A Primary User Authentication System for Mobile Cognitive Radio Networks

(Invited Paper)

Swathi Chandrashekar and Loukas Lazos
Dept. of Electrical and Computer Engineering
University of Arizona, Tucson, AZ, USA
{swathic, llazos}@ece.arizona.edu

***Abstract*—Cognitive radio networks (CRNs) exploit the idle portion of the licensed spectrum to establish network communications. Essential to the co-existence of this technology with legacy systems, is the reliable sensing of spectrum opportunities. However, existing spectrum sensing techniques are vulnerable to adversaries that mimic the characteristics of Primary User (PU) transmissions in order to reduce the bandwidth availability for the CRN. In this paper, we address the problem of authenticating the PU signal in order to mitigate PU emulation attacks. We propose a PU authentication system based on the deployment of "helper" nodes, fixed within the geographical area of the CRN. Our system relies on a combination of physical-layer signatures (link signatures) and cryptographic mechanisms to reliably sense PU activity and relay information to the CRN. Compared to prior work, our system can accommodate mobile secondary users and can be implemented with relatively low-power helpers.**

I. Introduction

Cognitive radio technology is expected to increase the spectrum utilization by allowing opportunistic use of the idle portion of the licensed spectrum by Secondary (unlincensed) Users (SUs) [1], [9], [15], [17]. The Federal Communications Commission (FCC) mandates that SUs are allowed to access licensed bands as long as they do not interfere with the transmissions of Primary (licensed) Users (PUs) [7]. Pivotal to the co-existence of SUs with legacy systems, is the implementation of robust spectrum sensing mechanisms.

Existing spectrum sensing methods rely on physical-layer characteristics of PU transmissions such as energy, spectral power density, modulation, cyclostationary features [9], [17] and pilot information. However, these methods do not authenticate the PU signal. An adversary equipped with a software defined radio can mimic the transmission characteristics of a PU in order to emulate PU activity on idle portions of the spectrum. The goal of this attack is to block SUs from utilizing the idle channels, thus reducing the available bandwidth and degrading the network performance.

As an example, Fig. 1 shows a SU sensing the idle spectrum in the presence of an adversary. Assume that a total of 10 channels are available to the legacy system, and that channels $(1, 3)$ and $(2, 4, 5)$ are occupied by two PUs within the range of the SU. In a non-adversarial setting, the SU would have sensed channels $(6, 7, 8, 9, 10)$ as idle. However, in the presence of an adversary emulating PU activity on channels $(6, 7, 8)$, the set of idle channels sensed by the SU is limited to $(9, 10)$.

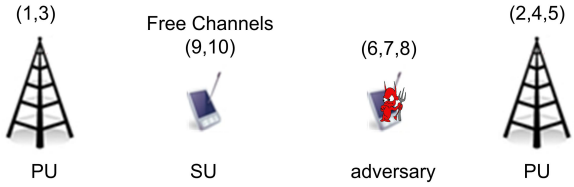

Fig. 1. Primary user emulation attack scenario.

Main Contributions–We propose a PU authentication system that securely and reliably delivers PU activity information to SUs. Our system does not require any modifications to the legacy system, as mandated by the FCC [7]. Provision of robust sensing information is facilitated by the deployment of a set of "helper" nodes. Similar architectures have been adopted in the past for detecting PUs (e.g., [4], [11], [15]). Helpers are deployed within the area of the secondary network, independent of the location of the PUs, and can be relatively cheap low-power devices. Moreover, the location of the PUs need not be known. Similarly to [11], our system relies on a combination of RF and cryptographic signatures. However, no SU training is necessary every time the location of a SU changes. Hence, our system is suitable for mobile CRNs.

Paper Organization–The remainder of the paper is organized as follows. In Section II, we present related work. The system and threat models are detailed in Section III. Section IV presents the proposed PU authentication system. We analyze the security of our system in Section V, and we present our conclusions in Section VI.

II. Related Work

The problem of PU signal authentication has received attention only recently [2], [4], [5], [11]. Chen et al. proposed an authentication method based on a network of monitoring nodes which verify the origin of PU signals using received signal strength (RSS) measurements [4]. If the estimated location of a PU deviates from the known PU location by a threshold, the signal is assumed to be emulated. However, location distinction methods based on RSS can be circumvented if the adversary employs antenna arrays [12].

Liu et al. proposed a PU authentication system assisted by helper nodes deployed in close proximity to the PUs [11]. Similar to our system, the authors employed a combination of cryptographic and RF signatures to authenticate PU activity.

However, there are distinct differences between the two systems. In [11], helpers are physically bound to PUs which may be TV towers with thousands of watts of transmission power, covering an area of tens of square miles [15]. Bi-directional communication between the helpers and the SUs requires both types of devices to have communication ranges similar to that of TV towers. In our system, helpers need only be deployed within the area of the SUs, independent of the location of the PUs. Hence, the helpers can be low-power. Moreover, in [11], a training phase is required before a SU can robustly sense PU activity. This phase must be repeated with every location change of the SU. In our system, the training phase is limited between the PUs and the helpers which are both stationary. Therefore, it need not be repeated due to SU mobility.

Anard et al. proposed an analytical model for detecting primary user emulation attacks [2]. In their system model, malicious devices emulating the PU signal are deployed at fixed locations, at least R_0 units away from any SU. Using simplified propagation models, they compute the probability of a successful PU emulation. Finally, Chen et al. modelled the PU emulation problem as an estimation theory problem [5].

III. Problem, Assumptions, and Threat Model

A. System Model

Our system consists of a set of PUs, co-existing with a CRN. PUs are licensed to use a fixed spectrum, which can be divided to a set $\mathcal{M} = \{1, 2, \ldots, m\}$ of m orthogonal frequency bands, referred to as *channels*. The PUs are assumed to be stationary (e.g., TV or cellular towers). The SUs are allowed to opportunistically use the set of channels $\mathcal{M}$, if they do not cause interference on PU communications. For this purpose, SUs are fitted with cognitive radio engines that can sense the spectrum using methods such as energy detection, cyclostationary feature extraction, and pilot signals [1], [9], [15], [17]. The SUs are assumed to be mobile. To provide PU signal authentication, we introduce a set of stationary helper nodes equipped with cognitive radio devices. Helpers cover the geographical area where SUs are deployed. To securely communicate with SUs, helpers are initialized with public/private keys and certificates from a trusted authority. Finally, helpers are assumed to be loosely synchronized.

B. Threat Model

The goal of the adversary is to mislead the SUs regarding the available spectrum opportunities, thus preventing them from utilizing idle channels. To achieve his goal, the adversary is capable of emulating the primary radio signal characteristics. This can be easily achieved if the adversary is equipped with a software defined radio, or records and replays primary radio signals. While the adversary can be present at any location within the deployment area, he cannot place a transceiver in close proximity to a PU. PUs are assumed to be physically secure, as mandated by the FCC.

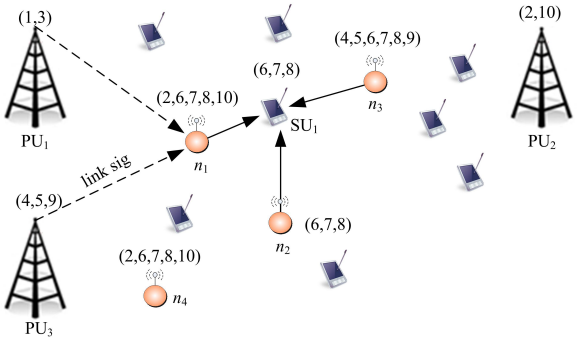

Fig. 2. System architecture.

IV. PU Authentication System

A. System Architecture

The problem of authenticating the PU signal at the SU can be modelled as a two-party authentication problem. The latter is well studied in the literature and can be addressed using known cryptographic primitives such as public key or symmetric key cryptography [14]. The technical challenge in applying such methods for PU signal authentication, however, is that, according to the FCC specifications [7], no modifications are allowed on the PU network.

Alternatively, SUs may authenticate PU signals by exploiting the unique characteristics of the RF channel. It has been shown that *link signatures* can be used to distinguish RF sources positioned at distinct locations [12]. For a SU sensing the spectrum, as long as the location of a PU remains static, the RF characteristics of its transmission can serve as a unique signature. This is achieved by sampling the RF channel during a training period and extracting unique features of the RF channel such as the impulse response. However, the RF signature between a PU and a SU changes if the SU is mobile, leading to the frequent repetition of the training process. This requirement poses additional challenges that have to be addressed. Firstly, the training period has to be kept short so that the sensing process remains within the mandated period of 2 seconds [7]. Secondly, SUs must have a mechanism for authenticating the PU training signals, every time their location changes.

To overcome the aforementioned challenges, we propose a PU authentication system that relies on the deployment of stationary helper nodes. These nodes are responsible for, (a) authenticating the PU signal and, (b) broadcasting spectrum status information. Initially, the helpers authenticate the PU signal using link signatures. Since both the helpers and the PUs are stationary, there is no need for repeating the training process after the initial training is completed. In the second phase, the helpers convey spectrum availability information to the SUs via a secure broadcast operation. This design can accommodate mobile SUs that do not need to be trained with every location change. The proposed system architecture is shown in Fig. 2. Four helpers sense the the activity of three PUs using link signatures, and determine the set of idle channels. The spectrum information is conveyed to the SU,

which computes the idle portion of the spectrum.

B. Authentication Mechanism

In this section, we describe the two steps of the spectrum authentication mechanism, i.e., the authentication of the PU signal at the helpers and the secure broadcasting of spectrum status information from the helpers to the SUs.

a) PU signal authentication at the helpers: To authenticate PU signals, a location distinction mechanism using multipath-based link signatures is employed. Authors in [12], [16] showed that a time-variant mutlipath fading channel between two fixed locations provides sufficient "uniqueness" to serve as a fingerprint of the fixed relationship between these locations. We briefly describe the link signature mechanism proposed in [12], in the context of PU-helper authentication. When PU i transmits a signal $s_i(t)$, helper j receives signal

$$r_j(t) = h_{ij}(t) \star s_i(t) = \sum_{\ell=1}^{L} \alpha_\ell e^{j\phi_\ell} s_i(t - \tau_\ell) \qquad (1)$$

where $h_{ij}(t)$ denotes the impulse response of the unique channel between i and j, "$\star$" denotes the convolution operation, and L denotes the distinct multipath components of $s_i(t)$ at the receiver, each one delayed by t_ℓ and phase-shifted by ϕ_ℓ. To obtain the desired impulse response, operations in the frequency domain yield

$$H_{ij}(f) = \frac{1}{P_s}|S_i(f)|^2 R_j(f) = \frac{R_j(f)}{S_i(f)}, \qquad (2)$$

where P_s denotes the transmission power at the sender, and $X(f)$ denotes the Fourier transform of a signal $x(t)$. To construct a link signature represented by $H_{ij}(f)$ or $h_{ij}(t)$, the $s_i(t)$ must be known at the helper. For this purpose, link signatures can be constructed using known sequences employed by the PUs for control. For instance, digital TV transmissions consist of a sequence of segments. For every 313 segments, a Data Field Sync segment of one known 511-bit PN sequence, and three known 63-bit PN sequences is used for synchronization [6]. Given that $S_i(f)$ of a PN sequence is approximately flat within the transmitted frequency band, the impulse response $H_{ij}(f)$ can be computed based on (1).

To obtain the impulse response, the helper samples the PU signal during the transmission of the known signal and stores the necessary samples to robustly "fingerprint" the fixed RF channel. During this training phase, which needs to be performed only once, it is assumed that no adversary is present. Once a link signature for a given PU has been constructed, the helper can authenticate subsequent transmissions by comparing their characteristics to the stored link signature. Note that the helper continues to sample the RF channel for keeping an up-to-date history of the channel's multipath components and their temporal variations.

Using link signatures, a helper i constructs an occupancy vector V_i indicating the set of channels where legitimate PUs are active. V_i is an m-bit vector (m is the number of channels of the legacy system). The j^{th} bit of V_i is set to zero if channel j is currently idle. Otherwise, it is set to one. For instance, in a system with $m = 10$ channels, an occupancy vector $V = [1001010000]$ indicates that channels 1,4 and 6 are occupied by legitimate PUs. The spectrum sensing process is repeated at the helpers at the frequency mandated by the FCC (e.g., every 2 seconds [7]).

Algorithm 1 Spectrum Authentication (SA) Algorithm

1: SU j collects all messages $m_i,\ i = 1, \ldots, k$ from the set of helpers $\mathcal{K}$ within its range.
2: For each $m_i \in \mathcal{K}$ SU j verifies the authenticity and integrity of m_i using $sig_i(m_i)$. Messages m_i that fail to be authenticated are discarded.
3: SU j checks if the transmission sequence number SN_i of each m_i is current. m_is with older SN_is are discarded.
4: SU j performs a location consistency test by checking if $|L_a - L_b| \leq 2r\ \forall a, b \in \mathcal{K}$. Here, r denotes the communication range of the helpers.
5: If the location test is consistent $\forall a, b \in \mathcal{K}$, the occupancy vector V of SU j is computed using an OR operation between all legitimate V_i's [13]. That is, $V = \cup V_i$.
6: If m_a, m_b are found such that, $|L_a - L_b| > 2r$, SU j employs the Helper Resolution (HR) algorithm to discard rogue $m_i's$.
7: Once all inconsistent messages have been discarded, the occupancy vector V is computed as in Step 5.

b) Secure distribution of authentic spectrum information to the SUs: The helpers are responsible for distributing spectrum information to the SUs. Contrary to the work in [11], in our design, this is achieved using solely cryptographic methods. This is preferred to avoid the need for frequent SU training due to mobility. A helper i periodically transmits the following information:

$$m_i || sig_i(m_i), \quad m_i : V_i || L_i || SN_i. \qquad (3)$$

Here, $L_i = (X_i, Y_i)$ denotes the location of helper i, SN_i denotes a transmission sequence number used for verifying the freshness of V_i, and $sig_i(m_i)$ denotes the signature of i on m_i. To avoid frequent the frequent broadcast of spectrum information, the helpers update the SUs if, (a) a change in PU activity has been sensed, (b) a threshold period of time has passed since the last update or, (c) a SU moving to a new location has requested for an update. Note that for PUs such as TV stations, the dynamics of PU activity are expected to be low (in the order of hours). Therefore, while the helpers continuously monitor the spectrum status, a frequent update of the SUs is not necessary.

Once an SU node j has obtained the occupancy vectors V_i from nearby helpers, it executes the Spectrum Authentication (SA) algorithm shown in Algorithm 1. Here, we assume that the network of helpers is synchronized to the same transmission sequence number. The SA algorithm includes several cryptographic and topology consistency checks to ensure that the spectrum information obtained by SUs is authentic and fresh. In the security analysis Section, we show how the SA

algorithm prevents adversaries from distorting the spectrum availability, and present the helper resolution algorithm.

V. Security Analysis

In this section, we show that the proposed PU authentication system is robust to various possible security threats.

A. PU emulation attack

In a PU emulation attack, the adversary can try to impersonate the features of a PU signal on the idle portion of the spectrum. This can be achieved by mimicking features of PU transmissions such as power, modulation type, synchronization sequences etc., or by recording and replaying PU transmissions [4], [11]. In this attack, the adversary must convince helpers that the emulated signal originates from an authentic PU.

However, the unique characteristics of the RF channel exploited in the construction of link signatures, prevent this type of attack. In order for this attack to be successful, the adversary must be located at very close proximity to a PU (less than 3m [12]). Assuming that PU such as TV and cellular stations are physically protected, as recommended by FCC regulations, it would not be possible to place an emulation transmitter close to a PU. Therefore, the occupancy vectors constructed by the helpers accurately reflect the PU activity.

B. Helper Impersonation Attacks

The adversary may attempt to impersonate a helper in order to provide false occupancy vectors to the SU. The use of signatures for authenticating the broadcast of the messages m_i containing the occupancy vectors, prevent the adversary from fabricating false spectrum information.

Without the opportunity of fabricating authentic messages, the adversary may choose to replay old ones, already broadcasted by the helpers. These replays will pass the signature verification test at the SUs since they originated from legitimate helpers and contain valid signatures. To avoid such replay attacks, the transmission sequence number SN_i is included with the broadcast of messages m_i. Assuming that a SU under attack hears at least one legitimate helper, the SN of the legitimate helper will be different (larger) than the SN of the replays. Here, we exploit the fact that the network of helpers is loosely synchronized to the same SN. If a SU receives m_is with older SN_is, he discards them as old replays.

If the SUs are not guaranteed to be within range of at least one legitimate helper at all times, it is possible that replay attacks are successful. To deal with cases of SUs isolated from legitimate helpers, a stronger condition of synchronization between the helpers and the SUs is required. The helpers timestamp messages m_i to prevent stale information from being replayed. Using the timestamp, SUs can reject replays even if fresh broadcasts from legitimate helpers are not available.

Finally, the adversary may replay spectrum authentication messages via a wormhole tunnel between two (or more) parts of the network [8]. This attack is depicted in Fig. 3. The adversary deploys a fast link (wired or long-range wireless) between two parts of the network A and B. He then records broadcasted information on one end, transmits it via the wormhole tunnel to the other end and replays it. Because messages m_i transmitted by the helpers are only *loosely* synchronized to the same SN value, a fast tunnelling and replay may contain m_is with up-to-date SN_is.

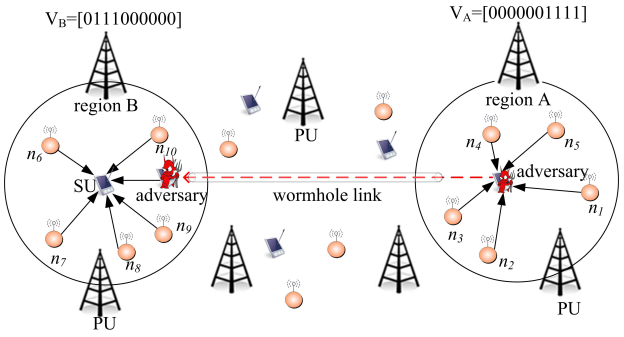

Fig. 3. Replay of helper broadcasts via a wormhole tunnel. Scenario 1: $V_A = [0000001111]$, $V_B = [0111000000]$, $V^* = [0111000000]$. Scenario 2: Adversary emulates PU signal in channels 7,8,9 and 10 so that $V^* = [0111001111]$.

Algorithm 2 Helper Resolution (HR) Algorithm

1: Initialize: $|L_a - L_b| > 2r$. Set of helpers $\mathcal{K}$.
2: Place all $i \in \mathcal{K}$ s.t. $|L_a - L_i| \leq 2r$ in group A.
3: Place all $i \in \mathcal{K}$ s.t. $|L_b - L_i| \leq 2r$ in group B.
4: Sense spectrum to construct own occupancy vector V^*.
5: Compute $V_A = \cup_A V_i$ and $V_B = \cup_B V_i$.
6: Compute counters $c_A(c_B)$ indicating the number of occupied channels in V_A (V_B), but not in V^*.
7: If $c_A > \varepsilon$ $(c_B > \varepsilon)$, discard V_A (V_B), $V^* \leftarrow V_B$ $(V^* \leftarrow V_A)$.
8: Else, locate closest helper using timing-based methods.

Wormhole attacks are detected by the location consistency checks of the SA algorithm. Let r be the communication range of the helpers. A broadcast received by a SU must originate from helpers located within a radius r from the SU's location. Therefore, the pairwise distance between two helpers a, b heard at the same SU, cannot be longer than $2r$. The SU uses the location consistency check to verify that the set of helpers he hears is consistent. If spectrum authentication messages from part A are replayed via a wormhole tunnel to part B, the helpers' locations included in each m_i will fail the location consistency test and reveal the wormhole attack.

Note that in our location test method, SUs are not required to be aware of their location (no GPS is necessary at the SUs). The location information of the helpers is sufficient to perform the test. However, without own location information, the SU cannot distinguish the set of helpers located nearby from the ones replayed. To resolve this ambiguity, the SU utilizes the Helper Resolution (HR) algorithm described in Algorithm 2.

To illustrate the steps of the HR algorithm, assume that the SU received two messages m_a, m_b for which $|L_a - L_b| > 2r$. The SU groups the helpers which are "location-consistent" with L_a on a group A and those who are location-consistent with L_b on a group B. For each group, it computes the

spectrum occupancy vectors $V_A = \cup_A V_i$ and $V_B = \cup_B V_i$. The SU uses its own occupancy vector V^* constructed by sensing the spectrum in order to discard replayed messages. The following attack scenarios are possible.

Attack Scenario 1–In the first scenario, the adversary simply replays information from far away helpers. Given the spatial variation of PU activity, occupancy vectors V_A and V_B are likely to be different, with the occupancy vector corresponding to nearby helpers being similar to V^*. On the other hand, the occupancy vector corresponding to replayed information likely indicates idle channels as occupied. To exploit this inconsistency, for each of the two vectors V_A and V_B, the SU computes counters c_A and c_B that indicate the number of channels that were sensed idle in V^*, but were marked occupied by a group of helpers. For example, counter c_A is increased by one if, for the i^{th} channel, $V^*(i) = 0$ and $V_A(i) = 1$. If the counter c_x increases more than a threshold value ε for a group of helpers X, occupancy vector V_X is rejected as a replay. Note that channels that are marked as occupied in vectors corresponding to the two groups and also sensed as occupied in V^* are not taken into account in the group selection process. This is because V^* may be distorted by a PU emulation attack.

To illustrate attack scenario 1, consider Fig. 3. The SU has identified that $|L_1 - L_6| > 2r$. SU creates two groups A, B with memberships $A = \{n_1, n_2, n_3, n_4, n_5\}$ and $B = \{n_6, n_7, n_8, n_9, n_{10}\}$ The corresponding occupancy vectors are, $V_A = \cup_{i=1}^{5} V_i = [0000001111]$ and $V_B = \cup_{i=6}^{10} V_i = [0111000000]$. Moreover, $V^* = [0111000000]$, since the SU is located in region B. The detection threshold value is set to $\varepsilon = 2$. The counter for group A is $c_A = 4 > \varepsilon$ while the counter for group B is $c_B = 0 < \varepsilon$. Therefore, V_A is discarded and the SU accepts V_B as the valid occupancy vector. However, the adversary can launch a more elaborate attack described in scenario 2.

Attack Scenario 2–In the second attack scenario, the adversary combines a wormhole attack with a PU emulation attack. The goal of the PU emulation attack is to distort the occupancy vector V^* sensed by the SU. Scenario 2 is illustrated with the assistance of Fig. 3. The adversary replays spectrum authentication messages from region A to region B as in scenario 1. However, in order to avoid the rejection of V_A based on the counter c_A, he emulates PU activity close to the SU, at occupied channels in region A. Therefore, the occupancy vector at the SU becomes $V^* = [0111001111]$. In this case, both counters c_A and c_B remain below ε for both groups A and B. To resolve this ambiguity, timing-based methods can be employed to identify which of the conflicting helpers is close to the SU [3], [10]. Once the close-by helper is identified (helper n_6), the SU rejects the occupancy vector of one of the groups.

VI. Conclusions

We addressed the problem of PU authentication in cognitive radio networks. We proposed an authentication system that relies on the deployment of a network of helper nodes for verifying the availability of idle spectrum. Compared to prior proposals, our system can accommodate mobile SUs without the need for repeated training with every location change. Moreover, the network of helpers is limited to the deployment area of the SUs and is decoupled from the PUs' locations. Our security analysis showed that our authentication system can withstand impersonation attacks of the PUs as well as of the helpers nodes.

Acknowledgments

This research was supported in part by the National Science Foundation (under NSF grants CAREER CNS-0844111 and CNS-1016943). Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of NSF.

References

[1] I. Akyildiz, W. Lee, M. Vuran, and S. Mohanty. NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey. *Computer Networks*, 50(13):2127–2159, 2006.

[2] S. Anand, Z. Jin, and K. Subbalakshmi. An analytical model for primary user emulation attacks in cognitive radio networks. In *Proceedings of IEEE DySPAN*, pages 1 –6, 2008.

[3] S. Capkun and J. Hubaux. Secure positioning in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2):221–232, 2006.

[4] R. Chen, J. Park, and J. Reed. Defense against primary user emulation attacks in cognitive radio networks. *IEEE Journal on Selected Areas in Communications*, 26(1):25–37, 2008.

[5] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Raez. Modeling primary user emulation attacks and defenses in cognitive radio networks. In *Proceedings of the 28th IEEE International Performance Computing and Communications Conference (IPCCC)*, pages 208 –215, 2009.

[6] A. T. S. Committee. ATSC digital television standard (a/53) revision e, with amendments no. 1 and 2,. http://www.atsc.org/cms/, 2006.

[7] FCC. Second report and order and memorandum opinion and order, FCC-08-260, 2008.

[8] Y. Hu, A. Perrig, and D. Johnson. Packet leashes: a defense against wormhole attacks in wireless networks. In *Proceedings of INFOCOM*, pages 1976–1986, 2003.

[9] H. Kim and K. Shin. In-band spectrum sensing in cognitive radio networks: energy detection or feature detection? In *Proceedings of MOBICOM*, pages 14–25, 2008.

[10] D. Liu and P. Ning. Detecting malicious beacon nodes for secure location discovery in wireless sensor networks. In *Proceedings of the 25th International Conference on Distributed Computing Systems*, pages 609–619, 2005.

[11] Y. Liu, P. Ning, and H. Dai. Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures. In *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, pages 286–301, 2010.

[12] N. Patwari and S. Kasera. Robust location distinction using temporal link signatures. In *Proceedings of MOBICOM*, page 122, 2007.

[13] E. Peh and Y. Liang. Optimization for cooperative sensing in cognitive radio networks. In *Proceedings of the IEEE Wireless Communications and Networking Conference*, pages 27–32, 2007.

[14] D. Stinson. *Cryptography: theory and practice*. CRC press, 2006.

[15] B. Wild and K. Ramchandran. Detecting primary receivers for cognitive radio applications. In *Proceedings of IEEE DySPAN*, pages 124–130, 2005.

[16] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe. Fingerprints in the ether: Using the physical layer for wireless authentication. In *Proceedings of IEEE ICC*, pages 4646–4651, 2007.

[17] Q. Yuan, P. Tao, W. Wenbo, and Q. Rongrong. Cyclostationarity-based spectrum sensing for wideband cognitive radio. In *Proceedings of the WRI International Conference on Communications and Mobile Computing*, volume 1, 2009.