(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 March 2006 (16.03.2006)

PCT

(10) International Publication Number
WO 2006/029208 A1

(51) International Patent Classification:
H04J 11/00 (2006.01)

(21) International Application Number:
PCT/US2005/031869

(22) International Filing Date:
6 September 2005 (06.09.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/522,235 3 September 2004 (03.09.2004) US

(71) Applicant *(for all designated States except US)*: **UNIVERSITY OF SOUTH FLORIDA** [US/US]; 4202 East Fowler Avenue, FAO 126, Tampa, FL 33620-7900 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **YUCEK, Tevfik** [TR/US]; 14247 Les Palms Circle, Apt.3, Tampa, FL 33613 (US). **ARSLAN, Huseyin** [TR/US]; 18167 Sandy Point Drive, Tampa, FL 33647 (US).

(74) Agent: **SMITH, Ronald, E.**; Smith & Hopen, P.A., 15950 Bay Vista Drive, Suite 220, Clearwater, FL 33760 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** COVERT OFDM TRANSMISSION USING CYCLIC PREFIX

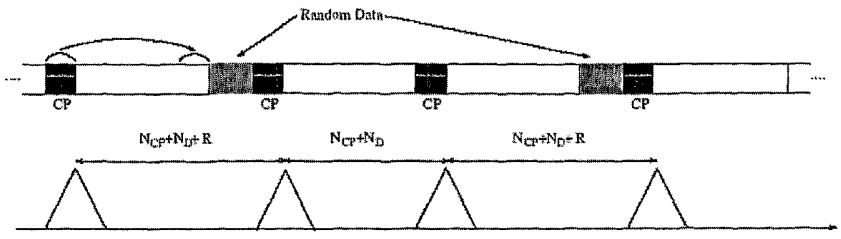

Illustration of the proposed transmission scheme. The resulting correlation peaks in the ideal case is shown as well.

(57) **Abstract:** Methods for secure OFDM communications include changing the length of OFDM symbols in a pseudo-random fashion by appending a totally random signal to some of the OFDM symbols. An adaptive cyclic prefix is provided for covert and spectrally efficient communication. A developed PN based random data addition provides further security by removing the chance of combining synchronization information over several OFDM symbols.

WO 2006/029208 A1

Covert OFDM Transmission Using Cyclic Prefix

STATEMENT OF INTEREST

This work has been supported by Raytheon, Inc. grant CHARTFIELD STRING: USF01 TPA 22000 210600 000000 0000000 210610060.

CROSS-REFERENCE TO RELATED APPLICATIONS

This disclosure is a non-provisional patent application based upon provisional patent application 60/522,235, filed 09/03/2004 by the same inventors and bearing the same title.

BACKGROUND OF INVENTION

1. Field of the invention.

This invention relates, generally, to security measures for wireless transmissions. More particularly, it relates to methods for preventing synchronization to a transmitted signal by an unauthorized user.

2. Description of the prior art.

Orthogonal frequency division multiplexing (OFDM) systems exhibit immunity to multipath distortion. In OFDM, the linear convolution of a transmitted signal with a channel impulse response (CIR) is converted to circular convolution by cyclically extending the transmitted OFDM symbols. The transmitted data symbols are recovered using a simple one-tap equalizer in the frequency domain. The redundancy introduced by cyclic prefix (CP) can be used for channel estimation and synchronization as well. However. CP may be undesirable for covert applications because unauthorized users may explore the periodicity introduced by the CP to synchronize to the transmitted signal.

To remove the distortion due to multipath, the length of the CP should be larger than the maximum excess delay of the channel. When the length of the CP is smaller than the maximum excess delay, previously transmitted OFDM symbols interfere with a current OFDM symbol as indicated in Fig. 1 (prior art). This type of interference is known as inter-symbol interference (ISI) or interblock interference (IBI) and the performance degradation due to ISI is investigated in equations [1] and [2] below. The

power spectral density of the interference is derived in terms of the CIR and the CP length in equation [1]. Assuming there are only post-cursors from the preceding symbol, the signal-to-noise ratio (SNR) of the received signal at each subcarrier position can be written as:

$$SNR(k) = \frac{1}{2} \frac{|H(k)|^2 N}{\sum_n^L N_{CP+1} |h_n|^2} \quad (1)$$

Where *H(k)* is the channel frequency response (CFR) at kth subcarrier, *N* is the fast Fourier transform (FFT) size, *h* is the nth tap of CIR, and *L* is the length of the CIR.

As indicated by equation (1), the degradation depends on the ratio between the tail power of the CIR and total power of CIR, as indicated in Fig. 2 (prior art), which shows BER degradation as a function of guard interval length in a noiseless environment. The length of the power delay profile (PDP) is denoted 20 and it is assumed to be exponentially decaying. Calculating the SNR in each sub-carrier and calculating the average BER provides theoretical results. As Fig. 2 shows, insufficient CP length causes irreducible error floor in OFDM.

The redundancy introduced by the CP can be used to estimate time and frequency offsets. Synchronization algorithms based on the maximum likelihood (ML), equation [3], minimum mean-square error (MMSE), equation [4], and the maximum correlation (MC), equation [5] criteria use the periodicity introduced by the cyclic prefix to estimate the timing and frequency offsets.

The ML method is illustrated in Fig. 3 where only one OFDM symbol is shown. The synchronization metric obtained by one OFDM symbol can be written as

$$M(m) = \sum_{n=0}^{N_{CP}-1} r(m-n) r^*(m-n+N_D) \quad (2)$$

where *r(n)* is the received signal, N_{CP} is the length of CP and N_D is the length of the useful data part. Using (2), the timing position can be found as

$$\hat{T}_n = \arg\max\left|M(m)\right| \tag{3}$$

and frequency offset estimation as

$$\hat{\varepsilon} = \frac{1}{2\pi}\angle M\left(\hat{T}_n\right) \tag{4}$$

These estimates should be averaged over different OFDM symbols to obtain reliable estimates. Adding the correlation metrics from different symbols and dividing by the number of symbols provides the needed average. As the number of available OFDM symbols increase, the estimates become more accurate. The resulting synchronization metric and the final metric obtained by averaging are shown in Fig. 5 (prior art) where the effect of averaging is depicted.

The respective lengths of the OFDM symbol and CP can be estimated blindly by exhaustive searching. This knowledge gives undesired or unauthorized users the ability to synchronize to the transmitted signal. Fig. 4 (prior art) shows the magnitude of the synchronization metric as a function of different CP and OFDM symbol sizes. As indicated in Fig. 4, the peak occurs when the hypothesized lengths are equal to the correct lengths.

The periodicity inherently introduced by the usage of CP can be explored by undesired users to synchronize to the transmitted signal.

Accordingly, what is needed in the art is a technique that prevents unauthorized synchronization while maintaining the advantages of the CP.

However, in view of the prior art considered as a whole at the time the present invention was made, it was not obvious to those of ordinary skill in this art how the needed additional security could be provided.

SUMMARY OF THE INVENTION

The novel methods maintain the advantages of the cyclic prefix but prevent unauthorized exploitation of the cyclic prefix (CP) for synchronization. By allowing use of the CP, the novel methods provide secure data transmission by lowering coding

requirements, thus providing high data transmission rates and decreased power consumption.

In a preferred embodiment, the size of the CP is changed, adaptively, depending upon channel conditions, and random signals are appended to some of the orthogonal frequency division multiplexing (OFDM) symbols in a pseudo-random manner to scramble the correlation peaks in the time domain.

When the correlation peaks are scrambled in time, unauthorized users who are not privy to the scrambling pattern cannot combine the synchronization information with the different symbols. The novel method therefore prevents unauthorized detection of the transmitted signal even if an unauthorized user achieves an initial synchronization.

The present invention makes wireless transmission more secure so that undesired users cannot probe transmitted information. This is especially important for military/defense applications. Moreover, commercial wireless system providers may incorporate this invention for the prevention of theft of service or for increasing user privacy.

More particularly, the novel method for preventing unauthorized exploitation of a cyclic prefix for synchronization, while maintaining the advantages of the cyclic prefix, includes the step of
changing the length of OFDM symbols in a pseudo-random fashion by appending a random signal to at least one of the OFDM symbols. The invention further includes the steps of providing extra scrambling of the correlation peaks by changing the size of the random signal depending on a PN sequence, reducing bandwidth loss due to transmission of the random signal by using a known PN sequence, using the known PN sequence in an authorized receiver for synchronization, increasing the immunity to the multipath by changing the length of the CP in each OFDM symbol according to a PN sequence, thereby scrambling the correlation peaks, combining the adaptive cyclic prefix with channel coding, making the cyclic prefix smaller than a maximum excess delay of the channel, compensating for a performance loss by providing additional coding power, providing additional coding power by using very tight coding, and changing the FFT/IFFT sizes of each OFDM symbol based on a PN

sequence, thereby providing two types of security by making synchronization and demodulation of a received signal difficult for unauthorized users.

BRIEF DESCRIPTION OF THE DRAWINGS

For a fuller understanding of the invention, reference should be made to the following detailed description, taken in connection with the accompanying drawings, in which:

Fig. 1 is a diagrammatic view illustrating the bit error rate degradation due to short cyclic prefix as known in the prior art.

Fig. 2 is a graph representing the bit error rate (BER) degradation as a function of guard interval length in a noiseless environment as known in the prior art.

Fig. 3 is an illustration of the maximum likelihood method as known in the art, showing only one OFDM symbol.

Fig. 4 is an illustration of the magnitude of the synchronization metric as a function of hypothesis cyclic prefix and data lengths.

Fig. 5 is an illustration of the noisy correlation outputs from different OFDM symbols and the resulting synchronization metric which is obtained by averaging these correlations.

Fig. 6 is an illustration of the novel transmission method, including the resulting correlation peaks in the ideal case.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Insufficient CP causes performance degradation and enables undesired users to synchronize to the transmitted signal as the length of the CP gets larger. Therefore, the present invention changes the length of the CP adaptively depending upon channel conditions. The length of the CP should be just enough to prevent ISI. By using a small CP, the present invention prevents synchronization of undesired users to the transmitted signal.

This adaptation requires knowledge of the maximum excess delay of the wireless channel that can be estimated using CFR [6] or channel frequency correlation (CFC) [7]. The length of the CP can be constant over a burst and the length information can be conveyed to the receiver by signaling. Changing the length of the CP adaptively also provides efficient channel utilization since the overall CP time is minimized.

In practical applications, extraction of the synchronization parameters by using the CP with only one OFDM symbol is difficult if not impossible, because the CP is perturbed by multipath components and additive noise. Moreover, the presence of frequency offset decreases the correlation between the repeated parts. To overcome this problem, averaging over a number of OFDM symbols is performed. Fig. 5 shows the noisy correlation outputs from different OFDM symbols and the resulting synchronization metric that is obtained by averaging said correlations. The instantaneous correlations are noisy and the resulting metric obtained by averaging has a peak around the correct timing point which is zero.

Averaging over different OFDM symbols can be done if the length of each OFDM symbol is precisely known.

The present invention changes the length of OFDM symbols in a pseudo-random fashion by appending a totally random signal to some of the OFDM symbols. The resulting frame structure and correlation peaks in a noiseless static channel is illustrated in Fig. 6 where the length of the CP is N_{CP}, the length of the data is N_D, and the length of the appended random signal is R. Using this method, the correlation peaks are scrambled in time. This prevents undesired users from using the CP for synchronization, since they cannot combine the information from different symbols as is possible with prior art systems. Even if an initial synchronization is obtained for the arriving frame, the receiver needs to know the exact start positions of the individual OFDM symbols. This is possible if the positions and lengths of the added random signals are known. An authorized user, on the other hand, can extract the transmitted information since the way the OFDM symbols are scrambled is known. The novel method prevents an unauthorized user from estimating the length of the CP and useful data by executive search method (see Fig. 4) as well.

A pseudo noise (PN)-based preamble is used for synchronization. Since only an authorized user knows the transmitted signal, unauthorized users cannot synchronize to the transmitted signal. Furthermore, the receiver can use the knowledge of scrambling pattern and the redundancy contained in the CP to obtain synchronization information by combining the correlation outputs from each OFDM symbol. Authorized users combine the synchronization information from the preamble and from the CP using an appropriate technique.

The decision on whether to append a random signal to a specific OFDM symbol or not can be made by using the transmitted preamble sequence, or by using the spreading and/or scrambling codes of users in MC-CDMA. If none of those are available, the transmitter must select some specific codes and convey the required information to the receiver.

The following novel method steps enhance the basic method:

1. Provide extra scrambling of the correlation peaks by changing the size of the random signal depending on a PN sequence.

2. Reduce the bandwidth loss due to the transmission of the random signal by using a known PN sequence Instead of a totally random signal. The known PN sequence is used in an authorized receiver for synchronization.

3. Increase the immunity to the multipath by changing the length of the CP in each OFDM symbol according to a PN sequence, thereby scrambling the correlation peaks.

4. Combine the adaptive cyclic prefix with channel coding. The cyclic prefix does not have to be the same as the maximum excess delay of the channel. It can be smaller but not larger (for security purposes). If it is smaller, the performance loss must be compensated for by additional coding power. In the limiting case, no CP is used and the 151 is compensated by using very tight coding.

5. Change the FFT/IFFT sizes of each OFDM symbol based on a PN sequence. This provides two types of security by making synchronization and demodulation of received signal difficult for unauthorized users.

It will thus be seen that the advantages set forth above, and those made apparent from the foregoing description, are efficiently attained and since certain changes may be made in the above construction without departing from the scope of the invention, it is intended that all matters contained in the foregoing description or shown in the accompanying drawings shall be interpreted as illustrative and not in a limiting sense.

It is also to be understood that the following claims are intended to cover all of the generic and specific features of the invention herein described, and all statements of the scope of the invention that, as a matter of language, might be said to fall therebetween. Now that the invention has been described,

What is claimed is:

1. A method for preventing unauthorized exploitation of a cyclic prefix for synchronization, while maintaining the advantages of the cyclic prefix, comprising the step of:

changing the length of OFDM symbols in a pseudo-random fashion by appending a random signal to at least one of the OFDM symbols.

2. The method of claim 1, further comprising the step of providing extra scrambling of the correlation peaks by changing the size of the random signal depending on a PN sequence.

3. The method of claim 1, further comprising the steps of:

reducing bandwidth loss due to transmission of the random signal by using a known PN sequence; and

using the known PN sequence in an authorized receiver for synchronization.

4. The method of claim 1, further comprising the step of:

increasing the immunity to the multipath by changing the length of the CP in each OFDM symbol according to a PN sequence, thereby scrambling the correlation peaks.

5. The method of claim 1, further comprising the step of:

combining the adaptive cyclic prefix with channel coding.

6. The method of claim 5, further comprising the step of:

making the cyclic prefix smaller than a maximum excess delay of the channel.

7. The method of claim 6, further comprising the step of:

compensating for a performance loss by providing additional coding power.

8. The method of claim 7, further comprising the step of:

providing said additional coding power by using very tight coding.

9. The method of claim 1, further comprising the step of:

changing the FFT/IFFT sizes of each OFDM symbol based on a PN sequence, thereby providing two types of security by making synchronization and demodulation of a received signal difficult for unauthorized users.

Fig. 1

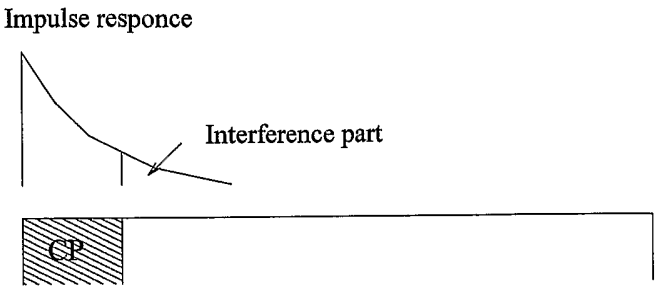

Fig. 2

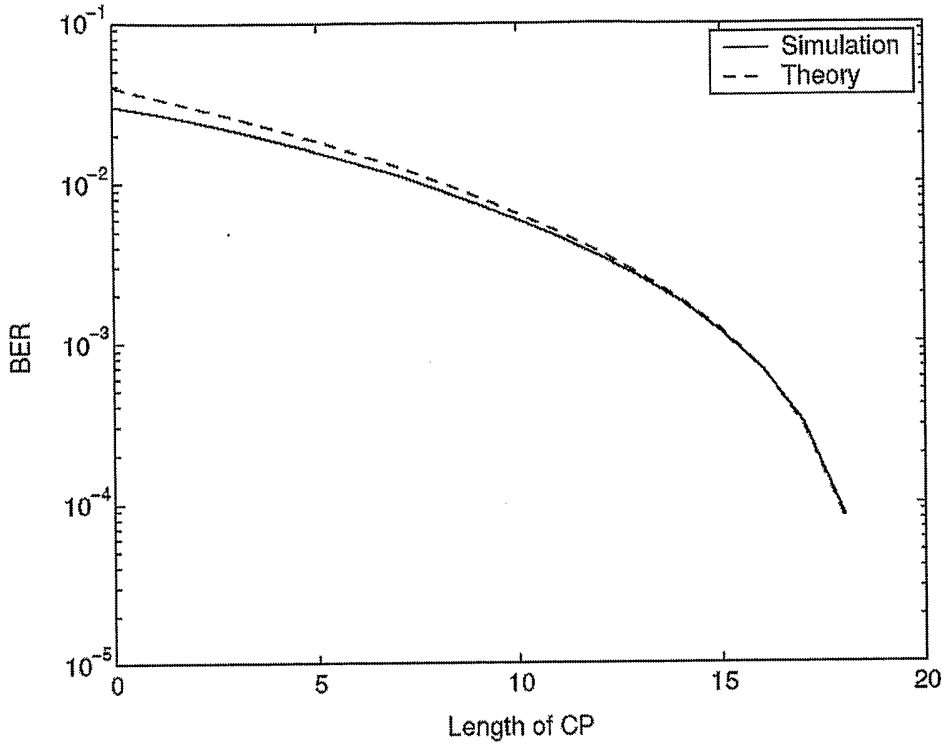

Figure 2: Bit error rate degradation due to short cyclic prefix.

Fig. 3

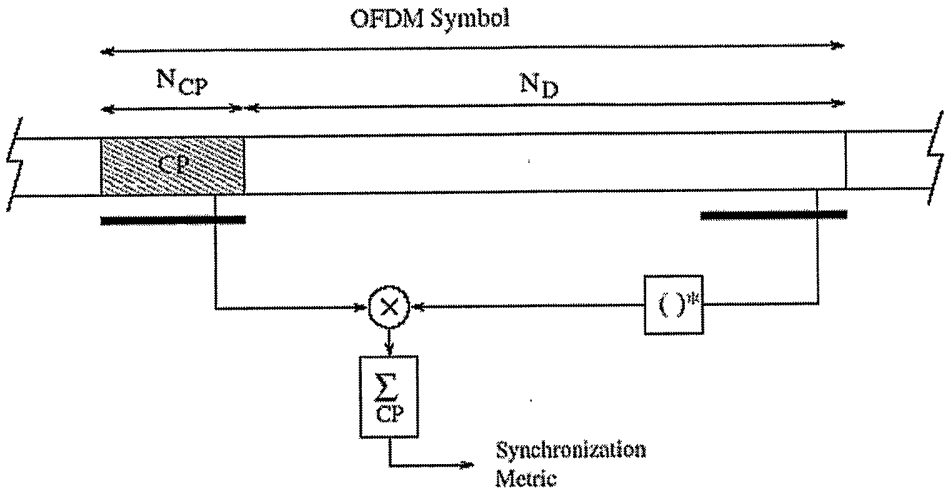

Figure 3: Illustration of cyclic prefix based maximum likelihood estimation.

Fig. 4

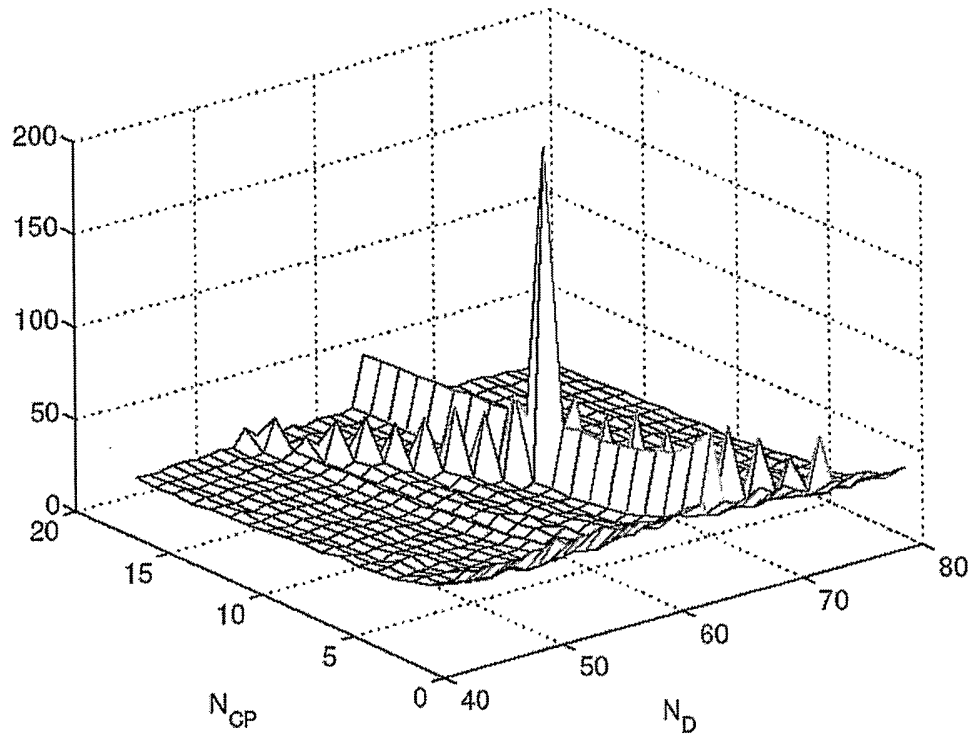

Figure 4: The magnitude of the synchronization metric as a function of hypothesis cyclic prefix and data lengths.

Fig. 5

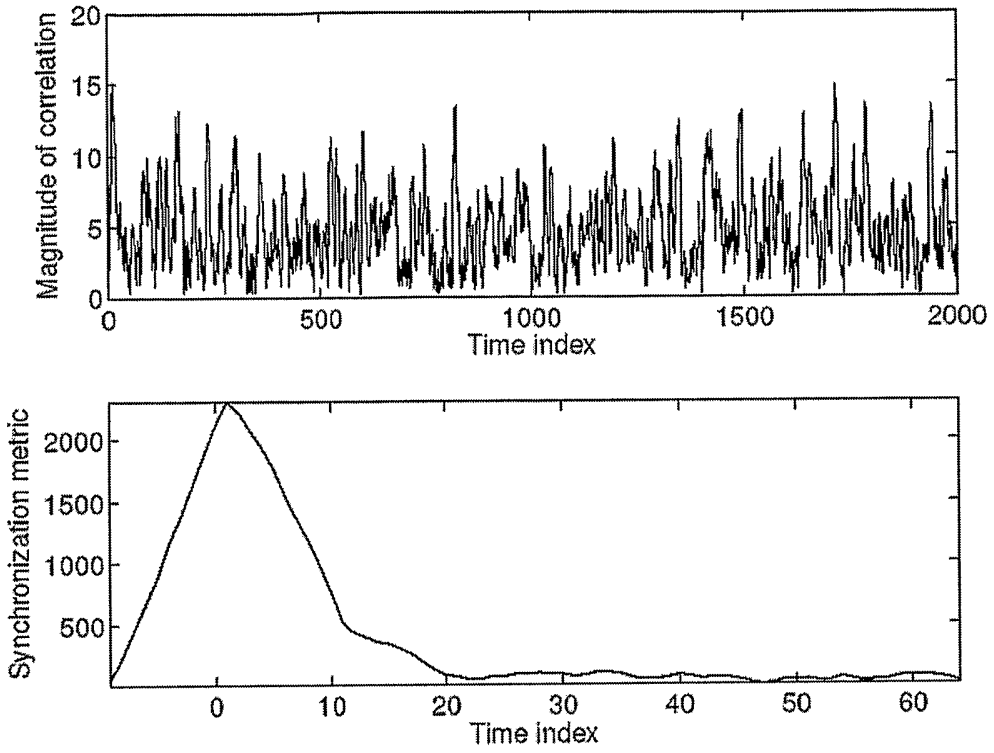

Figure 5: The correlations obtained by using the cyclic prefix and the resulting synchronization metric obtained by averaging.

Fig. 6

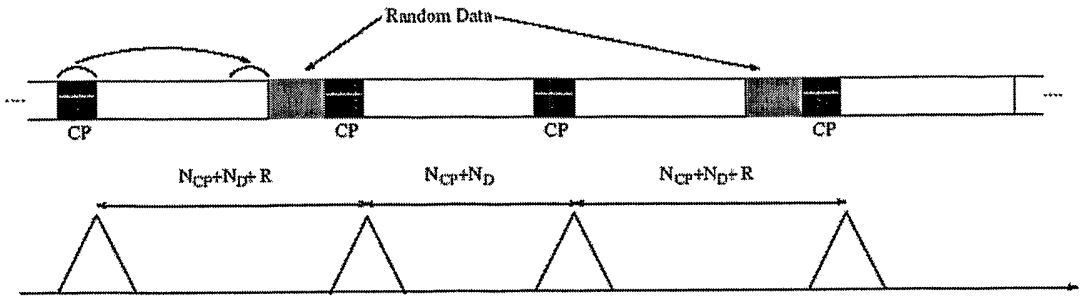

Figure 6: Illustration of the proposed transmission scheme. The resulting correlation peaks in the ideal case is shown as well.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 05/31869

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04J011/00
USPC - 370/206
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
US: 370/206, 208, 210, 212, 335; 375/141, 240, 240.29; 380/200, 253-255

IPC(8): : H04J011/00; H04J011/$; H04J012/$

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
www.whatis.com
definitions of: "cyclic prefix"; "zero padding"; postfix; interleave; "maximum excess delay"; "intersymbol interference"; "tight coding"; IFFT size; "pseudo random"

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

East; www.micropat.com; www.dialogpro.dialog.com; www.uspto.gov search portal
IEEE XPLORE http://www.ieee.org/ieeexplore
Search terms: ofdm; random; pseudorandom; prefix; (security or encoding or encryption); (cyclic prefix); length

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	A Pseudo Random Postfix OFDM modulator Part I: Semi-blind channel estimation and equalization in the static case Muck, Markus and De Courville, Mark B. Duhamel, Pierre This paper appears in: Signal Processing, IEEE Transactions on Publication Date: April 2004 See attached reference	1-3, 5
A	On the Comparison Between OFDM and Single Carrier Modulation With a DFE Using a Frequency-domain Feedforward Filter Benvenuto, Nevio and Tomasin, Stefano This paper appears in: IEEE Transactions on Communications Publication Date: June 2002 Volume 50, Issue: 6 On pages: 947-955 See attached reference	1-9
A	Interleaved Orthogonal Frequency Division Multiplexing (IOFDM) System Prasad, V.G. S. and Hari, K.V.S This paper appears in: Signal Processing, IEEE Transactions on Publication Date: June 2004 Volume: 52, Issue: 6 On pages: 1711-1721 Digital Object Identifier 10.1109/TSP.2004.827179 See attached reference	1-9
A	US2005/0002325 A1 (GIANNAKIS et al) 6 January 2005 (06.01.2005) paragraphs 0008-0022	1-9
A	US 6,842,487 B1 (LARSSON) 11 January 2005 (11.01.2005) Abstract; column 6	1-9
A	EP 1,416,689 A1 (MUCK et al) 06 May 2004 (06.05.2004) pages 1-4	1-9

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 December 2005	10 FEB 2006
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee. W. Young Telephone No. 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 05/31869

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2004/0174809 A1 (SHOR et al) 9 September 2004 (09.09.2004) columns 1-3; figure 3	1-9
A	US 6,928,047 B1 (XIA) 9 August 2005 (09.08.2005) columns 1-4; figures 3 and 4	1-9