Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks

Ruiliang Chen and Jung-Min Park

Bradley Department of Electrical and Computer Engineering
Virginia Polytechnic Institute and State University
Blacksburg, VA 24061
{rlchen, jungmin}@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 without inducing interference to incumbent communications. *Spectrum sensing* is one of the essential mechanisms of CRs that has attracted great attention from researchers recently. Although the operational aspects of spectrum sensing are being investigated actively, its security aspects have garnered little attention. In this paper, we describe an attack that poses a great threat to spectrum sensing. In this attack, which is called the *primary user emulation (PUE) 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. As a way of countering this threat, we propose a transmitter verification procedure that can be integrated into the spectrum sensing mechanism. The transmitter verification procedure employs a location verification scheme to distinguish incumbent signals from unlicensed signals masquerading as incumbent signals. Two alternative techniques are proposed to realize location verification: *Distance Ratio Test* and *Distance Difference Test*. We provide simulation results of the two techniques as well as analyses of their security in the paper.**

Index terms—**Cognitive Radio, Spectrum Sensing, Primary User Emulation Attack, Location Verification.**

I. INTRODUCTION

The need to meet the ever-increasing spectrum demands of emerging wireless applications and the need to better utilize spectrum has led the Federal Communication 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 primary users. In this new paradigm, unlicensed users (a.k.a. secondary users) "opportunistically" operate in fallow licensed spectrum bands without causing interference to licensed users (a.k.a. primary or incumbent users), thereby increasing the efficiency of spectrum utilization. This method of sharing is often called *Opportunistic Spectrum Sharing* (OSS).

Cognitive Radios (CRs) [13, 8] are seen as the enabling technology for OSS. 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 attributes 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 incumbent signals in the current operating band and candidate bands. Consider the following two scenarios. If a secondary user (with a CR) detects the presence of incumbent 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

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

are operating in hostile environments. In a hostile environment, an attacker may modify the air interface of a CR to mimic incumbent 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 denote this attack. There is a realistic possibility of PUE attacks since CRs are highly reconfigurable due to their software-based air interface [8]. To thwart such attacks, a robust *transmitter verification* scheme that can distinguish between legitimate incumbent signal transmitters and secondary signal transmitters (emulating incumbent signal transmitters) is needed. In hostile environments, such a scheme can be integrated into the spectrum sensing mechanism to enhance its trustworthiness.

The task of distinguishing incumbent signals from secondary user signals becomes even a greater challenge when one considers the requirement described in FCC's NPRM 03-322 [4], 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 a signature in a primary user's signal or employing an interactive protocol between an incumbent signal transmitter and a verifier, cannot be used.

The current research and standardization efforts suggest that one of the first applications of CR technology will be its use for OSS of fallow TV spectrum bands. FCC is considering opening up TV bands for OSS because TV bands often experience lower and less dynamic utilization compared to other incumbent networks such as cellular networks [5]. Throughput the paper, we assume an incumbent network composed of TV transmission towers and receivers placed at fixed locations. In such a setting, positions of incumbent transmitters can be used to distinguish primary user signals from secondary user signals. In this paper, we propose a transmitter verification procedure that employs a *non-interactive location verification* scheme to exploit the fact that the incumbent signal transmitters are placed at fixed locations. Because the location verification scheme is non-interactive, no modification to the incumbent signal transmitters is needed, thus satisfying the requirement stated in NPRM 03-322.

In the proposed location verification scheme, designated verifiers cooperatively verify the legitimacy of an incumbent signal transmitter's location by passively listening to its signal without interacting with the transmitter. We propose two alternative techniques that are at the heart of the location verification scheme. The first technique, the *Distance Ratio Test* (DRT), uses received signal strength (RSS) measurements obtained from a pair of verifiers to verify the transmitter's location. The second technique, *Distance Difference Test* (DDT), utilizes the phase difference of the primary user's signal observed at a pair of verifiers to verify the transmitter's location.

The main contribution of this work is threefold: identification of the PUE attack, demonstration of its harmful effects on a CR network, and the proposal of a transmitter verification procedure to detect such an attack. The proposed procedure can be integrated into existing spectrum sensing schemes to enhance their trustworthiness. To the best of our knowledge, there is no existing work that specifically addresses the security issues in spectrum sensing that we have addressed in this paper.

The rest of the paper is organized as follows. In Section II, we describe the PUE attack in detail. In Section III, we present a new transmitter verification procedure for spectrum sensing and describe DRT and DDT. Security analyses of DRT and DDT are given in Section IV. The simulation results are given in Section V, and related work is summarized in Section VI. In Section VII, we conclude the paper and discuss future work.

II. The Primary User Emulation (PUE) Attack

One of the major technical challenges in spectrum sensing is the problem of precisely distinguishing incumbent signals from secondary user signals. To distinguish the two signals, existing spectrum sensing schemes based on energy detectors [3, 15] implicitly assume a "naive" trust model. When energy detection is used, a secondary user can recognize the signal of other secondary users but cannot recognize primary users' signal. When a secondary user detects a signal that it recognizes, it assumes that the signal is that of a secondary user; otherwise it concludes that the signal is that of a primary user. Under such an overly simplistic trust model, a selfish or malicious secondary user (i.e., an attacker) can easily exploit the spectrum sensing process. For instance, an attacker may "masquerade" as an incumbent transmitter 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 [2]. Nodes that are 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. For instance, to defeat cyclostationary detectors, an attacker may make its transmissions indistinguishable from incumbent signals by transmitting signals that have the same cyclic spectral characteristics as incumbent signals.

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 usage of spectrum resources. 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 incumbent 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 OSS process of legitimate secondary users—i.e., prevent legitimate secondary users from detecting and using fallow licensed spectrum bands. 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 obstruct OSS in multiple bands simultaneously by exploiting two OSS mechanisms implemented by every legitimate secondary user. The first mechanism requires a secondary user to wait for a certain amount of time before using the identified fallow band to make certain that the band is indeed unoccupied. Existing research shows that this time delay is non-negligible [19, 3]. The second mechanism requires a secondary user to periodically sense the current operating band to detect the presence of incumbent 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.

Note that in PUE attacks, attackers only transmit in fallow bands; thus, interference to primary users is not a concern. We carried out rudimentary simulation experiments to showcase the disruptive effects of PUE attacks. In the simulated network, 300 secondary users (which include both legitimate and malicious users) are randomly located inside a 2000m × 2000m square area, each with a transmission range of 250m and an interruption range of 550m. These range values are consistent with the protocol interference model [9]. Two TV broadcast towers act as incumbent 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. The layout of the simulated network is shown in Fig. 1. Each secondary user node moves according to a random waypoint model via the following four steps:

1) It randomly chooses a destination in the square area according to a uniform distribution;
2) It chooses a velocity v that is uniformly distributed over $[0, v_{max}]$;
3) It moves along a straight line from its current position to the destination with velocity v until it arrives at the destination; and
4) It pauses in the destination for a random period that is uniformly distributed over $[0, t_{p\text{-}max}]$.

We chose the values v_{max} = 10m/s and $t_{p\text{-}max}$ = 60s. Each simulation instance spans a period of 24 hours. The number of attackers was varied from 1 to 30. Figs. 2 and 3 show the simulation results for the selfish PUE attack and the malicious PUE attack, respectively. The available link bandwidth in the figures represents the amount of bandwidth opportunities each secondary user detects. Results show that a selfish PUE attack can effectively steal bandwidth from legitimate secondary users while a malicious PUE attack can drastically decrease available network bandwidth to legitimate secondary users.

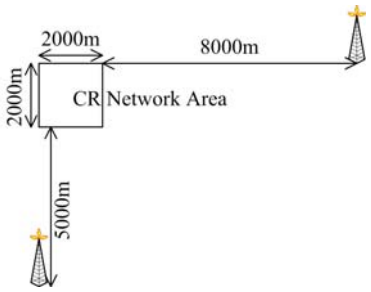


Fig. 1. Simulation layout for showcasing the effect of PUE attacks.

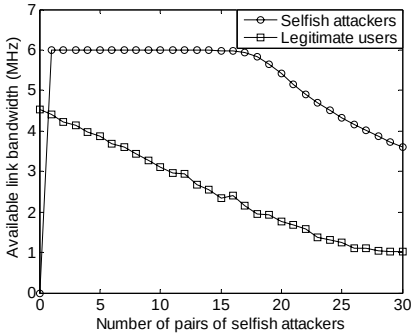


Fig. 2. Effect of selfish PUE attacks.

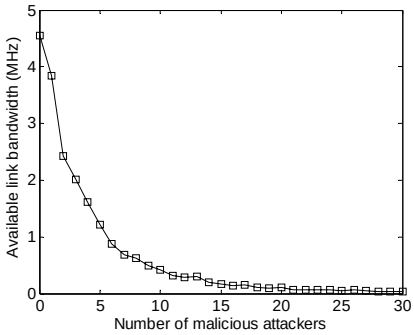


Fig. 3. Effect of malicious PUE attacks.

To thwart PUE attacks, we propose a transmitter verification procedure that can, under certain conditions, reliably distinguish between incumbent transmitters' signals and signals emitted by adversaries emulating incumbent transmitters. In the next section, we describe the transmitter verification procedure in detail.

III. A Transmitter Verification Procedure for Spectrum Sensing

A. The transmitter verification procedure

Before describing the proposed transmitter verification procedure for spectrum sensing, we state the assumptions that form the foundation of the transmitter verification procedure. The primary user is assumed to be a network composed of TV

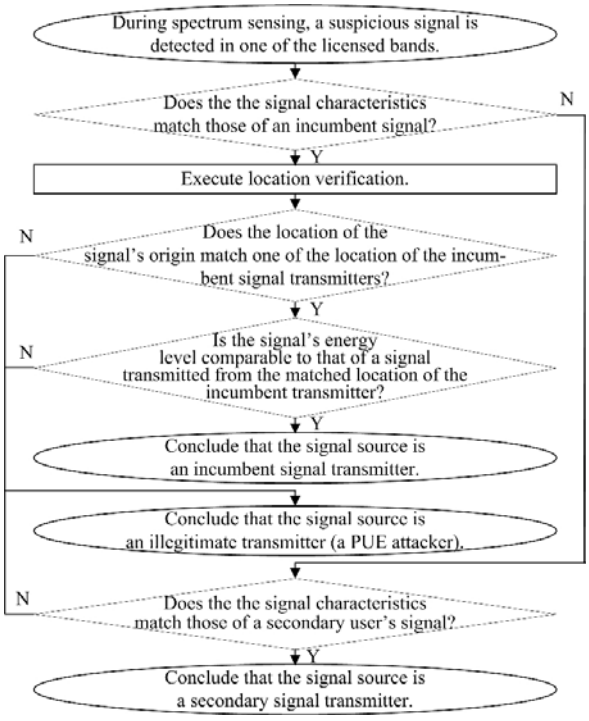


Fig. 4. A flowchart of transmitter verification procedure for spectrum sensing.

signal transmitters (i.e., TV broadcast towers) and receivers. A TV tower typically covers a circular area with a radius ranging from several miles to tens of miles, and its transmitter output power is typically hundreds of thousands of Watts [21]. The secondary users are assumed to be hand-held CR devices forming a mobile ad hoc network. Each CR is assumed to have a maximum transmission output power that is somewhere in the range from a few hundred milliwatts to a few watts—this corresponds to a transmission range of a few hundred meters. An attacker, equipped with a CR, is assumed to be capable of changing the radio's modulation mode and transmission output power as needed. The proposed transmitter verification procedure only considers PUE attacks, which is a security threat unique to CR networks. It should be noted that a CR network is also vulnerable to more conventional threats, such as jamming attacks and route disruption attacks, which are not discussed in this paper.

Based on the above assumptions, we propose a transmitter verification procedure for spectrum sensing that is appropriate for hostile environments; the transmitter verification procedure is illustrated in Fig. 4. The distinguishing feature of this transmitter verification procedure is that it determines the legitimacy of a given signal source using the signal source's *location*.

In the network model under consideration, the incumbent signal transmitters are TV broadcast towers placed at fixed locations. Hence, it is reasonable to assume that an estimate of a signal source's location can be used to help determine whether it is a primary user or a secondary user. If a node is transmitting in a location that deviates from the known locations of the TV towers and the signal characteristics resemble those of incumbent signals, then the possibility that the signal source is executing a PUE attack is high. 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 incumbent 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, other countermeasures can be carried out to identify and isolate the malicious node and to prevent further disruption in network operations. For instance, transmitter detector devices can be employed to pinpoint the location of the attacker once its presence has been detected. In this paper, however, we restrict our discussions to the *detection* of PUE attacks.

As discussed previously, the key aspect of the transmitter verification procedure is the estimation or verification of the location of a signal's origin. This problem—called by various names such as location estimation, location identification, localization, positioning etc.—has been studied extensively in the past. This particular problem, however, is different and more challenging. Recall that any OSS technology must abide by the fundamental requirement that no modification to the incumbent system should be required to accommodate opportunistic use of the spectrum by secondary users. Thus, the localization scheme referred to in the proposed transmitter verification procedure must be *non-interactive*—i.e., the location estimators/verifiers cannot interact with the signal transmitter to estimate or verify its location. In the rest of this section, we devote our discussions to the techniques to realize non-interactive location verification. We focus on two different techniques. The first one is called *Distance Ratio Test* (DRT), which utilizes the received signal strength (RSS) of a signal source. The other one is called *Distance Difference Test* (DDT), which relies on the received signal's relative phase difference when the signal is received at different receivers.

The following assumptions need to be made to support the operations of DRT and DDT. We assume that trusted *location verifiers* (LVs) exist for performing DRT or DDT. An LV can be a dedicated node, a secondary user with enhanced functions (to carry out DRT/DDT), or a fixed/mobile base station. We assume that the area spanned by the CR network is populated with two types of LVs: one or more *master* LVs and slave LVs. A master LV has a database of the coordinates of every TV tower whose signal reaches the area spanned by the CR network. Each LV is assumed to know its location from a secure GPS system [10]. In addition, we assume that all of the LVs are synchronized and can communicate with each other through a common control channel. Note that the existence of a common control channel is a characteristic

shared by most of the MAC protocols proposed for CR networks (e.g., [23, 12, 16]). In the following discussions, we restrict our discussions to two-dimensional localization.

B. Distance Ratio Test (DRT)

RSS-based localization is based on the fact that there is a strong correlation between the length of a wireless link and RSS [11, 18]. For radio systems that use tall towers, such as TV systems, the two-ray ground reflection model has been found to be reasonably accurate for predicting large-scale signal strength [18]. The model is represented as follows:

$$RSS = P_t G_t G_r \frac{h_t^2 h_r^2}{d^4 L}, \quad (1)$$

where P_t is the transmitted signal power, G_t and G_r are the antenna gains of the transmitter and the receiver, respectively, h_t is the height of the transmitter, h_r is the height of the receiver, d is the propagation distance, and L is other system loss.

In a hostile environment, parameters such as P_t, G_t, and h_t can be readily manipulated by an attacker launching a PUE attack. Thus, DRT employs a cooperative distance ratio verification scheme, which is independent of those parameters.

In a single iteration of DRT, a pair of LVs, represented by LV_1 and LV_2, simultaneously measure the RSS of a signal in the band of interest, obtaining results R_1 and R_2, respectively. The two LVs are assumed to be identical with respect to the parameters of (1) except for their distances to the signal source. Suppose that the positions of LV_1 and LV_2 are (x_1, y_1) and (x_2, y_2), respectively. The values of R_1, R_2, (x_1, y_1), and (x_2, y_2) are sent to a master LV (note that LV_1 or LV_2 or even another LV may act as a master LV). After receiving the parameters, the master LV goes through the following procedure for each TV tower's coordinate in its database.

(1) Suppose that the two dimensional coordinate of the first TV tower is (u_1, v_1). The master LV calculates the *reference* distance ratio as:

$$\rho = \frac{\sqrt{(x_1 - u_1)^2 + (y_1 - v_1)^2}}{\sqrt{(x_2 - u_1)^2 + (y_2 - v_1)^2}}. \quad (2)$$

(2) The master LV calculates the *measured* distance ratio, given by the following equation, using the RSS measurements:

$$\rho' = \frac{d_1}{d_2} = \sqrt[4]{\frac{R_2}{R_1}}, \quad (3)$$

where d_1 and d_2 are the respective distances between LV_1 and the signal source and LV_2 and the signal source.

(3) The master LV checks whether

$$\rho' \in [\frac{\rho}{(1+\varepsilon_1)}, (1+\varepsilon_1)\rho], \quad (4)$$

where ε_1 (≥ 0) is the expected maximum error; it includes both measurement error and modeling error.

If (4) does not hold, the signal source under scrutiny fails the location verification for the TV tower used in Step 1; otherwise, it passes the location verification. The above steps are repeated using the coordinates of the next TV tower, and the process is repeated until all of the coordinates in the database have been exhausted. If the signal source fails all of the location verifications, then the master LV concludes that the location of the signal source is not consistent with any of the TV towers in its database.

The practicality of DRT hinges on its accuracy. If an attacker is at a location that induces a similar distance ratio as that of an incumbent signal transmitter, the DRT may fail to recognize the signal as an attacker's signal, resulting in a false negative instance. On the other hand, if ε_1 is too small, DRT may mistakenly identify an incumbent signal as an attacker's signal, resulting in a false positive instance. To increase DRT's accuracy, multiple DRT iterations must be performed, each iteration using a different pair of LVs.

There are two caveats about the DRT that should be noted. First, since DRT relies on a large-scale propagation model, the possible fluctuations in RSS caused by small-scale fading are not considered. The effects of small-scale fading may vary the RSS by as much as three or four orders of magnitude when a receiver's position changes by only a fraction of a wavelength [18]. To effectively mitigate such effects, an "averaged" RSS value should be used—i.e., RSS should be averaged over multiple measurements made within a surrounding range of 5λ to 40λ [18], where λ is the wavelength of the signal. For TV signals transmitted at UHF 617MHz, this means that an LV needs to average multiple synchronous RSS measurements over a range of 2.5m to 20m. This approach, however, could be expensive to implement in practice. Second, DRT does not consider the fact that the radio propagation model is affected by various environmental variables. Different propagation environments may require the use of different parameters, and may even require the use of totally different propagation models. Recall that in DRT, the two LVs use the identical radio propagation model. This approach can result in erroneous location verification results if the two radio propagation paths from the signal source to each LV go through significantly different environments. Addressing such cases would require significant changes to the DRT technique.

C. Distance Difference Test (DDT)

We propose an alternate technique to DRT, namely *Distance Difference Test* (DDT), that verifies the difference in the two distances between a primary user and a pair of LVs. The difference in distance can be measured by measuring the phase shift of a signal at the two LVs. DDT does not suffer from DRT's drawbacks.

Analog TV signals have embedded synchronization pulses. In particular, such a pulse periodically appears every 64μs, with a maximum deviation of 0.25μs [20]. For digital

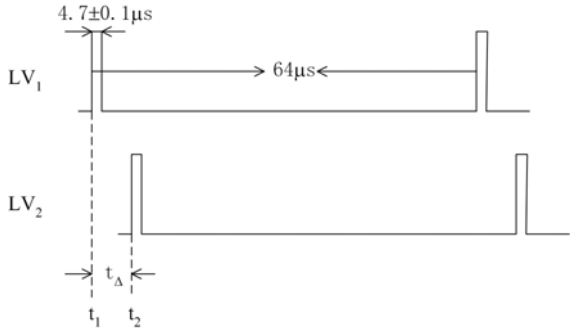


Fig. 5. The measurement of time gap for DDT.

TV systems, each symbol spans 224μs, in which 7μs is a silent period for inter-symbol separation [20]. If the incumbent signals are analog TV signals, the distance difference between a signal source and two LVs can be estimated by calculating the time difference in which each LV sees the same synchronization pulse. The time difference is readily converted to distance difference by multiplying the speed of light to the time difference. If the incumbent signals are digital TV signals, the time difference in which each LV sees the rising (or falling edge) of the same symbol is used.

Fig. 5 shows how the time difference is measured when incumbent signals are analog TV signals. In the figure, two synchronized LVs, LV_1 and LV_2, simultaneously record the time at which they see the synchronization pulse of the TV signal, and record the time values as t_1 and t_2, respectively. The time difference is calculated as $t_\Delta = t_1 - t_2$. Suppose that the coordinates of LV_1 and LV_2 are (x_1, y_1) and (x_2, y_2), respectively. The values of t_1, t_2, (x_1, y_1), and (x_2, y_2) are sent to the master LV. After receiving the parameters, the master LV goes through the following procedure for each TV tower's coordinate in its database.

1) Suppose that the two dimensional coordinate of the first TV tower is (u_1, v_1). The master LV calculates the reference distance difference as:

$$s = \sqrt{(x_1-u_1)^2+(y_1-v_1)^2} - \sqrt{(x_2-u_1)^2+(y_2-v_1)^2} \ . \quad (5)$$

2) Then the master LV calculates the observed distance difference using the time difference:

$$s' = c(t_1 - t_2) = ct_\Delta \ , \quad (6)$$

where c is the speed of light.

3) The master LV checks whether

$$s' \in [s - c\varepsilon_2, s + c\varepsilon_2] \ , \quad (7)$$

where ε_2 is the expected maximum time measurement error.

If (7) does not hold, the signal source under scrutiny fails the location verification for the TV tower used in Step 1; otherwise, it passes the location verification. The above steps are repeated using the coordinates of the next TV tower, and the process is repeated until all of the coordinates in the database have been exhausted. If the signal source fails all of the location verifications, then the master LV concludes that the location of the signal source is not consistent with any of the TV towers in its database.

In the above discussions, we have neglected to discuss a very important aspect of DDT's feasibility. If the temporal separation between two consecutive synchronization pulses (or symbols in case of digital TV signals) is too small, the DDT scheme may be infeasible. Suppose that the separation between pulses, represented by δ, is small enough for the relation $(t_\Delta \geq \delta / 2)$ to hold. In this case, it is nearly impossible for two LVs to make sure that they are recording the time of the same pulse since the time instants in which the two LVs see the same pulse may be separated by more than the length of the time duration in which each of them observes a different pulse. The value t_Δ is determined by the difference between the lengths of the two (line-of-sight) paths: one path from the signal source to LV_1, which we represent as α, and the other path from the signal source to LV_2, which we represent as β. In order for DDT to be feasible, this distance difference must be small enough so that the relation $|\alpha - \beta| < \delta \cdot c / 2$ is satisfied. See Fig. 6 for an illustration. Due to the triangle inequality theorem, the distance difference is always less than the distance between the two LVs, which we represent as γ. Hence, as long as the distance between the two LVs is small enough to satisfy $\gamma < \delta \cdot c / 2$, DDT is feasible. For example, in an analog TV system, two consecutive synchronization pulses are separated by 64μs, which is equivalent to 19,200m spatial separation. As long as the two LVs are less than 9,600m away from each other, DDT is feasible.

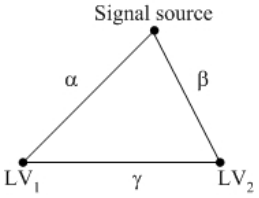


Fig. 6. DDT is feasible if $\gamma < \delta \cdot c / 2$.

IV. Security Analysis

For DRT and DDT to be effective in hostile environments, several security issues need to be addressed. In this section, we focus on two key problems that impact the security and reliability of DRT and DDT. The first problem is ensuring the robustness of the location verification process against attacks, and the second problem is ensuring secure data exchange among LVs.

A. Location verification scheme's robustness against attacks

There is a possibility that a PUE attacker may strategically position its transmitters and adjust their transmission power to circumvent the location verification procedure carried out by the LVs. Such an attack is possible only when an attacker has knowledge about the LVs' location. With the LVs' location information, an attacker can estimate the RSS and the time-of-flight of the signals emitted by its

transmitters when those signals reach the LVs. Recall that DRT and DDT utilize RSS and time-of-flight respectively to gauge the location of the signal source. Armed with such estimates, it is possible for an attacker to launch a PUE attack without failing the location verification tests carried out by the LVs.

A straightforward and effective countermeasure to such attacks is to use covert LVs. Here, covert LVs are LVs whose positions are known only to the authority controlling the location verification process. Note that the use of covert verifiers (or base stations) in secure localization schemes is not new (e.g., see [1]). To maintain the LV's covertness while not affecting communications among the nodes in a CR network, existing protocols for anonymous communications (such as MASK [22]) can be used.

An attacker may try to disrupt the location verification procedure by synchronizing its transmitters to send their signals simultaneously. In such a case, the LVs would receive a mixture of multiple signals. This, however, does not help the attacker's transmitters pass the transmitter verification process (see Fig. 4). For instance, the aggregate of the signals sent by a group of malicious transmitters will have synchronization pulses at irregular intervals (due to the overlapping of multiple signals). Such a signal deviates from the characteristic of a legitimate analog TV signal, and therefore would be readily identified as a non-incumbent signal.

B. Secure data exchange among LVs

Another security concern is the security of the data exchange between slave LVs and the master LV. The exchanged data must be encrypted and authenticated to avoid eavesdropping, insertion, modification, or replay attacks carried out by attackers.

The following protocol utilizes public-key cryptosystems to secure the messages exchanged between the master LV and slave LVs. We assume the existence of a PKI (public-key infrastructure) that takes care of key distribution, renewal, and revocation. The master LV initiates the protocol by broadcasting the following message to the slave LVs:

$$\{ID,\ E_{master\text{-}LV}[t_s,\ FLG,\ ID\text{-}1,\ D_{LV\text{-}1}[ID\text{-}1,\ B,\ t],\ ID\text{-}2,\ D_{LV\text{-}2}[ID\text{-}2,\ B,\ t],\ \ldots,\ ID\text{-}K,\ D_{LV\text{-}K}[ID\text{-}K,\ B,\ t]]\},$$

where *ID* indicates the master LV's identity, $E_{master\text{-}LV}[\ ]$ denotes an encryption operation using the master LV's private key, t_s is a timestamp, *FLG* is a flag indicating whether DRT or DDT should be carried out, *ID-i* ($i = 1, \ldots, K$, where K is the number of slave LVs) denotes the identity of a slave LV, $D_{LV\text{-}i}[\ ]$ represents an encryption operation with a slave LV's public key, *ID-LV* denotes the identity of a slave LV, B denotes the spectrum band in which location verification should be carried out, and t is the start time for the location verification procedure. Note that although the broadcast message reveals the sender's identity, it does not necessarily reveal the sender' position when an anonymous communications protocol is employed [22]. A slave LV that has received the broadcast message decrypts the appropriate portions of the message with its own private key and the master LV's public key. According to the information revealed in the decrypted message, the LV either measures the RSS (when DRT is indicated) or records the time of the first two consecutive pulses or rising/falling edges (when DDT is indicated) observed after time t. Suppose that the master LV has instructed the slave LVs to measure the RSS of a particular signal. A slave LV replies to the master LV with the following message:

$$\{ID\text{-}i,\ E_{LV\text{-}i}[t_s],\ D_{master\text{-}LV}[E_{LV\text{-}i}[B,\ t,\ t_a,\ x_{ID\text{-}i},\ y_{ID\text{-}i},\ P_{ID\text{-}i}]]\},$$

where *ID-i* is the sending slave LV's identity, $E_{LV\text{-}i}[\ ]$ denotes an encryption operation using the sender's private key, $D_{master\text{-}LV}[\ ]$ denotes an encryption operation with the master LV's public key, $(x_{ID\text{-}i},\ y_{ID\text{-}i})$ is the position of the sender, and $P_{ID\text{-}i}$ is the RSS measurement value in band B at time t_a, which is the time when the signal is first observed. If the master LV had instructed the LVs to record the times of the first two consecutive pulses (or two consecutive rising edges/falling edges of symbols when the signal source is transmitting digital TV signals), then the LV replies with the message

$$\{ID\text{-}i,\ E_{LV\text{-}i}[t_s],\ D_{master\text{-}LV}[E_{LV\text{-}i}[B,\ t,\ x_{ID\text{-}i},\ y_{ID\text{-}i},\ t_{ID\text{-}i\text{-}1},\ t_{ID\text{-}i\text{-}2}]]\}.$$

The above message replaces $P_{ID\text{-}i}$ and t_a with $t_{ID\text{-}i\text{-}1}$ and $t_{ID\text{-}i\text{-}2}$, which are the times when the first two consecutive synchronization pulses are seen. Two measurements are required because DDT requires that two LVs measure the same pulse. If only one measurement is taken starting from time t, then two LVs may be measuring two different pulses. When two consecutive measurements are taken, as long as two LVs are distanced closer than what the signal can travel within the time period between two consecutive pulses, there is at least one pulse that the two LVs have both measured (i.e., the pulse that is received at the two LVs within the time interval of δ / 2, as explained in subsection III.C). After receiving the messages from the slave LVs, the master LV carries out either DRT or the DDT as described in Section III.

V. SIMULATIONS

In this section, we present the simulation results for DRT and DDT. In particular, we focus on the impact of measurement error on the false negative ratio, which represents the probability of a PUE attacker passing location verification.

A. Simulation settings

The network layout used in the simulations is shown in Fig. 7. The CR network is located within a 2000m × 2000m square area A_1. The primary signal transmitter, a TV tower, is located at either position L_1 or L_2 in the figure. The former represents the scenario in which the transmitter is within the area spanned by the CR network, and the latter represents the scenario in which the transmitter is outside this area. We assume that a single PUE attacker equipped with a hand-held CR can be located either inside area A_1 or inside area A_2. Note that area A_2 is relatively close to area A_1 because the transmission range of the attacker's CR is rather limited. The

placement of A_2 and L_2 on the same side of A_1 represents the worst case—compared to other possibilities, in this case the relative position between the attacker and the LVs will be most similar to the relative position between the TV tower and LVs, so that the distance ratio or distance gap induced by an attacker in A_2 will be more likely to be close to that induced by L_2. The simulation experiments were carried out in four different settings; these are:

- Setting 1: the attacker is in A_1 and the primary user is at L_1.
- Setting 2: the attacker is in A_1 and the primary user is at L_2.
- Setting 3: the attacker is in A_2 and the primary user is at L_1.
- Setting 4: the attacker is in A_2 and the primary user is at L_2.

The attacker's transmitter was placed randomly within the area specified by the setting and each curve shown in Figs. 8 and 9 is the averaged result of 300 iterations. The LVs were placed randomly within A_1, and each curve is the averaged result of 100 iterations.

B. Simulation results

Figs. 8 and 9 show the simulation results for DRT and DDT, respectively. The false negative ratio is plotted as a function of the error value. As expected, the increase in the number of LVs caused a decrease in the false negative ratio.

The results indicate that the location of the attacker's transmitter relative to the primary signal transmitter has a noticeable impact on the false negative ratio. From Fig. 8, we can see that DRT performed poorly in Setting 2 and Setting 4 compared to its performance in the other two settings. The common feature shared by Settings 2 and 4 is that the primary signal transmitter is far away from area A_1 which is where the LVs are located. Hence, irrelevant of which two LVs were chosen, the distance between an LV and the primary signal transmitter would be similar to the distance between the other LV and the primary signal transmitter, thus resulting in a reference distance ratio close to one. In other words, increasing the number of LVs would not contribute significantly to the heterogeneity of the reference distance ratio values. For this reason, increasing the number of LVs, in Settings 2 and 4, did not decrease the false negative ratio dramatically as it did in Settings 1 and 3.

We also notice that DRT showed the poorest performance in Setting 4. This can be attributed to the fact that, in Setting 4, the attacker's transmitter is located in a region that is disjoint with the region that contains the LVs. This would decrease the heterogeneity of the measured distance ratios, thus increasing the false negative ratio even further compared to DRT's performance in Setting 2.

From Fig. 9, we can see that DDT's performance is less sensitive to the locations of the attacker's transmitter and the primary signal transmitter.

It should be noted that the false negative ratio values plotted in Figs. 8 and 9 are only confined to location verification. The other verification procedures in the transmitter verification procedure (see Fig. 4) also need to be considered to derive the overall false negative ratio.

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 [3], Challapali et. al propose to use the Hough transform and autocorrelation function to detect spectrum opportunities. In [15], the authors proposed an approach that observes an incumbent signal's signal-to-noise ratio (SNR) and entropy for seeking spectrum opportunities. A spectrum opportunity is recognized only when both the SNR and the entropy are low in the spectrum band of interest. These two schemes use the collocated sensing architecture, since a single secondary user device performs spectrum sensing and independently decides which spectrum band to use. In such approaches, however, the accuracy of spectrum sensing is unreliable due to various factors such as the limited sensitivity of a CR. To address this problem, *cooperative* spectrum sensing techniques were investigated in [6, 19, 21].

The design of MAC protocols for CR networks is another area of research that is active. To date, most of the proposed MAC protocols are more or less derived from conventional wireless MAC protocols. For example, DC-MAC [23] is a slotted MAC protocol similar to ALOHA but with an enhanced mechanism to optimize per-slot throughput; the DOSS protocol [12] was derived from MAC protocols based on busy tones; and the CR MAC protocol proposed in [16] is a modification of a MAC protocol designed for multi-channel 802.11.

The work presented in this paper is also related to the existing body of research on the location verification problem. The location verification schemes in [1] and [14] were designed to be used in sensor networks or wireless cellular networks. The two schemes require interaction between the localization object and the verifier(s), thus making the schemes not viable for verifying the location of primary signal transmitters in CR networks. In [7], location verification is used for authenticating Direct Broadcasting Satellite (DBS) receivers. The authors proposed three alternative techniques: a technique that uses the GPS, a technique based on cellular telephony, and a technique based on satellite ranging. The last technique measures the phase shift in the satellite signal

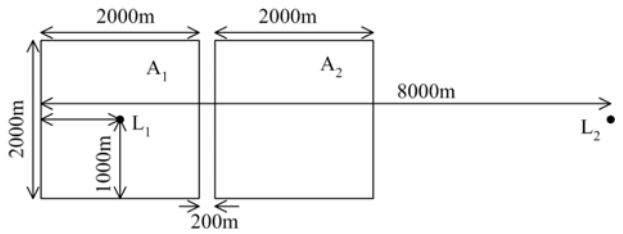
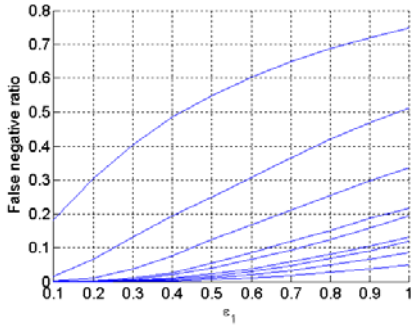
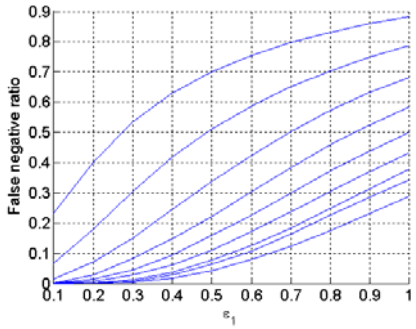


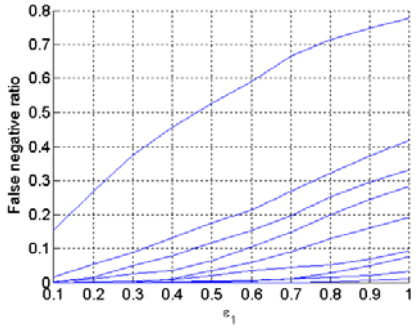
Fig. 7. The network layout used in the simulations.



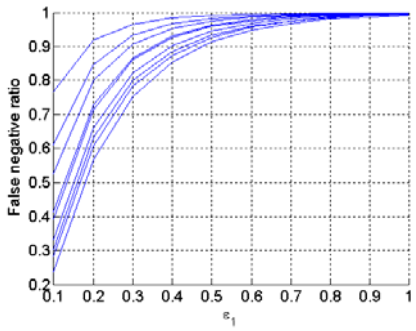
(a)



(b)

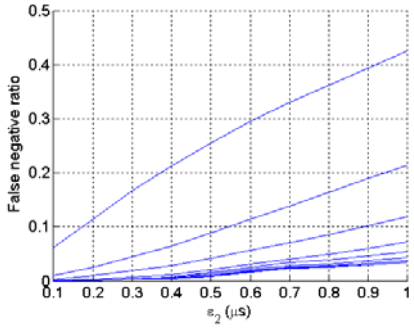


(c)

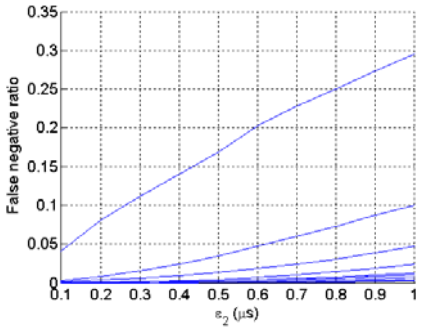


(d)

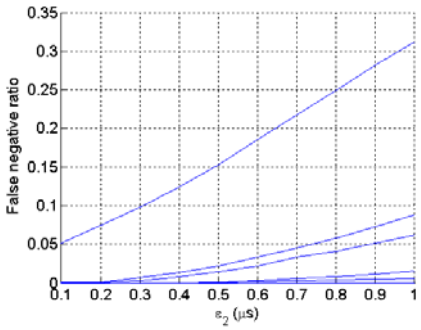
Fig. 8. DRT simulation results. There are nine curves in each plot. The nine curves, from top to bottom, were obtained by incrementing the number of LVs by one, starting from 2 to 10. (a) Setting 1; (b) Setting 2; (c) Setting 3; (d) Setting 4. The value ε_1 denotes the measurement and modeling error.



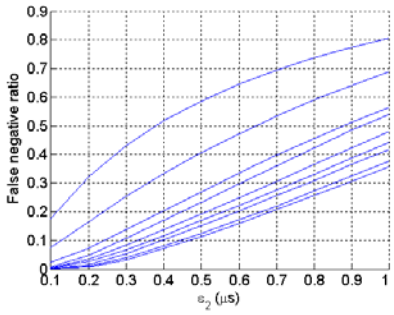
(a)



(b)



(c)



(d)

Fig. 9. DDT simulation results. There are nine curves in each plot. The nine curves, from top to bottom, were obtained by incrementing the number of LVs by one, starting from 2 to 10. (a) Setting 1; (b) Setting 2; (c) Setting 3; (d) Setting 4. The value ε_2 denotes the time measurement error.

relative to a synchronized clock. Although this technique is somewhat similar to DDT in that they both rely on the difference of radio's time-of-flight measurements, there is an important difference between the two: DDT verifies the location of the transmitter while the other technique verifies the location of the receiver.

VI. Conclusions and Future Work

In this paper, we have identified the PUE attack problem and demonstrated its disruptive effects in CR networks. We have proposed a *transmitter verification procedure* for detecting such an attack. One of the distinguishing features of the proposed transmitter verification procedure is the fact that it uses the transmitter's position in the verification process. We have proposed two different *location verification* schemes—DRT and DDT—that can be integrated into the aforementioned transmitter verification procedure. Simulation results show that several factors, such as the location of the attacker's transmitter relative to the LVs, can impact the performance of the two schemes.

Detection is only the first step in countering PUE attacks. Perhaps a more challenging problem is devising effective ways of responding to an attack once it has been detected. As part of our future research, we plan to develop such countermeasures for PUE attacks.

References

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

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

[3] K. Challapali, S. Mangold and Z. Zhong, "Spectrum agile radio: Detecting spectrum opportunities", *6th Annual International Symposium on Advanced Radio Technologies*, March 2004.

[4] Federal Communication Commission, "Notice for Proposed Rulemaking (NPRM 03-322): Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies," *ET Docket, No. 03-108*, Dec. 2003.

[5] 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.

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

[7] E. Gabber and A. Wool, "How to prove where you are: tracking the location of customer equipment," *Proceedings of the 5th ACM conference on Computer and communications security (CCS'98)*, Nov. 1998, pp. 142–149.

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

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

[10] M. G. Kuhn, "An asymmetric security mechanism for navigation signals," *Information Hiding Workshop*, May 2004, pp. 239–252.

[11] T. Locher, R. Wattenhofer, and Aaron Zollinger, "Received-Signal-Strength-Based Logical Positioning Resilient to Signal Fluctuation," *1st ACIS International Workshop on Self-Assembling Wireless Sensor Networks (SAWN)*, May 2005.

[12] L. Ma, X. Han, and C.-C. Shen, "Dynamic open spectrum sharing MAC protocol for wireless ad hoc networks," *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN 2005)*, Nov. 2005, pp. 203–213.

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

[14] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," *Proceedings of the 2003 ACM workshop on Wireless security*, Sept. 2003, pp. 1–10.

[15] 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," *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN 2005)*, Nov. 2005, pp. 170–179.

[16] P. Pawelczak, R. V. Prasad, X. Liang Xia, and I. G. M. M. Niemegeers, "Cognitive radio emergency networks - requirements and design," *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN 2005)*, Nov. 2005, pp. 601–606.

[17] P. Pawełczak, *Protocol requirements for cognitive radio networks*, AAF Deliverable WP4.11, TU. Delft, June 2005.

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

[19] S. Shankar N, C. Cordeiro, and K. Challapali, "Spectrum agile radios: utilization and sensing architectures," *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN 2005)*, Nov. 2005, pp. 160–169.

[20] E. P. J. tozer, *Broadcast Engineer's Reference Book*, Elsevier, 2004.

[21] B. Wild and K. Ramchandran, "Detecting primary receivers for cognitive radio applications," *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN 2005)*, Nov. 2005, pp. 124–130.

[22] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," *24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2005)*, Mar. 2005, pp. 1940–1951.

[23] Q. Zhao, L. Tong, and A. Swami, "Decentralized cognitive mac for dynamic spectrum access," *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN 2005)*, Nov. 2005, pp. 224–232.