On Secure Spectrum Sensing in Cognitive Radio Networks using Emitters Electromagnetic Signature

Afolabi, O. Richard, Kiseon Kim and Aftab Ahmad*
Department of Information and Communications, GIST
261, Oryong-dong, Buk-gu, Gwangju 500-712 Republic of Korea.
*Norfolk State University, Norfolk, VA, USA
E-mail: afolabicrystal@ieee.org

***Abstract*— As Cognitive Radio Network (CRN) emerges as an extremely promising next generation wireless technology that can ease the apparent spectrum scarcity and support novel wireless applications; they will become bigger targets for hackers. Moreover, they will also be exposed to diverse security threats especially at the physical layer (PHY) spectrum sensing module. Hence, security consideration is central in its development. Starting with overview of on-going research efforts in CR-based network security, this paper describes a PHY attacker model that exploits the adaptability and flexibility of CRN. In thwarting this attack, we propose a waveform pattern recognition scheme to identify emitters and detect camouflaging attackers by using the Electromagnetic Signature (EMS) of the transceiver. On the performance of the technique, our simulation results show that our approach is effective for spectrum monitoring, mitigating denial-of-service threats and facilitating spectral efficiency.**

I. Introduction

Future wireless communication system is expected to integrate existing disparate networks into a single heterogeneous structure with multitude of different proprietary wireless systems [1] coexisting in the usable radio spectrum via dynamic spectrum access techniques. Although, this radio spectrum band has been reported to be poorly allocated and underutilized [2], [3], however. Cognitive Radio (CR) is emerging as key enabling technology to facilitate the emergence of this high capacity future wireless communication networks. CR is a model where nodes sense and adapt their transmission and reception parameters to communicate efficiently without interfering with high priority users. They coexist with other users based on the real-time conditions of their environment. A unique function of cognitive radio is spectrum sensing which involves monitoring a given spectrum band, capturing the information and detecting the spectrum holes [4]. CR users may temporarily use the spectrum holes without causing harmful interference to the incumbents. However, CR must periodically sense the spectrum to detect the presence of incumbents and quit the band once detected.

Interestingly, the security aspect of CRN still remains an open research issue. Of specific interest is denial-of-service (DoS) threat induced by *incumbent emulation attacker* which was studied in [5], [7]. For example, a software-based CR-device user can deceptively skew and mimic incumbent to gain access to the spectral resource thereby causing unfair use of spectrum. It forces CRs within its proximity to vacate the channel falsely believing an incumbent is active. Hence, the core strength (flexibility) of CR becomes weapon that they use against one another in a cooperative network. This scenario shows the need for building *cognitive* intelligence security into CR Network to uniquely distinguish between emitters. This threat is lethal because as cognitive radio learns and adapts to its *manipulated* environment, it might learn to avoid this band. Such DoS threats would therefore incapacitate the network leading to security loopholes and loss of spectral efficiency.

Novel studies in [7] describe the weaknesses of existing sensing systems techniques and associated disruptive effect of incumbent emulation attacker. An analytical model to deal with this form of attacker was also presented in [6]. In [5], Chen and Park proposed a transmitter verification method called *LocDef (Localization-based defense)* which verifies the authenticity of a given signal by estimating its location and comparing it with the location of known incumbents. However, as noted by the author, the *LocDef* approach is insufficient in a full mobile network where the incumbents are mobile and have low power. The author further suggests future research direction to use *RF fingerprinting* for primary user emulation attacker detection.

RF fingerprinting (RFF) has been proposed as a means of enhancing security in wireless networks [8], [9], [10]. Hence, we investigate the extension of this idea to cognitive radio network. RF fingerprinting (RFF) [8] is the use of certain unique, short duration distinctive behavior of emitter present in the waveforms emitted by a transceiver when activated to identify an emitter. It has been attributed to the acquisition behavior of frequency synthesis systems, modulator subsystems, RF amplifiers as well as physical properties of the emitter. The idea is that by monitoring and analyzing a network's analog signal at the PHY, it is possible to identify emitters and address security related issues. The idea itself has been used to secure tactical and cellular networks against phone cloning. In such works, amplitude and profile(Amp-Phase) characteristics are often experimentally profiled as representative features for devices while device detection was determined using genetic algorithms[10], neural networks[11] or Hidden Markov Model. Although optimal solutions were claimed but these approaches require heavy computation and large samples for training data. Hence, we consider these techniques inappropriate for resource constraint and time-sensitive networks. The main contribution

978-1-4244-4581-3/09/$25.00 ©2009 IEEE

of this paper is a description of an interesting concept of a cross layer signal pattern recognition technique exploiting the unique property we call *Electromagnetic Signatures* (EMS) of each CR device to build a security sub-system (Section II). The objective of this technique is to provide a well-defined distinctive factor between emitters. In Section III, we present simulation and performance comparison results of our EMS-based attacker detection scheme with the Amplitude-Phase profile based wireless intrusion detection technique. Finally, we conclude the study in Section IV by providing some limitations and future directions.

II. EMS-Based Attacker Detection Scheme

In this section, we propose an incumbent emulating attacker detection scheme using the *Electromagnetic Signatures* (EMS) of a CR device. The scheme provides fine-grained information about the identity of each CR device. First, we highlight the general idea and then explain the operations in sequence.

A. Detection Overview

The EMS of an emitter can be compared to the human biometric feature. However, unlike human *biometrics* which is unique and deterministic, EMS is not completely deterministic because of aging factor of the device and degradation due to continual use [11]. These factors affect the signal pattern generated by the device components. However, changes in the EMS can be offset by periodically updating the EMS, hence, we can expect to detect a malicious device based on its signal pattern within certain level of deviations.

Generally, two processes are involved in the execution of the security scheme as shown in Fig. 1: *Enrollment* for data collection and *testing* to identify a user. The enrollment consists of recording sets (*clusters*) of feature vectors in a database on the Base Station (BS) as *prototypes* where the device MAC ID serves as the *Key*. Each key maps to a cluster and each cluster contains M signatures. During the testing, an input signal from a CR device already identified by the spectrum sensors as an incumbent is processed by extracting its EMS. The key is also decoded and maps to a cluster. The input EMS is then matched with the recorded EMS prototypes in the cluster for the device using our technique. The degree of deviation of the measured EMS and the recorded can then be exploited to detect a *camouflaging* attacker.

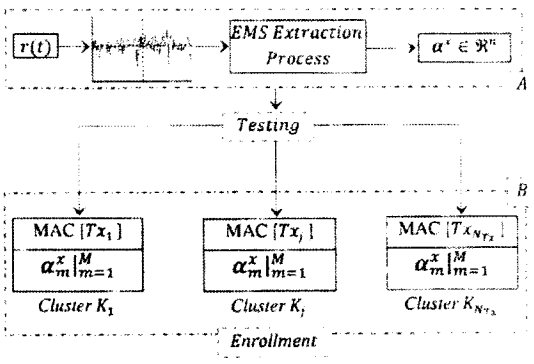

Fig. 1. Schematic diagram of EMS recognition phase. (A.) Real-time EMS capturing process. (B.) Enrolled prototypes in cluster in database on Base station.

B. Sensing & EMS Preprocessing Operations

The sensing operation involves intercepting, recording and gathering the signal of interest transmitted from the CR devices in its raw form. Similarly, the preprocessing operation involves capturing and extracting the transient portion that reflects the unique attributes of the CR device from the recorded raw signal and transforming it into an acceptable format for the EMS feature extraction phase. In [9], technique to capture and process sensed signal from the discriminator output of a receiver is explained; hence we shall not deal with it in this work. One crucial operation in CR-based network such as IEEE802.22WRAN is network entry and initialization which involves ranging, contention, registration, key exchange and synchronization. This sequence of requests/responses creates opportunities to perform *enrollment* and populate the cluster with EMS from the captured waveform.

C. EMS Extraction Operations

In CRN, incumbents should be protected against interference from CRs; hence, power should be prevented from spreading to adjacent channels. Using the overall EMS extraction process diagram shown in Fig.2, suppose $r_s(t)$ is the received, oversampled, preprocessed transient signal between times $t = [0, \tau]$ from a CR device where τ is the sample time. Then, to facilitate mathematical manipulations, the real-valued signal $r_s(t)$ is converted to complex analytic signal using *Hilbert transforms*. The transform produces the inphase, $r_I(k)|_{k=1}^N$ (real) and quadrature, $r_Q(k)|_{k=1}^N$ (imaginary) components of the signal. Using these two components, we obtain the instantaneous phase, $\varphi(k)|_{k=1}^N$, instantaneous amplitude, $A(k)|_{k=1}^N$, and instantaneous frequency, $f(k)|_{k=1}^N$ of the signal $r_s(t)$ where $N = \frac{\tau}{T_s}$ is the number of samples in each attributes and T_s is the uniform Nyquist sampling interval. To remove biases associated with differently scaled feature values and to preserve good numerical behavior due to time scale and time shift in waveform, we apply the normalized statistics on the inphase $r_I(k)|_{k=1}^N$ and quadrature $r_Q(k)|_{k=1}^N$ components as well as the attributes $\varphi(k)|_{k=1}^N$, $A(k)|_{k=1}^N$ and $f(k)|_{k=1}^N$. For instance, the normalized instantaneous amplitude is defined as shown in equation (1) below:

$$A_{N^*}(k)|_{k=1}^N = \frac{A(k)|_{k=1}^N}{max\{A(k)|_{k=1}^N\}}. \quad (1)$$

The result is sets of vectors of normalized attributes of the signal $r_s(t)$. We are then ready to extract the EMS feature vector which is a synthesis of feature representative of the signal $r_s(t)$. The EMS for each received signal emitted by a CR device Tx_j is an n-dimensional vector $\alpha_m^j|_{m=1}^M \in \Re^{n=6}$ where n is the dimension of each EMS feature vector α^j, and $m = 1...M$ is the population of EMS prototypes in a

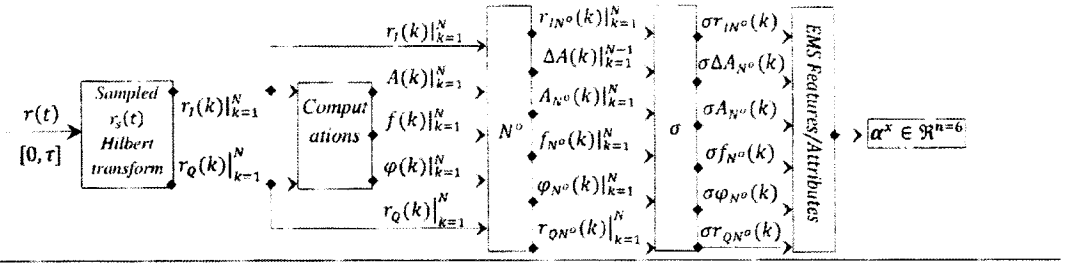

Fig. 2. Overall EMS extraction processes. N^o is the normalization process while σ is the standard deviation of the EMS vector components.

cluster K_j. Note that each cluster K_j contains M EMS vectors emitted from CR device Tx_j for $j = 1...N_{Tx}$ where N_{Tx} is the population of CR devices in the cell range of the base station. Components of the EMS vector is defined as shown in Fig. 2 using RFF features specified by Hall [11] but modified.

In Fig. 2, the σ-box produces the scalar standard deviation of the corresponding normalized components defining the feature vector $\boldsymbol{\alpha}^x \in \Re^{n=6}$ while ΔA is the change in instantaneous amplitude. Unlike work in [8] where amplitude and phase features are profiled and used with neural network for device recognition; a general definition for the standard deviation of attributes used in this work and listed in Fig. 2 is provided below in eqn. (2). We use deviations as feature parameter because it provides a measure of proximity between newly received signal and stored prototypes. We note that order of the vector components is immaterial provided it is consistent with order of each stored prototype in the cluster.

$$\sigma_{F_{iN^o}}|_{i=1}^{n=6} = \sqrt{\frac{1}{N}\sum_{k=1}^{N}|F_{iN^o}(k) - \mu_{F_{iN^o}}|^2}, \tag{2}$$

where $F_{iN^o}(k)$ is the normalized feature and $\mu_{F_{iN^o}}$ is its mean which is given as:

$$\mu_{F_{iN^o}} = \frac{1}{N}\sum_{k=1}^{N} F_{iN^o}(k). \tag{3}$$

All extracted EMS vector $\boldsymbol{\alpha}_m^x|_{m=1}^M$ from a CR device Tx_j are stored in cluster K_j in a database on the BS during the *enrollment* stage. To determine if a newly received signal $r(t)$ is emitted by an incumbent emulating attacker. EMS recognition needs to be performed. This is the focus of the next section.

D. EMS Detection Statistics: $\delta_M(\boldsymbol{\alpha}^o)$

In a cluster K_j where there exists M EMS vector i.e. $\boldsymbol{\alpha}_m^x|_{m=1}^M$, the covariance matrix $\boldsymbol{\Sigma}_{K_j}$ between them and centroid $\boldsymbol{\mu}_{K_j}$ can be defined as given in equations (4) and (5) respectively.

$$\boldsymbol{\Sigma}_{K_j} = \exp[(\boldsymbol{\alpha}^x - \boldsymbol{\mu}_{K_j})(\boldsymbol{\alpha}^x - \boldsymbol{\mu}_{K_j})^T]. \tag{4}$$

$$\boldsymbol{\mu}_{K_j} = \frac{1}{M}\sum_{m=1}^{M} \boldsymbol{\alpha}_m^x. \tag{5}$$

For a CR device with extracted EMS vector $\boldsymbol{\alpha}^o$, the Mahalanobis distance between $\boldsymbol{\mu}_{K_j}$ and new input vector $\boldsymbol{\alpha}^o$ is calculated. The Mahalanobis distance $\delta_M(\boldsymbol{\alpha}^o)$ is given as eqn. (6):

$$\delta_M(\boldsymbol{\alpha}^o) = [(\boldsymbol{\alpha}^o - \boldsymbol{\mu}_{K_j})^T \boldsymbol{\Sigma}_{K_j}^{-1}(\boldsymbol{\alpha}^o - \boldsymbol{\mu}_{K_j})]^{\frac{1}{2}}. \tag{6}$$

E. Attacker Detection & the Choice of threshold

The question of the attacker detection using the EMS detection statistics is: *how close should the measurement and centroid be before we declare a pattern recognized?* This requires certain *threshold* λ to be defined. It is immediately obvious that the choice of λ determines the performance of the recognizer. To ensure fairness however, a moderately scaled threshold would have to be chosen.

We define an expression for λ as a function of the prototype with the maximum deviation from the centroid, $max(\delta_M(\cdot))$ and Chebyshev's inequality controlled by certain constant C which provides the needed constraints that allow the recognizer to vary the ratio of acceptance or rejection of patterns. Using the modified Chebyshev inequality for multivariate normal distribution as explained by Monhor [12], a bound can be expected on the deviation that the random EMS feature vector prototypes fall into an hyper-ellipsoidally shaped cloud with center at the centroid $\boldsymbol{\mu}_{K_j}$ (or mean vector). The bound is expressed in terms of variance, similar to the classical one-dimensional inequality. The distance metric (i.e. deviation) of the input EMS from the centroid is expected to be within certain deviation from the EMS prototype with the maximum distance metric. The smaller the deviation, the more likely the input EMS belongs to the cluster K_j and an associated CR device Tx_j. The recognition equation is given as equation (7).

$$\boldsymbol{\alpha}^o \in K_j : \delta_M(\boldsymbol{\alpha}^o) \leq \lambda = C \max_x \delta_M(\boldsymbol{\alpha}_m^x \in K_j). \tag{7}$$

where the x-th element is the prototype with the longest distance from the centroid of the cluster. Hence, as the cluster grows or shrinks as a result of variation of the stored EMS, the threshold would still accommodate the differences. Continuously updating the values of the centroid, covariances and threshold will ensure that the cluster is a fair reflection of the CR devices.

III. Simulations & Evaluation Results

In this section, we provide results of simulations to evaluate the performance of our algorithm. The first part describes the simulation scenarios while subsequent parts present performance results.

A. Simulation Scenarios

The goal of the simulation is to demonstrate the performance of the proposed ems-based detection scheme. The key objective is to detect if a malicious CR device had mimicked and transmitted an incumbent-identical waveform. This requires modeling of emissions from both CR devices and incumbents. The simulation was implemented using the statistic and signal processing toolboxes in MATLAB 7.4. We expect a model waveform to gradually transmit power-up and power-down like a ramp waveform as shown in Fig. 3. Hence, our model equation for a received, oversampled, preprocessed transient signal $r_s(t)$ *already sensed as incumbent* by the spectrum sensor is shown in eqn. (8).

$$r_s(t) = A(t)sawtooth(2K\pi t)\sin(\tfrac{2\pi t}{F_c} + \phi(t)) + n(t). \quad (8)$$

We perform two classes of simulations. For both classes, we model three (3) CR devices (Tx_1, Tx_2, Tx_3). Using the model equation to generate several preprocessed transients, maximum of 10 EMS features prototypes are extracted from the preprocessed transients of each of the 3 CR devices and stored in a cluster; one cluster for each device. Based on the number of EMS prototypes in the cluster, the centroids, covariances and thresholds are calculated. Another 100 waveforms are also generated from these CR-device models and processed as input EMS feature vector for testing and evaluation purposes. Table I highlights parameter values of the scenario. For the first class, the CR device model are presumed to have modified their waveforms to mimic incumbents. Our goal is to pass the 100 modified signals from each of the 3 CR devices through our algorithm at varying values of threshold to determine the performance ratio of acceptance and rejection of the EMS features. If the signals are recognized based on the EMS features then the emitters are attacker since we already presumed the signal to emanate from incumbents. For the second class, valid incumbent signal from non-CR device having no stored EMS profile on cluster is considered. The goal of this scenario is to verify the performance of the EMS-based detection approach when signals from non-CR devices are passed to it. Here, we expect the algorithm to recognize that the signature do not match the EMS in the cluster. In the following section, we present performance result of detection.

TABLE I
SIMULATION PARAMETERS

Description	CR Device Tx_1	CR Device Tx_2	CR Device Tx_3
Peak Amplitude: A(t)	3.5	2.0	5.0
Ramp (K)	50	25	50
Carrier Frequency (F_c)	150MHz		
Uniformly random phase: $\phi(t)$	$[0, \pi]$		
Non – sinusoidal wave: sawtooth (·)			
Sinusoidal Carrier: sin (·)	*AWGN: n(t)*		
SNR	10dB	12dB	13dB
#(Input EMS Feature vector)	100	100	100
#(Stored prototypes per cluster)	10	9	10

B. Simulation Results

Table II shows the detection matching matrix. Supposing incumbent are accurately detected, then it is natural to fix ***Yes*** for *incumbent signal found* as shown in the table. The description of performance results are given below.

1) Comparing Detection Performances of Two Schemes: Observing Fig. 4, we point out two crucial points: First, based on extensive simulations, we observe similarities in the CDR (Sensitivity) of the two schemes with respect to threshold. Hence, we plot the ems-based and Amp-Phase curves using the average correct detection rates. Secondly, as observed in the figure, the ems-based scheme shows better average detection performance than the amplitude-phase profile. However, we note that when the threshold is very low or too large, the two techniques exhibit similar behavior.

2) Overall Performance Measures - ROC & AUC: A relative operating curve (ROC) curve shows the CDR and False Alarm Rate at different threshold values, hence, it can be used to compare the performances of different detection schemes

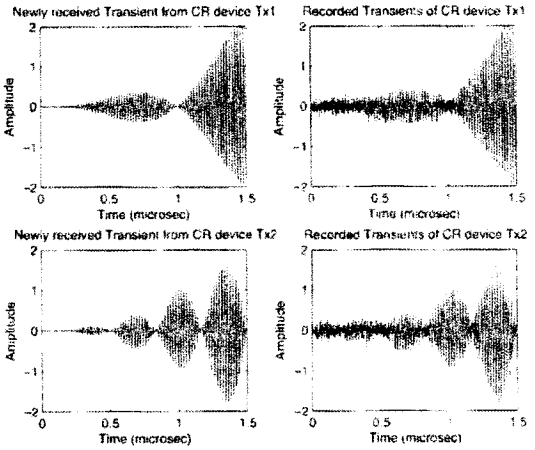

Fig. 3. Pattern output of preprocessed two newly received waveforms (above) and corresponding stored prototype (below) from certain CR devices Tx_1 and Tx_2. While the signals look similar, certain discrepancies are noticed

TABLE II
DETECTION MATCHING MATRIX

		PU Signal Found = Yes	
		EMS Recognized	***EMS Un-Recognized***
PU Signal Found = Yes	***EMS Present in Cluster***	*"Attacker" Correct Detection (Sensitivity)*	*"Attacker" False Alarm (1-Specificity)*
	EMS Absent in Cluster	*"Non-Attacker" Miss Detection (1-Sensitivity)*	*"Non-Attacker" Correct Rejection (Specificity)*

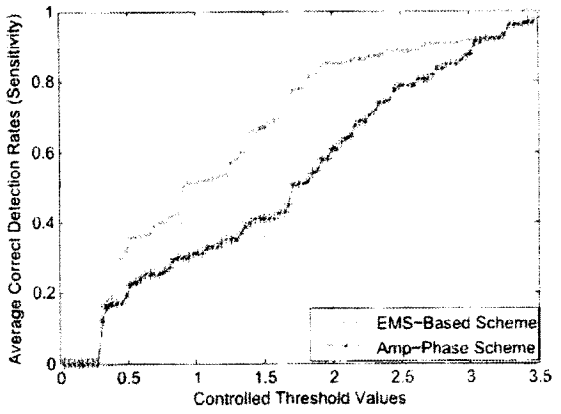

Fig. 4. Average performance of EMS-based and Amplitude-Phase Schemes

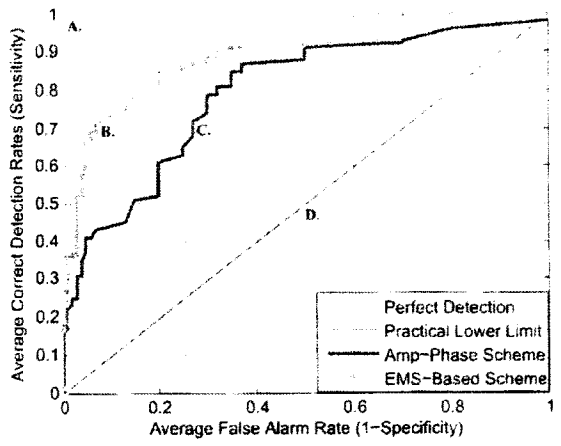

Fig. 5. Four ROC curves with difference AUC values. (A.) Perfect detection, AUC= 1. (B.) ems-based scheme, AUC = 0.8904. (C.) Amplitude-Phase Profile Scheme, AUC = 0.8099. (D.) Practical Lower limit, AUC = 0.5.

independently of the threshold by using the *Area Under Curve* (AUC). We compute the AUC by taking the summation of the areas of the trapezoids formed by the connecting the points on the ROC curve. Fig. 5 shows the overall performance of the proposed ems-based scheme (curve B) and the amplitude-phase profile scheme (curve C). The diagonal, (Curve D) is the practical lower limit, ($AUC = 0.5$) while the curve A is the perfect detection, ($AUC = 1.0$). The closer the AUC to 1.0 the better the overall performance, however, it is desirable to have $AUC > 0.5$. The AUC of the ems-based scheme is $0.8904\ (\pm)0.0464$ at 95% *confidence interval* while the AUC of the amplitude-phase profile based scheme is $0.8099\ (\pm)0.0462$ at 95% *confidence interval*. The difference shows that the overall performance of the ems-based scheme is 9.05% better than the amplitude-phase profile based scheme. Moveover, since the lower bound (0.8441) of the ems-based scheme is greater than 0.5, we conclude that the performance is statistically, significantly acceptable.

IV. CONCLUSIVE REMARKS & FUTURE WORKS

In this work, we propose a scheme to secure the spectrum sensing function in cognitive radio network using the electromagnetic signature of emitters. The EMS-based scheme is a cross-layer security module capably providing more specific and reliable distinction among CR devices. The technique is designed to learn the foul-proof initial unique characteristic of CR devices and compares it with subsequent transmissions for validation and authentication.

One significant benefit of our approach is its mitigation against DoS threats, thereby potentially providing better spectral efficiency. Although our approach promises good performances but not without certain sacrifices: There is a likely increase in storage requirement and total sensing time due to possible overhead of extra signal processing operations. As future works, it is highly crucial to collect *actual signal data* transmitted by software defined radio devices and investigate that the radio characteristics can or cannot be traced. This would be a huge advance for security in cognitive radio. Lastly, we note that other security issues in spectrum sensing are not considered in this work but through incremental advancements, secure cognitive radio network is feasible.

ACKNOWLEDGMENT

This work was partially supported by the Center for Distributed Sensor Network at GIST.

REFERENCES

[1] Jung P *et al* "Cognitive radio prototyping" in *Cognitive Radio Oriented Wireless Networks and Communications*, CrownCom May 2008.

[2] Haykin S., "Cognitive radio: brain-empowered wireless communications," in *IEEE Jnl., Selected Areas in Comm.*, Vol 23, Issue 2,pp.201-220,Feb 2005.

[3] Gandetto, M.,Regazzoni, C., "Spectrum sensing: A distributed approach for cognitive terminals," in *IEEE Jnl. Selected Areas in Comm.*, Vol.25, Issue 3, pp.546-557, April 2007

[4] D Cabric, S. M. Mishra and R.W Brodersen, "Implementation issues in spectrum sensing for cognitive radio" , in *Conf. Record, Thirty-Eighth Asilomar Conf. on Signals, Systems and Computers*, vol.1, pp.772-776, Nov 2004.

[5] Ruihang Chen, Jung-Min Park, Reed, J.H., "Toward secure distributed spectrum sensing in cognitive radio networks," in *IEEE Communications Magazine*, Vol.46, Issue 4, pp. 50-55, April 2008

[6] Anand, S.,Jin, Z., Subbalakshmi, K.P., "An analytical model for primary user emulation attacks in cognitive radio networks," in *3rd IEEE Symposium on DySPAN*, Oct. 2008.

[7] Ruihang Chen; Jung-Min Park; Reed, J.H., "Defense against primary user emulation attacks in cognitive radio networks," in *IEEE Jnl., Selected Areas in Comm.*, Vol.26, Issue 1, pp. 25-37, Jan. 2008.

[8] Ureten, O.; Serinken, N., "Wireless security through RF fingerprinting," *Can.Jnl of Elect. & Computer Engnr.*, Vol. 32, Issue 1, pp. 27-33, 2007

[9] O. Ureten and N. Serinken, "Bayesian detection of Wi-Fi transmitter RF fingerprints," Elect. Letters, vol. 41, pp. 373-374, 2005.

[10] J.Toonstra and W. Kinsner, "A Radio transmitter fingerprinting system ODO-1" in *proceeding CCECE*, pp.60-63, 1996.

[11] J. Hall, M. Barbeau, and E. Kranakis, "Enhancing Intrusion Detection in Wireless Networks Using Radio Frequency Fingerprinting (Extended Abstract)" in *Proc. 3rd International IASTED Conference on Communications, Internet, and Information Technology*, pp. 201-206

[12] Davaardorjin Monhor "A Chebyshev Inequality for Multivariate Normal distribution," in *Probability in the Engineering and Informational Sciences*, pp. 289300, 2007 Cambridge University Press.

[13] Richard Duda, P. Hart, D. Stock, "Pattern Classification," 2nd Edition, Wiley Interscience, ISBN 0-471-05669-3, 2001.