Research Article

Location Aided Cooperative Detection of Primary User Emulation Attacks in Cognitive Wireless Sensor Networks Using Nonparametric Techniques

Mariano García-Otero and Adrián Población-Hernández

Departamento Señales, Sistemas y Radiocomunicaciones, ETSI Telecomunicación, Universidad Politécnica de Madrid, Avenida Complutense 30, 28040 Madrid, Spain

Correspondence should be addressed to Mariano García-Otero; mariano@gaps.ssr.upm.es

Received 17 April 2015; Revised 13 September 2015; Accepted 14 September 2015

Academic Editor: Walid Saad

Copyright © 2016 M. García-Otero and A. Población-Hernández. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Primary user emulation (PUE) attacks are a major security challenge to cognitive wireless sensor networks (CWSNs). In this paper, we propose two variants of the PUE attack, namely, the relay and replay attacks. Such threats are conducted by malicious nodes that replicate the transmissions of a real primary user (PU), thus making them resilient to many defensive procedures. However, we show that those PUE attacks can be effectively detected by a set of cooperating secondary users (SUs), using location information and received signal strength (RSS) measurements. Two strategies for the detection of PUE relay and replay attacks are presented in the paper: parametric and nonparametric. The parametric scheme is based on the likelihood ratio test (LRT) and requires the existence of a precise path loss model for the observed RSS values. On the contrary, the nonparametric procedure is not tied to any particular propagation model; so, it does not require any calibration process and is robust to changing environmental conditions. Simulations show that the nonparametric detection approach is comparable in performance to the LRT under moderate shadowing conditions, specially in case of replay attacks.

1. Introduction

Cognitive radio (CR) is considered a key concept for the development of future wireless networks [1]. One of the technologies enabled by CR systems is dynamic spectrum access (DSA), which promises a much more efficient use of spectrum resources by reusing frequency channels in different networks as they become available. The usual approach in DSA is to assume the existence of a set of licensed primary users (PUs) who have unrestricted use of the available spectrum and a network of unlicensed secondary users (SUs), equipped with CR devices, who are allowed to occupy the portions of the spectrum left temporarily free by the PUs. The stringent requirement here is that SUs should not interfere with the PUs (*interweaving* paradigm), a fact that forces the SUs to continually perform *spectrum sensing* to determine the existence of a frequency band with no PU activity in the neighborhood of the SUs (also known as

“white space” or “spectrum hole”) so as to allocate their own transmissions. Notice that, for a given frequency, a spectrum hole can occur both in time (during a period when the PUs are not transmitting) and in space (if the communication ranges of the PUs and SUs do not overlap).

As the SUs are required to refrain from using the unlicensed band as soon as PU activity is detected, a potential attacker could exploit this fact by filling white spaces with fake emissions that mimic those of a real PU transmitter. This is the so-called primary user emulation (PUE) attack [2], that, if successful, could potentially render the CR network inoperative, because the SUs would not be able to find spectrum holes to establish links between them. A PUE attack can be launched by a set of malicious nodes, equipped with radio interfaces compatible with those of the PUs.

Although a number of detection schemes of PUE attacks have been suggested [3], the most effective countermeasures require some form of cooperation between the PUs and

the CR network by means of cryptographic protocols. For instance, the PUs and SUs could interchange in advance some secret keys, and then the PUs would use them to authenticate themselves by including digital signatures in their transmissions. In this way, as long as the malicious nodes do not have access to the secret keys, SUs could distinguish legitimate PU transmissions from fake ones, because the latter would not carry the correct signatures. However, as we will see, cryptographic protocols are vulnerable to two kind of threats, namely, the *relay* (or “wormhole”) and the *replay* (or “playback”) attacks.

A wormhole is a direct high-speed private communication link between two distant malicious nodes [4]. To launch a PUE relay attack, one of the wormhole nodes is placed near a PU and the other in the neighborhood of the CR network. Then, the node in the vicinity of the PU captures its transmissions and sends them through the wormhole to the other node, which simply relays the packets unaltered so that they are received by the SUs. Therefore, even if the SUs were too far from the PUs to cause interferences, they are deceived into believing there is a nearby PU, thus preventing them from using the unlicensed channel. On the other hand, a PUE replay attack can be carried out by a single malicious node that records network packets from an active PU and retransmits them whenever the PU is inactive. In this way, the malicious node fills white spaces with spurious PU transmissions and as the SUs in the neighborhood of the malicious node are continuously detecting emissions carrying valid PU signatures, they cannot use the channel for their own communications.

As PUE attacks using relay or replay techniques are resilient to cryptographic countermeasures, other strategies should be used to detect them. The conventional approach is to exploit the fact that the malicious nodes and the PU transmitter are located at different places and, assuming that the actual position of the PU is known by the SUs, use localization techniques to validate the origin of the detected PU transmissions. Such localization procedures are based on the capability of any radio receiver to obtain some kind of measurement related to its distance to the transmitter; in the case of a wireless sensor networks (WSNs) device, this is typically the average power measured at the receiver input, usually defined as received signal strength (RSS). However, most approaches assume the existence of a precise analytical model that relates RSS values to distances, which, in many cases, is a rather unrealistic assumption.

In this paper, we address the problem of detecting PUE relay and replay attacks based on localization techniques using RSS measurements in cognitive wireless sensor networks (CWSNs). In case the observations are guaranteed to fit a predefined path loss model, we propose the use of a cooperative detection strategy based on the likelihood ratio test (LRT); on the other hand, for most situations, we propose the use of a nonparametric model-free scheme to detect PUE attacks.

The rest of the paper is organized as follows: Section 2 reviews related work concerning PUE attack detection. Section 3 defines the particular attacks to be counteracted. Section 4.1 formulates the cooperative location-based PUE

detection problem under the framework of statistical hypothesis testing and derives the LRT. Section 4.2 presents our nonparametric approach to PUE detection. Section 5 evaluates the performance of the proposed PUE attack detection strategies through simulations. Finally, Section 6 draws some conclusions.

2. Related Work

The topic of PUE attacks has been extensively studied in recent years, and a lot of different defensive measures are described in the related literature.

The first reference to this kind of attacks is in [2], where they are classified under two different categories: *selfish* (the attacker tries to maximize its own spectrum usage) and *malicious* (the objective of the attacker is to disturb the DSA process of SUs). In this paper, a transmitter verification scheme is proposed to counteract PUE attacks that uses both signal characteristics and location information; the localization of the active transmitter is performed (using RSS values and a parametric measurement model) by an auxiliary WSN composed of a high number of devices distributed along the deployment area of the SUs.

The authors of [5] present a Wald’s sequential probability ratio test to detect PUE attacks conducted by a set of malicious nodes. Their approach is based on RSS observations and location information but assumes that there is no cooperation between SUs, so each node performs its own test independently of the others.

The use of a cooperative belief propagation procedure is proposed in [6] to detect a potential attacker by using RSS measurements and interactions between neighboring SUs. This approach also requires a parametric model relating the received power to the distance between transmitter and receiver.

In [7], the authors propose a method for the localization of attackers using time differential of arrival (TDOA) instead of RSS. Thus, it requires modifications of the physical layer to measure signal time delays.

The authors of [8] propose to analyze anomalous behavior (such as changes in transmitted power and/or bandwidth) and use collaboration between SUs to detect PUE attacks in CWSN scenarios. Therefore, for this method to be effective, it is needed to precisely define what is considered an anomaly.

In [9], a cryptographic method is proposed to authenticate the PU transmissions, but it requires modifications in the PU transmitter and receivers to accommodate encrypted data and also a mechanism to securely distribute secret keys to both the PUs and the SUs. Another cryptographic mechanism is proposed in [10] to authenticate PU transmissions with the aid of a helper node placed physically close to the PU transmitter. As stated before, cryptographic protocols can be defeated by relay and replay attacks.

Device-specific features (“fingerprints”) along with unique IDs are used in [11–13] to detect potential attackers in CR networks. Those fingerprints are features extracted directly from the analog signals transmitted by the network nodes, which vary from device to device because of the inevitable differences between hardware components of

FIGURE 1: PUE attack models. (a) Relay (wormhole) attack. (b) Replay (playback) attack.

compatible radio interfaces. Measuring those distinct features requires the analysis of the signals at the physical layer level, which is beyond the capabilities of low-cost WSN devices.

Most of the PUE attack detection methods described above have significant drawbacks when applied to CWSNs. In particular, those based on the use of location information lack robustness because they are tied to a parametric model for the measurements that must be precisely tuned to every specific environment.

3. Attack Models

We will consider two types of PUE attacks, namely, relay and replay attacks, as shown in Figure 1. Both have in common the existence of an adversary who tries to deceive the SUs into believing that there is a PU transmitting in their neighborhood, so that they are forced to refrain from using the PU frequency channel (i.e., they are *malicious* PUE attacks [2]).

Figure 1(a) represents an example of a relay attack. Here, we assume that there is an active PU transmitter, but it is located far away from the SUs so that the coverage areas of the PUs and SUs do not intersect; therefore, the SUs could use the unlicensed channel without causing interferences to PUs. However, a malicious node located in the neighborhood of the PU transmitter is sending the PU emissions through a private link to another node that, in turn, broadcasts them to the SUs. Thus, a PUE relay attack fills spectrum holes in the *space* domain by making remote PUs appear as local in the CR network.

Figure 1(b) illustrates a replay attack. Such attack assumes that the SUs are in the vicinity of a PU transmitter, which is presently inactive. However, a malicious node that has previously recorded a set of PU transmissions is now replaying them to the SUs. Therefore, a PUE replay attack fills spectrum holes in the *time* domain by making inactive PUs appear as active in the CR network.

Notice that as the malicious nodes do not manipulate the information contained in the packets, these PUE attacks resist defensive measures solely based on cryptographic protocols. In the sequel, we will see how location information, along with RSS measurements collected by the SUs, can be effectively used to defeat both relay and replay attacks.

4. PUE Detection Using RSS

Our detection schemes will be based on the following assumptions:

- (i) There is one (and only one) active transmitter that can be either a legitimate PU or a malicious attacker.
- (ii) There are N SUs carrying out a spectrum sensing stage, during which every SU takes one RSS measurement and sends it to a central fusion node.
- (iii) The fusion node is aware of the locations of the PU and SUs and uses this information and the N RSS values to decide whether there is an attack or not.

Therefore, following an approach analogous to [14], we state a PUE attack detection procedure as a binary hypothesis testing problem: given a vector of N RSS observations, we must decide between hypotheses H_0 (no attack) and H_1 (a PUE attack is launched).

In the sequel, we will use the following notation:

$\mathbf{p}$ is the position in the plane of the PU.

$\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_N$ are the positions of the SUs.

$\mathbf{r} = [r_1, r_2, \dots, r_N]^T$ (where the superscript T denotes “transpose”) is the vector of RSS values (in dBm) measured by the SUs.

$d(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|$ is the Euclidean distance between two arbitrary network nodes at positions $\mathbf{x}$ and $\mathbf{y}$.

$r(\mathbf{x}, \mathbf{y})$ is the RSS (in dBm) measured by the receiver of a node at position $\mathbf{y}$ for a signal transmitted by a node at position $\mathbf{x}$.

So, the observations collected by the SUs are, under H_0 (no attack), the RSS values of packets transmitted by the PU and received by the SUs. Thus, according to our notation, the null hypothesis (no PUE attack) can be formulated as

$$H_0: r_i = r(\mathbf{p}, \mathbf{s}_i), \quad i = 1, 2, \dots, N. \quad (1)$$

Now, depending on the assumed model for the observations, we can define both parametric and nonparametric tests, as explained in the following subsections.

4.1. Parametric Approach. In order to formalize a parametric test, we need a suitable statistical description of the observations. In our approach, we will use the standard log-distance path loss model [15] that links RSS values (in logarithmic scale) to distances between nodes as

$$r(\mathbf{x}, \mathbf{y}) = K - 10\alpha \log_{10} d(\mathbf{x}, \mathbf{y}) + e, \quad (2)$$

where K is the mean RSS at unit distance of the transmitter (depends on the transmitted power and antenna gains), α is the path loss exponent (depends on the specific environment), and e is a zero-mean Gaussian random variable with standard deviation σ (in dB) that takes into account shadowing effects. Therefore, $r(\mathbf{x}, \mathbf{y})$ is also a Gaussian random variable with standard deviation σ and mean $\mu(\mathbf{x}, \mathbf{y})$, with

$$\mu(\mathbf{x}, \mathbf{y}) = E[r(\mathbf{x}, \mathbf{y})] = K - 10\alpha \log_{10} d(\mathbf{x}, \mathbf{y}), \quad (3)$$

where $E[\cdot]$ stands for “expected value.” Now, assuming that the shadow fading is spatially uncorrelated, the observations are independent and identically distributed (IID) and, therefore, the distribution of the vector of RSS values $\mathbf{r}$ is multivariate normal with mean vector $\boldsymbol{\mu} = [\mu_1, \mu_2, \dots, \mu_N]^T$ and covariance matrix $\sigma^2 \mathbf{I}$, where $\mathbf{I}$ is the identity matrix of order N ; thus, the joint probability density function (PDF) of the RSS measurements is

$$f(\mathbf{r}; \boldsymbol{\mu}) = (2\pi\sigma^2)^{-N/2} \exp \left[-\frac{1}{2\sigma^2} (\mathbf{r} - \boldsymbol{\mu})^T (\mathbf{r} - \boldsymbol{\mu}) \right]. \quad (4)$$

The only parameter of (4) that depends on the position is $\boldsymbol{\mu}$, so we will formulate the PUE attack detection problem as a test of the mean vector of $\mathbf{r}$:

$$H_0: \boldsymbol{\mu} = \boldsymbol{\mu}_0, \quad (5a)$$

$$H_1: \boldsymbol{\mu} \neq \boldsymbol{\mu}_0, \quad (5b)$$

where $\boldsymbol{\mu}_0$ is determined assuming that there is no attack present.

According to (3), the elements of vector $\boldsymbol{\mu}_0$ in (5a) and (5b) are

$$\mu_{0,i} = K - 10\alpha \log_{10} d(\mathbf{p}, \mathbf{s}_i), \quad i = 1, 2, \dots, N. \quad (6)$$

We can see that H_0 is a simple hypothesis, because all the magnitudes involved in (6), namely, the path loss model parameters (K and α) and the positions of the PU and SUs ($\mathbf{p}, \mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_N$), are assumed known. On the other hand, under H_1 (PUE attack), the packets received by the SUs are transmitted by the local malicious node, as shown in Figure 1; therefore, the RSS values for these packets will be unrelated to position $\mathbf{p}$ of the emulated PU.

Therefore, we can obtain the likelihood ratio test (LRT) [16] as

$$\text{Decide } H_1 \text{ (attack present) iff } \Lambda(\mathbf{r}) > \eta, \quad (7)$$

where $\Lambda(\mathbf{r})$ is the likelihood ratio

$$\Lambda(\mathbf{r}) = \frac{\max_{\boldsymbol{\mu}} f(\mathbf{r}; \boldsymbol{\mu})}{f(\mathbf{r}; \boldsymbol{\mu}_0)} \quad (8)$$

and η is a threshold selected so that we have a given probability of false alarm (PFA).

The numerator of (8) is easily obtained, according to (4) as

$$\max_{\boldsymbol{\mu}} f(\mathbf{r}; \boldsymbol{\mu}) = (2\pi\sigma^2)^{-N/2} \quad (9)$$

while the denominator of (8) is, taking into account (4) and (6),

$$f(\mathbf{r}; \boldsymbol{\mu}_0) = (2\pi\sigma^2)^{-N/2} \exp \left[-\frac{1}{2\sigma^2} S(\mathbf{r}) \right] \quad (10)$$

with $S(\mathbf{r})$ the “sum of squares”

$$S(\mathbf{r}) = \sum_{i=1}^N [r_i - K + 10\alpha \log_{10} d(\mathbf{p}, \mathbf{s}_i)]^2. \quad (11)$$

Now, taking into account (8), (9), and (10), we can compute the logarithm of the likelihood ratio as

$$\ln \Lambda(\mathbf{r}) = \frac{S(\mathbf{r})}{2\sigma^2} \quad (12)$$

so that a test equivalent to (7) is

$$\text{Decide } H_1 \text{ iff } S(\mathbf{r}) > \eta', \quad (13)$$

where η' is another suitable threshold selected so that

$$P[S(\mathbf{r}) > \eta' | H_0] = P_{\text{FA}} \quad (14)$$

with P_{FA} the probability of false alarm. To determine the value of the threshold η' we can use the fact that, under H_0 , $S(\mathbf{r})/\sigma^2$ can be expressed as the sum of N independent standard normal random variables, and so it has chi-square distribution with N degrees of freedom.

We can see from (11) that $S(\mathbf{r})$ is a measure of “goodness of fit” of the PU position to the observations, assuming that the path loss model (2) is correct. Notice also that as the number of terms in (11) is N , the complexity of the LRT grows linearly with the number of SUs.

4.2. Nonparametric Approach. The PUE attack detection strategy of Section 4.1 assumes the existence of a well-defined measurement model that describes the statistical relationship between observed RSS values and distances. However, in most instances, such model can only be stated under idealized conditions or is tied to a specific scenario; in this latter case, estimating its parameters often requires a costly calibration phase which must be repeated every time the environmental conditions change. Therefore, it would be desirable to devise a PUE attack detection procedure that is “nonparametric” or “model-free” in the sense that, unlike test (13), this alternative strategy does not impose a particular distribution for the observations; thus, such test will be robust against departures from any predefined model.

As we will see, in order to obtain a nonparametric test, we only need a simple assumption: we will accept the universal

validity (under ideal conditions) of the “monotonicity constraint” that loosely relates the Euclidean distances of a single transmitting node ($\mathbf{x}$) to two different receiving nodes ($\mathbf{y}$ and $\mathbf{z}$) and the RSSs measured by the receivers as

$$\begin{aligned} r(\mathbf{x}, \mathbf{y}) &> r(\mathbf{x}, \mathbf{z}) \iff \\ d(\mathbf{x}, \mathbf{y}) &< d(\mathbf{x}, \mathbf{z}), \end{aligned} \quad (15)$$

$$\forall \mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{R}^2.$$

Such constraint is based on the fact that radio waves attenuate with distance and assumes that transmitters and receivers are using omnidirectional antennas. In practice, channel effects such as multipath and shadow fading could cause some violations of condition (15); however, we expect that if the number of SUs participating in the detection process is sufficiently high, such outlying RSS measurements will be averaged out in the computation of the test statistics. Notice that (15) implies the existence of an inverse relationship or negative correlation between RSS values and distances.

To carry out the PUE attack detection, a fusion node with complete location information collects RSS measurements from the SUs and uses them to look for possible violations of monotonicity constraint (15). If the CWSN network has been compromised by a PUE attack like those of Figure 1, the source of those packets will be the wormhole local node, whose position is, with a high probability, different from that of the PU, so that many of the measured RSSs will be in complete disagreement with the distances between the legitimate PU and the SUs.

As a measure of dissimilarity between distances and RSS measurements, we have used a slight modification of the classical Kendall tau distance [17], which is a metric that counts the number of pairwise disagreements between two lists. In our case, the test statistic counts the number of violations of monotonicity constraint (15) for every possible pair of PU to SU distances and the measured RSS values as

$$\begin{aligned} \tau(\mathbf{r}) = & \left| \left\{ (i, j), i < j : (r_i < r_j \wedge d(\mathbf{p}, \mathbf{s}_i) < d(\mathbf{p}, \mathbf{s}_j)) \right. \right. \\ & \left. \left. \vee (r_i > r_j \wedge d(\mathbf{p}, \mathbf{s}_i) > d(\mathbf{p}, \mathbf{s}_j)) \right\} \right|, \end{aligned} \quad (16)$$

where $|\Omega|$ denotes the cardinal number of a set Ω . As the test statistic $\tau(\mathbf{r})$ is a discrete random variable (it only takes integer values), the decision procedure should include two parameters to exactly obtain a predefined PFA: an integer detection threshold η and a real number γ (with $0 \leq \gamma \leq 1$), such that

$$P[\tau(\mathbf{r}) > \eta \mid H_0] + \gamma P[\tau(\mathbf{r}) = \eta \mid H_0] = P_{FA}, \quad (17)$$

where PFA is the desired probability of false alarm.

The number of comparisons between RSS measurements needed to obtain $\tau(\mathbf{r})$ in (16) is $\binom{N}{2}$, so the complexity of this test is approximately proportional to the square of the number of SUs.

Notice that the proposed test is not exactly a nonparametric version of the test described in Section 4.1: while the

sum of squares (11) tries to determine if the RSS observations are consistent with the PU position (assuming a particular path loss model), the Kendall tau distance (16) evaluates the correlation of the observed RSS values with the distances from the SUs to the PU transmitter.

5. Simulation Results

We have conducted some simulations to evaluate and compare the performance of the PUE attack detection strategies described in Sections 4.1 and 4.2. We consider a static scenario, where the location of a given network node is always modeled as a two-dimensional random variable, independent of the positions of other nodes, and uniformly distributed inside a region of the plane that depends on the type of the node and the simulated attack.

We consider three different types of nodes:

- (i) Secondary users: they constitute a CWSN composed of a set of N nodes at positions $\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_N$, deployed in an area modeled as a circle with radius R_s and centered around the coordinate origin.
- (ii) Primary user: it is a single transmitter located at position $\mathbf{p}$, which is assumed known by all the SUs.
- (iii) Attackers: they can be two malicious nodes (relay attack) or a single node (replay attack).

The locations of the PU and the attackers depend on the kind of attack:

Relay attack: the PU is located *outside* the deployment area of the SUs, so we choose its position $\mathbf{p}$ lying inside a ring with inner radius R_s and outer radius R_p (with $R_p > R_s$) and centered around the coordinate origin. Under this kind of attack, a wormhole is established between two malicious nodes: a remote receiver near the PU transmitter (whose exact position is irrelevant in our simulations) and a local wormhole transmitter located at a point $\mathbf{m}$ *inside* the deployment area of the SUs.

Replay attack: both the PU and the (single) attacker (at positions $\mathbf{p}$ and $\mathbf{m}$, resp.) are located *inside* the deployment area of the SUs.

In our simulations, we have chosen the following values for the location parameters: $R_s = 20$ m and $R_p = 40$ m.

On the other hand, the RSS values are computed using the log-distance path loss model (2), with parameter $\alpha = 2.3$, as suggested in [18]. We assume that both the PU and the attacker use the same transmission power, so the mean received power at unit distance K is the same in all cases.

For the simulated scenarios, we have conducted both the LRT (Algorithm 1) and the proposed nonparametric test (Algorithm 2). The detection thresholds are empirically obtained so that a predetermined PFA is obtained when no attack is present.

Some results are represented in Figure 2, where we have plotted the attained probability of detection for the PUE attack detection schemes of Sections 4.1 and 4.2 under

FIGURE 2: Probability of PUE attack detection using the proposed methods with varying path loss standard deviation ($P_{FA} = 0.05$ and $N = 40$). (a) Relay (wormhole) attack. (b) Replay (playback) attack.

Inputs:

PU position: $\mathbf{p}$
Set of SU positions: $\{\mathbf{s}_i, i = 1, 2, \dots, N\}$
Vector of RSS values: $\mathbf{r} = [r_1, r_2, \dots, r_N]^T$
Parameters of the path loss model: K and α
Detection threshold: η'

Steps:

- (1) Obtain the PU to SUs distances $\{d(\mathbf{p}, \mathbf{s}_i), i = 1, 2, \dots, N\}$.
- (2) Compute the test statistic $S(\mathbf{r})$ using (11).
- (3) **if** $S(\mathbf{r}) > \eta'$ **then**
- (4) $attack_flag \leftarrow true$
- (5) **else**
- (6) $attack_flag \leftarrow false$
- (7) **end if**
- (8) **return** $attack_flag$

ALGORITHM 1: Parametric PUE attack detection.

Inputs:

PU position: $\mathbf{p}$
Set of SU positions: $\{\mathbf{s}_i, i = 1, 2, \dots, N\}$
Vector of RSS values: $\mathbf{r} = [r_1, r_2, \dots, r_N]^T$
Detection threshold and “PFA adjustment” parameter: η, γ

Steps:

- (1) Obtain the PU to SUs distances $\{d(\mathbf{p}, \mathbf{s}_i), i = 1, 2, \dots, N\}$.
- (2) Compute the test statistic $\tau(\mathbf{r})$ using (16).
- (3) **if** $\tau(\mathbf{r}) > \eta$ **then**
- (4) $attack_flag \leftarrow true$
- (5) **else if** $\tau(\mathbf{r}) = \eta$ **then**
- (6) $attack_flag \leftarrow true$ with probability γ
- (7) **else**
- (8) $attack_flag \leftarrow false$
- (9) **end if**
- (10) **return** $attack_flag$

ALGORITHM 2: Nonparametric PUE attack detection.

different situations. The PFA is fixed at 0.05, the number of SUs was 40, and we conducted 1000 simulation runs with varying path loss standard deviation σ (that controls the effect of shadowing). In a real-world situation, the parametric approach requires a previous calibration phase during which the propagation model parameters (namely, the path loss exponent α and the mean received power at unit distance K) are estimated. So, for the case of the parametric test (LRT) of Section 4.1, we considered two situations: an ideal one that assumes that the environment is perfectly calibrated and the exact value of the path loss exponent α is known (perfect estimation) and another one that assumes that the value of α is underestimated by 10%, and so the PUE attack detector

uses in (11) a value of the path loss exponent that is slightly lower than the one used to generate the observations (biased estimation).

By examining Figure 2(a), we can observe that, for a relay attack, the parametric approach performs quite well as long as the path loss model parameters are well estimated; this can be easily explained because the local malicious node uses the same transmitting power as the remote PU, and so the values of the RSS at the SUs are usually too high to be accepted as originated from distant PU transmissions (assuming that shadowing effects are not too severe). On the contrary, the nonparametric test does not use any model parameters and so

it cannot be aware of the dissimilarity between the observed RSSs and their expected values provided by the path loss model. Notice, however, that when the model parameters used in the LRT depart from the “true” ones, the performance of the parametric test suffers a significant degradation and can be even surpassed by the nonparametric procedure.

In the case of a replay attack, we can see in Figure 2(b) that the nonparametric test achieves a comparable performance to that of the LRT and even performs better for moderately high values of the path loss standard deviation (specially if there is bias in the estimation of the model parameters). This is because, under this kind of attack, the LRT cannot take advantage of any significant differences between the average values of the RSSs induced by the attacker transmitter and those attributable to an active PU, as both the PU and the malicious node lie in the same region and, therefore, their averaged distances to the SUs are approximately the same. Notice also from Figure 2(b) that the detection performance of the LRT rapidly decreases with increasing shadowing, while the nonparametric attack detector only degrades smoothly. This may be explained because this latter detector is based on a nonparametric estimation of the correlation between the RSS measurements and the distances from the SUs to the PU, which appears to be fairly robust to significant deviations of the RSSs from their mean values due to channel impairments.

6. Conclusions

In this paper, we presented two models of PUE attacks to a CWSN that are resilient to naive defensive measures based on cryptographic protocols but can be effectively counteracted by using location information and RSS measurements. The attack detection process can be formulated as a problem of hypothesis testing for which we derived the LRT, assuming the RSS values follow a standard log-normal path loss model. In order to make the attack detection process robust to changing environmental conditions, we further proposed a nonparametric procedure that is not tied to any propagation model but instead assumes a simple monotonicity constraint for the RSS values. Simulations suggest that the nonparametric test can compete in performance with the parametric scheme and even performs better under moderate shadowing conditions or significant departures from the assumed measurement model, specially in case of replay attacks.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This research was partially supported by the Spanish Ministry of Economy and Competitiveness under Grant TEC2012-38402-C04-01.

References

- [1] S. Haykin, “Cognitive radio: brain-empowered wireless communications,” *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, 2005.
- [2] 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, 2008.
- [3] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, “A survey on security threats and detection techniques in cognitive radio networks,” *IEEE Communications Surveys and Tutorials*, vol. 15, no. 1, pp. 428–445, 2013.
- [4] Y.-C. Hu, A. Perrig, and D. Johnson, “Wormhole attacks in wireless networks,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 370–380, 2006.
- [5] Z. Jin, S. Anand, and K. P. Subbalakshmi, “Detecting primary user emulation attacks in dynamic spectrum access networks,” in *Proceedings of the IEEE International Conference on Communications (ICC '09)*, Dresden, Germany, June 2009.
- [6] Z. Yuan, D. Niyato, H. Li, J. B. Song, and Z. Han, “Defeating primary user emulation attacks using belief propagation in cognitive radio networks,” *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 10, pp. 1850–1860, 2012.
- [7] X. Xie and W. Wang, “Detecting primary user emulation attacks in cognitive radio networks via physical layer network coding,” *Journal of Ubiquitous Systems and Pervasive Networks*, vol. 5, no. 1, pp. 1–8, 2014.
- [8] J. Blesa, E. Romero, A. Rozas, A. Araujo, and O. Nieto-Taladriz, “PUE attack detection in CWSN using collaboration and learning behavior,” *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 815959, 8 pages, 2013.
- [9] A. Alahmadi, M. Abdelhakim, J. Ren, and T. Li, “Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard,” *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 772–781, 2014.
- [10] Y. Liu, P. Ning, and H. Dai, “Authenticating primary users’ signals in cognitive radio networks via integrated cryptographic and wireless link signatures,” in *Proceedings of the 31st IEEE Symposium on Security and Privacy (SP '10)*, pp. 286–301, Oakland, Calif, USA, May 2010.
- [11] O. R. Afolabi, K. Kim, and A. Ahmad, “On secure spectrum sensing in cognitive radio networks using emitters electromagnetic signature,” in *Proceedings of the 18th International Conference on Computer Communications and Networks (ICCCN '09)*, pp. 1–5, IEEE, San Francisco, Calif, USA, August 2009.
- [12] N. T. Nguyen, R. Zheng, and Z. Han, “On identifying primary user emulation attacks in cognitive radio systems using nonparametric Bayesian classification,” *IEEE Transactions on Signal Processing*, vol. 60, no. 3, pp. 1432–1445, 2012.
- [13] Y. Sharaf-Dabbagh and W. Saad, “Transfer learning for device fingerprinting with application to cognitive radio networks,” in *Proceedings of the 26th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC '15)*, pp. 2333–2337, IEEE, Istanbul, Turkey, September 2015.
- [14] M. García-Otero and A. Población-Hernández, “Secure neighbor discovery in wireless sensor networks using range-free localization techniques,” *International Journal of Distributed Sensor Networks*, vol. 2012, Article ID 763187, 12 pages, 2012.

- [15] T. S. Rappaport, *Wireless Communications: Principles and Practice*, Prentice Hall PTR, Upper Saddle River, NJ, USA, 2nd edition, 2002.
- [16] S. M. Kay, *Fundamentals of Statistical Signal Processing, Volume II: Detection Theory*, Prentice Hall PTR, Upper Saddle River, NJ, USA, 1998.
- [17] M. Kendall and A. Stuart, *The Advanced Theory of Statistics*, vol. 2, Charles Griffin, London, UK, 1979.
- [18] N. Patwari, A. O. Hero III, M. Perkins, N. S. Correal, and R. J. O'Dea, "Relative location estimation in wireless sensor networks," *IEEE Transactions on Signal Processing*, vol. 51, no. 8, pp. 2137–2148, 2003.