Optik 122 (2011) 787–791

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

# Security enhancement of OCDMA system against eavesdropping using code-switching scheme

Vishav Jyoti, R.S. Kaler*

*Thapar University, Patiala, India*

ARTICLE INFO

*Article history:*
Received 6 October 2009
Accepted 21 May 2010

*Keywords:*
Eavesdropping
OCDMA
Code-switching

ABSTRACT

In this paper, the security enhanced OCDMA system based on spectral encoding using code-switching scheme is analyzed. The security issues are investigated by measuring eye diagrams and received signals for various cases. It has been observed; an eavesdropper based on a simple energy detector can easily read the information being transmitted by a single user using on–off keying. In order to increase the security a code-switching scheme is implemented on OCDMA. It is shown that the eye diagram at the eavesdropper becomes true noise waveform due to code-switching scheme and at the receiver end a clear eye diagram is observed. Hence, it is concluded that the code-switching scheme shows an immunity of the OCDMA system against eavesdropping and like conventional OCDMA schemes an authorized user clearly decodes an original data when a single user is active in the network.



## 1. Introduction

The act of surreptitiously listening to a private conversation is known as eavesdropping. It can be done over telephone lines (wiretapping), email, instant messaging, and other methods of communication considered private. The security deals with data that is encoded in such a manner that decoding is difficult or impossible without some secret information, even if the coded or encrypted form of the data is easily read. The confidentiality assures that only the intended receivers of information actually receive the information. It can be compromised to various degrees and in the worst case; an eavesdropper can directly read the data. Even if an eavesdropper cannot read the data, the knowledge that two particular people (or computers) are communicating may compromise confidentiality. A part of information is available to potential adversaries just by knowing the traffic patterns.

The potential adversaries are technologically sophisticated, have significant resources, and know a great deal about the signals being transmitted [1]. In particular, the eavesdropper knows what types of OCDMA signals are being sent: the data rate, the type of encoding, and the structure of the codes – but not the particular code that an individual user employs. This is because it is reasonably easy for a user to change codes in the event his code is compromised. However, the other parameters mentioned, such as the data rates, the types of codes, etc., are difficult to change quickly, and might even require a hardware or software redesign of the communication equipment in the event that they were found out by an adversary. Underestimating an adversary is a poor security practice; one must assume, when doing a security analysis that an adversary may even know hard to change parameters.

Shake [1] examined the degree and types of security that may be provided by OCDMA encoding. A quantitative analysis of data confidentiality is presented for OCDMA encoding techniques. It is shown that increasing code complexity can increase the signal-to-noise ratio (SNR) required for an eavesdropper to "break" the encoding by only a few dB. Rapid reconfiguration of codes can also increase the difficulty of interception. The overall degree of confidentiality obtainable through OCDMA encoding is also compared with that obtainable through standard cryptography.

Leaird et al. [6] experimentally investigated spectrally phase coded OCDMA with a modulation format based on switching between two codes. The code-switching data modulation format enhances security compared to on–off keying by eliminating a vulnerability to eavesdropping based on a simple energy detector.

Chung et al. [8] experimentally demonstrated a security improved optical code division multiplexed access (CDMA) scheme based on spectrally encoded incoherent broadband light source with bipolar coding. The details of coding scheme are shown and security issues have been investigated by measuring eye diagrams and bit error rates for various cases. The analytical and numerical simulation results are presented for secure transmission of spectrally encoded incoherent optical CDMA signal.

* Corresponding author at: Electronics and Communication Engineering Department, Thapar University, Patiala 147 004, India.
*E-mail address:* daisykaler@yahoo.co.in (R.S. Kaler).

0030-4026/$ – see front matter © 2010 Elsevier GmbH. All rights reserved.
doi:10.1016/j.ijleo.2010.05.027

Up till now most arguments advocating OCDMA for secured communication in the research literature have been qualitative and vague. Various approaches have been suggested for enhancing the network security mechanisms in order to protect the network from attack by unauthorized users. In this paper a code-switching scheme is implemented for security enhancement and making the OCDMA system less vulnerable to eavesdropping.

The paper is divided into different sections. In Section 1, the brief introduction about the eavesdropping is presented. In Section 2 a descriptive model is proposed for security enhancement of OCDMA system when single user is transmitting. Section 3 describes the simulation setup for bipolar coding based OCDMA system. Section 4 includes the simulation results and the results have been discussed. Section 5 gives the conclusion of this paper.

## 2. Descriptive model

Up to recent days, various OCDMA schemes have been proposed and demonstrated based on time spreading, phase coding, spectral encoding, or two-dimensional (time-spectral) encoding. All these approaches used on–off keying (OOK) for data modulation [2] in which a coded transmission is sent during a bit interval to represent a "one," and no energy is sent during a bit interval to represent a "zero." This makes the implementation of optical transmitters and receivers relatively simple. It is also highly vulnerable to relatively simple eavesdropping techniques. The eavesdropper does not need to decode the signal; he can just read the ones and zeros directly. If an eavesdropper can isolate individual user's signals as in Fig. 1, he can use a simple energy detector to detect whether energy is present or not in each bit interval [3]. In this case, there is no need for the eavesdropper to "break" the coding scheme or steal the code; the energy detector output contains the user's data stream.

One of the many possible OCDMA schemes is illustrated in Fig. 2. A particular arrangement of different colors is representing a code at different time slots (known as chips) within a single data bit [4]. It should be clear that if only one data stream is present, the total energy in each bit time is all the information needed to obtain the data bits. When multiple users are present, deciphering the data bits becomes more difficult – especially, as in the case illustrated, when the data streams are asynchronous.

A solution that relies solely on the properties of the encoding would be to force the modulation technique to send a constant amount of energy for each transmitted bit by transmitting one code sequence for a "one" and a different code sequence for a "zero" as shown in Fig. 3. The user could send out a particular optical code for a "1" and an orthogonal optical code for a "0". This approach is called 2-code keying or code-switching scheme [1]. It is also known as bipolar coding. 2-code keying would require distribution of twice as many codes for a given set of users. It would produce significantly more multiple access interference for a given number of simultaneous transmitters compared with on–off keying based OCDMA, although it would also increase the receiver's average energy per data bit, since energy would be transmitted for both "zeros" and "ones." It would work with most proposed OCDMA technologies and would remove the vulnerability to eavesdroppers with simple energy detectors. Now an eavesdropper (no matter how good the signal-to-noise ratio is) cannot measure the signal. The eavesdropper is now forced to figure out the coding in order to decode the signal and obtain the data, which is a far more complicated and difficult task than tapping the user's signal and detecting the power transmitted during each bit period [6].

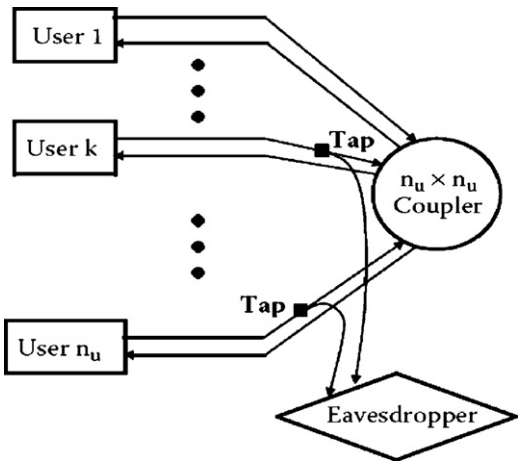


**Fig. 1.** An eavesdropper tapping into the optical fiber can isolate an individual user [1].

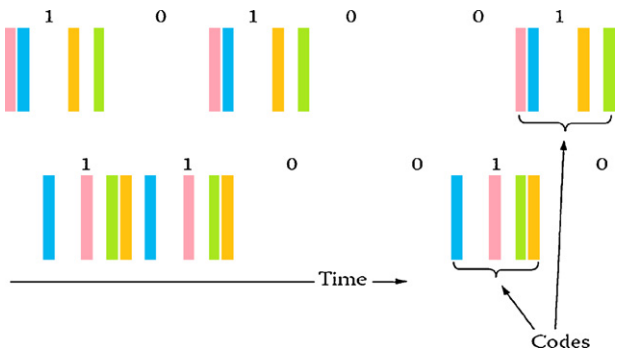


**Fig. 2.** Schematic of two, asynchronous incoherent OCDMA channels using on–off key modulation. Note that no decoding is needed if only one channel is present [5].

This increased security has its costs that are:

- Twice as many codes are needed.
- The increase in codes will increase multiuser interference, which may reduce the number of users.
- The increase in codes adds complexity to the network, which may increase the cost of network management.

## 3. Simulation setup

The simulation setup for the security enhanced OCDMA system based on spectral encoding with bipolar code and incoherent broadband light source is shown in Fig. 4. In bipolar coding, a particular code is used to transmit the data bit 1 and its complementary code to transmit the data bit zero. The setup that is shown is for the single transmitting user. The optical CDMA code used is a modified PN code [7]. The output of broadband light source which is DMLaser1 is demultiplexed into 32 spectral chips with the help of OptDeMUX1. The wavelengths of chips ranged from 1530.33 to 1554.94 nm with 100 GHz spacing. According to the modified PN code, 16 spectral components are connected to the

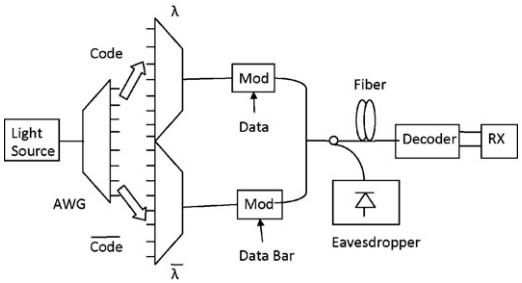


**Fig. 3.** Block diagram of OCDMA system based on spectral encoding with bipolar code.