Secure Cooperative Spectrum Sensing in Cognitive Radio Networks Using Interference Signatures

Seunghyun Choi and Kang G. Shin
Department of Electrical Engineering and Computer Science
The University of Michigan, Ann Arbor, MI 48109-2121
Email: {shkchoi, kgshin}@eecs.umich.edu

***Abstract*—Cooperative spectrum sensing has received considerable attention as a viable means to enhance the detection performance by exploiting spatial diversity in received signal strengths. However, this is vulnerable to sensing data falsification attacks due to the distributed nature of cooperative spectrum sensing. To overcome this problem, we introduce a *primary user emulation test* (PUET), under which a trustful central entity (e.g., a cellular base station) transmits a test signal while other users are sensing the spectrum. The core of PUET is to correlate the reported sensing data with the transmission power of the test signal. Since this test signal is, in reality, an interference to the sensing of a primary signal, sensors cannot distinguish the test signal from the primary signal. Considering this characteristic of sensors, PUET detects attacks by evaluating the consistency of channel parameters, which are not known to sensors. By recognizing this defense mechanism, PUET checks the validity of reports from each sensor separately. The efficacy of PUET is validated via experimentation on a testbed deployed in an indoor environment. Our measurement study shows that PUET achieves over 95% detection rate while keeping the false alarm rate under 5%.**

I. Introduction

Spectrum scarcity has recently become an important problem in the field of wireless communications since the demand for wireless spectrum has been increasing exponentially with the proliferation of new mobile users and wireless services [1], while the amount of the total wireless spectrum remains fixed or is increasing slowly. According to a report of the US Federal Communications Commission (FCC) [2], wireless communications services/applications are expected to experience spectrum shortage starting from 2013. However, researchers have also discovered that spectrum is severely under-utilized [3], [4] due mainly to the current *static* spectrum allocation policy, thus calling for more efficient and flexible spectrum access strategies/policies.

In order to utilize the wireless spectrum more flexibly, cognitive radio networks (CRNs) were introduced [5], in which unlicensed secondary users (SUs) opportunistically reuse spectrum bands licensed by primary users (PUs). Since PUs have right to use the spectrum at *any time*, SUs must discover spectrum holes in time, frequency, and space domains and can access the spectrum only when PUs are not using the spectrum in order not to interfere with PUs' communications. There have been numerous approaches proposed to protect PUs' communications, such as PU signal detection (spectrum sensing) [6], [7], auxiliary beacon detection [8], and geo-location database of PUs [9]. In particular, spectrum sensing has received significant attention for its simple design and adaptability as it does not require any prior knowledge of the PU's signal or networks [10]. SUs sense the channel and determine the presence of a PU signal by testing measured received signal strengths (RSSs). To enhance this detection performance, researchers have introduced temporal and spatial diversities by exploiting sensing scheduling (scheduling sensing multiple times) [11] and cooperative spectrum sensing (sharing sensing information among SUs) [12], [13], [14], respectively.

Cooperative spectrum sensing, however, is vulnerable to sensing data falsification attacks [15], [16], due to the distributed nature of spectrum sensing in CRNs. As the goal of a sensing data falsification attack is to cause an incorrect decision on the presence/absence of a PU signal, malicious or compromised SUs may intentionally distort the measured RSSs and share them with other SUs. Then, the effect of erroneous sensing results propagates to the entire CRN. This type of attacks can be easily launched since the openness of programmable software-defined radio (SDR) devices makes it easy for (malicious or compromised) SUs to access low-layer protocol stacks, such as PHY and MAC [17]. However, detecting such attacks is challenging due to the lack of coordination between PUs and SUs, and unpredictability in wireless channel signal propagation, thus calling for efficient mechanisms to protect CRNs.

In this paper, we propose a mechanism, called PUET, to detect the falsification of sensing results. PUET resides at a trustful central entity (e.g., a cellular base station) that transmits a test signal while other SUs are sensing the spectrum. Since this test signal is, in reality, an interference to the sensing of a PU signal, SUs' RSSs should be the sum power of the PU signal and the test signal. Then, the central entity can detect attacks by checking if the reported sensing data reflects the interference caused by the test signals.

The rest of this paper is organized as follows. Section 2 discusses existing approaches against sensing falsification attacks, differentiating PUET from them. Section 3 describes the network under consideration and the sensing models with various attack scenarios. Then, Section 4 presents the design rationale and the abstract framework of PUET. Section 5 details our attack-detection mechanism with sequential tests and channel parameter estimation. Section 6 evaluates PUET's performance via experiments on a testbed, and Section 7 concludes the paper.

II. Related Work

In order to entice SUs to follow the protocol, i.e., reporting the sensing results honestly, researchers used game-theoretic approaches to analyze SUs' behavior. Duan *et al.* [18] proposed attack prevention mechanisms with direct and indirect punishments. Assuming that SUs care for their rewards, their scheme prevents SUs from reporting falsified sensing data by setting appropriate reward and punishment functions. Woyach *et al.* [19] developed a model for the incentives associated with attacks and for the tradeoffs between the different elements of an enforcement structure.

To detect discrepancies among sensing data and ensure robust decisions in cooperative spectrum sensing, researchers have studied robust data-fusion in CRNs. Kaligineedi *et al.* [20] introduced a trust factor which gives a measure of reliability of each SU. By applying an outlier detection method, their data-fusion scheme assigns a lower trust factor to a SU whose sensing report is extremely high or low, reducing its effect on the sensing decision. Chen *et al.* [15] presented a weighted sequential probability ratio test which introduces a reputation-based mechanism to the sequential probability ratio test (SPRT). By increasing the reputation of a SU whose sensing report is consistent with the majority at each step, their scheme dynamically adjusts the weight of each SU so that a SU with higher reputation can have more influence on the sensing decision. Min *et al.* [16] proposed a correlation filter for the detection of abnormal sensing reports by exploiting the shadow fading correlation in RSSs. Assuming that RSSs at nearby SUs are correlated, they proposed a clustering method and data-fusion rules based on the correlation analysis of sensing reports.

These defense schemes, however, have their own limitations in that their assumptions may not hold. Game-theoretic attack prevention assumes that SUs try to maximize their utilities by following the protocol. However, considering that attackers outside of a network can compromise SUs inside of the network, these schemes may not work well if these attackers do not care about compromised SUs' utilities. Robust data-fusion schemes compare sensing data among SUs assuming that the number of honest SUs are much larger than that of malicious/compromised SUs which mount sensing data falsification attacks. Obviously, robust fusion schemes may not be suitable for detecting attacks when the number of honest SUs becomes small. Noting that this number can easily be reversed in a network of a small number of SUs, CRNs are required to be capable of detecting attacks even when the number of honest SUs is small.

III. System Models

A. Network Model

There are two different types of users, PUs and SUs [5]. PUs are legacy users who have the license to use the spectrum band, whereas SUs do not have license and use the spectrum only when PUs are not using it, i.e., PUs always have priority over SUs in accessing the spectrum. Thus, SUs should be equipped with a *cognition* engine which will discover spectrum holes/opportunities. In this setting, a cognitive radio network (CRN) is a network of SUs.

We assume that there exists a single stationary PU transmitter in the area of interest. Typical examples are TV base stations and frequency division duplex (FDD) based cellular base stations. The single PU assumption is reasonable because such base stations are preplanned and their locations determined *a priori* in the cell-planning stage. The PU's activities are modeled as a two-state Markov process with ON and OFF states [21], [22], [23]. ON and OFF states represent the phases/durations in which the PU is active and inactive, respectively. When the PU is in ON state, it transmits signals with fixed transmission power $P_{PU,ON}$, while it does not transmit any signal in OFF state:

$$P_{PU} = \begin{cases} P_{PU,ON} & \text{the PU is active} \\ 0 & \text{the PU is inactive.} \end{cases} \tag{1}$$

The sojourn time in ON/OFF state is assumed, as in [24], to be exponentially distributed with means $1/\mu_{ON}$ and $1/\mu_{OFF}$, respectively.

The CRN under consideration is overlaid on the current infrastructure-based cellular system. It consists of a single base station (BS) and a set of end-users, called *consumer premise equipments* (CPEs), which are associated with the BS. Thus, one-hop wireless links can be established between the BS and CPEs. Based on the current cellular system, we assume both the BS and CPEs are stationary. We will initially consider a single-cell CRN and will later cover a multi-cell CRN.

It is important to note that the PU is unaware of the CRN's existence. That is, the PU doesn't care about the CRN's existence or operation since the PU has the license of, and hence the right to use, the spectrum at any time. Consequently, we assume there is no coordination between the PU and the CRN. For spectrum sharing in a more general setting than the digital TV band (i.e., 802.22), we will assume a CRN's reliance on spectrum sensing for its operation, instead of relying solely on geo-location databases of the PU' activities. Note that assuming no coordination between the PU and the CRN will yield more general and realistic solutions.

In order for the CRN to opportunistically exploit a channel licensed by the PU, the BS schedules the sensing of the channel during *quiet periods* (QPs), i.e., when SUs do not transmit data. We assume that the length of a QP is short enough, compared to the BS's ON/OFF sojourn time, such that no ON/OFF transition happens in the middle of a QP. During a QP, all CRN nodes are not allowed to transmit any signal while letting CPEs sense the channel. The CPEs report their sensing results to the BS immediately after each QP. Based on these sensing reports, the BS decides on the presence/absence of PU signals and announces the decision to CPEs whether or not to use the channel. In our model, the CRN considers only a single spectrum band or channel. Therefore, when there is a PU signal in the channel, the CRN's data communication must wait until the channel becomes idle. Fig. 1 shows the information flows of cooperative spectrum sensing in a CRN.

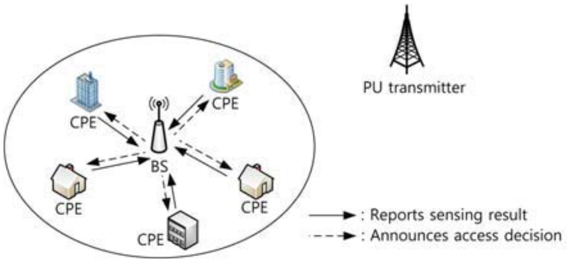

Fig. 1. Information flows of cooperative spectrum-sensing.

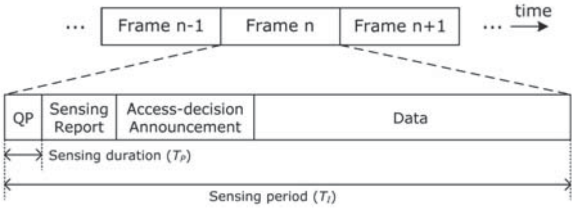

Fig. 2. The frame structure in the CRN.

B. Sensing Model

Fig. 2 shows the structure of frames in the CRN, which are scheduled by the BS for transmission. Each frame consists of QP, sensing report slot, access-decision announcement slot, and data transmission slot for uplink (UL) and downlink (DL). The sensing results acquired by CPEs within a QP (or distortions thereof) will be reported to the BS during the subsequent sensing report slot. Based on these reports, the BS makes a decision on the presence/absence of a PU signal and then transmits it as 1-bit information in an access-decision announcement slot. Data communications among the CRN nodes take place in the data transmission slot. The idea of allocating sensing report and access-decision announcement slots after every QP is widely adopted in CRNs [18]. To reduce SUs' potential interference to the PU, we assume that the CRN uses spread-spectrum for sensing reports and access-decision announcements as in [25].

In each QP, all the CPEs sense the channel and each collects M RSS samples via energy sensing. Energy sensing has the advantage of simple design and fast response [24]. Energy sensing typically takes less than 1ms, whereas feature sensing/detection takes much longer (e.g., 24.2ms for the field sync detector [26]).

We use a widely adopted signal propagation model in which the signal strength at a receiver at time t, $P_r(t)$, is expressed as [27]:

$$P_r(t) = g(t)P_t(t), \tag{2}$$

where $P_t(t)$ is the transmitted signal strength at time t and $g(t)$ the channel gain at time t between the transmitter and the receiver. The channel gain is assumed to follow a random distribution (e.g., Rayleigh or Rician distribution) with a probability density function (p.d.f.) $f(\mu_g, \sigma_g^2)$ when the transmitter and the receiver are stationery. Then, the distribution of a single RSS sample at CPE i, S_i, can be expressed as

$$S_i \sim \begin{cases} f\left(N_i, N_i^2\right) & \mathcal{H}_0 \text{ (no primary signal)} \\ f\left(R_{PU,i} + N_i, R_{PU,i}^2 + N_i^2\right) & \mathcal{H}_1 \text{ (a primary signal exists),} \end{cases} \tag{3}$$

where N_i is the average noise power at CPE i and $R_{PU,i}$ the average received primary signal strength at CPE i when the PU is active [16], [28]. $R_{PU,i}$ is the product of $g_{PU,i}$ and $P_{PU,ON}$, where $g_{PU,i}$ is the average channel gain between the PU and CPE i. Note that we use N_i, instead of the thermal noise power N_o, since each CPE has its own noise figure. Noise power at each CPE is assumed to be wide-sense stationary (WSS). The CRN is assumed to use a wide band (e.g., over 5MHz) so that the effect of multipath fading becomes negligible for frequency diversity [28], [29].

When CPE i reports its sensing results, it sends a test statistic R_i, not raw RSS samples. The test statistic is the average of M RSS samples. Assuming that M is large enough, we can apply the Central Limit Theorem (CLT) as in [30] so that R_i may follow a Gaussian distribution:

$$R_i \sim \begin{cases} \mathcal{N}\left(N_i, \frac{N_i^2}{M}\right) & \mathcal{H}_0 \\ \mathcal{N}\left(R_{PU,i} + N_i, \frac{R_{PU,i}^2 + N_i^2}{M}\right) & \mathcal{H}_1. \end{cases} \tag{4}$$

When the channel bandwidth is greater than 5MHz and the length of a QP is 1ms, M becomes greater than 5×10^3 with the Nyquist sample rate, which is large enough to make the CLT applicable [16].

C. Attack Model

A sensing data falsification attack makes cooperative spectrum sensing ineffective by reporting distorted sensing results to the BS [15], [16]. The objective of an attack is to mislead the BS to making wrong access-decisions, i.e., making the BS believe that there is no PU signal when there is a PU signal or making the BS believe that there is a PU signal although there is no PU signal. Therefore, the *success* of an attack refers to reaching a state in which the BS makes a wrong access-decision as a result of the attack.

Before describing attacks to be considered, we first clarify terms "*faulty report*" and "*faulty CPE*." A faulty report from a CPE contains a sensing test statistic distorted from the actual sensing results. Even when the distortion is unintended (e.g., because the CPE is malfunctioning), we regard the report as faulty since the reported result may degrade the sensing performance. We use the term "faulty CPE" to indicate a CPE which may generate one or more faulty reports. Malicious, compromised, or malfunctioning CPEs are all faulty CPEs. A faulty CPE sometimes reports correct sensing results and at other times reports distorted/fabricated sensing results.

Based on the above definition, an attacker is defined as a faulty CPE that generates a distorted/fabricated report. We also consider malfunctioning CPEs that make erroneous sensing reports. Obviously, malfunctioning CPEs are not affected by "utilities" defined in game-theoretic attack prevention schemes [18], [19]. We assume that attackers have the same

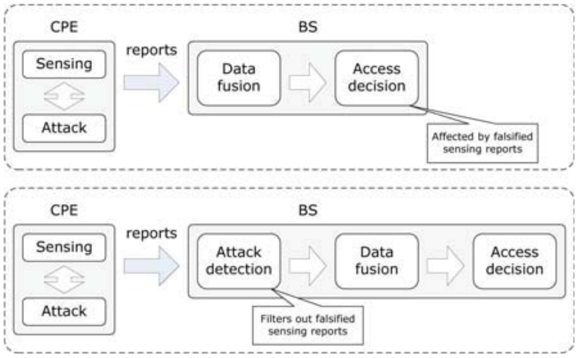

Fig. 3. The impact of the sensing data falsification attack on BSs with and without an attack detector.

capability as honest CPEs except they determine the presence/absence of a PU signal before the BS's announcement, and they can falsify their sensing results.

An attack is defined as an act of making a faulty report. Attacks disrupt the BS's decision in two different ways. When a faulty CPE balloons the test statistic in its report, the BS will incorrectly conclude that there is a PU signal in the channel even though there is not, thus increasing the false-positive rate. When a faulty CPE intentionally lowers the test statistic in its report, the BS will incorrectly conclude that there is no PU signal in the channel even though there is, thus increasing the false-negative rate. Thus, the sensing report of CPE i in the presence of attacks can be expressed as

$$\bar{R}_i \sim \begin{cases} \mathcal{N}(N_i + D_i, \frac{{N_i}^2}{M}) & \mathcal{H}_0 \\ \mathcal{N}(R_{PU,i} + N_i + D_i, \frac{R_{PU,i}^2 + N_i^2}{M}) & \mathcal{H}_1, \end{cases} \tag{5}$$

where D_i is the amount of deviation from the actual test statistic of the energy detector. We call D_i the *attack strength*. Attackers can change D_i in each QP. We can also regard a report with $D_i = 0$ (accordingly, $\bar{R}_i = R_i$) as a special case when there is no sensing data falsification attack.

When distorted sensing results are reported to the BS, the probability of the BS making a wrong decision increases. The impact of the sensing data falsification attack on the access-decision (with and without an attack detection module) is depicted in Fig. 3. In this paper, our defense mechanism verifies the integrity of reports, rather than verifying that of reporting CPEs. That is, it detects faulty reports, not faulty CPEs. As long as a CPE's report is an honest one, the sensing function of the CPE is considered normally operating even if the CPE was faulty. Therefore, the BS utilizes the report (as genuine) for its access-decision.

IV. The Proposed Approach

A. Nature of CPEs

Before developing a response to the sensing data falsification attack, let's look closely at the nature of cooperative spectrum sensing with CPEs. Recall that each CPE performs spectrum sensing with energy detection during a QP and reports the sensing result to the BS immediately after the QP. Since CPEs communicate via the BS and the deadline of sensing reports is relatively tight, we can assume CPEs are independent during a time span of spectrum sensing and reporting. That is, from the beginning of a QP to the end of the following report, no information is exchanged among CPEs. Therefore, malicious CPEs cannot cooperate during this time span unless they have a side channel. Since a CPE cannot decode the PU signal, it can only get the energy information, not the source of the signal when sensing the channel. Therefore, without cooperation from the BS or other CPEs, a CPE alone cannot verify that the sensed signal was indeed from the PU.

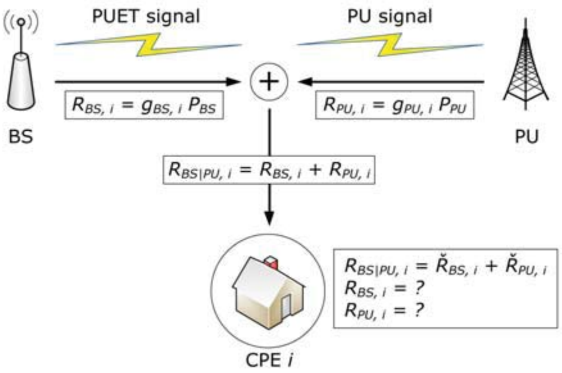
PUET signal
PU signal
BS
PU
$R_{BS,i} = g_{BS,i} P_{BS}$
$R_{PU,i} = g_{PU,i} P_{PU}$
$R_{BS|PU,i} = R_{BS,i} + R_{PU,i}$
$R_{BS|PU,i} = \check{R}_{BS,i} + \check{R}_{PU,i}$
$R_{BS,i} = ?$
$R_{PU,i} = ?$
CPE i

Fig. 4. Spectrum sensing from a CPE's perspective: test statistic measured at the CPE is the sum of signals from the PU and the BS. Note that the CPE does not know each signal separately.

Considering these characteristics of CPEs, we propose PUET that detects faulty reports by evaluating the sensing reports. The design rationale behind PUET is that the BS can acquire as much information of R_i as possible by contributing to the value of R_i. Specifically, the BS transmits *PUET signals* during every QP. PUET signals are noise-like and with certain strengths. Since the BS knows the transmission power of its previous PUET signals, it will expect that the sensing reports from CPEs should have a certain level of correlation with PUET signals.

In the presence of the PUET signal, the received signal during a QP at a CPE is the sum of signals from the PU and the BS. Thus, the RSS measured at the CPE is the sum of signal strengths received from the PU and the BS. However, since the CPE cannot distinguish signals from the PU and those from the BS, it cannot infer the portion of the RSS contributed by the PU or the BS. Fig. 4 illustrates the nature of spectrum sensing from a CPE's perspective when there is a PUET signal in the channel.

A test signal may sometimes interfere with PUs' communications. However, since the sensing result should be reported over the wireless channel, interference to the PU is unavoidable. That is, a certain degree of PU interference is inevitable when applying cooperative spectrum sensing. We can reduce the amount of interference by limiting the PUET signal power.

B. Problem Statement

The main objective of PUET is to detect sensing data falsification attacks with a high probability, thus reducing

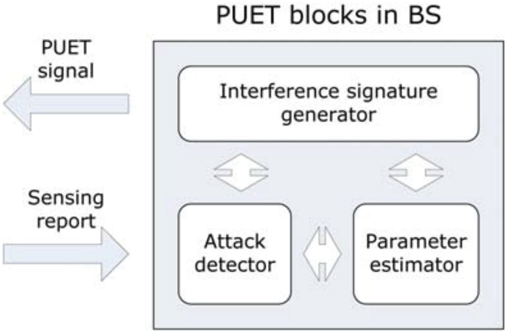

Fig. 5. PUET's building blocks residing in the BS.

both false-positive and false-negative rates. As shown in the previous section, our scheme detects faulty reports, not faulty CPEs. This is reasonable since the direct cause of a wrong access-decision is a faulty report itself.

The BS is the one who is responsible for detecting attacks. In order to detect attacks, the BS controls the power of PUET signal in each QP. The transmission power should be carefully selected so that CPEs cannot determine the received primary signal strengths. Our problem is stated as follows.

Objective:

Maximize the attack detection probability.

Condition/constraints:

CPEs cannot determine the received primary signal strengths.

The attack false-alarm probability is under a limit.

Control parameter:

PUET signal power in each QP.

C. PUET Framework

PUET consists of the following three building blocks:

- **Interference signature generator:** determines the transmission power of the PUET signal in each QP.
- **Parameter estimator:** estimates parameters of RSS including the average channel gains between the BS and CPEs $g_{BS,i}$ and received PU signal strength $R^i_{PU,ON}$ for all i.
- **Attack detector:** detects and filters out abnormal sensing reports based on the correlation between the reported data and the interference signature.

These three components closely interact with one another and form our secure sensing system. Fig. 5 shows the PUET building blocks at the BS interacting with each other. Note that PUET tests the validity of sensing reports from each CPE separately. That is, the sensing reports from other CPEs do not affect checking of the validity of a CPE's sensing report. Therefore, PUET works robustly even when the number of faulty CPEs is much larger than the number of honest CPEs.

V. Detection of Falsified Sensing Reports via PUET

A. Sequential Testing of Sensing Reports

We first study the basic structure of sequential testing which detects the presence of non-zero attack strength D_i. Let's consider a temporally-ordered sequence of QPs. Then, the actual test statistic $R_i[n]$ of CPE i at QP n and its reported value, $\bar{R}_i[n]$, can be expressed as

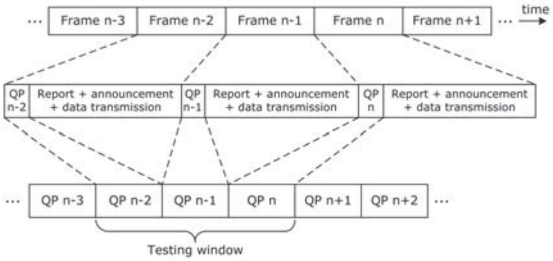
Frame n-3
Frame n-2
Frame n-1
Frame n
Frame n+1
time
QP n-2
Report + announcement + data transmission
QP n-1
Report + announcement + data transmission
QP n
Report + announcement + data transmission
QP n-3
QP n-2
QP n-1
QP n
QP n+1
QP n+2
Testing window

Fig. 6. A representation of QPs and testing window in the time domain.

$$\begin{aligned} R_i[n] &\sim \mathcal{N}(R_{BS,i}[n] + R_{PU,i}[n] + N_i, \\ &\qquad \frac{R^2_{BS,i}[n] + R^2_{PU,i}[n] + N_i^2}{M}) \\ &\sim \mathcal{N}(g_{BS,i}P_{BS}[n] + R_{PU,i}[n] + N_i, \\ &\qquad \frac{(g_{BS,i}P_{BS}[n])^2 + R^2_{PU,i}[n] + N_i^2}{M}) \\ &\sim \mathcal{N}\left(g_{BS,i}P_{BS}[n] + R_{PU,i}[n] + N_i, \sigma_i^2[n]\right) \end{aligned} \tag{6}$$

$$\begin{aligned} \bar{R}_i[n] &\sim \mathcal{N}(g_{BS,i}P_{BS}[n] + R_{PU,i}[n] + N_i + D_i[n], \\ &\qquad \frac{(g_{BS,i}P_{BS}[n])^2 + R^2_{PU,i}[n] + N_i^2}{M}) \\ &\sim \mathcal{N}\left(g_{BS,i}P_{BS}[n] + R_{PU,i}[n] + N_i + D_i[n], \sigma_i^2[n]\right) \end{aligned} \tag{7}$$

$$R_{PU,i}[n] = \begin{cases} 0 & \mathcal{H}_0 \text{ at } n \\ R^i_{PU,ON} & \mathcal{H}_1 \text{ at } n, \end{cases} \tag{8}$$

assuming that CPE i adds the attack strength $D_i[n]$ at QP n. $R_{BS,i}[n]$ is the received PUET signal strength at CPE i, $P_{BS}[n]$ the transmission power of PUET signal, and $g_{BS,i}$ the average channel gain between the BS and CPE i. Again, we assume that the multipath fading effect becomes negligible in a wide-band energy detector.

The BS transmits test signals over three consecutive QPs, QP$_{n-2}$, QP$_{n-1}$, and QP$_n$, as illustrated in Fig. 6. We call this span of time a *testing window*. The length of a testing window does not need to be 3, but we use 3 QPs for testing since it represents the simplest case, i.e., at least 3 QPs are required for the test. Upon receiving a sensing report from the CPE at QP$_n$, the BS sets the testing window to [QP$_{n-2}$, QP$_n$]. At QP$_{n+1}$, the moving testing window is likewise set to [QP$_{n-1}$, QP$_{n+1}$]. The BS transmits the PUET signal with a random amount of power at every QP. Let the BS transmit the PUET signal with power $P_{BS}[n-2]$, $P_{BS}[n-1]$, and $P_{BS}[n]$ at QP$_{n-2}$, QP$_{n-1}$, and QP$_n$, respectively. Then, the actual test statistic values and CPE i's reported values at QP$_{n-2}$, QP$_{n-1}$, and QP$_n$ will be:

$$\begin{aligned} R_i[n-2] &\sim \mathcal{N}\left(g_{BS,i}P_{BS}[n-2] + R_{PU,i}[n-2] + N_i,\right. \\ &\qquad \left.\sigma_i^2[n-2]\right) \\ R_i[n-1] &\sim \mathcal{N}\left(g_{BS,i}P_{BS}[n-1] + R_{PU,i}[n-1] + N_i,\right. \\ &\qquad \left.\sigma_i^2[n-1]\right) \\ R_i[n] &\sim \mathcal{N}\left(g_{BS,i}P_{BS}[n] + R_{PU,i}[n] + N_i,\right. \\ &\qquad \left.\sigma_i^2[n]\right) \end{aligned} \tag{9}$$

$$\begin{aligned}\bar{R}_i[n-2] &\sim \mathcal{N}\left(g_{BS,i}P_{BS}[n-2] + R_{PU,i}[n-2] + N_i \right.\\ &\qquad \left. +D_i[n-2], \sigma_i^2[n-2]\right)\\ \bar{R}_i[n-1] &\sim \mathcal{N}\left(g_{BS,i}P_{BS}[n-1] + R_{PU,i}[n-1] + N_i \right.\\ &\qquad \left. +D_i[n-1], \sigma_i^2[n-1]\right)\\ \bar{R}_i[n] &\sim \mathcal{N}\left(g_{BS,i}P_{BS}[n] + R_{PU,i}[n] + N_i \right.\\ &\qquad \left. +D_i[n], \sigma_i^2[n]\right). \end{aligned} \tag{10}$$

B. Estimation of Parameters

In order for the BS to detect attacks, it first needs to estimate the test statistic parameters including $g_{BS,i}$ and $R^i_{PU,ON}$. Then, by using the thus-estimated parameters, the BS decides on the presence of non-zero D_i.

Let's look at the actual test statistic values derived in (9). Note that the average channel gain $g_{BS,i}$ is used in all three distributions. Since test statistic values in a testing window are assumed independent of each other, we can derive:

$$\begin{aligned}\dot{g}_{BS,i}[n-1] \equiv& \frac{R_i[n-1]-R_i[n-2]}{P_{BS}[n-1]-P_{BS}[n-2]}\\ &\sim \mathcal{N}\left(g_{BS,i} + \frac{R_{PU,i}[n-1]-R_{PU,i}[n-2]}{P_{BS}[n-1]-P_{BS}[n-2]},\right.\\ &\qquad \left.\frac{\sigma_i^2[n-1]+\sigma_i^2[n-2]}{(P_{BS}[n-1]-P_{BS}[n-2])^2}\right)\end{aligned} \tag{11}$$

$$\begin{aligned}\dot{g}_{BS,i}[n] \equiv& \frac{R_i[n]-R_i[n-1]}{P_{BS}[n]-P_{BS}[n-1]}\\ &\sim \mathcal{N}\left(g_{BS,i} + \frac{R_{PU,i}[n]-R_{PU,i}[n-1]}{P_{BS}[n]-P_{BS}[n-1]},\right.\\ &\qquad \left.\frac{\sigma_i^2[n]+\sigma_i^2[n-1]}{(P_{BS}[n]-P_{BS}[n-1])^2}\right).\end{aligned} \tag{12}$$

Again, the average term of each distribution is in the form of $g_{BS,i} + \frac{R_{PU,i}[k]-R_{PU,i}[k-1]}{P_{BS}[k]-P_{BS}[k-1]}, k \in \{n, n-1\}$. Since $g_{BS,i}$ is fixed, the average of the distribution varies as $P_{BS}[k]$ and $R_{PU,i}[k]$ change. When $R_{PU,i}[k] = R_{PU,i}[k-1]$, the average term becomes $g_{BS,i}$. However, the BS does not have any information of $R_{PU,i}[k]$ at this step, although it has the information of $P_{BS}[k]$. So there is no guarantee that the average term will become $g_{BS,i}$. Instead, we derive

$$\begin{aligned}&\ddot{g}_{BS,i}[n] \equiv \dot{g}_{BS,i}[n] - \dot{g}_{BS,i}[n-1]\\ &\sim \mathcal{N}\left(\frac{R_{PU,i}[n]-R_{PU,i}[n-1]}{P_{BS}[n]-P_{BS}[n-1]} - \frac{R_{PU,i}[n-1]-R_{PU,i}[n-2]}{P_{BS}[n-1]-P_{BS}[n-2]},\right.\\ &\sigma_i^2[n]\left(\frac{1}{P_{BS}[n]-P_{BS}[n-1]}\right)^2\\ &\quad +\sigma_i^2[n-1]\left(\frac{1}{P_{BS}[n]-P_{BS}[n-1]}+\frac{1}{P_{BS}[n-1]-P_{BS}[n-2]}\right)^2\\ &\quad \left.+\sigma_i^2[n-2]\left(\frac{1}{P_{BS}[n-1]-P_{BS}[n-2]}\right)^2\right)\\ &\sim \mathcal{N}\left(\ddot{\mu}_i[n], \ddot{\sigma}_i^2[n]\right).\end{aligned} \tag{13}$$

Note that $\sigma_i^2[n]$ decreases as the number of signal samples M increases from (6). Thus, $\ddot{\sigma}_i^2[n]$ can be reduced significantly by increasing M. For example, when the channel bandwidth is greater than 5MHz, M becomes over 5×10^3 if CPEs sense the channel at the Nyquist rate for 1ms.

TABLE I
8 POSSIBLE CASES OF THE PU ACTIVITY AND THE CORRESPONDING $\ddot{\mu}_i[n]$ VALUE IN THE TESTING WINDOW.

Case	$R_{PU,i}[n-2]$	$R_{PU,i}[n-1]$	$R_{PU,i}[n]$
0	0	0	0
1	0	0	$R^i_{PU,ON}$
2	0	$R^i_{PU,ON}$	0
3	0	$R^i_{PU,ON}$	$R^i_{PU,ON}$
4	$R^i_{PU,ON}$	0	0
5	$R^i_{PU,ON}$	0	$R^i_{PU,ON}$
6	$R^i_{PU,ON}$	$R^i_{PU,ON}$	0
7	$R^i_{PU,ON}$	$R^i_{PU,ON}$	$R^i_{PU,ON}$

Case	$\ddot{\mu}_i[n]$
0	0
1	$R^i_{PU,ON}\left(\frac{1}{P_{BS}[n]-PBS[n-1]}\right)$
2	$-R^i_{PU,ON}\left(\frac{1}{P_{BS}[n]-PBS[n-1]}+\frac{1}{P_{BS}[n-1]-PBS[n-2]}\right)$
3	$-R^i_{PU,ON}\left(\frac{1}{P_{BS}[n-1]-PBS[n-2]}\right)$
4	$R^i_{PU,ON}\left(\frac{1}{P_{BS}[n-1]-PBS[n-2]}\right)$
5	$R^i_{PU,ON}\left(\frac{1}{P_{BS}[n]-PBS[n-1]}+\frac{1}{P_{BS}[n-1]-PBS[n-2]}\right)$
6	$-R^i_{PU,ON}\left(\frac{1}{P_{BS}[n]-PBS[n-1]}\right)$
7	0

At each QP$_k$, $R_{PU,i}[k]$ can have one of two values as expressed in (8). Thus, there are eight cases of received primary signal strengths at three QPs in the testing window, $\{R_{PU,i}[n-2], R_{PU,i}[n-1], R_{PU,i}[n]\}$, as shown in Table I. The table also shows $\ddot{\mu}_i^2[n]$ in each case. Note that $\left|\ddot{\mu}_i^2[n]\right|$ can have one of the following four values:

$$\left|\ddot{\mu}_i^2[n]\right| = \begin{cases} 0 \\ \left|R^i_{PU,ON}\left(\frac{1}{P_{BS}[n]-P_{BS}[n-1]}\right)\right| \\ \left|R^i_{PU,ON}\left(\frac{1}{P_{BS}[n]-P_{BS}[n-1]}+\frac{1}{P_{BS}[n-1]-P_{BS}[n-2]}\right)\right| \\ \left|R^i_{PU,ON}\left(\frac{1}{P_{BS}[n-1]-P_{BS}[n-2]}\right)\right|. \end{cases} \tag{14}$$

Based on this, one of the following cases will hold:

- When $\left|\ddot{\mu}_i^2[n]\right| = 0$, $R_{PU,i}[k]$ value should be identical during three QPs in the testing window. We cannot estimate $R^i_{PU,ON}$ at this point.
- When $\left|\ddot{\mu}_i^2[n]\right| \neq 0$, $R_{PU,i}[k]$ value changes during three QPs in the testing window. $R^i_{PU,ON}$ should be one of the following three values:
  - $\left|\left(\ddot{g}_{BS,i}[n]\right)\left(P_{BS}[n]-P_{BS}[n-1]\right)\right|$
  - $\left|\left(\ddot{g}_{BS,i}[n]\right)\left(\frac{(P_{BS}[n]-P_{BS}[n-1])(P_{BS}[n-1]-P_{BS}[n-2])}{P_{BS}[n]-P_{BS}[n-2]}\right)\right|$
  - $\left|\left(\ddot{g}_{BS,i}[n]\right)\left(P_{BS}[n-1]-P_{BS}[n-2]\right)\right|$.

Recall that the testing window is set to [QP$_{n-2}$, QP$_n$] at QP$_n$. The testing window moves forward with time, and hence, in every testing window, three candidates for $R^i_{PU,ON}$ are inferred by the above process. By keeping track of these values calculated at each testing window, the BS can estimate the common value as $R^i_{PU,ON}$.

C. Filtering out Falsified Sensing Reports

We now analyze the reported (not true) test statistic. Since the sensing report has the attack strength component

$D_i[k],\ k \in \{n-2, n-1, n\}$, the BS gets:

$$\begin{aligned}\bar{\dot{g}}_{BS,i}[n-1] \equiv & \frac{\bar{R}_i[n-1] - \bar{R}_i[n-2]}{P_{BS}[n-1] - P_{BS}[n-2]} \\ & \sim \mathcal{N}\left(g_{BS,i} + \frac{R_{PU,i}[n-1] - R_{PU,i}[n-2]}{P_{BS}[n-1] - P_{BS}[n-2]}\right. \\ & \quad + \frac{D_i[n-1] - D_i[n-2]}{P_{BS}[n-1] - P_{BS}[n-2]}, \\ & \quad \left.\frac{\sigma_i^2[n-1] + \sigma_i^2[n-2]}{(P_{BS}[n-1] - P_{BS}[n-2])^2}\right)\end{aligned} \tag{15}$$

$$\begin{aligned}\bar{\dot{g}}_{BS,i}[n] \equiv & \frac{\bar{R}_i[n] - \bar{R}_i[n-1]}{P_{BS}[n] - P_{BS}[n-1]} \\ & \sim \mathcal{N}\left(g_{BS,i} + \frac{R_{PU,i}[n] - R_{PU,i}[n-1]}{P_{BS}[n] - P_{BS}[n-1]}\right. \\ & \quad + \frac{D_i[n] - D_i[n-1]}{P_{BS}[n] - P_{BS}[n-1]}, \\ & \quad \left.\frac{\sigma_i^2[n] + \sigma_i^2[n-1]}{(P_{BS}[n] - P_{BS}[n-1])^2}\right)\end{aligned} \tag{16}$$

$$\begin{aligned}& \bar{\ddot{g}}_{BS,i}[n] \equiv \bar{\dot{g}}_{BS,i}[n] - \bar{\dot{g}}_{BS,i}[n-1] \\ & \sim \mathcal{N}\left(\frac{R_{PU,i}[n] - R_{PU,i}[n-1]}{P_{BS}[n] - P_{BS}[n-1]} - \frac{R_{PU,i}[n-1] - R_{PU,i}[n-2]}{P_{BS}[n-1] - P_{BS}[n-2]}\right. \\ & \quad + \frac{D_i[n] - D_i[n-1]}{P_{BS}[n] - P_{BS}[n-1]} - \frac{D_i[n-1] - D_i[n-2]}{P_{BS}[n-1] - P_{BS}[n-2]}, \\ & \quad \sigma_i^2[n]\left(\frac{1}{P_{BS}[n] - P_{BS}[n-1]}\right)^2 \\ & \quad + \sigma_i^2[n-1]\left(\frac{1}{P_{BS}[n] - P_{BS}[n-1]} + \frac{1}{P_{BS}[n-1] - P_{BS}[n-2]}\right)^2 \\ & \quad \left. + \sigma_i^2[n-2]\left(\frac{1}{P_{BS}[n-1] - P_{BS}[n-2]}\right)^2\right) \\ & \sim \mathcal{N}\left(\bar{\ddot{\mu}}_i[n], \ddot{\sigma}_i^2[n]\right)\end{aligned} \tag{17}$$

which are different from $\dot{g}_{BS,i}[n-1]$, $\dot{g}_{BS,i}[n]$, and $\ddot{g}_{BS,i}[n]$. Equation (17) indicates that the distribution of $\bar{\ddot{g}}_{BS,i}[n]$ also follows a Gaussian distribution. We thus set the lower and upper thresholds on the acceptable $\bar{\ddot{g}}_{BS,i}[n]$ value to determine if reports in the testing window are faulty. Then, with a $100 \times (1-\epsilon)\%$ confidence, $\bar{\ddot{g}}_{BS,i}[n]$ should satisfy

$$\Phi\left(\frac{\left|\bar{\ddot{\mu}}_i[n] - \ddot{\mu}_i[n]\right|}{\ddot{\sigma}_i[n]}\right) > 1 - \epsilon, \tag{18}$$

where $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2}\, dx$ is the cumulative distribution function (CDF) of a standard normal distribution. It is straightforward to derive the following equation from (18):

$$\left|\frac{D_i[n] - D_i[n-1]}{P_{BS}[n] - P_{BS}[n-1]} - \frac{D_i[n-1] - D_i[n-2]}{P_{BS}[n-1] - P_{BS}[n-2]}\right| < \ddot{\sigma}_i[n] Q^{-1}(\epsilon), \tag{19}$$

where $Q(x) = 1 - \Phi(x)$ is the Q-function. From (19), we notice that $\left|\frac{D_i[n]-D_i[n-1]}{P_{BS}[n]-P_{BS}[n-1]} - \frac{D_i[n-1]-D_i[n-2]}{P_{BS}[n-1]-P_{BS}[n-2]}\right|$ should approach 0 as $\ddot{\sigma}_i^2[n]$ decreases. Otherwise, the attack should be detected. Therefore, faulty CPEs have an incentive to decrease $\left|\frac{D_i[n]-D_i[n-1]}{P_{BS}[n]-P_{BS}[n-1]} - \frac{D_i[n-1]-D_i[n-2]}{P_{BS}[n-1]-P_{BS}[n-2]}\right|$ in order to evade detection. However, from the perspective of CPEs, $P_{BS}[k], k \in \{n-2, n-1, n\}$ are not known although they have the information of $D_i[k], k \in \{n-2, n-1, n\}$. If we assume that the attack strength $D_i[k]$ cannot be correlated with $P_{BS}[k]$, faulty reports can satisfy (19) only when $D_i[k]$ is fixed. When $D_i[k]$ is fixed, the BS can easily estimate $g_{BS,i}$ values from (15) and (16) since $D_i[k] - D_i[k-1]$ should be 0. Thus, $R_{BS,i}[k] = g_{BS,i} P_{BS}[k]$ can also be estimated.

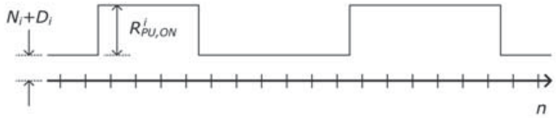

Fig. 7. A sequence of test statistical values at CPE i after subtracting the power of PUET signals.

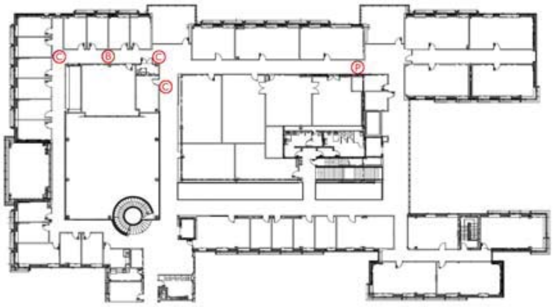

Fig. 8. The topology of our testbed: USRP2 nodes are placed at different locations on the fourth floor of our department building.

By observing the sequence of $\bar{R}_i[n] - g_{BS,i} P_{BS}[n]$, the BS may obtain the plot in Fig. 7 with $D_i[k] = D_i$ fixed. Since each CPE has its own noise figure, one can regard the attack strength D_i as a component of noise sources. Thus, the BS decides on the presence/absense of PU signals by only checking $R_{PU,i}[n]$ term in the sequence of test statistic values.

VI. Performance Evaluation

A. Testbed Setup

To evaluate the performance of PUET, we constructed a testbed with Universal Software Radio Peripheral 2 (USRP2) [31] in our Department building. We deployed 5 USRP2 nodes as in the topology shown in Fig. 8. The testbed consists of a PU (denoted as circled P in the figure), a BS (denoted as circled B in the figure), and 3 CPEs (denoted as circled C in the figure).

The USRP2 nodes are equipped with a set of WBX daughterboards and VERT900 omni-directional antennas. WBS daughterboards and the VERT900 antennas support 50MHz–2.2GHz and 824–960MHz bands, respectively [31]. Each USRP2 node is controlled by GNU Radio (version 3.6.2) [32] an open-source software development toolkit that provides signal processing blocks for SDR implementation.

We use the benchmark OFDM encoding/decoding module in GNU Radio to generate a PUET signal. The testbed operates on a 6MHz-wide band centered at 907MHz. From our experiments, we found that the power spectral density (PSD) of the transmitted signal is not constant over the considered band (i.e., 904–910MHz). Instead, the PSD increases as the frequency approaches the band's center frequency, creating subchannel dependency. Therefore, we set the bandwidth of the transmitter twice wider and use only one half of the

TABLE II
SYSTEM PARAMETERS USED IN EXPERIMENTS

Parameter	Value	Comments
B	6MHz	Channel bandwidth
f_c	907MHz	Center frequency of the channel
T_P	1s	Sensing period
T_I	1ms	Sensing duration
M	6×10^3	# of signal samples per sensing
P_{PU}	15.56dBm	Transmission power of the PU
$P_{BS_{max}}$	13.98dBm	Max transmission power of the BS
$P_{BS_{min}}$	9.54dBm	Min transmission power of the BS

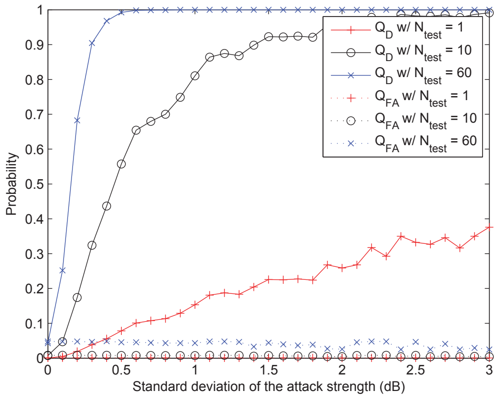

Fig. 9. Attack detection performance under random attacks: detection performance increases significantly as N_{test} increases.

subchannel to generate a PUET signal. This makes the PSD of the PUET signal flatter over the channel and also makes the transition more instantaneous in frequency. The measurements were taken for 1800 seconds in each scenario. Table II lists the system parameters used in our experiments.

B. Attack Detection Performance

As a first line of defense, the attack detector in PUET must be able to correctly identify faulty reports and filter them out before making a final decision on the presence of the PU. Fig. 9 shows the performance of PUET while varying the number of testing windows, N_{test}, for the identification of faulty reports. That is, PUET determines the existence of a non-zero attack strength by using N_{test} consecutive testing windows. Only when reports in N_{test} consecutive testing windows show a consistent $R^i_{PU,ON}$ value, PUET regards the reports as not faulty. On the other hand, when PUET detects an inconsistency in the estimated $R^i_{PU,ON}$ at least once in N_{test} tests, it concludes that there is an attack with non-zero attack strength, and marks the report as faulty.

The CPE generates a faulty report with randomly-generated attack strengths in each QP. The attack strength follows a Gaussian distribution with mean 0 and standard deviation σ_{Att}. The figure shows that the detection performance increases as σ_{Att} increases in all cases. Especially when $N_{test} = 60$, the detection probability approaches 1 as σ_{Att} gets higher than 0.5dB. Note that the probability of false alarm, i.e., PUET mistakenly marks an honest report as faulty, is as low as 0.05 even when $N_{test} = 60$. Therefore, it is desirable to use 60 consecutive testing windows for detection of faulty reports.

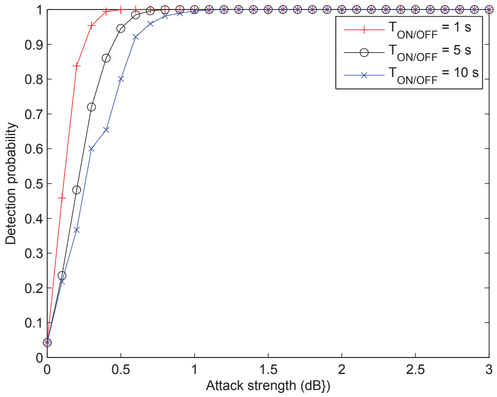

Fig. 10. Detection performance under attacks with the ON/OFF strength model.

The detection performance also depends on the pattern of attack strength. In order to mislead the BS about the PU's presence/absence, a CPE may also model the attack strength as an ON/OFF alternating renewal process. Fig. 10 shows the detection performance under attacks with the ON/OFF strength model. We vary the ON/OFF sojourn time, $T_{ON/OFF}$, from 1 to 10s. The figure shows that the detection performance increases as $T_{ON/OFF}$ decreases, because the larger the sojourn time, the more zero $\ddot{\mu}_i[n]$ occur in N_{test} testing windows. As mentioned earlier, PUET cannot detect faulty reports when $D_i[n]$ is fixed. Thus, when $T_{ON/OFF}$ is larger than N_{test}, PUET cannot detect faulty reports. Therefore, we again need to set N_{test} high enough.

C. PU Detection Performance

By using PUET, attacks can be detected with a high confidence (e.g., Q_D approaches 1 when $N_{test} = 60$ and σ_{Att} is greater than 0.5dB). We now evaluate the performance of detecting PU signals. The BS determines the presence/absense of PU signals by collecting sensing reports that are not filtered out by PUET. As a baseline data-fusion scheme, we use the majority rule for this experiment.

Fig. 11 shows the performance of detecting PU signals with and without PUET: "MAJ" represents the majority-rule-based data-fusion, and "PUET" represents application of the majority rule after PUET filtered out attacks separately. In this scenario, each CPE independently generates faulty reports with 0.5dB ON/OFF attack strengths. From the figure, we can easily confirm that the detection probability decreases as the number of attackers (i.e., CPEs with faulty reports) increases since the number of faulty reports also affects the majority decision. Especially when the number of attackers is greater than a half number of the total CPEs, Q_D^{PU} of MAJ becomes lower than 0.2. However, Q_D^{PU} of PUET is over 0.8 even when there are two attackers. This is because PUET fusions sensing data after filtering out attacks separately. Similarly, Q_{FA}^{PU} or PUET is kept under 0.11 whereas that of MAJ is not.

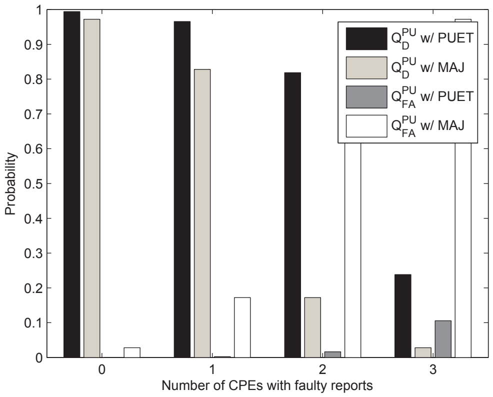

Fig. 11. PU detection performance under ON/OFF attacks: PUET correctly determines the presence/absence of PU signals even when two CPEs provide faulty reports.

VII. Conclusion

The design of reliable distributed sensing for opportunistic spectrum use is a major research challenge in DSA networks. To meet this challenge, we proposed PUET that detects the falsification of sensing results. The key idea behind PUET is that CPEs can acquire only RSSs, not the information of the signal source. To realize this idea, the BS transmits a test signal when CPEs sense the channel. Since CPEs cannot distinguish a test signal from a PU signal, the BS can detect sensing data falsification attacks by checking if the reported sensing data reflects the test signals it transmitted. In order to check the validity of sensing reports, the BS tests three consecutive sensing reports in a testing window. By checking the consistency of estimation of the received primary signal strength, the BS determines if there exist non-zero attack strengths in the sensing reports. We have evaluated the performance of attack detection with an indoor USRP2-based testbed. By conducting experiments on the testbed, we have confirmed that PUET detects attacks with both random and ON/OFF attack strengths. We have also found that PUET correctly detects PU signals even when more than a half of reports are faulty.

Acknowledgements

The work reported in this paper was supported in part by the ARO under Grant W81NF-12-1-0530 and the NSF under Grant CNS-1160775.

References

[1] "Cisco visual networking index: Forecast and methodology, 2011-2016," Cisco, May. 2012.

[2] "Mobile broadband: The benefits of additional spectrum," FCC, Oct. 2010.

[3] M. McHenry, "NSF spectrum occupancy measurements project summary," http://www.sharedspectrum.com/measurements/, Shared Spectrum Company Report, Aug. 2005.

[4] M. McHenry, P. Tenhula, D. McCloskey, D. Roberson, and C. Hood, "Chicago spectrum occupancy measurements & analysis and a long-term studies proposal," in *Proc. ACM TAPAS*, Aug. 2006.

[5] J. Mitola and G. Maguire, "Cognitive radio: Making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, Apr. 1999.

[6] A. Fehske, J. Gaeddert, and J. Reed, "A New Approach to Signal Classification Using Spectral Correlation and Neural Networks," in *Proc. IEEE DySPAN*, Nov. 2005.

[7] B. Wild and K. Ramchandran, "Detecting Primary Receivers for Cognitive Radio Applications," in *Proc. IEEE DySPAN*, Nov. 2005.

[8] G. B. et al., "The Design and Operation of the IEEE 802.22.1 Disabling Beacon for the Protection of TV Whitespace Incumbents," in *Proc. IEEE DySPAN*, Oct. 2008.

[9] D. G. et al., "Geo-Location Database Techniques For Incumbent Protection in the TV White Space," in *Proc. IEEE DySPAN*, Oct. 2008.

[10] K. Shin, H. Kim, A. Min, and A. Kumar, "Cognitive radios: From concept to reality," *IEEE Wireless Communications Magazine*, vol. 17, no. 5, pp. 64–74, Dec. 2010.

[11] Y. Liang, Y. Zeng, E. Peh, and A. Hoang, "Sensing-throughput tradeo? for cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1326–1337, Apr. 2008.

[12] E. Visotsky, S. Kuffner, and R. Peterson, "On collaborative detection of tv transmissions in support of dynamic spectrum sharing," in *Proc. IEEE DySPAN*, Nov. 2005.

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

[14] S. Mishra, A. Sahai, and R. Brodersen, "Cooperative Sensing among Cognitive Radios," in *Proc. IEEE ICC*, Jun. 2006.

[15] R. Chen, J. Park, and K. Bian, "Robust Distributed Spectrum Sensing in Cognitive Radio Networks," in *Proc. IEEE INFOCOM*, Apr. 2008.

[16] A. Min, K. Shin, and X. Hu, "Secure Cooperative Sensing in IEEE 802.22 WRANs Using Shadow Fading Correlation," *IEEE Transactions on Mobile Computing*, vol. 10, no. 10, pp. 1434–1447, Apr. 2008.

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

[18] L. Duan, A. Min, J. Huang, and K. Shin, "Attack Prevention for Collaborative Spectrum Sensing in Cognitive Radio Networks," *IEEE Journal on Seleted Areas in Communications*, vol. 30, no. 9, pp. 1658–1665, Oct. 2012.

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

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

[21] H. Kim and K. G. Shin, "Efficient discovery of spectrum opportunities with MAC-layer sensing in cognitive radio networks," *IEEE Transactions on Mobile Computing*, vol. 7, no. 5, pp. 533–545, May. 2008.

[22] S. Geirhofer, L. Tong, and B. Sadler, "Dynamic spectrum access in the time domain: Modeling and exploiting white space," *IEEE Communications Magazine*, vol. 45, no. 5, pp. 66–72, May. 2007.

[23] A. Motamedi and A. Bahai, "MAC protocol design for spectrum-agile wireless networks: Stochastic control approach," in *Proc. IEEE DySPAN*, Apr. 2007.

[24] H. Kim and K. Shin, "In-band Spectrum Sensing in Cognitive Radio Networks: Energy Detection or Feature Detection?" in *Proc. ACM MOBICOM*, Sep. 2008.

[25] R. Pickholtz, D. Schilling, and L. Milstein, "Theory of spread-spectrum communications-a tutorial," *IEEE Transactions on Communications*, vol. 30, no. 5, pp. 855–884, May. 1982.

[26] C. Cordeiro, K. Challapali, and M. Ghosh, "Cognitive PHY and MAC layers for dynamic spectrum access and sharing of TV bands," in *ACM TAPAS*, Aug. 2006.

[27] A. Goldsmith, *Wireless Communications*. Cambridge Univ., 2005.

[28] 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*, Aug. 2006.

[29] A. Min and K. Shin, "An Optimal Sensing Framework Based on Spatial RSS-Profile in Cognitive Radio Networks," in *Proc. IEEE SECON*, Jun. 2009.

[30] 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, Apr. 2006.

[31] USRP: Universal Software Radio Peripheral, http://ettus.com/.

[32] GNU Software Radio Project, http://gnuradio.org/.