Security enhancement in optical code division multiplexed system using anti jamming technique

SIMRANJIT SINGH*, KAWALPREET KAUR
Department of Electronics and Communication Engineering, Punjabi University, Patiala, Punjab, 147002 India

In this paper, anti-jamming technique is proposed using semiconductor optical amplifier (in a Mach-Zehnder configuration) based wavelength converter. This is an effective approach for simultaneously improvement in security of the spectrally encoded optical code division multiplexed access (OCDMA) system against the jammer and unauthorized user by using wavelength conversion and multi-diagonal (MD) coding, respectively. Also, the result shows that the proposed system has improved capability of anti-jamming even at high jamming powers.

(Received July 31, 2015; accepted September 29, 2016)

Keywords: OCDMA, Multi-Diagonal codes, Anti jamming and semiconductor optical amplifier

1. Introduction

Optical code division multiple access resembles spread spectrum CDMA techniques employed in wireless communication. CDMA in the radio frequency is said to be inherently secure but OCDMA can be attacked at the physical layer of the network by launching an interferer signal to jam the system [1]. The attack method considered in this work is jamming which is used to describe the deliberate use of attack signals in an attempt to degrade or disrupt communication. Basically, jamming is the overpowering of authorized network signals with the jammer signals. Jamming signals are threat to signal availability which can degrade the performance of OCDMA system. Signal availability means that information transmitted over the link is not lost or disrupted in some way. Jammer transmits at the same waveband as the authorized user but at higher power as compared to the user which cause the original signal to become unreadable by the receiver [2]. Jammer can jam the system either by flipping some message bits or by overpowering the original message. Hence, the jammer signal overlaps the transmitted information reducing the original signal to noise in the jammer' signal. Since the attacker is transmitting in the same waveband, the original message gets replaced by the jammer's message. When the decoder tries to decode it, the decoded signal will be a jammer signal rather than the original data.

The wavelength conversion is a promising technique to provide anti jamming in OCDMA by translating the data from one optical wavelength to another without modifying the content of the data [3]. The main features of a wavelength converter are compactness, transparency to bit rates and modulation formats, low optical power operation, polarization insensitivity, amplification and wide conversion bandwidth. In wavelength converters, basically the physical properties of a nonlinear element are used to perform conversion function [4]. It is observed that jammer has no effect on OCDMA network even at high jamming powers by using this technique. The role of the wavelength converter can be to act as a wavelength slot interchanger to direct signals to a given node in the network; or simply to increase the capacity and the flexibility of the network by re-using the available wavelengths.

Several techniques have been proposed in the literature to perform the wavelength conversion function, e.g: i) crosstalk and four wave mixing in semiconductor optical amplifiers ii) gain saturation in DBR lasers as well as iii) four wave mixing in short length Bismuth non linear fiber (Bi-NLF) , code conversion using periodically poled LiNbO3 waveguides [5]. The converters based on Bi-NLF fiber have splice loss disadvantages such as mode field diameter mismatch and thermal expansion mismatch, when spliced with conventional single mode fiber which limit their application in practical communication systems . Additionally, bismuth-based fibers exhibit large propagation loss which is intrinsic to the material, i.e. bismuth-oxide. Also, the converters based on fibers have low conversion efficiency. The converters based on PPLN waveguides require very high pump power (18-23dBm) and long lengths [4].

Therefore, based on the above discussion an efficient anti-jamming technique is required which ensures signal availability at high jammer power. Here, a wavelength converter relying on optically controlled refractive index change in semiconductor optical amplifiers (SOA's) is demonstrated. The SOA's are situated in a Mach-zehnder configuration in order to transfer the phase modulation into an amplitude modulated signal [6-9]. The advantage of this concept is the low operation power needed (< -10 dBm) as well as the ability to improve the signal quality of the converted signal with respect to extinction ratio and chirp.

The paper is organised as follows: after this introductory part, the working of the wavelength converter and the construction of multi-diagonal codes is discussed in Section 2. In Section 3, the system parameters for the wavelength conversion are presented. The simulation set up is done in section 4. Their results are discussed in section 5. Section 6 summarizes the conclusions.

2. Working of proposed model

The proposed model consists of MD-OCDMA codes and an anti-jamming technique using SOA in Mach-zender configuration.

2.1. Working of wavelength converter

A schematic of the wavelength converter configuration is depicted in Fig. 1. It consists of a Mach-zehnder interferometer with SOA's inserted in the two arms as phase shifting elements. In principle only one SOA is needed but two SOA's give a higher gain. In order to use the configuration for wavelength conversion, asymmetry is required in the MZI, e.g., different splitting ratios in the couplers or asymmetric biasing of the SOA's. The operation is [4]: CW light is injected into the MZI at the wavelength**,** and at the output of the converter it will experience constructive or destructive interference depending on the phase shift through the SOA's. The SOA phase shift relies on the change in carrier density that can be controlled via the bias current or the optical input power (gain saturation). If optical power is injected into the MZI at λ_i the carrier density, N in the SOA's will change due to the increased stimulated emission. Consequently, the phase, ϕ and there by the output power at λ_c, will change. So it is possible to vary the output power at λ_c, by varying the input power at λ_i; consequently, wavelength conversion is achieved.

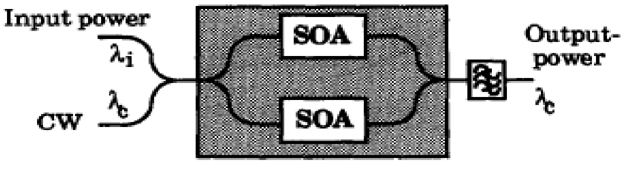


Fig. 1. Schematic of SOA MZI wavelength converter [4]

2.2. Multi-Diagonal Codes

To improve security in the network, the system design should minimize the amount of energy that an eavesdropper can receive by tapping fiber signals. This requires that each transmitter minimize the power it sends into the network. This minimization cannot be done without affecting the BER performance of the system. An authorized receiver's BER performance is the function of the received SNR which is given by [7]

$$\frac{E_u}{N_{ou}} = \frac{E_u}{N_{OM}+N_{Or}} \qquad (1)$$

Where $N_{OM}$the total is noise spectral density due to multiple user interference and N_{Or} represents the spectral density of the receiver noise. $N_{OM}$is proportional to both the number of active transmitters and to the transmitted power of each user while N_{Or} is fixed for a given receiver implementation.

If $N_{Or}$is negligible compared to N_{OM}, the resulting SNR at an authorized user's receiver will be sufficient to maintain the specified BER. If each transmitter reduces its power level sufficiently to increase confidentiality, thoughN_{OM}, will also be reduced and N_{Or}will become significant compared to N_{OM} . The ratio E_u/N_{ou} determines BER, and this will be reduced by reducing the power level of each user and hence, increasing the BER. If the transmitted power is reduced arbitrarily, the only way to keep the BER from exceeding a specified value is to reduce the N_{OM} term as well. So there is a need of zero crosses correlation in order to increase confidentiality .The MD codes provide no cross correlation between the transmitting users as per their construction. In this technique we have taken three users with code weight two i.e, K=3and W=2.

The position matrix is defined [8] as:

$$P_{i,1} = \begin{bmatrix}1\\2\\3\end{bmatrix}, \qquad P_{i,2} = \begin{bmatrix}3\\2\\1\end{bmatrix},$$

and,

$$Q_{i,1} = \begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}, Q_{i,2} = \begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix}$$

So, the MD code matrix will be of order 3× 6 and is given as:

$$MD = \begin{bmatrix}1&0&0&0&0&1\\0&1&0&0&1&0\\0&0&1&1&0&0\end{bmatrix}$$

Hence the codeword for each user will be:
Codeword for user 1 = λ_1,λ_6,
Codeword for user 2 = λ_2,λ_5,
Codeword for user 3= λ_3,λ_4,

It is cleared from their construction that the MD code design is constructed with zero cross correlation properties, which cancels the MUI.

3. System setup

System setup has been proposed for three users which transmit the data using MD codes on optical fiber simultaneously. To protect the data from jamming by a high power signal in the same frequency band,anti-jamming technique is used. Using this technique data is transmitted outside the actual wavelength range to protect against jamming and this is done using wavelength conversion. Wavelength conversion is done using SOA in mach-zender configuration as explained previously. Setup of anti-jamming technique in OCDMA system is shown in Fig. 2 with three users transmitting data over an optical fiber. Coding is done using MD codes. Wavelength conversion and deconversion is performed at transmitter and receiver side respectively.

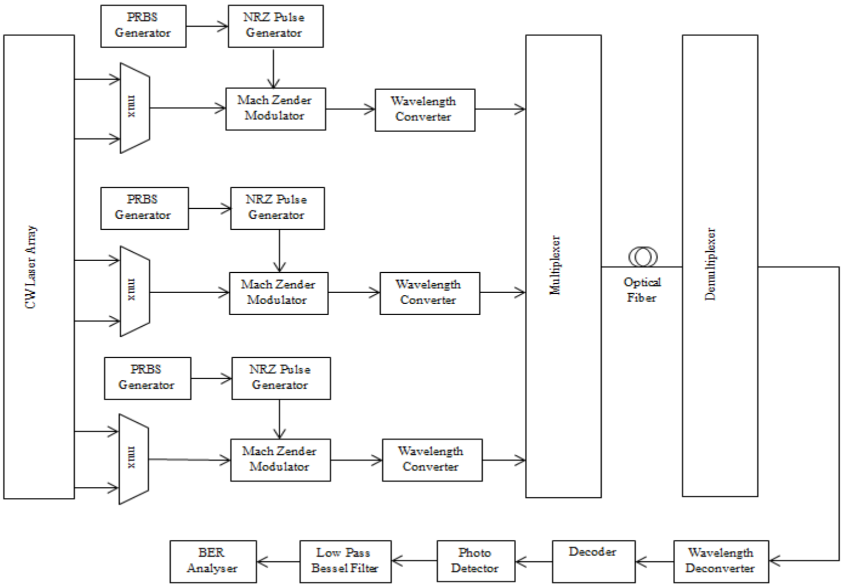


Fig. 2. System setup for anti-jamming OCDMA system

4. System parameters for wavelength conversion

For a proof of concept, the MZI converter was constructed by discrete SOA's and fiber couplers. The continuous wave lasers having wavelength range 193.1–193.6 THz are used to create the carrier signal. The carrier signal is then spectrally encoded using the multi diagonal code. The use of MD codes enables a large number of asynchronous users to transmit information efficiently and reliably. The NRZ data is PRBS at bit rate of 1 Gbps. The transmission data is modulated on an optical CDMA sequence at modulator [10]. The modulated data is then sent to wavelength converter before being combined in the optical fiber. The detailed block diagram of SOA based wavelength converter is shown in Fig. 1. This will translate the input signal out of jamming window according to the pump wavelength. The optical pump source pumps at input power of -20 dBm. By changing the pump wavelength, we can change the output signal but the pump signal is according to code. The pump and OCDMA encoded signal are then combined by a coupler. Then this combined signal is fed to both the arms and then to SOA's where wavelength conversion takes place to the pump signal. After that the signals from both SOA's are combined using coupler and as a result signals come out of first arm are the original wavelengths and at second arm converted wavelengths [11]. Converted wavelengths are transmitted using optical fiber and original wavelengths are blocked. In order to see the effect of jamming, a jammer is incorporated in the network. Jammer is transmitting at the same waveband as the authorized user's encoder with the signal power of 1 mW.

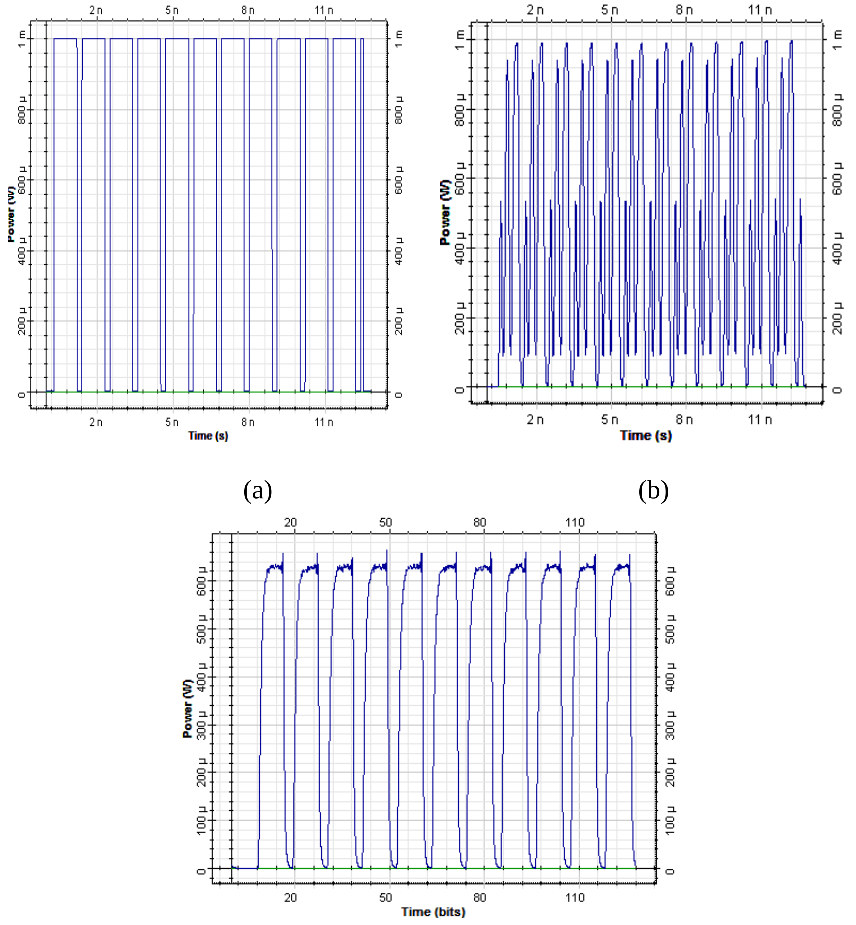
The parameters of SOA to act as wavelength converter in mach-zender configuration at the transmitter side are shown in Table 1. At the receiver side, deconversion process has to be performed. At the receiver side to perform deconversion operation the parameters of SOA are different from the parameters of SOA at the transmitter side. At receiver side the pump source is taken at the power of 3 dBm and the pump wavelength is the original wavelength at which data is to be transmitted. Deconversion operation is performed in similar way as wavelength conversion The pump signal and the converted signal are combined in coupler and fed to both arms of mach-zender configuration and then to the SOA where the deconversion process takes place after that the signals are combined again in coupler resultant of which in one arm there are original wavelengths and in another arm there are converted wavelengths and now the converted wavelengths are detected using photo detector and then the data is received.

Table 1. Parameters for wavelength conversion and deconversion

Parameters	Wavelength Conversion	Wavelength Deconversion
Injection current	0.06 A	.001 A
Length	.0007	.0005
Width	$1{\times}10^{-6}$m	$1{\times}10^{-6}$m
Height	$8{\times}10^{-8}$	$8{\times}10^{-8}$
Confinement factor	0.1	0.5
Loss	0 1/m	0 1/m
Differential gain	3m^{2}	$3{\times}\ 10^{-20}\text{m}^{2}$
Carrier density at transparency	$1{\times}10^{20}\text{m}^{3}$	$1{\times}10^{21}\text{m}^{3}$

5. Results and discussion

In this section the results of the system setup shown above of anti-jamming technique for OCDMA network are presented. The input bits over time domain is shown in the Fig. 3(a). Fig. 3(b) shows the received signal when the jammer is disrupting. It is observed that the signal received by the unauthorized user/ jammer is different from the input signal (shown in Fig. 3(a)). The wavelength conversion translates the data from encoder wavelength onto other wavelengths which are out of the jamming window. The received signal using the wavelength converter in the OCDMA network is shown in Fig. 3(c).It is observed that the received signal is same as the user input signal even when the jammer is on. The bit pattern shown in Fig. 3 (c) is same as input pattern transmitted at transmitter side (shown in 3 (a)) but with little distortion due to fiber length.



(a) (b)

(c)

Fig. 3. (a) Input signal. (b) Received signal in the presence of jammer (c). Received signal using wavelength conversion

BER at the receiver for both the systems with and without anti jamming are measured at different jammer powers is shown in the Fig. 4. It is observed that the BER value remains below than 10^{-18}at all the power levels for the proposed anti jamming system. This means the receiver get the acceptable BER to decode the data which is being transmitted even when the jammer power is very high. Therefore, jammer has no effect on OCDMA network when wavelength conversion is used.

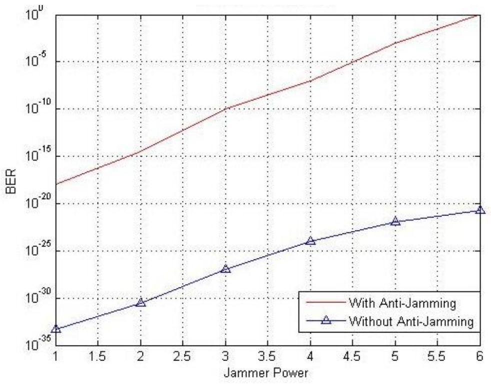
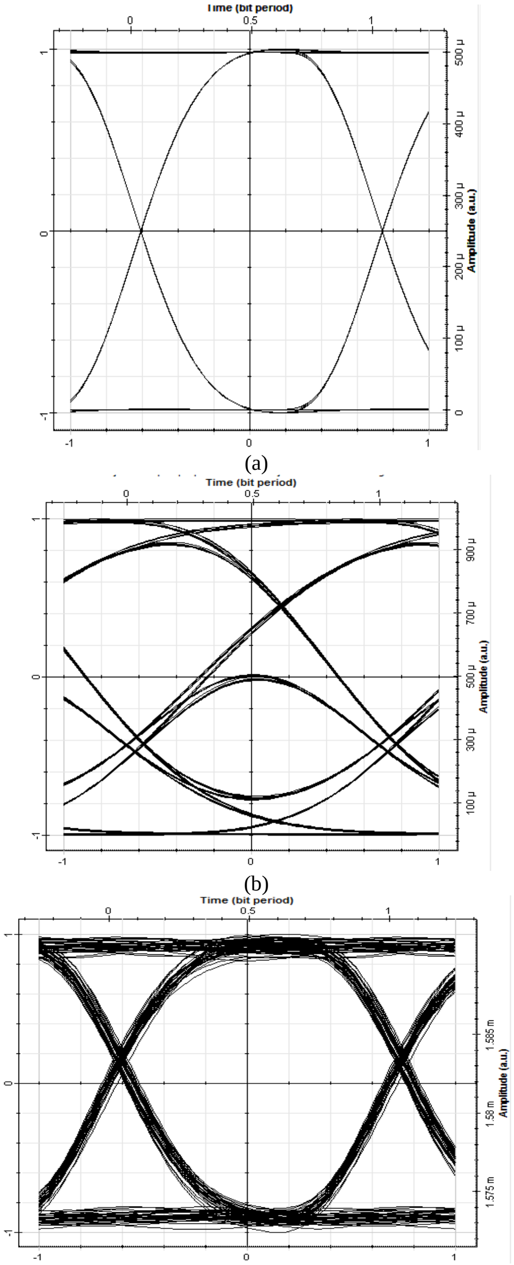


Fig. 4. BER versus jamming power

In a more distinct way, Fig. 5 represents the information about our postulate of security [12]. The security concerns are clearly elaborated with the help of eye diagrams at different stages. The Fig. 5(a) show the eye diagrams at the transmitter end (at 0 km), this is the reason that these diagrams shows large eye opening.



(a)

(b)

(c)

Fig. 5. Eye diagrams at different stages (a) input signal; (b) Received signal when jammer is on with BER 0.98; (c) Received signal using wavelength conversion with $BER\ 10^{-30}$

Fig. 5 (b) shows the eye diagram of the received signal when jammer is on. It can be seen that the received signal is different from the input signal which means jammer is disrupting the communication successfully. In order to mitigate the effect of jammer wavelength conversion is used to translate the data from encoder wavelength onto other wavelengths which are out of the jamming window. The received signal using wavelength converter in the OCDMA is shown in Fig. 5(c)

6. Conclusions

In this paper, the multi-diagonal codes along with anti-jamming technique through the use of a new type of wavelength converter based on semiconductor optical amplifiers in a Mach-Zehnder configuration is investigated. OCDMA signal can be easily jammed with high power jamming signal. The wavelength conversion right after the transmitter negates the jamming attack by moving the user's wavelengths out of jamming window. Hence, the security of spectrally encoded OCDMA system based on wavelength conversion technique has been enhanced. The MD format enhances the security compared to others a code against the vulnerability to eavesdropping. It is shown that the proposed system has improved capability of anti-jamming even at high jamming powers. After having good results, the proposed setup is recommend for information security in all-optical networks with large number of users.

References

[1] W. Zhexing, D. Yanhua, P. R. Prucnal, IEEE Transactions on Information Forensics and Security **6**, 725 (2011).

[2] V. Jyoti, R. S. Kaler, Optical Fiber Technology **19,** 259 (2013).

[3] T. Durhuuseral, IEEE Photonics Technology Letters **29**, 184 (1992).

[4] T. Durhuus, C. Joergensen, B. Mikkelsen, R. J. S. Pedersen, K. E. Stubkjaer, IEEE Photonics Technology Letters **6**, 53 (1994).

[5] M. Schillinger, IEEE Photonic Technol. **3**, 1054 (1991).

[6] S. Singh, R. Kaur, R. S. Kaler, Optical Engineering **53**(1-8), 116102 (2014).

[7] T. H. Shake, Journal of Lightwave Technology **23**, 655 (2005).

[8] T. H. Abd, S. A. Aljunid, H. A. Fadhil, R. A. Ahmad, N. M. Saad, Optical Fiber Technology **17**, 273 (2011).

[9] S. Singh, R. S. Kaler, IEEE Photonics Technology Letters **26**, 173 (2014).

[10] S. Singh, R. Kaur, R. S. Kaler, Optical Engineering **54**(1-4), 016104 (2015).

[11] S. Singh, A. Singh, R. S. Kaler, Optik-International Journal of Light and Electron Optics **124**, 95 (2013).

[12] S. Singh, R. Kaur, A. Singh, R. S. Kaler, Optical Fiber Technology **84**, 22 (2015).

[*] Corresponding author: simrankatron@gmail.com