Based on the sensors' reports, the BS updates the location estimate of the primary transmitter, followed by an action, e.g., admission or transmit-power control, to protect PUs from the SUs' interference.

Although the problem of mobile PU detection entails various challenging issues at the physical and network layers, we focus on improving the robustness of the PU tracking process by making the best of the information available to the secondary system, i.e., measured RSSs, instead of addressing all of these issues.

2.4 Attack Model

In CRNs, sensors often deployed in unattended and hostile environments, and thus vulnerable to attacks, such as node capture and can thus be easily compromised. Or, sensors can be simply mal-functioning due to hardware/software faults. The main objective of attackers (compromised sensors) is to disrupt the primary transmitter localization/tracking process by manipulating their (RSS) measurement reports to the BS. Specifically, we consider the attack scenario where malicious (or faulty) sensors intentionally (or erroneously) raise or lower the RSSs with a certain probability. As a consequence, the above two cases make the sensing reports to the fusion center (i.e., the BS) inaccurate, degrading the localization/tracking performance. Unfortunately, it is not feasible in CRNs to use secure authentication mechanisms such as cryptography-based authentication since the FCC mandates no modification to the primary (incumbent) system for accommodation of opportunistic spectrum use by secondary devices [16]. As a result, secure mechanisms that require explicit cooperation between the primary and secondary systems are not realizable. Therefore, we opt to design an *attack-tolerant* sensing mechanism that accurately detect such manipulated sensing reports. This allows the BS to discard the sensing reports or exclude the malicious/faulty sensors in cooperative sensing to achieve high localization accuracy.

[4]The energy detector is the most widely-used PHY-layer sensing technique due to its simple design and small sensing overhead.

[5]In practice, the standard deviation of Rayleigh fading, σ_m, can be as large as 5.5 dB, making it difficult to exploit shadow fading correlation.

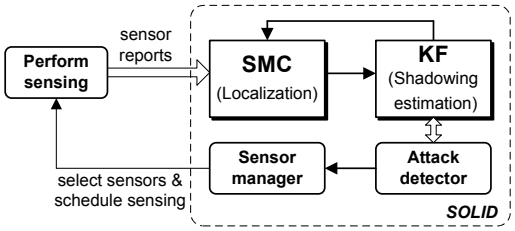


Figure 2: *The SOLID framework*: Malicious/faulty sensors may report falsified measurement data, degrading the accuracy of localization. SOLID estimates/monitors the shadow-fading gains between the primary transmitter and sensors, and detects and filters out abnormal sensor reports based on the shadowing-correlation profile.

3. THE PROPOSED APPROACH

In this section, we first describe the overall architecture of SOLID and present its design rationale. We then introduce the *sequential Monte Carlo* (SMC) localization process that underlies SOLID.

3.1 SOLID Architecture

SOLID consists of the following four building blocks:

- **location estimator** that tracks the location of a mobile, small-scale primary transmitter based on sensor reports,
- **shadowing estimator** that builds and maintains the profile of normal behavior of the shadow-fading correlation,
- **attack detector** that detects and discards abnormal sensor reports, and updates the normal profile, and
- **sensor manager** that selects sensors for cooperative sensing and localization based on the estimated location of the primary transmitter.[6]

The above four components closely interact with each other and constitute an accurate and robust primary user tracking system. In particular, the shadowing estimator introduced in SOLID offers two main benefits: It

- improves the localization accuracy by mitigating the randomness induced by shadow fading in RSSs, and
- enables the attack detector to accurately detect abnormal sensor reports by providing the shadow-fading profile.

SOLID also minimizes communication and processing overhead since it exploits physical-layer signal propagation characteristics, which is readily available from cooperative sensing. The SOLID framework is depicted in Fig. 2.

3.2 Design Rationale for Attack Detection

To maximize attack-tolerance and preserve localization accuracy, SOLID resides at the BS and exploits the *temporal* correlation in shadow fading in received primary signal strengths. The shadow-fading gains between the primary transmitter and sensors are estimated by the Kalman filter (KF), as shown in Fig. 2. The attack detector in SOLID takes an *anomaly-detection* approach to identify and discard abnormal sensor reports in the localization process. The key insight behind SOLID is that, in shadow-fading environments, the sequence of RSSs measured at each sensor is highly likely to be correlated. So, if attackers aggressively raise or lower the RSSs reported to the BS in order to influence the localization outcome, the BS can easily detect them by examining the sensor reports with the predicted value computed based on the history of the sensor reports. Hence, the attacker must lower its attack strength (i.e., deviation) so as not to be detected by the BS.

One important but not so obvious feature of our detection mechanism is that it is *cooperative* even though SOLID independently estimates and monitors the shadowing gains of individual primary transmitter and sensor pairs. This is because the accuracy of shadowing-gain estimation depends heavily on the location estimate, which is updated based on the reports from all the cooperating sensors. In other words, the robustness of attack detection is directly correlated with localization accuracy. Consequently, the BS can improve the attack detection performance by enhancing localization accuracy with a larger number of sensors.

3.3 Tracking a Mobile Primary Transmitter

We now describe the mobile primary transmitter tracking process. Let $\{\boldsymbol{\theta_t} \,|\, \boldsymbol{\theta_t} = (x_t, y_t)\}$ denote the sequence of a mobile primary's locations in two-dimensional coordinate at time slot t. The BS estimates the location of the primary transmitter based on the vector of received primary signal strengths, denoted by $\mathbf{m_t} \triangleq \mathbf{P_t}$ where $\mathbf{P_t}$ is defined in Eq. (2). For mobile, small-scale primary tracking, the BS performs the following two steps based on the sensor reports: *prediction* and *estimation* [21]. At the end of each sensing period t, the BS (i) calculates the conditional density $p(\boldsymbol{\theta_t}|\mathbf{m_{1:t}})$ of the state (primary user location) $\boldsymbol{\theta_t}$ based on the history of measured RSSs at sensors $\mathbf{m_{1:t}} = [\mathbf{m_1}, \ldots, \mathbf{m_t}]^T$, and (ii) estimates the location of primary $\boldsymbol{\theta_t} = (x_t, y_t)$ by taking the expectation $\mathbb{E}[(x_t, y_t) \,|\, \mathbf{m_{1:t}}]$.

The prediction step can be done according to the following Chapman-Kolmogorov equation:

$$p(\boldsymbol{\theta_t}|\mathbf{m_{1:t-1}}) = \int p(\boldsymbol{\theta_t}|\boldsymbol{\theta_{t-1}})\, p(\boldsymbol{\theta_{t-1}}|\mathbf{m_{1:t-1}})\, \mathrm{d}\boldsymbol{\theta_{t-1}}, \quad (3)$$

where the p.d.f. can be computed via Bayes' rule, after the BS collects the measurements $\mathbf{m_t}$ from the sensors:

$$p(\boldsymbol{\theta_t}|\mathbf{m_{1:t}}) = \frac{p(\mathbf{m_t}|\boldsymbol{\theta_t})\, p(\boldsymbol{\theta_t}|\mathbf{m_{1:t-1}})}{\int p(\mathbf{m_t}|\boldsymbol{\theta_t})\, p(\boldsymbol{\theta_t}|\mathbf{m_{1:t-1}})\, \mathrm{d}\boldsymbol{\theta_t}}, \quad (4)$$

where the denominator is the normalization constant.

Unfortunately, however, the analytical solution of Eq. (4) is intractable for our problem. Therefore, as an alternative approach, we use the *Sequential Monte Carlo* (SMC) with shadow-fading estimation as we discuss next.

3.4 Sequential Monte Carlo Combined with Shadow-Fading Estimation

We use *Sequential Monte Carlo* (SMC) [21] for small-scale primary user tracking. The SMC has been widely used as a localization method in mobile wireless systems [2, 35]. The key idea of SMC is to represent the required posterior density function by a set of random samples (or particles) with their associated weights, and then compute the estimated location $\mathbb{E}[(x_t, y_t)|\mathbf{m_{1:t}}]$ by taking their weighted average. The particle set is denoted by the set of tuples $\{(\boldsymbol{\theta_t^{(i)}}, w_t^{(i)})\}_{i=1}^{N_s}$

[6] Although there are many sophisticated sensor-selection methods for target tracking (e.g., [8]), optimal sensor-selection is not our focus.

where each sample $\boldsymbol{\theta_t^{(i)}}$ is associated with its weight $w_t^{(i)}$, where $\sum_{i=1}^{N_s} w_t^{(i)} = 1$.

Specifically, SOLID incorporates shadow-fading estimation into the conventional SMC to achieve high tracking accuracy and robustness against malicious (or faulty) sensors. In SOLID, the entire primary user tracking process consists of the following five steps:

1. Initially, the BS randomly selects N_s sample points $\boldsymbol{\theta_0} = \{\boldsymbol{\theta_0^{(i)}}\}_{i=1}^{N_s}$ in the detection region to represent candidate locations of the mobile primary user.
2. At the end of sensing period t, the BS draws N_s new samples using transition probabilities $p(\boldsymbol{\theta_t^{(i)}}|\boldsymbol{\theta_{t-1}^{(i)}})$, which is determined based on the mobility model.
3. The BS then updates the weights $\{w_t^{(i)}\}_{i=1}^{N_s}$ and computes the expected location of the primary user $\boldsymbol{\theta_t} = (\hat{x}_t, \hat{y}_t)$ by taking the weighted average of the samples.
4. Based on the estimated location, the BS estimates the shadow-fading gains $\widehat{\mathbf{X}}_\mathbf{t} = [\widehat{X}_{t,1}, \ldots, \widehat{X}_{t,|S_t|}]^T$ between the primary user and the cooperating sensors, constituting the main contribution of this paper (see Section 4 for details).
5. The BS terminates the process and waits until the next sensing period if $\widehat{N}_{eff} > N_{thr}$; otherwise, go to Step 2 and repeats the process (re-sampling).

We elaborate the above process as follows. First, the transition probability in Step 2 is given by:

$$p(\boldsymbol{\theta_t^{(i)}}|\boldsymbol{\theta_{t-1}^{(i)}}) = \begin{cases} \frac{1}{\pi(v_{max}+\beta)^2} & \text{if } d(\boldsymbol{\theta_t^{(i)}}, \boldsymbol{\theta_{t-1}^{(i)}}) < v_{max} \\ 0 & \text{otherwise,} \end{cases} \tag{5}$$

where v_{max} is the maximum speed of the mobile primary user, and β is used to generate better samples [35]. We set $\beta = 0.2\, v_{max}$ empirically in our simulations.

After generating N_s new samples using Eq. (5), the BS updates the weights associated with the samples as:

$$w_t^{(i)} = w_{t-1}^{(i)}\, \mathcal{L}(\mathbf{m_t} \,|\, \boldsymbol{\theta_t^{(i)}}), \tag{6}$$

where the likelihood $\mathcal{L}(\mathbf{m_t} \,|\, \boldsymbol{\theta_t^{(i)}})$ can be calculated based on multivariate Gaussian in Eq. (2), i.e., $\mathcal{L}(\mathbf{m_t} \,|\, \boldsymbol{\theta_t^{(i)}}) \sim \mathcal{N}(\mathbf{h(d_t)} + \widehat{\mathbf{X}}_\mathbf{t}, \sigma_m^2\, \mathbf{I})$, where $h(d_{t,n}) = P_o + \alpha 10 \log(d_o) - \alpha 10 \log(d_{t,n})$, and $\mathbf{I}$ is an $N \times N$ identity matrix where $N = |S_t|$ is the number of cooperating sensors in time slot t. Note that here the shadow-fading gains, $\widehat{\mathbf{X}}_\mathbf{t}$, are estimated by the Kalman filter, and hence considered as a constant. The weights are normalized such that $\sum_{i=1}^{N_s} w_t^{(i)} = 1$.

Based on Eqs. (5) and (6), the posterior density $p(\boldsymbol{\theta_t}|\mathbf{m_{1:t}})$ in Eq. (3) can be approximated as:

$$p(\boldsymbol{\theta_t}|\mathbf{m_{1:t}}) \approx \sum_{i=1}^{N_s} w_t^{(i)}\, \delta(\boldsymbol{\theta_t} - \boldsymbol{\theta_t^{(i)}}), \tag{7}$$

where $\delta(\cdot)$ is the *Dirac delta measure*.

Then, the location of the primary user can be estimated by taking the weighted average of the samples:

$$\boldsymbol{\theta_t} \triangleq (\hat{x}_t, \hat{y}_t) = \Big(\sum_{i=1}^{N_s} w_t^{(i)} x_t^{(i)}, \sum_{i=1}^{N_s} w_t^{(i)} y_t^{(i)} \Big). \tag{8}$$

Once the location of the primary user is estimated, the BS estimates the shadow-fading gains $\widehat{\mathbf{X}}_\mathbf{t}$ between the primary user and the sensors using the Kalman filter. We will detail this in Section 4.

Algorithm 1 SMC WITH SHADOW-FADING ESTIMATION

At the end of each sensing round $t \in \mathcal{T}$, the BS does
// Step 1. Localization
Initialization
$\boldsymbol{\theta_0^{(i)}} \sim p(\boldsymbol{\theta_0}), w_0^{(i)} = 1/N_s$ for $i = 1, \ldots, N_s$
$\widehat{N}_{eff} \leftarrow 0$
while $(\widehat{N}_{eff} < N_{thr})$ **do**
  for $i = 1$ to N_s **do**
    Draw $\boldsymbol{\theta_t^{(i)}} \sim p(\boldsymbol{\theta_t} \,|\, \boldsymbol{\theta_{t-1}^{(i)}})$
    Update $w_t^{(i)}$ using Eq. (6) // $w_t^{(i)}$ is un-normalized
    Calculate the total weight $W_t = \sum_{i=1}^{N_s} w_t^{(i)}$
  end for
  for $i = 1$ to N_s **do**
    $w_t^{(i)} = w_t^{(i)} / W_t$ // Normalization
    $(\hat{x}_t, \hat{y}_t) = \big(\sum_{i=1}^{N_s} w_t^{(i)} x_t^{(i)}, \sum_{i=1}^{N_s} w_t^{(i)} y_t^{(i)} \big)$
    $\widehat{N}_{eff} \leftarrow (\sum_{i=1}^{N_s} (w_t^{(i)})^2)^{-1}$
  end for
end while
return $(\hat{x}_t, \hat{y}_t)$
// Step 2. Shadowing Estimation
Estimate the shadowing gains $\widehat{\mathbf{X}}_\mathbf{t}$ using Kalman filter

The above process repeats until the effective number of particles, $\widehat{N}_{eff}$, is equal to or greater than a given threshold N_{thr}. Otherwise, the BS re-samples using the posterior probability in Eq. (7) to replace the current particle set with this new one, and set the weights $w_t^{(i)} = 1/N_s$ for $i = 1, \ldots, N_s$. **Algorithm 1** describes the overall process.

Our simulation results shows that the shadowing estimator in SOLID significantly improves localization accuracy over the conventional SMC. In what follows, we will focus on the use of shadowing estimation to improve attack-tolerance of SOLID.

4. DETECTION OF ABNORMAL SENSOR REPORTS VIA MONITORING SHADOWING CORRELATION

In this section, we describe the generation of temporally-correlated shadow fading and the shadowing-estimation component in SOLID, and discuss the attack-detection algorithm of SOLID.

4.1 Generation of Temporally-Correlated Shadow Fading

As we mentioned, SOLID exploits the shadow-fading correlation to improve both localization and attack-detection accuracy. For the analysis and simulation, we need a method to generate temporally-correlated shadow fading that closely represents the real-world shadowing environments. Gudmundson's empirical shadow fading model [17] has been widely used in accounting for the shadow-fading correlation. So, we use this model to propose a two-step approach for the generation of temporally-correlated shadowing gains between the primary transmitter and sensors.

Let $Z_{t,n} = e^{X_{t,n}}$ denote the shadowing gain in RSSs at sensor $n \in S_t$ where $X_{t,n} \sim \mathcal{N}(0, \sigma_{dB}^2)\ \forall t$. To simplify the notation, we will omit the sensor index n if it does not cre-

ate any confusion. We first derive the conditional p.d.f. of shadowing gain, i.e., Z_{t+1}, at sensor n at time slot $(t+1)$ given the previous measurement Z_t at time slot t as in [29]:

$$f_{Z_{t+1}|Z_t}(z_{t+1}\,|\,z_t) = \frac{1}{z_{t+1}\sigma_{X_{t+1}|X_t}\sqrt{2\pi}} \exp\Big[-\frac{1}{2}\Big(\frac{\ln(z_{t+1})-\mu_{X_{t+1}|X_t}}{\sigma_{X_{t+1}|X_t}}\Big)^{1/2}\Big], \quad (9)$$

where

$$\mu_{X_{t+1}|X_t} = \mu_{X_{t+1}} + \rho\frac{\sigma_{X_{t+1}}}{\sigma_{X_t}}\big[\ln(z_t)-\mu_{X_t}\big], \quad (10)$$

and

$$\sigma_{X_{t+1}|X_t} = \sigma_{X_{t+1}}\sqrt{1-\rho^2(d_{t,t+1})}, \quad (11)$$

where the correlation coefficient $\rho(\Delta d)=e^{\Delta d/d_{corr}}$ exponentially decays as the distance Δd that a primary transmitter traveled between two consecutive sensing events increases [17]. The decorrelation distance for shadowing d_{corr} is assumed to be 150 m in simulation studies [1]. Here $\mu_{X_t}=0\ \forall t$, $\sigma_{X_t}=\sigma_{dB}\ \forall t$. Then, a time sequence of shadow-fading gains can be generated using Eq. (9).

To improve the temporal correlation properties of the thus-generated time sequence, we next apply the *moving average* (MA) filter to the generated sequence of samples. We then correct the sample vales, which are distorted by the filter, to achieve the desired mean (i.e., 0) and standard deviation (i.e., σ_{dB}). A similar method was used in [29], and it was shown to provide a realistic shadow-fading environment. Fig. 3 illustrates such an example of shadowing gain, indicating strong temporal correlations.

4.2 Monitoring Shadow Fading for Attack Detection

We now describe the design of an attack detector in `SOLID` and present an attack-detection criterion.

4.2.1 Construction of Shadowing Profile

In `SOLID`, the BS constructs and maintains a profile of normal shadow-fading behavior for each cooperative sensor n, based on the history of reports from the sensors during the primary transmitter tracking process. We define the shadowing component in the received primary signal strength of sensor n, i.e., $X_{t,n}$, as a basic *profile element* (PE) as:

$$X_n(t) = P_{t,n} - P_o - \alpha 10\log(d_o) + \alpha 10\log(\hat{d}_{t,n}) - Y_n(t), \quad (12)$$

where $P_{t,n}$ is the sensor n's report at sensing period t, P_o the signal power at primary transmitter, $\hat{d}_{t,n}$ the estimated distance between the primary transmitter and sensor n, which is obtained via the SMC, and $Y_n(t)\sim\mathcal{N}(0,\sigma_m^2)$ the noise power.

Recall that the BS monitors shadowing correlation at each cooperating sensor. In the k^{th} sensing period after sensor n is employed by the BS for cooperative sensing, the BS has processed k PEs for sensor n, i.e., $\{X_n(t)\}_{t=1}^{k}$. To exploit the temporal correlation in PEs, we define a profile vector consisting of the entire history of PE records:

$$X_n(k;1) = [X_n(k),\ldots,X_n(1)]^T, \quad 1\le n\le N. \quad (13)$$

Note that PEs exhibit a strong temporal correlation, because the BS keeps track of each sensor's shadowing gain at each sensing period, as we observed in Fig. 3. Thus, by monitoring the estimates of the shadowing gain X_n in reports from each sensor, the BS can construct a compact description of the normal shadowing profile.

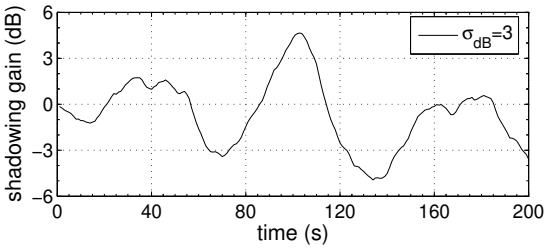


Figure 3: *Temporally-correlated shadow fading*: An example of shadow-fading gain between the primary transmitter moving at speed 10 m/s and a fixed sensor under shadowing dB-spread of $\sigma_{dB}=3$ dB.

4.2.2 Shadowing Estimation using Kalman Filter

In practice, the *observed* shadowing gain in Eq. (12) may not be accurate due to localization error and multi-path fading. This noisy estimates of shadow fading makes it difficult for the BS to capture the temporal correlation in shadow fading, thus degrading `SOLID`'s attack-detection capability as well as localization accuracy.

We describe how `SOLID` accurately estimates the shadowing gain from the observed RSSs, achieving high attack-tolerance. Specifically, the attack-detector in `SOLID` wants to find the shadow-fading estimator that minimizes the *mean squared errors* (MSE):

$$MSE_n(k) = \mathbb{E}\Big\{\sum_{t=1}^{k}\big|X_n(t)-\widehat{X}_n(t)\big|^2\Big\}. \quad (14)$$

`SOLID` employs the Kalman filter (KF) [20], a recursive estimator that produces optimal estimates in the sense of minimizing the mean squared errors (MMSE). First, the system can be modeled as:

$$\mathbf{s}_n(k+1) = \mathbf{\Phi}_n(k)\,\mathbf{s}_n(k) + \mathbf{w}_n(k), \quad (15)$$

where $\mathbf{s}_n(k)$ represents the state (i.e., shadowing gain) of the system, $\mathbf{\Phi}_n(k)$ is the state-transition matrix that relates the state $\mathbf{s}_n(k)$ to the next state $\mathbf{s}_n(k+1)$, $\mathbf{w}_n(k)\sim\mathcal{N}(0,\mathbf{Q})$ is system noise vector where the covariance matrix $\mathbf{Q}$ represents the degree of variability in the state variables.

Second, the measurement of the system is defined as:

$$\mathbf{x}_n(k) = \mathbf{H}_n(k)\,\mathbf{s}_n(k) + \mathbf{v}_n(k), \quad (16)$$

where the matrix $\mathbf{H}_n(k)$ represents an observation model that relates the true state variable $\mathbf{s}(k)$ to the measurements $\mathbf{x}_n(k)$ and $\mathbf{v}\sim\mathcal{N}(0,\mathbf{R})$ is the observation noise where the covariance matrix $\mathbf{R}$ represents the measurement uncertainty. We consider the measurement noise due to noise power (i.e., Y_t in Eq. (1)) by setting $\mathbf{R}=\sigma_m^2$, and set $\mathbf{Q}=0.1^2$ empirically.

Our simulation results show that KF accurately predicts the shadowing gain in the sensor reports by recursively updating the model parameters [20]. See [20] for a detailed description of KF.

4.3 Attack Detection

A compromised or malfunctioning sensor node may report a falsified sensing value to the BS. The manipulated sensor reports may increase the localization error, resulting in either a waste of spectrum opportunities or excessive interference to the primary communication. Therefore, the BS must verify the trustworthiness of the sensor reports and filter out or penalize the bad ones before executing the attack detection and filtering processes.

For this, the BS activates the attack-detection scheme when it employs a sensor for cooperating sensing, and monitors the prediction error $e_n(k)$ in Eq. (17), which quantifies the deviation of sensor n's shadowing gain from the value predicted from its history. The prediction error of KF can be computed as:

$$e_n(k) = \mathbf{x}_n(k) - \mathbf{H}_n(k)\,\widehat{\mathbf{s}}_n(k \,|\, k-1), \tag{17}$$

where $\mathbf{x}_n(k)$ is the observed shadow fading in Eq. (12).

Specifically, we introduce a metric for attack detection, called *prediction error distance* (PED), as the difference in two consecutive prediction errors, which is defined as:

$$PED_n(k) = \big|e_n(k) - e_n(k-1)\big|. \tag{18}$$

This is an efficient metric because the prediction error is also correlated under no attack, and consequently, the difference in two consecutive errors is kept small. We also observed in our simulation study that $PED_n(k)$ is smaller than the prediction error itself.

In particular, the BS raises a flag on sensor n's report as compromised or misbehaving if:

$$PED_n(k) \geq \eta, \tag{19}$$

where $\eta > 0$ is a pre-defined threshold for detecting anomalies. The BS classifies a sensor as malicious and excludes it from the localization process if the cumulative number of flags raised by the BS is greater than N_B.

There is an interesting tradeoff in the design of the detection threshold η and it must be carefully chosen to maximize localization accuracy. If the threshold is too small, the localization performance will suffer from lack of sensing samples due to *over-filtering*. On the other hand, if the threshold is too large, the performance will suffer from manipulated samples due to *under-filtering*. The impact of the detection threshold η on tracking performance will be detailed in Section 5.5. **Algorithm 2** describes the pseudocode of the attack-detection algorithm in `SOLID`.

Algorithm 2 ATTACK-DETECTION ALGORITHM IN `SOLID`

For every newly joint cooperating sensor n, the BS performs

Initialization
$k \leftarrow 0$
blacklist_count$(n) \leftarrow 0$
while $n \in S_k$ **do**
  $k \leftarrow k+1$ // Start the k^{th} iteration
  The BS estimates $X_n(k)$ using Kalman filter
  Compute $PED_n(k)$ using Eq. (18)
  if $PED_n(k) > \eta$ **then**
    if $++$ blacklist_count$(n) \geq N_B$ **then**
      blacklist n
    end if
    if Sensor n is blacklisted **then**
      Exclude sensor n from localization
    end if
  end if
end while

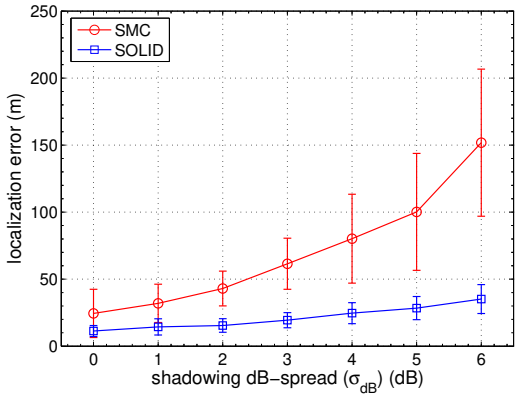


Figure 4: ***Localization performance of*** `SOLID` ***in various fading environments*****:** `SOLID` **lowers the tracking error significantly, whereas the SMC's localization error drastically increases with** σ_{dB}**.**

5. PERFORMANCE EVALUATION

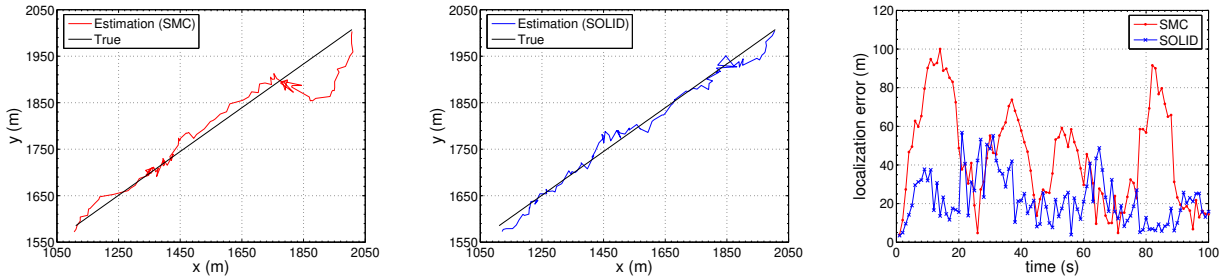
In this section, we evaluate `SOLID` using MATLAB-based simulation. We first describe the simulation setup and then show the efficacy of `SOLID` in accurately tracking a small-scale primary in the absence of attacks. Finally, we demonstrate the attack-detection/tolerance of `SOLID` and the tradeoff in determining the attack-detection threshold.

5.1 The Simulation Setup

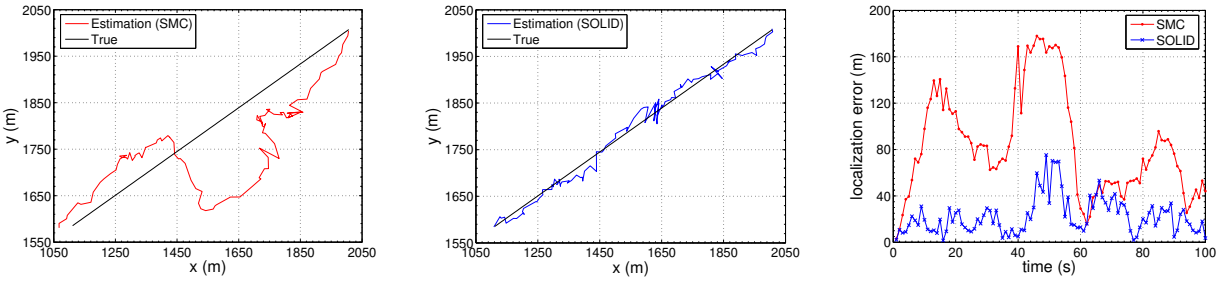
To demonstrate the effectiveness of `SOLID`, we consider a CRN where sensors are randomly distributed according to a point Poisson process with the average sensor density 5 sensors/km^2 in a 6×6 km^2 area. We assume that a WM is randomly located in the area with the transmit-power of 250 mW, which is the WM's maximum transmit-power set by the FCC [10]. We fix the sensing interval to 1 second and the path-loss exponent to $\alpha = 4$. The shadow fading dB-spread is assumed to be in the range $\sigma_{dB} \in [0, 6]$ (dB)[7] and the decorrelation distance for shadow fading is assumed to be $d_{corr} = 150$ m. We assume the standard deviation of noise power is assumed to be $\sigma_m = 0.3$ dB. The radius of cooperative sensing is fixed at $R_s = 1$ km, i.e., the BS employs the sensors located within a unit-disc of radius R_s centered at the estimated location of the mobile primary transmitter. We assume the the sensing interval is 1 second and, during each sensing period, sensors measure the RSS using ED for 1 ms.

For localization, we set the number of samples for SMC to $n_s = 40$ and set the re-sampling thresholds N_{thr} empirically in the range $N_{thr} \in [3, 5]$, depending on the shadow-fading environment. For primary transmitter mobility, we assume the Random Waypoint model without pause time [45]. A mobile primary transmitter moves at a fixed speed of 10 m/s with the moving direction uniformly distributed in $[0, 2\pi]$. The simulation results are generated from 20

[7]While it is typically assumed $\sigma_{dB} = 5.5$ dB for the link between the TV transmitter and CPEs in IEEE 802.22, it can vary with the distance between transmitter and receiver [13].

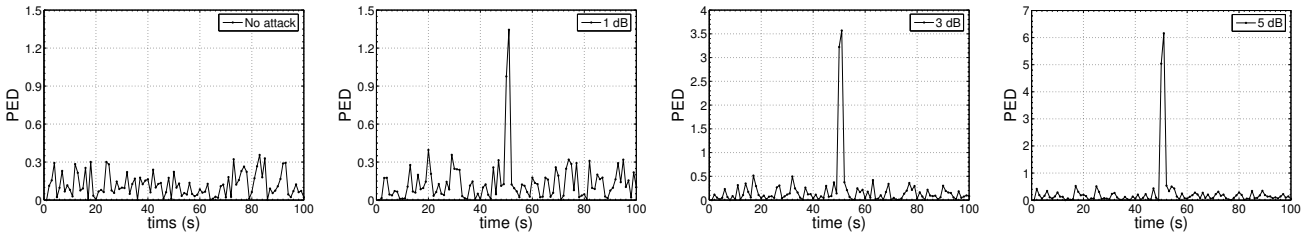


(a) SMC, $\sigma_{dB} = 3\,\text{dB}$ (b) SOLID, $\sigma_{dB} = 3\,\text{dB}$ (c) Localization error, $\sigma_{dB} = 3\,\text{dB}$



(d) SMC, $\sigma_{dB} = 5\,\text{dB}$ (e) SOLID, $\sigma_{dB} = 5\,\text{dB}$ (f) Localization error, $\sigma_{dB} = 5\,\text{dB}$

Figure 5: ***Impact of shadow fading on localization error*****: The figure shows that SOLID reduces the tracking error significantly thanks to its ability to accurately estimate the shadow fading gains.**



(a) No attack (b) 1 dB (c) 3 dB (d) 5 dB

Figure 6: ***The attack-detection capability of*** **SOLID: SOLID can accurately detect even a small deviation in sensor reports (i.e., RSSs) since such a deviation boosts the prediction error distance (PED), which makes it easy for SOLID to detect any abnormal sensor reports.**

randomly-generated topologies.

5.2 Effects of Shadow-Fading Estimation under No Attack

The attack-detection performance of SOLID hinges on accurate location and shadow-fading estimation, which are designed to refine each other throughout the tracking process. We first demonstrate the effectiveness of the shadow-fading estimation introduced in SOLID on localization accuracy in the absence of attacks. Fig. 5 plots examples of tracking a mobile small-scale primary transmitter during a period of 100 s under different shadowing environments, i.e., $\sigma_{dB} = 3, 5\,\text{dB}$. The figure shows that SOLID accurately tracks the location of the mobile primary transmitter, maintaining small localization error for the entire tracking process. On the other hand, in the conventional SMC, the tracking becomes less accurate as the shadow fading becomes severer, i.e., a larger dB-spared, as the shadow fading makes the RSSs more random, which makes the localization difficult.

Fig. 4 plots the average localization error, as well as the interval $(-0.5\,\sigma, +0.5\,\sigma)$, achieved by SMC and SOLID under various shadow fading dB-spreads. The figure clearly shows that the localization accuracy of the conventional SMC suffers from the unpredictability in RSSs due to shadow fading, resulting in a fast increase of error as shadowing dB-spread increases. By contrast, SOLID maintains a small average localization error ($< 35\,\text{m}$) for all simulated scenarios, thanks to its ability to accurately estimate the shadow-fading gains between the mobile primary transmitter and sensors.

The accurate localization provided by SOLID allows the secondary BS to plan/perform efficient admission and transmit-power controls of secondary users/devices, thus greatly improving the spectrum efficiency in the space domain.

5.3 Performance of Attack Detector

To evaluate the attack detector in SOLID, we consider attack scenarios where a malicious sensor injects manipulated sensing reports at time slot 50. A malicious sensor introduces a deviation (or *attack strength*) from its actual measurements (i.e., RSSs) by 1, 3, 5 dB, where the deviation di-

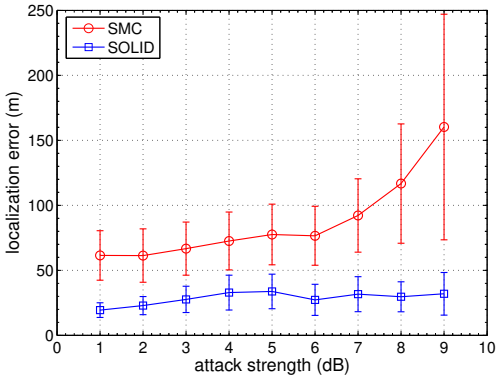


Figure 7: *Attack-tolerance of* SOLID: SOLID successfully tolerates attacks thanks to its ability to exploit temporal shadowing correlation to accurately detect abnormal sensing reports.

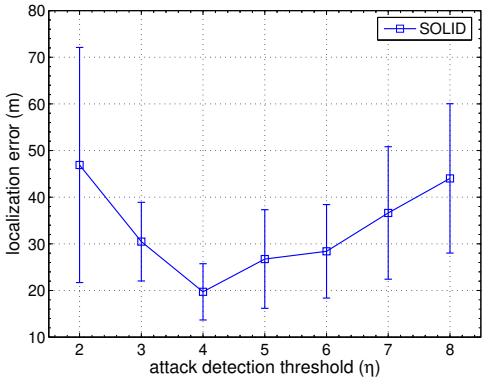


Figure 8: *Impact of detection threshold*: There is a tradeoff in selecting the detection threshold, indicating that the performance of SOLID can be optimized by adjusting the detection threshold.

rection (i.e., $\pm$) is randomly chosen. We use the *prediction error distance* (PED) as the main detection performance metric since it effectively identifies/quantifies the deviation in sensor reports. Fig. 6 clearly shows that the deviation injected by an attacker at the 50-th iteration increases the PED proportionally to the attack strength, yielding high detection accuracy. This high attack-detection accuracy of SOLID can be used in designing the detection (filter) threshold (see Fig. 8). Moreover, even a small deviation (e.g., 1 dB) causes an abrupt increase in PED, and can thus be easily detected by SOLID, thanks to SOLID's ability to closely estimate/track temporally-correlated shadow fading in the measured RSSs.

5.4 Attack-Tolerance

We now demonstrate SOLID's attack-tolerance by comparing its localization accuracy with the conventional SMC-based localization under various attack scenarios. In the simulations in Figs. 7 and 8, we assume that each sensor is malicious with probability 0.3 and the malicious sensors launch attacks independently with probability 0.3 in each time slot. We assume shadowing dB-spread $\sigma_{dB} = 3$ dB and set the detection and blocking thresholds to $\eta = 4$ and $N_B = 1$, respectively. Fig. 7 plots the average as well as $(-0.5\,\sigma, +0.5\,\sigma)$ interval of localization error, under various attack strengths. As expected, the localization error of the SMC increases with increasing attack strength due to the lack of any counteractive mechanism to sensor-report manipulation attacks. To cope with this large error and unpredictability in tracking the primary transmitter, the secondary users/devices must be conservative when they use spatial spectrum opportunities. This can significantly undermine the spectrum efficiency or cause excessive interference to PUs' communications.

By contrast, in SOLID, the localization error remains low (< 35 m) regardless of the attack strength for the following reasons. SOLID successfully withstands weak attacks, e.g., below the detection threshold, because they do not influence the localization outcome even though they are not detected by the attack detector. On the other hand, SOLID can easily detect strong attacks, e.g., above the detection threshold, because the spikes in the prediction error is almost proportional to the attack strength. Although the performance loss due to the reduced number of measurements is inevitable, Figs. 4 and 7 indicate that such loss is not significant even with a very low sensor density of $5/\text{km}^2$.

In summary, the shadow-fading estimator in SOLID allows the localization and attack detection components to refine each other. As a result, SOLID improves localization accuracy when there is no attack, and it successfully tolerates the adverse impact of attacks, if any.

5.5 Tradeoff in Determining the Attack Detection Threshold

Fig. 8 shows the impact of attack-detection threshold η on the primary transmitter tracking performance. The figure indicates that the localization performance of SOLID suffers in case of low detection thresholds for the following two reasons. First, the attack detector is too aggressive in detecting malicious sensors, resulting in *over-filtering*, i.e., some of well-behaving sensors are flagged as malicious and then excluded from cooperative sensing or their reports are discarded. Second, when the attack detector correctly identifies all the attackers, the localization performance may degrade due to lack of RSS samples for localization. On the other hand, too high a detection threshold also degrades the localization performance because of *under-filtering*, where some of the attackers are not detected, adversely influencing the localization process. The figure indicates that SOLID performs best (in terms of average localization error) when the detection threshold is 4 dB, with the average error 19.71 m. This error is only slightly higher than the average value under no attack, i.e., 19.39 m, observed in Fig. 4.

6. RELATED WORK

In this section, we first review the related work on spatial opportunistic spectrum reuse and existing sensing-targeted attacks. We then discuss existing target-tracking schemes in wireless sensor networks.

Spatial Spectrum Reuse in CRNs: While most previous work on spectrum sensing focused on exploiting time and frequency domain spectrum opportunities, efficient reuse of *spatial* spectrum opportunities created by small-scale PUs has received far less attention. Vu *et al.* [42] characterized the statistical behavior of the total interference at the pri-

mary receiver caused by secondary devices in fading environments. Hanif *et al.* [19] addressed the problem of CR deployment under the interference constraints to the primary receiver. The IEEE 802.22 Working Group (WG) proposed a coexistence model with a wireless microphone (WM) to maximize spatial spectrum reuse in 802.22 [9]. While they aim to improve spatial spectrum reuse, they implicitly assume that the location of the primary transmitter is available to secondary devices and did not consider the PUs' mobility. Recently, we proposed a small-scale PU detection/localization scheme, called `DeLOC` [30]. It is designed to accurately detect the existence of a small-scale PU and, if it exists, provides an estimate of its location. The work presented in this paper can be considered as a significant extension of our earlier work.

Secure Spectrum Sensing in CRNs: Security in CRNs has recently started receiving attention from the research community. Among the various potential threats, two types of attack that exploit the vulnerabilities in spectrum sensing have been studied: primary user emulation attack (PUEA) and spectrum sensing data falsification (SSDF) attack. The defense against PUEA has been studied in [26, 36]. Chen *et al.* [6] proposed an RSS-based location verification scheme, called *LocDef*, to detect a fake primary signal. This scheme, however, requires the deployment of a dense sensor network for estimating the location of a signal source, and thus, incurs a high system overhead. Liu *et al.* [26] developed a primary signal verification scheme by jointly exploiting the location-dependent link signature, i.e., multi-path fading profile, and conventional cryptographic authentication method. The proposed scheme does not require any modification to primary system nor training period for link signature. However, their scheme assumes the availability of a *helper node*, which is located closely to each primary transmitter. Moreover, these link signature-based authentication methods may not be feasible for mobile PUs due to its location sensitivity. The problem of ensuring the robustness in distributed sensing has also been studied [23, 29]. Kaligineedi *et al.* [23] presented a pre-filtering scheme based on a simple outlier method that filters out extremely low or high sensor reports. However, their method is unsuitable for a very low SNR environment such as 802.22 WRANs where a final data-fusion decision is very sensitive to small deviations in RSSs. Min and Shin [29] proposed an attack-tolerant secure cooperative sensing scheme that exploits shadow-fading correlation in RSS among close-by sensors.

This paper focuses on a new type of attack, i.e., falsifying sensor reports to disrupt the location tracking of a mobile primary transmitter. To the best of our knowledge, this is the first to study the problem of secure primary tracking in CRNs.

Secure mobile target tracking: The problem of node localization and target tracking has been studied extensively in the area of wireless sensor networks [3, 14, 18, 39, 46]. The primary tracking in CRNs is different from this related work, since it is not desirable to modify the primary system, and thus, there is no additional information (except for RSS) available from the primaries. The solution approach taken by `SOLID` to overcome this problem is unique in that it only relies on the PHY-layer signal propagation characteristics (i.e., temporally-correlated shadow fading) to accurately detect malicious sensors, which has not been considered before.

7. CONCLUSION AND FUTURE WORK

Secure tracking of mobile small-scale primary users is important for efficient spatial reuse of spectrum opportunities, but has not been studied before. To address this problem, we proposed a RSS-based secure tracking scheme, called `SOLID`, tailored to mobile small-scale PUs in CRNs. The key idea behind `SOLID` is that the observed received primary signal strengths at cooperating sensors exhibit temporal correlation due to slowly-varying shadow fading induced by the PU mobility. `SOLID` realizes this idea by jointly performing localization and shadow-fading estimation, thus improving the localization accuracy and achieving high sensitivity in attack detection. Our evaluation results in a realistic shadow-fading environments show that `SOLID` reduces the localization error significantly in the absence of attacks, successfully detects attacks, and maintains small localization error, thus being highly tolerant to attacks.

While `SOLID` achieves high attack-tolerance, our evaluation results indicate that attackers can exploit the inherent tradeoff in the design of the detection threshold to maximize their impact on the PU tracking. Therefore, it would be interesting to study an optimal attack/detection strategy under various attack scenarios.

8. REFERENCES

[1] A. Algans, K. I. Pedersen, and P. E. Mogensen. Experimental Analysis of the Joint Statistical Properties of Azimuth Spread, Delay Spread, and Shadow Fading. *IEEE Journal on Selected Areas in Communications*, 20(3):523–531, April 2002.

[2] A. Baggio and K. Langendoen. Monte-Carlo Localization for Mobile Wireless Sensor Networks. In *Proc. MSN*, Dec 2006.

[3] P. Bahl and V. N. Padmanabhan. RADAR: An In-Building RF-based User Location and Tracking System. In *Proc. IEEE Infocom*, March 2000.

[4] N. B. Chang and M. Liu. Optimal Channel Probing and Transmission Scheduling in a Multichannel System. In *Proc. ACM MobiCom*, Sep 2007.

[5] D. Chen, S. Yin, Q. Zhang, M. Liu, and S. Li. Mining Spectrum Usage Data: a Large-scale Spectrum Measurement Study. In *Proc. ACM MobiCom*, Sep 2009.

[6] H.-S. Chen, W. Gao, and D. G. Daut. Spectrum Sensing for Wireless Microphone Signals. In *Proc. IEEE SECON '08*, June 2008.

[7] R. Chen, J.-M. Park, and J. H. Reed. Defense against Primary User Emulation Attacks in Cognitive Radio Networks. *IEEE Journal on Selected Areas in Communications*, 26(1):25–37, Jan 2008.

[8] W.-P. Chen, J. C. Hou, and L. Sha. Dynamic Clustering for Acoustic Target Tracking in Wireless Sensor Networks. *IEEE Transactions on Mobile Computing*, 3(3):258–271, Jul–Sep 2004.

[9] G. Chouinard. Wireless Microphone Sensing. IEEE 802.22-07/0530r1, Nov 2007.

[10] G. Chouinard. Sensing Performance with the 802.22.1 Wireless Microphone Beacon. IEEE 802.22-09/0068r1, Mar 2009.

[11] K. R. Chowdhury, M. D. Felice, and I. F. Akyildiz. TP-CRAHN: A Transport Protocol for Cognitive

Radio Ad-hoc Networks. In *Proc. IEEE INFOCOM*, April 2009.

[12] C. Cordeiro, K. Challapali, D. Birru, and S. Shankar. IEEE 802.22: An Introduction to the First Wireless Standard based on Cognitive Radio. *Journal of Communications*, 1(1):38–47, April 2006.

[13] Dean Kitchener *et al.* Correlated Lognormal Shadowing Model. IEEE C802.16j-06/059, July 2006.

[14] M. Ding and X. Cheng. Fault Tolerant Target Tracking in Sensor Networks. In *Proc. ACM MobiHoc*, May 2009.

[15] V. Erceg, L. J. Greenstein, S. Y. Tjandra, S. R. Parkoff, A. Gupta, B. Kulic, A. A. Julius, and R. Bianchi. An Empirically Based Path Loss Model for Wireless Channels in Suburban Environments. *IEEE Journal on Selected Areas in Communications*, 17(7):1205–1211, July 1999.

[16] FCC. Facilitating opportunisties for flexible, efficient, and reliable spectrum use employing spectrum agile radio technologies. Rep. ET Docket No. 03-108, Dec 2003.

[17] M. Gudmundson. Correlation Model for Shadow Fading in Mobile Radio Systems. *Electronic Letters*, 27(23):2145–2146, Nov 1991.

[18] C. Gui and P. Mohapatra. Power Conservation and Quality of Surveillance in Target Tracking Sensor Networks. In *Proc. ACM MobiCom*, Sep 2004.

[19] M. F. Hanif, M. Shafi, P. J. Smith, and P. Dmochowski. Interference and Deployment Issues for Cognitive Radio Systems in Shadowing Environments. In *Proc. IEEE ICC*, June 2009.

[20] S. Haykin. *Adaptive Filter Theory.* 2nd ed. Prentice Hall, 1991.

[21] L. Hu and D. Evans. Localization for Mobile Sensor Networks. In *Proc. ACM MobiCom*, Sep 2004.

[22] H. Jiang, L. Lai, R. Fan, and H. V. Poor. Optimal Selection of Channel Sensing Order in Cognitive Radio. *IEEE Transactions on Wireless Communications*, 8(1):297–307, Jan 2009.

[23] P. Kaligineedi, M. Khabbazian, and V. K. Bharava. Secure Cooperative Sensing Techniques for Cognitive Radio Systems. In *Proc. IEEE ICC*, May 2008.

[24] Y.-C. Liang, Y. Zeng, E. C. Y. Peh, and A. T. Hoang. Sensing-Throughput Tradeoff for Cognitive Radio Networks. *IEEE Transactions on Wireless Communications*, 7:1326–1337, April 2008.

[25] S. Liu, Y. Chen, W. Trappe, and L. J. Greenstein. ALDO: An Anomaly Detection Framework for Dynamic Sptectrum Access Networks. In *Proc. IEEE INFOCOM*, April 2009.

[26] Y. Liu, P. Ning, and H. Dai. Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures. In *Proc. IEEE Symposium on Secureity and Privacy*, May 2010.

[27] M. McHenry. NSF Spectrum Occupancy Measurements Project Summary. Shared Spectrum Company Report, Aug 2005.

[28] A. W. Min and K. G. Shin. An Optimal Sensing Framework Based on Spatial RSS-profile in Cognitive Radio Networks. In *Proc. IEEE SECON*, June 2009.

[29] A. W. Min, K. G. Shin, and X. Hu. Attack-Tolerant Distributed Sensing for Dynamic Spectrum Access Networks. In *Proc. IEEE ICNP*, Oct 2009.

[30] A. W. Min, X. Zhang, and K. G. Shin. Spatio-Temporal Fusion for Small-scale Primary Detection in Cognitive Radio Networks. In *Proc. IEEE INFOCOM (mini conference)*, March 2010.

[31] M. Mishra and A. Sahai. How much white space is there? Technical Report, Jan 2009.

[32] S. M. Mishra, A. Sahai, and R. W. Brodersen. Cooperative Sensing among Cognitive Radios. In *Proc. IEEE ICC*, pages 1658–1663, June 2006.

[33] S. M. Mishra, R. Tandra, and A. Sahai. Coexistence with Primary Users of Different Scales. In *Proc. IEEE DySPAN*, April 2007.

[34] E. Reihl. Wireless Microphone Characteristics. IEEE 802.22-06/0070r0, May 2006.

[35] M. Rudafshani and S. Datta. Localization in Wireless Sensor Networks. In *Proc. IEEE IPSN*, April 2007.

[36] S. Anand and Z. Jin and K. P. Subbalakshmi. An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks. In *Proc. IEEE DySpan '08*, Oct 2008.

[37] Senhua Huang and Xin Liu and Zhi Ding. Distributed Power Control for Cognitive User Access based on Primary Link Control Feedback. In *Proc. IEEE INFOCOM*, March 2010.

[38] S. Shellhammer, S. Shankar, R. Tandra, and J. Tomcik. Performance of Power Detector Sensors of DTV Signals in IEEE 802.22 WRANs. In *Proc. ACM TAPAS '06*, Aug 2006.

[39] A. Smith, H. Balakrishnan, M. Goraczko, and N. Priyantha. Tracking Moving Devices with the Cricket Location System. In *Proc. ACM MobiSys*, June 2004.

[40] C. R. Stevenson, C. Cordeiro, E. Sofer, and G. Chouinard. RAN Requirements. IEEE 802.22-05/0007r46, Sep 2005.

[41] R. Tandra, S. M. Mishra, and A. Sahai. What is a spectrum hole and what does it take to recognize one? *Proceedings of the IEEE*, 97(5):824–848, May 2009.

[42] M. Vu, S. S. Ghassemzadeh, and V. Tarokh. Interference in a Cognitive Network with Beacon. In *Proc. IEEE WCNC*, June 2008.

[43] D. Willkomm, A. W. S. Machiraju, and J. Bolot. Approved Primary Users in Cellular Networks: A Large-scale Measurement Study. In *Proc. IEEE DySPAN*, Oct 2008.

[44] Y. Yang, Y. Liu, Q. Zhang, and L. Ni. Cooperative Boundary Detection for Spectrum Sensing Using Dedicated Wireless Sensor Networks. In *Proc. IEEE INFOCOM*, March 2010.

[45] J. Yoon, M. Liu, and B. Noble. Sound Mobility Models. In *Proc. ACM MobiCom*, Sep 2003.

[46] P. Zhang and M. Martonosi. LOCALE: Collaborative Localization Estimation for Sparse Mobile Sensor Networks. In *Proc. ACM IPSN*, April 2008.