Defense against Primary User Emulation Attacks in Cognitive Radio Networks

Ruiliang Chen, Jung-Min Park, and Jeffrey H. Reed
Bradley Department of Electrical and Computer Engineering
Virginia Polytechnic Institute and State University
Blacksburg, VA 24061
{rlchen, jungmin, reedjh}@vt.edu

***Abstract*—Cognitive Radio (CR) is a promising technology that can alleviate the spectrum shortage problem by enabling unlicensed users equipped with CRs to coexist with incumbent users in licensed spectrum bands while causing no interference to incumbent communications. Spectrum sensing is one of the essential mechanisms of CRs and its operational aspects are being investigated actively. However, the security aspects of spectrum sensing have garnered little attention. In this paper, we identify a threat to spectrum sensing, which we call the *primary user emulation (PUE) attack*. In this attack, an adversary's CR transmits signals whose characteristics emulate those of incumbent signals. The highly flexible, software-based air interface of CRs makes such an attack possible. Our investigation shows that a PUE attack can severely interfere with the spectrum sensing process and significantly reduce the channel resources available to legitimate unlicensed users. To counter this threat, we propose a transmitter verification scheme, called *LocDef (localization-based defense)*, which verifies whether a given signal is that of an incumbent transmitter by estimating its location and observing its signal characteristics. To estimate the location of the signal transmitter, LocDef employs a *non-interactive localization* scheme. Our security analysis and simulation results suggest that LocDef is effective in identifying PUE attacks under certain conditions.**

***Index Terms*—Cognitive Radio, Communication System Security, Primary User Emulation Attack, Localization, Spectrum Sensing, Wireless Sensor Network.**

I. Introduction

The need to meet the ever-increasing spectrum demands of emerging wireless applications and the need to better utilize spectrum have led the Federal Communications Commission (FCC) to revisit the problem of spectrum management. In the conventional spectrum management paradigm, most of the spectrum is allocated to licensed users for exclusive use. Recognizing the significance of the spectrum shortage problem, the FCC is considering opening up licensed bands to unlicensed operations on a non-interference basis to licensed users. In this new paradigm, unlicensed users (a.k.a. secondary users) "opportunistically" operate in fallow licensed spectrum bands without interfering with licensed users (a.k.a. primary or incumbent users), thereby increasing the efficiency of spectrum utilization. This method of sharing is often called *Dynamic Spectrum Access* (DSA).

A preliminary version of portions of this material has been presented in [6]. This work was supported in part by the National Science Foundation under grants CNS-0627436 and CNS-0716208.

Manuscript received 2 Feb. 2007; revised 26 Aug. 2007; accepted 29 Sept. 2007.

Cognitive Radios (CRs) [12], [17] are seen as the enabling technology for DSA. Unlike a conventional radio, a CR has the capability to sense and understand its environment and proactively change its mode of operation as needed. CRs are able to carry out *spectrum sensing* for the purpose of identifying fallow licensed spectrum—i.e., spectrum "white spaces". Once white spaces are identified, CRs opportunistically utilize these white spaces by operating in them without causing interference to primary users.

The successful deployment of CR networks and the realization of their benefits will depend on the placement of essential security mechanisms in sufficiently robust form to resist misuse of the system. Ensuring the trustworthiness of the spectrum sensing process is a particularly important problem that needs to be addressed. The key to addressing this problem is being able to distinguish primary user signals from secondary user signals in a robust way. Recall that, in a CR network, secondary users are permitted to operate in licensed bands only on a non-interference basis to primary users. Because the primary users' usage of licensed spectrum bands may be sporadic, a CR must constantly monitor for the presence of primary user signals in the current operating band and candidate bands. If a secondary user (with a CR) detects the presence of primary user signals in the current band, it must immediately switch to one of the fallow candidate bands. On the other hand, if the secondary user detects the presence of an unlicensed user, it invokes a coexistence mechanism[1] to share spectrum resources.

The above scenarios highlight the importance of a CR's ability to distinguish between primary user signals and secondary user signals. Distinguishing the two signals is non-trivial, but it becomes especially difficult when the CRs are operating in hostile environments. In a hostile environment, an attacker may modify the air interface of a CR to mimic a primary user signal's characteristics, thereby causing legitimate secondary users to erroneously identify the attacker as a primary user. We coin the term *primary user emulation (PUE) attack* to refer to this attack. There is a realistic possibility of PUE attacks since CRs are highly reconfigurable due to their software-based air interface [12]. To thwart such attacks, a scheme that can reliably distinguish between legitimate primary signal

[1]For example, in IEEE 802.22, the Coexistence Beacon Protocol is used to achieve self-coexistence amongst overlapping 802.22 cells.

transmitters and secondary signal transmitters masquerading as primary users is needed. In hostile environments, such a scheme should be integrated into the spectrum sensing mechanism to enhance the trustworthiness of the sensing result.

The current research and standardization efforts suggest that one of the first applications of CR technology will be its use for DSA of fallow TV spectrum bands. FCC is considering opening up TV bands for DSA because TV bands often experience lower and less dynamic utilization compared to other primary user networks such as cellular networks [9]. In the paper, we focus on a scenario in which a primary user network is composed of TV transmission towers and receivers placed at fixed locations. In such a setting, the *location* of a given transmitter (along with other factors) can be utilized to determine whether the transmitter is a primary transmitter or a PUE attacker.

Estimating the location of a wireless device is a well studied problem [7], [13], [15], [18], [26]. However, localization of primary user transmitters in the context of DSA is not a trivial problem when one considers the requirement prescribed by FCC [8], which states that *no modification to the incumbent system should be required to accommodate opportunistic use of the spectrum by secondary users.* For this reason, conventional approaches, such as embedding signed location information in a primary user's signal or employing an interactive protocol between an primary signal transmitter and a localization device, cannot be used.

In this paper, we propose a transmitter verification scheme, called *LocDef (localization-based defense)*, which utilizes both signal characteristics and location of the signal transmitter to verify primary signal transmitters. A robust *non-interactive localization* scheme is introduced to detect PUE attacks and pinpoint PUE attackers. The localization scheme utilizes an underlying wireless sensor network (WSN) to collect snapshots of received signal strength (RSS) measurements across a CR network. By smoothing the collected RSS measurements and identifying the RSS peaks, one can estimate the the transmitter locations. We describe, in detail, the technique for localizing transmitters both in and out of the range of the WSN. We also discuss the security properties of the localization scheme and evaluate its performance using simulations.

The main contribution of this work is twofold. First, we identify a security issue that poses a serious threat to CR networks. The existing body of research on CR network security is very small. The work presented in this paper is a contribution to this body of research. Second, the paper proposes LocDef as a transmitter verification scheme that is capable of detecting PUE attacks and pinpointing PUE attackers. As the core component of LocDef, the proposed non-interactive localization scheme can be employed in hostile environments. LocDef can be integrated into existing spectrum sensing schemes to enhance the trustworthiness of the sensing decisions.

The rest of the paper is organized as follows. In Section II, we describe the PUE attack in detail. In Section III, we present the high-level structure of LocDef. As a major component of LocDef, a robust non-interactive localization scheme is detailed and its security properties are discussed in Section IV. Simulation results are shown in Section V and related research is summarized in Section VI. In Section VII, we conclude the paper and discuss future work.

II. Security Threats in CR Networks and the PUE Attack

The emergence of the DSA paradigm and software/cognitive radio technology raises new security implications. The distinguishing aspects of CR systems and networks can be exploited or attacked by adversaries. For instance, spectrum access-related functionalities of CR networks are vulnerable to attacks. Besides the PUE attack, spectrum access-related security threats include attacks against cooperative spectrum sensing [11], [16], [24], [27] and attacks against self-coexistence mechanisms. Although cooperative spectrum sensing can significantly improve the accuracy of spectrum sensing compared to individual sensing, it raises a security concern: a subset of the CR terminals may report false sensing measurements due to malfunctioning or malicious radio software, thus increasing the likelihood of incorrect sensing decisions. The problem of devising a cooperative spectrum sensing scheme that is robust against such a threat is challenging. Self-coexistence mechanisms are needed in overlapping coverage areas of CR networks to minimize self-interference and utilize spectrum efficiently. Unfortunately, adversaries can modify/forge self-coexistence control packets to exploit self-coexistence mechanisms, which can result in drastic reduction of network capacity. What makes the task of protecting self-coexistence control packets, using conventional cryptosystems, difficult is the need to use an "inter-operator" key management system. It is likely that the networks that contend for spectrum (via self-coexistence mechanisms) will be managed by different wireless service operators. Designing and maintaining an inter-operator key management system could be complex and expensive. In addition to spectrum access-related security threats, software-centric signal processing by (software-based) CR systems also raises new security implications. For instance, the download process of the radio software needs to be secured. Moreover, the radio software itself needs to be tamper resistant once it is downloaded on the radio terminal so that software changes cannot be made to cause a radio to operate with parameters outside of those that were approved. To date, most of the aforementioned problems, especially spectrum access-related security threats, have not been addressed—in this paper, we address one of them: PUE attacks.

One of the major technical challenges in spectrum sensing is the problem of precisely distinguishing primary user signals from secondary user signals. To distinguish the two signals, existing spectrum sensing schemes based on energy detectors [5], [19] implicitly assume a "naive" transmitter verification scheme. When energy detection is used, a secondary user can recognize the signals of other secondary users but cannot recognize primary user signals. When a secondary user detects a signal that it recognizes, it assumes that the signal is that of a secondary user; otherwise it determines that the signal is that

of a primary user. Under such an overly simplistic transmitter verification scheme, a selfish or malicious secondary user (i.e., an attacker) can easily exploit the spectrum sensing process. For instance, a PUE attacker may "masquerade" as an primary user by transmitting unrecognizable signals in one of the licensed bands, thus preventing other secondary users from accessing that band.

There exist alternative techniques for spectrum sensing, such as matched filter and cyclostationary feature detection [4]. Devices capable of such detection techniques are able to recognize the intrinsic characteristics of primary user signals, thus enabling them to distinguish those signals from those of secondary users. However, such detection techniques are still not robust enough to counter PUE attacks. To defeat cyclostationary detectors, an attacker may make its transmissions indistinguishable from primary user signals by transmitting signals that have the same cyclic spectral characteristics as primary user signals. For example, when the nodes of a TV broadcast network are primary users, an attacker may emit signals that emulate TV signals. This attack scenario is possible since low-power, portable TV UHF transmitters can be readily obtained as commercial off-the-shelf (COTS) products. If an attacker uses such a transmitter to transmit signals, CRs that receive the signal will falsely identify the attacker's signal as that of a primary user[2].

In PUE attacks, the adversary only transmits in fallow bands. Hence, the aim of the attackers is not to cause interference to primary users, but to preempt spectrum resources that could have been used by legitimate secondary users. Depending on the motivation behind the attack, a PUE attack can be classified as either a selfish PUE attack or a malicious PUE attack.

- *Selfish PUE attacks*: In this attack, an attacker's objective is to maximize its own spectrum usage. When selfish PUE attackers detect a fallow spectrum band, they prevent other secondary users from competing for that band by transmitting signals that emulate the signal characteristics of primary user signals. This attack is most likely to be carried out by two selfish secondary users whose intention is to establish a dedicated link.
- *Malicious PUE attacks*: The objective of this attack is to obstruct the DSA process of legitimate secondary users—i.e., prevent legitimate secondary users from detecting and using fallow licensed spectrum bands, causing denial of service. Unlike a selfish attacker, a malicious attacker does not necessarily use fallow spectrum bands for its own communication purposes. It is quite possible for an attacker to simultaneously obstruct the DSA process in multiple bands by exploiting two DSA mechanisms implemented in every CR. The first mechanism requires a CR to wait for a certain amount of time before transmitting in the identified fallow band to make sure that the band is indeed unoccupied. Existing research shows that this time delay is non-negligible [5], [24]. The second mechanism requires a CR to periodically sense the current operating band to detect primary user signals and to immediately switch to another band when such signals are detected. By launching a PUE attack in multiple bands in a round-robin fashion, an attacker can effectively limit the legitimate secondary users from identifying and using fallow spectrum bands.

Both attacks could have disruptive effects on CR networks. (Their disruptive effects will be studied using simulation in Section V.) To thwart PUE attacks, one needs to first detect the attack. In the next section, we describe a transmitter verification scheme that can be integrated into a spectrum sensing scheme to detect PUE attacks under certain conditions.

III. A Transmitter Verification Scheme for Spectrum Sensing

Before describing the transmitter verification scheme for spectrum sensing, we state some of the assumptions that form the foundation of the scheme. The primary user is assumed to be a network composed of TV signal transmitters (i.e., TV broadcast towers) and receivers. A TV tower's transmitter output power is typically hundreds of thousands of Watts [27], which corresponds to a transmission range from several miles to tens of miles. We assume that the secondary users, each equipped with a hand-held CR device, form a mobile ad hoc network. Each CR is assumed to have self-localization capability and have a maximum transmission output power that is within the range from a few hundred milliwatts to a few watts—this typically corresponds to a transmission range of a few hundred meters. An attacker, equipped with a CR, is capable of changing its modulation mode, frequency, and transmission output power.

Based on the above assumptions, we propose a transmitter verification scheme for spectrum sensing that is appropriate for hostile environments; the transmitter verification scheme is illustrated in Fig. 1. In the network model under consideration, the primary signal transmitters are TV broadcast towers placed at fixed locations. Hence, if a signal source's estimated location deviates from the known location of the TV towers and the signal characteristics resemble those of primary user signals, then it is likely that the signal source is launching a PUE attack. An attacker, however, can attempt to circumvent this location-based detection approach by transmitting in the vicinity of one of the TV towers. In this case, the signal's energy level in combination with the signal source's location is used to detect PUE attacks. It would be infeasible for an attacker to mimic both the primary user signal's transmission location and energy level since the transmission power of the attacker's CR is several orders of magnitude smaller than that of a typical TV tower. Once an instance of a PUE attack has been detected, the estimated signal location can be further used to pinpoint the attacker.

As Fig. 1 shows, the transmitter verification scheme includes three steps: verification of signal characteristics, measurement of received signal energy level, and localization of the signal source. To date, the technical problems related to the first two steps, in the context of CR networks, have attracted a

[2]Note that a TV UHF transmitter may not be very energy efficient. For example, today's typical 2.2W TV UHF transmitter requires a 20W power supply.

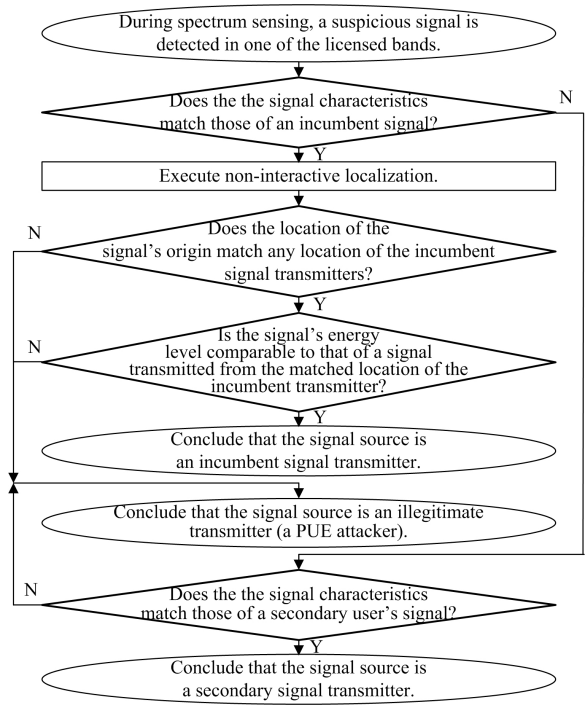


Fig. 1. A flowchart of the transmitter verification scheme.

lot of attention [1]. In contrast, there is very little existing research that directly addresses the third step. Therefore, in the following discussions, we focus on the problem of transmitter localization. This problem—called by various names such as location estimation, location identification, localization, positioning etc.—has been studied extensively in the past. The primary signal transmitter localization problem (which is referred to as the *PST localization problem* hereafter), however, is more challenging for two reasons. First, the following requirement must be met: no modification should be made to primary users to accommodate the DSA of licensed spectrum. Because of this requirement, including location information in a primary user's signal is not a viable solution. The requirement also excludes the possibility of using a localization protocol that involves interaction between a primary user and the localization device(s). Thus, the PST localization problem becomes a *non-interactive* localization problem. Second, it is the transmitter but not the receiver that needs to be localized. When a receiver is localized, one does not need to consider the existence of other receivers. However, the existence of multiple transmitters may add difficulty to transmitter localization. In the next section, we describe the proposed solution to the non-interactive PST localization problem in detail.

IV. Non-interactive Localization of Primary Signal Transmitters

A. Existing Localization Techniques

Before introducing the proposed localization system, in this subsection, we first summarize conventional localization techniques in wireless networks and then discuss how these techniques should be improved to address the PST localization problem in CR networks.

The conventional localization approaches are based on one or several of the following techniques: Time of Arrival (TOA), Time Difference Of Arrival (TDOA), Angle of Arrival (AOA), and RSS.

GPS [26] is a typical localization system based on TOA. A mobile node receives signals from satellites that contain their location and time information. Based on the information, the node can calculate its own position.

TDOA is a passive localization technique that utilizes the difference between the arrival times of pulses transmitted by a transmitter but does not rely on any knowledge of the pulse transmission time. The technique measures the time differences at multiple receivers with known locations and subsequently computes a location estimate [7].

In the AOA technique, a receiver measures the angel of arrival from two or more transmitters. If the locations of the transmitters are known, the receiver can calculate its own location using triangulation [18]. Using the same principle, angle of arrival information to multiple receivers can be used to determine the transmitter's location.

RSS-based localization techniques arise from the fact that there is a strong correlation between the distance of a wireless link and RSS [15], [20]. Specifically, given a transmitter-receiver pair, RSS can be modeled as a function of transmitted power and transmitter-receiver distance. Therefore, if a correct model is used and there are multiple observers taking RSS measurements from a transmitter, then the transmitter location can be estimated using the model. For example, Wireless E911 [10] uses "location signature" for localization, i.e., stores and matches multipath patterns (fingerprints) that mobile phone signals are known (via on-site calibration) to exhibit at different locations.

Among the above techniques, TOA is a receiver-localization technique and needs to be enhanced to support transmitter localization so that it can be applied to the PST localization problem. Such an enhancement is not trivial, especially when one considers the possibility that a malicious transmitter may craft its transmitted signal. TDOA and AOA techniques can both be used for transmitter localization and have relatively high localization precision. To apply them to the PST localization problem, special care must be taken to consider the situations where multiple transmitters or an attacker equipped with a directional antenna exists. The common drawback of both techniques is the requirement of expensive hardware, preventing them from a large-scale deployment. In contrast, RSS-based techniques are more practical for most consumer premise devices in a CR network. However, for the PST localization problem in CR networks, one should also consider the issues of possible manipulation of a malicious transmitter or multiple transmitters and the innate inaccuracy of RSS measurement. In the following subsections, we show that these issues can be addressed by taking many RSS measurements and properly processing the measured RSS data.

B. Architecture of the Localization System

The basic idea of the proposed localization system uses the fact that the magnitude of an RSS value typically decreases

as the distance between the signal transmitter and the receiver increases [13]. Therefore, if one is able to collect a sufficient number of RSS measurements from a group of receivers spread throughout a large network, the location with the peak RSS value is likely to be the location of a transmitter. The advantage of this technique is twofold, when it is used for the PST localization problem in CR networks: it both obviates modification of primary users and supports localizing multiple transmitters that transmit signals simultaneously.

The requirement to collect RSS distribution in a network naturally leads us to resort to an underlying WSN that can help collect RSS measurements across the network. It should be noted that the idea of using an underlying WSN to facilitate the operation of a CR network is not new. For example, in [24], it was proposed that a spectrum-aware sensor network be used for distributed spectrum sensing, so that the sensor network can provide secondary users with information about spectrum opportunities throughout a network. If sensor nodes in a WSN have the capability to measure RSS and are aware of their positions [13], they can be used to solve the PST localization problem. However, there are two problems that need to be addressed in order for the aforementioned approach to be viable.

First, path fading may change over time and a PUE attacker may constantly change its location or vary its transmission power to evade localization, thus causing RSS measurements to fluctuate drastically within a short period of time. This problem cannot be mitigated by taking the average of measurements taken at different times, since the RSS values measured at a given position at different times have different distributions. A possible solution to this problem is to take a "snapshot" of the RSS distribution in a given network, i.e., requiring the sensors of a WSN to take a synchronized RSS measurements in a given band.

The second problem arises from the fact that RSS usually varies by a large magnitude (30dB to 40dB) [20] over short distances. This makes it very challenging to decide the location of primary users just by reading the raw data in a snapshot of RSS distribution. We conducted a simulation experiment to illustrate this problem. A 2000m$\times$2000m network with two transmitters located at (800m, 1800m) and (1300m, 550m) was simulated. Each transmitter's transmission power was 500mW, working at the UHF frequency of 617MHz. The phase shift between the two transmitters was randomly chosen. A statistical log-loss signal propagation model, which was shown to be appropriate for modeling signal propagation behavior in many situations [23], was employed in the simulation. In this model, the expected RSS in decibels is given by:

$$\mu = p + \beta_0 + \beta_1 \ln s, \tag{1}$$

where s is the transmitter-receiver distance, p is the transmitted power in decibels, and β_0 and β_1 are constant parameters that need to be calibrated for a specific environment. Note that this is offsite calibration, and no onsite calibration is required [23]. In the offsite calibration, one needs to tune the parameters related to the channel environment (e.g., rural, urban, etc.). Using the model, the distribution of RSS is characterized as a Gaussian random variable with a mean of μ and a variance of σ^2. In [23], a set of parameters approximating real-world results were used, where (β_0, β_1, σ) = (-30.00, -10.00, 10.0). We used the same set of parameters for our simulation. Fig. 2(a) shows a snapshot of the RSS in dBm. It can be seen that because of the large variance of the RSS, the snapshot does not reveal obvious RSS peaks (which can be used as approximations for the transmitter locations).

However, if the variance can be reduced to a sufficiently low level, the snapshot would clearly indicate the RSS peaks as illustrated in Fig. 2(b). It is therefore reasonable to conjecture that if one is able to decrease the variance using an appropriate *data smoothing* technique, it may be possible to solve the PST localization problem by using the aforementioned localization approach. In the next subsection, we focus on the design of such a data smoothing technique.

C. The RSS smoothing procedure

Data smoothing techniques [25] aim to capture important patterns in raw data, while leaving out noise. By smoothing a snapshot of an RSS distribution in a network, one can decrease the variance in the raw RSS measurements, thus making it possible to identify the RSS peaks.

There are three data smoothing techniques that are usually used to eliminate noise: local averaging, Fourier filters, and loess fitting. In our RSS smoothing problem, robustness against outliers is an important requirement for two reasons. First, the large variance in RSS measurements may result in a large number of outliers. Second, when an adversarial environment is considered, compromise of sensor nodes may lead to false data injection. Among the three data smoothing techniques, Fourier filters is known to be vulnerable to large variation. Loess fitting requires a large, densely sampled dataset and its robustness against outliers depends on careful design of the weight mechanism used for computing least squares [25]. In contrast, local averaging, especially when the median value is taken, provides the best robustness against outliers. Therefore, we use local averaging, using median values, to smooth RSS measurement data. The details of the smoothing technique are described below.

Without loss of generality, we assume that the coverage area of the WSN is identical to that of a CR network under consideration, which covers an area of $D_x \times D_y$ (m^2). Suppose that we sample a group of "pivot" points that are placed at the intersections of the vertical and horizontal lines of a two-dimensional grid, where each element on the grid is a square with a side of length d. For each pivot point we calculate a "smoothed" RSS value by calculating the median value from the set of RSS measurements collected by neighboring sensor nodes that are located inside an area enclosed by a circle of radius r centered at the pivot point. See Fig. 3 for an illustration of how the pivot points are positioned. (Note that the centers of the circles marked with "1's" denote pivot point positions.) Once data smoothing is applied to RSS measurements, one can estimate the positions of the primary signal transmitters by identifying the positions of the pivot points that generate "peak" median values.

Next we discuss the details of how to set the values of r and d and how to identify RSS peak values. We discuss these

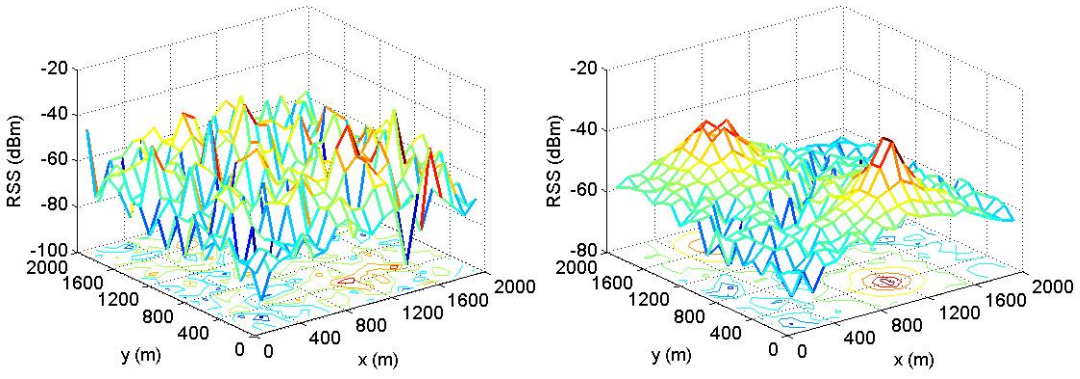


Fig. 2. RSS distributions obtained from the underlying WSN. (a) A snapshot of the RSS raw-data distribution. (b) The RSS distribution in the network when $\sigma = 0$.

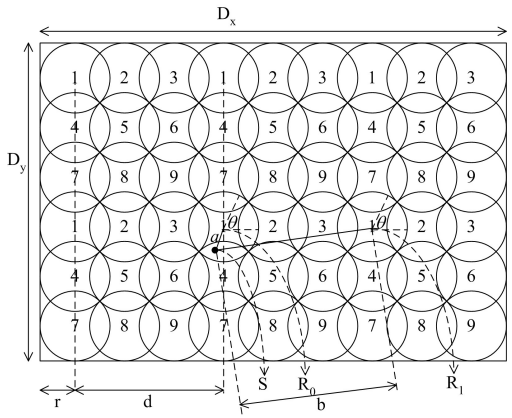


Fig. 3. Using local averaging to smooth RSS measurement.

problems in the context of the statistical log-loss propagation model described in Subsection IV-B. We assume that the values of β_1 and σ have been estimated[3], and the density of the sensor nodes is ρ (m^{-2}). Suppose that a primary signal transmitter S is transmitting inside an area defined by a circle of radius r centered at pivot point x. Our objective is to derive the values of r and d so that the median RSS value calculated from x is greater than the RSS value calculated from its neighboring pivot points, which are located at a distance of d from point x, by at least mdB at a confidence level of P.

Suppose the circular region of radius r centered at x is R_0, and let R_1 denote a circular region centered at a neighboring pivot point that is at a distance of d (see Fig. 3). In R_0, the expected RSS after averaging[4] is:

$$\begin{aligned}\mu_0 &= E[p + \beta_0 + \beta_1 \ln s] \\ &= p + \beta_0 + \tfrac{\beta_1}{\pi r^2} \int_0^{2\pi}\int_0^{r} \ln \sqrt{(r\cos\theta + a)^2 + (r\sin\theta)^2}\, r dr d\theta,\end{aligned} \tag{2}$$

where a is the distance between the transmitter to the center of R_0. Because $a \le r$ and $\beta_1 < 0$, it holds that

$$\begin{aligned}\mu_0 &\ge p + \beta_0 + \tfrac{\beta_1}{\pi r^2} \int_0^{2\pi}\int_0^{r} \ln \sqrt{(r\cos\theta + r)^2 + (r\sin\theta)^2}\, r dr d\theta \\ &> p + \beta_0 + \beta_1 \ln \tfrac{1}{\pi r^2} \int_0^{2\pi}\int_0^{r} \sqrt{(r\cos\theta + r)^2 + (r\sin\theta)^2}\, r dr d\theta \\ &= p + \beta_0 + \beta_1 \ln \tfrac{8r}{3\pi}.\end{aligned} \tag{3}$$

Similarly, in R_1, the expected RSS after averaging is

$$\mu_1 = p + \beta_0 + \tfrac{\beta_1}{\pi r^2} \int_0^{2\pi}\int_0^{r} \ln \sqrt{(r\cos\theta + b)^2 + (r\sin\theta)^2}\, r dr d\theta \tag{4}$$

where b is the distance between the transmitter and the center of R_1. It holds that $b \ge d - r$. If we further assume that $d > 2r$, it is obvious that

$$\mu_1 < p + \beta_0 + \beta_1 \ln(d - 2r). \tag{5}$$

The results from (3) and (5) enable us to calculate a loose lower bound of the difference between the medians of measured RSS values in R_0 and R_1:

$$\Delta\mu = \mu_0 - \mu_1 > |\beta_1| \ln[\pi(\frac{3d}{8r} - \frac{3}{4})]. \tag{6}$$

Because the RSS measurement can be modeled as a Gaussian random variable [15], [23], $\Delta\mu$ is also a Gaussian random variable. It has a mean of $\mu_0 - \mu_1$ and a variance of $2\sigma^2/(\rho\pi r^2)$. To obtain a sufficient condition that guarantees the difference is greater than m at a confidence level P, we first define a variable x_0 that satisfies:

$$Q(x_0) = 1 - P, \tag{7}$$

where the Q-function represents the right-tail probability of a normalized Gaussian variable. Then based on the properties of Gaussian variables, a sufficient condition can be derived:

$$\frac{|\beta_1| \ln[\pi(\frac{3d}{8r} - \frac{3}{4})] - m}{\sqrt{2}\sigma} \cdot \sqrt{\rho\pi} r \ge x_0. \tag{8}$$

The values of d and r should satisfy the above condition so that solving the PST localization problem in CR networks becomes equivalent to finding the circular regions whose median RSS

[3]As mentioned before, the two values can be estimated using the offsite calibration technique presented in [23].

[4]Note that for a random variable with Gaussian distribution, its median is equal to its mean.

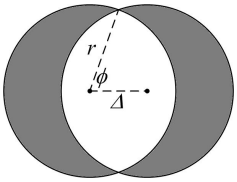


Fig. 4. Illustration of calculating the sample interval.

value is at least mdB greater than those in its neighboring regions (i.e., the closest region that is sampled in the same round) that are at a distance of d. If the the topology of WSN varies, an easy way to adjust the values of d and r is to keep d/r as a constant while changing the value of r to satisfy (8).

Because the above derivation assumed $d > 2r$, the sampled regions cannot cover the entire coverage area of the WSN. Therefore, multiple rounds of sampling should be performed. Fig. 3 shows how multiple rounds (nine in total) of sampling cover the whole area. It is obvious that the total number of rounds will be $O = \left\lceil d/(\sqrt{2}r)\right\rceil^2$ and the distance between two neighboring samplings will be d/O.

After all rounds of samplings are finished, a set of regions are identified to have a median RSS value that is at least mdB greater than those in its neighboring regions sampled in the same round. This set, R, indicates the approximate locations of the primary signal transmitters. Next we need to sample more points within the sets to obtain more precise locations. The following steps are executed for this purpose:

1) Group the regions in R into a minimum number of mutually exclusive sets $R_1, R_2, \ldots, R_T$ so that all regions in each set R_v ($v = 1, 2, \ldots, T$) are interconnected[5].
2) For the area covered by each R_v, sample all points that are horizontally or vertically apart by $(w \cdot \Delta)$, where w is an integer and Δ is a sample interval determined by the sensor density ρ (see below). For each sampled point, the median is calculated for the RSS measurements over a circular region centering the point with radius r. The location of the point with the maximum median RSS value in R_v is the estimated location of a primary signal transmitter.

Now, we explain how to decide the value of Δ. The value of Δ needs to be sufficiently large so that computation overhead is not exorbitant, while being small enough to capture all possible variations in RSS measurements between adjacent samples. Therefore, an appropriate strategy is to expect exactly one sensor to exist in the non-overlapping area of two circles centered at two adjacent sampled points. In Fig. 4, this means that there is one sensor in the shaded area, which results in the following condition for choosing Δ:

$$2\rho[(\pi - 2\phi)r^2 + r\Delta\sin\phi] = 1, \tag{9}$$

where $\phi = \arccos[\Delta/(2r)]$.

[5]Suppose we use a set of regions to form a graph. The center of each region is denoted as a vertex. An edge between two vertexes is drawn if the corresponding two regions intersect. The set of regions is said to be interconnected if and only if the formed graph is a connected graph.

D. The Special Case of Out-of-range Primary Users

When an estimated location of a primary signal transmitter appears close to the border of the WSN, it is possible that the transmitter is a legitimate user located out of the WSN[6]. Given this special case, it is necessary to distinguish whether a detected transmitter is a PUE attacker located on the border of the WSN or it is a transmitter of a primary user that is located out of the range of the WSN. We assume that a primary user's location is known ahead of time, since only TV systems are considered and the location of a TV tower is public information. Then we develop the following approach to compute the likelihood that a detected signal is coming from the primary user's location and from the border of the WSN. By comparing the likelihoods of the two events, one can derive the transmitter's location.

Assume that one transmitter's position derived in Subsection IV-C to be (X_1, Y_1). When (X_1, Y_1) is located close to the border of the deployed WSN, we want to know whether it is more probable that the transmitter is in fact at a known position (X_2, Y_2) that is out of the range of the WSN. Assume that the RSS measurement in the WSN has been smoothed by taking the median of the RSS values within a circular region of radius r. We randomly sample K smoothed measurements across the WSN, with each measurement corresponding to a location (x_k, y_k) and a smoothed RSS value R_k (in dBm) from n_k sensors in the region, where $k = 1, \ldots, K$. As discussed before, since a reasonable sampling space is Δ, when all sampling possibilities are considered, the maximum K will be $D_x D_y/\Delta^2$. Then a two-step process is executed to calculate the likelihood that the transmitter is from (X_h, Y_h), where $h = 1, 2$. In the first step, a linear optimization operation is executed to make an estimation of transmission power p_h, in which the difference between the smoothed RSS values and what are predicted by the log-loss signal propagation model is minimized.

$$\begin{aligned} &\min \sum_{k=1}^{K} (u_k + o_k) \\ &\text{s.t.} \forall k = 1, ..., K : \\ &R_k + u_k - o_k \\ &\quad = p_h + \beta_0 + \beta_1 \ln \sqrt{(X_h - x_k)^2 + (Y_h - y_k)^2} \\ &u_k, o_k \geq 0. \end{aligned} \tag{10}$$

The variables u_k and o_k both represent the absolute difference between R_k and the value predicted by the model. The formulation of the above linear optimization problem mandates that when R_k is greater than what is predicted by the model, u_k is zero and o_k is the difference. When R_k is smaller, o_k is zero and u_k is the difference. The solution to (10) generates an estimated p_h. With the knowledge of p_h, the normalized difference for the scenario that the transmitter is located at (x_h, y_h) is computed as

$$D_h \quad = \quad \frac{1}{K} \sum_{k=1}^{K} |R_k - p_h - \beta_0$$

[6]Note that since a PUE attacker transmits at relatively low transmission power, the attacker has been assumed to be always within the range of the CR network and its underlying WSN so that the attack remains effective.

$$-\beta_1 \ln \sqrt{(X_h - x_k)^2 + (Y_h - y_k)^2} \Big| \frac{\sqrt{n_k}}{\sigma}. \tag{11}$$

When (X_h, Y_h) is indeed the transmitter's location, the expected value of each item in the summation should approach zero. In contrast, if (X_h, Y_h) is not the transmitter's location, each item in the summation will deviate from zero. Therefore, D_h can be used to compare the likelihoods that the transmitter is at specific locations—i.e., the location of the transmitter is decided to be (X_{h_0}, Y_{h_0}), where

$$h_0 = \arg\min_h D_h. \tag{12}$$

E. Security Analysis

In this subsection, we explore the security aspects of the proposed localization system in a hostile environment. In particular, we consider two categories of potential attacks and analyze their impacts.

The first category of attacks aim to escape localization by disrupting RSS measurements. Attackers may manipulate their signal transmission either temporally or spatially. In temporal manipulation, an attacker may take either of the following two approaches. With the first approach, the attacker may vary its transmission power over time in an attempt to cause confusion. However, this attack has limited impact since the proposed localization scheme collects and analyzes a snapshot of RSS measurement, in which only one transmission power value is in effect. With the second approach, the attacker may temporarily stop transmission when it knows that a snapshot of RSS measurement is being taken. However, RSS measurement is not only used for localization, but more importantly, it is the premise of spectrum sensing. To successfully launch a PUE attack, an attacker's signal has to be detected in the spectrum sensing process. Therefore, an attacker cannot benefit from keeping silent while RSS measurements are being collected.

An attacker has two options to conduct spatial manipulation of its transmission. As the first option, the attacker can install a directional antenna so that it is detected by less number of sensors. Because the attacker's signal is still detected by some sensors, the effect of its PUE attack remains unchanged. On the other hand, less RSS information will lead to vaguer peak locations in an RSS snapshot, thereby adding difficulty to localization. In Section V, we will further investigate this problem using simulation. The second method for spatial manipulation is to use multiple transmitters deployed at different locations. Because the signals emitted by the transmitters interfere with each other, the signal characteristics (e.g., time of arrival, angel of arrival, RSS) of different transmitters may be mixed together, causing wrong localization results. However, the proposed localization system is able to identify multiple transmitters if multiple RSS peaks are observed. In Section V, its performance will be evaluated when multiple transmitters are present.

The second category of attacks disrupt localization by injecting false data to the localization system. This is possible when some sensor nodes are compromised. This attack is partly mitigated by the fact that the median value has been used for RSS smoothing. It is known that in the absence of noise, taking the median can tolerate up to 50 percent outliers among all measurements [22].

V. Simulation

A. Simulation on the Effects of PUE Attacks

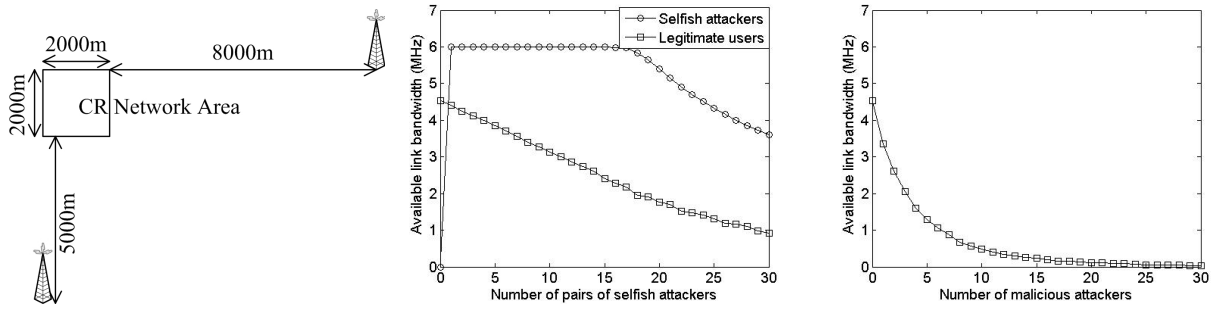
We carried out simulation experiments to showcase the disruptive effects of PUE attacks. In the simulated network, 300 secondary users (which include both legitimate users and attackers) are randomly located inside a 2000m×2000m square area, each with a transmission range of 250m and an interference range of 550m. These range values are consistent with the protocol interference model used in [14]. Two TV broadcast towers act as primary signal transmitters. Each TV tower has ten 6MHz channels, and the duty cycle of all the channels is fixed at 0.2. One tower is located 8000m east of the square area and has a transmission radius of 9000m; the other tower is located 5000m south of the square area with a transmission radius of 7000m[7]. The layout of the simulated network is shown in Fig. 5(a). Each secondary user node is randomly placed in the network area and moves according to a random waypoint model by repeatedly executing the following four steps: 1) It randomly chooses a destination in the square area with a uniform distribution; 2) It chooses a velocity v that is uniformly distributed over [v_{min}, v_{max}]; 3) It moves along a straight line from its current position to the destination with velocity v; and 4) It pauses in the destination for a random period that is uniformly distributed over [0, t_{p-max}]. We chose the values $v_{min} = 5$m/s, $v_{max} = 10$m/s, and $t_{p-max} = 60$s. Each simulation instance spans a period of 24 hours. Another one hour before the 24 hours was simulated to ensure that the random waypoint model entered steady state. The number of malicious PUE attackers was varied from 1 to 30 and that of selfish PUE attackers was varied from 1 to 30 pairs. Figs. 5(b) and 5(c) show the simulation results for the selfish PUE attack and the malicious PUE attack, respectively. The y-axis in the figures represents the amount of link bandwidth each secondary user is able to detect. The results show that a selfish PUE attack can effectively steal bandwidth from legitimate secondary users while a malicious PUE attack can drastically decrease the link bandwidth available to legitimate secondary users.

B. Simulation of the Localization System

1) Simulation Setting and Objectives: We conducted a set of simulation experiments to evaluate the proposed transmitter localization scheme. Note that verification of signal characteristics and measurement of signal energy level are not included in this simulation study.

In the simulation, a 2000m×2000m CR network with an underlying WSN of the same size was assumed and the

[7]We set the values of 9000m and 7000m for the primary users' transmission radiuses based on realistic assumptions. Suppose the following parameters: EIRP (Equivalent Isotropically Radiated Power) of the TV towers (transmitters) is 2500KW, transmitters' effective antenna height is 100m, receivers' effective antenna height is 1m, and receivers' energy detection sensitivity is -94dbm. Under these conditions, one can derive a transmission radius of 8000m using the rural environment version of the HATA model [20].



(a) (b) (c)

Fig. 5. Simulation showcasing the effect of PUE attacks. (a) Simulation layout. (b) Effect of selfish PUE attacks. (c) Effect of malicious PUE attacks.

TABLE I
SIMULATION SETTINGS FOR THE LOCALIZATION SYSTEM.

Sensor density (m^{-2})	Number of sensors	r (m)	d (m)
2.5×10^{-5}	100	305	1,294
5×10^{-5}	200	300	1,273
1.25×10^{-4}	500	200	849
2.5×10^{-4}	1,000	200	849
5×10^{-3}	2,000	100	424
1.25×10^{-4}	5,000	100	424
2.5×10^{-3}	10,000	50	212

statistical log-loss propagation model with $(\beta_0, \beta_1, \sigma) = (-30.00, -10.00, 10.0)$ was used. The exact values of these parameters are unknown to the localization system, but we assume that they are estimated using the offsite calibration scheme proposed in [23], where a realistic estimation was given as $(\beta_0, \beta_1, \sigma) = (-32.03, -9.73, 10.0)$. Then based on (8), assuming $m = 3$dB and $P = 0.9$, we generated seven simulation settings representing various density of sensors in the WSN and their corresponding parameters r and d, which are shown in Table I. We used $\Delta = r/15$ for the simulation so that the condition in (9) is satisfied as well. We consider four cases when there is a single transmitter, when an attacker uses a directional antenna, when multiple PUE attackers exist, and when it is the special case of out-of-range primary users.

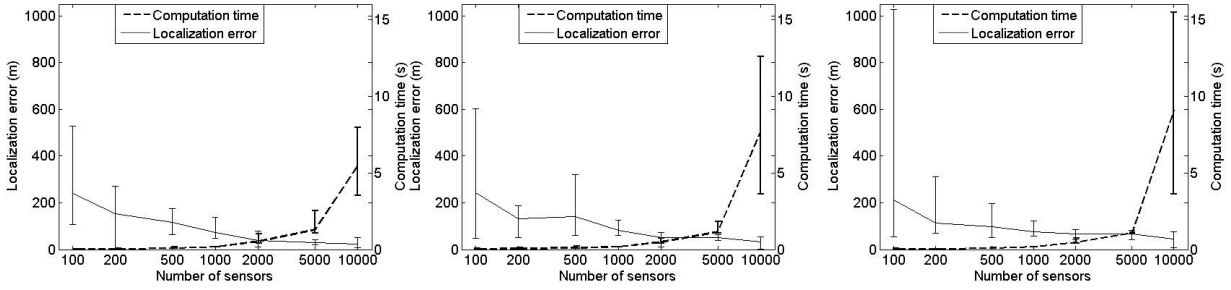
We evaluate the system's localization error and computation time. Based on the discussion in Section III, the metric of localization error has the following meaning. When a primary signal transmitter is found to be away from any known location of primary users more than the localization error, the transmitter is deemed as a PUE attacker. Once a PUE attacker is detected, the localization error defines a range of area for pinpointing the attacker. The computation time is the time to run the localization algorithm but does not include the WSN's network delay for collecting data. The computation time shows the relative computation overhead in different scenarios. It is measured in our specific simulation environment and its absolute value could change as the environment varies[8].

2) The Case of a Single Transmitter: We consider three scenarios, in which a 500mW primary signal transmitter is in the center, on the border, and on the corner of the WSN, i.e., T_1 at (1000m, 1000m), T_2 at (1000m, 50m), and T_3 at (50m, 50m), respectively. The localization errors of the proposed localization system under various settings are shown in Fig. 6. In the figure, every datum is the average of ten independent simulations. The results prove the localization system to be effective. For example, under the 10,000-sensor scenario, the expected space of two adjacent sensors is 20m, which is close to the localization error of T_1, i.e., 21.9m. T_2 and T_3 have relatively greater localization error because on the border or on the corner of the WSN, there are less number of sensors around, resulting in less number of measurements and thus poorer accuracy. Meanwhile, the computation time is shown to be affordable. T_2 and T_3 require relatively greater computation time because less number of measurements means more ambiguity and causes the localization algorithm to sample greater number of regions (i.e, the set R has more elements).

3) The Case of Directional Antenna: An attacker may mount a directional antenna to evade localization. To investigate its impact, we repeated the previous simulation assuming that the primary signal transmitter used a ten-element Yagi-Uda antenna. A ten-element Yagi-Uda antenna is a typical directional antenna and its radiation pattern can be found in [21]. In the simulation, the major lobe in the antenna's radiation pattern pointed toward the increasing direction of the x-axis (i.e., the direction from T_1 to T_2). As the results in Fig. 7 show, the directional antenna has increased the localization error and computation time. We reason that the use of directional antennas caused less number of sensors to detect the transmitted signals and this had the same effect as decreasing the density of the sensors.

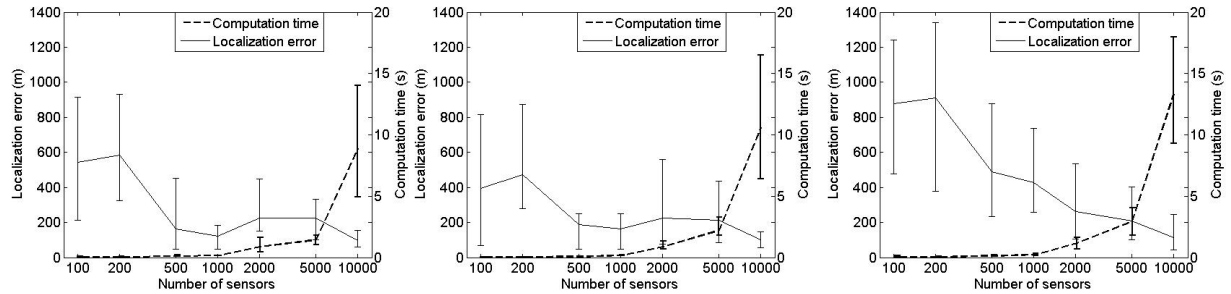
Another observation is that for locations T_1 and T_2, the localization errors for 500-sensor and 1,000-sensor scenarios are smaller than those for 2,000-sensor and 5,000-sensor scenarios, which is counter-intuitive. Further research revealed that because the directional antenna brought about the equivalent effect of decreasing the sensor density ρ, the derived values of r and d using (8) became too small, causing the localization algorithm to be trapped at a local maximum. To confirm this reasoning, we doubled the values of r and d and repeated the previous simulation. Fig. 8 shows that with this change, for high-sensor-density scenarios, the performance was greatly improved. However, for other scenarios with low sensor densities, this caused overly large region sizes and the

[8]In particular, the simulation was run in MATLAB on a P4 2.8GHz, 512M RAM PC.



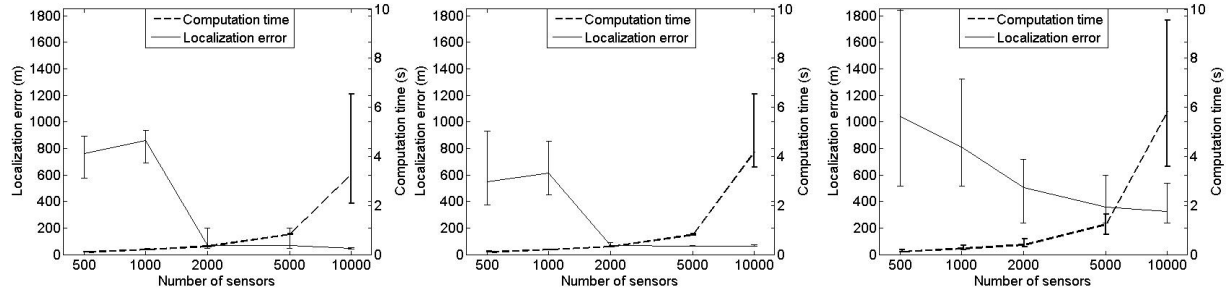
(a) (b) (c)

Fig. 6. The localization error of the proposed localization system. (a) T_1(1000m, 1000m). (b) T_2(1000m, 50m). (c) $T_3(50m, 50m)$.



(a) (b) (c)

Fig. 7. The system's localization error when a primary signal transmitter uses a ten-element Yagi antenna. (a) T_1(1000m, 1000m). (b) T_2(1000m, 50m). (c) $T_3(50m, 50m)$.



(a) (b) (c)

Fig. 8. The system's localization error when r is doubled in case that a primary signal transmitter users a ten-element Yagi antenna. (a) T_1(1000m, 1000m). (b) T_2(1000m, 50m). (c) T_3(50m, 50m).

localization error was significantly increased.

4) The Case of Multiple PUE Attackers: A two-transmitter scenario is considered under 2,000-sensor and 5,000-sensor deployments. Both are assumed to be transmitting signals at the same UHF 617MHz band and their phase shift was randomly chosen. We varied the distance between the two transmitters and observed the estimated number of transmitters and their locations by the localization system. Based on 100 independent simulation runs, Fig. 9 shows the ratio of the runs that output correct number of transmitters, i.e., two. Fig. 10 shows the corresponding localization errors when the number of transmitters was correctly recognized. When the two transmitters are within 500 meters of each other, the localization system only recognizes one signal source most of the time. However, when the distance increases, the two transmitters can be both correctly localized, with a localization error similar to that in single-transmitter scenarios.

5) The Case of Out-of-range Primary Users: In Subsection IV.D, the value of D_h was used to compare the likelihoods that a primary signal transmitter is on the border of the WSN and in out-of-range locations. We fixed a PUE attacker at location (1950m, 1000m) and set a primary user at location ((1950 + δ_x)m, 1000m), where δ_x is a variable in the simulation. The PUE attacker is transmitting while the primary user is not transmitting. The result in Fig. 11 shows that when the distance between the PUE attacker and the out-of-range primary user is large, the D_h value induced by the attacker is much smaller than that induced by the primary user, showing that the attacker's location will be correctly output by (12). However, when the distance between the PUE attacker and the

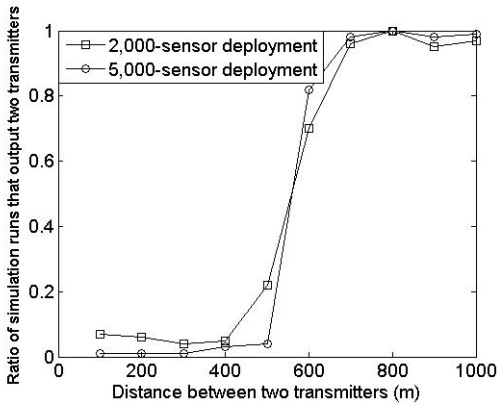


Fig. 9. The ratio of simulation runs that correctly recognize the number of transmitters in a two-transmitter scenario.

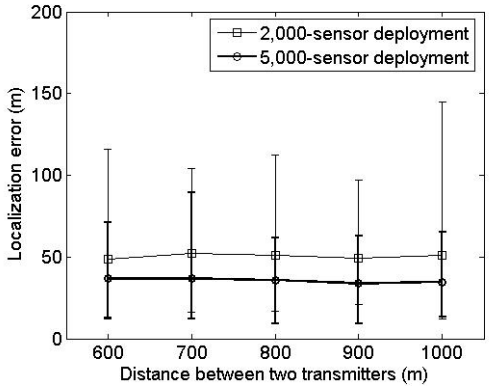


Fig. 10. The localization error in a two-transmitter scenario.

primary user is relatively small, due to the modeling error and the localization error, D_h cannot be used for distinguishing the attacker from the primary user. In this case, as the flowchart in Fig. 1 shows, the signal energy level will be further examined to judge the legitimacy of the transmitter.

VI. Related Research

CR-related research has received great attention recently. A major thrust in this research area is the development of spectrum sensing techniques capable of accurately detecting the existence of primary users or spectrum opportunities. In [5] and [19], schemes were proposed in which a single secondary user device performs spectrum sensing and independently decides which spectrum band to use. However, with these schemes, the accuracy of spectrum sensing is unreliable due to various factors such as the limited sensitivity of a single CR. To address this problem, *cooperative* spectrum sensing techniques were investigated in [11], [16], [24], [27].

The work presented in this paper is also related to the existing body of research on localization systems [7], [13], [15], [18], [26]. As discussed in Section IV, the existing research is inadequate for solving the PST localization problem. Recently, secure localization schemes have been proposed [2], [3]. These schemes, however, are inappropriate for solving the PST localization problem in CR networks. The technique proposed in [2] is for receiver localization, and cannot be used for transmitter localization. Moreover, localization schemes proposed in [2], [3] require interaction between the localized object and the localizing devices. In [6], two location verification schemes were proposed for verifying the location of primary users in CR networks. However, the schemes do not have localization capabilities and they are ineffective against simultaneous transmission by multiple attackers and attacks that involve directional antennas.

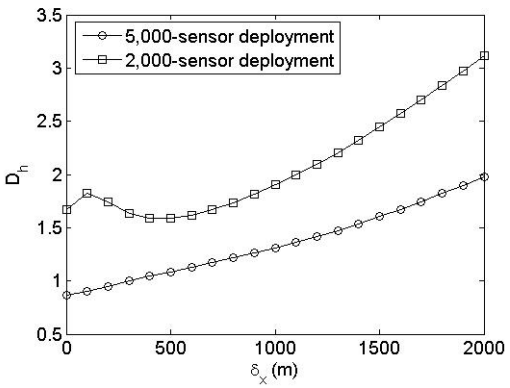


Fig. 11. D_h vs. δ_x.

VII. Conclusion and Future Work

We identified the PUE attack in CR networks and demonstrated its disruptive effect on spectrum sensing. To counter the attack, we proposed LocDef as a transmitter verification scheme, which can be integrated into the spectrum sensing process. LocDef employs a non-interactive localization scheme to detect and pinpoint PUE attacks. Security analysis and simulation results show that the proposed localization scheme is effective and can be employed in hostile environments.

A localization-based approach is not the only way to defend against PUE attacks. We are investigating an alternative approach that uses the intrinsic characteristics of RF signals to distinguish and identify emitters—i.e., RF fingerprinting. In network environments where the primary transmitters are mobile and have low power, localization-based approaches for thwarting PUE attacks do not work. For instance, a localization-based approach does not work when the network environment includes Part 74 devices (e.g., wireless microphones) as primary transmitters. These Part 74 devices are also licensed to operate in the TV bands. In such an environment, RF fingerprinting may provide an alternative countermeasure against PUE attacks.

As discussed in Section II, in addition to the security problems in spectrum sensing, there are other security issues in DSA—those related to spectrum access and software protection. These issues also require further research.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions.

REFERENCES

[1] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Elsevier Computer Networks Journal*, Vol. 50, Sept. 2006, pp.2127–2159.

[2] S. Capkun, M. Cagalj, and M. Srivastava, "Secure localization with hidden and mobile base stations," *Proc. IEEE Infocom*, Apr. 2006.

[3] S. Capkun and J.-P. Hubaux, "Secure positioning in wireless networks," *IEEE J. Selected Areas in Communications*, Vol.24 (2), Feb. 2006, pp. 221–232.

[4] D. Cabric, S. M. Mishra, and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," *Proc. Thirty-Eighth Asilomar Conf. Signals, Systems and Computers*, Nov. 2004, pp. 772–776.

[5] K. Challapali, S. Mangold and Z. Zhong, "Spectrum agile radio: Detecting spectrum opportunities," *Proc. 6th Annual Int'l Symp. Advanced Radio Technologies*, Mar. 2004.

[6] R. Chen and J.-M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," *Proc. IEEE Workshop on Networking Technologies for Software Defined Radio Networks*, Sept. 2006.

[7] K. Dogancay and D. A. Gray, "Closed-form estimators for multi-pulse TDOA localization," *Proc. 8th Int'l Symp. Signal Processing and Its Applications*, Aug. 2005, pp. 543–546.

[8] Federal Communications Commission, "Facilitating opportunities for flexible, efficient, and reliable spectrum use employing spectrum agile radio technologies," *ET Docket No. 03-108*, Dec. 2003.

[9] Federal Communications Commission, "Unlicensed operation in the TV broadcast bands and additional spectrum for unlicensed devices below 900 MHz in the 3GHz band," *ET Docket No. 04-186*, May 2004.

[10] Federal Communications Commission, "E911 requirements for IP-enabled service providers," *ET Docket No. 05-196*, May 2005.

[11] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio networks," *Proc. IEEE DySPAN*, Nov. 2005, pp. 137–143.

[12] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE J. Selected Areas in Communications*, Vol 23 (2), Feb. 2005, pp. 201–220.

[13] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. F. Abdelzaher, "Range-free localization schemes in large scale sensor networks," *Proc. ACM MobiCom*, Sept. 2003, pp. 81–94.

[14] K. Jain, J. Padhye, V. N. Padmanabha, and L. Qiu, "Impact of interference on multi-hop wireless network performance," *Proc. ACM Mobicom*, Sept. 2003, pp. 66–80.

[15] T. Locher, R. Wattenhofer, and A. Zollinger, "Received-signal-strength-based logical positioning resilient to signal fluctuation," *Proc. 1st ACIS Int'l Workshop on Self-Assembling Wireless Sensor Networks*, May 2005.

[16] S. M. Mishra, A. Sahai, and R. Brodersen, *Cooperative sensing among cognitive radios*, available at: http://www.eecs.berkeley.edu/šahai/Papers /ICC06_final.pdf, 2006.

[17] J. Mitola, *Cognitive radio: an integrated agent architecture for software defined radio*, PhD Dissertation, Royal Institute of Technology (KTH), Stockholm, Sweden, June 2000.

[18] D. Niculescu and B. Nath, "Ad hoc positioning system (APS)," *Proc. IEEE GLOBECOM*, Nov. 2001, pp. 2926–2931.

[19] M. P. Olivieri, G. Barnett, A. Lackpour, A. Davis, and P. Ngo, "A scalable dynamic spectrum allocation system with interference mitigation for teams of spectrally agile software defined radios," *Proc. IEEE DySPAN*, Nov. 2005, pp. 170–179.

[20] T. S. Rappaport, *Wireless communications: principles and practice*, Prentice Hall, 1996.

[21] J. H. Reisert, *Understanding and using antenna radiation patterns*, available at: http://www.astronwireless.com/radiation_patterns.html, 2007.

[22] P. Rousseeuw and A. Leroy, *Robust regression and outlier detection*, Wiley-Interscience, Sept. 2003.

[23] T. Roos, P. Myllymaki, and H. Tirri, "A statistical modeling approach to location estimation," *IEEE Trans. Mobile Computing*, Vol. 1(1), Jan.-March 2002, pp. 59–69.

[24] S. Shankar, C. Cordeiro, and K. Challapali, "Spectrum agile radios: utilization and sensing architectures," *Proc. IEEE DySPAN*, Nov. 2005, pp. 160–169.

[25] J. S. Simonoff, *Smoothing Methods in Statistics*, Springer-Verlag, 1996.

[26] B. H. Wellenhoff, H. Lichtenegger, and J. Collins, *Global positioning system: theory and practice*, Fourth edition, Springer Verlag, 1997.

[27] B. Wild and K. Ramchandran, "Detecting primary receivers for cognitive radio applications," *Proc. IEEE DySPAN*, Nov. 2005, pp. 124–130.

Ruiliang Chen received his Bachelor's degree in Communications Engineering in 2000, and his Master's degree in Communications and Information Systems in 2003, both from Fudan University, China. From June 2003 to July 2004 he worked as a product engineer at the Intel Shanghai Product Corporation. He is currently a Ph.D. student in the Bradley Department of Electrical and Computer Engineering at Virginia Tech. His research interests include traceback and mitigation mechanisms for thwarting denial-of-service attacks, attack-resilient routing protocols for wireless ad hoc networks, and security issues in cognitive radio networks. He is a student member of the IEEE.

Jung-Min Park received his Bachelor's degree and Master's degree both in Electronic Engineering from Yonsei University, Seoul, Republic of Korea, in 1995 and 1997, respectively. From 1997 to 1998, he was a cellular systems engineer at Motorola Korea, Inc. Dr. Park received the PhD degree in electrical and computer engineering from Purdue University in 2003. He is currently an Assistant Professor in the Bradley Department of Electrical and Computer Engineering at Virginia Tech. Dr. Park conducts research in network attack countermeasures, applied cryptography, and security in cognitive radio networks. Dr. Park has published numerous papers in leading journals and conference proceedings in the area of network/computer security. He was a recipient of a 1998 AT&T Leadership Award. Current research sponsors include the National Science Foundation, SANS (SysAdmin, Audit, Network Security) Institute, and Samsung Electronics. More details about his research interests and publications can be found at http://www.arias.ece.vt.edu/index.html. He is a member of the IEEE and ACM.

Jeffrey H. Reed is the Willis G. Worcester Professor in the Bradley Department of Electrical and Computer Engineering. Dr. Reed's area of expertise is in software/cognitive radios, smart antennas, wireless networks and communications signal processing From June 2000 to June 2002, Dr. Reed served as Director of the Mobile and Portable Radio Research Group (MPRG). He currently serves as Director of the newly formed umbrella wireless organization Wireless@Virginia Tech. Dr. Reed is a co-founder of Cognitive Radio Technologies, in Lynchburg, VA. In 2005, Dr. Reed became Fellow to the IEEE for contributions to software radio and communications signal processing and for leadership in engineering education.