

# Specific Emitter Identification for Cognitive Radio with Application to IEEE 802.11


Ihsan Akbar

## Cite this paper

Downloaded from [Academia.edu](#) 

[Get the citation in MLA, APA, or Chicago styles](#)

## Related papers

[Download a PDF Pack](#) of the best related papers 



[A Parallel Computing Based Spectrum Sensing Approach for Signal Detection under Conditio...](#)

Kiruthikha Chandrasekaran

[A Practical Demonstration of Spectrum Sensing for WiMAX Based on Cyclostationary Features](#)

Raimondo Giuliani

[60 GHz Technology for Gbps-Wlan-Wpan, Su-Khiong \(SK\) Yong ,Pengfei Xia, Alberto Valdes-Garcia](#)

Alberto Albuquerque

# Specific Emitter Identification for Cognitive Radio with Application to IEEE 802.11

Kyouwoong Kim, Chad M. Spooner\*, Ihsan Akbar\*\*, and Jeffrey H. Reed

Virginia Polytechnic Institute and State University

Wireless @ Virginia Tech

\*NorthWest Research Associates, \*\*Tyco Electronics

{kyouwook, reedjh}@vt.edu, \*cmspooner@nwra.com, \*\*ihsan.akbar@tycoelectronics.com

**Abstract**—Cognitive radio (CR) is believed to be an enabling technology for increasing spectrum efficiency. A CR collects spectrum usage information from not only its own spectrum sensing module, but also from peer CRs. The heavy dependence on spectrum knowledge from other CRs requires identification of malicious CR devices that could generate spoofed information. In addition, it also needs to track the users associated with problematic CR devices which unintentionally violate spectrum usage etiquette. The specific emitter identification (SEI) concept is applied to identification of such non-cooperative CR devices. In this paper, second-order cyclic features of OFDM signals are proposed as a means of increasing CR network security and stability through SEI. For this exploratory work, IEEE 802.11a/g signals from different WLAN cards are measured and classified using hidden Markov Models (HMMs).

**Index Terms**— Cognitive Radio, Specific Emitter Identification, Cyclostationarity.

## I. INTRODUCTION

THE tremendous ongoing growth of wireless communication technology and new wireless services demands stronger security. In particular, the heavy dependence on knowledge regarding spectrum measurement that originates from peer cognitive radios (CRs) requires the identification of spoofing devices. Therefore, automatic identification of malicious or malfunctioning signal transmitters is a major concern in CR. To minimize the threat from spoofing radio devices, the specific emitter identification (SEI) concept is introduced to provide for CR devices' electromagnetic fingerprinting. This fingerprinting of CR devices allows not only tracking the spoofing radio devices but also enhancing physical-layer security. Although most radio systems have network-layer protocols to secure the exchanging of data, physical-layer security offers some advantages. The most vulnerable point of network-layer security is that it cannot differentiate cloned security related data such as user identification or authentication keys. However, the duplication of physical-level security measures is more challenging than that for network-level security. The forgery of a device-specific electromagnetic fingerprint by a network intruder is thought to be as difficult as duplication of a human fingerprint.

The SEI idea originated in military intelligence to allow the classification of an enemy's radar signal for threat evaluation. SEI utilizes emitter-specific non-intentional transmissions due to non-ideal electrical component characteristics of the

transmitter caused by degraded or low quality components. The interpulse information, such as pulse repetition interval and pulse width, is investigated in [1] for simple radar signal identification. For complex radar signals, the intrapulse [2] information, such as pulse rising and falling times, pulse rising and falling angles, angle of pulse, and pulse point, is utilized for SEI [2]. The SEI technology used for radar signal identification usually relies on high SNR and good channel propagation conditions. However, such inter and intra pulse information gets easily obscured at low and fluctuating SNR. In addition, modern communication often employs high data rate and irregular burst transmission and is deployed in indoor or urban areas where multipath fading is common. Therefore, the inherent features caused by the advanced transmitter are usually not available for emitter-specific feature extraction in low, varying SNR, and in a fading channel. For this reason, the recognition features need to have some tolerance to the varying noise and channel conditions. This leads us to consider statistical signal features instead of time-domain features as in the radar problem.

The structure of this paper is as follows. In Section II, a brief review of conventional technologies for SEI is provided. In Section III, the IEEE 802.11a/g WLAN signal characteristics are discussed, and in Section IV, the measurement setup of a WLAN signal is illustrated. In Section V, the second-order cyclic spectral analysis of IEEE 802.11a/g signal is presented. In Section VI, the device-specific second-order cyclic features are summarized. In Section VII, an SEI classifier for six 802.11a/g WLAN cards is presented. Finally, conclusions and future research directions are discussed in Section VIII.

## II. BRIEF REVIEW OF CONVENTIONAL SEI TECHNOLOGIES

Successful SEI depends on radio-specific feature extraction from the transmitted electromagnetic waveform. Any feature which represents distinctive characteristics of a specific radio can be a candidate for SEI. Some features utilized in the conventional techniques found in previous work are discussed in the following list.

### A. Time-Domain Features

SEI for radar signals depends heavily on the time domain feature caused by on and off transients of the transmitter [2, 3]. Some well-known time-domain features are pulse duration, pulse repetition rate, pulse rising and falling times, pulse rising and falling angles, angle of pulse, and pulse point [2, 3]. When

line-of-sight propagation and a high-power radar signal are provided, such features can be extracted by an SEI module mounted on an airplane for monitoring signals originating from the ground or ocean. The major difficulty of using time-domain features is that they may not be improved by averaging in low and varying SNR due to relatively small observation length.

### B. Frequency-Domain Features

The second common feature used for SEI is the power spectrum of the transmitted signal [3]. The power spectral density (PSD) provides signal power as well as the spectral shape for the signal of interest and may provide device-specific features. The spectral features include the symmetry of main and side-lobe shape, roll-off rate of passband, bandwidth, unintended tone in passband, passband shape, or out-of-band shape. Those frequency-domain features are also easily corrupted by noise and interference.

### C. Phase-Space Features

One of the common methods for nonlinear system analysis is the phase-space (PS) investigation. The PS analysis can provide the distinctive features of nonlinear power amplifier of a radio signal transmitter [4]. In PS analysis, the nonlinear system analysis begins by reconstructing the PS trajectory of a target system by using a time-delayed version of an observed scalar quantity, which is known as embedding [5] a scalar time series signal, and these delayed quantities serve as coordinates for the PS.

SEI for modern communication signals should combine all available features discussed above to increase classification performance. The SEI approach of using second-order cyclic features is one attempt at finding an additional useful feature set.

## III. IEEE 802.11A/G WLAN SIGNAL CHARACTERISTICS

To investigate the existence a device-specific electromagnetic fingerprint for orthogonal frequency division multiplexing (OFDM) signals, the IEEE 802.11a/g WLAN signal is chosen for our SEI exploration. The OFDM signal is commonplace and is easily measured. Figure 1 shows the 802.11a/g physical-layer frame which uses OFDM. As Figure 1 indicates, the physical frame starts with two training symbols. The training symbols are highly periodic and their characteristics can be easily identified using conventional signal processing methods. Therefore, the 16  $\mu$ s training portion of the frame is not considered for use in SEI in this work. The training symbols are automatically removed during signal capture process.

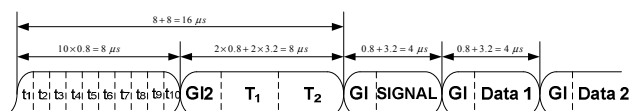


Fig. 1. IEEE 802.11a/g physical layer frame [6].

## IV. MEASUREMENT SETUP OF IEEE 802.11A/G SIGNAL

A signal interceptor was built to capture 802.11a/g signals in the ISM (Industrial, Scientific, and Medical) band, as shown in

Figure 2. The interceptor is located about 40 cm away from the laptop computer that is equipped with the WLAN card. This measurement setup minimizes the chance of signal corruption through multipath fading and ensures strong signal when a 54 Mbps OFDM signal is captured. For these measurements, we focus on the uplink signal, which is transmitted from WLAN card to the access point (AP). WLAN cards from six vendors—Motorola, LinkSys, DLink, Netgear, IBM, and Belkin—were tested. Ninety uplink signals are collected per WLAN card.

The RF front end of the interceptor is built using standard RF components such as LNA, BPF SAW filter, LPF, and signal mixer. The omni-directional antenna captures the RF signal, which is then converted to an 11 MHz intermediate frequency (IF) signal. The IF signal is sampled using a digital oscilloscope at a 50MHz sampling rate. The maximum number of samples per measurement is set to 30,000 and thus the digital oscilloscope can capture up to 0.6 ms of a WLAN signal burst. The digitized signal is transferred to the host computer for processing.

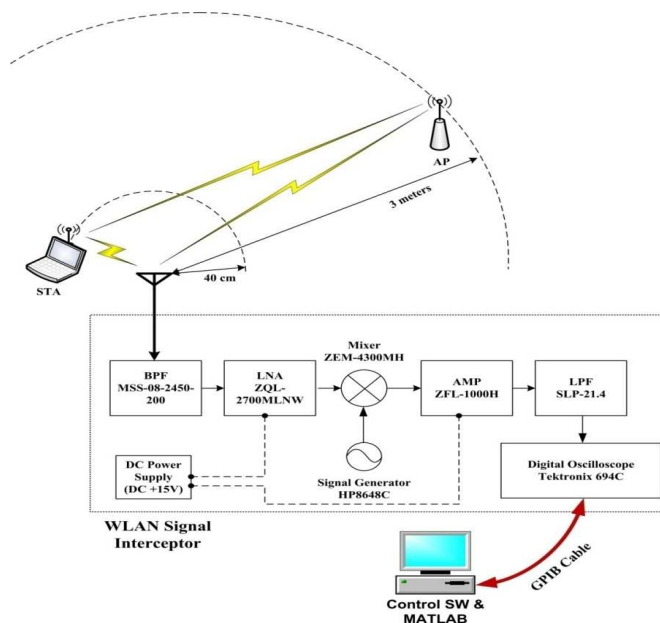


Fig. 2. Signal Measurement Setup.

The transferred signal is normalized to have unit power and converted to complex baseband using a Hilbert transformation and down conversion of positive spectral components to DC. The spectral correlation function (SCF) and spectral coherence (SC) for the complex baseband signals are then measured [8-10]. The device-specific fingerprint is generated by evaluation of cycle-frequency domain profile (CDP) [7]. The CDP is the maximum magnitude of the spectral correlation function (SCF) or spectral coherence (SC) over the spectral frequency variable. These functions are described in the following section.

## V. CDP ANALYSIS OF IEEE 802.11A/G SIGNALS

Most communication signals exhibit second-order cyclo-

stationarity, which implies the existence of correlation between distinct spectral components, which is also called spectral redundancy. The objective of all cyclic spectral analysis applications is to exploit the spectral redundancy of a signal to increase signal reliability or extract information. A favorable characteristic of exploiting spectral redundancy is that it can be extracted in strong time-varying noise and/or co-channel interference.

The SCF [8, 9] is a second-order measurement, and is a function of two frequency variables: the spectral frequency  $f$  and the cycle frequency  $\alpha$ . The former is the usual continuous frequency parameter encountered in conventional spectral analysis, whereas the latter is a discrete parameter that takes on values related to the signal's embedded periodicities, such as symbol rate, chip rate, and carrier frequency offset. The SCF can be accurately measured even when the signal is subjected to strong and varying noise or co-channel interference, and the cycle frequencies can be accurately measured for these impairments and also when the signal undergoes linear distortion such as that for multipath propagation. When the SCF is normalized to obtain a correlation coefficient we obtain the spectral coherence.

The dominant cyclic features of normal and conjugate CDPs for OFDM are related to the four pilots which are perfectly correlated. However, the cyclic features related to the QAM (QPSK, 16QAM, and 64QAM) data subcarriers are ideally zero except for harmonics of the symbol rate cycle frequency. The cycle frequencies of dominant OFDM cyclic features consist of two parts: normal (or lower region) and conjugate (or upper region). The dominant cycle frequencies for the lower and upper regions are given by

$$\begin{aligned}\alpha_{lower} &= \pm\{0.0, 4.25, 4.5, 8.75, 13.0, 13.25\} \text{ MHz} \\ \alpha_{upper} &= 2f_c + \alpha_{lower}\end{aligned}\quad (1)$$

where  $f_c$  is the carrier offset frequency of the complex baseband signal. Those cycle frequencies can be obtained from the general formula in [10] and are given by

$$\begin{aligned}\alpha_a &= \pm \left( 2k_1\Delta_F + \left\{ -\left(\frac{\beta_1}{G/2}\right), \left(1 - \frac{\beta_1}{G/2}\right) \right\} \times f_s \times \bar{\delta}(\beta_1) \right) \\ \alpha_b &= \pm \left( (k_1 + k_2)\Delta_F + \left\{ -\left(\frac{\beta_{1,2}}{G}\right), \left(1 - \frac{\beta_{1,2}}{G}\right) \right\} \times f_s \times \bar{\delta}(\beta_{1,2}) \right)\end{aligned}\quad (2)$$

where  $\beta_1 = \text{mod}(k_1, G/2)$ ,  $\beta_{1,2} = \text{mod}(k_1 + k_2, G)$ ,  $G=4$  is the ratio of data to guard interval (GI) duration as shown in Figure 1,  $k_1=7$  and  $k_2=21$  are the pilot subcarrier indexes,  $\Delta_F=312.5$  KHz is the subcarrier spacing,  $f_s=250$  KHz is the OFDM symbol rate, and  $\bar{\delta}(\cdot)$  is zero if the argument is zero, and one otherwise. The  $\alpha_a$  and  $\alpha_b$  indicate the cycle frequency from single pilot and two pilots.

The averaged normal and conjugate maximum SCF CDP is evaluated for the measurement data and plotted from Figure 3 to Figure 8.

The magnitudes of the dominant cyclic features (SCF and SC) related to OFDM pilots vary measurement by measurement due to channel, noise, and random effects. In addition, the nominal cycle frequencies for the dominant

OFDM cyclic features also vary, but the deviation from the nominal values is small. However, the small changes in the cycle frequency bring substantial variation of cyclic feature strength due to the discrete nature of cycle frequency. Therefore, the cycle frequencies for the dominant OFDM features are used as a guide for finding the exact cycle frequencies for each collected signal. This is achieved by finding the actual dominant cyclic features in a small cycle-frequency band around the nominal dominant cycle frequency. One of the causes for cycle frequency shift is the local oscillator drift at the transmitter side; another could be time variations in the interceptor.

## VI. DEVICE-SPECIFIC SECOND-ORDER CYCLIC FEATURES

To investigate the statistical characteristics of the dominant OFDM features, their mean and standard deviation are evaluated over 90 records per WLAN station. Those results are plotted in Figures 9 and 10. For the statistics of the normal SCF CDP, only positive cycle frequencies are shown due to symmetry. From these plots, the SCF's dominant features have distinctive device-specific attributes for SEI except for IBM and Netgear, which give rise to features that are quite similar, but there are still potentially exploitable differences in the sequence of dominant features taken as a whole.

As discussed earlier, the SCF can be measured accurately in low and varying SNR. Therefore, if we increase the observation length in terms of the number of measurement data, then we reduce the variation of dominant features and can achieve more reliable identification of WLAN devices.

## VII. SPECIFIC EMITTER CLASSIFICATION USING HMM

The WLAN card identification is performed using hidden Markov models (HMM) [11] that are widely used in speech and handwriting recognition. The purpose of using HMMs is to identify the OFDM cyclic features' potential for SEI. There may be better signal classifiers than HMMs, but they are a convenient tool for our use in this exploratory study.

### A. Feature Extraction for HMM Identifier

Feature extraction is the process of producing application specific distinctive features from input data. This stage must extract sufficiently distinct features to allow the HMM identifier to work properly. For HMM training and recognition purposes, the following features are extracted.

$$\begin{aligned}F_{1,i} &= \max_f \left| \hat{S}_x^{\alpha_i}(f) \right|, \quad \alpha_i \in A_1 \\ F_{2,j} &= \max_f \left| \hat{C}_x^{\alpha_j}(f) \right|, \quad \alpha_j \in A_2 \\ F_{3,k} &= \max_f \left| \hat{S}_x^{\alpha_k}(f) \right| \text{ and } F_{4,k} = \max_f \left| \hat{C}_x^{\alpha_k}(f) \right|, \quad \alpha_k \in A_3\end{aligned}\quad (3)$$

where the cycle frequency sets  $A_1$ ,  $A_2$ , and  $A_3$  are defined by

$$\begin{aligned}A_1 &= \alpha_{lower\_pos} \\ A_2 &= \alpha_{lower\_pos} \cup \{k \times f_{sym}\}_{k=1}^{15} \\ A_3 &= \alpha_{upper}\end{aligned}\quad (4)$$



in which  $\alpha_{lower\_pos}$  are the non-negative cycle frequencies in  $\alpha_{lower}$ . The estimated SCF is denoted by  $\hat{S}_x^\alpha(f)$  and the estimated coherence is  $\hat{C}_x^\alpha(f)$ . The conjugate versions use  $x^*$  as the subscript. An extracted feature vector for WLAN recognizer is generated by combining the features in the following manner.

$$FV = \{\{F_{1,i}\}, \{F_{2,j}\}, \{F_{3,k}\}, \{F_{4,k}\}\} \quad (5)$$

### B. Identification

To train the HMM, twelve randomly selected feature vectors are used per WLAN card to form a training set. The 12 feature vectors are averaged to reduce variance. Instead of just using one training vector for a particular WLAN card, four training vectors are used to obtain better identification. The Baum-Welch algorithm [12] is used to train the HMM.

In the identification stage, twelve feature vectors are selected randomly from the specific WLAN card measurement data and they are averaged before input to the identifier. The identification is performed by choosing the maximum log-likelihood value generated by the HMMs related to the specific WLAN card manufacturer for the given averaged feature vector input. The confusion matrix for HMM identification with 100 trials is shown in Table 1.

Table 1: Confusion matrix for identification of six WLAN cards

Input Card	Identified card					
	DLink	IBM	Link.	Moto.	Netg.	Belkin
DLink	96	0	0	0	4	0
IBM	0	89	0	0	11	0
LinkSys	0	0	100	0	0	0
Motorola	0	0	0	99	0	1
Netgear	0	14	1	0	85	0
Belkin	9	0	0	0	0	91

## VIII. CONCLUSIONS

The potential for specific emitter identification using second-order cyclic OFDM features is demonstrated. For this purpose, we developed an automated measurement environment for IEEE 802.11a/g OFDM WLAN signals from six different manufacturers. The SCF and SC CDPs are evaluated and their distinctive features are compared. Using the second-order cyclic features and HMMs, the six different WLAN cards can be identified successfully. Based on the results, the second-order statistics may have some potential value for performing SEI for 802.11a/g OFDM radios.

However, the IEEE 802.11a/g signal transmitter identification is performed in a benign condition with high SNR and line-of-sight propagation. It is now required to investigate the WLAN signals at low or time-varying SNR and in fading channel environments to verify the results shown in this paper. Finally, several cards of the same model from the same manufacturer must be included to determine the feasibility of distinguishing between radio signals that arise from identical hardware design.

## REFERENCES

- [1] L. E. Langley, "Specific emitter identification (SEI) and classical parameter fusion technology," Proceedings of WESCON, pp. 377-381, San Francisco, CA, 1993.
- [2] A. Kawalec and R. Owczarek, "Specific emitter identification using intrapulse data," EURAD. First European Radar Conference, pp. 249-252, 2004.
- [3] K. A. Remley, C. A. Grosvenor, R. T. Johnk, D. R. Novotny, P. D. Hale, M. D. McKinley, A. Karygiannis, and E. Antonakakis, "Electromagnetic signatures of WLAN cards and network security," Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology, pp. 484-488, Dec. 2005.
- [4] T. L. Carroll, "A nonlinear dynamics method for signal identification," Chaos: An Interdisciplinary Journal of Nonlinear Science, vol. 17, June, 2007.
- [5] T. Sauer, J. A. Yorke, and M. Casdagli, "Embedology," Journal of Statistical Physics, vol. 65, no. 3-4, pp. 579-616, November, 1991.
- [6] "Part 11: Wireless LAN Medium Access Control and Physical Layer Specifications: High-Speed Physical Layer in the 5GHz Band," IEEE Standard 802.11a, 1999.
- [7] K. Kim, and et al, "Cyclostationary Approaches to Signal Detection and Classification in Cognitive Radio," DySPAN 2007, pp. 212-215, 2007.
- [8] W. A. Gardner, "Introduction to Random Processes with Applications to Signals and Systems," New York: Macmillian, 1985.
- [9] W. A. Gardner, "Statistical Spectral Analysis: A Non-Probabilistic Theory", Prentice Hall, 1988.
- [10] K. Kim, "Second-Order Cyclic Features of OFDM Pilots and Its Application for Cognitive Radio", Dissertation chapter, Virginia Tech.
- [11] Y. Ephraim and N. Merhav, "Hidden Markov Processes," IEEE Transactions on Information Theory, vol. 48, no. 6, July 2002.
- [12] L. Rabiner and B. H. Juang, Fundamentals of Speech Recognition, Prentice Hall, Englewood Cliffs, New Jersey, 1993.

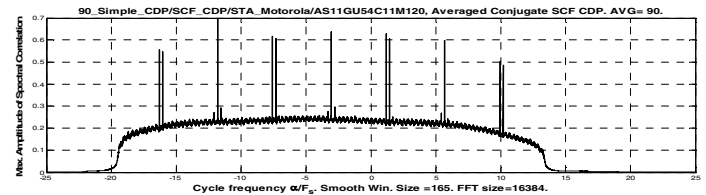
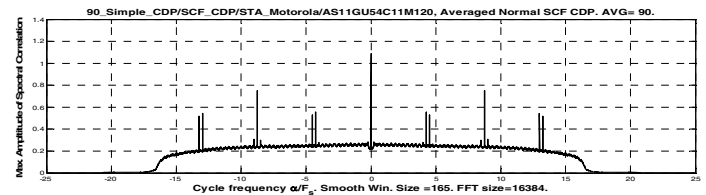


Fig. 3. Averaged Normal/Conjugate SCF CDP for Motorola STA

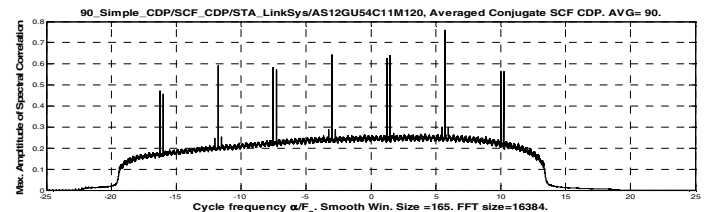
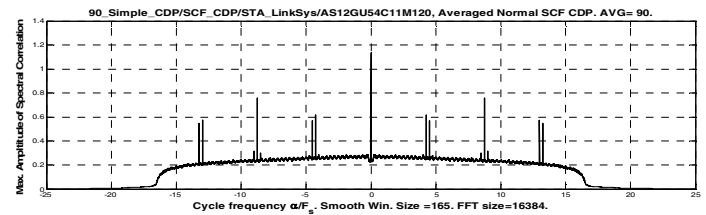


Fig. 4. Averaged Normal/Conjugate SCF CDP for LinkSys STA

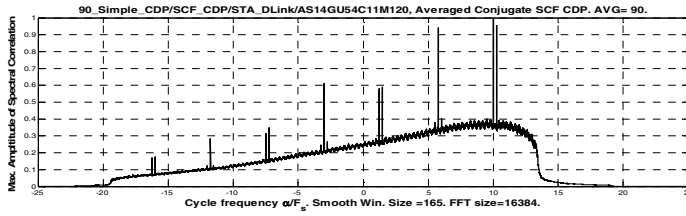
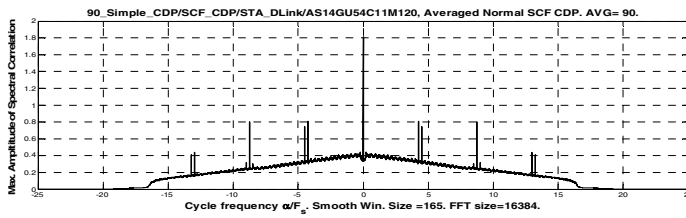


Fig. 5. Averaged Normal/Conjugate SCF CDP for DLink STA

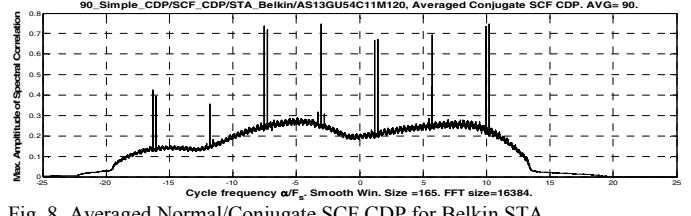
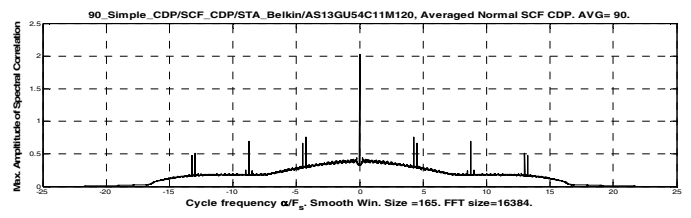


Fig. 8. Averaged Normal/Conjugate SCF CDP for Belkin STA

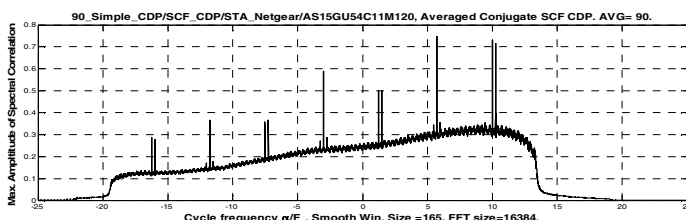
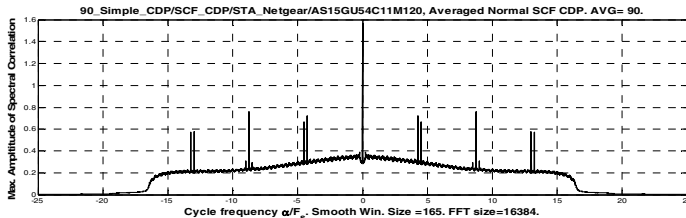


Fig. 6. Averaged Normal/Conjugate SCF CDP for STA Netgear

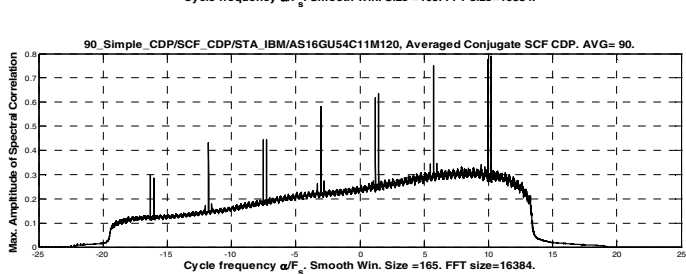
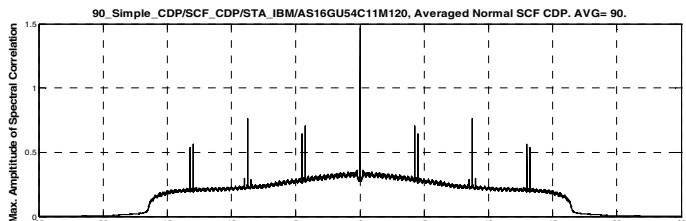


Fig. 7. Averaged Normal/Conjugate SCF CDP for IBM STA

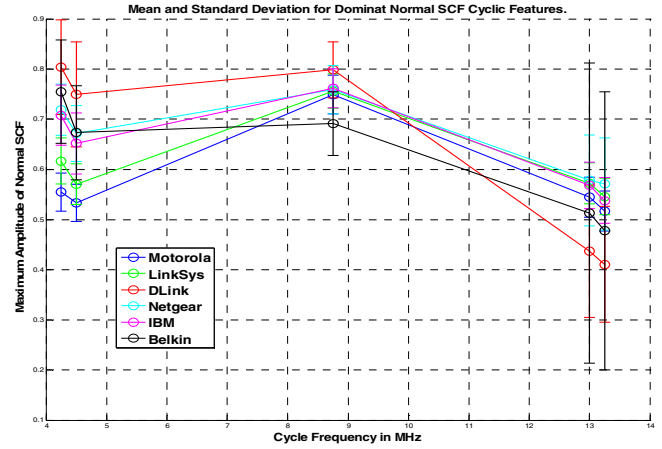


Fig. 9. Mean and standard deviation for dominant cyclic features for normal SCF

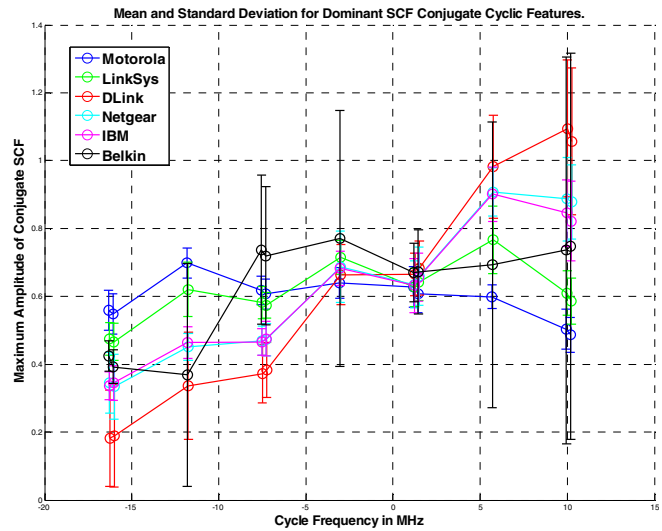


Fig. 10. Mean and standard deviation for dominant cyclic features for conjugate SCF