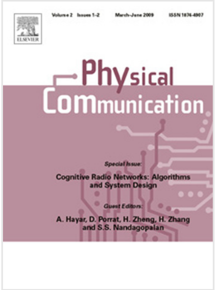
Volume 2 Issues 1-2 March-June 2009 ISSN 1874-4907
Physical
Communication
Special Issue
Cognitive Radio Networks: Algorithms and System Design
Guest Editors
A. Hayar, D. Porrat, H. Zheng, H. Zhang and S.S. Nandagopalan

Cyclic feature suppression for physical layer security

Z. Esat Ankaralı, Hüseyin Arslan

PII: S1874-4907(16)30128-8
DOI: http://dx.doi.org/10.1016/j.phycom.2016.09.003
Reference: PHYCOM 341

To appear in: *Physical Communication*

Received date: 21 December 2015
Revised date: 5 September 2016
Accepted date: 14 September 2016

Please cite this article as: Z. Esat Ankaralı, H. Arslan, Cyclic feature suppression for physical layer security, *Physical Communication* (2016),
http://dx.doi.org/10.1016/j.phycom.2016.09.003

Cyclic Feature Suppression for Physical Layer Security

Z. Esat Ankaralı, *Student Member, IEEE* and Hüseyin Arslan, *Fellow, IEEE*

***Abstract*—Cyclic prefix (CP) deploying techniques such as orthogonal frequency division multiplexing (OFDM) and single carrier frequency domain equalization (SC-FDE) offer considerable advantages in terms of equalizing time dispersive effect of wireless channel at the expense of a reasonable spectral redundancy. However, CP introduces cyclic features to the signal which can also be exploited for signal interception, blind parameter estimation and synchronization, and therefore, compromise the security of the signal against eavesdropping attacks. In order to provide a covert communication against such attacks, in this paper, we present two novel techniques that suppress the cyclic features of the CP utilizing signals while maintaining their advantages in equalization without reducing spectral efficiency. The first technique is built on a CP selection strategy while the second one is based on randomizing the symbol time. We also performed peak-to-average power ratio mitigation and out-of-band leakage suppression along with the cyclic feature concealing in the second technique at the expense of a reasonable complexity and signaling. Subsequent to the presentation of the proposed techniques, their performances are discussed and compared for OFDM and SC-FDE in terms of complexity and bit-error rate along with cyclic feature suppression.[1]**

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

I. Introduction

Cyclic prefix (CP) is a very useful signal component in broadband wireless communication techniques such as single-carrier frequency domain equalization (SC-FDE) and orthogonal frequency division multiplexing (OFDM). In time dispersive channels, its usage offers a considerable advantage in equalization complexity. For instance, when an OFDM symbol in time domain is cyclically extended longer than the maximum excess delay of the multipath channel, linear convolution of the transmitted signal and the channel impulse response (CIR) can be considered as a circular convolution at the receiver. Therefore, transmitted symbol bins mixed up with the previous ones due to the time dispersion effect of multipath channel can be recovered with a single-tap frequency domain equalizer and equalization complexity decreases significantly. In addition to these advantages, CP introduces cyclic features to the signal and they can be utilized for many useful receiver operations such as signal parameter estimation [1]–[4], synchronization [5], [6] and channel estimation [7], [8] without needing extra training signals.

Considering the aforementioned advantages, CP might be assumed as a very beneficial component of the signal rather than a redundant extension. On the other hand, unauthorized users may also attempt to exploit the cyclic features introduced by CP in order to extract the signal parameters, achieve synchronization and decode the data for malicious purposes. In such a scenario, even well-known secure communication techniques such as frequency hopping (FH) and direct sequence spread spectrum (DSSS) may remain vulnerable, since the cyclic features exist anyways when the CP is conventionally deployed [9]. Conventional encryption based techniques providing bit-level security have already been deployed at the application layer to secure the data against eavesdroppers. However, further secrecy precautions might still be essential for many applications especially for the critical domains such as health care, public safety and military. Physical layer (PHY) security offers a promising solution to meet this requirement by providing the security in the transmission level. In this context, cyclic feature suppression is also very critical and should be achieved for a covert signaling.

In the literature, various techniques are presented to achieve cyclic feature suppression especially for OFDM systems. One of the first studies in this direction is done in [10] where cyclic features introduced by the preambles are highlighted. In order to facilitate time and frequency synchronization pseudo-random sequences are used instead of conventional preambles and then, a random frequency offset is added to each preamble to mask the spectral lines further. In [11], embedding OFDM symbols into a notched ultra wide band (UWB) noise signal is proposed. The goal here is to build a secure network among radars via making the system spectrally undetectable. However, sharp filters are used for designing such a system, and bit error rate (BER) performance is degraded due to the noise addition. Another technique for achieving a covert communication is UWB-OFDM where the signal spreads over a very large band in frequency domain and the power level of the signal becomes smaller than the noise level. However, UWB suffers from in-band interference and has practical difficulties in hardware design. OFDM signals are generated with a random frequency jitter in [9] to conceal cyclic signatures. Time

[1] A part of this study is presented in IEEE Military Communication Conference (MILCOM), 2014. The corresponding author, Z. Esat Ankarali (zekeriyya@mail.usf.edu) is with Department of Electrical Engineering, University of South Florida. Also, Dr. Huseyin Arslan (arslan@usf.edu) is with Department of Electrical Engineering, University of South Florida and Department of Electrical and Electronics Engineering, Istanbul Medipol University.