A PHYSICAL LAYER AUTHENTICATION SCHEME FOR COUNTERING PRIMARY USER EMULATION ATTACK

Kapil M. Borle *Biao Chen* *Wenliang Du*

Syracuse University, Dept. of EECS, Syracuse, NY 13210

ABSTRACT

This paper develops a physical layer user authentication scheme for wireless systems. The approach can be used as an effective counter measure against the primary user emulation attack in cognitive radios. The developed scheme applies to general digital constellations and we establish its optimality in terms of error probability for user authentication. Trade-off analysis is provided that balances the performance of the user authentication for the secondary user and symbol detection for the primary user. In particular, we show that arbitrarily reliable user authentication can be achieved at the price of an almost negligible performance degradation for the primary user under realistic system settings.

Index Terms— cognitive radio, physical layer, security, authentication, primary user emulation attack.

1. INTRODUCTION

In a typical cognitive radio (CR) system [1], a *primary user* (PU) is the spectrum license holder. A *secondary user* (SU) is an unlicensed user who intends to use the spectrum opportunistically. Priority is given to the PU in the sense that a SU can only transmit if its transmission is deemed to be harmless to that of the PU . Often times this is done through the policy that SU is not allowed to transmit whenever the PU is transmitting, a premise adopted in the present work. Consequently, it requires the SU to reliably detect the PU's transmission, which is typically done through either the simple energy detection or more sophisticated schemes involving transmission features of the PU [2, 3, 4]. These approaches, however, can be easily compromised by a malicious *user* who may emulate the characteristics of the PU 's signals. Referred to as the primary user emulation attack (PUEA) [5], such an attack intends to mislead a benign SU into believing that the PU is transmitting, while in fact the PU is silent. This results in spectrum underutilization, thereby defeating the purpose of CR.

An effective countermeasure to PUEA is user authentication, *i.e.*, the SU is capable of authenticating the PU 's transmission. Contemporary authentication solutions exist in layers above the physical layer. For example, IP layer can use IPSec protocol to address the authentication problem, transport layer can use SSL, application layer can use SSH and so on. The problem with these solutions is that they need the PU and the SU to use the same protocol at the layer where authentication takes place and often require recovering at the SU information transmitted by the PU . In many existing and potential applications, the SU and the PU do not necessarily operate the same protocols at these higher layers. Furthermore, they may not even have the same layered network architecture. It is therefore desirable to achieve user authentication at the lowest possible layer. Physical layer authentication, first proposed in [6], appears to be an attractive solution.

The physical layer authentication scheme developed in the present work builds on an earlier approach described in [7]. There, authentication is done in two stages: authentication tag generation using a one-way hash chain and tag embedding through constellation shift. The developed scheme is transparent to the primary receiver, requires minimum alteration of the primary transmitter, and allows simple detection scheme at the *SU*. Note that such a tag embedding scheme resembles that of digital watermarking where the embedded tag needs to induce minimum distortion of the cover signal [8]. The scheme described in [7], however, is suitable only to quadrature phase shift keying (QPSK) and the analysis there uses a simple additive Gaussian channel model. It is not clear *a priori* what is the optimal way of generalizing the tag embedding scheme to more general digital constellations. Moreover, as the one-way hash chain is highly sensitive to tag bit error, it is imperative to carry out a thorough trade-off analysis such that the tag bit detection error probability can be controlled to be arbitrarily small under realistic wireless channel conditions. The present work addresses these two important issues.

2. A PHYSICAL LAYER AUTHENTICATION SCHEME

In this section, we briefly review the authentication scheme presented in [7]. The scheme consists of two stages: tag generation and tag transmission, which we describe below.

2.1. Tag Generation

Tag generation is done using a one-way hash chain [7]. A hash chain is a successive application of a hash function to the input data [9]. A one-way hash function takes in a string of data and returns a fixed length string. It is characterized by the following properties.

Property 1: Given the input string, the output string can be computed easily but given the output string it is computationally infeasible to recover the input string.

Property 2: It is very sensitive to changes in the input, e.g., two input strings that differ by a single bit can give completely different output strings.

The PU sets its initial tag bit string h_n, which is known only to itself. It then uses a hash chain to generate a sequence

The work was supported in part by AFOSR under award FA9550-09-1-0224 and AFRL under Award FA8750-11-1-0040.

of tags.

$$h_n \to h_{n-1} \to \cdots \to h_1 \to h_0, \tag{1}$$

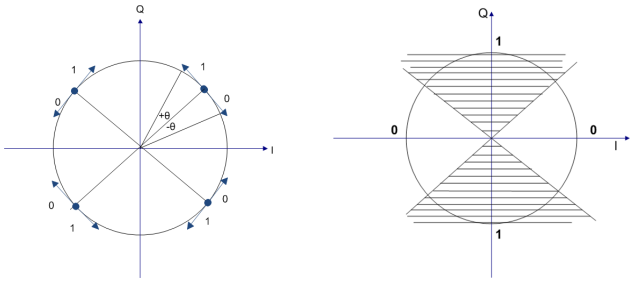
where $h_i = \text{hash}(h_{i+1})$ and $\text{hash}(\cdot)$ is a hash function.

The last tag h_0 is broadcast to all users, hence is known to both the cognitive receivers and any adversaries. The subscript i of h_i indicates the time index during which the PU will transmit the tag h_i. At time $t = 1$, which is indicative of a short time window, the PU transmits h_1. The cognitive receivers, upon receiving the PU's transmitted signal, constructs its estimate of h_1, say, $\hat{h}_1$. It then computes $\hat{h}_0 = \text{hash}(\hat{h}_1)$ and compare it to the known h_0. If $\hat{h}_0 = h_0$, authentication is successful, *i.e.*, the PU is believed to be transmitting. It then continues the authentication processing at the next time interval by estimating h_2 and applying to the hash function and compare with h_1. The process repeats until we use up the entire hash chain. At any interval i, if the computed $\hat{h}_{i-1} = \text{hash}(\hat{h}_i)$ differs from h_i obtained from the previous interval, the SU declares that the signal is not from the legitimate PU and appropriate measures can be taken.

From Property 2, it is clear that at each stage the SU needs to detect the tag bits correctly in order for the authentication process to continue. Therefore, it is imperative that tag bit detection error be controlled to be arbitrarily small.

2.2. Tag Transmission

The bit sequence corresponding to each tag is transmitted by superimposing it over the PU's own transmitted symbols. The scheme described in [7] applies only to QPSK symbols and is illustrated in Fig. 1. If the tag bit is 0, we rotate the QPSK constellation symbol by an angle θ towards the I axis, whereas to transmit tag bit 1 we rotate it towards the Q axis. At the receiver, the maximum likelihood detector detects tag bit 1 if it the received symbol falls in the shaded region while it detects 0 if it falls in the unshaded region. Clearly, the scheme is specialized to QPSK and does not directly apply to general QAM constellations. Additionally, the analysis carried out in [7] assumes an additive Gaussian channel, hence its applicability to wireless channels is not clear.

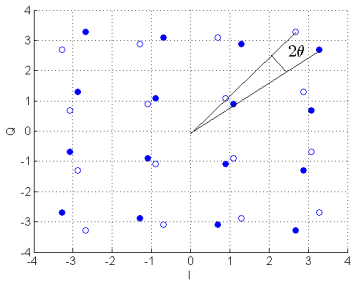


(a) Tag transmission (b) Tag Detection

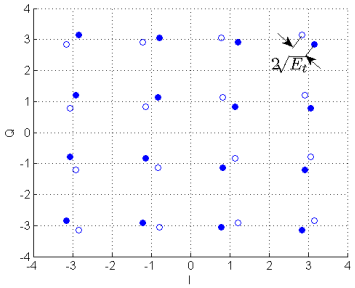
Fig. 1: Tagging scheme for QPSK modulation

We address these limitations in the current work. The contributions of this paper are summarized below.

- Generalize the tagging scheme to arbitrary constellations and prove its optimality for tag detection.
- Provide a trade-off analysis using a Rayleigh fading channel between tag detection at SU and symbol detection at PU .



(a) Tagging over 16 QAM with uniform angular degradation.



(b) Tagging over 16 QAM with uniform energy degradation.

Fig. 2: Constellation Diagrams

3. TAG EMBEDDING FOR GENERAL CONSTELLATIONS

The tag embedding scheme described in [7] can be modified in various ways to apply to more general digital modulations. Two of the natural generalizations are illustrated in Fig. 2. The first scheme is to rotate each constellation point by a fixed angle in the I-Q plane (Fig. 2(a)), with the direction of rotation depending on the polarity of the tag bit. The second scheme is to rotate each constellation point by a constant-length offset (Fig. 2(b)), again, the offset direction depending on the polarity of the tag bit. It is clear that for PSK modulations, the two schemes are identical to each other. For the general QAM modulations, however, the first scheme will result in an SNR degradation of the PU signal that is roughly proportional to the SNR of the constellation point. For the second scheme, a constant SNR degradation is imposed on all constellation points. It is not known *a priori*, however, which scheme yields a better tag detection performance.

We now formally define the two embedding schemes. Let $\mathcal{S} = \{s_0, s_i, \ldots, s_{M-1}\}$ be the original set of constellation points in the I-Q plane for a given digital modulation scheme. Let $t \in \{0, 1\}$ denote the tag bit to be embedded. Tag embedding is thus defined by a mapping from (s_i, t) to a new constellation point $s_{t,i} = g(s_i, t)$ where $g(\cdot)$ is an appropriately defined mapping function. Formally stated, the first scheme, referred to as uniform angular offset, rotates $\mathcal{S}$ by θ if $t = 1$ or $-\theta$ if $t = 0$ depending on the polarity of the tag bit, resulting in two rotated set of constellation points:

$$\mathcal{S}_\theta = \{s_{i,\theta} : s_{i,\theta} = e^{j\theta} s_i,\ s_i \in \mathcal{S}\} \tag{2}$$

$$\mathcal{S}_{-\theta} = \{s_{i,-\theta} : s_{i,-\theta} = e^{-j\theta} s_i,\ s_i \in \mathcal{S}\} \tag{3}$$

where the design parameter $\theta > 0$ is the angle offset. The mapping $g(\cdot)$ is defined simply as $s_{t,i} = e^{j\theta} s_i$.

As the scheme needs to be transparent to the primary receiver, θ needs to be small and the rule of thumb is that the induced offset on the signal constellation should be much smaller than that of the noise standard deviation. For small θ, the scheme induces an SNR degradation at s_i that is proportional to $|s_i|^2$, i.e., the degradation is proportional to the SNR at the constellation point. Assuming that the constellation points have equal prior probabilities, the average SNR degradation of this scheme is given in the following lemma.

Lemma 1. *Let θ be small such that $\theta^2|s_i|^2 \ll N_0$, where $s_i \in \mathcal{S}$ and N_0 is the noise spectral density. With constant angular offset the SNR at the primary receiver is given by*

$$\rho' = \rho(1 - \rho\theta^2) \tag{4}$$

where $\rho = \frac{1}{M}\sum_0^{M-1} \frac{|s_i|^2}{N_0}$ is the SNR in the absence of tag.

Proof. For small θ, the offset at s_i is simply $\theta|s_i|$. The SNR can be computed as

$$\begin{aligned}\rho' &= \frac{1}{M}\sum_0^{M-1} \frac{|s_i|^2}{|s_i|^2\theta^2 + N_0} \\ &= \frac{1}{M}\sum_0^{M-1} \frac{|s_i|^2}{N_0}\left(1 - \frac{\theta^2|s_i|^2}{|s_i|^2\theta^2 + N_0}\right) \\ &\approx \rho(1 - \rho\theta^2) \end{aligned} \tag{5}$$

The last step follows form the condition $\theta^2|s_i|^2 \ll N_0$. □

While N_0 above is the noise power density at the primary receiver, we assume for simplicity that the noise power at the SU is identical to N_0. Otherwise, the derivation still holds except new notations need to be defined.

The second scheme, which we refer to as uniform energy degradation, rotates each constellation point by a constant offset $\sqrt{E_t}$. The constant offset results in a constant SNR degradation for all constellation point, hence the overall average SNR degradation equals to that of any given constellation point which can be approximated to be E_t/N_0 for small E_t. The offset constellation sets are given by, for small E_t,

$$\mathcal{S}_0 = \left\{ s_{0,i} : s_{0,i} = s_i e^{-j\theta_i}, \theta_i = \sin^{-1}\sqrt{E_t/|s_i|^2}, s_i \in \mathcal{S} \right\} \tag{6}$$

$$\mathcal{S}_1 = \left\{ s_{1,i} : s_{1,i} = s_i e^{j\theta_i}, \theta_i = \sin^{-1}\sqrt{E_t/|s_i|^2}, s_i \in \mathcal{S} \right\} \tag{7}$$

A different perspective on the two generalizations is that both schemes introduce a phase rotation of the constellation points, with the first scheme using a fixed phase offset while the latter using a phase offset depending on the constellation point. It is not known *a priori* which one leads to a better tag detection performance. Next, we compare the performance of the two schemes under the constraint that the average SNR degradation at the primary receiver is the same, *i.e.*, $\rho^2\theta^2 = E_t/N_0$.

We assume for simplicity a narrowband Rayleigh fading channel. Let h be the channel coefficient and z be the additive complex Gaussian noise distributed as $\mathcal{CN}(0, \sigma^2)$. Then the received signal at the SU is given by,

$$y = hx + z \tag{8}$$

where $x = g(s_i, t)$ with $g(\cdot)$ specified by the chosen scheme. We further assume that the receiver knows the channel coefficient h perfectly, and that the symbols s_i and data bits t follow independent and identically distributed (*i.i.d*) with equal prior among their respective constellation sets. Detecting the tag bit is then equivalent to deciding which constellation set $\mathcal{S}_0$ or $\mathcal{S}_1$ (or $\mathcal{S}_\theta$ or $\mathcal{S}_{-\theta}$) that x belongs to. Let $\hat{t}$ be the estimate at the SU of the tag bit t. The tag bit error probability is,

$$P_e = P(t \neq \hat{t}) = \frac{1}{2}\left[P(\hat{t} = 1|t = 0) + P(\hat{t} = 0|t = 1)\right] \tag{9}$$

Minimizing P_e entails a Bayesian detector [10] which reduces to the following maximum likelihood detector.

$$\hat{t} = \begin{cases} 0 & \text{if } \sum_{i=0}^{M-1} e^{-\frac{1}{\sigma^2}|y - h s_{0,i}|^2} > \sum_{i=0}^{M-1} e^{-\frac{1}{\sigma^2}|y - h s_{1,i}|^2} \\ 1 & \text{otherwise} \end{cases}$$

While error probability analysis is generally intractable for the above detector, closed form expression can be obtained under the high SNR regime, i.e., $\frac{\mathcal{E}(xx^*)}{\sigma^2} >> 1$, where $\mathcal{E}$ is the expectation operator. This allows us to approximate the decision rule as follows.

$$\hat{t} = \begin{cases} 0 & \text{if } \min_i\{|y - h\, s_{0,i}|^2\} < \min_i\{|y - h\, s_{1,i}|^2\} \\ 1 & \text{otherwise} \end{cases}$$

Suppose the PU transmits $s_{t,k}$. Under high SNR conditions at the SU the symbol detection error probability is negligible. Hence, the tag detection error at the SU will be dominated by the event of incorrect tag detection but correct symbol detection. Therefore,

$$P(\hat{t} \neq t) \approx P(|y - h\, s_{1-t,k}| < |y - h\, s_{t,k}| \,\big|\, x = s_{t,k}). \tag{10}$$

As such, the above high SNR approximation results in the detection that is reminiscent of that of an antipodal signal. Therefore, the error probability can be expressed using that of BPSK signaling over a Rayleigh fading channel [11], *i.e.*, $P(|y - h\, s_{1-t,k}| < |y - h\, s_{t,k}| \mid x = s_{t,k}) \approx \frac{1}{2}\left(1 - \sqrt{\frac{\rho_t}{1+\rho_t}}\right)$, where $\rho_t = E_t/\sigma_z^2$, the signal to noise power ratio of the tag bit. Therefore,

$$P_e \approx \frac{1}{2}\left(1 - \sqrt{\frac{\rho_t}{1 + \rho_t}}\right) \tag{11}$$

3.1. Scheme Optimality

We now establish that the second scheme, i.e., the one that shifts the constellation by a constant offset $\sqrt{E_t}$ is optimal under high SNR condition for a Rayleigh fading channel. This is given in the following theorem.

Theorem 1. *Let $\mathcal{W}_0 = \{w_{0,0}, w_{0,1}, \ldots, w_{0,M-1}\}$ be a set of complex numbers. Similarly, define $\mathcal{W}_1 = \{w_{1,0}, w_{1,1}, \ldots, w_{1,M-1}\}$ with $w_{1,m} \neq w_{0,m}$ for $m = 0, \cdots, M-1$. Define the sets $\mathcal{S}_0'$ and $\mathcal{S}_1'$ as follows.*

$$\mathcal{S}_0' = \left\{ s_{0,i}' : s_{0,i}' = s_i - w_{0,i},\ s_i \in \mathcal{S} \right\} \tag{12}$$

$$\mathcal{S}_1' = \left\{ s_{1,i}' : s_{1,i}' = s_i + w_{1,i},\ s_i \in \mathcal{S} \right\} \tag{13}$$

such that $\frac{1}{M}\sum_{i=0}^{M-1} |s_{0,i} - s_{1,i}|^2 = 2E_t$. Let $g'(t, s_i) = s_{t,i}'$ and the transmitter sends $x = g'(t, s_i)$ such that t and s_i

follow i.i.d. uniform distribution over their respective sets. Let P_e' be the approximate tag bit error probability under the assumptions $\frac{\mathcal{E}(xx^*)}{\sigma_z^2} >> 1$ and $\mathcal{E}(xx^*) >> E_t$. Then, under Rayleigh fading channel conditions,

$$P_e \leq P_e' \tag{14}$$

Proof. The probability of error P_e' for the channel model in (8) can be approximated as.

$$P_e' \approx \frac{1}{M}\sum_{i=0}^{M-1}\frac{1}{2}\left(1-\sqrt{\frac{|s_{0,i}'-s_{1,i}|^2/2\sigma_z^2}{1+|s_{0,i}'-s_{1,i}|^2/2\sigma_z^2}}\right) \tag{15}$$

Using the concavity of the expression $\sqrt{\frac{x}{1+x}}$, we can show that the RHS of (15) is greater than or equal to the RHS of (11). Hence, $P_e \leq P_e'$. □

4. TRADE-OFF ANALYSIS

The requirement that the primary receiver not be affected dictates that ρ_t has to be very small, which will lead to a high value of P_e. A simple way to reduce the raw tag bit detection error probability P_e is to repeat the same tag bit multiple times (i.e., using a repetition code). An additional benefit is that it may utilize the time diversity in a fast fading channel.

Consider sending the same tag bit t, K times using K primary symbols. For simplicity we assume that the channel realizations are independent for the K symbols. Let, $k \in \{0, 1, \ldots, K-1\}$ and the received sequence is given by

$$y_k = h_k x_k + z_k \tag{16}$$

where h_k is distributed as $\mathcal{CN}(0,1)$ and z_k is the additive white noise distributed as $\mathcal{CN}(0,\sigma_z^2)$. The transmitted symbols $x_k = g(s_k, t)$ are the result of the mapping with identical t but independent s_k. The maximum likelihood decision rule that minimizes the probability of error is given as follows.

$$\hat{t} = \begin{cases} 0 & \text{if} \quad \sum_{k=0}^{K-1}\log\left(\sum_{i=0}^{M-1} e^{-\frac{1}{\sigma^2}|y_k - h_k s_{0,i}|^2}\right) > \\ & \quad \sum_{k=0}^{K-1}\log\left(\sum_{i=0}^{M-1} e^{-\frac{1}{\sigma^2}|y_k - h_k s_{1,i}|^2}\right) \\ 1 & \text{if} \quad \text{otherwise} \end{cases}$$

For $\frac{\mathcal{E}(xx^*)}{\sigma^2} >> 1$ and $\mathcal{E}(xx^*) >> E_t$, the decision rule can be approximated as follows.

$$\hat{t} = \begin{cases} 0 & \text{if} \quad \sum_{k=0}^{K-1}\min_{s_{0,i}}|y_k - h_k s_{0,i}|^2 < \\ & \quad \sum_{k=0}^{K-1}\min_{s_{1,i}}|y_k - h_k s_{1,i}|^2 \\ 1 & \text{if} \quad \text{otherwise} \end{cases}$$

Similarly to the case with no repetition we can approximate the tag bit error probability as follows.

$$P_{e,K} \approx \left(\frac{1-\mu}{2}\right)^K \sum_{k=0}^{K-1}\binom{K-1+k}{k}\left(\frac{1+\mu}{2}\right)^k \tag{17}$$

where, $\mu = \sqrt{\frac{\rho_t}{1+\rho_t}}$. $P_{e,K}$ has the same form as that of BPSK signaling with repetition coding over Rayleigh fading channel [11]. From Fig. 3 we can see that the analytical approximations agree quite well with the Monte Carlo simulation results at an SNR of 25 dB and a 16 QAM signal constellation. Given that for typical authentication purpose, tag length in the order of 100 bit is considered sufficiently secure. Thus the error probability in the order of $< 10^{-5}$ can essentially guarantee error free tag bit detection.

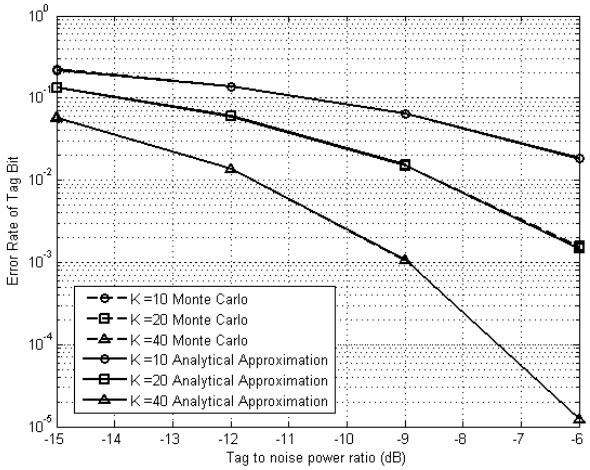


Fig. 3: Average error probability of the tag bit as function of tag signal to noise power ratio for a 16 QAM system with $\rho = 25$ dB.

We now discuss briefly the effect of the constellation shift on the primary receiver's performance. The offset $\sqrt{E_t}$ introduces an SNR degradation at the primary receiver. Let ρ be the nominal SNR at the secondary receiver when the signal is tag free and ρ' be the SNR when the tag is present in the signal and ρ_t be the tag to noise power ratio *at the primary receiver*. For small ρ_t, the SNR degradation can be approximated as follows (whose derivation is similar to that of Lemma 1).

$$\rho' \approx \rho - \rho_t = \rho\left(1 - \frac{\rho_t}{\rho}\right) \tag{18}$$

As an example, suppose that the primary receiver is operating at a high SNR of, say 25 dB, and the tag to noise power ratio is -10 dB, then ρ' is within 99.9% of the nominal SNR ρ. Thus, by proper choice of E_t and K we can make sure that the tag bits are transmitted reliably with negligible SNR degradation at the legacy receivers.

5. CONCLUSION

In this paper we have provided a method to reliably transmit cryptographic signatures at the modulation level, without compromising the performance at the legacy receivers, for the purpose of countering PUEA attacks.

One can further improve the tag bit detection performance by replacing the repetition code with a strong error correcting code (ECC). ECCs perform poorly when the number of errors in the codeword are comparable to that of their error correcting capability [12]. A compromise is to use a simple code that permits maximum likelihood decoding with low complexity (such as the repetition code) as an inner code to bring down the raw tag bit error rate in the range of $10^{-2} - 10^{-3}$. We can then use an appropriate ECC as an outer code to guarantee essentially perfect tag recovery at the *secondary user*.

6. REFERENCES

[1] J. Mitola III and G.Q. Maguire Jr., "Cognitive radio: making software radios more personal," *IEEE Personal Commun. Mag.*, vol. 6, no. 4, pp. 13 –18, Aug 1999.

[2] H. Kim and K.G. Shin, "In-band spectrum sensing in cognitive radio networks: energy detection or feature detection?," in *Proc. of the 14th ACM int. conf. on Mobile computing and networking*, San Francisco, California, USA, Sep. 2008.

[3] L.P. Goh, Z. Lei, and F. Chin, "DVB Detector for Cognitive Radio," in *Proc. IEEE Int. Conf. on Commun.*, Glasgow, Scotland, Jun. 2007.

[4] Q. Yuan, P. Tao, W. Wang, and R. Qian, "Cyclostationarity-Based Spectrum Sensing for Wideband Cognitive Radio," in *Proc. WRI Int. Conf. on Commun. and Mobile Computing*, Kunming, Yunnan, China, Jan. 2009.

[5] R. Chen and J.M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in *Proc. 1st IEEE Workshop Netw. Technol. Software Define Radio Netw.*, Reston, VA, USA, Sep. 2006.

[6] P. Yu, J.S. Baras, and B.M. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 38–51, 2008.

[7] X. Tan, K. Borle, W. Du, and B. Chen, "Cryptographic link signatures for spectrum usage authentication in cognitive radio," in *Proc. of the fourth ACM conf. on Wireless network security*, Hamburg, Germany, Jun. 2011.

[8] I. Cox, M. Miller, J. Bloom, and C. Honsinger, *Digital Watermarking*, Morgan Kaufman, San Francisco, CA, 2001.

[9] L. Lamport, "Password authentication with insecure communication," *Commun. of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[10] S. Kay, *Fundamentals of Statistical Signal Processing II: Detection Theory*, Prentice Hall, Englewood Cliffs, NJ, 1998.

[11] D. Tse and P. Viswanath, *Fundamentals of Wireless Communications*, Cambridge University Press, Cambridge, UK, 2005.

[12] D. Forney, "*6.451 Principles of Digital Communication II, Spring 2005*," (Massachusetts Institute of Technology: MIT OpenCourseWare), http://ocw.mit.edu (Accessed Oct 10, 2012). License: Creative Commons BY-NC-SA.