Available online at www.elixirpublishers.com (Elixir International Journal)

Network Engineering

Elixir Network Engg. 57A (2013) 14429-14431

ISSN: 2229-712X

OFDM based transit data encryption scheme

Kiran V. Shanbhag
Department of ECE, AITM, India.

ARTICLE INFO

Article history:
Received: 10 November 2012;
Received in revised form:
18 April 2013;
Accepted: 23 April 2013;

Keywords
OFDM,
Encryption,
Matlab,
Security,
Pseudo Noise sequence.

ABSTRACT

Orthogonal frequency division multiplexing (OFDM) has been one of the key contenders in various broadcasting standards, due to its immunity towards multipath fading and ease of implementation. But the issue security has not been addressed much, which calls for a separate modules performing encryption. Here a scheme of Encryption jointly with OFDM has been proposed based on rearranging the OFDM subcarriers to make the data non intelligible, which provides transit data security. Simulation results show that the proposed scheme provides both security and immunity against fading, together. Also, compared to the conventional OFDM system, this scheme provides encryption with no BER performance degradation and no additional bandwidth.

Introduction

Orthogonal frequency-division multiplexing (OFDM) is a method of encoding digital data on multiple carrier frequencies. Here a large number of closely spaced orthogonal sub-carrier signals are used to carry data. The orthogonality allows for efficient modulator and demodulator implementation using the FFT algorithm on the receiver side, and inverse FFT on the sender side. The primary advantage of OFDM over single-carrier schemes is its ability to cope with severe channel conditions (for example, attenuation of high frequencies in a long copper wire, narrowband interference and frequency-selective fading due to multipath) without complex equalization filters. Hence OFDM has developed into a popular scheme for wideband digital communication, used in applications such as digital television and audio broadcasting, DSL broadband internet access, wireless networks, and 4G mobile communications [1].

When using wireless channel, the broadcast nature exposes transmission to eavesdropping. Securing communication links from eavesdropping is commonly done by implementing encryption algorithms in software, and is usually detached from the physical layer of communication. There are some encryption methods which rely on the physical layer of communication for their implementation, such as spread spectrum Frequency Hopping (FH) and Direct Sequence (DS) [2]. In these methods Encryption and decryption impose overheads on data throughput, energy consumption, memory space, and computation power [3].

Since OFDM/OFDMA forms the integral part of most of the communication channels, we propose a transit data encryption scheme which is carried out along with OFDM. The scheme provides a robust security solution. The scheme proves to advantageous for the channels which are already employing OFDM technology, as it gives an ease of providing security without much changes in the existing hardware or extra bandwidth as compared to the other physical layer encryption schemes[4],[5]. For the systems which do not employ OFDM, this scheme provides security along with all the advantages of OFDM.

Proposed scheme

The scheme works as follows. Initially any type of data whether text, audio or image shall be converted into a data string. This string is then divided into substrings of length N which would be a radix of 2. These segments will be transformed to frequency domain using N point IFFT (which is similar to FFT). Now these individual N IFFT coefficients are circularly shifted, with different shift factor for each segment. These shifts carry out the encryption process. The amount of circular shift per segment is determined by a sequence generator for example PN sequence generator which generates almost random sequence. Now the data has lost its original form and scrambled. This encrypted data now can be either stored or transmitted. The decryption process would include the circular shift in the reverse direction, which would be possible only for the authorized decoders with the knowledge of the particular sequence generators used at the encoder end, which forms the secret key. Then perform N point FFT to get the original data.

The task obtaining IFFT is equivalent to dividing the data into low frequency subcarriers which is a part of OFDM implementation. Similarly the reverse process of taking FFT is also done at OFDM receiver. Hence for these tasks there is no need for additional hardware if the channel is already employing OFDM, thus reducing system cost & complexity.

Implementation

The figure below shows the implementation of the scheme. The focus in this paper is not the mere implementation of the encryption scheme but to do so by slightly altering the already existing OFDM structure. Except for the encryption/decryption block, rest of the blocks pertain to a simple BPSK based N point OFDM with cyclic prefix. The circular shifter block carries out the task of encryption. The use of modulation and cyclic prefix is not necessary if the transmission scheme is other than OFDM.

Tele:
E-mail addresses: shanbhagkiranv@gmail.com

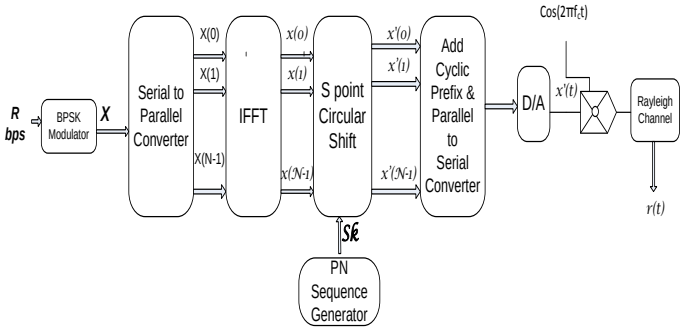


Fig.1 Scheme showing OFDM transmission with Encryption

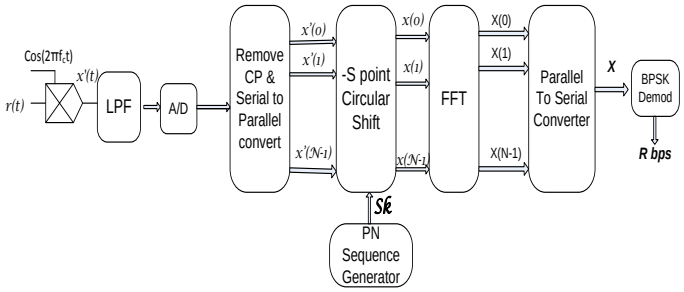
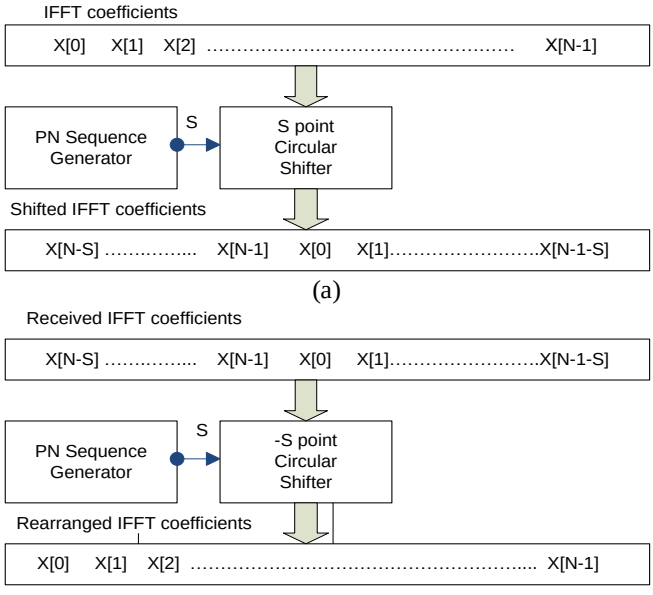


Fig.2 Scheme showing OFDM reception with Decryption

Fig.3a shows the scheme for scrambling the data by circularly shifting the individual, N IFFT coefficients by S points, where the value of S is generated by a PN sequence generator. The sequence generator can be either a simple one or it can be one of the cryptographically secure pseudo-random number generator (CSPRNG) [4].Fig.3b shows the rearrangement of IFFT coefficients by reverse shifting the coefficients using the same PN sequence generator at decoder thus decrypting the data. The period for the sequence generator should be equal to or greater than N. Security strength of the method is decided by the type of PN sequence generator used, and increases with increase in the value of N. As the shift is circular or modular in nature, a shift value greater than N will not affect the performance but it increases the possible number of initial values which makes it difficult for the attackers.



(b)

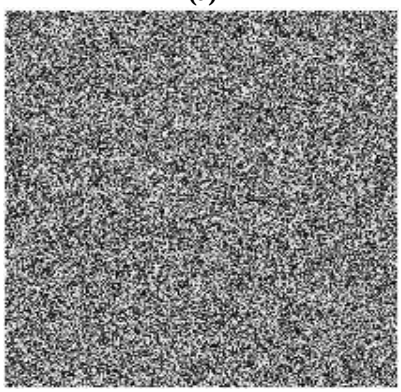
Fig.3 The detailed description of encryption /decryption block

(a) Scheme showing the S point IFFT Co-efficient shift or encryption (b) Scheme showing rearrangement of coefficients or decryption

Simulation Results

The proposed system was tested on a sample text and an image data on Matlab platform and the results have been summarized in this section. BPSK modulation with raised cosine pulse shaping was used. 1024 point IFFT & FFT were used with 4 point cyclic prefix. The data , both text and grey scale image image were first converted into binary form and broken into chunks of 1024 bits and fed to the block. A 10 bit PN sequence generator was used as the key to perform circular shift. The results have been encouraging as both the text and the image were not intelligible without the authorized key, as shown Table 1 in case of text and Fig.4 in case of a grey scale image. Moreover the encryption process has not affected the OFDM performance compared to the one without encryption and hasn't conceded extra bandwidth.

(a)



(b)

(c)

Fig.4 (a) Original grey scale image of lena.bmp (b) The encrypted image (c) Decrypted image

Conclusion

A novel scheme to perform encryption employing OFDM was proposed and its performance was analysed for both text and image data. The scheme uses the existing OFDM architecture with an encryption block inserted, which shifts the IFFT coefficients in a known pseudo random manner thus achieving encryption and it was concluded that the said scheme performs correctly and efficiently.

Table 1. Original sample text data compared with the encrypted data derived through simulation

Original Data:
'The sea of tears becomes crowded with other animals and birds that have been swept away by the rising waters.
Alice and the other animals convene on the bank and the question among them is how to get dry again. The mouse gives them a very dry lecture on William the Conqueror.'

Encrypted Data:
;bBi%tP^5%SRLqMa*z-x#gpUbq|]1Y6&<V1Mm|3QY□&wK=[KD31Tjb'^yYg%
L-a*hK#i$Q4p`x|kAuZ^&2a=2](g7}_a]ORhGJX[aIj#B5%M)./N{y&>qgd!f<khHI`FJ,Afqf9J\"<;_C-{2dPRAZ;!E^.HB|uC&_eX$Ap`-
DE"/{(/-N#?9\=Xc4M<gV VOg□ch;~ [-z'_,hjwB;8l]m+tC\8gi

Decrypted Data:
'The sea of tears becomes crowded with other animals and birds that have been swept away by the rising waters. Alice and the other animals convene on the bank and the question among them is how to get dry again. The mouse gives them a very dry lecture on William the Conqueror.'

The low computational complexity and feasibility of implementation make the method a good solution for securing OFDM transmission in wireless systems where the complexity associated with implementing traditional security algorithms is prohibitive.

References

[1] A. Goldsmith, *Wireless Communications*, Cambridge University Press, Cambridge, UK, 2006

[2] M.K.Simon, J.K.Omura, R.A.Scholtz and B.K.Levitt, *Spread Spectrum Communications Handbook*, McGraw-Hill, New York, NY, USA, 2002.

[3] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, "A study of the energy consumption characteristics of crypto-graphic algorithms and security protocols," *IEEE Transactions on Mobile Computing*, vol. 5, no. 2, pp. 128– 143, 2006.

[4] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 38–47, 2004

[5] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no.6,pp. 644–654, 1976.

[6] Michael Luby, *Pseudorandomness and Cryptographic Applications*, Princeton University Press, 1996.