Cyclic Feature Concealing CP Selection for Physical Layer Security

Z. Esat Ankaralı[1], Murat Karabacak[1] and Hüseyin Arslan[1,2]
[1]Department of Electrical Engineering, University of South Florida
[2]Department of Electrical and Electronics Engineering, Istanbul Medipol University
Email: {zekeriyya,murat}@mail.usf.edu, arslan@usf.edu

***Abstract*—Cyclic prefix (CP) utilizing techniques such as orthogonal frequency division multiplexing (OFDM) and single-carrier frequency domain equalization (SC-FDE) offer significant advantages in equalizing the effect of time dispersive channels at the expense of a reasonable spectral redundancy. However, cyclic features introduced by CP to the signal can also be exploited for blind parameter estimation and synchronization which compromise the security and privacy of the signal against eavesdropping attacks. In this paper, we propose a novel CP selection technique that conceals the cyclic features of the signal while maintaining the advantages in equalization without reducing spectral efficiency. After presenting the proposed technique, its performance is discussed for OFDM and SC-FDE in terms of bit-error rate and complexity as well as cyclic feature suppression.**

***Index Terms*—Cyclostationarity, Low probability of interception (LPI), OFDM, Physical layer security, SC-FDE.**

I. Introduction

Cyclic prefix (CP) is a widely used signal extension in broadband wireless communication techniques such as orthogonal frequency division multiplexing (OFDM) and single-carrier frequency domain equalization (SC-FDE) [1]. It provides a substantial advantage in equalizing the effect of multipath channels. For example, when an OFDM time domain symbol is cyclically extended longer than the maximum excess delay of the multipath channel, linear convolution of the transmitted signal with the channel impulse response (CIR) is converted to a circular convolution at the receiver. Then, transmitted symbols interfered by the previous ones due to the multipath channel effect can be recovered using a simple single-tap frequency domain equalizer and equalization complexity decreases significantly. Moreover, CP can be utilized for signal parameter estimation [2] – [5], synchronization [6] – [7] and channel estimation [8] – [9] along with the trivial equalization.

Although, CP seems to be a very useful part of the signal rather than a redundant extension by having the aforementioned advantages, it degrades the secrecy of the communication and makes the signal vulnerable to eavesdropping attacks. Unauthorized users can exploit the cyclic features introduced by CP to extract the signal parameters, achieve synchronization and decode the data. Even when the secure communication techniques are used such as frequency hopping (FH) and direct sequence spread spectrum (DSSS), cyclic features are discernible if the CP is conventionally deployed and wireless signals are still under threat of malicious reception [11]. In order to prevent eavesdroppers from decoding the data, classical encryption techniques that provide bit-level security at the application layer have been deployed. However, in the case of signal decryption by a malicious user, further secrecy is essential especially for the critical communication scenarios such as the ones in military and health care. In order to meet this requirement, physical layer (PHY) security offers a promising solution by providing the secrecy in the transmission level. Since CP based cyclic features cause drawbacks in terms of signal covertness, their concealment is an important issue in PHY security. In the literature, various techniques are developed in this direction especially for OFDM systems. In [10], OFDM symbols are embedded into a notched ultra wide band (UWB) noise signal. The goal is to carry out a spectrally undetectable system for building a network among radars. However, sharp filters should be used at the transmitter and receiver for designing such a system, and bit error rate (BER) performance is degraded due to the added noise. UWB-OFDM is another technique for achieving secrecy as the signal is spread over a very large band and the transmitted power remains below the noise level. However, UWB suffers from in-band interference and has challenges in hardware design. OFDM signals are generated with a random frequency jitter in [11] to conceal OFDM signatures. Also, time jitter can be used in frequency hopping OFDM (FH-OFDM) signals to remove the spectral lines at symbol and hopping periods. In [12], CP and pilot tones are completely removed to suppress OFDM features, and inter-symbol interference (ISI) is removed using a decision feedback equalizer (DFE). However, the obvious disadvantage of such an approach is the increased complexity which eliminates the advantage of OFDM in handling multipath by using CP. Pseudo-random sequences are used instead of preambles in [13], in order to facilitate time and frequency synchronization. A random frequency offset is added to each preamble to further mask the spectral lines. Random data insertion between OFDM symbols is proposed in [14] to remove the periodicity of

978-1-4799-6770-4/14 $31.00 © 2014 IEEE
DOI 10.1109/MILCOM.2014.85

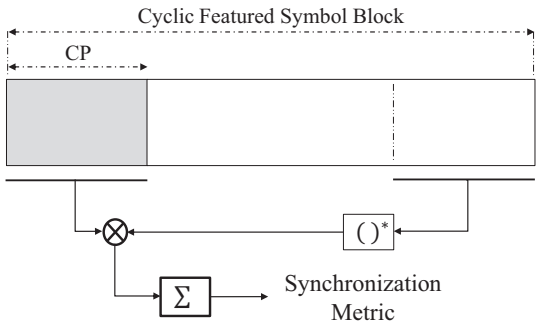

Fig. 1: Cyclic prefix based estimation for synchronization

CP. Also, CP length variation according to the maximum excess delay of the channel is offered as an extra precaution. Alternatively, CP length is changed in a pseudo-random manner for slow fading channels in [15]. The aim is to avoid the complexity caused by continuous channel estimation and to provide a channel independent secrecy. However, both techniques introduce spectral redundancy by either using the CP longer than required or using irrelevant data. If the CP size is set shorter than maximum excess delay of the channel for some of the symbols not to degrade spectral efficiency, then ISI will be another problem.

In this study, we propose a novel CP selection technique, concealing the cyclic features of the signals to prevent malicious users from blind parameter estimation and synchronization without introducing spectral redundancy. For an OFDM system designed based on the proposed technique, CP selection region is shifted towards the next OFDM symbol by a positive random variable while the CP size is kept the same. Since CP will not be correlated periodically with the data part where it is selected, cyclic features are suppressed without adding any redundancy to the signal. At the legitimate receiver side, if the aforementioned random variable is known and the equalization is performed considering these variable as an extension in symbol duration, extended symbol can be assumed as a regular OFDM symbol cyclically convolved with the channel impulse response. Therefore, equalization is performed for each extended symbol as usual and then, the redundant part is removed to obtain the actual data. The proposed technique is presented for OFDM and SC-FDE schemes, and its performance is investigated in terms of error probability and complexity as well as cyclic feature suppression. The rest of the paper is organized as follows. Section II provides an overview of blind parameter estimation and synchronization algorithms based on cyclostationary introduced by CP. The proposed method is presented in Section III. Some numerical results are given in Section IV and Section V concludes the paper with a final discussion.

II. Blind Parameter Estimation, Synchronization and Equalization with CP

Blind receiver design is a well investigated area in the literature. The algorithms developed in this direction to achieve parameter estimation [**?**] – [5] and channel identification [8] – [9] are mostly based on cyclostationarity for the signals that utilize CP. Therefore, suppressing the cyclic features makes difficult to carry out such a receiver design.

If the transmission parameters, e.g., OFDM symbol duration (frame duration for SC-FDE) and CP size, are estimated, blind synchronization in time and frequency can be performed by exploiting the CP. In Fig. 1, the maximum-likelihood (ML) based synchronization is illustrated. The synchronization metric which provides the sample index where OFDM symbol starts, can be obtained as

$$R(l) = \sum_{n=0}^{N_{CP}-1} s[l-n]s^*[l-n+N_S], \tag{1}$$

where $s[n]$ is the received signal, N_{CP} is the length of CP and N_S is the length of the useful portion. Then, synchronization parameters, i.e. the timing position of the symbol and the frequency offset caused by the mismatch between local oscillators of the transmitter and receiver can be found as

$$\hat{n}_0 = \arg\max_l \{|R(l)|\}, \tag{2}$$

$$f_0 = \frac{1}{2\pi}\angle R(\hat{n}_0). \tag{3}$$

However, since the received signal is distorted by the multipath channel and the additive noise, performing the given algorithm with one symbol is not enough to obtain synchronization parameters. Also, frequency offset leads to an extra degradation in the correlation between the repeated parts. Therefore, a number of symbols should be collected and averaged to achieve a reliable synchronization. Then, the effect of multipath channel can be compensated with a single tap equalization in frequency domain and the data can be decoded.

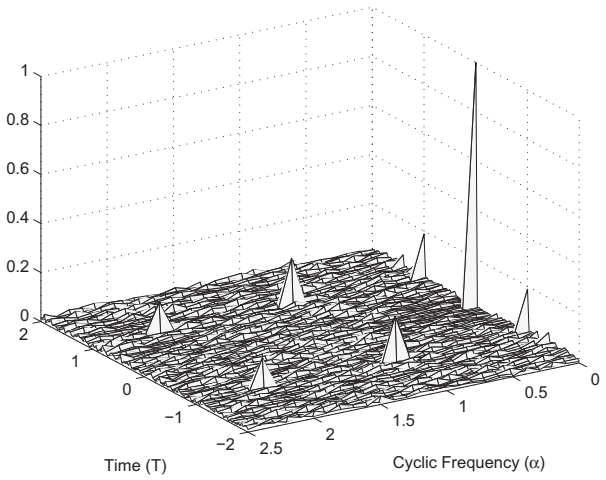

Fig. 2: Cyclic autocorrelation function (CAF) of a conventional OFDM signal.

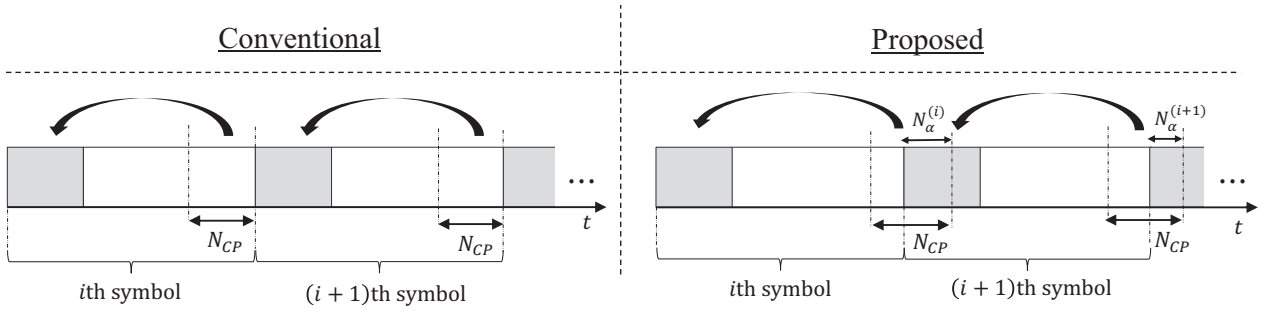

Fig. 3: Cyclic feature concealing cyclic prefix selection

III. Cyclic Feature Concealing CP Selection

As discussed in previous sections, cyclostationarity introduced by CP can be exploited for blind signal demodulation and this can enable unauthorized users to obtain the transmitted data. Cylic features are illustrated in Fig. 2 by using the cyclic autocorrelation function (CAF) for a conventional OFDM signal. Therefore, in order to protect the data and carry out a secure transmission, suppressing the cyclostationarity of the signal is a crucial task. In this study, we propose a novel CP selection methodology that conceals the cyclic features introduced by the CP while maintaining the low complexity in the equalization without introducing any redundant data to the signal. Unlike the conventional CP selection procedure, i.e., copying the last N_{CP} samples of the time domain symbol (frame for SC-FDE), the CP selection region is shifted towards the next block by a positive random variable as illustrated in Fig. 3. Since, the time duration between CP and its selection region changes for each symbol, cyclic features are suppressed and blind decoding of the data becomes much more difficult. Note that, the shifting information of each symbol should also be sent to the receiver. In order to improve security further, guard time between frames, i.e., packets, can also be changed randomly. Then, each frame should individually be synchronized for eavesdropping and the suppressed cyclic features remain useless for the limited number of symbols in a frame.

For analytical representation of the proposed method, let us define the ith time domain symbol vector within the context of the proposed technique as

$$\hat{\mathbf{x}}^{(i)} = [\mathbf{\Gamma}^{(i)} \;\; \mathbf{x}^{(i)}], \tag{4}$$

where $\mathbf{\Gamma}^{(i)}$ is the CP whose selection region is shifted by $N_\alpha^{(i)}$ towards the $(i+1)$th data block, and $\mathbf{x}^{(i)} = [x_1^{(i)}, x_2^{(i)}, \dots, x_N^{(i)}]$ is the useful data part. Assuming $N_\alpha^{(i)}$ takes value between zero and N_{CP}, $\mathbf{\Gamma}^{(i)}$ is defined as

$$\mathbf{\Gamma}^{(i)} = [x^{(i)}_{N-N_{CP}+N_\alpha^{(i)}},\; x^{(i)}_{N-N_{CP}+N_\alpha^{(i)}+1},\; \cdots$$

$$x_N^{(i)},\; \hat{x}_1^{(i+1)},\; \hat{x}_2^{(i+1)},\; \dots,\; \hat{x}^{(i+1)}_{N_\alpha^{(i)}}]. \tag{5}$$

One may note that, if the transmitted signal is generated in this fashion, individual symbols or data blocks are not cyclicly convolved with the channel. Therefore, the signal in the air may not be considered as a conventional OFDM or SC-FDE signal. However, this does not degrade the performance of multipath effect compensation unless the linear time-varying multipath channel $h(t,\tau)$ changes through the extension duration. Also, $N_\alpha^{(i)}$ may be larger than N_{CP} as long as the extended symbol duration is not more than coherence time of the channel. At the receiver, equalization is performed considering the CP selection mechanism, for maintaining the advantage of CP. For achieving this, each symbol is processed with an additional extension of $N_\alpha^{(i)}$ samples from the next time domain symbol as illustrated in Fig. 4. Let us define the extension including time domain samples of the lth symbol copied from the received signal as $\mathbf{y}^{(l)} = [y_1^{(l)}, y_2^{(l)}, \dots, y^{(l)}_{N+N_{CP}+N_\alpha^{(l)}}]$. After CP removal, i.e., removing the first N_{CP} elements of $\mathbf{y}^{(l)}$, frequency domain equalization is performed to estimate the data including the aforementioned extension in frequency domain as

$$\hat{Y}_k^{(l)} = \frac{Y_k^{(l)} H_{kl}^*}{|H_{kl}|^2} \tag{6}$$

where H_{kl} is the frequency response for the lth symbol, assumed to be known by the receiver, that corresponds to kth bin in frequency domain, and

$$Y_k^{(l)} = \sum_{n=0}^{N+N_\alpha^{(l)}} y_n^{(l)} e^{-j2\pi kn/(N+N_\alpha^{(l)})}. \tag{7}$$

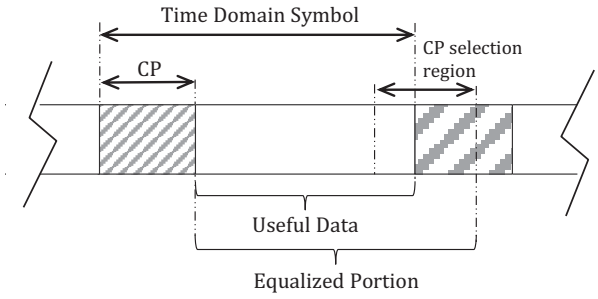

Fig. 4: Illustration of the equalization part for an OFDM symbol designed with the proposed method

Since $\mathbf{y}^{(l)}$ is circularly convolved with the channel, one-tap frequency domain equalization, given in (6), compensates the multipath channel effect. However, the extension introduced by the proposed CP selection whose size is $N_\alpha^{(l)}$ for the lth symbol still exists in the symbol. The process after this stage including $N_\alpha^{(l)}-$ point extension removal and its effect on the performance are different for OFDM and SC-FDE schemes.

A. OFDM

In order to remove the redundant portion after equalization in OFDM, symbols should be transformed back to the time domain. After removing the redundant extension, fast Fourier transformation (FFT) of the actual time domain symbol is taken to obtain the estimated elements of the useful data set, $\mathbf{S}^{(l)}$ as

$$S_k^{(l)} = \sum_{n=0}^{N} s_n^{(l)} e^{-j2\pi kn/N}, \tag{8}$$

where the data set of $s_n^{(l)}$ selected from the first N element of the equalized $\mathbf{y}^{(l)}$ can be defined as $\mathbf{s}^{(l)} = [\hat{y}_1^{(l)}, \hat{y}_2^{(l)}, \dots, \hat{y}_N^{(l)}]$ and

$$\hat{y}_n^{(l)} = \frac{1}{N + N_\alpha^{(l)}} \sum_{k=0}^{N+N_\alpha^{(l)}} \hat{Y}_k^{(l)} e^{j2\pi nk/(N+N_\alpha^{(l)})}. \tag{9}$$

Although, the time dispersion effect of the channel can easily be compensated and the actual data can be obtained at the expense of a reasonable complexity introduced by an extra FFT/IFFT operation, the proposed technique may lead to a degradation in bit-error-rate (BER) performance for OFDM. In conventional OFDM, subcarriers are independent of each other and in the case of a deep fading in the transmission frequency, only the data assigned to the deep faded subcarriers suffers. However, since the number of samples changes through the extension removal process after equalization, the fading effect cannot be kept only in the corresponding frequencies and the enhanced noise after equalization expands to the neighboring frequencies. Therefore, the BER performance of the proposed scheme is expected to be degraded.

B. SC-FDE

In SC-FDE schemes, IFFT is applied to the signal for obtaining the transmission data after equalization as

$$\hat{y}_n^{(l)} = \sum_{n=0}^{N+N_\alpha^{(l)}} \hat{Y}_k^{(l)} e^{-j2\pi kn/(N+N_\alpha^{(l)})}. \tag{10}$$

As the random extension is included in the time domain, it can be directly removed from the lth signal and the useful data can be obtained as $\tilde{y}_n^{(l)} = [\hat{y}_1^{(l)}, \hat{y}_2^{(l)}, \dots, \hat{y}_N^{(l)}]$. Note that, unlike OFDM, there is no requirement of an extra conversion to remove the redundant part and the proposed technique does not introduce complexity. Also, BER performance is not affected as long as the channel remains the same through the extension duration.

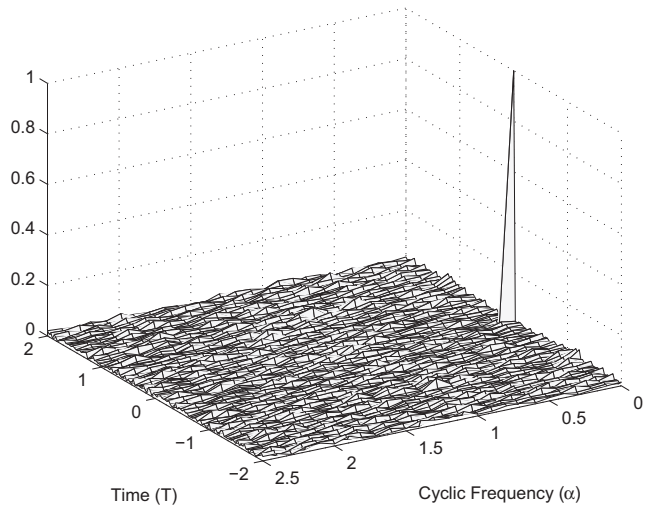

Fig. 5: CAF with the proposed CP selection method

IV. Numerical Results

Simulation parameters for an OFDM system are determined based on IEEE 802.11 standard where the number of subcarriers is 64, the transmission bandwidth is 20 MHz [16], and the modulation type is chosen as 64-QAM. Also, the number of transmitted QAM symbols in an SC-FDE frame is specified as 64 with the same transmission bandwidth and modulation.

In order to show the performance of proposed technique in cyclic feature suppression, CAF of an OFDM signal is given in Fig. 5 for 100 symbols with 1/4 CP rate in a

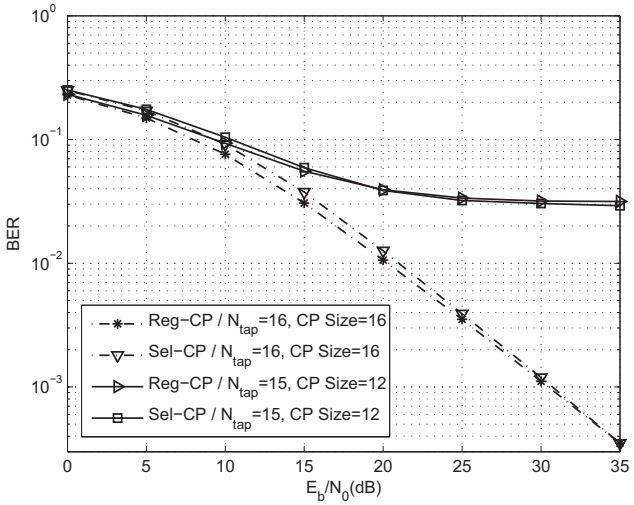

Fig. 6: BER performance of OFDM with regular CP (Reg-CP) and selective CP (Sel-CP) for different number of channel taps (Modulation type is $64-\mathrm{QAM}$)

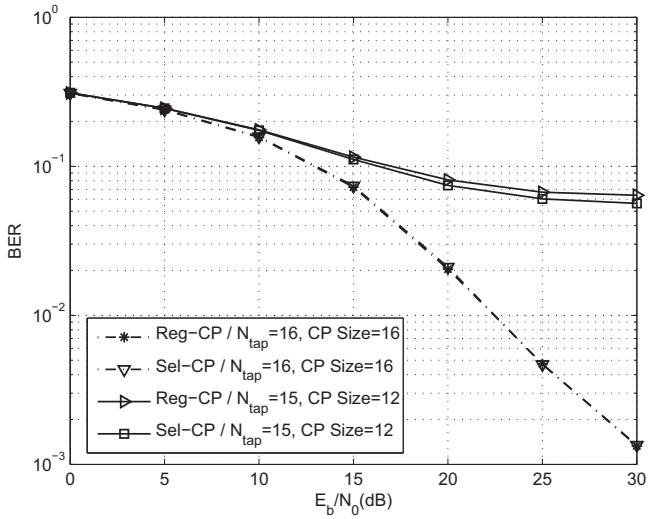

Fig. 7: BER performance of SC-FDE with regular CP (Reg-CP) and selective CP (Sel-CP) for different number of channel taps (Modulation type is $64-\mathrm{QAM}$)

channel and noise free scenario. Since similar results are obtained for SC-FDE, it is not included here. It is clearly seen that all the peaks except the one at zero index in time and frequency are suppressed with the proposed technique even without noise and channel effect. For BER analysis, we consider multipath Rayleigh channel with different number of taps for symbols with different CP sizes. On the legitimate receiver side, the multipath dispersion in the signal can easily be compensated by using CP, as long as the time shift amount in the CP selection is known and the CP size is not shorter than channel tap number. However, due to the aforementioned noise expansion in OFDM, BER performance is slightly degraded compared to conventional OFDM especially for low signal-to-noise ratio (SNR) values as seen in Fig. 6. On the other hand, no negative effect is observed on BER performance when the proposed technique is implemented for SC-FDE as given in Fig. 7. Another interesting benefit of our technique is to improve the robustness against ISI in the case of insufficient CP usage. By selecting CP at least partially from the next symbol, symbol duration used for equalization is kind of extended. Since ISI caused by insufficient CP is related with the ratio of the interference amount and symbol duration, our technique exhibits a better performance than the classical approach by spreading the interference over a larger symbol.

V. Conclusion

In this paper, we presented a cyclic feature suppression technique improving physical layer security against eavesdropping attacks for CP deploying transmission schemes. By changing the CP selection region for each symbol in a pseudo-random fashion, cyclic features are concealed without any degradation in spectral efficiency. While OFDM achieves that with the expense of a reasonable complexity and degradation in BER performance, no disadvantage appears for SC-FDE. As an additional improvement to this study, CP selection index can also be extracted from the channel impulse response to avoid extra signaling and to improve secrecy further. However, we confine this study here and leave the possible extensions for future studies.

VI. Acknowledgment

In this study, Dr.Arslan is supported by Scientific and Technological Research Council of Turkey (TUBITAK).

References

[1] D. Falconer, S.L. Ariyavisitakul, A. Benyamin-Seeyar, and B. Eidson, "Frequency Domain Equalization for Single-Carrier Broadband Wireless Systems," *IEEE Commun. Mag.*, vol. 40, no. 4, pp. 58-66, Apr. 2002

[2] H. Ishii and G. W. Wornell, "OFDM blind parameter identification in cognitive radios," *in Proc. IEEE Int. Symposium on Personal, Indoor and Mobile Radio Commun.*, vol. 1, Berlin, Germany, Sept. 2005, pp. 700-705.

[3] L. Zou, "Detection of the guard interval length in OFDM systems," *in Proc. IEEE Consumer Commun. and Networking Conf*, vol. 2, Las Vegas, Nevada, USA, Jan. 2006, pp. 1048-1051.

[4] H. Li, Y Bar-Ness, A. Abdi, O. Somekh, and W. Su, "OFDM modulation classification and parameters extraction," *in Proc. IEEE Int. Conf.: Cognitive Radio Oriented Wireless Networks and Commun. (Crowncom)*, Mykonos Island, Greece, June 2006, pp. 1-6.

[5] T. Yucek and H. Arslan, "OFDM signal identification and transmission parameter estimation for cognitive radio applications," *in Proc. IEEE Instrumentation and Measurement Technology Conference*, Washington, D.C., USA, Nov. 2007.

[6] J. van de Beek, M. Sandell, and P. Borjesson, "ML estimation of time and frequency offset in OFDM systems,," *IEEE Trans. Signal Processing*, vol. 45, no. 7, pp. 1800-1805, July 1997.

[7] T. Keller, L. Piazzo, P. Mandarini, and L. Hanzo, "Orthogonal frequency division multiplex synchronization techniques for frequency-selective fading channels," *IEEE J. Select. Areas Commun.*, vol. 19, no. 6, pp. 999-1008, June 2001.

[8] R. Heath Jr and G. Giannakis, "Exploiting input cyclostationarity for blind channel identification in OFDM systems," *IEEE Trans. Signal Processing*, vol. 47, no. 3, pp. 848-856, Mar. 1999.

[9] C. Shin, R. W. Heath, and E. J. Powers, "Non-redundant precodingbased blind and semi-blind channel estimation for MIMO block transmission with a cyclic prefix," *IEEE Trans. Signal Process.*, vol. 56, no. 6, pp. 2509âĂŞ2523, Jun. 2008.

[10] S. C. Surender and R. M. Narayanan, "Synchronization for wireless multi-radar covert communication networks," *in Proceedings of SPIE Defense Transformation and Net-Centric Systems*, Orlando, Florida, USA, Apr. 2007.

[11] R. Meyer and M. Newhouse, "OFDM waveform feature suppression," *in Proc. IEEE Military Commun. Conf.*, vol. 1, Anaheim, California, USA, Oct. 2002, pp. 582-586.

[12] X. Wang, P. Ho, and Y. Wu, "Robust channel estimation and ISI cancellation for OFDM systems with suppressed features," *IEEE J. Select. Areas Commun.*, vol. 23, no. 5, pp. 963-972, May 2005.

[13] H. L. Hurd, P. Ho, and Y. Wu, "Stationarizing properties of random shifts," *SIAM Journal on Applied Mathematics*, 26.1 (1974): 203-212.

[14] T. Yucek and H. Arslan, "Feature Suppression for Physical-layer Security in OFDM Systems," *in Proc. IEEE Military Commun. Conf.*, pp. 1-5, May 2007.

[15] M. Bouanen, F. Gagnon, K. G. Kaddoum, D. Couillard, and C. Thibeault, "An LPI Design for Secure OFDM Systems," *in Proc. IEEE Military Commun. Conf.*, pp. 1-6, 2012.

[16] Local and metropolitan area networks - specific requirements. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: high-speed physical layer in the 5 GHz band, *The Institute of Electrical and Electronics Engineering, Inc. Std.* IEEE 802.11a, Sept. 1999.