Robust Tracking of Small-Scale Mobile Primary User in Cognitive Radio Networks

Alexander W. Min, *Member*, *IEEE*, and Kang G. Shin, *Fellow*, *IEEE*

Abstract—In cognitive radio networks (CRNs), secondary users must be able to accurately and reliably track the location of small-scale mobile primary users/devices (e.g., wireless microphones) in order to efficiently utilize *spatial* spectrum opportunities, while protecting primary communications. However, accurate tracking of the location of mobile primary users is difficult due mainly to the CR-unique constraint, i.e., localization must rely solely on reported sensing results (i.e., measured primary signal strengths), which can easily be compromised by malicious sensors (or attackers). To cope with this challenge, we propose a new framework, called *S*equential m*O*nte car*L*o comb*I*ned with shadow-fa*D*ing estimation (SOLID), for accurate, attack/fault-tolerant tracking of small-scale mobile primary users. The key idea underlying SOLID is to exploit the temporal shadow fading correlation in sensing results induced by the primary user's mobility. Specifically, SOLID augments conventional Sequential Monte Carlo (SMC)-based target tracking with shadow-fading estimation. By examining the shadow-fading gain between the primary transmitter and CRs/sensors, SOLID 1) significantly improves the accuracy of primary tracking regardless of the presence/absence of attack, and 2) successfully masks the abnormal sensing reports due to sensor faults or attacks, preserving localization accuracy and improving spatial spectrum efficiency. Our extensive evaluation in realistic wireless fading environments shows that SOLID lowers localization error by up to 88 percent in the absence of attacks, and 89 percent in the presence of the challenging "slow-poisoning" attack, compared to the conventional SMC-based tracking.

Index Terms—Cognitive radio, mobile primary user, location tracking, security, log-normal shadowing, Kalman filter

1 Introduction

Cognitive radio (CR) has great potential to enhance spectrum efficiency by allowing secondary (unlicensed) users/devices to utilize spectrum opportunities temporarily unused by primary users (PUs). CRs are key components of efficient detection and reuse of spectrum opportunities, thus mitigating the spectrum-scarcity problem that we may soon face due to the explosive growth of wireless/mobile users, services and applications. As a first step toward realizing opportunistic spectrum access, the FCC recently finalized a ruling that permits the operation of unlicensed CR devices in TV white space (TVWS) [1]. This new use of TVWS has generated an interest in and need for developing numerous standards and proposals, such as IEEE 802.22 wireless regional area networks (WRANs) [2], IEEE 802.11af [3], Ecma 392 [4] and White-Fi [5].

Unlike the detection of large-scale primaries, e.g., DTV users, where localization is not the primary concern in opportunistic spectrum reuse, accurately tracking the physical location of small-scale *mobile* primaries, such as wireless microphones (WMs), is crucial in achieving the core objectives and functionalities of CRNs, such as spatial spectrum reuse [6], interference management [7], [8], routing decisions [9], and falsified primary signal detection [10], [11]. For example, knowing the location of the primary transmitter enables secondary users (SUs) to reuse licensed spectrum more efficiently without causing excessive interference to primary communications [6], [7], [8], [12]. In the IEEE 802.22 WRANs, without knowing the location of a WM, all the SUs, also called *consumer premise equipment* (CPE) in an 802.22 cell (of radius up to 100 km), must immediately vacate the current operating channel upon detection of the WM, resulting in significant waste of spatial spectrum opportunities [6]. Furthermore, location information is very useful in cooperative sensing by enabling the secondary base station (BS) (or the fusion center) to select an optimal set of sensors,[1] especially when a very weak primary signal like a WM signal is to be detected [13], [14].

However, CRN faces unique challenges, such as the absence of primary-secondary coordination and low sensor density, that make it difficult to track mobile primaries accurately. According to the FCC, opportunistic spectrum access should require no modification to the primary system [15]. Thus, SUs (sensors) must rely solely on measured received signal strengths (RSSs) (obtained via spectrum sensing) for primary tracking. This makes the primary tracking vulnerable to attacks, since the tracking process can be disrupted by malicious or faulty sensors that report incorrect RSSs. A sensing report falsification attack can easily be launched by attackers due to the open nature of low-layer protocol stacks in software-defined radio (SDR) devices, such as USRP [16] and Sora [17]. Moreover, low sensor density in CRNs hampers the accurate tracking of mobile PUs, e.g., the average sensor density in 802.22 WRANs is only about $1.25/\mathrm{km}^2$ [18]. Inaccurate location estimation may ultimately cause SUs to generate excessive

- *A.W. Min is with the Circuits and Systems Research, Intel Labs, 2111 N.E. 25th Avenue, Hillsboro, OR 97124. E-mail: alexander.w.min@intel.com.*
- *K.G. Shin is with the Real-Time Computing Laboratory (RTCL), Department of Electrical Engineering and Computer Science, The University of Michigan, 2260 Hayward Street, Ann Arbor, MI 48109-2121. E-mail: kgshin@eecs.umich.edu.*

Manuscript received 29 Sept. 2011; revised 19 Jan. 2012; accepted 31 May 2012; published online 22 June 2012.
Recommended for acceptance by X.-Y. Li.
For information on obtaining reprints of this article, please send e-mail to: tpds@computer.org, and reference IEEECS Log Number TPDS-2011-09-0738.
Digital Object Identifier no. 10.1109/TPDS.2012.191.

1. We use the terms *secondary user/device* and *sensor* interchangeably because secondary devices also function as sensors.

interference to the primary system, violating the basic premise of CRNs and discouraging PUs from sharing their licensed spectrum bands with SUs. Therefore, there is a clear need for an efficient and secure tracking scheme for small-scale mobile PUs in CRNs.

In this paper, we address the problem of accurately and reliably tracking small-scale mobile PUs in CRNs. Specifically, we design an RSS-based tracking scheme, called SOLID, that augments the conventional Sequential Monte Carlo (SMC)-based localization with shadow fading estimation. The shadowing estimation in SOLID greatly improves localization performance. Besides, by monitoring temporally-correlated shadow fading, SOLID accurately detects both manipulated and erroneous sensing reports, thus achieving high robustness. The key motivation behind exploiting temporal shadowing correlation in attack detection is that malicious sensors cannot control the physical-layer signal-propagation characteristics. While we focus on the robust tracking of the WMs' locations in 802.22 WRANs, our proposed techniques 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.

1.1 Contributions

This paper makes the following main contributions:

- Development of a new tracking scheme, SOLID, that jointly estimates the mobile PU's location and shadow-fading gains using an adaptive filter. By exploiting the temporal correlation in shadow fading, SOLID
  - improves localization accuracy and
  - accurately identifies abnormal sensing reports.

  To the best of our knowledge, this is the first attempt to incorporate shadow fading into cooperative localization.
- In-depth evaluation of SOLID in a realistic shadow-fading environment under various attack scenarios. Our extensive simulation study shows that in the absence of an attack, SOLID lowers the average localization error by up to 88 percent compared to the conventional Sequential Monte Carlo-based tracking scheme, since the two components of SOLID—SMC-based localization and shadow-fading estimation—refine each other throughout the tracking process.
- High attack and fault-tolerance of SOLID. Our evaluation results show that SOLID can detect compromised sensing reports with high accuracy, e.g., attack false-alarm and misdetection rates below 1 and 7 percent, respectively. It also shows that in a realistic shadowing and multipath environment, SOLID lowers the average error by up to 89 percent, even under "slow-poisoning" attacks.
- Investigation of the tradeoff in the design of the attack detector in SOLID. When the base station filters out sensors or sensing reports too aggressively (or conservatively), the localization can suffer from lack of samples (compromised sensing reports). Via in-depth simulation, we identify the impact of attack detection thresholds, and the results provide practical guidelines for the design of a robust and efficient tracking scheme.

1.2 Organization

The rest of this paper is organized as follows. Section 2 reviews related work, while Section 3 describes the system models and assumptions, and introduces the attack models. Section 4 presents our proposed approach for attack detection, and the underlying localization protocol. Section 5 details our approach to the estimation of shadow fading, and the design of SOLID's attack detector. Section 6 evaluates the performance of SOLID, and Section 7 concludes the paper.

2 Related Work

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

2.1 Secure Spectrum Sensing in CRNs

CRN security has recently become a topic of great interest to the research community. Of the various potential threats, two types of attacks 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 [19], [20]. Chen et al. [10] proposed an RSS-based location verification scheme, called LocDef, to detect fake primary signals. Liu et al. [20] developed a primary signal verification scheme by jointly exploiting the location-dependent link signature, i.e., multipath fading profile, and conventional cryptographic authentication methods. However, their scheme assumes the availability of a *helper node*, located close to each primary transmitter. The problem of ensuring robustness in distributed sensing has also been studied [21], [22], [23]. Kaligineedi et al. [22] presented a prefiltering 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, in which the final data-fusion decision is very sensitive to small deviations in RSSs. Min and Shin [23] proposed an attack-tolerant secure cooperative sensing scheme that exploits shadow-fading correlation in RSS among neighboring sensors. Recently, Duan et al. [24] considered scenarios, in which attackers collaborate to maximize their impact, and proposed mechanisms to discourage and disincentivize the attackers from mounting collaborative attacks. Min et al. [25] developed a collaborative attack-detection framework, called IRIS, that accurately detects the presence of an attack and identifies the attacker by checking for consistency among sensing reports. Unlike these studies, we focus on a new type of attack, i.e., disruption of location tracking of a mobile primary transmitter by falsifying sensor reports.

2.2 Secure Mobile Target Tracking

The problem of node localization and target tracking has been studied extensively in the area of wireless sensor networks [26], [27], [28], [29], [30]. For example, Sheng et al. [31] proposed the use of distributed particle filters to track multiple mobile targets in wireless sensor networks. The primary tracking in CRNs, however, faces unique challenges.

In CRNs, it is not desirable to modify the primary system, and thus, the information on the received primary signal strengths obtained via spectrum sensing is only available to the secondary system. The solution approach taken by SOLID to overcome this challenge differs from others in that it only relies on PHY-layer signal-propagation characteristics (i.e., temporally correlated shadow fading) to accurately detect malicious sensors, which has not been considered before.

3 System and Attack Models

In this section, we describe the network, spectrum sensing, and signal-propagation models that we use throughout the paper. We then present an overview of our model for tracking a small-scale mobile primary transmitter and introduce the attack model.

3.1 CR Network Model and Assumptions

We consider a CRN that consists of primary and secondary users/devices in the same geographical area. The secondary network is an infrastructure-based network, such as an IEEE 802.22 WRAN, in which each cell consists of a BS and multiple sensors, called *customer premise equipments*. The main goal of IEEE 802.22 WRANs is to provide Internet access to rural areas by reusing unused TV spectrum bands, without causing excessive interference to PUs. In an 802.22 WRAN, the BS manages the dynamic spectrum access of the SUs in the network by 1) scheduling sensors to perform spectrum sensing, and 2) performing data fusion and primary location estimation to determine the presence or absence of a primary signal based on the sensing reports. For cooperative spectrum sensing, the BS employs the sensors located within a fusion range centered at the estimated primary location [14].[2] We call such sensors *cooperative sensors*. The BS uses sensing reports to update the estimate of the primary transmitter's location, and estimates shadow-fading gains between the primary transmitter and each cooperative sensor.

Sensors are stationary and the BS has the location information of the sensors within its own cell. For example, the IEEE 802.22 WRAN standard draft requires the BS to know the sensor locations. 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. The Poisson process is widely used to describe sensor distributions in wireless networks. However, the design of SOLID is generic and does not depend on any particular sensor distribution, so it can be applied to CRNs with arbitrary sensor distributions. The Poisson process is a reasonable assumption in the absence of a known distribution that accurately models the sensor (i.e., CPE) distribution in 802.22 WRANs. Unlike in a typical wireless sensor network environment, in which sensors are densely distributed, we assume a low sensor density ρ because the typical density of CPEs in rural areas is only $1.25/\text{km}^2$ [32]. We assume that the BS and sensors communicate sensing information over a common control channel.

2. We focus on the tracking of a mobile PU's location after its detection. The problem of detecting a PU and its location estimate has been addressed in [14].

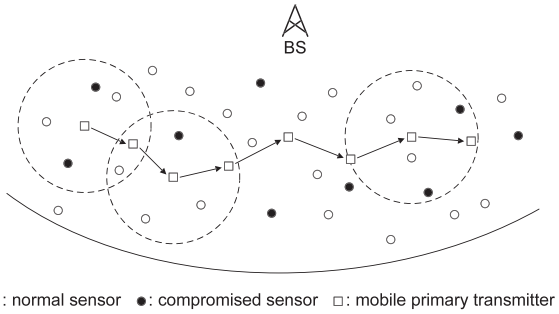


Fig. 1. An illustrative example of small-scale primary tracking. The BS tracks the location of a mobile PU (e.g., a WM) based on sensing reports (i.e., received primary signal strengths) from the sensors located within the fusion range (the dotted circle).

3.2 Spectrum-Sensing and Signal-Propagation Models

Due to the lack of primary-secondary cooperation, primary tracking must be done based only on the received primary signal strengths measured at cooperative sensors.[3] We consider energy detection [33] for spectrum sensing in the PHY-layer. Energy detection is the most widely used PHY-layer sensing technique due to its simple design and low sensing overhead. The test statistics of the energy detector are an estimate of the sum of received primary signal strength and noise power [33]. We assume that the BS employs only the sensors located close to the primary transmitter, i.e., located within the fusion range R_s (e.g., 1 km) from the estimated location of a primary transmitter, for location tracking. This is a reasonable assumption because the reports from 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 [14]. The BS directs the cooperative sensors to perform spectrum sensing at a periodic time interval $t \in \mathcal{T}$, and report their sensing results to the BS for localization. Fig. 1 depicts an example scenario, tracking a mobile primary transmitter in a CRN.

Assuming that the noise power is much smaller than the received primary signal strength, sensor n's measurement in sensing time slot t can be expressed as [34]

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

where α is the path-loss exponent, d_o the reference distance, P_o the received primary signal strength at the reference distance, $d_{t,n}$ the distance between the primary transmitter and sensor n in time slot t. Log-normal shadow fading, denoted by $X_{t,n}$, can be characterized by dB-spread, σ_{dB}, where $X_{t,n} \sim \mathcal{N}(0, \sigma_{dB}^2)$.[4] We assume that nonfading 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 $Y_{t,n} \sim \mathcal{N}(0, \sigma_m^2)\ \forall n$.

Let S_t denote a set of cooperating sensors in time slot t. Then, the received primary signal strength at cooperating sensors in (1) can be expressed in a vector form as

3. Cooperative sensors refer to a set of sensors in a 802.22 WRAN, which are employed by the BS for spectrum sensing.

4. Measurement studies [35] indicate that a typical σ_{dB} values is 4-8 dB depending on geographical environments, e.g., urban or suburban.

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

where $\mathbf{H}(\mathbf{d_t}) = [\, h(d_{t,1}), \ldots, h(d_{t,|S_t|}) \,]^T$ represents the received signal strength due to path-loss, where $h(d_{t,i}) = P_o + \alpha 10 \log(d_o) - \alpha 10 \log(d_{t,i})$. The shadow fading gain and noise vectors are denoted by $\widehat{\mathbf{X}}_\mathbf{t}$ and $\mathbf{Y_t}$, respectively.

Note that while we consider PU tracking in an outdoor environment where large-scale transmitters' signal propagation can be accurately modeled or trained based on terrain profiles, the problem would be more challenging if the signal propagation were more random and unpredictable, e.g., an indoor environment. The extension of SOLID to such a challenging environment will be part of our future inquiry.

3.3 Attack Model

In CRNs, sensors are often deployed in hostile and unattended areas, so they can be captured by attackers. The compromised sensors' reports can then be manipulated to amplify localization error, resulting in either inefficient use of available spectrum (due to conservative spectrum reuse to avoid interference to PUs' communications), or excessive interference to PUs (due to aggressive spectrum reuse based on incorrect PU location estimation). Selfish SUs can manipulate their sensing reports to influence the localization result so that neighboring SUs vacate the channel. As a result, selfish SUs can receive higher bandwidth at the expense of other honest SUs.

The main objective of attackers (compromised or selfish sensors) is to disrupt the primary transmitter localization/tracking process by manipulating sensing reports. Specifically, we consider the following scenarios: a sensor is

- *compromised*, reporting manipulated (i.e., higher or lower than real) RSSs to the BS,
- *malfunctioning or faulty*, generating sensor readings that significantly deviate from the true RSS.

In particular, we introduce the following metrics to describe attack scenarios:

- *attacker population* represents the fraction of attackers among sensors participating in cooperative sensing (i.e., those employed by the BS for sensing),
- *attack strength* represents the deviation in the sensing reports introduced by an attacker.

We assume that attackers are noncooperative and each attacker can thus introduce a different attack strength.

The above attack scenarios render the sensing reports to the fusion center (i.e., the BS) inaccurate, degrading localization/tracking performance. Such large localization error will require SUs to be more conservative in reusing spectrum opportunities, resulting in a waste of *spatial* spectrum opportunities (see Section 6.5). Therefore, we opt to design an *attack- or fault-tolerant* primary tracking mechanism that successfully tolerates such manipulated (or erroneous) sensing reports. The attack detection mechanism in SOLID will allow the BS to detect/discard sensing reports or exclude malicious/faulty sensors in cooperative sensing, thus achieving high localization accuracy.

Although there exist other security threats, such as jamming or denial-of-service attacks, in the primary tracking process, the sensing report manipulation attack that we consider in this paper is more stealthy due to the attacker's ability to control sensing reports in a more fine-grained manner. Thus, we focus on detecting manipulated (or erroneous) sensing reports instead of addressing all the attack scenarios.

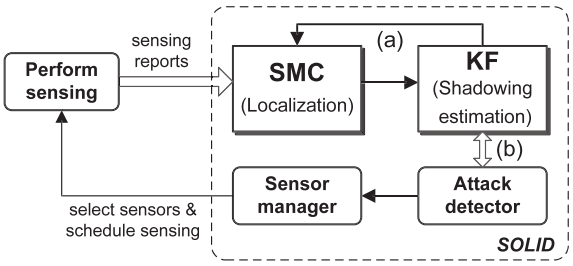


Fig. 2. The SOLID framework. SOLID provides high accuracy and robustness in mobile primary tracking by (a) estimating/monitoring the shadow-fading gains between the primary transmitter and sensors using the Kalman filter, and (b) detecting and filtering out abnormal sensing reports based on the shadowing-correlation profile.

4 The Proposed Approach

We first describe the overall architecture of SOLID and present its design rationale. We then introduce the *sequential Monte Carlo* localization process that underlies SOLID.

4.1 SOLID Architecture

SOLID (Fig. 2) resides at the BS and consists of the following three building blocks:

- **Location estimator** that tracks the location of a small-scale mobile primary transmitter based on sensing reports,
- **Shadowing estimator** that tracks the shadowing gain at cooperative sensors using the Kalman filter (KF), and
- **Attack detector** that detects and discards abnormal sensing reports, and updates the normal profile.

These three components interact with each other synergistically and collectively enable accurate and robust primary tracking. Based on the estimated primary location, the sensor manager selects sensors to cooperate with each other based on their (ab)normality and proximity to the primary transmitter.[5]

In particular, the shadowing estimator introduced in SOLID offers two main benefits:

- Improved localization accuracy by mitigating the effect of shadow fading in RSSs (in Fig. 2a), and
- Accurate detection of abnormal sensing reports (in Fig. 2b).

SOLID also minimizes communication and processing overhead since it exploits physical-layer signal-propagation characteristics, extracted from the cooperative sensing results.

4.2 Design Rationale for Attack Detection

To maximize attack tolerance and preserve localization accuracy, SOLID exploits the *temporal* correlation in shadow

5. Although there are many sophisticated sensor-selection methods for target tracking (e.g., [36]), optimal sensor-selection is not our focus.

fading in received primary signal strengths. The key insight behind the attack detector is that, in shadow-fading environments, the sequence of RSSs measured at each sensor is highly likely to be correlated as indicated in measurement studies (e.g., [35], [37], [38]). Thus, the attack detector takes an *anomaly-detection* approach to identifying and discarding abnormal sensing reports in the localization process. So, if attackers raise or lower the sensing results (i.e., RSSs) reported to the BS in order to influence the localization result, SOLID can easily detect them by examining the consistency of the sensing reports. Hence, the attacker must lower its attack strength to evade detection by SOLID, exerting only a negligible impact on localization.

One important, but not so obvious feature of the attack detector in SOLID is that it is *cooperative* in the sense that the accuracy of shadowing-gain estimation depends heavily on the location estimate, which is updated based on reports from all the cooperating sensors. In other words, the robustness of attack detection is directly correlated with localization accuracy.

4.3 SOLID: Sequential Monte Carlo Combined with Shadow-Fading Estimation

SOLID employs *sequential Monte Carlo* [39] as the baseline scheme for tracking small-scale mobile PUs. SMC has been widely used as a localization method in mobile wireless systems [40], [41]. The key idea of SMC is to represent the required posterior density function as a set of random samples (or particles) with their associated weights, and then compute the estimated location by taking their weighted average. SOLID augments the conventional SMC with shadow-fading estimation to further improve the tracking accuracy and achieve robustness against malicious/faulty sensors.

Let $\{\phi \mid \phi_t = (x_t, y_t)\ t \in \mathbb{N}\}$ denote the sequence of a mobile primary's locations in 2D coordinates where t is the index for (sensing) time slots. The BS estimates the primary transmitter's location based on the vector of received primary signal strengths, denoted by $\mathbf{P_t}$ in (2).

Let the particle set denote the set of tuples $\{(\boldsymbol{\theta}_t^{(i)}, w_t^{(i)})\}_{i=1}^{N_s}$ where each sample $\boldsymbol{\theta}_t^{(i)}$ represents potential PU location and each sample is associated with its weight $w_t^{(i)}$, where $\sum_{i=1}^{N_s} w_t^{(i)} = 1$, and N_s is the number of particle samples. Then, the primary tracking process in SOLID consists of the following seven steps.

Step 1. At the end of sensing period t, SOLID draws N_s new samples[6] using transition probabilities $p(\boldsymbol{\theta}_t^{(i)}|\boldsymbol{\theta}_{t-1}^{(i)})$, given by

$$p\big(\boldsymbol{\theta}_t^{(i)}|\boldsymbol{\theta}_{t-1}^{(i)}\big) = \begin{cases} \min\left[\frac{1}{\pi(v_{max}+\beta)^2}, 1\right] & \text{if } d\big(\boldsymbol{\theta}_t^{(i)}, \boldsymbol{\theta}_{t-1}^{(i)}\big) < v_{max} \\ 0 & \text{otherwise,} \end{cases} \quad (3)$$

where v_{max} (m/s) is the maximum speed of the mobile primary transmitter, and β is used to generate better samples [41]. We set $\beta = 0.2\ v_{max}$ empirically in our simulations.

Step 2. After generating N_s new samples using (3), SOLID updates the weights associated with the samples as

$$w_t^{(i)} = w_{t-1}^{(i)}\ \mathcal{L}(\mathbf{P_t} \mid \boldsymbol{\theta}_t^{(i)}), \quad (4)$$

where the likelihood $\mathcal{L}(\mathbf{P_t} \mid \boldsymbol{\theta}_t^{(i)})$ can be calculated based on multivariate Gaussian in (2), i.e., $\mathcal{L}(\mathbf{P_t} \mid \boldsymbol{\theta}_t^{(i)}) \sim \mathcal{N}(\mathbf{H(d_t)} + \widehat{\mathbf{X}}_{\mathbf{t-1}}, \sigma_m^2\ \mathbf{I}_{N\times N})$ where

$$h(d_{t,n}) = P_o + \alpha 10\log(d_o) - \alpha 10\log(d_{t,n}), \widehat{X}_{t-1}$$

is the shadow-fading gain matrix estimated in the previous time slot. When $t = 1$, $\widehat{X}_1$ is initialized to a zero vector. $\mathbf{I}_{N\times N}$ is an identity matrix where $N = |S_t|$ is the number of cooperating sensors in time slot t. The weights are normalized such that $\sum_{i=1}^{N_s} w_t^{(i)} = 1$.

Step 3. Based on (3) and (4), SOLID approximates the posterior density $p(\boldsymbol{\phi}_t|\mathbf{P_{1:t}})$ as

$$p(\boldsymbol{\phi}_t|\mathbf{P_{1:t}}) \approx \sum_{i=1}^{N_s} w_t^{(i)}\ \delta(\boldsymbol{\phi}_t - \boldsymbol{\theta}_t^{(i)}), \quad (5)$$

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

Step 4. Then, SOLID estimates the location of the primary transmitter by taking the weighted average of the samples

$$\widehat{\boldsymbol{\phi}}_t \triangleq (\hat{x}_t, \hat{y}_t) = \left(\sum_{i=1}^{N_s} w_t^{(i)} x_t^{(i)}, \sum_{i=1}^{N_s} w_t^{(i)} y_t^{(i)}\right). \quad (6)$$

Step 5. SOLID then calculates the effective number of particles, i.e., $\widehat{N}_{eff} = (\sum_{i=1}^{N_s}(w_t^{(i)})^2)^{-1}$, and compares it against the given threshold N_{thr}. If $\widehat{N}_{eff} < N_{thr}$, SOLID resamples the particles using the posterior probability in (5) to replace the current particle set with this new one, and sets the weights $w_t^{(i)} = 1/N_s$ for $i \in \mathcal{S}_t$. Steps 1-4 repeat themselves until the effective number of particles, $\widehat{N}_{eff}$, is equal to, or greater than a given threshold N_{thr}.

Step 6. Given the estimated primary transmitter location in (6) and shadowing gains in the previous time slot, SOLID estimates the shadow-fading gains between the primary transmitter and the sensors, $\widehat{\mathbf{X}}_\mathbf{t}$, using the Kalman filter. The presence of temporal correlation in shadow fading allows the Kalman filter to track shadowing gains. It is important to note that the estimated shadowing gains improve localization accuracy by mitigating the uncertainty caused by shadow fading, i.e., $X_{t,n}$ in (1), in sensing results (i.e., measured primary RSS). Likewise, the improved localization enables more accurate shadow fading estimation, and thus, the two methods help each other to improve. As a result, the incorporation of shadow fading estimation in SMC-based localization improves the localization accuracy significantly. This will be detailed in Section 5.2.

Step 7. Based on the estimated shadow-fading gains $\widehat{\mathbf{X}}_\mathbf{t}$ in Step 6, the attack detector in SOLID filters out abnormal sensors from the tracking process. Joint localization and shadowing estimation enables SOLID to accurately predict the correlated shadow fading. Therefore, even a small disturbance in manipulated sensing reports will make the shadow fading estimation deviate from its prediction, allowing the attack detector to easily identify the compromised ones. We will elaborate on attack-detection design and filtering algorithms in Section 5.3.

Algorithm 1 describes the primary tracking process of SOLID.

6. Initially, SOLID 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 PU.

Algorithm 1. SMC WITH SHADOW-FADING ESTIMATION
At the end of each sensing round $t \in \mathcal{T}$, SOLID does
//1. Localization
1: **Initialization**
2: $\boldsymbol{\theta}_0^{(i)} \sim p(\boldsymbol{\theta}_0), w_0^{(i)} = 1/N_s$ for $i = 1, \ldots, N_s$
3: $\widehat{N}_{eff} \leftarrow 0$ //Effective number of particles
4: **while** $(\widehat{N}_{eff} < N_{thr})$ **do**
5: **for** $i = 1$ to N_s **do**
6: Draw $\boldsymbol{\theta}_t^{(i)} \sim p(\phi_t \mid \boldsymbol{\theta}_{t-1}^{(i)})$ using (3)
7: Update $w_t^{(i)}$ using (4)
8: **end for**
9: Calculate the total weight $W_t = \sum_{i=1}^{N_s} w_t^{(i)}$
10: **for** $i = 1$ to N_s **do**
11: $w_t^{(i)} \leftarrow w_t^{(i)}/W_t$ //Normalization
12: $(\hat{x}_t, \hat{y}_t) \leftarrow (\sum_{i=1}^{N_s} w_t^{(i)} x_t^{(i)}, \sum_{i=1}^{N_s} w_t^{(i)} y_t^{(i)})$
13: $\widehat{N}_{eff} \leftarrow (\sum_{i=1}^{N_s} (w_t^{(i)})^2)^{-1}$
14: **end for**
15: **end while**
16: **return** $(\hat{x}_t, \hat{y}_t)$
// 2. Shadowing Estimation
17: Estimate the shadowing gains $\widehat{\mathbf{X}}_\mathbf{t}$ using Kalman filter
// 3. Attack Detection and Filtering
18: Monitor the shadowing estimation error to detect and filter out abnormal sensing reports

5 Detection of Abnormal Sensing Reports via Monitoring Shadowing Correlation

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

5.1 Construction of Shadowing Profile

SOLID constructs and maintains the *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 basic *profile element* (PE) of sensor n as the shadowing component in the received primary signal strengths in (1), i.e.,

$$X_{t,n} = P_{t,n} - P_o - \alpha 10 \log(d_o) + \alpha 10 \log(\widehat{d}_{t,n}) - Y_{t,n}, \quad (7)$$

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

Suppose that, at time t, SOLID has processed $k(\geq 1)$ PEs for sensor n. Note that k may vary among sensors based on the time they joined the cooperative sensor set. This sequence of PEs exhibits a strong temporal correlation, because SOLID keeps track of each sensor's shadowing gain at each sensing period (e.g., once every 2 seconds). To exploit the temporal correlation in PEs, we define a profile vector consisting of the entire history of PE records:

$$\mathbf{X}_{t,n}(k;1) = [X_{t,n}, \ldots, X_{t-k+1,n}]^T, \quad 1 \leq n \leq N. \quad (8)$$

Thus, the estimates of the shadowing gain $X_{t,n}$ provide a compact description of the normal shadowing profile. We henceforth omit the subscript t for brevity.

5.2 Shadowing Estimation Using Kalman Filter

We now describe how SOLID accurately estimates the PE (i.e., shadowing gain) from the observed primary signal strengths. Specifically, the attack detector in SOLID seeks the shadow-fading estimator that minimizes the mean squared errors (MSE):

$$MSE_n(k;1) = \mathbb{E}\left\{ \sum_{\tau=t-k+1}^{t} \left| \mathbf{X}_n(\tau) - \widehat{\mathbf{X}}_n(\tau) \right|^2 \right\}, \quad (9)$$

where k is the index of the sensing stage since sensor n joined the set of cooperative sensors. We thus need an efficient estimator that minimizes the MSE in (9).

To meet this requirement, SOLID employs the Kalman filter [42], a recursive estimator that produces optimal estimates by minimizing the MSE in (9). Note that other adaptive filters, such as the recursive least squares (RLS) filter, can also be used to track the log-normal shadowing gain at the expense of additional computational complexity. In the KF, the system can be modeled as

$$\mathbf{S}_n(k+1) = \mathbf{\Phi}_n(k)\, \mathbf{S}_n(k) + \mathbf{W}_n(k), \quad (10)$$

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 the system noise vector where the covariance matrix $\mathbf{Q}$ represents the degree of variability in the state variables.

The measurement of the system is defined as

$$\mathbf{X}_n(k) = \mathbf{H}_n(k)\, \mathbf{S}_n(k) + \mathbf{V}_n(k), \quad (11)$$

where the matrix $\mathbf{H}_n(k)$ represents an observation model that relates the true state variable $\mathbf{S}_n(k)$ to the measurements $\mathbf{X}_n(k)$. The initial value of $\mathbf{X}_n(k)$ is set to 0. The measurement noise is denoted as $\mathbf{V}_n \sim \mathcal{N}(0, \mathbf{R})$, where the covariance matrix $\mathbf{R}$ represents measurement uncertainty. We consider the measurement noise in spectrum sensing due to noise power (i.e., $Y_{t,n}$ in (1)) by setting $\mathbf{R} = \sigma_m^2$, and setting $\mathbf{Q} = \sigma^2 = 0.1^2$ empirically.

The Kalman-filter-based shadow fading estimation in SOLID for sensor n is described as follows:

$$\widehat{\mathbf{S}}_n(k \mid k-1) = a\, \widehat{\mathbf{S}}_n(k-1 \mid k-1),$$
$$M_n(k \mid k-1) = a^2\, M_n(k-1 \mid k-1) + \sigma^2,$$
$$\mathcal{K}_n(k) = \frac{M_n(k \mid k-1)}{M_n(k \mid k-1) + \sigma_m^2},$$
$$\widehat{\mathbf{S}}_n(k \mid k) = \widehat{\mathbf{S}}_n(k \mid k-1) + \mathcal{K}_n(k)(\mathbf{X}_n(k) - \widehat{\mathbf{S}}_n(k \mid k-1)),$$
$$M_n(k \mid k) = (1 - \mathcal{K}_n(k))\, M_n(k \mid k-1),$$

where $M_n(k \mid k-1)$ is the one-step minimum prediction MSE, $M_n(k \mid k)$ is the MMSE, and $\mathcal{K}_n(k)$ is the Kalman gain at stage k. $\widehat{\mathbf{S}}_n(k \mid k-1)$ is the shadow fading prediction based on the observations $\{\mathbf{X}_n(i)\}_{i=0}^{k-1}$. The coefficient a is set to 1.

5.3 Attack Detection and Filtering

A compromised or malfunctioning sensor node may report a falsified sensing value to the BS. Such manipulated sensing reports may render the localization less reliable, hampering efficient reuse of spectrum opportunities in the spatial domain. To mitigate this problem, SOLID verifies the trustworthiness of sensing reports and filters out or penalizes the bad ones before performing the localization.

SOLID activates an instance of attack-detection scheme whenever the BS employs a sensor for cooperative sensing. The attack detector in SOLID quantifies the deviation of a sensor's shadowing gain from the value predicted from its history by monitoring the prediction error (or measurement residual), which can be computed as

$$e_n(k) = \mathbf{X}_n(k) - \mathbf{H}_n(k)\,\widehat{\mathbf{S}}_n(k \mid k-1), \tag{12}$$

where $\mathbf{X}_n(k)$ is the observed shadow fading in (7).

We introduce a metric for attack detection called *prediction error distance* (PED) that indicates the euclidean distance in two consecutive prediction errors, i.e.,

$$PED_n(k) = \Big|\, e_n(k) - e_n(k-1) \,\Big|. \tag{13}$$

This is a very useful, yet simple, metric because the prediction error is correlated in the absence of an attack, and consequently, the difference in two consecutive errors is kept small. We also observed from our simulation results that $PED_n(k)$ is smaller than the prediction error itself.

The attack detector in SOLID raises a flag to indicate that sensor n's report is compromised (or abnormal) if

$$PED_n(k) \geq \eta, \tag{14}$$

where $\eta \in \mathbb{R}$ is a predefined threshold for detecting anomalies. SOLID classifies a sensor as malicious and excludes it from the localization process if the cumulative number of flags raised is greater than N_B, which is a design parameter. **Algorithm 2** describes the pseudocode of the attack-detection algorithm in SOLID.

Algorithm 2. ATTACK-DETECTION ALGORITHM IN SOLID
For every newly employed cooperating sensor n, the BS performs

Initialization
$k \leftarrow 0$
$\text{blacklist\_count}(n) \leftarrow 0$
while $n \in S_t$ **do**
  $k \leftarrow k+1$ //Start the k^{th} iteration
  The BS estimates $X_n(k)$ using Kalman filter
  Compute $PED_n(k)$ using (13)
  if $PED_n(k) > \eta$ **then**
    if $++\,\text{blacklist\_count}(n) \geq N_B$ **then**
      blacklist n
    end if
    if Sensor n is blacklisted **then**
      Exclude sensor n from localization
    end if
  end if
end while

Note that the attack-detection threshold η is carefully designed and securely maintained by the attack detector at the BS, and hence, it may be very difficult, if not impossible, for an attacker to manipulate its attack strength based on the threshold value.

6 Performance Evaluation

SOLID is evaluated using Matlab-based simulation. We first describe the simulation setup and show the efficacy of shadow-fading estimation in SOLID in the absence of attacks. We then demonstrate SOLID's robustness against various attack scenarios including *slow-poisoning* attacks, and show the tradeoff in determining the attack-detection threshold. Finally, we show SOLID's efficacy in spatial spectrum reuse.

6.1 Simulation Setup

We consider a CRN in which sensors are randomly distributed according to a point Poisson process (as discussed in Section 3.1) in a $6\,\text{km} \times 6\,\text{km}$ area with an average sensor density of $3/\text{km}^2$, unless otherwise specified. We assume a WM with a transmit-power of 250 mW, which is the maximum transmit-power allowed by the FCC in the UHF band [43]. For WM's mobility, we assume a Random Waypoint model without pause time [44], which is frequently used in simulations for wireless networks. We assume that the WM moves at a fixed speed of 5 m/s with a destination randomly selected in the simulated network area. For each testing scenario, we ran simulations over at least 60 randomly generated secondary network topologies to study average behavior.

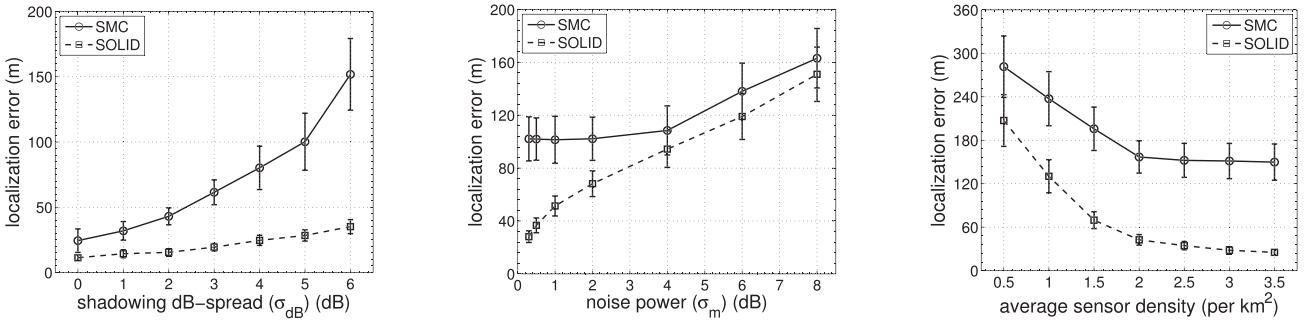
For WM sensing, we fix the sensing interval at 2 seconds [45], and during each sensing period, sensors measure the RSS using the energy detector for 1 ms, as is typically assumed in 802.22 WRANs [46]. The radius of the fusion range for cooperative sensing is fixed at $R_s = 1$ km, which is shown to be near optimal for WM sensing in an 802.22 WRAN [14]. The shadow fading dB-spread σ_{dB} is assumed to be 5 dB, as it is typically assumed in IEEE 802.22 WRANs. The shadowing-decorrelation distance is set to 150 m,[7] and the path-loss exponent α is 4. We assume these parameters are estimated at the time of system deployment, and thus known a priori to the secondary system.

For WM tracking, we set the number of samples for SMC to $n_s = 40$ and set the resampling threshold N_{thr} empirically in the range $N_{thr} \in [3, 5]$, depending on the network environment. In what follows, the figures of localization error plot the average as well as $\pm\, 0.25\,\sigma$ interval.

6.1.1 Effects of Shadow Fading

Fig. 3a shows that SMC-based tracking suffers from the unpredictability in RSSs due to shadow fading, resulting in a rapid increase in error as σ_{dB} increases. By contrast, SOLID maintains a small average localization error (<35 m) for all simulated scenarios thanks to its estimation of the primary location and shadow-fading gains, which refine each other throughout the tracking process.

7. A previous measurement study [35] indicates that a typical decorrelation distance is in the range of 120-150 m in suburban areas.



(a) Effects of shadow fading (σ_{dB}) (b) Effects of noise power (σ_m) (c) Effects of sensor density (ρ)

Fig. 3. Tracking performance under no attack. SOLID (a) successfully withstands shadow fading-induced unpredictability, (b) achieves high performance gain when the measurement noise (σ_m) is small, and (c) outperforms SMC-based tracking for various sensor densities.

6.1.2 Effects of Noise Power

The measurement noise (including the effects of multipath fading) in RSSs can adversely affect the accuracy of shadow-fading estimation. Fig. 3b shows that the average localization error increases with noise power (σ_m) since a large σ_m makes the shadow-fading estimation less accurate. Therefore, it is crucial to combat or reduce the effect of noise power σ_m at each cooperative sensor in order to fully benefit from shadow-fading estimation in SOLID.

Although the standard deviation of Rayleigh fading, σ_m, can be as large as 5.5 dB in practice, many techniques can be used to significantly reduce the effect of multipath fading, e.g., exploiting antenna diversity [47]. For sensors with a single transceiver, this can be accomplished by extending the sensing time (longer than the channel coherence time) [48] at the expense of increased sensing overhead (e.g., time and energy). In what follows, we assume the standard deviation of the noise power is fixed at $\sigma_m = 0.3$ dB.

6.1.3 Effects of Sensor Density

Fig. 3c plots the localization error for various average sensor densities. The figure shows that the average localization error decreases as the sensor density increases for both schemes. However, the error drops faster with SOLID, significantly outperforming the SMC-based tracking scheme thanks to its ability to accurately track the shadow fading gains. When the average sensor density is $\rho = 3.5/\text{km}^2$, SOLID reduces the error by up to 88 percent compared to SMC-based tracking.

6.2 Attack-Tolerance of SOLID

We now demonstrate SOLID's attack-tolerance while varying two key attack parameters; *attack strength* and *attack population*. We fix the attack frequency at 0.3, i.e., compromised sensors launch attacks independently with probability 0.3 in each sensing stage. We set the detection and blocking thresholds to $\eta = 5$ dB and $N_B = 2$, respectively.

To demonstrate the efficacy of SOLID, we compare the following three testing schemes: 1) *SMC-based tracking*, 2) SOLID *without attack detector*, and 3) SOLID *with attack detector*.

6.2.1 Impact of Attack Strength

Here, we show the impact of attack strength on the localization accuracy, while varying the attack strengths in the range between 0 and 10 dB. We assume that the attack population is 30 percent, i.e., each sensor is compromised with probability 0.3.

Fig. 4 shows that the localization performance of SMC-based tracking suffers from large attack strengths due to its lack of ability to detect and filter out manipulated sensing reports. For a similar reason, the localization error of SOLID *without attack detector* also increases with increasing attack strengths. However, this scheme significantly lowers the average error compared to the SMC-based tracking, because of its ability to accurately track the shadowing gains.

In contrast, SOLID *with attack detector* maintains a low localization error even in the case of large attack strengths. This performance superiority can be explained as follows. On one hand, the attack detector in SOLID successfully withstands weak attacks, i.e., $<\eta = 5$ dB, because such attacks do not influence the localization outcome much even though they can evade the attack detector. On the other hand, the attack detector can easily detect strong attacks, i.e., $>\eta = 5$ dB, thanks to its ability to detect large deviations in shadowing estimation caused by manipulated sensing reports.

However, Fig. 4 shows that the localization error of SOLID *with attack detector* still increases slowly with increasing attack strength for the following two reasons. First, the detection delay (i.e., N_B) allows an attacker to influence the localization outcome. Second, the localization error induced by the attackers increases the attack false-alarm rate, i.e., misclassifying legitimate sensors as

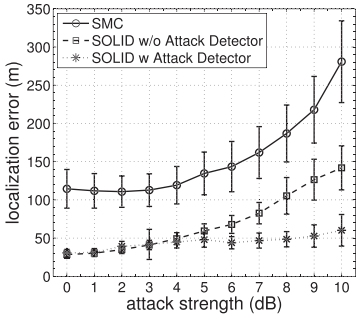


Fig. 4. Attack-tolerance of SOLID. SOLID successfully tolerates attacks thanks to its ability to exploit temporal shadowing correlation to accurately detect abnormal sensing reports.

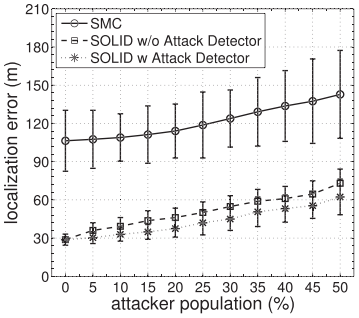


Fig. 5. Impact of attacker population. The localization accuracy of SOLID depends on the design of attack detection threshold η, making a tradeoff between under-/overfiltering.

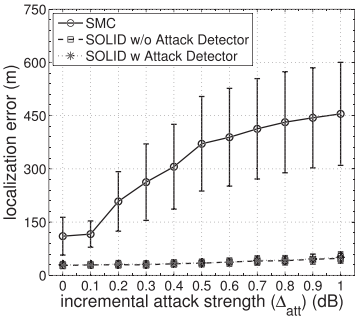


Fig. 6. Attack-tolerance of SOLID against slow-poisoning attack. SOLID successfully tolerates slow-poisoning attacks, safeguarding the tracking process.

malicious/faulty, thus increasing the fraction of attackers in the set of cooperative sensors.

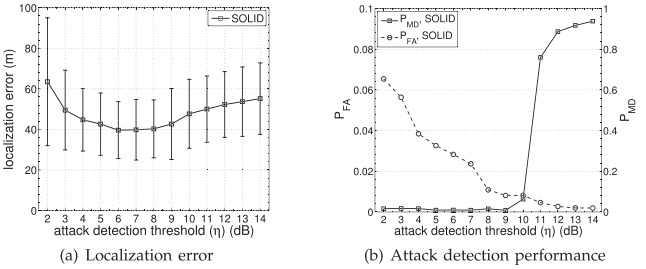
6.2.2 Impact of Attacker Population

Next, we examine the impact of the attacker population by varying the fraction of compromised sensors from 0 to 50 percent. We fix the attack strength at 5 dB. As expected, Fig. 5 shows that a larger attacker population degrades localization performance because it is harder to identify compromised sensors. Moreover, a large fraction of compromised sensors will remove a large number of sensors from the cooperating group, which, in turn, negatively affects localization performance. Nevertheless, localization error is significantly reduced by SOLID *with attack detector* compared to the conventional SMC-based tracking scheme even with a large fraction of compromised sensors, demonstrating its robustness against attacks.

6.3 Tolerance against "Slow-Poisoning" Attack

To further demonstrate SOLID's high attack-tolerance, we evaluate SOLID's tracking performance under a challenging, *slow-poisoning* attack, such that malicious sensors incrementally raise the attack strength by Δ_{att} (dB) in order to evade detection, while disrupting the localization process. Specifically, we assume that a malicious sensor reports the falsified value $P^a_{t,n}(k)$ in the kth sensing stage after joining the set of cooperative sensors, i.e., $P^a_{t,n}(k) = P_{t,n} + k \cdot \Delta_{att}$.

Fig. 6 shows that SOLID performs well under a slow-poisoning attack, even without the attack detector, while the performance of the SMC-based tracking suffers greatly from the attack. Thus, the figure demonstrates that SOLID efficiently mitigates the effects of a slow-poisoning attack.



(a) Localization error (b) Attack detection performance

Fig. 7. Impact of attack detection threshold. The attack detection threshold η affects (a) localization accuracy, as well as (b) false-alarm and misdetection probabilities. In simulations, the attack strength is fixed at 5 dB.

6.4 Tradeoff in Determining the Attack Detection Threshold

We now study the impact of detection threshold η. In our simulation, we fixed the attack strength at 5 dB, and measured localization accuracy and attack detection performance (in terms of false-alarm and misdetection probabilities), while varying the detection threshold in the range $\eta \in [2, 14]$ dB.

Fig. 7a indicates that the localization performance of SOLID suffers in the case of low detection thresholds, i.e., $\eta < 6$ dB, due mainly to *overfiltering*, i.e., some of the well-behaving sensors are flagged as malicious and then their reports are discarded. On the other hand, too high a detection threshold, i.e., $\eta > 6$ dB, also degrades localization performance because of *underfiltering*, in which some of the attackers evade detection, thus adversely influencing the localization process.

Fig. 7b clearly shows the tradeoff in determining the attack-detection threshold η in terms of false-alarm (denoted by P_{FA}) and misdetection (denoted by P_{MD}) probabilities. SOLID is shown to achieve near zero P_{MD} and to maintain a low false-alarm rate, i.e., $P_{FA} < 6\%$, unless the detection threshold is significantly larger than the attack strength, i.e., $\eta > 10$ dB.

Therefore, the attack detection threshold must be chosen carefully to balance the tradeoff between false-alarm and misdetection probabilities, while considering their dependency on attack strengths and SOLID's tolerance to weak attacks, as observed in Fig. 4.

6.5 Improvement in Spatial Spectrum Reuse

The SUs located within a keep-out-radius of R_e from a small-scale PU (e.g., a WM) must vacate the channel to avoid excessive interference with primary communications [6]. The keep-out-radius needs to be enlarged when the localization is inaccurate, thus reducing not only spatial spectrum utilization, but also spectrum sensing efficiency. SOLID achieves high spatial spectrum efficiency by providing accurate location of mobile primary transmitters. We quantify the improvement in spectrum efficiency made by SOLID by introducing the metric of *spatial spectrum opportunity loss* (SSOL), which is defined as the extended area of PU protection due to the inaccuracy of PUs' localization. Assuming a localization error of ϵ, the spatial spectrum opportunity loss due to the inaccuracy of the

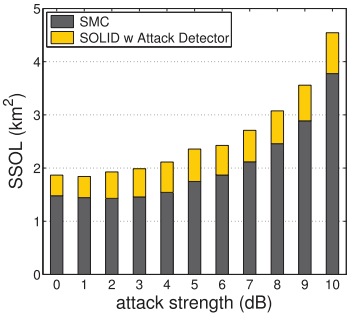


Fig. 8. Spatial spectrum opportunity loss. SOLID significantly reduces the spatial spectrum loss by significantly improving accuracy in mobile primary tracking.

tracking process can be roughly approximated as $SSOL \approx \pi(R_e+\epsilon)^2 - \pi R_e^2 = \pi\epsilon^2 + 2\pi R_e\epsilon$.

Fig. 8 compares the spatial spectrum opportunity loss of SMC-based tracking and SOLID, assuming the keep-out-radius of $R_e = 2$ km, which is reasonably sufficient to provide a typical WM transmission range of 100-150 m. The figure clearly indicates that SOLID maintains small $SSOL$, improving spatial spectrum efficiency substantially. Note that the improved spectrum efficiency can be translated to other performance metrics, such as network throughput of SUs. For example, the increased keep-out-radius R_e indicates that more SUs must vacate the channel to avoid potential interference to primary communications. Therefore, when the keep-out-radius is increased by ϵ, additional SUs, i.e., on average $\rho\,(\pi\epsilon^2 + 2\pi\epsilon)$ where ρ is average SU density, must remain silent on the target channel, thus degrading the overall SU network throughput.

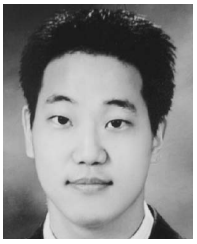
7 Conclusion

In this paper, we have introduced SOLID, which enables accurate and robust location tracking of small-scale mobile primary users in CRNs. By jointly performing localization and shadow-fading estimation, SOLID significantly improves the accuracy of mobile primary user tracking and masks the effect of manipulated sensing reports by accurately detecting and filtering them out. Our in-depth evaluation results, in realistic wireless environments, show that SOLID reduces localization error significantly both in the absence/presence of attacks, including the "slow-poisoning" attack. The enhanced primary tracking capability offered by SOLID enables the secondary system to improve considerably in overall spectrum efficiency.

References

[1] "Second Memorandum Opinion and Order,"FCC 10-174, Sept. 2010.
[2] *IEEE 802.22 Working Group on Wireless Regional Area Networks,* http://www.ieee802.org/22/, 2011.
[3] *IEEE 802.22 Working Group on Wireless Local Area Networks,* http://www.ieee802.org/11/, 2011.
[4] J. Wang, M. Song, S. Santhiveeran, K. Lim, G. Ko, K. Kim, S. Hwang, M. Ghosh, V. Gaddam, and K. Challapali, "First Cognitive Radio Networking Standard for Personal/Portable Devices in TV White Spaces," *Proc. IEEE Symp. New Frontiers in Dynamic Spectrum Access Networks (DySPAN),* Apr. 2010.
[5] P. Bahl, R. Chandra, T. Moscibroda, R. Murty, and M. Welsh, "White Space Networking with Wi-Fi like Connectivity," *Proc. ACM SIGCOMM,* Aug. 2009.
[6] G. Chouinard, "Wireless Microphone Sensing," IEEE 802.22-07/0530r1, Nov. 2007.
[7] M. Vu, S.S. Ghassemzadeh, and V. Tarokh, "Interference in a Cognitive Network with Beacon," *Proc. IEEE Wireless Comm. Networking Conf. (WCNC),* June 2008.
[8] M.F. Hanif, M. Shafi, P.J. Smith, and P. Dmochowski, "Interference and Deployment Issues for Cognitive Radio Systems in Shadowing Environments," *Proc. IEEE Int'l Conf. Comm. (ICC),* June 2009.
[9] K.R. Chowdhury, M.D. Felice, and I.F. Akyildiz, "TP-CRAHN: A Transport Protocol for Cognitive Radio Ad-hoc Networks," *Proc. IEEE INFOCOM,* Apr. 2009.
[10] R. Chen, J.-M. Park, and J.H. Reed, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks," *IEEE J. Selected Areas Comm.,* vol. 26, no. 1, pp. 25-37, Jan. 2008.
[11] S. Liu, Y. Chen, W. Trappe, and L.J. Greenstein, "ALDO: An Anomaly Detection Framework for Dynamic Spectrum Access Networks," *Proc. IEEE INFOCOM,* Apr. 2009.
[12] S. Huang and X. Liu, and Z. Ding, "Distributed Power Control for Cognitive User Access Based on Primary Link Control Feedback," *Proc. IEEE INFOCOM,* Mar. 2010.
[13] A.W. Min, X. Zhang, and K.G. Shin, "Spatio-Temporal Fusion for Small-Scale Primary Detection in Cognitive Radio Networks," *Proc. IEEE INFOCOM,* Mar. 2010.
[14] A.W. Min, X. Zhang, and K.G. Shin, "Detection of Small-Scale Primary Users in Cognitive Radio Networks," *IEEE J. Selected Areas Comm.,* vol. 29, no. 2, pp. 349-361, Feb. 2011.
[15] FCC, "Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Spectrum Agile Radio Technologies,"Rep. ET Docket No. 03-108, Dec. 2003.
[16] "USRP: Universal Software Radio Peripheral," http://www.ettus.com, 2012.
[17] K. Tan et al., "Sora: High Performance Software Radio Using General Purpose Multi-core Processors," *Proc. USENIX Symp. Networked Systems Design and Implementation,* Apr. 2009.
[18] S.M. Mishra, R. Tandra, and A. Sahai, "Coexistence with Primary Users of Different Scales," *Proc. IEEE Symp. New Frontiers in Dynamic Spectrum Access Networks (DySPAN),* Apr. 2007.
[19] S. Anand, Z. Jin, and K.P. Subbalakshmi, "An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks," *Proc. IEEE Symp. New Frontiers in Dynamic Spectrum Access Networks (DySPAN),* Oct. 2008.
[20] Y. Liu, P. Ning, and H. Dai, "Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures," *Proc. IEEE Symp. Security and Privacy,* May 2010.
[21] R. Chen, J.-M. Park, and K. Bian, "Robust Distributed Spectrum Sensing in Cognitive Radio Networks," *Proc. IEEE INFOCOM,* Apr. 2008.
[22] P. Kaligineedi, M. Khabbazian, and V.K. Bharava, "Secure Cooperative Sensing Techniques for Cognitive Radio Systems," *Proc. IEEE Int'l Conf. Comm. (ICC),* May 2008.
[23] A.W. Min and K.G. Shin, "Secure Cooperative Sensing in IEEE 802.22 WRANs Using Shadow Fading Correlation," *IEEE Trans. Mobile Computing,* vol. 10, no. 10, pp. 1434-1447, Oct. 2011.
[24] L. Duan, A.W. Min, J. Huang, and K.G. Shin, "Attack Prevention for Collaborative Spectrum Sensing in Cognitive Radio Networks," *J. Selected Areas Comm.,* vol. 30, no. 9, pp. 1658-1665, Oct. 2012.
[25] A.W. Min, K.-H. Kim, and K.G. Shin, "Robust Cooperative Sensing via Stat Estimation in Cognitive Radio Networks," *Proc. IEEE Symp. New Frontiers in Dynamic Spectrum Access Networks (DySPAN),* May 2011.
[26] P. Bahl and V.N. Padmanabhan, "RADAR: An In-Building RF-Based User Location and Tracking System," *Proc. IEEE INFOCOM,* Mar. 2000.
[27] C. Gui and P. Mohapatra, "Power Conservation and Quality of Surveillance in Target Tracking Sensor Networks," *Proc. ACM MobiCom,* Sept. 2004.
[28] A. Smith, H. Balakrishnan, M. Goraczko, and N. Priyantha, "Tracking Moving Devices with the Cricket Location System," *Proc. ACM Int'l Conf. Mobile Systems, Applications, and Services (MobiSys),* June 2004.
[29] P. Zhang and M. Martonosi, "LOCALE: Collaborative Localization Estimation for Sparse Mobile Sensor Networks," *Proc. ACM Int'l Conf. Information Processing in Sensor Networks (IPSN),* Apr. 2008.

[30] M. Ding and X. Cheng, "Fault Tolerant Target Tracking in Sensor Networks," *Proc. ACM MobiHoc,* May 2009.
[31] X. Sheng, Y.-H. Hu, and P. Ramanathan, "Distributed Particle Filter with GMM Approximation for Multiple Targets Localization and Tracking in Wireless Sensor Networks," *Proc. IEEE Int'l Conf. Information Processing in Sensor Networks (IPSN),* Apr. 2005.
[32] C.R. Stevenson, C. Cordeiro, E. Sofer, and G. Chouinard, *RAN Requirements,* IEEE 802.22-05/0007r46, Sept. 2005.
[33] S. Shellhammer, S. Shankar, R. Tandra, and J. Tomcik, "Performance of Power Detector Sensors of DTV Signals in IEEE 802.22 WRANs," *Proc. ACM First Int'l Workshop Technology and Policy for Accessing Spectrum (TAPAS),* Aug. 2006.
[34] 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 J. Selected Areas Comm.,* vol. 17, no. 7, pp. 1205-1211, July 1999.
[35] 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 J. Selected Areas Comm.,* vol. 20, no. 3, pp. 523-531, Apr. 2002.
[36] W.-P. Chen, J.C. Hou, and L. Sha, "Dynamic Clustering for Acoustic Target Tracking in Wireless Sensor Networks," *IEEE Trans. Mobile Computing,* vol. 3, no. 3, pp. 258-271, July-Sept. 2004.
[37] M. Gudmundson, "Correlation Model for Shadow Fading in Mobile Radio Systems," *Electronic Letters,* vol. 27, no. 23, pp. 2145-2146, Nov. 1991.
[38] G. Chandrasekaran, M.A. Ergin, M. Gruteser, R.P. Martin, J. Yang, and Y. Chen, "DECODE: Exploiting Shadow Fading to DEtect COMoving wireless Devices," *IEEE Trans. Mobile Computing,* vol. 8, no. 12, pp. 1663-1675, Dec. 2009.
[39] L. Hu and D. Evans, "Localization for Mobile Sensor Networks," *Proc. ACM MobiCom,* Sept. 2004.
[40] A. Baggio and K. Langendoen, "Monte-Carlo Localization for Mobile Wireless Sensor Networks," *Proc. Int'l Conf. Mobile Ad-Hoc and Sensor Networks (MSN),* Dec. 2006.
[41] M. Rudafshani and S. Datta, "Localization in Wireless Sensor Networks," *Proc. IEEE Int'l Conf. Information Processing in Sensor Networks (IPSN),* Apr. 2007.
[42] S. Haykin, *Adaptive Filter Theory,* second ed. Prentice Hall, 1991.
[43] G. Chouinard, *Sensing Performance with the 802.22.1 Wireless Microphone Beacon,* IEEE 802.22-09/0068r1, Mar. 2009.
[44] J. Yoon, M. Liu, and B. Noble, "Sound Mobility Models," *Proc. ACM MobiCom,* Sept. 2003.
[45] A.W. Min and K.G. Shin, "On Sensing-Access Tradeoff in Cognitive Radio Networks," *Proc. IEEE Symp. New Frontiers in Dynamic Spectrum Access Networks (DySPAN),* Apr. 2010.
[46] A.W. Min and K.G. Shin, "An Optimal Sensing Framework Based on Spatial RSS-Profile in Cognitive Radio Networks," *Proc. IEEE Sixth Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON),* June 2009.
[47] S.M. Alamouti, "A Simple Transmit Diversity Technique for Wireless Communications," *IEEE J. Selected Areas Comm.,* vol. 16, no. 8, pp. 1451-1458, Oct. 1998.
[48] B. Sklar, "Rayleigh Fading Channel in Mobile Digital Communication Systems Part I: Characterization," *IEEE Comm. Magazine,* vol. 35, no. 7, pp. 90-100, July 2002.



Alexander W. Min (S'08-M'11) received the BS degree in electrical engineering from Seoul National University, Korea, in 2005 and the PhD degree in electrical engineering and computer science from the University of Michigan, Ann Arbor, in 2011. He is currently a research scientist in the Circuits and Systems Research at Intel Labs. In 2010, he was a research intern at Deutsche Telekom, Inc., R&D Labs, Los Altos, California. His research interests include cognitive radio and dynamic spectrum access networks, wireless security, low-power mobile platform, and mobile sensing. He has served on technical program committees for leading conferences in the wireless networking area. He is a member of the IEEE and the ACM.

Kang G. Shin (F'92) is the Kevin & Nancy O'Connor Professor of computer science in the Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor. He has supervised the completion of 73 PhDs, and authored/coauthored about 800 technical articles (about 300 of these are in archival journals), one a textbook and more than 20 patents or invention disclosures, and received numerous best paper awards, including the Best Paper Awards from the 2011 ACM International Conference on Mobile Computing and Networking (MobiCom'11), the 2011 IEEE International Conference on Autonomic Computing, the 2010 and 2000 USENIX Annual Technical Conferences, as well as the 2003 IEEE Communications Society William R. Bennett Prize Paper Award and the 1987 Outstanding IEEE Transactions of Automatic Control Paper Award. His current research focuses on computing systems and networks as well as on embedded real-time and cyber-physical systems, all with emphasis on timeliness, security, and dependability. He has also received several institutional awards, including the Research Excellence Award in 1989, Outstanding Achievement Award in 1999, Distinguished Faculty Achievement Award in 2001, and Stephen Attwood Award in 2004 from The University of Michigan (the highest honor bestowed to Michigan Engineering faculty); the Distinguished Alumni Award of the College of Engineering, Seoul National University in 2002; 2003 IEEE RTC Technical Achievement Award; and 2006 Ho-Am Prize in Engineering (the highest honor bestowed to Korean-origin engineers). He is a fellow of the IEEE.