Attack-Tolerant Distributed Sensing for Dynamic Spectrum Access Networks

Alexander W. Min, Kang G. Shin, and Xin Hu
Real-Time Computing Laboratory, Dept. of EECS
The University of Michigan, Ann Arbor, MI 48109-2121
{alexmin, kgshin, huxin}@eecs.umich.edu

***Abstract*—Accurate sensing of the spectrum condition is of crucial importance to the mitigation of the spectrum scarcity problem in dynamic spectrum access (DSA) networks. Specifically, distributed sensing has been recognized as a viable means to enhance the incumbent signal detection by exploiting the diversity of sensors. However, it is challenging to make such distributed sensing secure due mainly to the unique features of DSA networks—openness of a low-layer protocol stack in SDR devices and non-existence of communications between primary and secondary devices. To address this challenge, we propose *attack-tolerant distributed sensing protocol* (ADSP), under which sensors in close proximity are grouped into a cluster, and sensors in a cluster cooperatively safeguard distributed sensing. The heart of ADSP is a novel shadow fading correlation-based filter tailored to anomaly detection, by which the fusion center pre-filters abnormal sensor reports via cross-validation. By realizing this correlation filter, ADSP minimizes the impact of an attack on the performance of distributed sensing, while incurring minimal processing and communications overheads. The efficacy of our scheme is validated on a realistic two-dimensional shadow-fading field, which accurately approximates real-world shadowing environments. Our extensive simulation-based evaluation shows that ADSP significantly reduces the impact of attacks on incumbent detection performance.**

I. Introduction

Accurate sensing of spectrum condition is a key to the opportunistic use of licensed spectrum bands in dynamic spectrum access (DSA) networks, thus mitigating the spectrum scarcity problem. The goal of spectrum sensing is to reliably detect in real time the presence or absence of primary signals on a spectrum band. To achieve this goal, numerous sensing techniques and algorithms have been proposed, including physical-layer signal detection [1], [2], optimal channel selection [3], [4], MAC-layer sensing scheduling and sensor selection [5], sensor mobility [6], and associated performance tradeoffs [7], to name a few.[1]

In particular, distributed sensing [8], [9] has recently received considerable attention from the research community as a viable means to enhance the detection performance by exploiting spatial diversity in received signal strengths (RSSs) at sensors. However, the sensor reports from the sensors can be manipulated by attackers in various ways, such as primary signal emulation [10], [11] and sensing results falsification [12]. These sensing-targeted attacks can severely undermine the primary/incumbent detection performance because the fusion rule for a final decision relies solely on the reported RSSs. Sensing-targeted attacks pose a significant threat as they can disable opportunistic spectrum access, the basic premise of DSA. We call these unique sensing-targeted attacks in DSA networks *sensing-disorder attacks*.

A sensing-disorder attack aims to obscure the existence of a primary signal by manipulating the spectrum sensing information (e.g., measured RSSs) either by raising or lowering the signal strength. When no primary signal exists, attackers can raise RSSs to generate an illusion of a primary signal. For example, in the IEEE 802.22 WRANs [13], an attacker can transmit a fake sensor report to force all users in the entire cell (of radius up to 100 km) to immediately vacate the channel [14]. Once users in the cell vacate the channel, the attacker can freely use the channel without any interruption. When there is a primary signal, on the other hand, attackers can lower the RSSs to veil the presence of a primary signal, resulting in an unacceptable level of interference to the primary users. In both cases, attackers mislead the fusion center (i.e., BS) to make an incorrect decision on the existence of a primary signal, causing a waste of spectrum resources or unacceptable interference to the primary communications. Therefore, there is a clear incentive for attackers to launch the sensing-disorder attacks.

While the sensing-disorder attacks can be easily launched with the aid of programmable software-defined radio (SDR) devices, their detection is difficult. Unlike the ordinary Denial-of-Service (DoS) attacks that exhaust all the network resources, they can be easily mounted by using SDR devices, such as USRP [15] and Sora [16]. These open-source SDR platforms can be an attractive target for attackers because of their accessibility of low-layer protocol stacks like PHY and MAC [17]. Detecting these attacks, however, is not an easy task. While secure mechanisms such as MAC-layer or crypto-based authentication work well in traditional wireless networks, lack of primary-secondary communications precludes their usage. Moreover, the detection is exacerbated by the volatile nature of wireless medium itself, which makes it hard to differentiate between the legitimate and deliberately manipulated sensor reports. Despite the seriousness of these threats, they have been overlooked in the design of existing distributed sensing schemes. The authors of [12] proposed a reputation management scheme to minimize the impact of falsified sensing results. The reputation scheme, however, is based on a simple voting rule without considering the randomness in physical-layer signal propagation characteristics. We thus need to devise a mechanism that can protect distributed sensing from the above-mentioned attacks.

In this paper, we propose an attack-tolerant distributed sensing protocol (ADSP) for DSA networks that filters out the abnormal sensor reports (caused by either adversaries or mal-

[1]In this paper, we use terms *secondary user* and *sensor* interchangeably as we focus on the sensing functionality of secondary users.

functioning sensors) by exploiting shadow fading correlation in RSSs. This RSS-based filtering approach is motivated by the fact that a DSA network relies only on the physical-layer signal detection for dynamic spectrum access, while attackers cannot control the physical-layer signal propagation.

A. Contributions

This paper makes the following main contributions:

- Proposal of a novel *correlation filter* for detecting abnormal sensor reports that (i) exploits *shadow fading correlation* in RSSs without any additional communication, (ii) safeguards *both* types of attacks that aim to increase either the incumbent false-alarm (type-1) or misdetection (type-2) rates, and (iii) minimizes processing and sensing overheads as it requires only a single sample from each sensor, while achieving high accuracy. Despite their importance, type-2 attacks have not been considered in previous work.
- Introduction of a cluster-based distributed sensing to exploit shadowing correlation. Correlation between sensors, which is entailed by sensor clustering, is known to have a detrimental impact on incumbent detection performance [8], [9], [18]. Our simulation study, however, shows that the proposed clustering does not incur perceivable performance degradation even in a very low SNR environment. Therefore, the sensor clustering is an efficient and useful approach to the sensing disorder attacks.
- Development of a new data fusion rule tailored to attack-tolerance. Specifically, we propose *weighted gain combining* (WGC) that adaptively assigns different weights to sensor reports according to their statistical significance based on the normal shadowing profile. As a result, it minimizes the influence of the unfiltered attacks (due to their small deviations) on a final decision, and thus further improves attack-tolerance.
- In-depth evaluation in a realistic two-dimensional shadow fading environment, which has not been considered before; most previous work uses a simple but inaccurate one-dimensional model. Our simulation results show that the proposed filtering scheme successfully withstands the attacks by reducing the false-alarm rate up to $99.2\,\%$ and achieving up to $97.4\,\%$ of maximum achievable detection rate (see Section VI for details).

B. Organization

The remainder of this paper is organized as follows. Section II reviews the related work in distributed spectrum sensing and highlights the original contributions of our work. Section III describes the system and attack models used in this paper. Section IV presents our proposed approach for attack detection, and the generation of a realistic two-dimensional shadowing correlation model. Section V details our approach for the filter design and the proposed data-fusion model. Section VI evaluates the performance of ADSP, and Section VII concludes the paper.

II. Related Work

In this section, we first summarize distributed spectrum sensing and then review existing sensing-related attacks and their countermeasures in DSA networks.

Distributed Sensing in DSA Networks: Distributed sensing has been recognized as a viable means to improve the sensing performance, thus meeting the stringent incumbent detection requirements imposed by the FCC. Performance of distributed sensing has been studied extensively [3]–[9], [18]. While most of previous work has considered the benign use of distributed sensing to improve incumbent detection under the assumption that the sensors are completely reliable, we focus on quantifying the extent to which detection performance can suffer and tolerate if sensors operate incorrectly or maliciously.

Robust Distributed Sensing: Despite its importance, the problem of ensuring the robustness in distributed sensing has only started to receive attention. Our work also belongs to this category. Anand *et al.* [11] analyzed the feasibility of the Primary User Emulation Attack (PUEA) and presented a lower-bound on the probability of a successful PUEA. However, they did not address the impact of PUEA on the performance of distributed sensing. Chen *et al.* [10] proposed an RSS-based location verification scheme to detect a fake primary transmitter. 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. They also proposed a robust data-fusion scheme that dynamically adjusts the reputation of sensors based on the majority rule [12]. Similarly, in the IEEE 802.22 standard draft, a voting rule [19] has been proposed for secure decision fusion. However, the voting rule may not work well in a very low SNR environment where a majority of sensors fail to detect the primary signal. Kaligineedi *et al.* [20] presented a pre-filtering scheme based on a simple outlier method that filters out extremely low or high sensing reports. However, their method is not suitable 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. This scheme will be used as a reference in evaluating our proposed scheme (see Section VI for details).

Detecting Unauthorized Spectrum Use: The problem of enforcing/enticing secondary users to observe the spectrum etiquette has also started to receive attention from the research community. Woyach *et al.* [21] studied how to entice secondary users to observe the spectrum etiquette by giving them incentives via a game-theoretic approach. In a similar context, Liu *et al.* [22] studied the problem of detecting unauthorized use of a licensed spectrum. They exploited the path-loss effect as a main criterion for detecting anomalous spectrum usage and presented a machine-learning approach for more general cases. By contrast, we focus on intelligent filtering of suspicious sensor reports.

In summary, our scheme differs from previous work in several key aspects. First, we exploit shadow fading correlation for anomaly detection, which has not been considered previously. Second, our scheme is unique in that it enables normal spectrum sensing operation even in a hostile environment by *proactively* filtering out suspicious sensing reports, and then assigning different weights for the remaining sensor reports, while most previous approaches are reactive in case of attack detection. Third, our scheme can detect the attacks that purposely lower the RSS to obscure the existence of a primary signal (i.e., type-2 attacks), whereas most of previous work focused on detecting spoofed primary signals (i.e., type-1 attacks).

III. System and Attack Model

We now describe the DSA network model and the received signal strength (RSS) model to be used throughout the paper. We then review the energy-detection technique and introduce the data-fusion model, and finally present the attack model.

A. Network Model

We consider a DSA network where primary (licensed) and secondary (unlicensed) users coexist. Secondary users form an infrastructure-based system where a central entity (i.e., a base station or fusion center) manages their DSA via distributed spectrum sensing. The central node, which we assume adversaries cannot compromise, schedules sensing and decides the presence/absence of a primary signal based on the sensing reports. The sensors can be stationary or mobile.

In general, two types of primary users exist in DSA networks according to their relative location to the secondary network and transmission power level: (i) long-range primary signal (e.g., TV transmitters) and (ii) short-range primary signal (e.g., wireless microphones). In this paper, we consider a DSA network where the short-range primaries does not exist or their use is prohibited,[2] and focus on long-range primaries, which are located far away (e.g., tens of kilometers) from the secondary network, and use high transmit power. Thus, the entire secondary network (or cell) lies within the detection range of the primary signal. A typical example of this type is a TV transmitter in the IEEE 802.22 WRANs. While the techniques we propose here can be applied to any distributed sensing, without loss of generality, we will focus on 802.22 WRANs with a DTV transmitter.

B. Signal Propagation and Sensing Models

1) RSS Model: As mentioned earlier, our scheme relies solely on the RSS (i.e., the energy-detector's output) at sensors where the received primary signal strength at sensor i can be expressed as the propagation model [24]:

$$P_i = P_o\Big(\frac{d_o}{d_i}\Big)^{\alpha} e^{X_i} e^{Y_i} \quad \text{(Watt)}, \tag{1}$$

where P_o is the signal strength at the primary transmitter, α the path-loss exponent, d_o the reference distance, and d_i the distance from the primary transmitter to the sensor i. Shadow fading is accounted for in e^{X_i} where $X_i \sim \mathcal{N}(0, \sigma^2)\ \forall i$, while e^{Y_i} accounts for small-scale multi-path fading, antenna and device caused losses. The log-normal shadow fading is often characterized by its dB-spread, σ_{dB}, which has the relationship $\sigma = 0.1\log_e(10)\sigma_{dB}$. We assume that the channel bandwidth is much larger than the coherent bandwidth, so the effect of multi-path fading is negligible, i.e., $Y_i = 0\ \forall i$ [1].

2) Spectrum Sensing Model: The energy detector is the most widely-used detection technique for its simple design and efficiency [1], [25]. Although the feature detector is more accurate, it takes much longer (e.g., 24 ms for the field-sync detector for ATSC) [2] because it looks for a specific signature of the primary signal that appears infrequently. The test statistic of the energy detector is an estimate of average RSS (including the noise power), and it can be approximated as a Gaussian using the Central Limit Theorem (CLT) as [13]:

$$T_i \sim \begin{cases} \mathcal{N}\big(N_o, \frac{N_o^2}{M}\big) & \mathcal{H}_0 \text{ (no primary signal)} \\ \mathcal{N}\big(P_i + N_o, \frac{(P_i+N_o)^2}{M}\big) & \mathcal{H}_1 \text{ (primary signal exists)}, \end{cases} \tag{2}$$

where P_i is the power of a received primary signal, N_o the noise power, and M the number of signal samples.

C. Data-Fusion Model

In distributed sensing, the final decision on the presence or absence of a primary signal can be made via either *decision fusion* or *data fusion* [7]. Here we consider data fusion rather than decision fusion as the final rule for incumbent detection. While the decision fusion reduces the overhead in reporting the sensing results, it is difficult to thwart the sensing-disorder attacks since it only provides a binary value based on a local decision.

In fading channels, equal gain combining (EGC) is known to have near-optimal performance without needing to estimate the channel gains [26]. EGC has the following decision statistic:

$$T_\Sigma \triangleq \sum_{i=1}^{n_s} w_i\, T_i, \tag{3}$$

where T_i is the test statistic of the energy detector at sensor i, n_s is the number of cooperative sensors, and the sensors have an identical weight, i.e., $w_i = 1\ \forall i$. The decision threshold to achieve the desired level of Q_{FA} can be derived as [25]:

$$\eta = Q^{-1}(Q_{FA})\,\frac{\sqrt{n_s}N_o}{\sqrt{M}} + n_s N_o. \tag{4}$$

The performance of EGC will be used as a baseline in evaluating the efficacy of the proposed scheme.

Moreover, in order to achieve better attack-tolerance, we propose *weighted gain combining* (WGC) that adjusts the weights so as to minimize the impact of mis-detections on the final decision (detailed in Section V-D).

D. Attack Model

1) Attack Scenarios: Sensing can be disrupted as follows.

- A sensor is compromised, and then manipulates its sensing reports, i.e., raises or lowers RSSs.
- A sensor is malfunctioning or faulty, yielding readings that deviate from the actual RSS.

A common consequence of the above two cases is that the sensor reports to the fusion center are distorted, thus increasing the probability for the fusion center to make a wrong decision. To solve this problem efficiently, we focus on the detection of any abnormal sensing report instead of pinpointing the actual cause of abnormality, which is part of our future work.

Note that another possible attack scenario is a primary user emulation attack (PUEA), as studied in [10], [11], [22]. However, this attack is relatively easy to detect mainly because the attacker has only a coarse-grained control of RSS at sensors since signals are broadcast. In the above two scenarios, however, the attacker has a fine-grained control of RSSs on individual sensors, and thus, the attacks are stealthier than PUEA, making their detection harder. Therefore, we will focus on the above two attack scenarios.

[2]For example, the FCC recently decided to prohibit low power auxiliary devices such as wireless microphones operating within 700 MHz band, after the end of DTV transition on June 2009 [23].

2) Attack Types: We consider two types of attacks that can be mounted (caused) by attackers (faulty nodes):

- **Type-1 Attacks**: increase the *false-positive* rate (classifying a non-primary signal as primary) by raising RSSs, and
- **Type-2 Attacks**: increase the *false-negative* rate (causing failure to detect a primary signal) by lowering RSSs.

We assume that the attackers are intelligent, and thus know the presence/absence of a primary signal regardless of the decision made by the fusion center, and launch type-1 (type-2) attacks under $\mathcal{H}_0$ ($\mathcal{H}_1$); otherwise, attacks only serve to improve the incumbent detection performance.

3) Final Sensor Reports: Under the above model, a final sensor report to the fusion center can be expressed (in Watt) as:

$$R_i = \underbrace{P_i + N_o + E_i}_{\text{ED output } (T_i)} + D_i \quad \forall i, \tag{5}$$

where T_i is the test statistic of the energy detector (ED) (Eq. (2)) including the measurement error $E_i \sim \mathcal{N}(0, \frac{N_o^2}{M})$, and $D_i \in \mathbb{R}$ is the deviation or *attack strength*, tampered with by a compromised sensor; $D_i = 0$ for normal sensors. Note that no loss of reporting packets is assumed, so we can focus on the detection of abnormal sensor reports.

IV. The Proposed Approach

It is, in reality, impossible to prevent all possible attacks or misbehavior that can affect the sensor reports. Therefore, we aim to make distributed sensing *attack-tolerant*, i.e., minimize the impact of compromised sensor reports on the final decision. For this, we propose an *attack-tolerant distributed sensing protocol* (ADSP) that has the following salient features: It

1) successfully tolerates attacks (or faults or effects) of malicious (or faulty) sensors,
2) exploits physical-layer signal propagation characteristics with low processing overhead,
3) preserves compatibility with existing security and data-fusion mechanisms, and
4) achieves high detection accuracy and efficiency.

In what follows, we present the design rationale behind ADSP, its framework, and the methodology to generate a spatially-correlated shadow fading field.

A. Design Rationale

To maximize attack-tolerance and preserve the detection accuracy of data fusion, ADSP employs anomaly detection based on statistics. Specifically, ADSP exploits physical-layer signal propagation characteristics, or the spatial correlation in RSSs among neighboring sensors. The key insight behind ADSP is that, in shadow fading environments, RSSs among nearby sensors are likely to be highly correlated, which can be used to identify the manipulated sensor reports. The adversaries must be aggressive in raising or lowering the RSSs reported to the fusion center in order to influence the outcome of the final decision. However, any sensor report that significantly deviates from what is expected is deemed suspicious of being malicious or malfunctioning, and those sensing results will be discarded or penalized by the fusion center in making a final decision. Adversaries must, therefore, lower their attack strength, reducing the chance for the fusion center to make a wrong decision; otherwise, they must risk getting caught by the detector. This way, the fusion center can achieve a high level of attack-tolerance, provided the majority[3] of its neighbors are well-behaving.

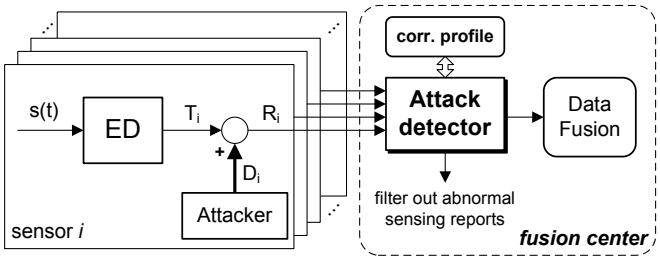


Fig. 1. *The ADSP framework*: Compromised (or malfunctioning) sensors might contaminate their sensing reports R_i. The attack detector filters out these contaminated sensor reports based on the shadowing correlation profile and then feeds the remaining ones to the final fusion center.

B. ADSP Framework

ADSP consists of the following three building blocks:

- **sensing manager** that manages sensor clusters and directs the sensors to report their readings at the end of each scheduled sensing period,
- **attack detector** that detects and discards (or penalizes) the abnormal sensing reports based on the pre-established shadowing correlation profile, and
- **data-fusion center** that determines the presence or absence of a primary signal based on the filtered sensing results.

These three components closely interact with each other and form a robust distributed sensing system. Fig. 1 depicts the ADSP framework, which is *lightweight* in that it can be implemented at the fusion center without requiring any modification to sensors or incurring additional communication overhead.

One important and unique feature of the attack detector is the ability to tolerate *both* type-1 and 2 attacks. This feature is attributed to the fact that the detector *cross-checks* the sensor reports and the assumption that at least $2/3$ of the sensors are well-behaving. As a result, under type-1(2) attacks, the sensor reports with relatively high (low) values are likely to be flagged by more of its neighboring sensors, thus making our scheme applicable regardless of the existence of a primary signal. This makes the system design simple and efficient, while achieving high attack-tolerance (see Section VI for detailed results).

C. Generation of Spatially-Correlated Shadow Fading

To incorporate the spatially-correlated shadow fading in our analysis and simulation, we need a shadow correlation model in which the statistics accurately reflect the real-world wireless shadowing environment. Note that a model-based approach is unavoidable since measurement data for shadow fading is very scarce, and conducting a field test is too expensive to do. Gudmundson's model [27] is one of the most widely-used models in accounting for the shadowing correlation. However, it cannot capture spatial shadowing correlation, and hence, analyses based on this model might yield results that

[3]We assume that at least $2/3$ of sensors are well-behaving.

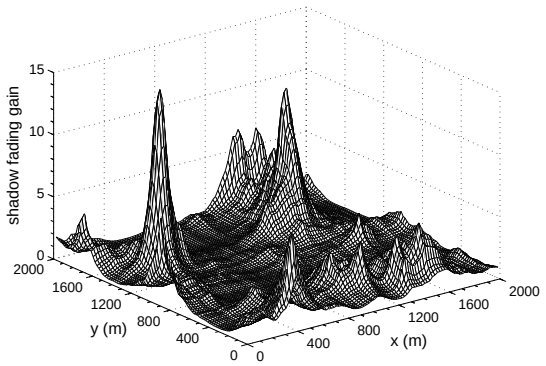


Fig. 2. *Spatially-correlated shadowing random field* $\mathbf{p}(\cdot,\cdot)$: An example of $\mathbf{p}(\cdot,\cdot)$ with exponentially-decaying spatial correlation, where the dB-spread and decorrelation distance are assumed to be $\sigma_{dB} = 4.5\,\text{dB}$ and $D_{corr} = 150\,\text{m}$, respectively. The spatial correlation is assumed to be *isotropic*, i.e., the shadowing correlation depends only on the distance between sensors.

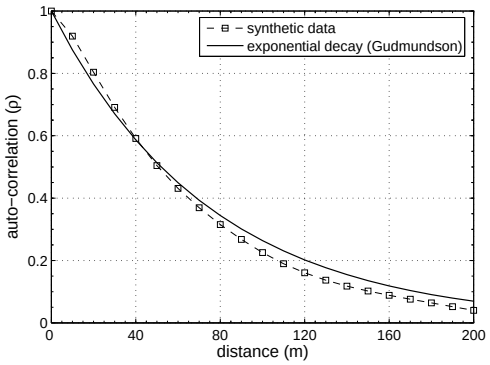


Fig. 3. *Comparison of auto-correlation function*: Theoretical model (solid line) vs. synthetic data from a random field $\mathbf{p}(\cdot,\cdot)$ (dotted line). The correlation is below 0.2 beyond the decorrelation distance $D_{corr} = 150\,\text{m}$.

are significantly different from those in real-world wireless environments, as evidenced in both a theoretical study [28] and empirical measurements [29]. Recently, the authors of [30] proposed a statistical modeling approach to characterization of the spatial spectrum behavior of primary signals in the context of DSA networks.

Along the same line as in [30], we generate spatially-correlated shadow fading in a two-dimensional area by applying the convolution method proposed in [31]. We refer to the thus-generated data set as a *shadowing random field* $\mathbf{p}$ where $\mathbf{p}(x,y)$ represents the shadowing gain at a unit grid area, i.e., $\Delta \times \Delta\,\text{m}^2$, centered at the coordinate $(x,y) \in \mathbb{R}^2$.

The shadowing random field $\mathbf{p}(\cdot,\cdot)$ is assumed to be an isotropic,[4] wide-sense stationary, and log-normally distributed random field with zero mean and exponentially-decaying spatial correlation. Then, the covariance between the two points $\theta_i = (x_i, y_i)$ and $\theta_j = (x_j, y_j)$ in $\mathbf{p}$ is given as:

$$\mathbb{E}\big[\mathbf{p}(\theta_i), \mathbf{p}(\theta_j)\big] = R_{\mathbf{p}}(d_{ij}) = \sigma^2 \cdot e^{-d_{ij}/D_{corr}}, \qquad (6)$$

where $d_{ij} = \|\mathbf{p}(\theta_i) - \mathbf{p}(\theta_j)\|$ is the Euclidean distance between the locations θ_i and θ_j, σ is the standard deviation of shadow fading, and D_{corr} is the decorrelation distance, which depends on local wireless environments (e.g., urban or suburban).[5]

Fig. 2 shows an example *shadowing random field* in a $2 \times 2\,\text{km}^2$ region, which clearly exhibits a strong spatial correlation in shadow fading. To demonstrate the accuracy of this method, Fig. 3 compares the one-dimensional auto-correlation function (ρ) of the random field against the Gudmundson's empirical model with the same set of parameters, i.e., $\sigma_{dB} = 4.5\,\text{dB}$ and $D_{corr} = 150\,\text{m}$. The figure indicates that the synthetic data in the shadowing random field accurately emulates the real-world shadowing correlations. Note that our detection scheme only requires the one-dimensional auto-correlation function of the shadowing field, which can be estimated by the service provider at the time of system deployment.

[4]Note that we do not consider the angular dependency in shadowing correlation for analytical tractability.

[5]For example, a measurement study [32] indicates that a typical decorrelation distance is in the range of $120 - 200\,\text{m}$ in suburban areas.

V. Detection of Abnormal Sensor Reports via Correlation Analysis

In this section, we formulate the anomaly-detection problem as a hypothesis testing, and present the design of a correlation-based filter. To further improve the attack-tolerance of our scheme, we propose a new data-fusion rule, called the *weighted gain combining* (WGC), followed by the description of ADSP.

For distributed sensing, the designated sensors (in a form of clusters) report their energy-detector's output along with its location information to the fusion center, at the end of each sensing period.[6] The location information is required to exploit the shadowing correlation in RSSs; it may be available at the fusion center when the sensors are fixed, e.g., CPEs in 802.22 WRANs. On the other hand, when they are mobile, sensors can obtain their location via location service, e.g., GPS, and then report it along with the RSS. Sensors can employ existing secure localization protocols (e.g., [33]) to obtain accurate sensor location information.

A. Characterization of the Correlation in Sensor Reports

We first study the correlation structure of the sensor reports, which the fusion center actually receives from the sensors. A key observation is that the correlation structure of shadowing components $\{e^{X_i}\}$ is preserved in the sensor reports $\{R_i\}$ under the following conditions:

- no attack (or misbehavior), i.e., $D_i = 0$, and
- weak primary signal, i.e., $P_i + N_o \approx N_o$.[7]

Under the above conditions, and treating all the other terms in Eq. (1) (except e^{X_i} and E_i) as constants, we can express sensor i's report in Eq. (5) as:

$$R_i = C_1\, e^{X_i} + C_2 + E_i \quad \text{(Watt)}, \qquad (7)$$

where $C_1 = P_o\big(d_o/d_i\big)^{\alpha}$, $C_2 = N_o$, and $E_i \sim \mathcal{N}(0, \frac{N_o^2}{M})$ is the measurement error of ED. The correlation in shadowing component e^{X_i} does not change when we add/multiply the same number to/by all of the shadowing components.

[6]We consider two-dimensional sensor coordinates for simplicity, while the actual terrain profile is three-dimensional.

[7]This is a reasonable assumption in a very low SNR environment, e.g., $-20\,\text{dB}$, where the average primary signal power is only about $1\,\%$ of the noise power, i.e., $\mathbb{E}[P_i] = 0.01 \times \mathbb{E}[N_o]$.

Moreover, the variance in measurement error is much smaller than that of shadowing component, i.e., $Var[E_i] < Var[e^{X_i}]$, since the number of samples M is sufficiently large even with a short sensing time, e.g., $M = 6 \times 10^3$ for $T_S = 1$ ms. So, the correlation in the received sensor reports R_i almost preserves the correlation of the shadow fading e^{X_i}, i.e., $Corr(R_i, R_j) \approx Corr(e^{X_i}, e^{X_j})$; furthermore, the degree of correlation varies with their relative locations.

B. Cluster-based Hypothesis Testing

Although we try to exploit shadowing correlation for attack detection, the degree of correlation decreases exponentially with the distance between sensors. This motivates us to form *sensor clusters* $\{\mathcal{C}_k\}_{k=1}^{N_c}$ among the sensors in close proximity so that sensors within the same cluster are highly correlated.[8] In 802.22 WRANs, clusters can be easily formed since the sensors (i.e., CPEs) represent households, and hence clustered by their nature. Therefore, for each sensor i, the correlation-filter checks whether or not it exhibits a proper correlation behavior by examining the following hypothesis testing for each of its neighbors:

$$\mathcal{H}_0^a : Corr(R_i, R_j) = \rho(d_{ij}) \quad j \in N(i), \tag{8}$$

where the neighbor set $N(i)$ is defined as the sensors belong to the same cluster of sensor i. As a result of the cross-validation, the number of flags raised by the neighboring sensors will be used as a filtering criterion (see Section V-E for details). From now on, we focus on the analysis of shadowing correlation in sensor reports.

C. Correlation Analysis for Filter Design

Although the shadowing correlation coefficient (ρ) is an obvious metric for the above hypothesis testing (i.e., Eq. (8)), it is not suitable to use it directly in our problem for the following reasons. First, estimation of the correlation coefficient would require a sequence of samples; this can incur significant time and energy overheads for sensing, and can also slow down the detection of returning primary users. Second, when the sensors are mobile, it is difficult to estimate the correlation between the sensors since their relative distances are not fixed. Therefore, we detect a per-sample abnormal behavior by examining their *similarity* using the conditional probability distributions of the sensor reports. This is an alternative, but efficient approach since higher correlation entails greater similarity, which can be measured via a conditional distribution of sensor reports, as we will describe next.

In order to capture the similarity between sensor reports, we first derive the probability distribution of R_i, which is the sum of non-zero mean normal (i.e., E_i) and log-normal (i.e., e^{X_i}) random variables, as indicated in Eq. (7). To the best of our knowledge, there is no closed-form expression for such a distribution. However, a close examination of Eq. (7) implies that R_i can be approximated as a *shifted log-normal random variable*, i.e., the sum of a log-normal random variable and a constant.

Let us denote the sensor reports by a shifted log-normal random variable, i.e., $R_i = e^{Z_i} + C$ where $Z_i \sim \mathcal{N}(\mu_Z, \sigma_Z^2)$.

[8]The locations of clusters are assumed to be uniformly distributed with in the secondary network, and the issue of optimal selection (or formation) of sensors (or clusters) is not our focus in this paper.

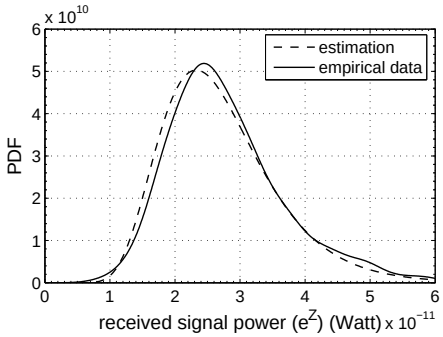


Fig. 4. *Estimation of sensor report as a shifted log-normal distribution*: The empirical data for sensor reports (solid line) obtained from the shadowing field can be accurately approximated as a log-normal distribution (dashed line).

From Eq. (7), we have the following approximation after simple manipulation:

$$e^{Z_i} + C \approx e^{X_i + \ln C_1} + E_i, \tag{9}$$

where $Z_i \sim \mathcal{N}(\mu_Z, \sigma_Z^2)$ and $X_i \sim \mathcal{N}(0, \sigma_X^2)$ with $\sigma_X = \sigma$. We set the constant $C = 4\,\sigma_E$ so that the probability of the right-hand side of Eq. (9) become less than C is close to zero (i.e., $\approx 3 \times 10^{-5}$). This is important because the log-normal random variable e^{Z_i} cannot have a negative value.

Then, we estimate the mean and variance of e^{Z_i} using a moment-matching method. By matching the mean and variance of both sides of Eq. (9), we obtain $\hat{\sigma}_Z^2$ and $\hat{\mu}_Z$ as:[9]

$$\hat{\sigma}_Z^2 = \log\left[\frac{C_1^2\,(e^{\sigma_X^2} - 1)\,e^{2\mu_X + \sigma_X^2} + \sigma_E^2}{(C_1\,e^{\mu_X + \sigma_X^2/2} + \mu_E + C)^2} + 1\right], \tag{10}$$

and

$$\hat{\mu}_Z = \log\left[\frac{C_1\,e^{\mu_X + \sigma_X^2/2} + \mu_E + C}{e^{\hat{\sigma}_Z^2/2}}\right]. \tag{11}$$

Fig. 4 shows an example of such an approximation. While the figure indicates that the sensor reports can be accurately estimated by such a distribution, it becomes less accurate as the sensing duration T_S increases. Note, however, that we would like to capture the correlation among sensors in a tractable form, not an accurate approximation that only complicates the analysis without yielding a considerable improvement in detection performance. The impact of the approximation error will be discussed in Section VI.

Based on Eqs. (9), (10), and (11), the p.d.f. of a sensor report can be expressed as:

$$f_R(r) = \frac{1}{(r - C)\,\sigma_Z\sqrt{2\pi}} \exp\left[-\frac{(\ln(r - C) - \mu_Z)^2}{2\,\sigma_Z^2}\right], \quad z \geq 0. \tag{12}$$

Recall that we are interested in examining the similarity of the reports measured at nearby (thus spatially-correlated) sensors. To measure the similarity between sensor reports, we derive the conditional p.d.f. of R_i given $R_j = r_j$ using Eq. (12) as:

$$f_{R_i|R_j}(r_i|r_j) = \frac{1}{(r_i - C)\,\sigma_{R_i|R_j}\sqrt{2\pi}} \exp\left[-\frac{1}{2}\left(\frac{\ln(r_i - C) - \mu_{Z_i|Z_j}}{\sigma_{Z_i|Z_j}}\right)^{1/2}\right], \tag{13}$$

[9]The derivations of Eqs. (10) and (11) are straightforward, and omitted due to space limit.

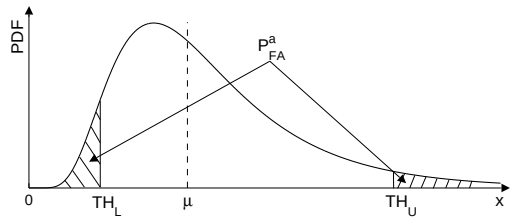


Fig. 5. *The correlation filter for anomaly detection*: Sensor i's report r_i will be flagged if it resides outside of the lower and upper thresholds, i.e., TH_L and TH_U. The conditional p.d.f. is derived using Eq. (13). Thus, the attack false alarm probability can be calculated as $P^a_{FA} = Prob(r_i < TH_L) + Prob(r_i > TH_U)$.

where

$$\mu_{Z_i|Z_j} = \mu_{Z_i} + \rho_{ij}\frac{\sigma_{Z_i}}{\sigma_{Z_j}}\big[\ln(r_j - C) - \mu_{Z_j}\big], \tag{14}$$

and

$$\sigma_{Z_i|Z_j} = \sigma_{Z_i}\sqrt{1-\rho^2_{ij}(d_{ij})}. \tag{15}$$

Eq. (15) indicates that $\sigma_{Z_i|Z_j}$ decreases as the correlation ρ_{ij} increases, and thus greater similarity between sensor reports.

Eqs. (13), (14), and (15) indicate that the conditional distribution of the sensor reports are also log-normally distributed. We thus set the lower and upper thresholds on the sensor reports based on conditional p.d.f. in Eq. (13), and then mark any outlier that resides outside of the thresholds. To set the thresholds, we first derive the cumulative distribution function (c.d.f.) of sensor i's report r_i, given sensor j's report r_j as:

$$\begin{aligned} F_{R_i|R_j}(x) &= Prob(R_i \le x \,|\, R_j = r_j) \\ &= \frac{1}{2} + \frac{1}{2}erf\left[\frac{\ln(x-C) - \mu_{Z_i|Z_j}}{\sigma_{Z_i|Z_j}\sqrt{2}}\right], \quad x \ge 0, \end{aligned} \tag{16}$$

where $erf(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}\mathrm{d}t$.

Using Eq. (16), the thresholds $TH_{\{L,U\}}$ with a $100\times(1-\epsilon)\,\%$ confidence interval can be derived as:

$$TH_{\{L,U\}}(\epsilon) = \exp\Big[\sqrt{2}\cdot erf^{-1}\big(g(\epsilon)\big)\cdot\sigma_{Z_i|Z_j} + \mu_{Z_i|Z_j}\Big] + C, \tag{17}$$

where

$$g(\epsilon) = \begin{cases} \epsilon - 1 & \text{for } TH_L \\ 1-\epsilon & \text{for } TH_U \end{cases} \quad 0 \le \epsilon \le 0.5, \tag{18}$$

where $\mu_{Z_i|Z_j}$ and $\sigma_{Z_i|Z_j}$ are conditional mean and variance in Eqs. (14) and (15), respectively.

Therefore, the null hypothesis $\mathcal{H}^a_0$, i.e., $Corr(R_i, R_j) = \rho(d_{ij})$, cannot be rejected if $r_i \in [TH_L, TH_U]$, as depicted in Fig. 5. Note that the thresholds are set differently for each neighboring sensor, depending on their relative distance and measured RSSs. Clearly, there is a tradeoff in determining the threshold parameter ϵ; i.e., the higher the threshold, the higher (lower) the attack false-alarm (mis-detection) rates.

D. The Proposed Data-Fusion Rule

While the correlation filter accurately detects RSS deviations, we observed that it often mis-detects small deviations (e.g., ≤ 0.3 dB). These small deviations can still influence the data-fusion results in a very low SNR environment due to the high sensitivity of the fusion decision to RSSs. Unfortunately, however, with our design of *hard* filtering, this problem might not be easily overcome by simply increasing the cluster size due to the correlated nature of the sensor clusters. Therefore, as a second line of defense, we propose a new data-fusion rule, namely *weighted gain combining* (WGC), to provide a better attack-tolerance to such small deviations. The idea is to assign different weights to the sensor reports according to their significance level based on the conditional c.d.f. in Eq. (16). This way, the mis-detected (unfiltered) attacks are highly likely to be assigned relatively small weights compared to the legitimate sensor reports because of their lack of significance. Thus, the weights in WGC are defined as:

$$w_i \triangleq \frac{\sum_{j\in N_v(i)} w_{ij}}{|N_v(i)|} \;\text{ where }\; w_{ij} = 1 - 2\,\big|F_{R_i|R_j}(r_i \,|\, r_j) - 0.5\big|, \tag{19}$$

where $N_v(i)$ is the set of valid neighbors of sensor i. The thus-obtained weights are used in calculating the decision statistic T_Σ (in Eq. (3)), and compared with the threshold η (in Eq. (4)).

Algorithm 1 ATTACK-TOLERANT DISTRIBUTED SENSING WITH WEIGHTED GAIN COMBINING

Procedure **ADSP_WGC**($\{R_i\}, Q_{FA}, \beta$)
1: Initialize the decision statistic $T_\Sigma \leftarrow 0$
2: Initialize the number of normal sensor reports $N_{normal} \leftarrow 0$
// Step 1. Filtering
3: **for** each sensor cluster $\mathcal{C}_k$ $k = 1, \ldots, N_c$ **do**
4: **for** each sensor $i \in \mathcal{C}_k$ **do**
5: $(\mathsf{Isnormal}(i), \mathbf{w}_i) \leftarrow$ **CorrFilter**$(i, \{R_j\}_{j\in N(i)}, \beta)$
6: **end for**
7: **end for**
// Step 2. Data fusion
8: **for** each sensor cluster $\mathcal{C}_k$ $k = 1, \ldots, N_c$ **do**
9: **for** each sensor $i \in \mathcal{C}_k$ **do**
10: **if** $\mathsf{Isnormal}(i) = 1$ **then**
11: update w_i using Eq. (19)
12: $T_\Sigma \leftarrow T_\Sigma + w_i\, R_i$
13: $N_{normal} \leftarrow N_{normal} + 1$
14: **end if**
15: **end for**
16: **end for**
17: $T_\Sigma \leftarrow T_\Sigma \times N_{normal} / \sum w_i$ // Normalization
18: Calculate the decision threshold η using Eq. (4)
19: **if** $T_\Sigma > \eta$ **then**
20: **return** 1 // Primary exists
21: **else**
22: **return** 0 // No primary signal
23: **end if**

E. Protocol Description

We now present the attack-tolerant distributed sensing protocol (ADSP) with the proposed WGC for final fusion. **Algorithm 1** describes the overall data-fusion procedure in ADSP. At the end of each sensing period, the fusion center collects sensor reports $\{R_i\}$ from the designated sensors, which are co-located in clusters. Then, it invokes the correlation filter to selectively discard the abnormal sensor reports. Note that the weights are assigned after the filtering process (line 11) so that the filtered abnormal sensor reports would have no influence on them. **Algorithm 2** details the filtering procedure. For each sensor report, the filter counts the number of flags raised by its neighbors in the cluster. Then, it will return $\mathsf{Isnormal}=0$ if more than $\beta \in [0,1]$ fraction of its neighboring sensors mark it as abnormal, where β is a design parameter; otherwise, it will return $\mathsf{Isnormal}=1$. The filter also returns the weight vector ($\mathbf{w}_i$) for future use in the final data-fusion process (i.e., WGC).

Algorithm 2 FILTERING ALGORITHM BASED ON CORRELATION ANALYSIS

Procedure **CorrFilter**$(i, \{R_j\}_{j\in N(i)}, \beta)$

Initialize the counter $\mathsf{blacklist\_counter}(i) \leftarrow 0$
Initialize the weight vector $\mathbf{w}_i \leftarrow [0, \ldots, 0]^T$
Initialize the indicator $\mathsf{Isnormal} \leftarrow 1$
for each neighbor $j \in N(i)$ **do**
  $w_{ij} \leftarrow$ update using Eq. (19)
  if $Corr(R_i, R_j) \neq \rho(d_{ij})$ using Eq. (17) **then**
    $++\,\mathsf{blacklist\_counter}(i)$
  end if
end for
if $\mathsf{blacklist\_counter}(i) > \beta \cdot N(i)$ **then**
  $\mathsf{Isnormal} \leftarrow 0$ // Mark it as abnormal
end if
return $(\mathsf{Isnormal}, \mathbf{w}_i)$

The computational complexity of the algorithm is bounded by $\mathcal{O}(|\mathcal{C}|^2)$ where $|\mathcal{C}|$ is the number of sensors in a cluster.

VI. PERFORMANCE EVALUATION

The performance of ADSP is evaluated via MATLAB-based simulation. We first describe the simulation setup and then present the simulation results for both types of attacks under various attack scenarios.

A. Simulation Setup

To demonstrate the effectiveness of ADSP, we consider an IEEE 802.22 WRAN environment with a single DTV transmitter with 6 MHz bandwidth and multiple secondary users (sensors) located at the edge of the *keep-out radius* of 150.3 km from the DTV transmitter [1]. A secondary network (cell) of radius 30 km is considered for our evaluation, and we generate a two-dimensional shadowing field with a unit grid of $20 \times 20\,\mathrm{m}^2$ to emulate a realistic shadow fading environment in a cell. Throughout the simulation, we assume 5 sensor clusters located randomly within the cell, with 6 sensors in each cluster; the sensors are located in different grids, and the distances between sensors within a cluster range from 0 m to 70 m. We consider the worst-case attack scenario; in each cluster, one-third of the sensors are malicious. Table I lists the system parameters used in our simulation. Each simulation is conducted on 5×10^4 randomly-generated shadowing fields and their average values are taken as the performance measures.

TABLE I
SYSTEM PARAMETERS USED IN SIMULATION

Parameter	Value	Comments
N_s	30	Number of collaborating sensors
N_c	5	Number of clusters
T_S	1 ms	Sensing duration
M	$6 \times 10^6 \times T_S$	# of signal samples per sensing
σ_{dB}	4.5 dB	Shadow fading dB-spread
D_{corr}	150 m	Decorrelation distance
Δ	20 m	Dimension of a grid
N_o	-95.2 dBm	Noise power
γ	-20 dB	Signal-to-noise ratio (SNR)
Q_{FA}	0.01	Target false-alarm probability
β	0.34	Attack detection threshold

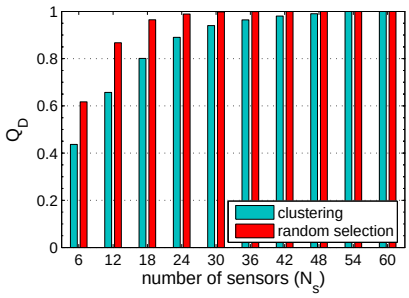


Fig. 6. *Effect of sensor clustering on incumbent detection performance*: Sensor clustering with $N_c = 5$ achieves 94 % of the detection performance without clustering, in a very low SNR environment, i.e., $\gamma = -20$ dB. Each cluster consists of 6 sensors and Q_{FA} is set to 0.01 in all scenarios.

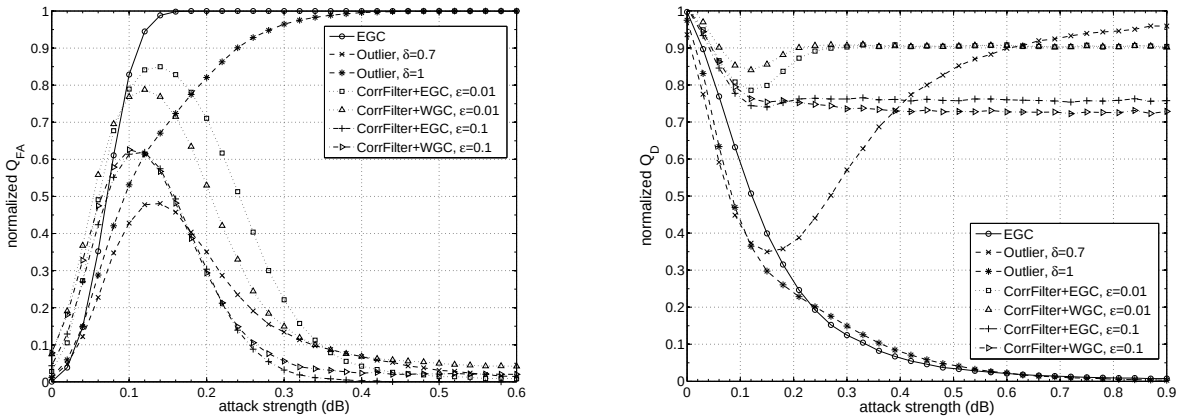
B. Effect of Sensor Clustering

While ADSP exploits shadowing correlation via sensor clustering, correlated sensor readings is, in general, known to degrade the detection performance as it limits diversity gain [8], [9], [18]. Therefore, we first study the effect of sensor clustering on detection performance to understand the efficiency vs. robustness tradeoff in ADSP. Fig. 6 compares the achieved incumbent detection probabilities (Q_D) with and without sensor clustering (i.e., random sensor selection). As expected, distributed sensing without clustering yields higher detection probability than with sensor clustering with -20 dB SNR. However, the performance gap decreases as more sensors are involved in distributed sensing, e.g., sensing with 5 clusters achieves 94 % of that without clustering. Note that this performance with clustering gets even closer to that of random selection as the SNR increases. Therefore, we can conclude that sensor clustering is not critical to incumbent detection, while it provides an efficient means of attack detection.

C. Attack-Tolerance

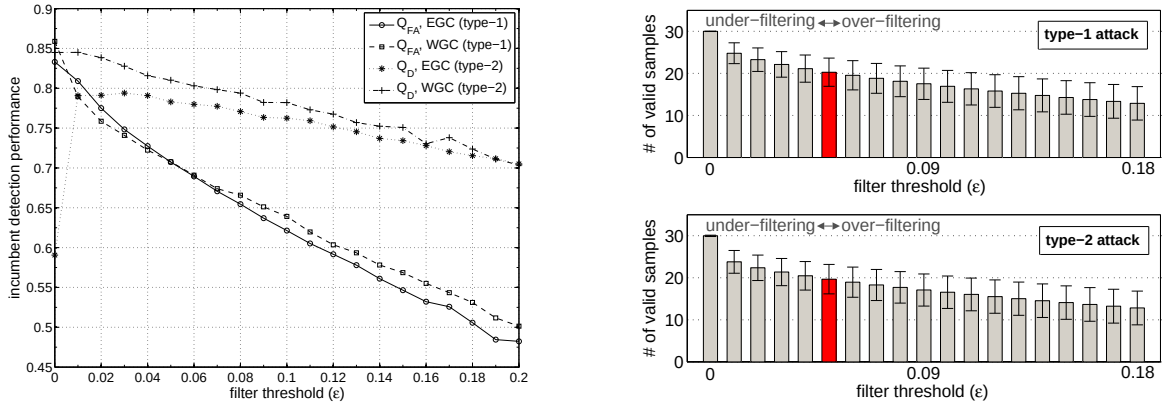
We now demonstrate the robustness of ADSP to both type-1 and type-2 attacks. Fig. 7 plots the normalized incumbent false-alarm (Q_{FA}) and detection (Q_D) probabilities under type-1 and type-2 attacks, respectively. The figure shows that the correlation filter is efficient in mitigating the effect of attacks on incumbent detection performance, e.g., 99.2 % for type-1 and 97.4 % for type-2 attacks, thanks to its ability to accurately filter out manipulated sensor reports. By contrast, without ADSP (denoted by EGC in Fig. 7), Q_{FA} and Q_D rapidly converge to 1 and 0, respectively, i.e., attacks have maximal influence on the data-fusion results.

We make the following four main observations. First, the performance of ADSP suffers in case of low strength attacks (e.g., < 0.4 dB for type-1 attack). This is because they do not exhibit deviations significant enough to be detected (thus causing *under-filtering*), yet they affect data-fusion decisions. The proposed weighted gain combining (WGC) mitigates this performance deficiency for both types of attacks by adaptively adjusting sensor reports' weights based on their statistical significance. However, WGC performs as well as, or even worse than, EGC when the attack strength is either (i) extremely low so that most of attacks will not be filtered out or (ii) large enough so that most (or all) of attacks are filtered out, as can be seen in Fig. 7 with $\epsilon = 0.01$. This is because, in the first case, the unfiltered attacks will adversely affect the weights



(a) Type-1 attack (b) Type-2 attack

Fig. 7. *Attack-tolerance of ADSP*: ADSP (a) minimizes the false-alarm probability by up to $99.2\,\%$ for type-1 attacks, and (b) achieves $97.4\,\%$ of maximum achievable detection probability (i.e., with 20 normal sensor reports in 5 clusters) for type-2 attacks.



(a) Incumbent detection performance (b) Number of valid sensor reports

Fig. 8. *Effect of threshold parameter (ϵ)*: (a) Q_{FA} and Q_D exhibit different behaviors under various ϵ values, and (b) the number of sensor reports to be used in the data fusion decreases as ϵ increases, under both type-1 (upper) and type-2 (lower) attacks.

of the legitimate sensor reports, while sharing large weights among themselves. On the other hand, in the second case, the legitimate sensor reports with extreme values are likely to be assigned small weights despite their critical role in accurate detection of incumbents.

Second, ADSP outperforms the statistics-based filtering method proposed in [20] (denoted by Outlier in Fig. 7). In Outlier, the fusion center filters out the sensor reports falls outside the range $[\,e_1 - \delta \cdot e_{iqr}, e_3 + \delta \cdot e_{iqr}\,]$ where e_1 and e_3 represent the first and third quartile of the samples, respectively, and $e_{iqr} = e_3 - e_1$ is the interquartile range (see Eq. (4) in [20]). This method does not require sensor clustering, and thus, one might think that it performs well when attack strength is strong enough to be easily detected as an outlier. However, the performance depends strongly on the filtering range, i.e., the choice of δ, the result of which varies with attack scenarios. For example, when $\delta = 0.7$, the performance suffers from over-filtering with a high attack mis-detection rate. On the other hand, when $\delta = 1$, the performance suffers from under-filtering, and as a results, Q_{FA} and Q_D converges to 1 and 0, respectively, even in case of high attack strengths. By contrast, ADSP accurately detects the manipulated sensing reports by considering shadowing correlation and its heavy-tailed distributions.

Third, even in case of high attack strengths, ADSP does not completely eliminate the effects of attacks for the following reasons. First, the fixed threshold parameter ϵ does not work optimally for all attack strengths, thus causing either over- or under-filtering, both of which degrade the detection performance. The over-filtering caused by a large threshold value (e.g., $\epsilon = 0.1$) turned out to lower both Q_{FA} and Q_D, as shown in Fig. 7. The impact of ϵ on incumbent detection performance will be detailed in Section VI-D. Second, as a result of filtering, the fusion center will have less samples to be used for data fusion. Since the data fusion is sensitive to the number of samples used, especially in very low SNR environments (as shown in Fig. 6), the incumbent detection performance degrades. For example, with 20 sensor reports remaining after filtering out all the 10 manipulated sensor reports, the average achievable Q_D is 0.88, which corresponds to the normalized Q_D of 0.93 in Fig. 7.

Fourth, in the absence of attacks, the correlation filter incurs a small increase in both Q_{FA} and Q_D. This is caused by the inaccuracy in the log-normal approximation of sensor reports, which causes over-filtering even in case of no attacks. We observed that this performance anomaly can be mitigated by

reducing the sensing duration T_S (e.g., <1 ms), which makes the approximation more accurate because the distribution of the sensing reports becomes closer to a normal distribution.

D. Tradeoff in Detection Threshold

Fig. 8 plots the impact of the filtering threshold ϵ on incumbent detection performance. In this simulation, we fixed the attack strength at 0.1 dB for both types of attacks. Fig. 8(a) shows that Q_{FA} monotonically decreases as ϵ increases for both fusion rules, implying that filtering out more sensor reports always helps lower the false-alarm rate of incumbents. For the same reason, however, a large ϵ degrades the detection probability Q_D. This can be explained by the heavy-tail of a log-normal distribution of shadow fading; filtering out high RSSs at the tail lowers the decision statistics significantly, thus reducing the chance of generating false-alarms (or detecting incumbents). Another observation is that WGC outperforms EGC in case of under-filtering, e.g., $\epsilon \in [0.01, 0.06]$, for type-1 attacks, as discussed in Section VI-C. For type-2 attacks, WGC also outperforms EGC, but the performance gain decreases as ϵ increases. Fig. 8(b) shows the average number of valid sensor reports (i.e., those that passed the filter) along with their standard deviations for both types of attacks. It clearly indicates that the filter becomes more aggressive in rejecting the sensor reports as ϵ increases, thus reducing the number of sensor reports to be used for making a final fusion decision. Therefore, the filter must be carefully designed to make the tradeoff between false-alarm and detection probabilities, while considering their dependency on attack strengths.

VII. Conclusion and Future Work

The design of reliable distributed sensing for opportunistic spectrum use is a major research challenge in DSA networks. To meet this challenge, we have developed a novel attack-tolerant distributed sensing protocol (ADSP) that selectively filters out abnormal sensor reports, and thus maintains the accuracy of incumbent detection. The key idea behind this mechanism is that the measured primary signal strength at nearby sensors should be correlated due to shadow fading, which had not been considered before. To realize this idea, we proposed a sensor clustering method and designed filters and data-fusion rules based on the correlation analysis of the sensor reports. ADSP can readily be implemented in 802.22 WRANs, incurring very low processing and communication overheads. Our proposed scheme is evaluated in realistic shadowing environments, demonstrating its ability to tolerate both type-1 and type-2 attacks.

Acknowledgement

The work reported in this paper was supported in part by the NSF under grants CNS-0519498 and CNS-0721529.

References

[1] 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.

[2] S. Shellhammer and R. Tandra, "An Evaluation of DTV Pilot Power Detection," IEEE 802.22-06/0188r0, Sep 2006.

[3] A. W. Min and K. G. Shin, "Exploiting Multi-Channel Diversity in Spectrum-Agile Networks," in *Proc. IEEE INFOCOM '08*, April 2008.

[4] T. Shu and M. Krunz, "Throughput-efficient Sequential Channel Sensing and Probing in Cognitive Radio Networks Under Sensing Errors," in *Proc. ACM MobiCom '09*, Sep 2009.

[5] A. W. Min and K. G. Shin, "An Optimal Sensing Framework Based on Spatial RSS-profile in Cognitive Radio Networks," in *Proc. IEEE SECON '09*, June 2009.

[6] ——, "Impact of Mobility on Spectrum Sensing in Cognitive Radio Networks," in *Proc. ACM CoRoNet '09*, Sep 2009.

[7] 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*, vol. 7, pp. 1326–1337, April 2008.

[8] A. Ghasemi and E. S. Sousa, "Collaborative Spectrum Sensing for Opportunistic Access in Fading Environments," in *Proc. IEEE DySPAN '05*, Nov 2005.

[9] S. M. Mishra, A. Sahai, and R. W. Brodersen, "Cooperative Sensing among Cognitive Radios," in *Proc. IEEE ICC '06*, June 2006.

[10] 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*, vol. 26, no. 1, pp. 25–37, Jan 2008.

[11] S. Anand, 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.

[12] R. Chen, J.-M. Park, and K. Bian, "Robust Distributed Spectrum Sensing in Cognitive Radio Networks," in *Proc. IEEE INFOCOM '08*, April 2008.

[13] 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*, vol. 1, no. 1, pp. 38–47, April 2006.

[14] W. Rose, "Enhanced Protection for Low Power Licensed devices Operating in TV Broadcast Bands," IEEE 802.22-06/0073r2, May 2006.

[15] USRP: Universal Software Radio Peripheral. [Online]. Available: http://www.ettus.com

[16] K. Tan et al., "Sora: High Performance Software Radio Using General Purpose Multi-core Processors," in *Proc. USENIX NSDI '09*, April 2009.

[17] W. Xu, P. Kamat, and W. Trappe, "TRIESTE: A Trusted Radio Infrastructure for Enforcing SpecTrum Etiquettes," in *Proc. Allerton '06*, Sep 2008.

[18] A. Ghasemi and E. S. Sousa, "Asymptotic Performance of Collaborative Spectrum Sensing under Correlated Log-Normal Shadowing," *IEEE Communications Letters*, vol. 11, no. 1, pp. 34–36, Jan 2007.

[19] A. Mody et al., "Collaborative Sensing for Security," IEEE 802.22-08/0301r011, Dec 2008.

[20] P. Kaligineedi, M. Khabbazian, and V. K. Bharava, "Secure Cooperative Sensing Techniques for Cognitive Radio Systems," in *Proc. IEEE ICC '08*, May 2008.

[21] K. A. Woyach, A. Sahai, G. Atia, and V. Saligrama, "Crime and Punishment for Cognitive Radios," in *Proc. Allerton '08*, Sep 2008.

[22] S. Liu, Y. Chen, W. Trappe, and L. J. Greenstein, "ALDO: An Anomaly Detection Framework for Dynamic Sptectrum Access Networks," in *Proc. IEEE INFOCOM '09*, April 2009.

[23] FCC, "Notice of Proposed Rulemaking and Order," FCC 08-188, Aug 2008.

[24] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.

[25] F. F. Digham, M.-S. Alouini, and M. K. Simon, "On the Energy Detection of Unknown Signals over Fading Channels," in *Proc. IEEE ICC '03*, May 2003.

[26] A. Taherpour, Y. Norouzi, M. Masiri-Kenari, A. Jamshidi, and Z. Zeinalpour-Yazdi, "Asymptotically optimum detection of primary user in cognitive radio networks," *IET Communications*, vol. 1, no. 6, pp. 1138–1145, Dec 2007.

[27] M. Gudmundson, "A correlation model for shadow fading in mobile radio," *Electronic Letters*, vol. 27, no. 23, pp. 2146–2147, Nov 1991.

[28] T. Muetze, P. Stuedi, F. Kuhn, and G. Alonso, "Understanding Radio Irregularity in Wireless Networks," in *Proc. IEEE SECON '08*, June 2008.

[29] N. Patwari and P. Agrawal, "Effects of Correlated Shadowing: Connectivity, Localization, and RF Tomography," in *Proc. IEEE IPSN '08*, April 2008.

[30] J. Riihijärvi, P. Mähönen, M. Wellens, and M. Gordziel, "Characterization and Modelling of Spectrum for Dynamic Spectrum Access with Spatial Statistics and Random Fields," in *Proc. IEEE PIMRC '08*, Sep 2008.

[31] I. Forkel, M. Schinnenburg, and M. Ang, "Generation of Two-Dimensional Correlated Shadowing for Mobile Radio Network Simulation," in *Proc. WPMC*, Sep 2004.

[32] 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*, vol. 20, no. 3, pp. 523–531, April 2002.

[33] Y. Chen, W. Trappe, and R. P. Martin, "Attack Detection in Wireless Localization," in *Proc. IEEE INFOCOM '07*, May 2007.