Security Enhancement in Optical Code Division Multiple Access Network

A Thesis
submitted in partial fulfillment of the requirement for the award of the degree of

Doctor of Philosophy

Submitted by

VISHAV JYOTI
Regd. No. 900906001

Under the guidance of

Dr. R. S. Kaler
Senior Professor

Department of Electronics & Communication Engineering
Thapar University,
Patiala-147004, Punjab, India
July 2014

Certificate

This is to certify that the thesis entitled "**Security Enhancement in Optical Code Division Multiple Access Network**" being submitted by Ms. Vishav Jyoti, to the Department of Electronics and Communication Engineering, Thapar University, Patiala, Punjab for the award of Doctor of Philosophy in Electronics and Communication engineering is a bonafide research work carried out by her under the supervision and guidance of the undersigned. The matter presented in this thesis has not been submitted in any other University or Institute for the award of any degree.

Dr. R. S. Kaler
Senior Professor
ECED, Thapar University
Patiala, Punjab, India.

Abstract

Optical code division multiple access (OCDMA) technology has become a promising technology to implement all-optical communication for transporting high-volume, high-quality multipurpose information reliably with fully asynchronous access and simplified decentralized network control. Due to its coded nature OCDMA is considered to be relatively secure as compared to other optical networks, but a deeper study of OCDMA has revealed that it is easy to intercept and jam the data. Hence, the photonic layer security has become a crucial issue in OCDMA networks. The physical layer of the network can be attacked by an eavesdropper to intercept the data and by the jammer to disrupt communication. Therefore, the main focus of this thesis is to increase optical layer security in OCDMA network by providing data confidentiality against eavesdropping and signal availability against jamming.

Firstly, the security issue of confidentiality enhancement against eavesdropping in an OCDMA network is addressed. An eavesdropper can effortlessly intercept the transmitted data whenever he gets isolated user's signal access. Hence, eavesdropper's code interception performance for single transmitting user in OCDMA network is evaluated first. A novel technique called virtual user scheme is proposed to increase the security against the unauthorized access. It is shown that the information is successfully transmitted without compromising its confidentiality with the proposed scheme.

Secondly, security concern of signal availability against jamming in an OCDMA network is taken into account. A high power jammer can easily disrupt the OCDMA transmission by transmitting at the same waveband as of the authorized user. Therefore, a novel anti-jamming technique using wavelength conversion principle is proposed to mitigate the effect of jammer. An OCDMA network is simulated with proposed wavelength converter and it is shown that data can be securely transmitted even in the presence of high power jammer.

Lastly, the proposed security techniques against eavesdropping and jamming are validated in order to evaluate their effectiveness. The validation of novel virtual user scheme is done using mathematical analysis. The minimum increase in the probability of false detection of data at eavesdropper with the use of proposed scheme is analyzed with different OCDMA modulation schemes. It is validated that the novel virtual user scheme increases immunity against eavesdropping. Additionally, the validation of proposed wavelength converter technique for anti-

jamming is done by simulating it on multiple softwares. The OCDMA system with anti-jamming scheme is simulated with different types of codes. It is shown that use of wavelength conversion technique increases the signal availability by providing the resistance to jamming attack.

Hence, information security of an OCDMA system is improved significantly using the virtual user scheme and wavelength converter technique.

List of Publications

1. Vishav Jyoti and R. S. Kaler, "Novel anti-jamming technique for OCDMA network through FWM in SOA based wavelength converter", Optical Fiber Technology (Elsevier), Vol. 19, No. 3, pp. 259–263, March 2013. (SCI indexed, IF=1.187)

2. Vishav Jyoti and R. S. Kaler, "Isolated User Security Enhancement in Optical Code Division Multiple Access Network against Eavesdropping", Optical Engineering (SPIE), Vol. 51, No. 9, pp. 090501(1-3), September 2012. (SCI indexed, IF=0.88)

3. Vishav Jyoti and R. S. Kaler, "Simulation analysis of security performance of DPSK-OCDMA network via virtual user scheme", Maejo International Journal of Science and Technology, Vol. 6, No. 02, pp. 238-248, July 2012. (SCI indexed, IF=0.456)

4. Vishav Jyoti and R. S. Kaler, "A novel virtual user scheme to increase data confidentiality against eavesdropping in OCDMA network", Chinese Optics Letters (OSA), Vol. 09, No. 12, pp.120602, December 2011. (SCI indexed, IF=0.968)

5. Vishav Jyoti and R. S. Kaler, "Design and implementation of 2-dimensional wavelength/time codes for OCDMA", Optik - International Journal for Light and Electron Optics (Elsevier), Vol. 122, No. 10, pp. 851-857, May 2011. (SCI indexed, IF=0.524)

6. Vishav Jyoti and R. S. Kaler, "Design and performance analysis of various one dimensional codes using different data formats for OCDMA system", Optik - International Journal for Light and Electron Optics, (Elsevier), Vol. 122, No. 10, pp. 843-850, May 2011. (SCI indexed, IF=0.524)

7. Vishav Jyoti and R. S. Kaler, "Security enhancement of OCDMA system against eavesdropping using code-switching scheme, "Optik - International Journal for Light and Electron Optics (Elsevier), Vol. 122, No. 9, pp. 787–791, May 2011. (SCI indexed, IF=0.524)

Acknowledgement

I would like to use this opportunity to express sincere gratitude to my supervisor, **Dr. R. S. Kaler** for providing me with the research opportunities. His superb guidance and consistent support enabled me to achieve all the goals to complete this research to the best of my ability. Without his help and motivation, I could never have gotten this far.

I would like to thank **Dr. R. K. Khanna**, Professor and Head, ECED, Thapar University for providing encouragement, support and the necessary facilities for the completion of my research work. I would also like to thank my doctoral committee members, **Dr. Sanjay Sharma and Dr. Maninder Singh** for taking time to consider my work. Further, I would like to extend my gratitude to **Dr. V. K. Jain**, Professor, IIT Delhi for his valuable comments and suggestions.

My profound love and appreciation goes to my mother, **Ms. Kamlesh Kumari** who has been the ultimate source of support not only during my studies but also throughout my life. Also, special thanks go to my dearest husband, **Simranjit Singh**, for his continuous encouragement, ever-lasting love and care. I am also very thankful to my family and friends for their direct–indirect help, cooperation, and affection.

Last but not least; I would like to thank the Almighty, who has always guided me to work on the right path of the life.

(Vishav Jyoti)

Table of Contents

List of Figures

List of Tables

List of Acronyms

1-D	One Dimensional
2-D	Two Dimensional
3-D	Three Dimensional
ASE	Amplified Spontaneous Emission
BPF	Band Pass Filter
BER	Bit Error Rate
Bi-NLF	Bismuth Non Linear Fiber
CDMA	Code Division Multiple Access
CSK	Code Shift Keying
Demux	De-multiplexer
DPSK	Differential Phase Shift Keying
EDFA	Erbium Doped Fiber Amplifier
FTTH	Fiber to the Home
FWM	Four Wave Mixing
Gbps	Gigabits per Second
IFC	Intelligent Feedback Control
LAN	Local Area Network
MAI	Multiple Access Interference
MZI	Mach Zehnder interferometer
Mux	Multiplexer
MAC	Media Access Control
NRZ	Non Return to Zero

OCDMA	Optical Code Division Multiple Access
OCF	Optical Confinement Factor
OOC	Optical Orthogonal Codes
OOK	On-Off Keying
OSI	Open System Interconnections
PRBS	Pseudo Random Bit Sequence
PPLN	Periodically Poled Lithium Niobate
Pol	Polarization
PSK	Phase Shift Keying
PSO	Pseudo Orthogonal
SBR	Signal to Background Ratio
SNR	Signal to Noise Ratio
SOA	Semiconductor Optical Amplifier
TDMA	Time Division Multiple Access
VUS	Virtual User Scheme
WDM	Wavelength Division Multiplexing
WDMA	Wavelength Division Multiple Access
WHTS	Wavelength Hopping Time Spreading
W/T	Wavelength/time
XOR	Exclusive-OR
ZCC	Zero Cross-Correlation

Chapter 1

Introduction

1.1 Introduction

Information technology has had an exponential growth in the modern telecommunication systems. The phenomenal growth in the internet traffic has increased the bandwidth demand on the telecommunication industry. As the demand for data bandwidth rises steadily, the move to optical networking is the focus of new technologies, because of fiber optic technology's immense potential bandwidth [1]. Optical communication has huge transporting capacity of carrying hundreds of gigabits per second (Gbps) over thousands of kilometers, in a more reliable, secure and efficient manner as compared to radiofrequency systems. Optical fiber communication has made the twenty first century an era of barrier free communication.

Fiber-optic communication systems have revolutionized the telecommunications industry and played a major role in the advent of the information age. Today's telecommunication networks have widely adopted optical fiber as the backbone transmission medium. Fiber-optic communication is a method of transmitting information from one place to another using light as the carrier and optical fiber as the transmission media. The main advantages of optical fiber communications are high speed, low loss, no crosstalk, large bandwidth capacity and high reliability by the use of broadband of the optical fiber [2, 3].

Therefore, the move to optical networking seems to be the only solution to cater the increased demand for bandwidth. An enormous growth in internet leads to an increased data transmission rate demand in fiber-optical networks. Scaling capacity further will require much more efficient use of available fiber spectrum. To satisfy the bandwidth demand on future information networks, the huge bandwidth of optical fiber communication system can be exploited to its maximum via multiplexing low rate data streams onto the optical fiber. A multiple access scheme is required for multiplexing and demultiplexing traffic on a shared physical medium [4]. It is an idea of allowing several users to transmit data simultaneously over a communication channel. There are several techniques to provide multiple access like time division multiple access (TDMA) where each user is allocated a specific time slot, wavelength division multiple

access (WDMA) where each user is allocated a specific wavelength (frequency) slot and code division multiple access (CDMA) where each user is allocated a unique code [5, 6].

CDMA is the method for transmitting the signals simultaneously over a shared portion of the spectrum. This channel access technology utilizes spread-spectrum technology and coding scheme to allow multiple users to be multiplexed over the same physical channel. It uses unique spreading codes to spread the baseband data before transmission [6]. The signal is transmitted in a channel, which is below the noise level. The receiver then uses a correlator to despread the wanted signal, which is passed through a narrow bandpass filter. Unwanted signals are not despread and will not pass through the filter. Codes take the form of a carefully designed one/zero sequence and are produced at a much higher rate than that of the baseband data [7].

In a world of finite spectrum resources, CDMA made it possible to increase the number of users to share the available bandwidth at the same time. The additional bandwidth required by spread spectrum can be accommodated by using a fiber-optic channel [8]. To take the full advantage of both of the technologies, CDMA and optical fiber communication, one of the basic concepts is the idea of allowing several users to transmit data simultaneously over the optical fiber communication channel by simultaneously allocating the available bandwidth to each user [9]. This is called optical code division multiple access (OCDMA).

1.2 OCDMA System: A Review

1.2.1 Introduction to OCDMA

OCDMA is a multiplexing and multiple access technology for future optical networks which supports multiple simultaneous transmissions in the same timeslot and over the same frequency band using a unique code in optical domain [10]. Every user has access to the entire spectrum all the time. A typical OCDMA network with N pairs of transmitters and receivers is shown in figure 1.1. Each transmitter consists of a data source and a laser that converts the signal from electrical form to an optical pulse by using a modulator, followed by an optical encoder which maps each bit into a very high rate (code length * data rate) optical sequence [11]. As the name implies, OCDMA assigns unique codes to each user to differentiate it from other users in the same spectrum [12]. The encoded optical signals from all active users are broadcasted in the

network by a star coupler. At the receiver end, first the reverse decoding operation is done followed by an optical correlator to extract the information being transmitted.

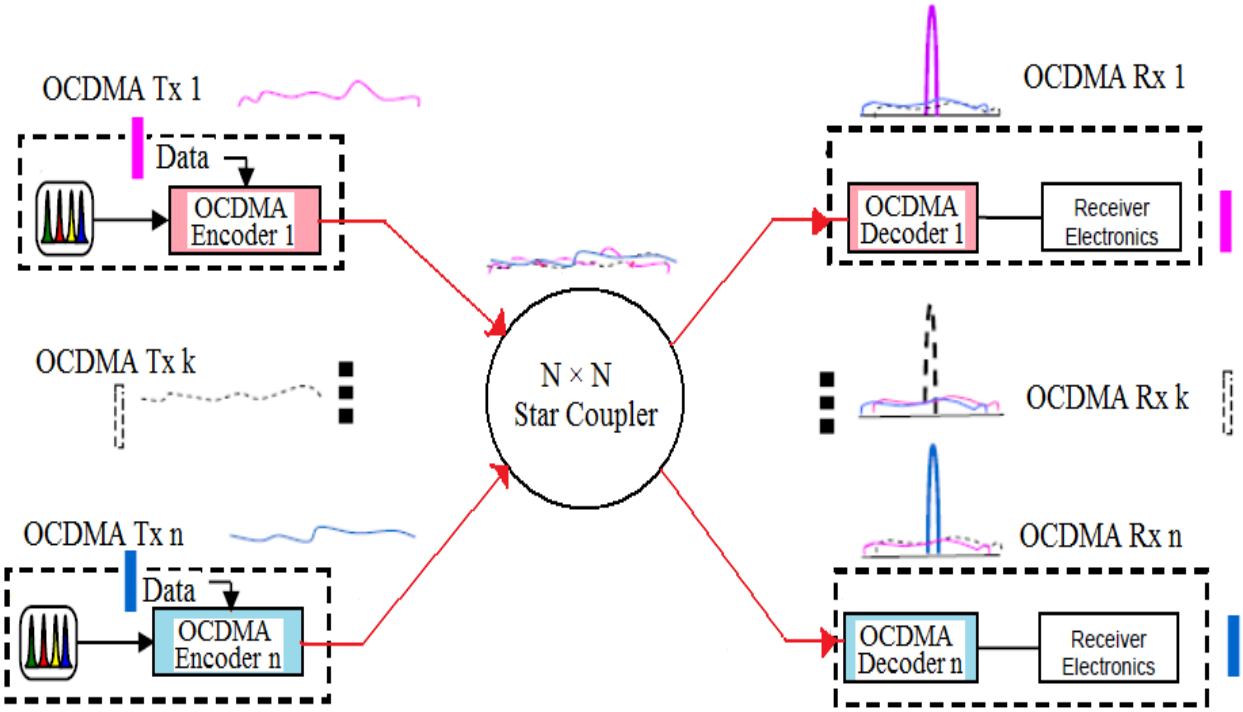


Figure 1.1: OCDMA network

Optical CDMA systems can be further classified into two broad categories, i.e. incoherent and coherent schemes, based on the way, a particular user's code is applied to the optical signal. In coherent OCDMA, phase coding of optical signal field is done to apply an optical code, while amplitude modulated codes are used for encoding in incoherent OCMDA [13]. Coherent OCDMA can support more number of simultaneous users due to its less sensitivity to interference caused by other active users as compared to incoherent OCDMA. Moreover, the system is more complex for coherent scheme and it allows the use of bipolar codes while incoherent scheme allows the use of unipolar codes [14].

1.2.2 OCDMA Coding

In an OCDMA system, each user is assigned a unique codeword. Each data bit is encoded using the codeword which consists of number of smaller bits called chips. When data bit "one" is transmitted, a codeword is present hence, light is transmitted. However when the data bit "zero"

is sent then a number of zeros equal to the length of the codeword are transmitted representing no light pulses [15].

The encoded data of each user, transmitted on the optical fiber are then added together chip by chip. This is called superposition and which has the following properties.

0 + 1 = 1 + 0 = 1 + 1 = 1 (where 1 means presence of light pulse)

0 + 0 = 0 (where 0 means no light pulse)

The decoder at the receiver side consists of optical correlator which continuously observes the superposition of all incoming pulse transmissions and recovers the data from the corresponding transmitter by correlating the incoming signal with the codeword given to receiver. The correlator will give a peak if the incoming stream of optical pulses contains the unique sequence and the presence of other users will be considered as noise.

1.2.2.1 Optical Code

Optical codes take the form of a carefully designed sequence of 0's and 1's produced at a much higher rate than that of the baseband data. The rate of a spreading code is referred to as chip rate rather than bit rate. An (n, w, λ_a, λ_c) optical orthogonal code C is a set of (0, 1) sequences of length 'n' and weight 'w' (the number of ones in every codeword) [16].

The codes employed in any OCDMA system should have the following desirable properties to satisfy the code orthogonality condition [17, 18, 19].

1) ***Auto-Correlation Property***

$$\sum_{t=0}^{n-1} x_t \, x_{t+\tau} \leq \lambda_a \qquad (1.1)$$

for any $x \in C$ and any integer τ, $0 < t < n$.

for $\tau = 0$, $\lambda_a = w$

λ_a is the auto-correlation constraint of a sequence in (1.1) and for each sequence it should exhibit the thumbtack shape to enable the effective detection of the desired signal. This means a sequence can be easily distinguished from its time shifted version, if λ_a takes on the minimal value.

2) Cross-Correlation Property

$$\sum_{t=0}^{n-1} x_t \, y_{t+\tau} \leq \lambda_c \qquad (1.2)$$

for any $x \neq y \in C$ and any integer τ.

λ_c is the cross-correlation constraint between two sequences in (1.2) and it should remain low throughout to reduce interference due to other users and channel noise. This means a sequence can be easily distinguished from the other sequence, if λ_c takes on the minimal value.

1.2.2.2 Types of Codes

The various types of codes that have been proposed for OCDMA technologies can be divided into: one-dimensional (1-D) codes, two-dimensional (2-D) codes and three-dimensional (3-D) codes as shown in figure 1.2.

a) One-Dimensional Codes

The one-dimensional codes spread either in time or in frequency according to the way the optical signal is encoded. The coding done in time domain by using very short optical pulses is called temporal OCDMA [20]. Optical delay lines are used to encode the optical signal. On the other hand, coding of the phase or intensity of the spectral content of a broadband optical signal by using phase or amplitude masks is known as spectral OCDMA [21].

b) Two-Dimensional Codes

The two-dimensional codes spread both in time and wavelength simultaneously. Wavelength-hopping time spreading is a 2-D coding approach in which pulses are placed in different chips across the bit period and each chip is on a different wavelength, thus following a wavelength-hopping and time spreading pattern [22, 23]. The 2-D codes can provide more flexibility and greater capacity than 1-D codes [19]. They also provide high cardinality and better spectral efficiency than 1-D codes and are more secure than one dimensional codes [22, 23]. The wavelength-time schemes provide lower probability of interception and offers scalability and flexibility. The probability of interception is

reduced because the pulses of each code sequence are transmitted in different wavelengths, making eavesdropping more difficult. In 2-D codes, all active users share the same wavelength and time domain space, providing a fair division of the bandwidth. It provides truly asynchronous access, which in turn greatly simplifies network control and management.

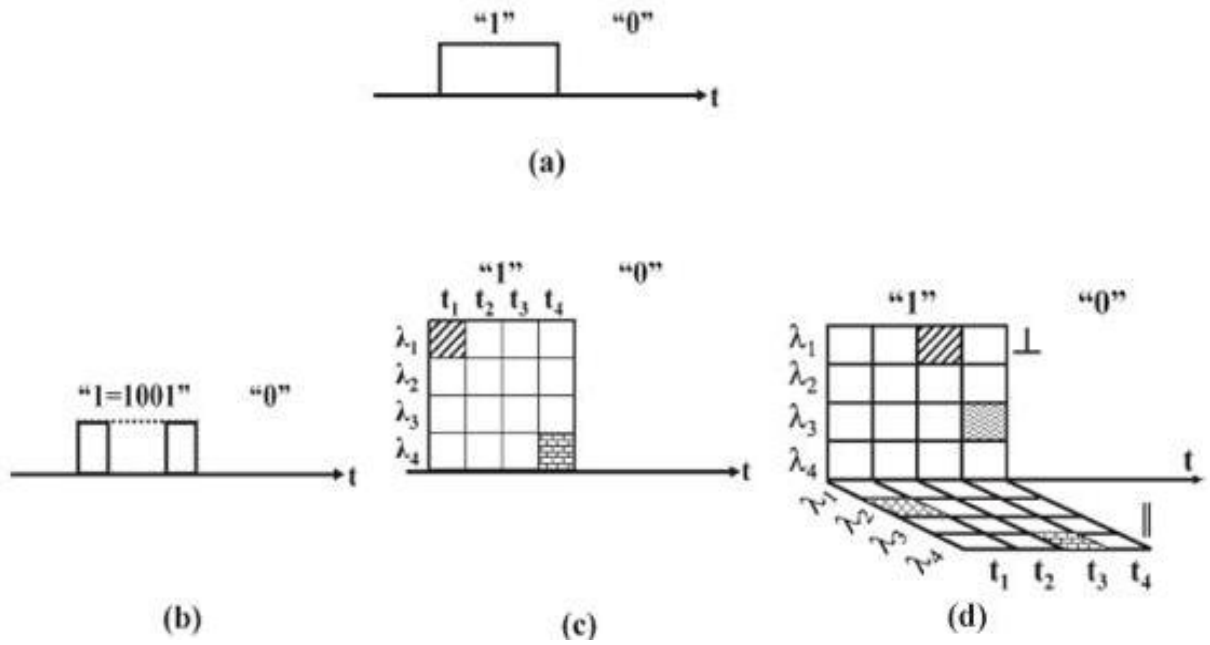


Figure 1.2: Representation of bits in 1-D, 2-D and 3-D codes [27]

(a) Standard set of non return to zero (NRZ) data bits.

(b) 1-D (time domain) OCDMA representation of those bits shown in (a).

(c) 2-D (time, wavelength) representation of those bits shown in (a).

(d) 3-D (time, wavelength, polarization) representation of those bits shown in (a)

c) Three-Dimensional Codes

3-D optical codes are the simple extension of the 2-D optical codes, in which the optical pulses are spread in three dimensions time, wavelength and space/polarization [24, 25, 26, 27]. To take the advantage of the fact that light can be transmitted on two orthogonal polarization states, polarization can be used as the third degree of freedom when generating OCDMA user codes. Such a three-dimensional user code uses the two polarization states along with chip times and discrete wavelengths to uniquely identify

users such that each code is sufficiently orthogonal for high auto-correlation and low cross-correlation [26]. This technique of polarization coding can significantly increase the number of potential users in a system, under the condition that the polarization states do not overly couple [27]. These codes have shown improved performance as compared to the previously proposed two-dimensional prime code [25]. 3-D codes decrease the interception probability even further as compared to 1-D and 2-D codes due to the additional dimension.

1.2.3 Advantages and Limitations of OCDMA

OCDMA technology is one of the promising technologies to implement all-optical networks due to its potential for increased bandwidth capacity, fully asynchronous access, simplified and decentralized network control, improved spectral efficiency and robust information security [28, 29]. The large cardinality and flexibility in coding in OCDMA makes it soft limited which means the number of users can be varied according to network demand as opposed to TDMA and WDMA. The new users can be accommodated at the cost of increased bit error rate (BER). All these advantages of OCDMA make it a favorable for dynamic optical networks.

In addition, the main limitation of OCDMA system is multiple access interference (MAI), which affects the BER and the number of concurrent users in the network. It is co-channel interference caused by multiple users transmitting in the same frequency band at the same time, but using different codes [30]. It is the dominant source of BER in an OCDMA system. This is caused due to the asynchronous transmission between the users and the superposition of the transmitting data in the fiber. The asynchronous transmission causes different transmission delay between the active users and the superposition principle causes the overlapping of differently delayed bits of all the transmitting users. When the optical pulses in the codeword overlap, their power will be added, thus, optical pulses from one codeword may be detected by other receivers tuned to other code-words. As a result, a receiver may incorrectly detect the other user's code-words, resulting in packet transmission errors [31]. As the number of simultaneous users increases, the bit error rate degrades because the effect of MAI increases.

1.3 Demand of Secure Fiber Optical Networks

Network security is gaining lots of attention due to the increasing network usage in various personal, commercial and military applications. Optical access networks' security can be easily attacked because of installation of optical fiber cables in the open outside plant [32]. Therefore, it is important to improve security in different layers of the network. When evaluating the security of a communications technique, it is important to define the type of security under consideration. The various classes of security are confidentiality, availability, integration and authentication of the information signal as shown in figure 1.3.

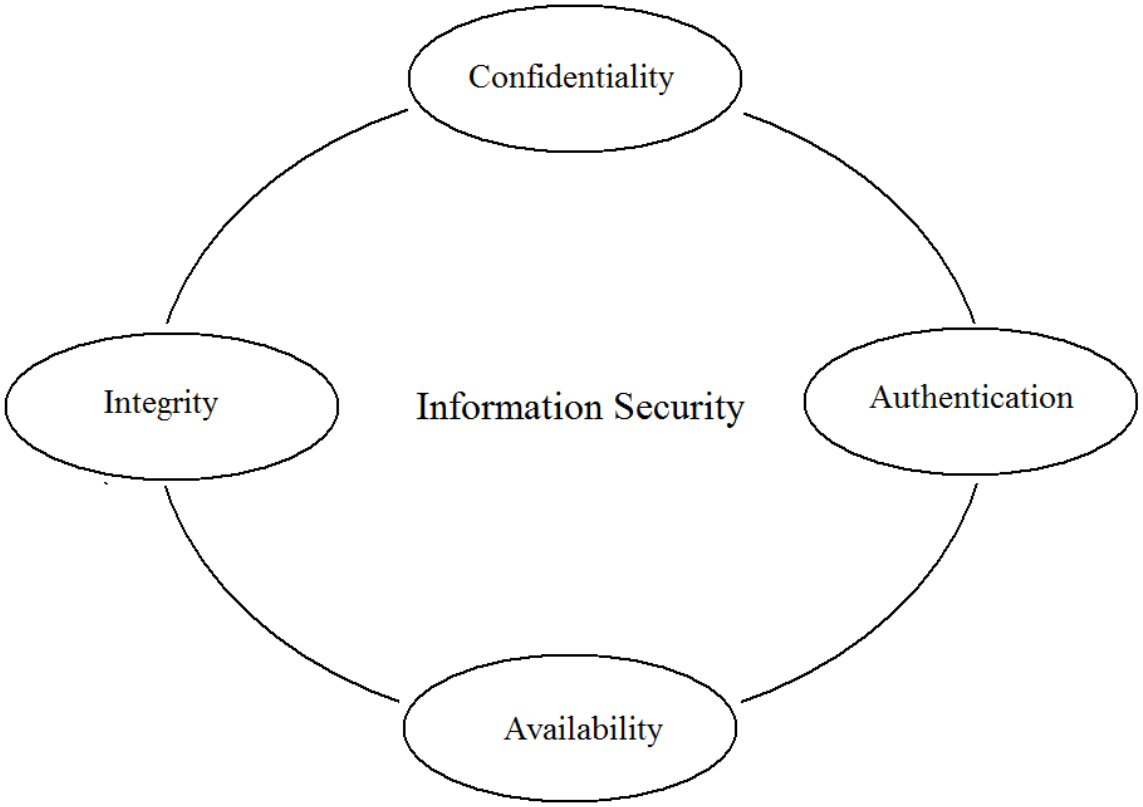


Figure 1.3: Various classes of security

Confidentiality means that the information is not disclosed to any unauthorized access [33]. Availability means that the data transmitted is not destroyed en-route. Integrity means that information is not altered by an unauthorized access while transmission. Authentication allows the receiver to ascertain the identity of the transmitter and vice versa [28].

1.4 Vulnerability of Fiber Optic Communication Systems

Although it was initially thought that the fiber optic systems would be inherently secure, however, optical fiber cables are exposed to physical attacks in customer premises owing to the wide use of fiber-to-the-home systems (FTTH).

It has been discovered that the extraction of information from optical fibers is relatively simple and is aided by the increasing sophistication and availability of inexpensive equipment [34]. By tapping the fiber optic cable, communications can be easily monitored without noticeably altering the signal en-route to the recipient [35]. There are various fiber optic tapping methods, but most fall into the following main categories [36]:

***Splice*:** The simplest method of tapping is by splicing the optical fiber briefly and inserting equipment to allow for the signal to transit to the end party while also being intercepted by the intruder [34].

***Splitter and Coupler*:** An optical splitter 'splits' a single optical signal into two identical signals. However, in order for the device to be installed, the target fiber must be cut and both ends spliced onto the optical splitter [37]. Evanescent coupling utilizes the same process without requiring the target fiber to be cut and field-constructs a 1x2 optical splitter rather than using a pre-manufactured device.

***Non-touching methods*:** One of the lesser-known properties of optical fibers is that, a small fraction of optical signals, often leaks from both the jacket and the cladding of the fiber, particularly if the fiber is bent, or clamped, in such a way that micro-bends or ripples are formed on its surface [38]. The amount of light leakage is small, but detectable with a photon counting detector. The simplest example of such performance is that one is able to see the light in an optical fiber by holding it in the hands. The equipment designed to interpret the light can. Just as simply as one sees the light, so does the equipment designed to interpret it.

Network Disruption: Some tapping devices may be utilized not just for passive tapping, but for active tapping, in which there occurs an injection of signals into the fiber plant for network disruptions and attacks [34]. Such techniques could be used in order to introduce false information or to corrupt existing information flows. Unlike blatant physical attacks on the network infrastructure, such as cutting an optical cable, optical taps used in today's networks for

disruption purposes are subtle in nature, not detectable in real-time, difficult to locate and reap havoc on infrastructure integrity and availability.

1.5 Security Concerns of OCDMA System

The security sensitive data such as military transactions, financial transactions, medical records, intellectual property etc., which is to be securely transmitted, is done through the internet. The physical carrier of the internet is mostly the optical fiber which constitutes high speed, large capacity global optical networks. To protect the internet from security attacks, various security protocols and mechanisms are utilized at different layers of the network stack. The physical layer security in photonic network remains an open area of research as an additional security layer in transmission systems. The physical layer is the lowest layer in the open system interconnections (OSI) model.

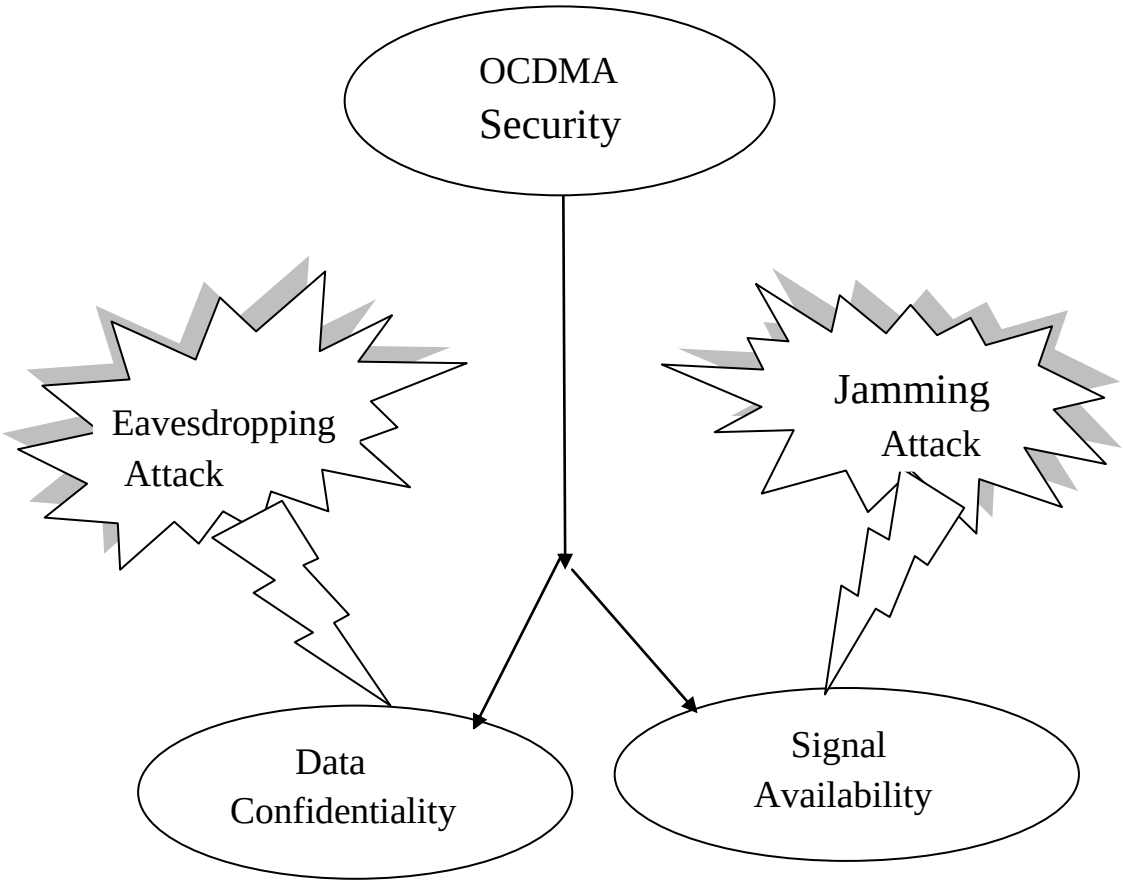


Figure 1.4: Security issues in OCDMA network

Optical code-division multiple access has been considered as a good candidate to provide optical layer security [28]. This is due to the fact that if multiple codes operate simultaneously, it would be nearly impossible to get any meaningful information from the data signal [39]. However, increased sophistication of optical tapping devices placed in public and private optical networks today allow unrestrained access to all communications and information transiting in any fiber segment. The optical layer security tries to protect the transmitted optical signal from unauthorized access, so that the optically encoded binary data will not be intercepted by eavesdroppers and altered by jammers. Hence, the security issues addressed in this thesis are data confidentiality against eavesdropping and signal availability against jamming in OCDMA network as shown in figure 1.4.

1.5.1 Data Confidentiality against Eavesdropping

Confidentiality assures that only the intended receivers of information actually receive information, and nobody else. ***Eavesdropping*** of a signal is a threat to the signal confidentiality, which can be compromised to various degrees. It is an act of secretly listening to a private conversation. It can be done over telephone lines, email, instant messaging and other methods of communication considered private [40]. In the worst case, an interceptor can directly read the information. The knowledge that two particular people are communicating may also compromise confidentiality. Some information is available to potential adversaries only by observing the traffic patterns. The malicious attackers are technologically sophisticated, have significant resources and know a great deal about the signals being transmitted [39].

The goal of eavesdropping is to obtain some confidential information that should be kept hidden during the communication. The confidential information may include the location, public key, private key or even passwords of the nodes. Such data is very important to the security state of the nodes; and it should be kept hidden from unauthorized access. This attack imperils the confidentiality and integrity of the data because the information might be analyzed and modified before being forwarded to the legitimate user [28]. Confidentiality has been one of the major security issues in OCDMA networks because of the ease of eavesdropping despite the optical pulse in OCDMA being encoded into a noise- like signal by the optical encoder according to a unique optical code [41].

1.5.1.1 Types of Eavesdropper

The different types of eavesdroppers are simple energy detector and differential eavesdropper.

a) Simple Energy Detector

It consists of a simple photodetector. It basically detects the energy in a given bit period by acquiring bit interval synchronization from the encoded data. If the energy is present in a particular bit period, the bit“1”is being transmitted otherwise bit“0”is being transmitted. It is also known as simple power detector where it integrates the received power over the entire bit period to find whether or not energy is present in that bit period.

b) Differential eavesdropper

It consists of DPSK demodulator followed by a balanced photodetector as shown in figure 1.5. The DPSK demodulator is a Mach Zehnder interferometer (MZI) with one-bit delay in one arm and the balanced detector consists of two photodetectors followed by the subtractor. At the differential detector, the incoming signal splits into two paths and combined again with one-bit difference between the two paths followed by a balanced photo detector. Differential detection detects the difference between two encoded signals to get the transmitted signal [42]. Hence, the resultant signal is formed according to the different combinations of the consecutive bits.

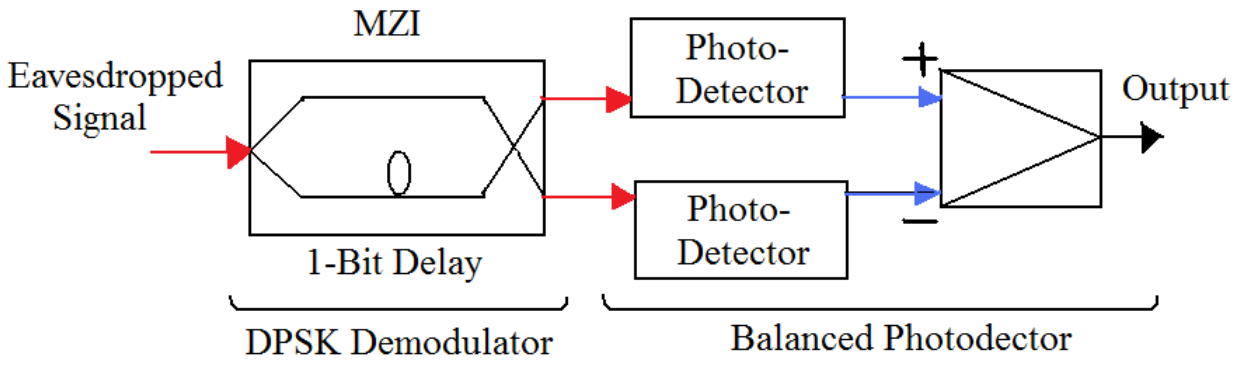


Figure 1.5: Differential eavesdropper

1.5.2 Signal Availability against Jamming

Availability means that a node should maintain its ability to provide all the designed services regardless of its security state [43]. It means that information transmitted is not “lost” or destroyed en-route [28]. Physical infrastructure destruction attacks the availability of signal by destroying the transmission link between transmitter and receiver [44]. Another way that challenges the availability of signal in the network is signal jamming. Both of these attacks can lead to denial-of-service attack.

Jamming signals can degrade the performance of the OCDMA system dramatically in terms of availability of the signal. Jamming is done by injecting an interference signal at the same frequency band or sub-band as the transmitter so that the actual signal is completely over shadowed by interference. The term "jamming" is used to describe the deliberate use of attack signals in an attempt to degrade or disrupt communication whereas; the term "interference" is used to describe unintentional forms of disruption [45]. Unintentional jamming occurs when an operator transmits on a busy frequency without checking that it is in use first, or without being able to hear distant stations on the same frequency. Intentional jamming is the overpowering of authorized network signals with the jammer signals [28]. Jamming signals are a threat to signal availability which can degrade the performance of OCDMA system drastically under certain conditions [46].

Further, a jammer can attack the target node making some of the network services unavailable [47]. It is important to notice that transmission can never be jammed - jamming hinders the reception at the other end.

1.5.2.1 Different Jamming Schemes in OCDMA

The different jamming schemes are pulse jamming and partial band jamming. Both of these are in band jamming attack signals because they have same frequencies as of data signals.

a) Pulse Jamming

Pulse jammer is a high power jammer whose pulses are same as of the OCDMA authorized user’s signal pulses. If the jammer does not have the output power to jam a wide band continuously, it can increase its instantaneous jamming level by pulsed jamming. It sends the high power pulses for a fraction of time but over the entire user’s bandwidth *W*.

The baseband Fourier spectrum of jammer signal is given by (1.3) [46]:

$$A_{PJ}(\omega)=\begin{cases}\sqrt{\dfrac{J_{avg}/\rho}{W}}, & -\dfrac{W}{2}\le\omega\le\dfrac{W}{2}\\ 0, & \text{elsewhere}\end{cases} \tag{1.3}$$

where,

J_{avg} is average power transmitted by the jammer; and ρ is the probability that jammer is on and transmits its pulses.

b) Partial band jammer

As the name suggests, it covers only a part of the user's bandwidth instead of user's entire bandwidth. In partial band jammer, the jamming signal consists of pulses of spectrally flat noise that covers the partial signal bandwidth W_J. The baseband Fourier spectrum of jammer signal is given by (1.4) [46]:

$$A_{PBJ}(\omega)=\begin{cases}\sqrt{\dfrac{J_{avg}}{W_J}}, & -\dfrac{W_J}{2}\le\omega\le\dfrac{W_J}{2}\\ 0, & \text{elsewhere}\end{cases} \tag{1.4}$$

1.6 Research Motivation

The exponential growth in information throughput on the Internet increases the transmission of confidential and commercially sensitive data through optical networks. With this, the potential risk of security of this valuable information also increases as tapping of the optical signal from a fiber could be easily done by using inexpensive equipment. Physical layer security is thus becoming an impelling request in the next generation of optical networks.

OCDMA is a potential technology to eliminate the problem of traffic growth and multiple user access on the internet in optical networks. Enhanced information security is often said to be inherent in OCDMA technology due to its coded nature. If multiple codes operate simultaneously, it is almost impossible for an eavesdropper to get any meaningful information because of multiple access interference (MAI) caused by all the transmitting users and also, it is difficult to jam the noise like OCDMA encoded signal but the literature revealed otherwise.

Recently, studies discovered that OCDMA systems are vulnerable to eavesdropping and jamming attacks. The physical layer of the OCDMA network can be attacked by an eavesdropper to intercept the data and by launching an interferer signal to jam the system. A jamming attack can easily manipulate information being transmitted, if jamming signals have the same frequency band as data signals. In addition, the increase in the number of attacks as well as in diverse methods of the attacks which are becoming more difficult to defend makes information security a crucial issue in OCDMA networks. Hence, our aim is to investigate the security issues in OCDMA network and to provide the solution that defines the objective of our thesis as given below.

1.7 Objectives

Keeping in view the above mentioned aspects, the objectives of research were formulated which are listed as follows:

i. To propose a technique to increase the confidentiality of OCDMA system against eavesdropping.
ii. To propose a technique for security enhancement of OCDMA system in terms of availability of signal against jamming.
iii. To validate the proposed techniques for OCDMA system.

1.8 Organization of Thesis

Based on the proposed objectives, the main aim of this thesis is to enhance the security of OCDMA network. The thesis has been organized into six chapters. The content of each chapter is briefly described below.

The introduction to optical code division multiple access network and its security concerns are covered in chapter 1. The motivation and problem formulation are also presented. The objectives of the thesis are crystallized in this chapter. Further, the organization of the thesis is presented.

Chapter 2 of this dissertation gives a comprehensive literature review of various existing techniques enhancing security of OCDMA system and their limitations.

Chapter 3 deals with the first objective of the thesis which is to propose a technique to increase the confidentiality of OCDMA system against eavesdropping. A novel technique named virtual

user scheme is proposed and implemented to increase the confidentiality of OCDMA network. From eavesdropper's point of view, the easiest way to intercept the information is to tap isolated subscriber signals avoiding multiple access interference automatically. Therefore, the security performance of only a single-user OCDMA system is discussed. The proposed technique is simulated with on-off keying (OOK), code shift keying (CSK) and differential phase shift keying (DPSK). The results obtained for the proposed technique are compared with the conventional schemes already existing in literature. The results show that the virtual user scheme is very effective for enhancing security of OCDMA network against eavesdropping.

Chapter 4 deals with the second objective of the thesis which is to propose a technique for security enhancement of OCDMA system in terms of availability of signal against jamming. The technique proposed to avoid jamming attack is based on the use of wavelength conversion process. Firstly the system model for anti-jamming scheme based on wavelength conversion is proposed and assumptions made are discussed. The proposed technique is implemented and simulated with the OCDMA system. The results obtained for the proposed anti-jamming technique are compared with OCDMA system without any jamming resistance. The results show that the proposed anti-jamming technique is very effective and completely negates the jamming attack by moving the user's wavelengths out of jamming window. Hence, the OCDMA system with the proposed technique has improved capability of jamming resistance.

Chapter 5 deals with the third objective of the thesis which is to validate the above proposed techniques for OCDMA system. The simulation of the newly proposed techniques is done in chapter 3 and chapter 4. In this chapter, the proposed virtual user for confidentiality enhancement is mathematical analyzed. The analyses show that confidentiality of the system is effectively increased. Further, the proposed anti-jamming technique is validated using the other software. Similar results are obtained for the proposed anti-jamming technique using both the software.

Finally, chapter 6 covers the summary/conclusions drawn; recommendations on the basis of results obtained in chapters three to five and the scope of future work has been presented.

Chapter 2

Literature Review

In this chapter, we present a comprehensive literature review of optical code division multiple access network and its security concerns as discussed in chapter 1. In section 2.1, we step back to provide a brief overview of the previous developments in OCDMA. In section 2.2, various OCDMA security strategies against eavesdropping are studied and discussed. Further, in section 2.3, different security schemes for OCDMA against jamming are studied.

2.1 Evolution of OCDMA

The history of Optical Code Division Multiple Access dates back to the 1970s. But, the paper by Prucnal, Santoro, and Fan in 1986 is considered to be the foundation of OCDMA because they showed that pseudo-orthogonal codes can be implemented as tapped delay lines based on optical fibers. Prucnal et al. [8] showed the wide bandwidth channel required by CDMA for asynchronous access to a local area network (LAN) can be provided by fiber optic channel. Further, fiber optic spread spectrum CDMA is proposed and demonstrated with newly designed CDMA sequences and its performance is compared with the conventional CDMA. It was shown that the capacity of CDMA LAN can be increased using all optical processing.

Second important publication was by Weiner, Heritage, and Salehi in 1988 which is also regarded as foundation of most developments in OCDMA. Weiner et al. [9] demonstrated the frequency domain manipulation of coherent ultrashort light pulses. It was found that the developments of radio frequency communications can be applied to optical communication.

In 1989, the concept optical orthogonal codes with desired auto-correlation and cross-correlation properties were introduced. Jawed A. Salehi [17] introduced optical orthogonal codes for OCDMA. He reported the desirable auto-correlation and cross-correlation properties for the codes used. Further, introduced the optical disk patterns to represent the optical orthogonal codes (OOC's) and to derive the probability density functions of any two interfering users.

Chung et al. [18] introduced the optical orthogonal codes and addressed their application in the communication area. The upper and lower bounds on the maximum size of OOC's were derived. It was shown that the use of optical orthogonal codes enables a large number of asynchronous users to transmit data effectively.

Salehi and Brackett [19] derived the BER of OCDMA system with OOC's as a function of data rate, code length, code weight, number of users, and receiver threshold. Further, the use of optical hard limiter to reduce the multiple access interference was introduced. It was shown that the OCDMA system with optical hard limiter has improved system performance as compared to conventional OCDMA in terms of number of users that can be accommodated.

Further, to enhance OCDMA network performance, coding in different dimensions simultaneously was introduced.

Bin Ni et al. [20] studied the effect of the coherence time of light sources on the performance of an incoherent temporal-spreading optical-code-division multiple-access system. Broadband noise-like light sources, such as amplified spontaneous emission sources, were used by the transmitters. Three different kinds of receiver structures were examined and compared. Results showed the impact of the non ideal light sources on the system performances relative to the ideal case. Analysis showed that to achieve the best performance when the available optical bandwidth and data rate are fixed, there is an optimal range for the spreading code length.

E. Inaty et al. [21] presented a bit rate flexible optical fast frequency hopping CDMA system architecture using a sequence of fiber Bragg gratings (FBGs). The bit rate of the system was limited by time spacing, the chip duration, and the number of gratings. Also, a power control algorithm was proposed for multimedia multirate applications. Further, it was shown that power control can increase system performance considerably.

K. Yu et al. [22] proposed a two-dimensional code family and transmitter/receiver structures for incoherent multi-wavelength- time spread optical CDMA networks in which the coder/decoder structures uses wavelength multiplexer and mirrored fiber delay lines in fold-back configuration as a frequency-time domain spreading device. It was shown experimentally that the proposed

code family and encoding/decoding devices can be used successfully in secure high-speed local area network.

Antonio J. Mendez et al. [23] presented a technique for generating PSO matrices from sets of optimum Golomb rulers. It was shown that 2-D codes have higher cardinality and good spectral efficiency than that of the generating sequences. Further, it was shown that the matrices can be implemented as space/time or wavelength/time matrix codes for OCDMA applications.

Sangin kim et al. [25] constructed a new family of space/wavelength/time spread 3-D optical orthogonal codes by extending the 2-D prime codes, and 3-D codes have shown the performance improvement as compared to 2-D prime codes. Further, suggested the wavelength^2/time scheme using arrayed waveguide grating to implement three dimensional codes in order to eliminate the requirement of fiber ribbons and multiple star couplers.

J. E. McGeehan et al. [26] experimentally demonstrated a three dimensional OCDMA system to encode data in time, wavelength, and polarization. The light can be transmitted on two orthogonal polarization states was taken as an advantage and further shown that it can be used as third dimension to generate OCDMA user codes. It was found that the sample codeset can support >2x the users of a 2-D codeset.

J. E. McGeehan et al. [27] demonstrated a 3-D OCDMA system that uses time, wavelength, and polarization as degrees of freedom within the code set which may be ideal for use in short distance optical local area networks, where polarization states remain fairly stable.

In the end, some general research papers published on OCDMA are also reviewed which further helped us in understanding the different OCDMA technologies.

A Stok and E. H. Sargent [10] proposed OCDMA to achieve asynchronous and high speed in local area network. It was shown that OCDMA is more flexible with simple protocols and decentralized network control which make it better than TDMA and WDMA. Kerim Fouli and Martin Maier [11] gave the overview of optical coding dimensions and encoding techniques. Further, discussed was its application as OCDMA passive optical network. Nikos Karafolas [13] reviewed various OCDMA schemes based on encoding and decoding techniques.

In the previous section, the basics of OCDMA are presented where all the authors consider OCDMA to be an inherently secure communication technique due to its coded nature. Hence, the various security aspects of OCDMA are discussed in the following sections.

2.2 Security against Eavesdropping

Enhanced security has been told as one of the important advantage of OCDMA technology but the vulnerability of OCDMA network at physical layer is discussed in various literatures. Shake in 2005 has shown the arguments favoring OCDMA as potential technology for secure communication are ambiguous. It is found that it is very easy to breach the OCDMA security based on only the coded nature of technology.

T. H. Shake [39] examined different types of security that should be provided by OCDMA. He quantitatively analyzed data confidentiality and also presented different eavesdropping strategies. The probability of successful data interception was calculated as a function of several parameters, including signal-to-noise ratio and fraction of total available system capacity. It was shown that an intelligently encoded O-CDMA signal and rapid reconfiguration of codes can make the interception more difficult.

Confidentiality has been one of the major issues in OCDMA networks because of the ease of eavesdropping despite the optical pulse in OCDMA being encoded into a noise like signal by the optical encoder according to a unique optical code [42]. The research done on the security shows that the confidentiality of an OCDMA network can be easily compromised whenever an eavesdropper gets isolated user access [39, 40]. An eavesdropper in an OCDMA network can isolate a single user's signal at various locations within the network [48]. One way to isolate an individual user's signal is to put a tap before the multiplexer, i.e., the signal is tapped out even before it gets multiplexed with the multiple user signals. The network confidentiality is also pretty susceptible when only one user is transmitting and all the other users are sitting idle in the same time period.

T. H. Shake [40] presented a theoretical analysis of confidentiality that can be provided by spectral-phase-encoded OCDMA. Further, he presented two eavesdropping detectors. It was

shown that the authorized user was vulnerable to an eavesdropper whenever the latter can isolate a single user signal.

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 for data modulation 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". The code interceptor can easily read the data bits by simply integrating energy over the bit period [49]. In this case, there is no need for the eavesdropper to "break" the coding scheme; the energy detector output contains the user's data stream. It is found that an isolated OCDMA user with on-off keying data modulation format does not have any security of information transmission and is highly vulnerable to relatively simple eavesdropping techniques [50]. A new modulation format is proposed where a constant amount of energy is sent for each transmitted bit by transmitting a code sequence for a "one" and a different code sequence for a "zero" [49, 51, 52, 53].

D.E. Leaird et al. [50] demonstrated that the code switching data modulation format for spectrally phase coded OCDMA. It was shown that modulation format based upon switching between two codes increases confidentiality of OCDMA system as compared to OOK-OCDMA. It was demonstrated that code switching eliminates the vulnerability to eavesdropping based on a simple energy detector.

Xu Wang et al. [51] proposed coherent CSK-OCDMA with balanced detection. It was theoretically investigated that the proposed system has enhanced security and simpler threshold settings as compared to conventional OCDMA systems.

Hwan Seok Chung et al. [52] proposed spectrally encoded OCDMA using bipolar codes. It was shown that the proposed scheme increases security against eavesdropping while maintaining an error free operation at receiver. Further, Hwan Seok Chung et al. [53] experimentally demonstrated the security-improved OCDMA with bipolar coding. It was shown that bipolar coding scheme is more secure than the on-off keying. Furthermore, it was demonstrated that bipolar coding enhances security in physical transmission link.

Similarly, to provide security against a standard power detector, a advanced modulation format i.e. DPSK-OCDMA system was implemented [54]. X. Wang et al. [54] proposed DPSK-OCDMA with DPSK data format. It was demonstrated that DPSK OCDMA has improved security over OOK-OCDMA. Further, the theoretical modeling shows that the proposed system has improved receiver sensitivity, better noise tolerance, no need for optical and dynamic thresholding. It was experimentally shown that the DPSK-OCDMA is a more practical approach compared to OOK-OCDMA.

The vulnerability of an OOK-OCDMA system to a simple energy detector can be avoided by code shift keying and differential phase shift keying, but it is reported in Ref. [42, 55, 56, 57] that the confidentiality of a CSK and DPSK OCDMA can be easily compromised by a differential eavesdropper.

Z. Jiang et al. [55] demonstrated that the security enhanced code switching scheme OCDMA is vulnerable to an eavesdropper. It was shown that the security of code switching scheme can be broken by using a DPSK de-modulator even without knowing the codes used. Additionally, D.E. Leaird et al. [56] also experimentally demonstrated vulnerability of two code keyed OCDMA against DPSK based eavesdropper.

B. Dai [42] proposed the vulnerability of single user CSK-OCDMA to differential detection. The differential eavesdropping of the transmitted information in temporal phase coding CSK-OCDMA was experimentally demonstrated. It was proposed that the differential detection can be used to distinguish the discrepancy in the two encoded signals. It was shown that differential detection helps in distinguishing the two encoded bits because of bit-to-bit comparison.

B. Dai et al. [57] experimentally demonstrated the security vulnerability of the temporal phase coding single-user DPSK-OCDMA and CSK-OCDMA systems. The existence of the eavesdropping vulnerability was observed even without proper decoding. It was analyzed that DPSK eavesdropper can easily detect the data being transmitted for single user CSK and DPSK systems without knowing about the codes used.

Also, confidentiality of data transmission can be increased using phase masking scheme [58]. Fei Xue et al. [58] proposed a 2-code keyed OCDMA system based on time-varying phase-masking

scheme. It was shown that phase masking provides security. Different levels of phase shifts are analyzed and it was shown that a complex phase-mask provides a high level of confidentiality.

Another solution to increase the security against eavesdropping is to transmit chaotic signals using scrambling. Scrambling modifies the content of the original signal by distorting it, to prevent eavesdropping [59]. Valentina Sacchieri et al. [59] proposed scrambling of an OCDMA signal to distort it fully before transmission as a solution to increase confidentiality. It was shown that scrambling an OCDMA signal by using one or more additional encoders in cascade increases security. Further, it was shown that it makes the search space of brute force attack very large.

While other solution in enhancing the data network confidentiality is based on optical signal processing, are optical encryption [60, 61, 62] and optical steganography [63, 64]. Optical encryption allows the signal to be encrypted with low latency. The term steganography denotes secret communication that allows users to hide information. Optical steganography is achieved using spread spectrum to hide the optical transmission underneath the noise and inhibit eavesdropping [59]. It provides an additional layer of security that can supplement data encryption by hiding the existence of data transmission underneath the public channel [63].

Mable P. Fok et al. [60] experimentally demonstrated an all-optical encryption scheme with interleaved waveband-switching modulation using a 35-cm bismuth-oxide nonlinear fiber. It was shown that there is no intensity change between bit 0 and bit 1 using interleaved waveband switching modulation. Therefore, the eavesdropper cannot analyze the encrypted data by temporally monitoring the intensity change of every bit. Further, the wavelength of the encrypted data can be changed by controlling the wavelength of the encryption key. Further, it was shown that ability to change the encrypted signal wavelength provides the anti-jamming capability.

Natalie Kostinski et al. [61] demonstrated the variable two-code keying for encryption and decryption in OCDMA system. The nonlinear optical loop mirror based exclusive-OR (XOR) was used for encryption. It was shown that the variable two-code keying modulation format is random alternation in bit representation. Fiber Bragg grating arrays create wavelength hopping time spreading (WHTS) codes from broadband pulses at output ports of the exclusive-OR which

results in this code-switching modulation format. It was shown that this scheme has immunity to differential analysis.

Zhenxing Wang et al. [62] proposed a novel all-optical exclusive OR encryption architecture for OCDMA transmission system. It was shown that the code swapping based on XOR operation improves the confidentiality of the OCDMA system.

Mable P. Fok et al. [63] experimentally demonstrated optical steganography using a matched pair of chirped fiber Bragg gratings. The stretching and compression of stealth channel pulses were provided by chirped fiber Bragg gratings. The stealth channel was hidden in both the temporal and the spectral domain underneath the public channel.

Paul R. Prucnal et al. [64] implemented optical steganography for data hiding using group velocity dispersion for temporal spreading of a stealth signal. It was demonstrated the use of both WDM and optical CDMA public channels to mask the stealth signal transmission. It was shown that the stealth channel can be successfully hidden in both the time and the frequency domains. Further, shown that this approach can be used to prevent the observation and analysis of traffic patterns in optical networks.

In summary, various researchers have worked on different techniques to provide confidentiality against unauthorized interception of data. The techniques like CSK and DPSK with OCDMA surely increase security against eavesdropping but the access to isolated user signal makes them vulnerable to rather simple eavesdropping detectors. CSK and DPSK provide immunity against standard power detector but isolated user signal access makes the system vulnerable to differential eavesdropping. Therefore, in this thesis, confidentiality of single active OCDMA user against eavesdropping has been taken as one of the objective.

2.3 Security against Jamming Attack

Besides confidentiality against eavesdropping, network availability is also an important issue of concern. It should always be provided because it is simpler to launch an interference signal to jam the system. Jamming is threat to signal availability which can lead to denial of service under certain conditions [65].

Mohammad J. Emadi et al. [65] introduced and modeled three types of jammers which are Pulse Jammer, Partialband Jammer, and Follower Jammer. The effects of these jammers on the performance of the SPE-OCDMA systems that use On-Off keying modulation scheme were mathematically analyzed. It was shown that jamming signals can degrade the performance of the OCDMA system drastically under certain conditions.

To ensure the availability of information, real-time optically processed anti-jamming technique is to hop the signal frequency in a pattern that is unknown to the hostile transmitter; the jammer cannot identify and inject a powerful interfering signal containing the spectral characteristics of the data signal.

Firstly, the ability to change the encrypted signal wavelength provides the anti-jamming capability. The wavelength of the encrypted signal in OCDMA system can be changed by simply controlling the wavelength of the encryption key [60]. Secondly, to provide anti-jamming, code conversion of wavelength is a good solution. One is four wave mixing (FWM) which is used to translate the signal into another waveband [66]. In the presence of optical jamming, FWM can be used to translate the frequency simply by controlling the pump wavelength [67].

Mable P. Fok et al. [66] experimentally demonstrated all-optical encryption and anti-jamming for optical network security in an optical CDMA system. FWM in a 32-cm Bi-NLF for XOR operation of the encryption key and data improves security. The wide FWM conversion bandwidth allows the encrypted OCDMA signal to be transmitted at a different wavelength range, by changing the wavelength of the encryption key to avoid signal jamming.

Mable P. Fok et al. [67] proposed the use of optical processing using compact passive devices for enhancing network security. Optical steganography, anti-jamming, and optical encryption were experimentally demonstrated. It was shown that service availability is also improved during physical using optical CDMA for backup channels.

Another solution proposed for anti-jamming is periodically poled lithium niobate (PPLN) waveguides for code conversion in the wavelength domain [68]. If jamming signals are injected to block the channels of the original codes with the aim of denying service, the codes can still be transmitted after conversion to other available channels.

Zhenxing Wang et al. [68] proposed OCDMA code conversion for security enhancement. Code conversion in wavelength domain using periodically poled $LiNbO_3$ was demonstrated. It was analytically shown that both the confidentiality and availability of the codes are improved by code conversion. It was also shown that in case of jamming to block the channels of original codes, the codes can still be transmitted after conversion to other available channels.

In summary, it can be seen that little work is done on secure communication against jamming in an OCDMA network. Hence, security against jamming is still an open area of research. Moreover, the already proposed techniques for anti-jamming (discussed above) suffer from their own limitations which are discussed in chapter 4. Hence, to propose a novel technique for signal availability against jamming is taken as second objective in this thesis.

2.4 Conclusion

In this chapter, the contribution by various researchers on the developments of OCDMA and its security concerns are described in detail which are summarized in table 2.1. Since the OCDMA technology is relatively new as compared to other optical networks, the research papers giving the introduction and overview of various OCDMA technologies are reviewed. Table 2.1 also summarizes the various eavesdropping and jamming techniques and the solutions proposed to enhance the security against these threats.

Table 2.1: Security concerns of OCDMA network

OCDMA	**Work done**	**Authors, Year**
Foundation of OCDMA	Showed CDMA can be implemented on optical fibers using optical delay lines	Prucnal, Santoro, and Fan [8], 1986
	Demonstrated the frequency domain manipulation of coherent ultra short light pulses to implement CDMA in Optical domain	Weiner, Heritage, and Salehi [9], 1988
OOC and 1-D codes	Introduced optical orthogonal codes for OCDMA and their representation as optical disk patterns	Jawed A. Salehi [17], 1989
	Derived the BER of OCDMA system with OOC's, Introduced optical hard limiter to reduce the MAI	Salehi and Brackett [19], 1989

2-D codes	Proposed 2-D multi-wavelength time spread OCDMA	K. Yu, J. Shin, and N. Park [22], 2000
	Presented a technique for generating 2-D codes from PSO matrices from sets of optimum Golomb rulers	Antonio J. Mendez et al. [23], 2003
3-D codes	Constructed space/wavelength/time 3-D optical orthogonal codes by extending the 2-D prime codes with improved performance.	Sangin kim, Kyungsik Yu, and Namkyoo Park [25], 2000
	Experimentally demonstrated a 3-D OCDMA system to encode data in time, wavelength, and polarization.	J. E. McGeehan et al. [26], 20004
Security Concerns of OCDMA		
Different eavesdropping strategies	Examined security issues in OCDMA and data confidentiality	Thomas H. Shake [39], 2005
	Presented eavesdropping strategies for an isolated single user signal	Thomas H. Shake [40], 2005
To increase confidentiality against simple energy eavesdropping	Demonstrated the code switching data modulation format for spectrally phase coded OCDMA	D. E. Leaird, Z. Jiang, and A. M.Weiner [50], 2005
	Proposed coherent CSK-OCDMA with balanced detection	X. Wang, N. Wada, T. Miyazaki, G. Cincotti, and K. Kitayama [51] 2007
	Proposed spectrally encoded OCDMA using bipolar codes	Hwan Seok Chung, Sun Hyok Chang, Bong Kyu Kim, and Kwangjoon Kim [52], 2007
	Experimental demonstrated the security-improved OCDMA with bipolar coding	HwanSeok Chung, Sun Hyok Chang, BongKyu Kim, and Kwangjoon Kim [53], 2008
	Proposed DPSK-OCDMA for improved performance than OOK-OCDMA	X. Wang, N. Wada, T. Miyazaki and K. Kitayama [54], 2006
Vulnerability of CSK and DPSK OCDMA	Experimentally demonstrated the security vulnerability of the temporal phase coding single-user DPSK-OCDMA and CSK-OCDMA systems.	B. Dai, Z. Gao, X. Wang, N. Kataoka and N. Wada [57], 2010

Vulnerability to differential eavesdropping	Demonstrated that security of code switching scheme OCDMA can be broken by DPSK demodulator.	Z. Jiang, D.E. Leaird, A.M. Weiner, [55], 2006
	Experimentally demonstrated vulnerability of two code keyed OCDMA against DPSK based eavesdropper	D.E. Leaird, C.-B. Huang, Z. Jiang1, S.-G. Park2, A.M. Weiner [56], 2008
	Proposed the vulnerability of single user CSK-OCDMA to differential detection	B. Dai, Z. Gao, X. Wang, N. Kataoka and N. Wada [42], 2010
Other methods of security against eavesdropping	Proposed a 2-code keyed OCDMA system based on time-varying phase-masking scheme	Fei Xue, Yixue Du, S.J. Ben Yoo, Zhi Ding, [58], 2006
	Proposed scrambling of an OCDMA signal to distort it fully before transmission as a solution to increase confidentiality	Valentina Sacchieri, Pedro Teixeira, Antonio Teixeira, Gabriella Cincotti [59], 2008
	Experimentally demonstrated an all-optical encryption scheme with interleaved waveband-switching modulation	Mable P. Fok and Paul R. Prucnal [60], 2009.
	Demonstrated the variable two-code keying for encryption and decryption in OCDMA system.	Natalie Kostinski, Konstantin Kravtsov, and Paul R. Prucnal [61], 2008
	Proposed a novel all-optical exclusive OR encryption architecture for OCDMA transmission system	Zhenxing Wang, Yue-Kai Huang, Yanhua Deng, John Chang, and Paul R. Prucnal [62], 2009
	Experimentally demonstrated optical steganography using a matched pair of chirped fiber Bragg gratings.	Mable P. Fok and Paul R. Prucnal, [63] 2009
	Implemented optical steganography for data hiding using group velocity dispersion	Paul R. Prucnal, Mable P. Fok, Konstantin Kravtsov, and Zhenxing Wang [64], 2009
Different Jammers for OCDMA	Introduced and modeled three types of jammers which are Pulse Jammer, Partialband Jammer, and Follower Jammer	Mohammad J. Emadi , and Jawad A. Salehi [46], 2009

Security against jamming	Experimentally demonstrated all-optical encryption and anti-jamming using four wave mixing in Bi-NLF	Mable P. Fok and Paul R. Prucnal, [66], 2008
	Proposed the use of optical processing using compact passive devices for enhancing network security	Mable P. Fok, Yanhua Deng, and Paul R. Prucnal [67], 2009
	Proposed OCDMA code conversion for security enhancement using periodically poled $LiNbO_3$	Zhenxing Wang, Aref Chowdhury, and Paul R. Prucnal [68], 2009

Based on the findings in the literature, it is evident that OCDMA technology is not as secure as it was initially perceived to be. Hence, information security is an important issue to be addressed in an OCDMA network. The first two objectives of this dissertation are therefore dedicated to the proposal of novel techniques for improving security against eavesdropping and jamming.

Chapter 3
Confidentiality Enhancement of OCDMA System against Eavesdropping

This chapter deals with the first objective of the research work which is to propose a technique to increase the confidentiality of OCDMA system against eavesdropping.

3.1 Introduction

As discussed in chapter 1, confidentiality assures that the information transmitted is not disclosed to an unintended receiver by any means. However, confidentiality can be easily attacked by malicious interceptors known as eavesdroppers. The aim of an eavesdropper is to breach the communication security by acquiring the transmitted data. This attack jeopardizes the signal confidentiality because the data might be modified and analyzed before being forwarded to the legitimate user [18].

At first, the notion that an OCDMA encoded signal is similar to a noise waveform makes it difficult for an eavesdropper to read the transmitted data. Nevertheless, the single-user on-off keying OCDMA system can be easily attacked by a simple energy detector without any knowledge of the code [39, 40, 49]. To provide security against simple energy detector, code shift keying and differential phase shift keying OCDMA systems were proposed. In CSK, the data bits ‘0’ and ‘1’ were encoded by two different codes making it impossible to detect using a simple power detector [49, 51, 52, 53]. However, the single-user CSK-OCDMA system is susceptible to eavesdropping by using differential phase-shift keying demodulator followed by a balanced photodetector [42, 55, 56]. Also, the single-user DPSK-OCDMA technique which is immune to a standard power detector is vulnerable to eavesdropping if the eavesdropper is equipped with a DPSK demodulator [57]. Therefore, based on the limitations of both CSK and DPSK systems, a generic OCDMA technique is required to increase the security of isolated user signal.

In this chapter, eavesdropper’s code interception performance for single transmitting user in OCDMA network is evaluated first. Then the proposed virtual user model for security

enhancement against eavesdropping is discussed. To increase the bandwidth efficiency of the virtual user technique, an intelligent feedback control is incorporated in it. This technique is called modified virtual user scheme. Then the analysis of security performance of the proposed scheme for an isolated user signal is done. The proposed technique is simulated with on-off keying, code shift keying and differential phase shift keying. The results obtained for the proposed technique are compared with the existing techniques.

3.2 Isolated User Signal Access in OCDMA Network

In the OCDMA system, multiple users transmit data simultaneously and data from all the users is multiplexed before transmission onto an optical fiber. These multiple users act as a source of multiple access interference to each other. In the network, there are times when only single user is active while all others are sitting idle at the same time.

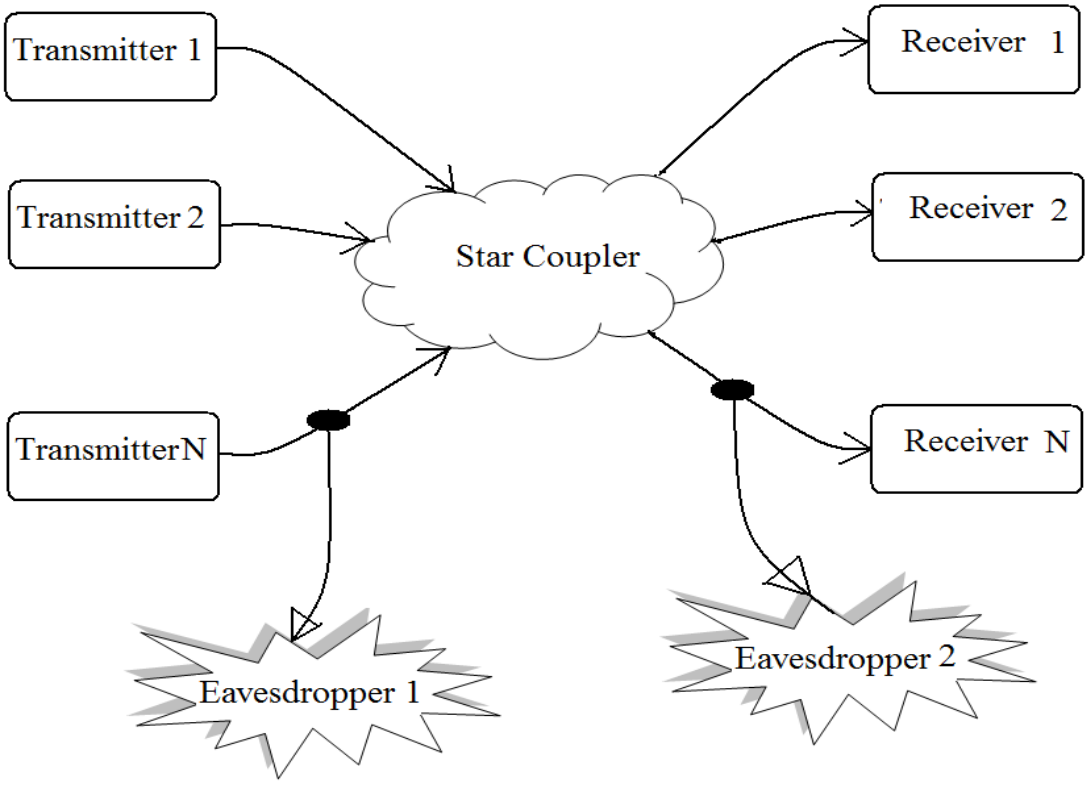


Figure 3.1: Various locations of an eavesdropper

There are two ways of intercepting the data by tapping into the optical fiber, i.e. before and after the coupler as shown in the figure 3.1. Before the coupler, eavesdropper 1 can have access to isolated user's signal and after the coupler a multiple user (multiplexed) signal can be tapped. If only one user is active in the network at some moment then eavesdropper 2 can also access the isolated user signal after the coupler.

3.2.1 Eavesdropper's Code Interception Performance for Single Transmitting User

From eavesdropper's point of view, the easiest way to intercept the information is to tap isolated subscriber signals, avoiding multiple access interference automatically. Therefore, we first discuss the security performance of a single-user OCDMA system.

The figure of merit for code interception performance is the probability that an eavesdropper can detect the user's codeword without any error is P. This requires two probabilities; the possibility of false detection of a pulse in the codeword (P_{fd}) and the possibility of missing a "1" pulse in a given codeword (P_m).

The probabilities P_{fd} and P_m can be represented as in (3.1) and (3.2) respectively [39].

$$P_{fd} = \exp\left(-\frac{\gamma}{N_0}\right), \tag{3.1}$$

$$P_m = 1 - Q\left(\sqrt{2E_p/N_0}, \sqrt{2\gamma/N_0}\right), \tag{3.2}$$

where, E_p/N_0 is the ratio of peak pulse energy to noise power spectral density, γ is optimum detection threshold and $Q(\alpha,\beta)$ is the Marcum Q-function given by [38]

$$Q(\alpha,\beta) = \int_{\beta}^{\infty} z I_0(\alpha z) \exp\left(-\frac{z^2+\alpha^2}{2}\right) dz, \tag{3.3}$$

where, $I_0(z)$ is the zero-order modified Bessel function of first kind.

Hence, the probability that an eavesdropper can correctly detect the data in the bit interval by intercepting the codeword is given by

$$P = (1-P_m)^{\text{Number of 1s in the codeword}} \times (1-P_{fd})^{\text{Number of 0s in the codeword}} \quad (3.4)$$

The generalized equation developed in (3.4) is applicable for 1-D, 2-D and 3-D codes as shown below. The probability that an eavesdropper can correctly detect the data:

- for 1-D codes having length L of the codeword and weight w (number of 1s in the codeword),

$$P = (1-P_m)^{w}(1-P_{fd})^{L-w} \quad (3.5)$$

- for 2-D codes having length L, wavelengths λ and weight w,

$$P = (1-P_m)^{w}(1-P_{fd})^{L\times\lambda-w} \quad (3.6)$$

- for 3-D codes having length L, wavelengths λ and polarization (Pol),

$$P = (1-P_m)^{w}(1-P_{fd})^{L\times\lambda\times Pol-w} \quad (3.7)$$

In 3-D codes, each chip in a code is assigned a time slot, a wavelength, and one of two orthogonal polarizations states [22]. Hence, for orthogonal polarization, Pol=2. The 3-D codes can also be designed using space as the third dimension instead of polarization. Therefore, the probability for 3-D codes having length L, wavelengths λ and space S is given by

$$P = (1-P_m)^{w}(1-P_{fd})^{L\times\lambda\times S-w}. \quad (3.8)$$

When a single user is active in the network, the probability of correct bit interception is plotted against eavesdropper's E_p/N_o for 1-D, 2-D and 3-D codes as shown in figure 3.2. The interception probability increases with increase in E_p/N_o, whereas, it decreases with the increase in the code dimensions. Hence, with increase of the code dimension from 1-D to 3-D, the interception probability is increasing. However, there are two ways to implement to 3-D codes which are based on polarization or space as the third dimension. The limitation of polarization is that it can have only two states, whereas the spatial dimension allows us to have more freedom

with 3-D codes. Therefore implementation of 3-D codes using space (S = 5) as the third dimension has increased security over polarization. From the results and above discussion, it is clear that as compared to 3-D codes, 1-D and 2-D codes are more vulnerable to eavesdropping. Therefore, most of the analysis is done using 1-D and 2-D codes.

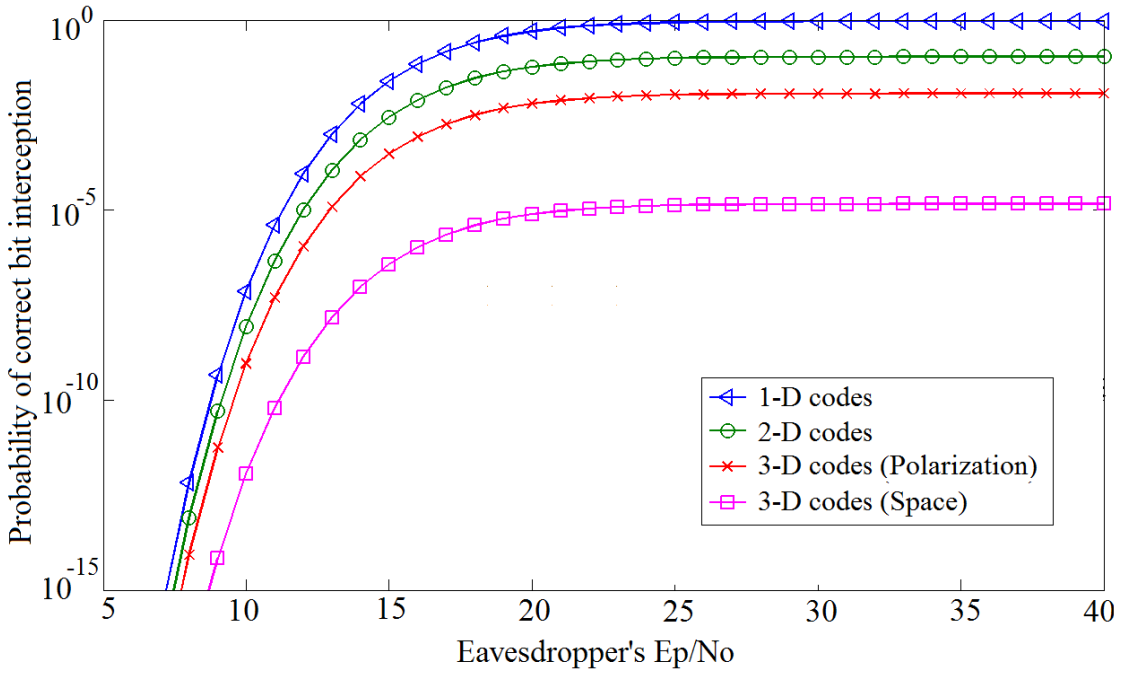


Figure 3.2: Eavesdropper's probability of error free code word detection for different E_p/N_o for 1-D, 2-D and 3-D codes.

3.3 Proposed Model for Security Enhancement against Eavesdropping

A key observation is that if at any time an eavesdropper finds a single transmitting user, then it can easily take the advantage to sift the data by tapping into an optical fiber. Thus, user transmissions are confidential only if other signals are being transmitted simultaneously. The notion that the difficulty of deciphering the data bits increases in the presence of multiple users is used as the underlying principle for the proposal of virtual user scheme (VUS).

We describe a simple and feasible approach against eavesdropping by introducing a dummy user in parallel with the primary OCDMA user to block the access to a single transmitting user. In a star network, data from all users is collected at a central point and then distributed to all users. Local area network has this broadcast and select system architecture in which a fiber carries

individual user data signal over 50% of total fiber length. This makes the system very vulnerable to eavesdropping.

3.3.1 System Model with Virtual User Scheme

By forcing the eavesdropper to detect multiple signals simultaneously, the eavesdropping attack on the targeted signal can be avoided. This can be done by incorporating a virtual user in the system as shown in figure 3.3.

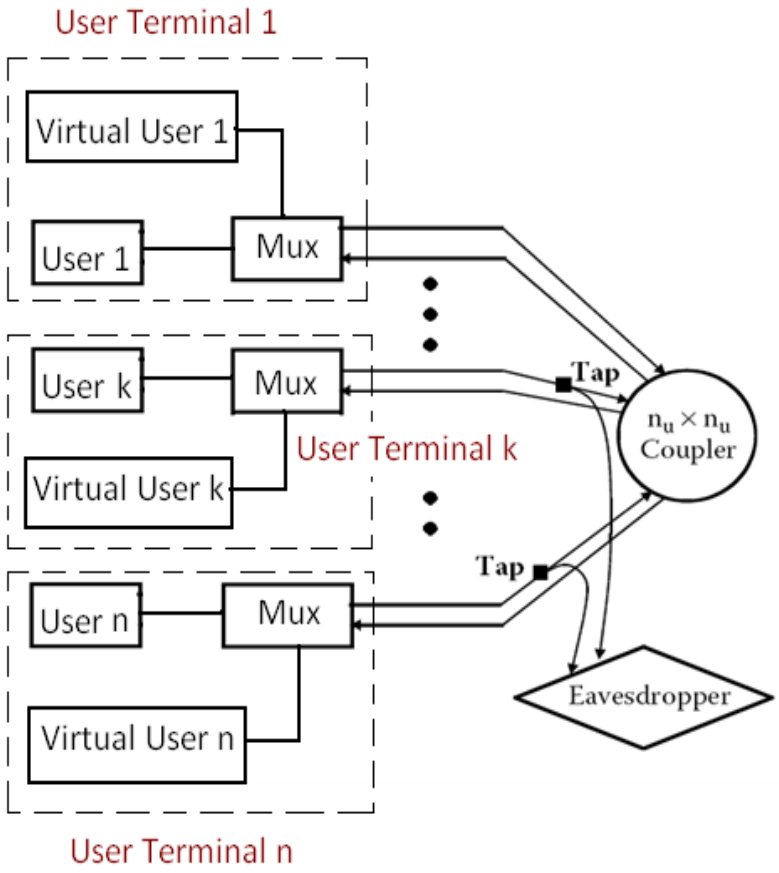


Figure 3.3: An eavesdropper tapping into the optical fiber can't isolate an individual user

A virtual user environment is created in the network by incorporating a virtual user with every authorized user. A virtual user will enhance the confidentiality of an OCDMA system by always transmitting in parallel to the authorized user. The pseudo random noise is used as the data input to the virtual user. Both users are encoded using different codes and then multiplexed before transmitting the signal over the optical fiber. This virtual user acts as interferer and appears as an

authorized user to the eavesdropper; this would prevent eavesdropping. Hence, the presence of multiple users makes it more difficult to sift the data.

In the VUS, twice as many codes are needed as compared to conventional OOK-OCDMA because each authorized user has its own virtual user which requires a unique code. This results in wasting half of the codewords on the virtual users which is similar to the case of CSK-OCDMA.

To illustrate this, the information capacity (C) of an OCDMA network may be given as (3.9) [69]:

$$C = K.[1 - \log_2(1 + e^{-SNR})] \tag{3.9}$$

where, K is the number of users and SNR is the signal to noise ratio which depends on MAI noise.

For the virtual user scheme and CSK-OCDMA, the number of users is halved because two codes are used in encoding for a single user. Therefore, the system capacity is halved. So, the enhanced security of information transmission in the network is obtained at the expense of sacrificing network resources.

3.3.2 System Model with Modified Virtual User Scheme

In order to minimize the wastage of network resources, the virtual user scheme is slightly modified by introducing a common virtual user for all the users. This means each user has its dummy user but same codeword is shared amongst all the dummy users which will become active only whenever the authorized user is isolated in the network as shown in figure 3.4. This will increase only the hardware cost but does not degrade the system performance by decreasing the number of simultaneously active users from the given code set.

In this scheme, a pseudo user is present with all the authorized users which will transmit in parallel with the authorized user once it is isolated. All the dummy users share the same codeword. The pseudo random noise is given as the data input to the virtual user and the data is encoded using a unique optical code from the code set used. Both the legitimate signal and the virtual user signal are multiplexed together before being sent on the optical fiber. This virtual user will act as an interferer. Hence, the level of confidentiality will automatically increase when the eavesdropper is deliberately made to detect multiple user signals in the same time instant.

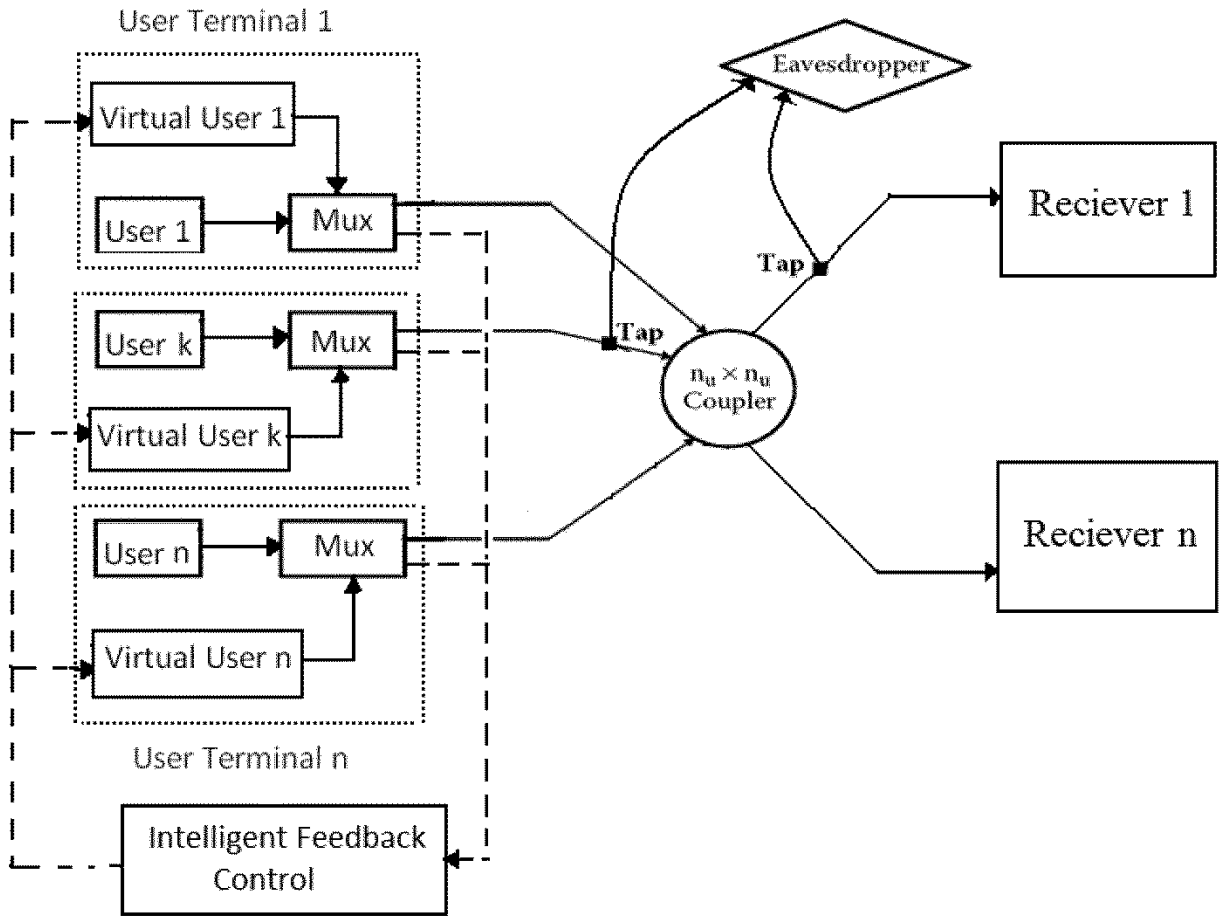


Figure 3.4: OCDMA network in virtual user environment

The intelligent feedback control (IFC) monitors the network for isolated user signals and acts as a switch for virtual users. Whenever a single user is transmitting, the IFC sends an 'ON' feedback signal to the virtual user transmitter attached with the isolated user. This virtual user will act as a source of multiple access interference and start transmitting instantly. So, each time an eavesdropper tries to access the system only the multiplexed data will be available to it. The virtual user will serve as an interferer but appears as an authorized user to an eavesdropper, thus hindering eavesdropping. Therefore, an eavesdropper can never isolate an individual user's signal because there is always an active user in the network that serves as interferer, and deciphering the data bits when multiple users are present is very difficult [39]. The IFC allows the virtual user to transmit as long as all the other users in the network are dormant. As soon as another user in the network starts transmitting, the IFC sends an 'OFF' signal to the virtual user.

This will secure the system without affecting the system performance and wasting the precious bandwidth.

The algorithm developed for IFC is given below:

N are the number of simultaneous active users

If N=1,

IFC will send the 'ON' signal; %Virtual user starts transmitting

If N=0 or N>1then,

IFC will send the 'OFF' signal; %Virtual user is not transmitting

When only a single user is transmitting while all other users are sitting idle, the virtual user is the source of multiple access interference for the eavesdropper. Moreover, the technique is bandwidth efficient as it does not impose any additional bandwidth penalty as compared to conventional CSK-OCDMA network.

3.4 Eavesdropper's Probability of Correct Bit Interception in Presence of Virtual User

In this section, an analytical framework is developed to analyze the security performance of an isolated user signal in an OCDMA network in the presence of a virtual user. For CSK-OCDMA, the probability that a pulse belonging to a virtual user overlaps with one of the pulses of the desired user is given by (3.10) [70, 71]

$$q = \frac{w^2}{L \times \lambda}, \tag{3.10}$$

where, L is length of code and λ is the number of wavelengths and w is weight of the code.

In optical orthogonal codes, two code words cannot overlap at more than one pulse position. There are w^2 ways of pairing the w pulses of an authorized user with its virtual user. Hence, one virtual user is created and it generates w hit-of-one over a bit period.

The probability of having a pulse's peak v in anyone of (L-1) undesired time slot location is defined as (3.11)

$$P_r(v) = \binom{w}{v}\left[\sum_{i=0}^{v}(-1)^i\binom{v}{i}\left(1-q+\frac{vq}{w}-\frac{iq}{w}\right)\right], \tag{3.11}$$

The probability that t time slot locations have pulse intensity of at least w and remaining (L-1-t) have intensity less than w is given by (3.12)

$$P_r(w,t) = \binom{L-1}{t}\left[P_r(w)\right]^t\left[\sum_{j=0}^{w-1}P_r(j)\right]^{L-1-t}, \tag{3.12}$$

The probability of correct bit interception at eavesdropper is, when virtual user is active is defined as (3.13)

$$P(\text{virtual}) = P_r(w,0)+\frac{1}{2}P_r(w,1), \tag{3.13}$$

For virtual user scheme where only one user is introduced, by putting the values from eq. (3.11) in (3.13), the probability becomes (3.14)

$$P(\text{virtual}) = \left[\sum_{j=0}^{w-1}P_r(j)\right]^{L-1}+\frac{1}{2}(L-1)\left[P_r(w)\right]\left[\sum_{j=0}^{w-1}P_r(j)\right]^{L-2} \tag{3.14}$$

Figure 3.5 shows the probability of correct detection of the transmitted bit for both the cases when a single user is transmitting and second is when virtual user is active along with the single user. Therefore, an eavesdropper is forced to detect multiple signals simultaneously even when a single user is active in the network. It is shown that eavesdropper's probability of correct bit interception decreases from 7.5×10^{-1} to 1.85×10^{-5} with the inclusion of a virtual user. The interference caused by the virtual user degrades the code interception performance of an eavesdropper. One can see that the obscuration of the targeted signal in this scenario would significantly increase the level of confidentiality.

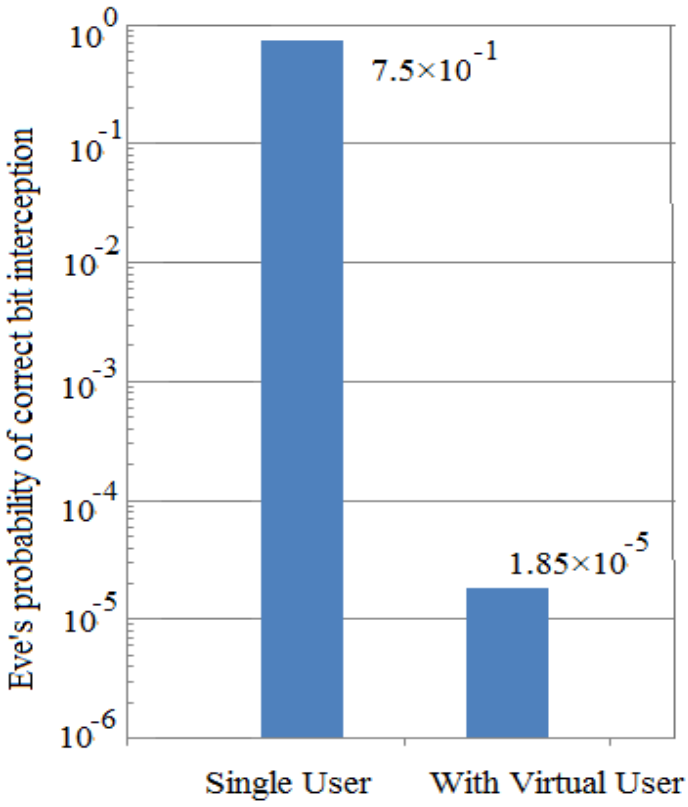


Figure 3.5: Eavesdropper's probability of correct bit interception

3.5 Simulation Setups for Different OCDMA Networks with Proposed Virtual User Scheme

To verify the effectiveness of the virtual user scheme to prevent the eavesdropping attack, different types of OCDMA systems are simulated. The OCDMA network is considered with different modulation schemes, i.e. on-off keying, code shift keying and differential phase shift keying.

3.5.1 On-Off Keying OCDMA

The security enhanced OCDMA system using virtual user scheme is shown in figure 3.6. An OCDMA system based on on-off keying for a single transmitting user is implemented using the software OptSim as follows.

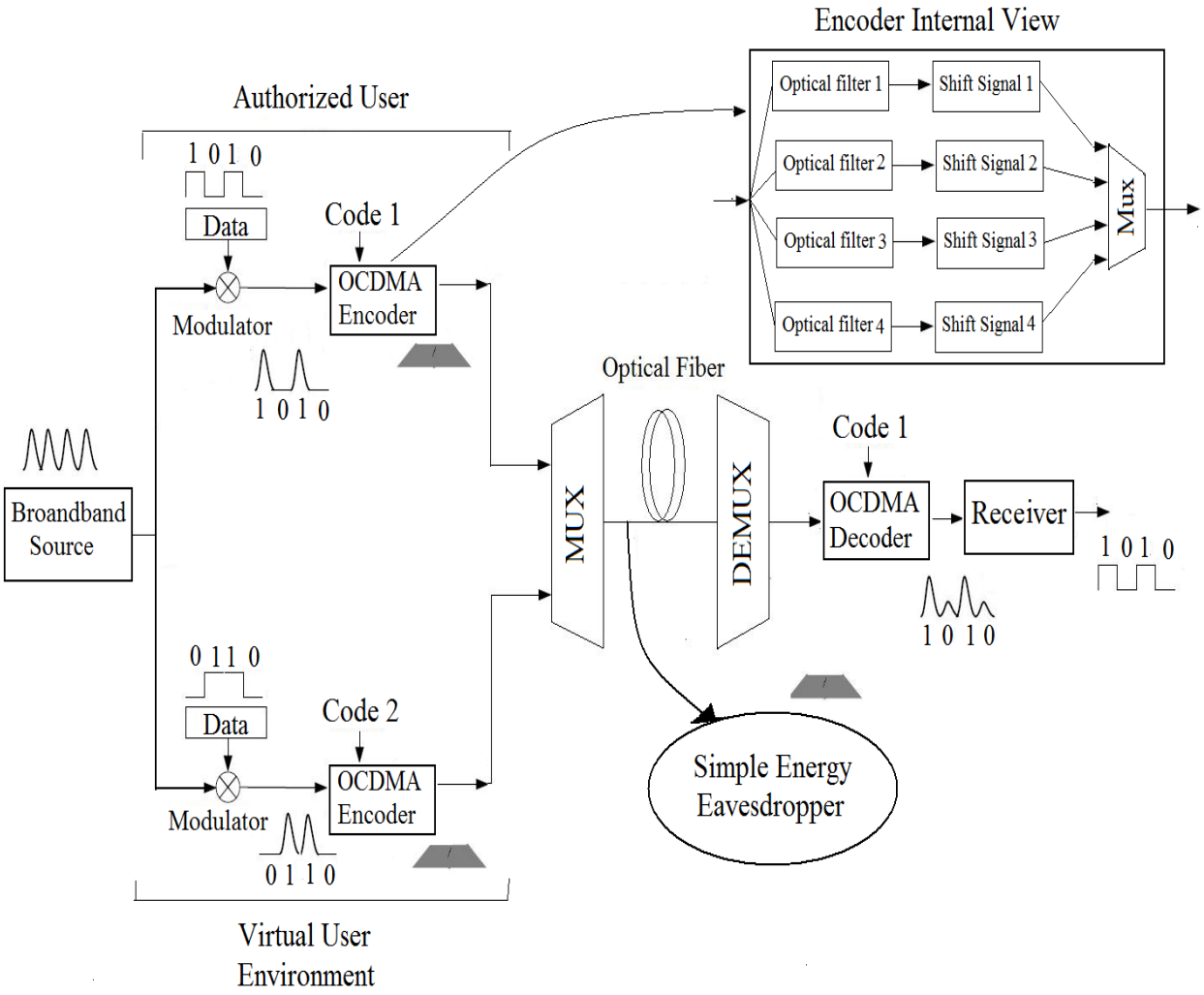


Figure 3.6: Simulation setup of OOK-OCDMA system in virtual user environment for single transmitting user

The broadband signal consists of the multiplexed output of the four mode locked lasers ranging from 1550 nm to 1551.2 nm with a wavelength spacing of 0.4 nm. The repetition rate of lasers is 2.5 Gbps which is same as the bit rate. The PRBS generator is used to produce pseudo random binary sequence (PRBS) and on-off type electrical generator is used with NRZ modulation format. In order to implement on-off keying OCDMA system, amplitude modulation is done at modulator. Further at the encoder, two dimensional wavelength/time (W/T) matrix codes are used for encoding [23, 72]. In an encoder four optical filters and four signal shifters are used to produce the encoded bit stream. The optical filter is used to filter out one spectral wavelength and then the Shift Signal is used to produce a pulse at specified chip. The optical multiplexer

(Mux) combines four of the displaced pulses to form an encoded signal. Encoders and decoders respectively use delay and inverse delay line arrays providing delays in terms of integer multiples of chip times [73]. The placement of the delay-line arrays and the amount of each delay are dictated by the specifics of the user signatures.

The encoded data from both the users is multiplexed and then transmitted through a 25 km of standard single mode fiber with attenuation of 0.25 dB/km, followed by a loss compensating optical amplifier with gain 30 dB. The output signal from an optical fiber then passed through a de-multiplexer (Demux) and routed to the user's decoder. At the receiver, only the authorized user code is given to decoder. The decoded signal finally arrives at optical receiver and BER tester. After the transmitter, eavesdropper employing simple energy detector is placed to sift the data.

3.5.2 Code Shift Keying OCDMA

The system setup for 1.25 Gbps CSK-OCDMA system is shown in figure 3.7 with proposed security scheme. The PRBS data modulates the carrier signal which consists of eight wavelengths from 1550 nm to 1551.4 nm spaced 0.2 nm apart. Input power is varied from 0.1 mW to 3 mW. Encoders are placed in a manner to implement code shift keying [50]. The data generators are used to generate random data of length 2^7 bits with 2^5 points per bit to modulate the light signal. For spectral encoding, each encoder is assigned a unique Walsh Hadamard code [74]. Similarly, a virtual user is placed in parallel to authorized user. For transmission, a single mode fiber of length 35 Km is used, with an attenuation of 0.25 dB/km followed by an amplifier having gain of 30 dB. In between the transmitter and receiver, eavesdroppers employing simple energy detector and differential detector are placed. For differential detection the input signal is combined with its one bit delayed version followed by balanced detection [56, 42]. Finally, at the receiver, composite signal is decoded optically using an optical decoder that is matched to the desired user code followed by balanced photodetector for the recovery of transmitted data.

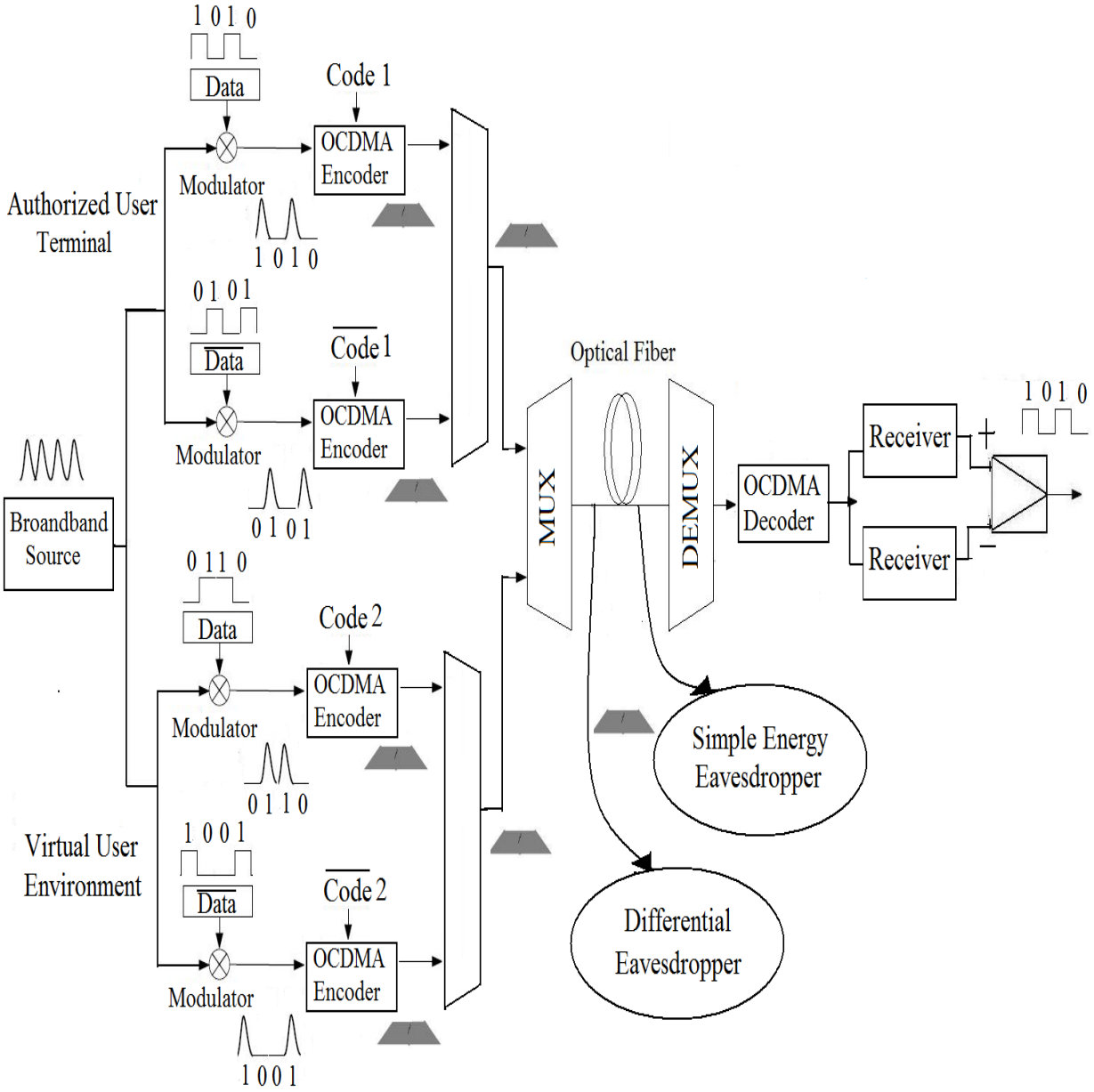


Figure 3.7: Simulation setup of CSK-OCDMA system in virtual user environment for single transmitting user

3.5.3 Differential Phase Shift Keying OCDMA

An OCDMA system with DPSK signalling and balanced detection is simulated as shown in figure 3.8. The simulation parameters of this system are presented in table 3.1. The DPSK system with balanced detection is an attractive modulation format for long-haul transmission as compared to the OOK modulation [75, 76].

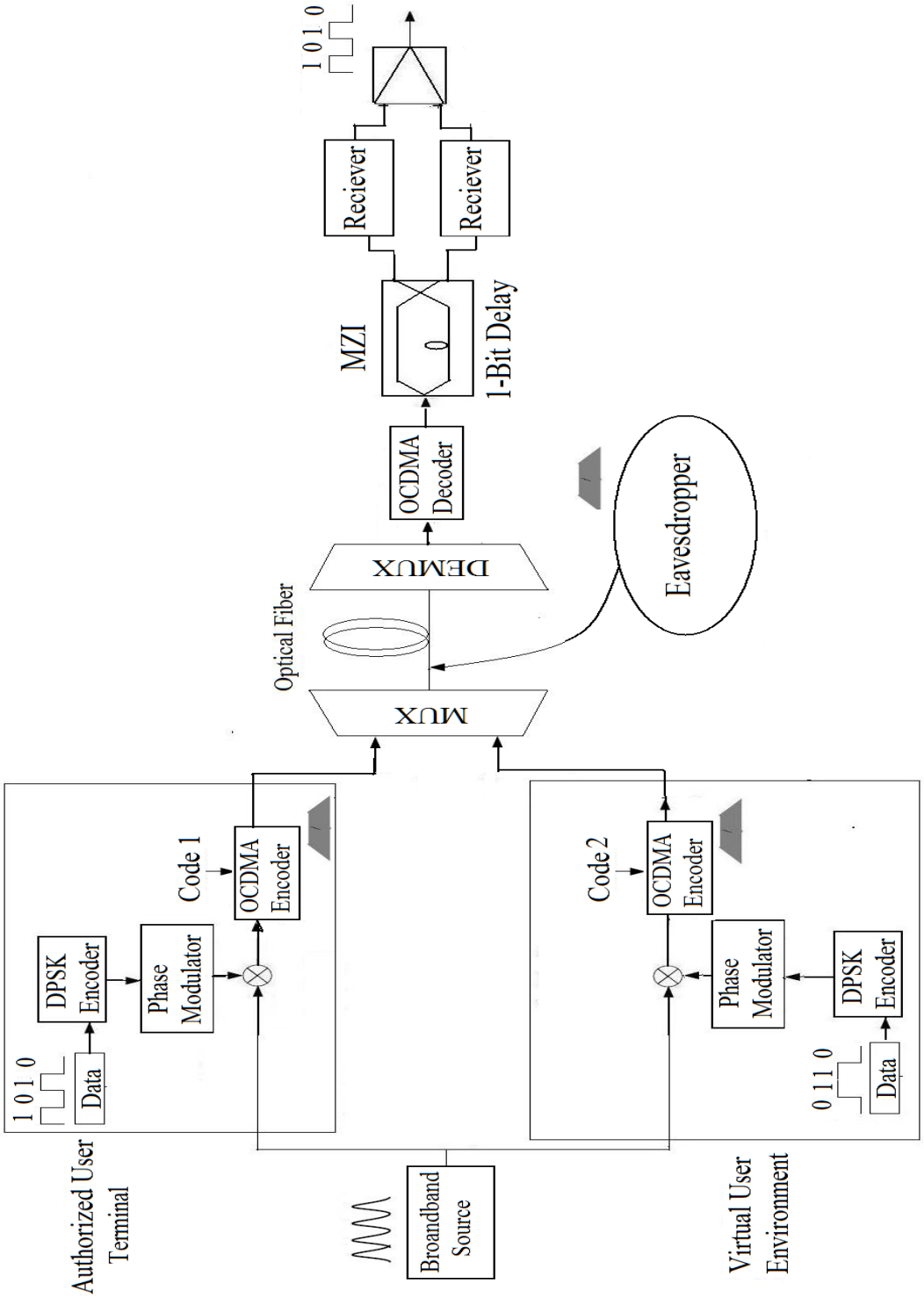


Figure 3.8: Simulation setup for DPSK-OCDMA system in virtual user environment for single transmitting user

The DPSK format is a subset of the phase-shift keying (PSK) format in which the information carrying part for the DPSK encoded data is the phase difference applied to the carrier corresponding to two consecutive data bits. If the previous bit is 0, no phase shift is applied for encoding the current bit. If the previous bit is 1, the phase of the carrier for the current bit is applied with a phase shift of 180 degrees [77]. Next, a virtual user is created which is always transmitting in parallel to the authorised user. The outputs of the authorised and virtual users are combined by an optical multiplexer before transmission. A conventional single mode optical fiber having a length of 25 km is used for transmission, after which the DPSK modulated signal enters the receiver section of the topology.

Table 3.1: Simulation parameters for DPSK-OCDMA system

Parameter	Value
Bit rate (Data rate)	2.5 Gbps
Number of optical sources	12 mode-locked lasers
Wavelength range	1550–1552.2 nm
Wavelength spacing	0.2 nm
Repetition rate of laser pulses	2.5 Gbps
Input power	1 –5 mW
Drive type of electric generator	On-off
Signal type of electric generator	Voltage
Modulation type	Phase modulation (with a phase shift of π)
Codes used	Zero cross-correlation codes (ZCC)
Code weight	3
Code length	12
Fiber length	25 km
Attenuation	0.25 dB/km
Amplifier gain	30 dB
Delay in MZI	0.4 ns (1-bit delay)

At the receiver, a spectrally encoded signal is decoded by an authorised user sharing the same zero cross-correlation (ZCC) code [78] with the transmitter. One of the consequences of the

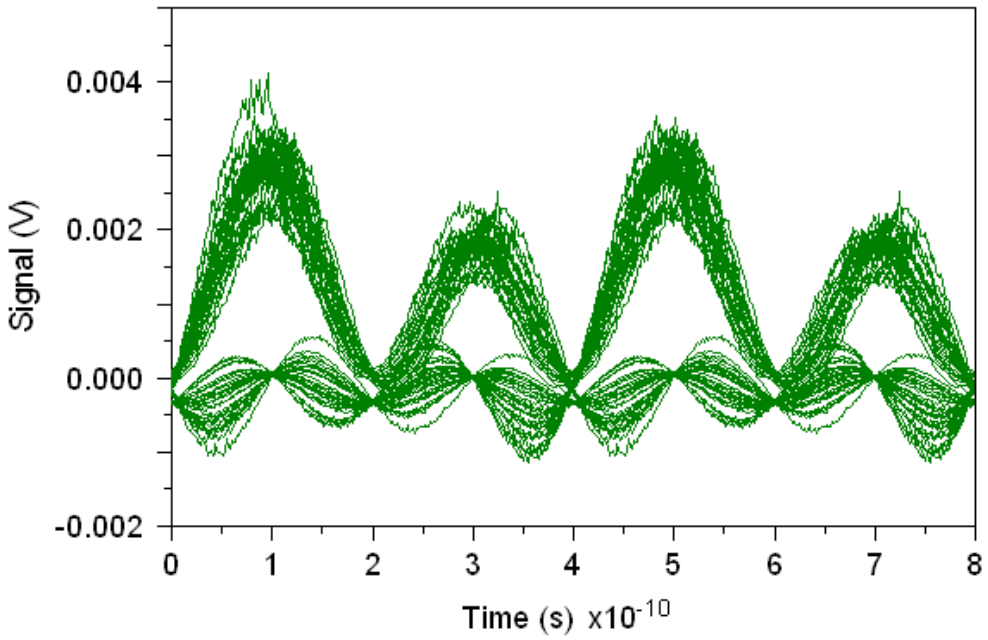
DPSK format is that optical intensity remains constant during all bits, and thus the direct-detection receivers cannot be used to detect the PSK signals. The demodulator consists of a delay line interferometer that has a 1-bit delay; therefore, 2 bits can be compared at one time [42]. Differential time delay is set to the bit duration. Two outputs of the interferometer corresponds to 'constructive port' and 'destructive port' where maximum power appears at the former when there is no phase change between adjacent bits, and at the latter when the phase in adjacent bits differs by π. Then two outputs of the demodulator are input to a balanced receiver that transforms the optical field into an electric current [79]. Next, the output electrical signal from one of the receivers is inverted and both electrical signals are combined by an electrical summer. Two separate eavesdroppers employing a simple energy detector and a differential detector are placed between the transmitter and receiver. At the differential detector, the incoming signal is split into two paths and combined again with 1-bit difference between the two paths followed by a balanced photodetector [42].

3.6 Results and Discussion for Security Enhanced OCDMA Network

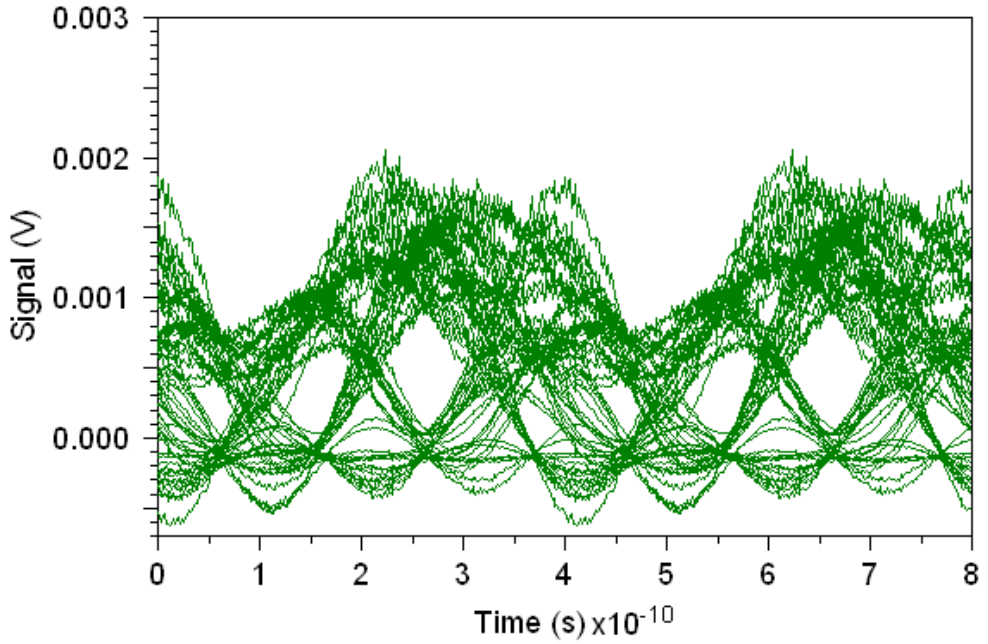
The results obtained for OOK, CSK and DPSK OCDMA systems are evaluated in terms of BER, eye diagrams and signals measured at eavesdropper and receiver. The results for both the proposed technique and the conventional schemes already existing in literature are compared and discussed.

3.6.1 On-Off Keying OCDMA

Firstly, OOK-OCDMA system is simulated with and without the proposed scheme. Figures 3.9(a) and 3.9(b) show the eye diagrams detected by the eavesdropper for single user and virtual user, respectively. It is observed that the eye diagram of the single user eavesdropper is open and the signal is correctly detected at eavesdropper. On the contrary, the eye diagram measured for the eavesdropper in virtual user environment has many levels, leaving the signal fully distorted, and this prevents a malicious attacker from sifting the transmission. An eavesdropper tapping a signal in a virtual user environment will have significant difficulty in deciphering the transmission without prior knowledge of the code.

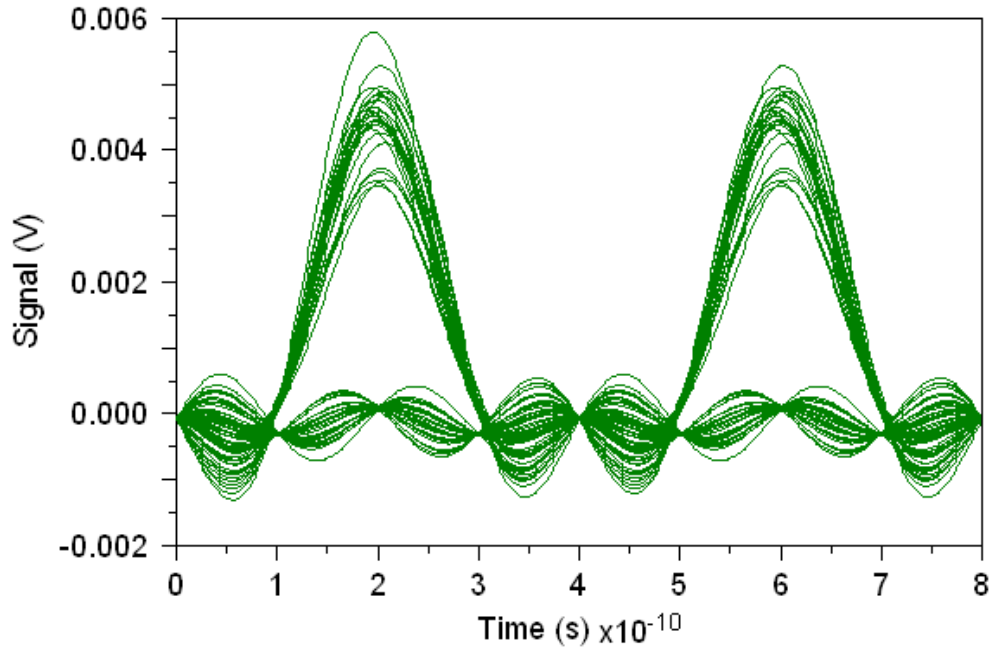


a) Single User

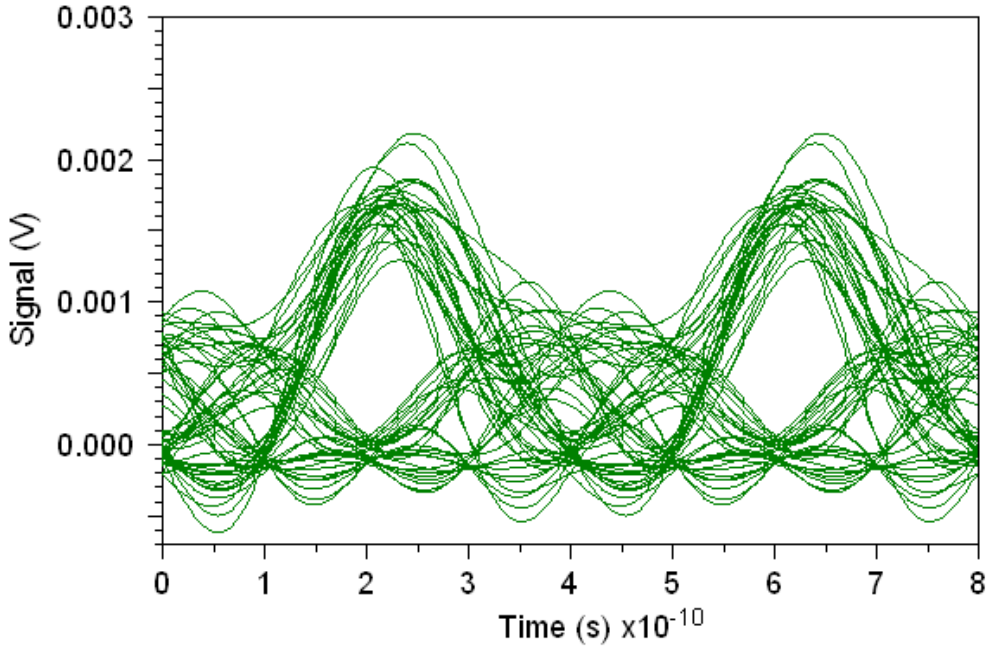


b) Virtual User Environmnet

Figure 3.9: Eye diagrams at eavesdropper for OOK-OCDMA



a) Single User



b) Virtual User Environmnet

Figure 3.10: Eye diagrams at authentic receiver for OOK-OCDMA

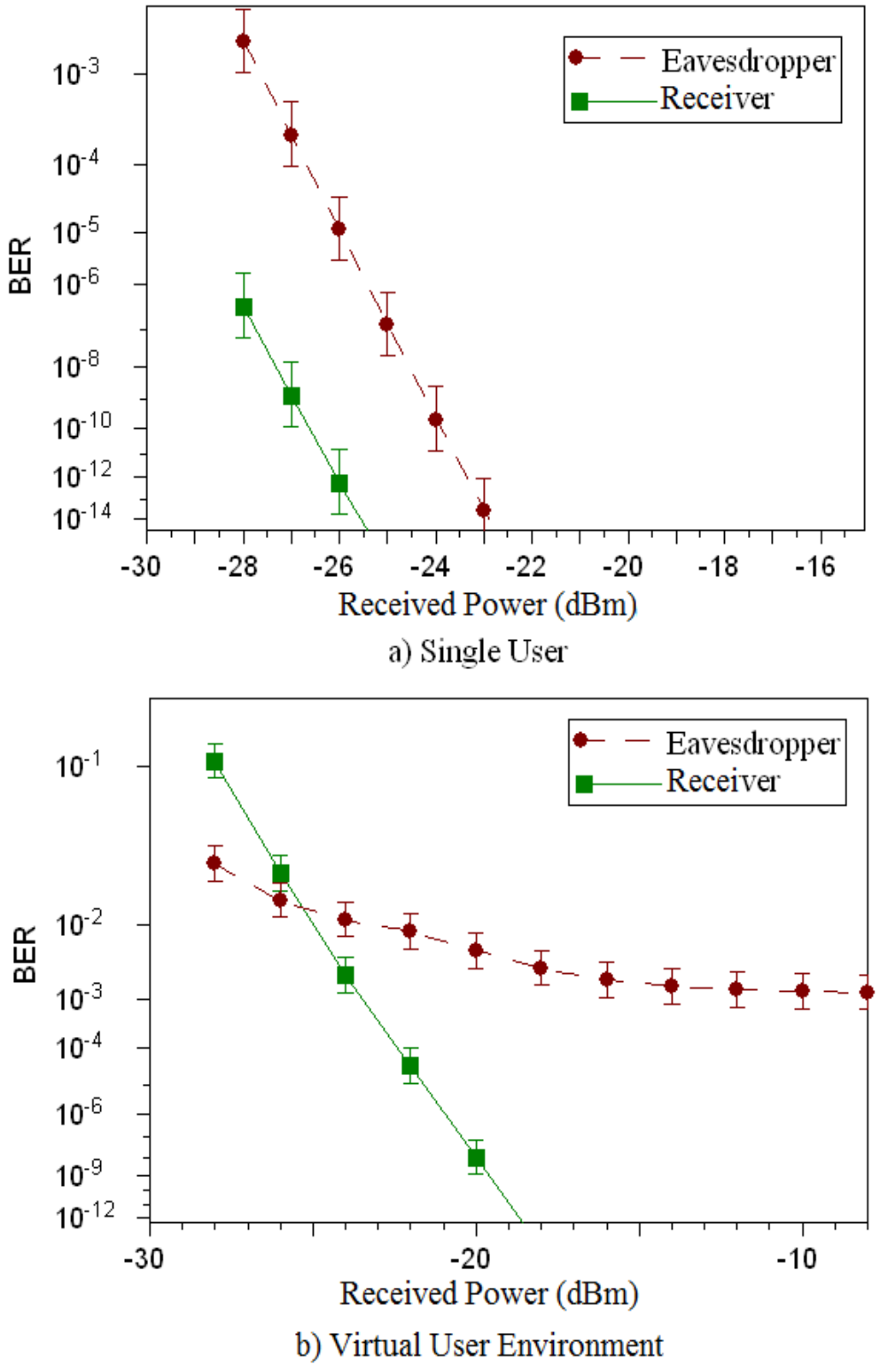


Figure 3.11: BER versus received power for OOK-OCDMA

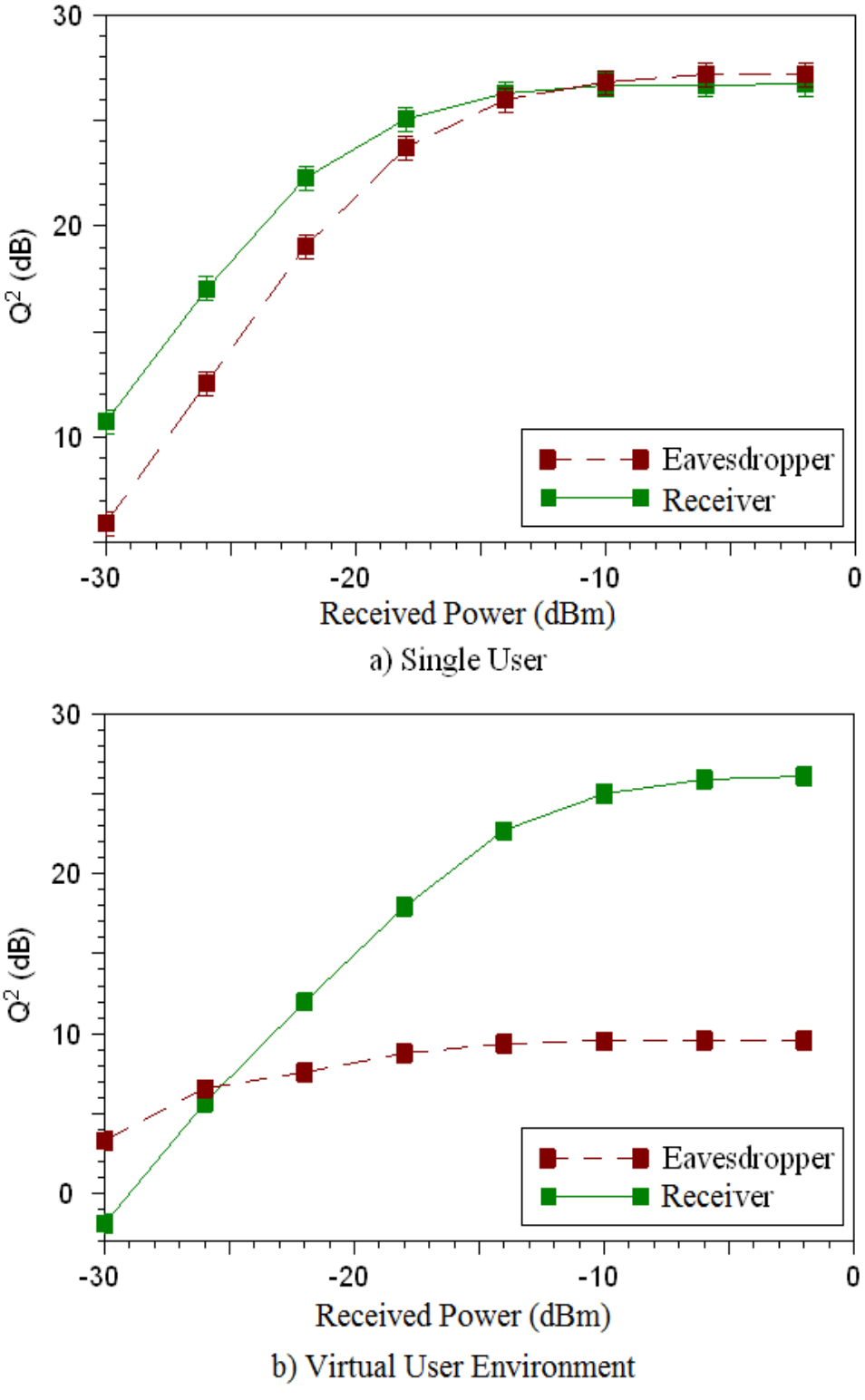


Figure 3.12: Q factor versus received power for OOK-OCDMA

In figure 3.10, the eye diagrams of the signal received at the authorized receiver are shown for conventional OOK and virtual user OOK scheme. With the matching codes the signal is correctly decoded in both the cases as the eye diagrams are completely open. As shown in figure 3.10(b) some distortion is observed at the authorized receiver in the presence of virtual user due to multiple access interference.

In order to compare the performance of the authorized and unauthorized users, the BER and Q factor measurements are shown in figure 3.11 and figure 3.12 respectively. It can be observed from figure 3.11(a) that the BER for both the eavesdropper and receiver is very low for a single transmitting user which means that the data is correctly decoded at the eavesdropper even without knowing the code used at the transmitter. On the contrary, figure 3.11(b) shows a large difference in performance between the authorized user (solid line) and the eavesdropper (dotted line). By creating a virtual user environment in which the authorized user has to transmit in the presence of a virtual user, BER for an eavesdropper is very high (ranges from 10^{-3} to 10^{-2}). This means that the eavesdropper is not able to decode any received signal. Similar results are obtained for the Q factor measurement as shown in figure 3.12.

3.6.2 Code Shift Keying OCDMA

After on-off keying, CSK-OCDMA system is simulated with and without the proposed scheme. For both CSK and virtual user scheme CSK, the variation of BER with respect to input power and fiber length is plotted for simple energy detector and differential detector at eavesdropper and authorized receiver. The variation of BER against input power and fiber length at 1.25Gbps is shown in figure 3.13 and figure 3.14 respectively. It is observed that both the CSK and virtual user CSK schemes are immune to eavesdropping using a simple power detector. For the simple energy eavesdropper, the BER is so close to unity that an accurate determination is not possible because the eye is so noisy that it is essentially closed [80]. However, the conventional CSK scheme is vulnerable to eavesdropping using a differential detector. It is also observed that the BER of differential eavesdropper is high in the presence of virtual user CSK scheme. The differential eavesdropper's BER is in the order of 10^{-2} with the proposed scheme. Hence, unlike conventional CSK-OCDMA, high BER is observed against differential eavesdropping in presence of a virtual user. This means that the proposed scheme makes the OCDMA system robust against both the simple power detector and differential eavesdropper. Further, at receiver

side comparable BER is found for both the schemes. So, the virtual user scheme maintains the acceptable BER at receiver while thwarting the eavesdropper from compromising the user security for the input power above 1mW and fiber length up to 30 km.

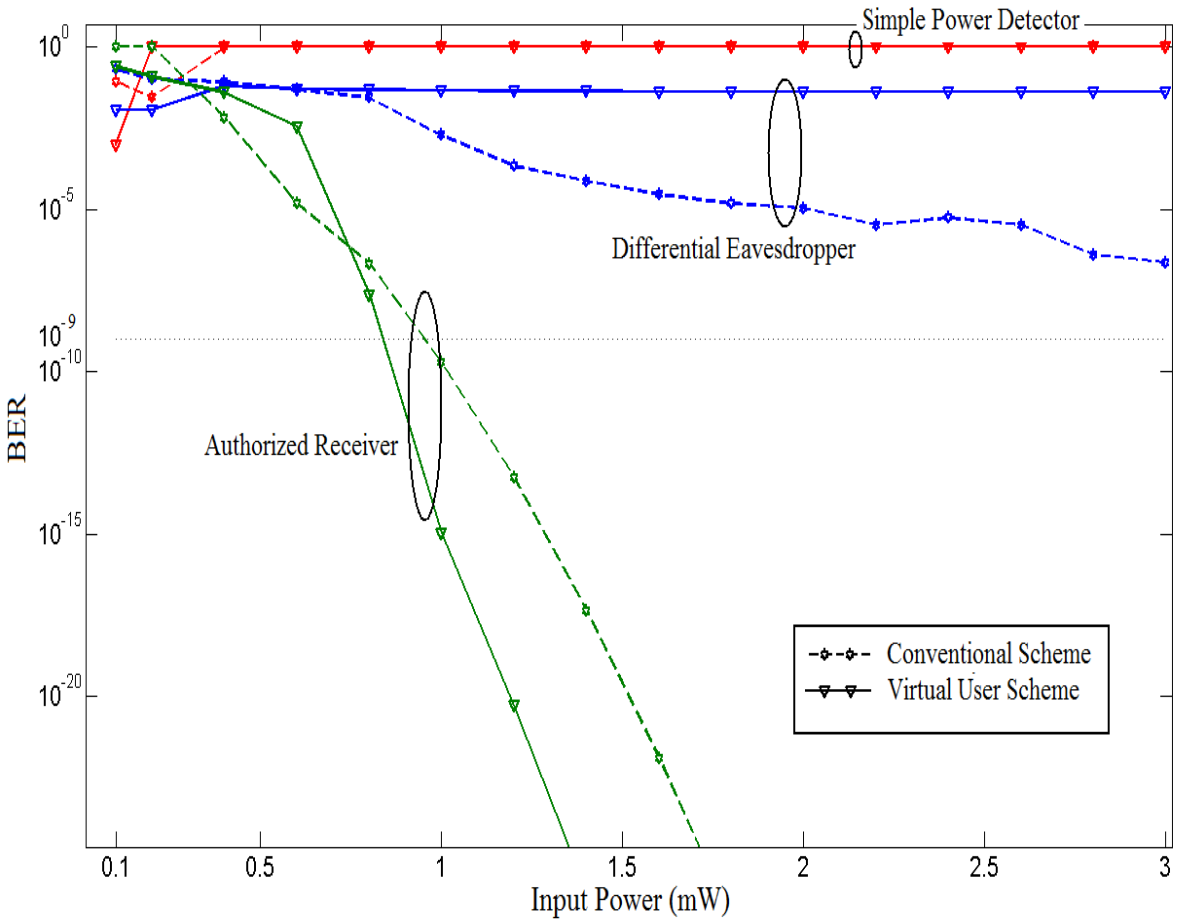


Figure 3.13: BER versus input power for CSK-OCDMA

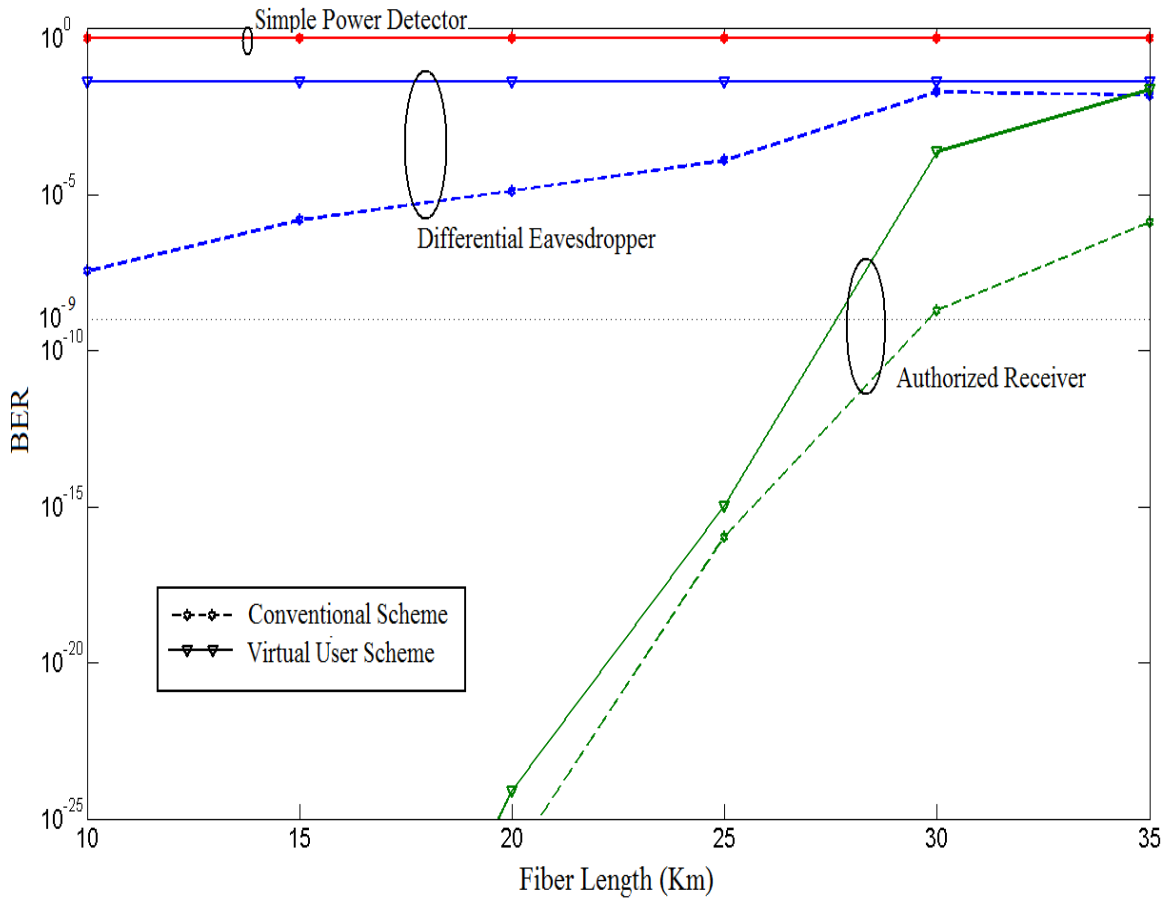


Figure 3.14: BER versus fiber length for CSK-OCDMA

The eye diagrams and the signals taken at 1.25 Gbps for the virtual user scheme are shown in figures 3.15 to 3.20. As shown in figure 3.18, the signal detected by a simple energy detector consists of all ones because both the '0' and '1' bits are encoded before transmission. Therefore, no eye is found at simple energy eavesdropper as shown in figure 3.15. This demonstrates the ability of CSK to enhance security against a simple power detector. It has already been discussed that, although CSK improves the security against a power detector, it is susceptible to differential detection. The proposed virtual user scheme enhances the security not only against simple power detector but also against differential detection.

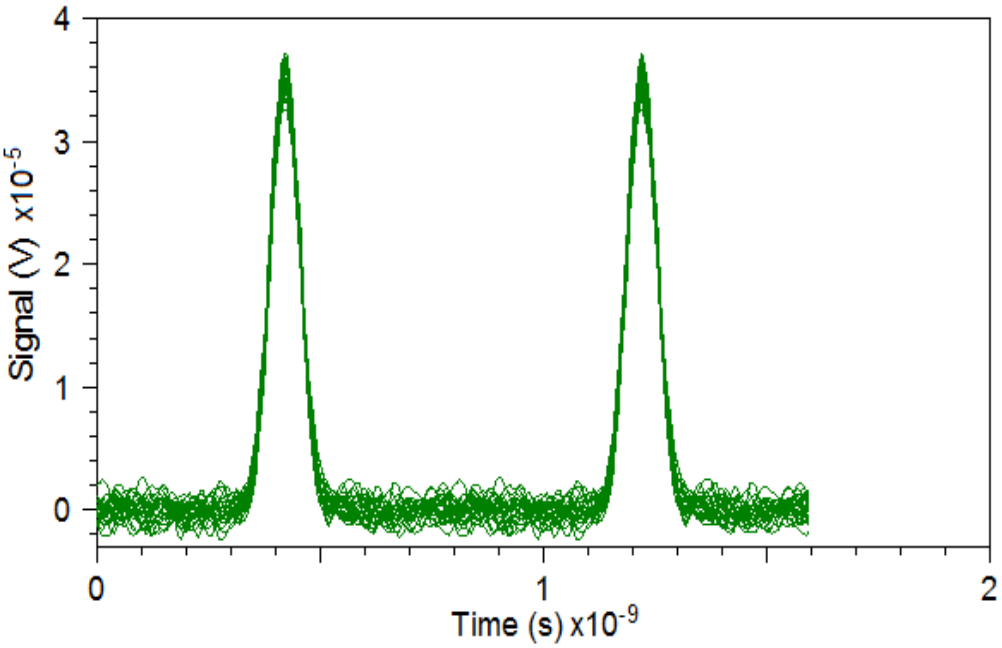


Figure 3.15: Waveform at simple energy detector for CSK-OCDMA virtual user scheme

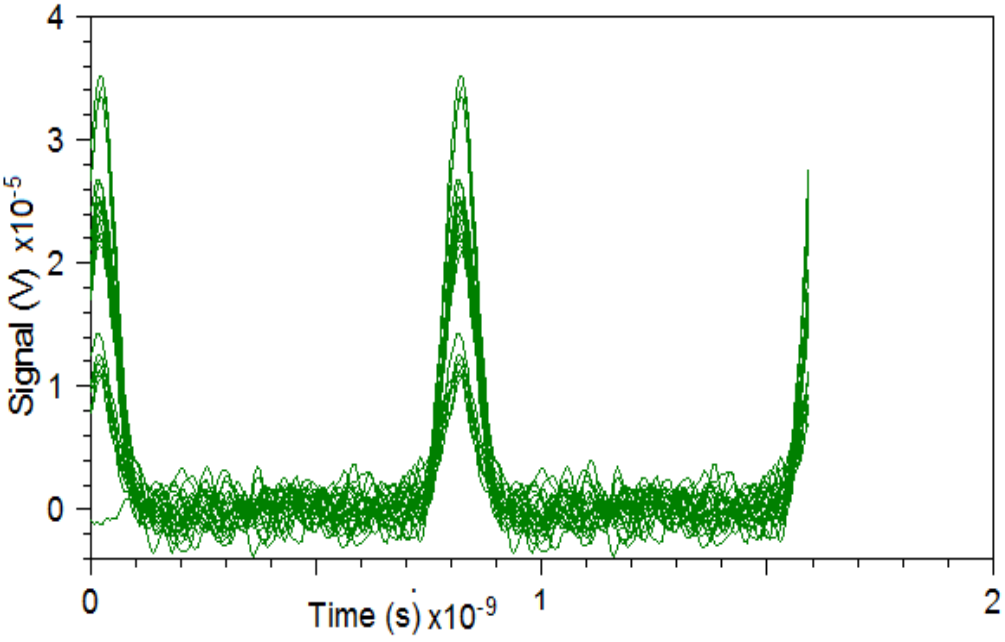


Figure 3.16: Waveform at differential eavesdropper for CSK-OCDMA virtual user scheme

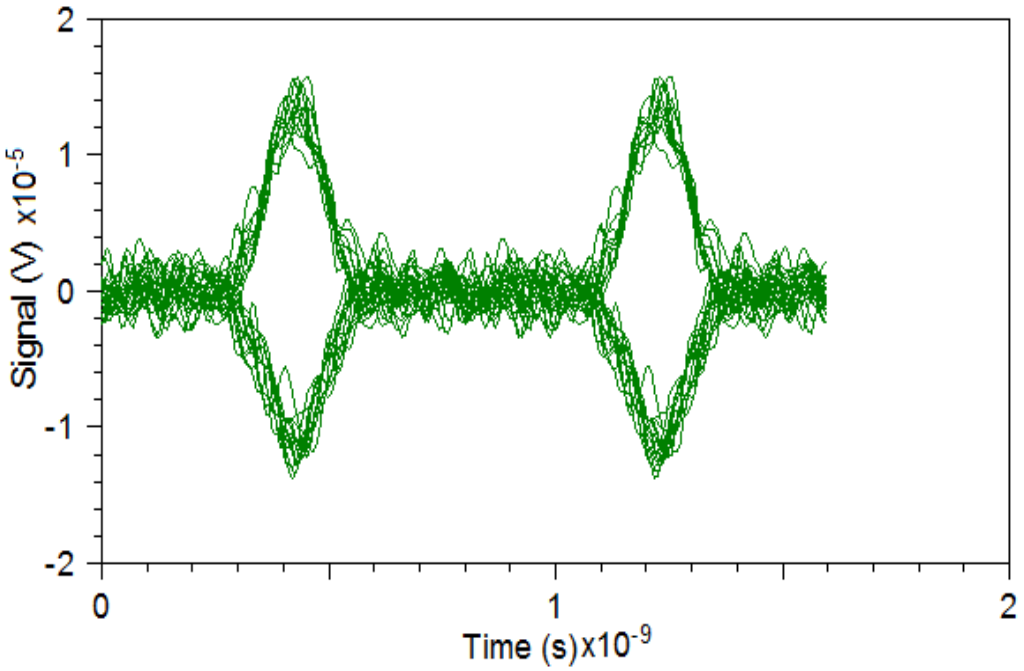


Figure 3.17: Eye diagram at receiver for CSK-OCDMA virtual user scheme

The waveform shown in figure 3.16 measured for differential eavesdropper in the presence of virtual user has many levels, leaving the signal fully distorted which prevents data interception. Also, the signal at differential eavesdropper (shown in figure 3.19) is completely distorted and not intelligible to the eavesdropper. So, the proposed technique enhances the security as compared to the code switching scheme against differential eavesdropper. Although, in the presence of virtual user, the signal obtained at the eavesdropper is distorted, the received signal at the legitimate receiver is completely intelligible as shown in figure 3.20. Therefore, the information gets transmitted reliably to the desired receiver and eavesdropping is avoided by using the virtual user technique. From the above discussion, it is clear that the proposed scheme is better than conventional CSK.

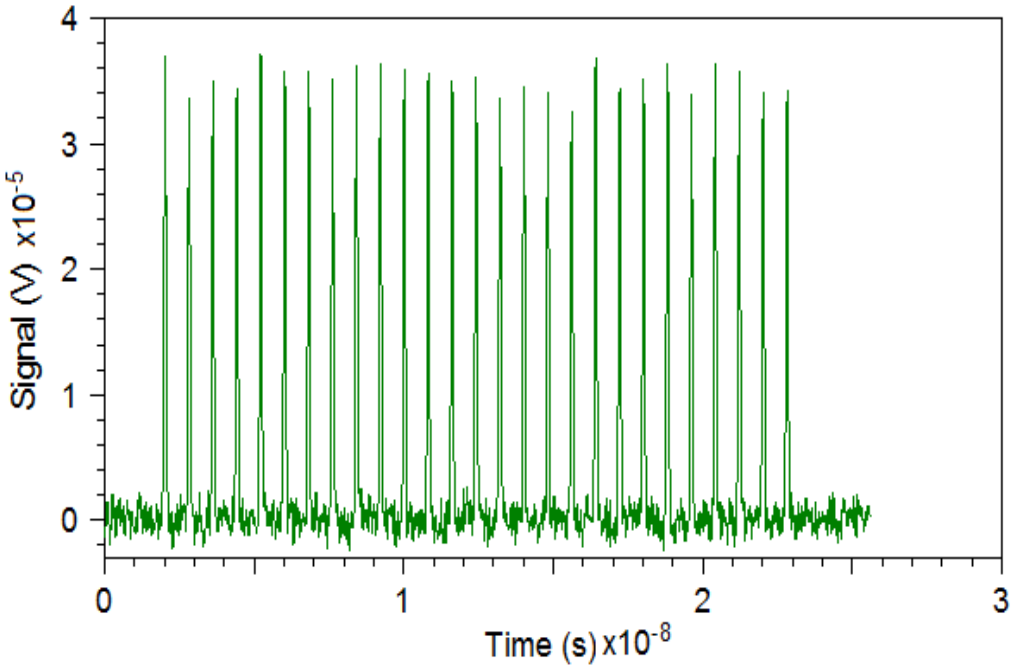


Figure 3.18: Signal at simple energy detector for CSK-OCDMA virtual user scheme

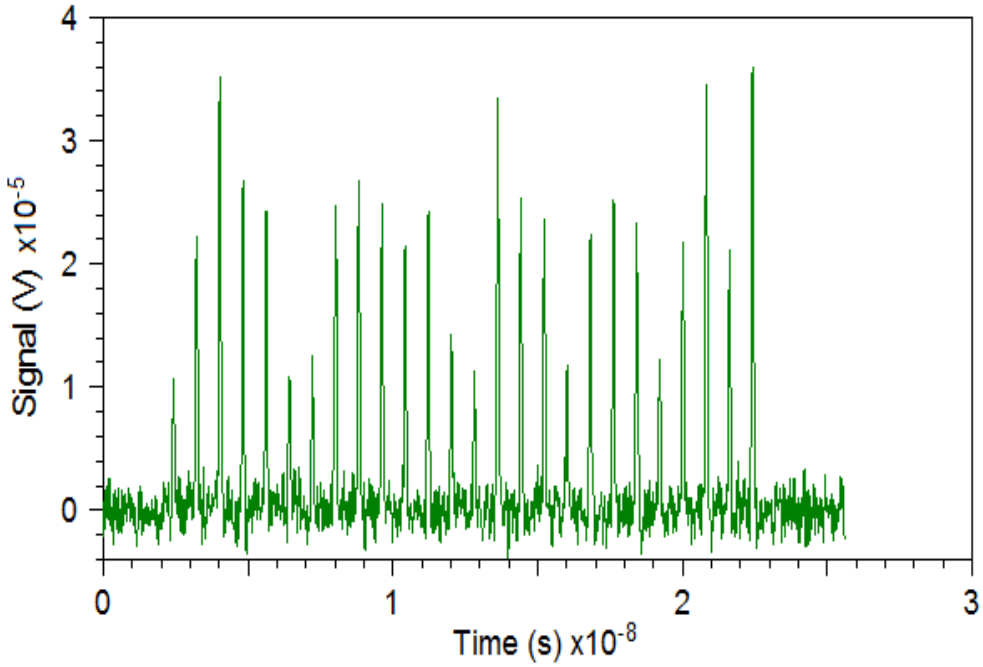


Figure 3.19: Signal at differential eavesdropper for CSK-OCDMA virtual user scheme

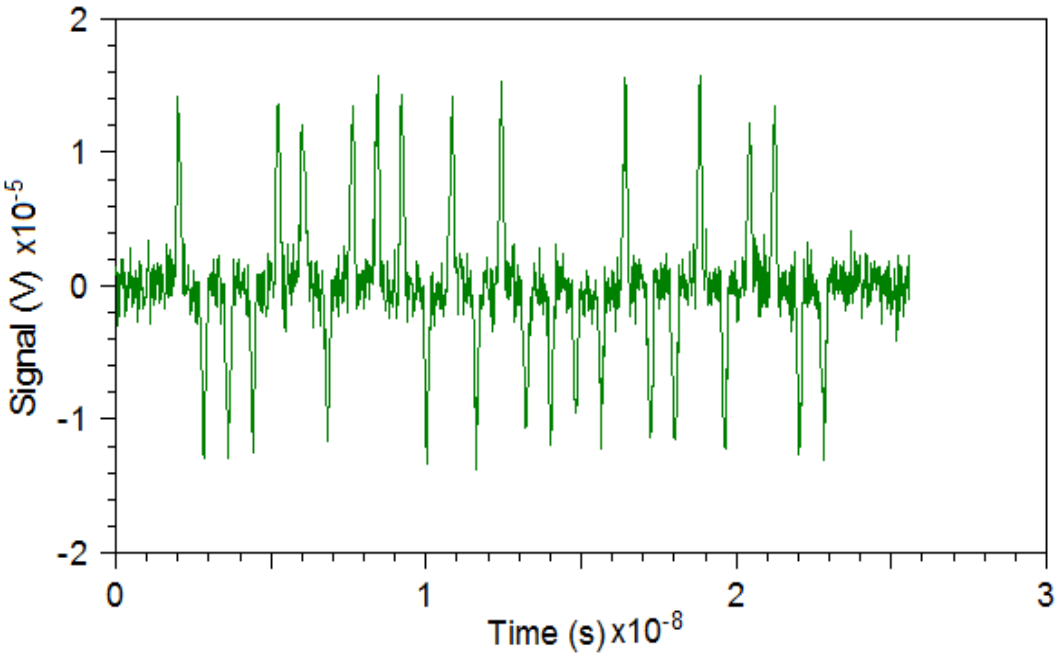


Figure 3.20: Received signal for CSK-OCDMA virtual user scheme

Further, for both CSK and virtual user CSK, the variation of the eavesdropper's BER with respect to received power is shown in figure 3.21. It is seen that the BER for conventional CSK at the differential interceptor is low which decreases further with the increase in received power, whereas, the BER for the virtual user CSK is high and remains unchanged with an increase in received power. This confirms that the virtual user CSK scheme provides robustness against differential eavesdropping to which the ordinary CSK is susceptible. Low values of BER for the conventional CSK receiver make it possible for the eavesdropper to correctly detect the transmitted information, whereas the high BER using a virtual user scheme suggests that the information is unintelligible to the eavesdropper.

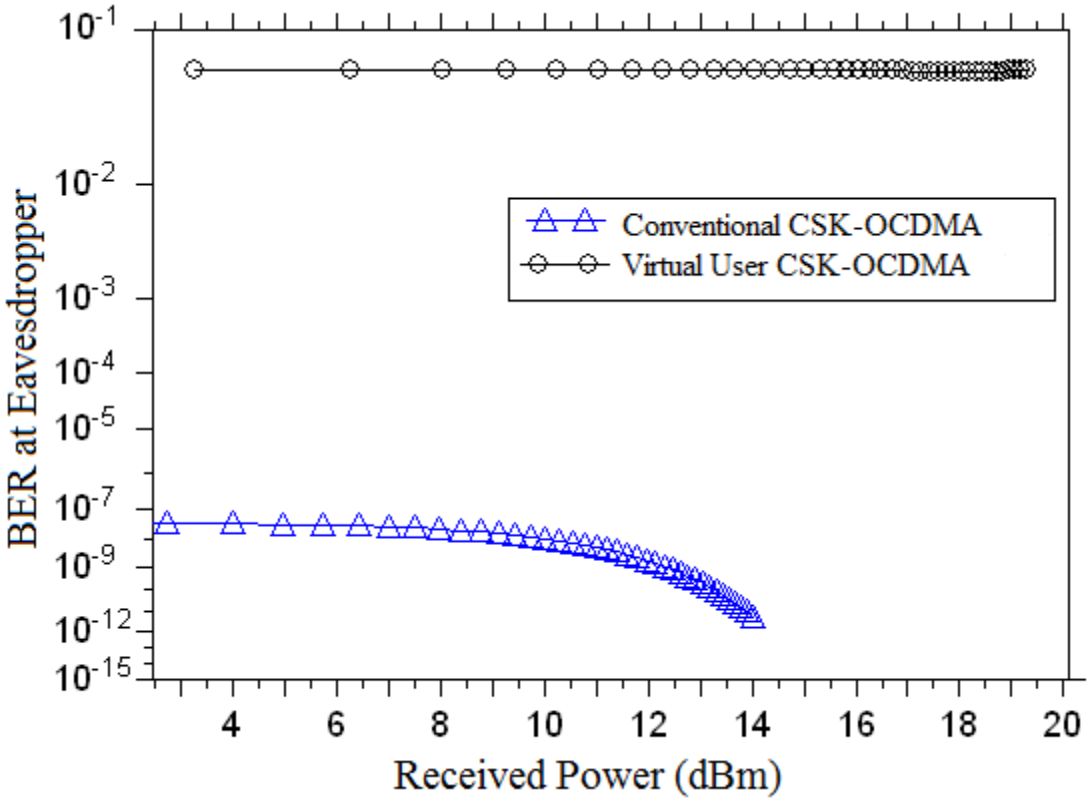


Figure 3.21: BER versus received power at eavesdropper in CSK-OCDMA network

3.6.3 Differential Phase Shift Keying OCDMA

Lastly, DPSK-OCDMA system is simulated with and without proposed virtual user. For both the DPSK-OCDMA and virtual user DPSK-OCDMA schemes, eye diagrams, BER and signals at different locations in the network are measured. The input signal of an authorised user is shown in figure 3.22.

The input spectrum consists of 12 wavelengths as shown in figure 3.23. After applying the ZCC code, only three wavelengths pass through the encoder as shown in figure 3.24. The code weight is 3 and the code length is 12 as justified by the encoded and input spectrum respectively.

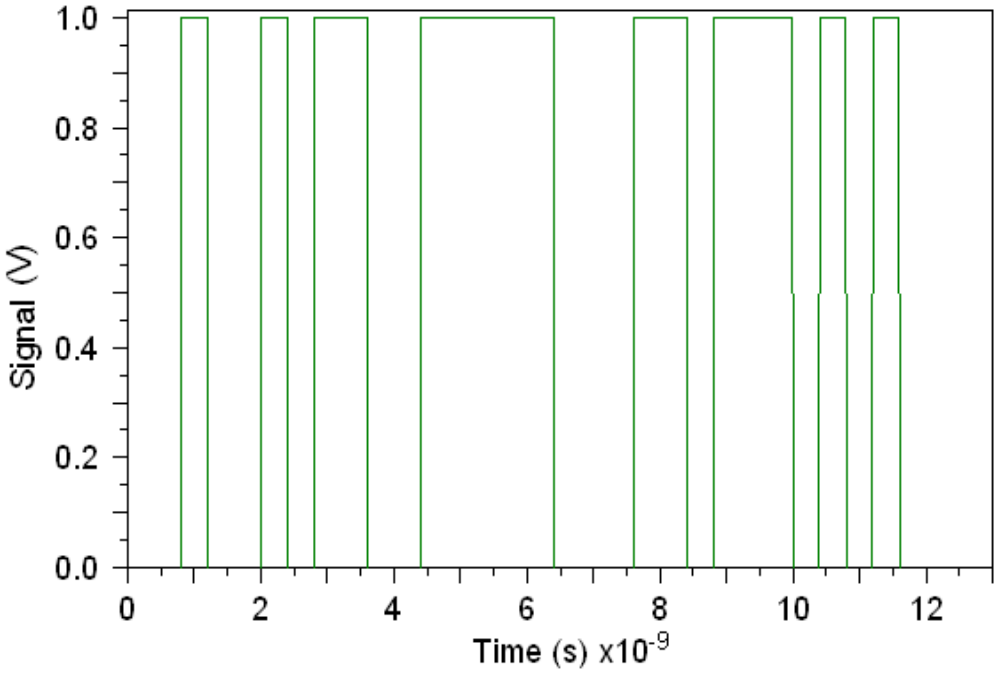


Figure 3.22**:** Input signal of authorised user

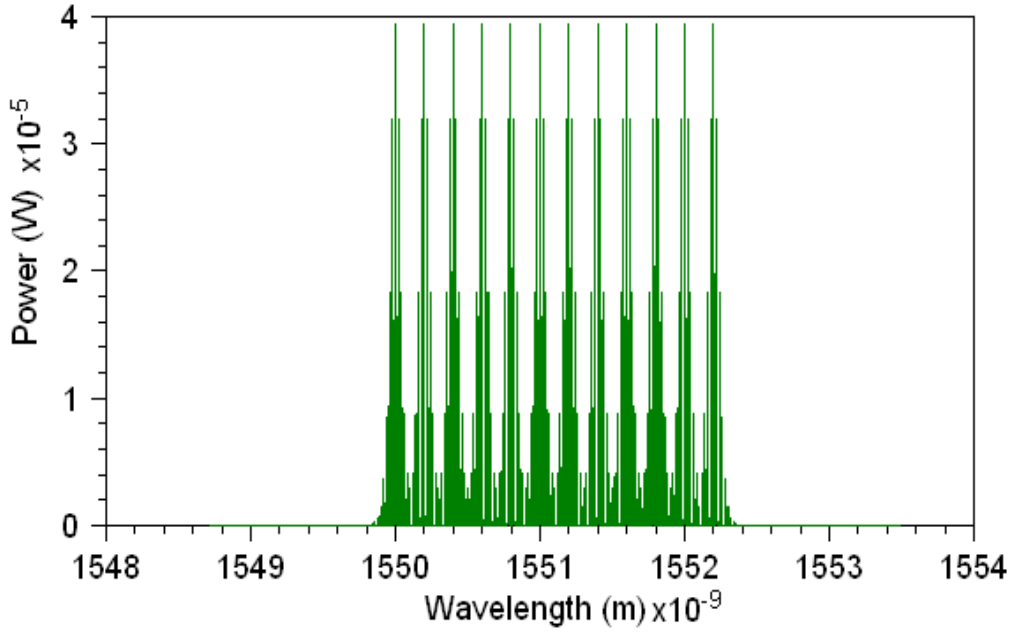


Figure 3.23: Input wavelength spectrum

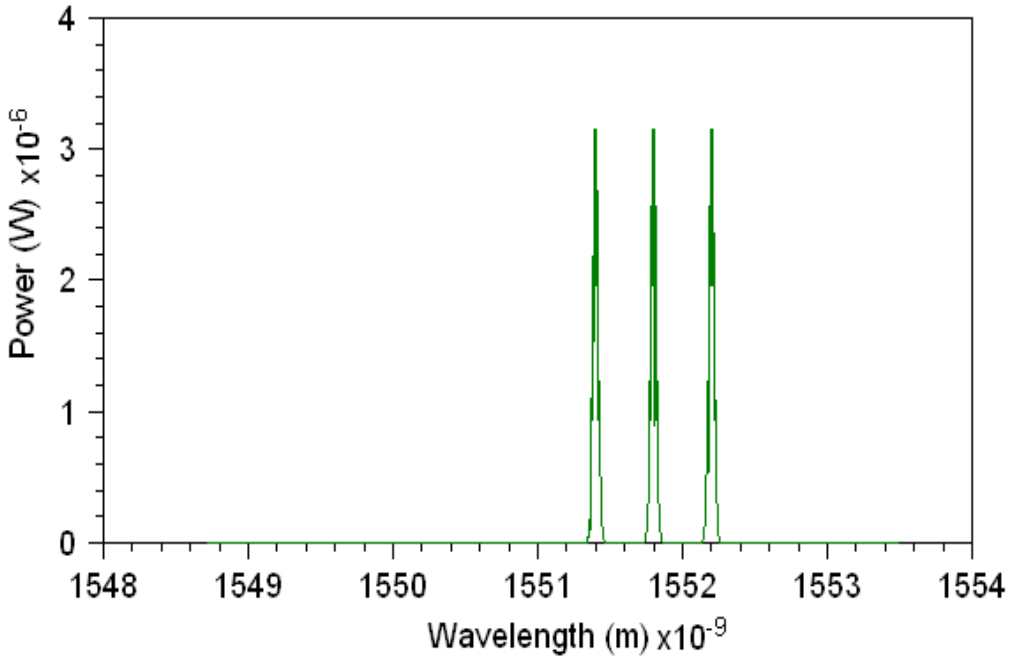


Figure 3.24: Encoded wavelength spectrum

Figure 3.25 shows an eye diagram at the eavesdropper using a simple energy detector when only one user is transmitting. There is no eye opening (which is required) and no intelligible signal is present at the eavesdropper, as shown in figure 3.26. The eye in the diagram is closed because the optical intensity remained constant during all bits, which demonstrates the ability of DPSK-OCDMA system to enhance security. At the differential eavesdropper, differential detection is simulated directly without decoding. In this case, the differential detector clearly decoded the data signal without even knowing the code. A clear eye diagram is observed for the DPSK eavesdropper as shown in figure 3.27, and the detected signal waveform is shown in figure 3.28. At the authorised receiver, differential detection is simulated after the OCDMA decoder. In figure 3.29 also, a clear eye diagram is observed. The received signal is shown in figure 3.30. It can be seen that the signals at the DPSK eavesdropper and the receiver completely overlap each other. This indicates that an eavesdropper can easily intercept the transmitted information by using differential detection. Therefore, the DPSK-OCDMA system is not secure for a single transmitting user in presence of differential eavesdropping.

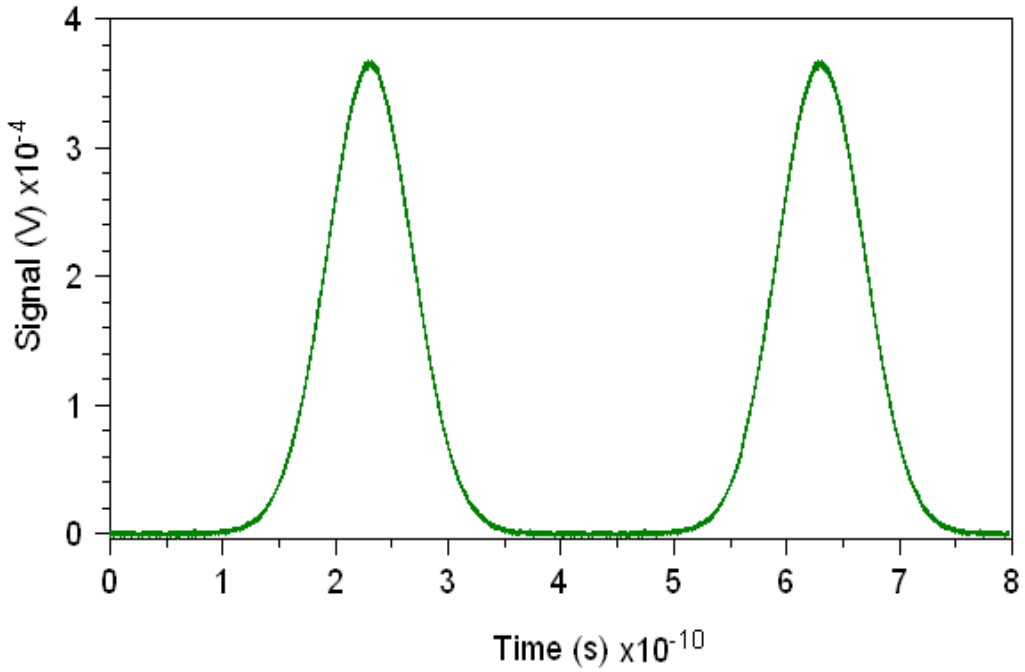


Figure 3.25: Eye at eavesdropper (simple energy detector) for single user DPSK-OCDMA

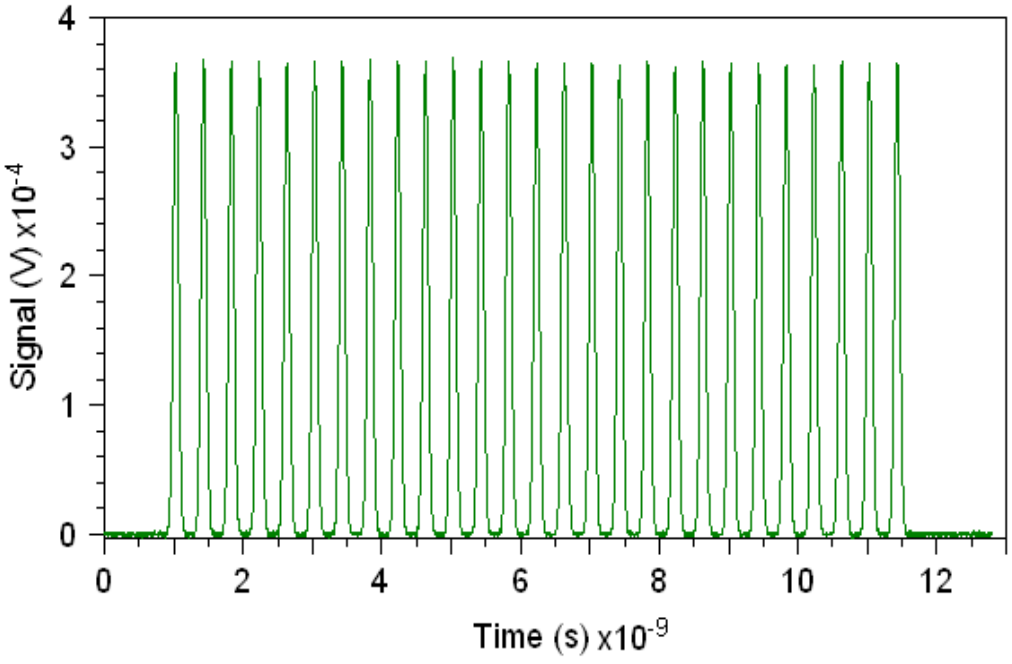


Figure 3.26: Signal at eavesdropper (simple energy detector) for single user DPSK-OCDMA

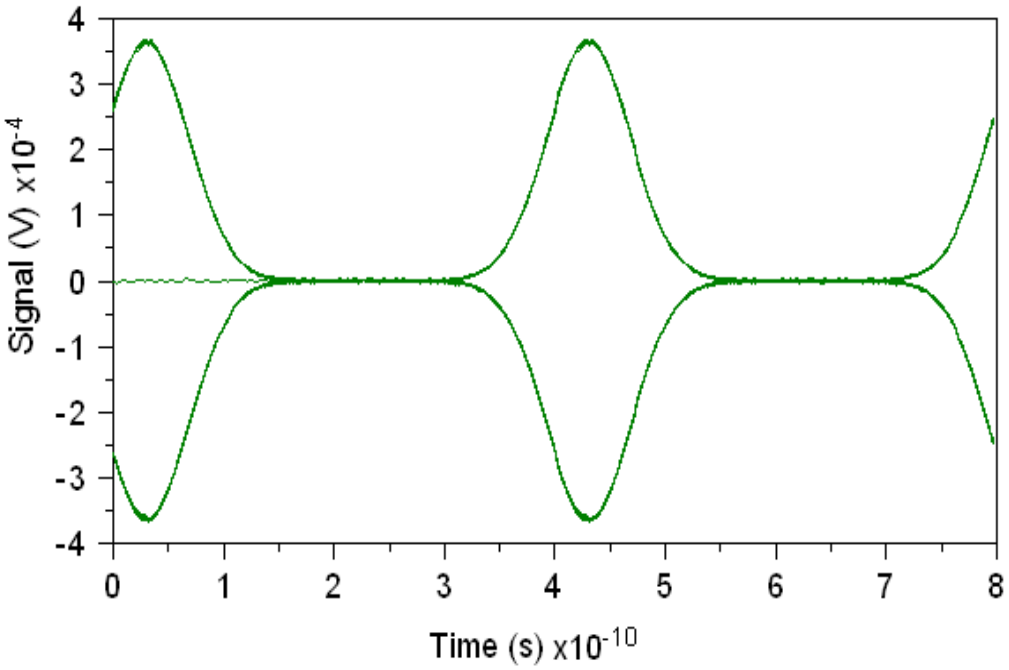


Figure 3.27: Eye at differential eavesdropper for single user DPSK-OCDMA

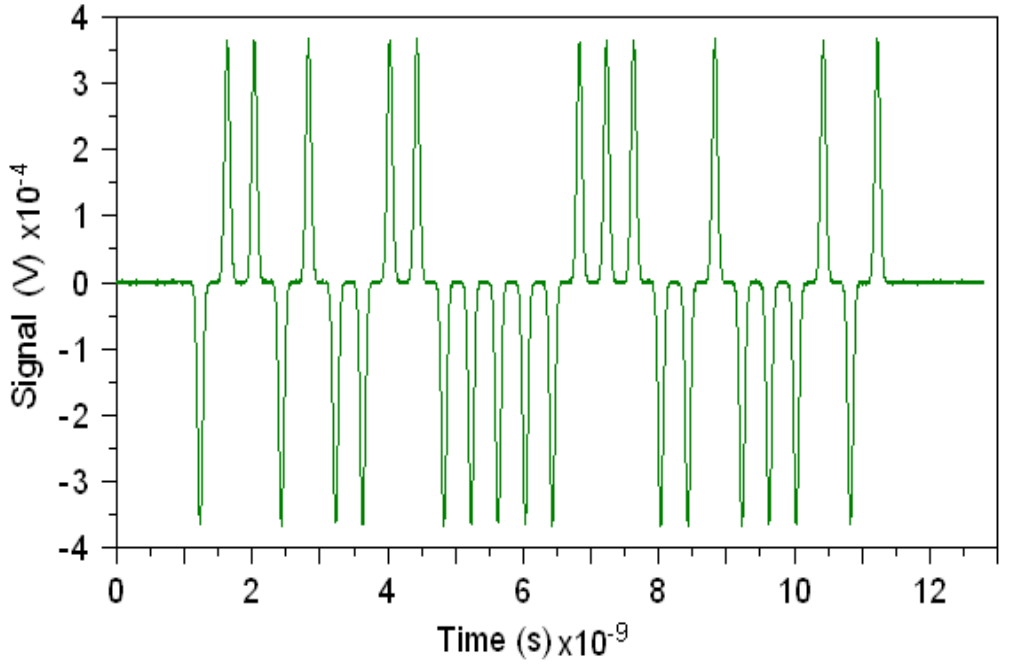


Figure 3.28: Signal at differential eavesdropper for single user DPSK-OCDMA

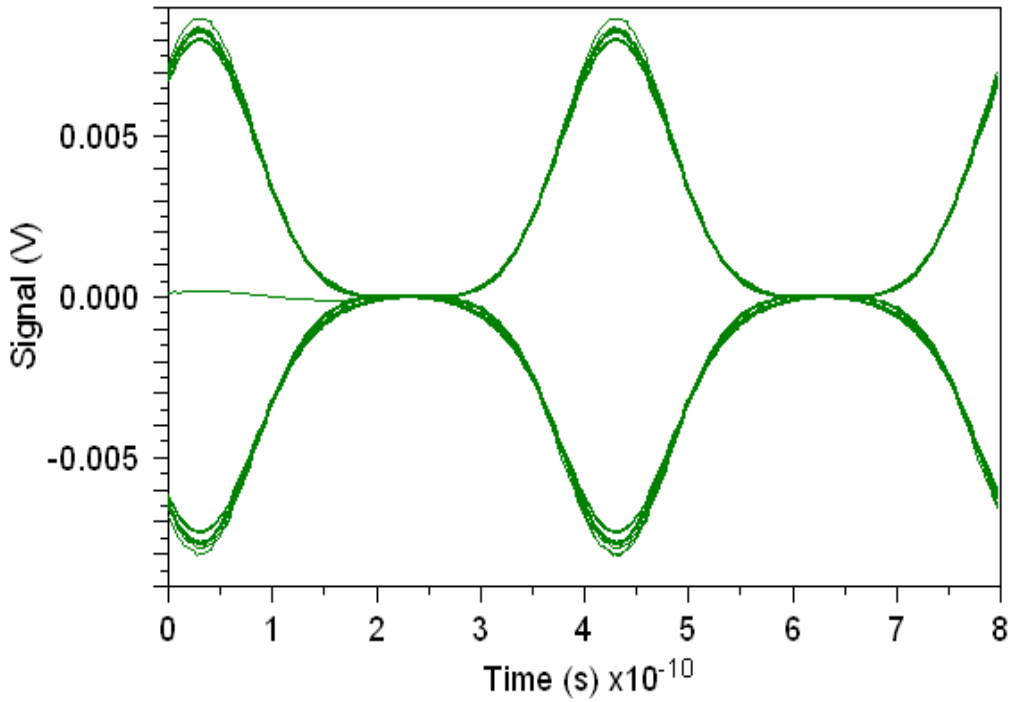


Figure 3.29: Eye diagram at receiver for single user DPSK-OCDMA

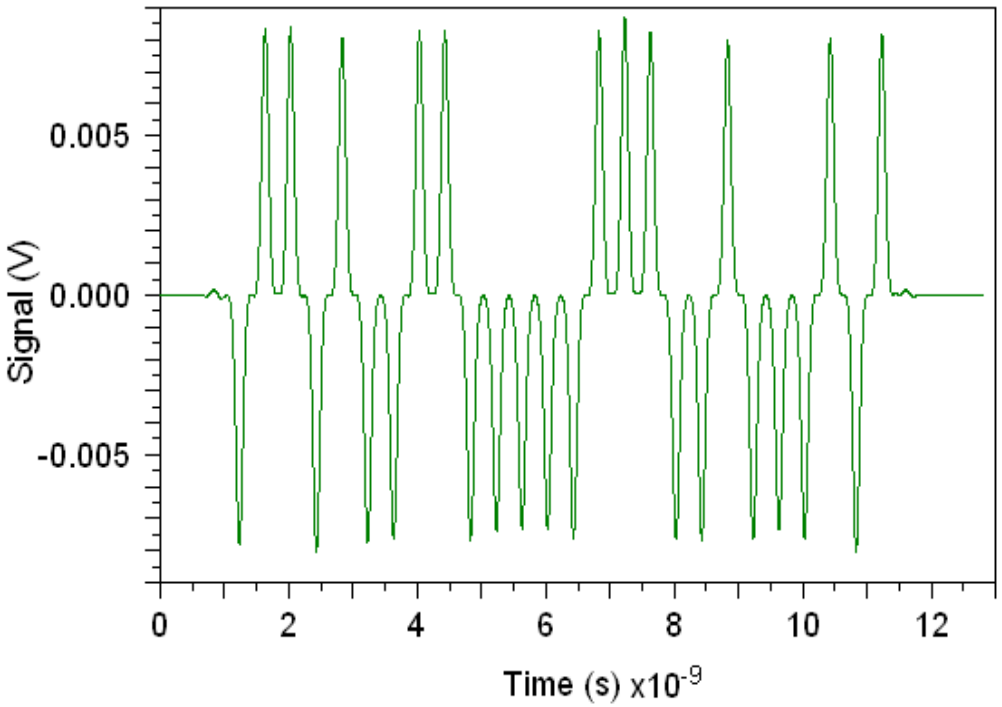


Figure 3.30: Received signal for single user DPSK-OCDMA

For the virtual user scheme where one user is always transmitting in parallel to the authorised user asynchronously, no eye is observed at the simple power detector, as shown in figure 3.31, and the received optical signal had all ones as shown in figure 3.32. Therefore, the data could not be detected by the simple energy eavesdropper. Figure 3.33 and figure 3.34 show the eye diagram and detected signal at differential eavesdropper respectively. The signal present at the DPSK eavesdropper does not overlap the received signal (figure 3.36), which indicates that differential eavesdropper is getting a false data sequence instead of the original one. Figure 3.35 shows that a clear eye diagram is observed at authorised receiver. The virtual user acts as an interferer making it difficult for an eavesdropper to properly decode the signal even when a single user is active in the network.

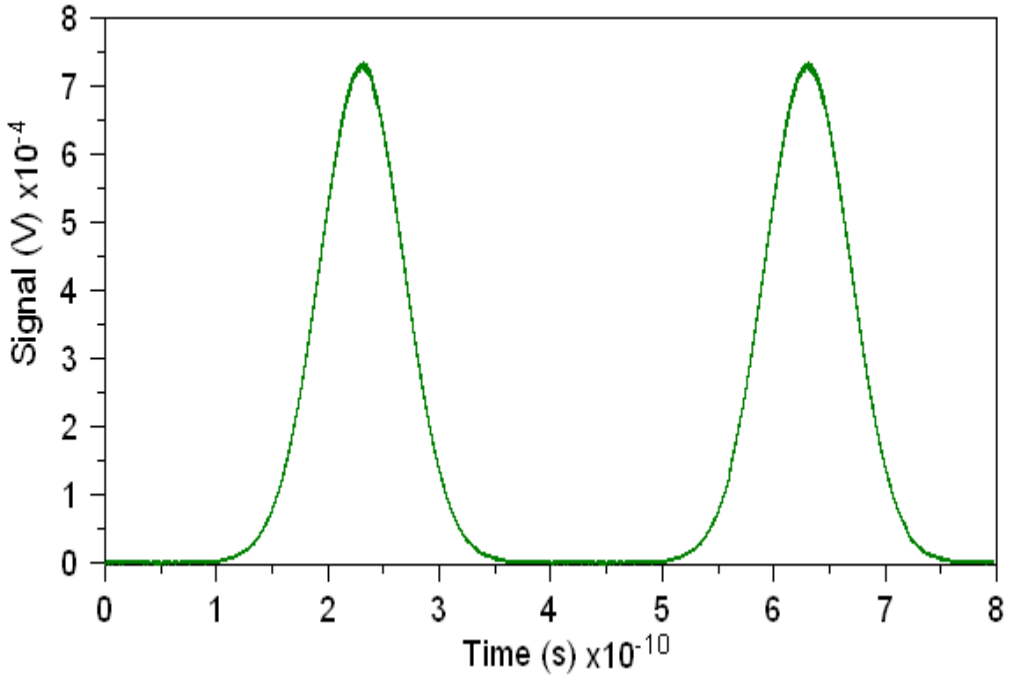


Figure 3.31: Eye at eavesdropper (simple energy detector) for virtual user DPSK-OCDMA

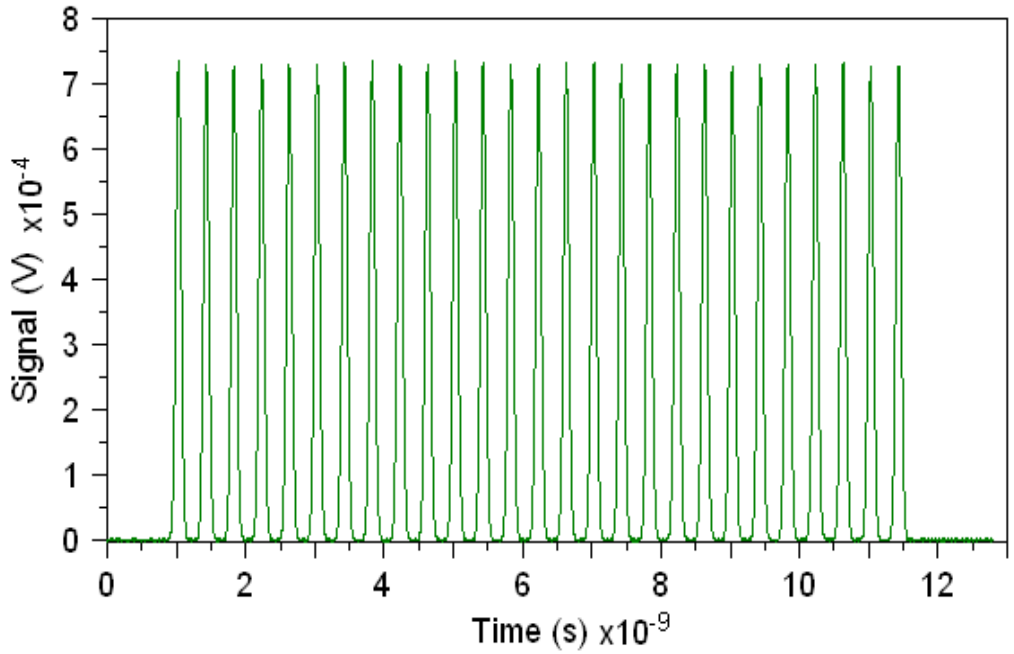


Figure 3.32: Signal at eavesdropper (simple energy detector) for virtual user DPSK-OCDMA

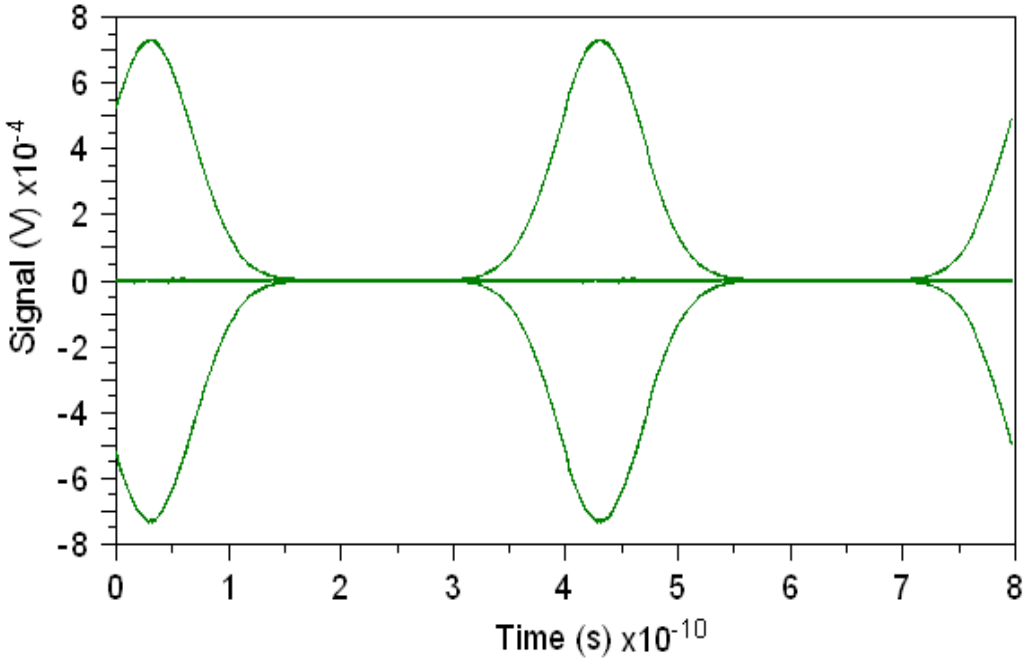


Figure 3.33: Eye at differential eavesdropper for virtual user DPSK-OCDMA

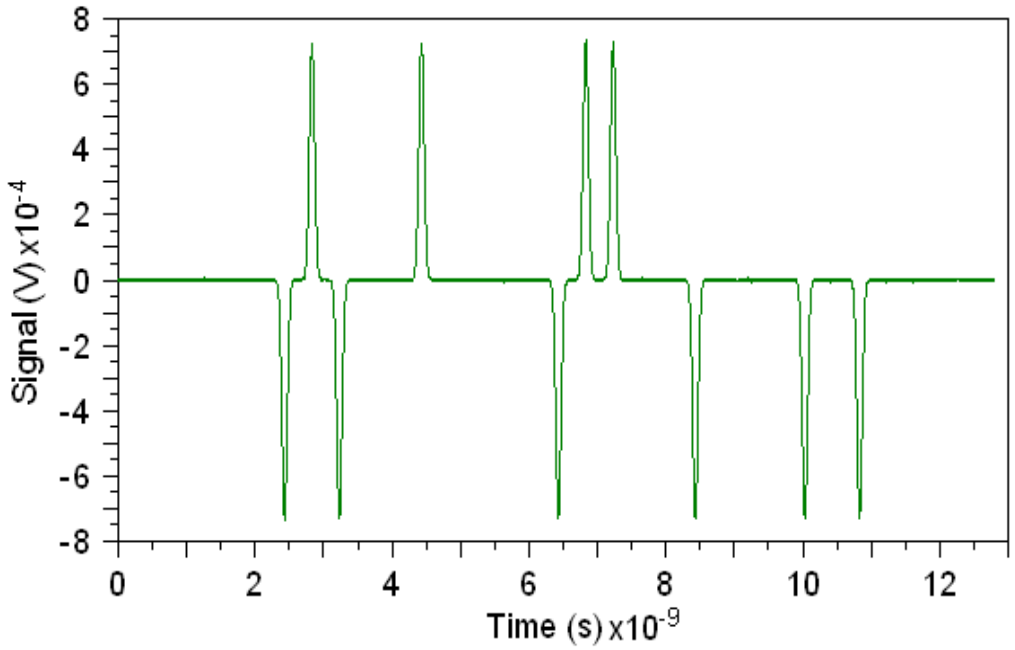


Figure 3.34: Signal at differential eavesdropper for virtual user DPSK-OCDMA

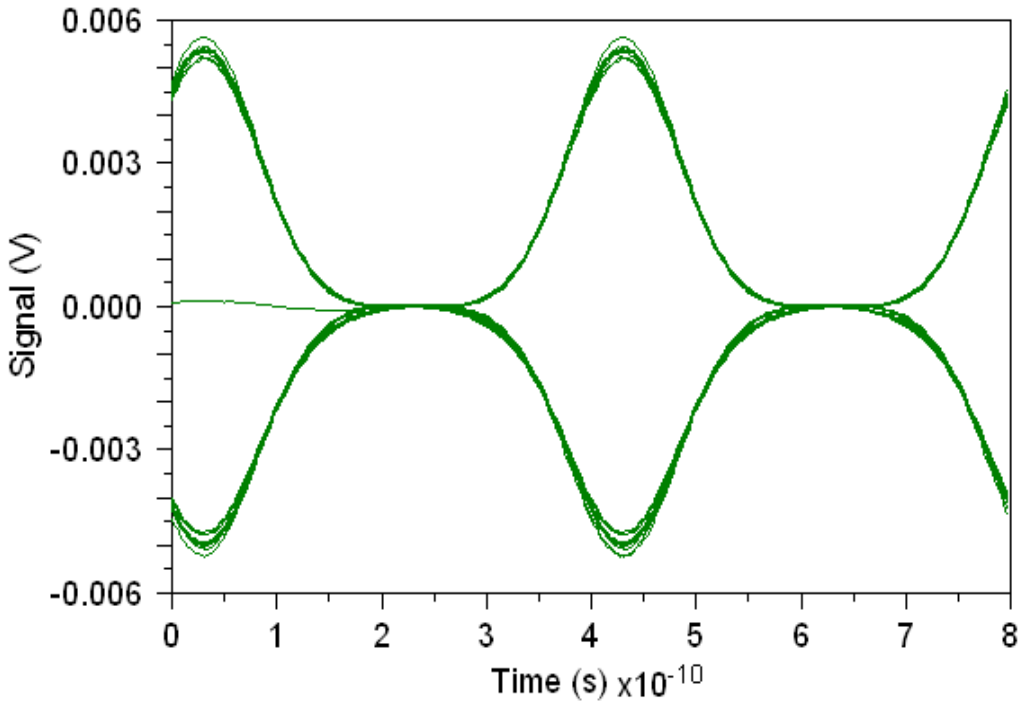


Figure 3.35: Eye diagram at receiver for virtual user DPSK-OCDMA

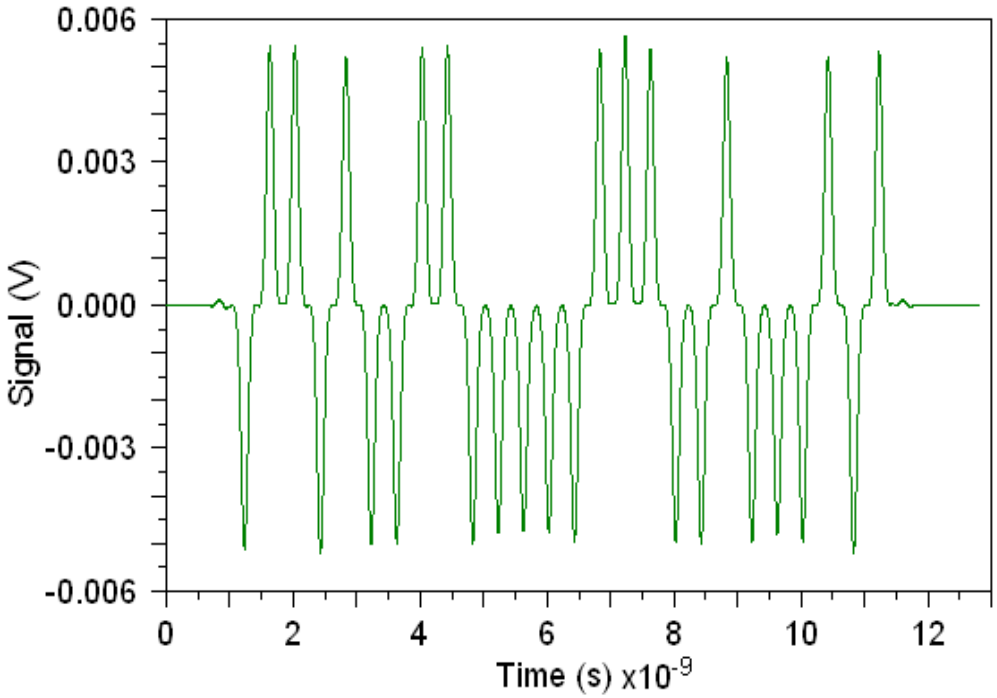


Figure 3.36: Received signal for virtual user DPSK-OCDMA

Further, figure 3.37 shows the variation of BER as a function of input power at 2.5 Gbps for the DPSK-OCDMA network. It can be seen that eavesdropping with the differential detector can be harmful for conventional DPSK scheme as the BER varies from 10^{-9} to 10^{-11} with an increase in input power. This level of BER at the eavesdropper is sufficient to detect the transmitted signal correctly and the user security is compromised. Hence, the conventional DPSK scheme is susceptible to differential eavesdropping. On the other hand, eavesdropping in the presence of the virtual user scheme gives a high value of BER regardless of the input power. Although the virtual user scheme gives a high BER at the eavesdropper, the BER obtained at the authorised receiver is below the threshold level (dotted red line) at all time and thus the information is successfully conveyed without compromising the security. So, it is deduced that implementing the OCDMA system with a virtual user scheme ensures high security against eavesdropping with differential detection without affecting the received signal.

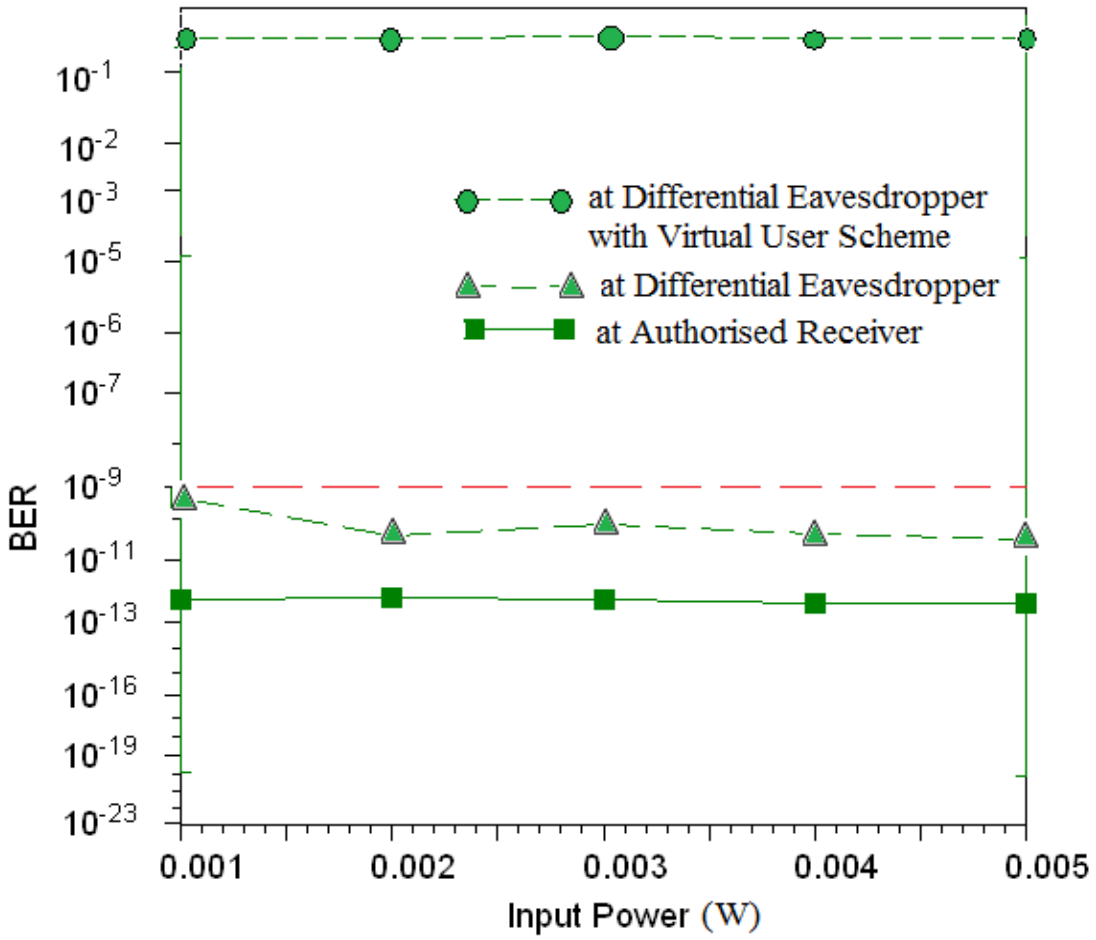


Figure 3.37: BER versus input power in DPSK-OCDMA network with virtual user scheme

3.7 Conclusion

From eavesdropper's point of view, the easiest way to intercept the information is to tap isolated user signals to avoid multiple access interference. To increase the confidentiality of an OCDMA network a novel virtual user technique is proposed and implemented. The proposed scheme never allows an eavesdropper to isolate a single user's signal even when all the other users are dormant. A virtual user alongside an actual user in an OCDMA system mimics multiple access interference to make eavesdropping difficult. The proposed technique is simulated with OOK-OCDMA, CSK-OCDMA and DPSK-OCDMA. The results obtained for the proposed technique are compared with the existing schemes. OOK-OCDMA is vulnerable to simple power detector while CSK and DPSK-OCDMA are vulnerable to differential eavesdropping. The results obtained show that the virtual user scheme is very effective in enhancing the security of

OCDMA network against both the simple power detector and differential eavesdropper for all the modulation formats. Hence, the scheme clearly increases the confidentiality of an OCDMA network without affecting the system performance or incurring any additional bandwidth penalty as compared to conventional OCDMA system.

Chapter 4

Security Enhancement of OCDMA System against Jamming

After improving the data confidentiality of OCDMA network against eavesdropping in the previous chapter, the attack method addressed in this chapter is jamming. This chapter deals with the second objective of the research work which is to propose a technique to increase the availability of signal against jamming.

4.1 Introduction

Security and reliability are two important properties of today's networks. While reliability of a network is concerned with accidental faults, security deals with malicious attacks. OCDMA can be attacked at the physical layer of the network by launching an interfering signal to jam the system. Jamming is defined as the process of overpowering of authorized user's signals with the jammer signals to disrupt communication [28]. Jammer is a hostile communicator that transmits the interfering signal over the same communication range as that of the legitimate user. Jamming signals are threat to signal availability which can degrade the performance of OCDMA system [28]. Signal availability means that information transmitted over the fiber is not lost and is available at receiver [39, 45]. Hence, signal availability is a major concern against the forceful shutdown of communication called jamming.

Till date the different techniques proposed for jamming resistance are: wavelength conversion based on four wave mixing in short length Bismuth non linear fiber (Bi-NLF) [66, 67], code conversion using periodically poled LiNbO3 waveguides [68], self phase modulation of pulses through fiber. Each technique has its own limitations. 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 [81]. Additionally, bismuth-based fibers exhibit large propagation loss which is intrinsic to the material, i.e. bismuth-oxide [82]. 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 [83]. Therefore, based on the above

discussion an efficient anti-jamming technique is required which ensures signal availability at high jammer power.

In this chapter, the OCDMA network with jammer is modeled first. Then a novel technique is proposed for jamming resistance. The technique proposed to avoid jamming attack is based on the use of wavelength conversion through four-wave mixing by exploiting the nonlinearities in semiconductor optical amplifier. Then the optimization of SOA is done for the maximum four wave mixing and efficient wavelength conversion process. The proposed technique is implemented and simulated with the OCDMA system. The results obtained for the proposed anti-jamming technique are compared with OCDMA system without any jamming resistance.

4.2 OCDMA Network with Jammer

In this section, an OCDMA network is modeled with jammer as shown in figure 4.1. The effect of jammer is studied for a single OCDMA user, where jammer is transmitting at the same waveband as that of the desired user. While other OCDMA users are also transmitting, their signals are considered to be contributing only as multiple access interference. Jammer is transmitting 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 [65]. Jammer can jam the system either by flipping some message bits or by overpowering the original message.

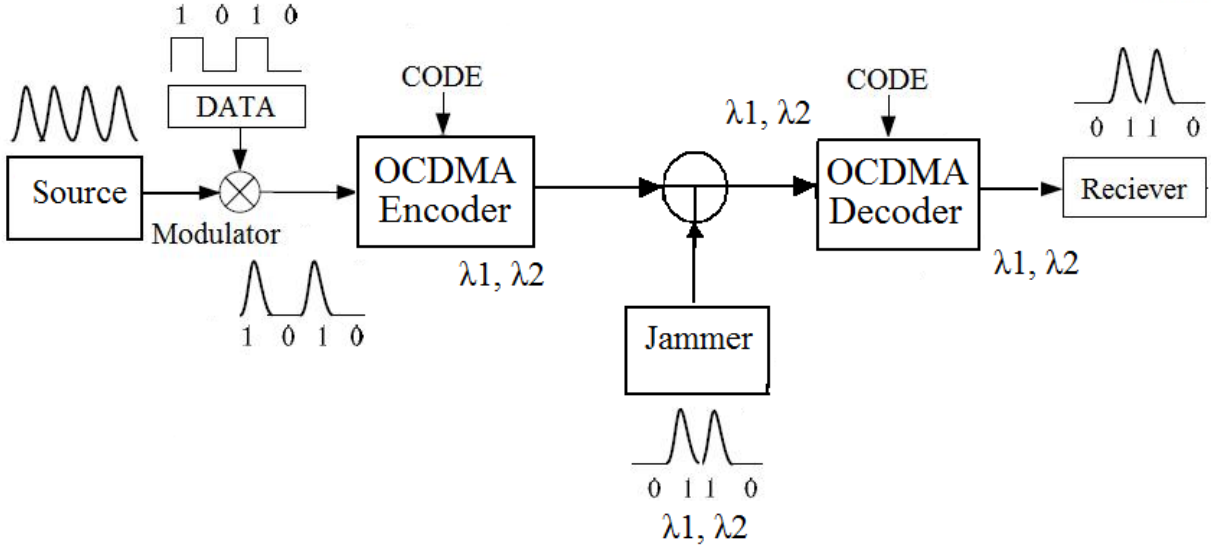


Figure 4.1: OCDMA network with jammer

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 as depicted in figure 4.1. It shows that the task of the attacker has been achieved and the communication is disrupted, making the jamming successful.

4.3 Proposed System Model for Security Enhancement against Jamming Attack

It has already been proven in the literature that 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 message [67, 84]. But, previously proposed wavelengths converters for anti-jamming in OCDMA suffers from many disadvantages as discussed in section 4.1.

Therefore, a novel technique proposed to achieve anti-jamming in OCDMA network is based on the use of wavelength conversion process through four-wave mixing by exploiting the nonlinearities in SOA.

4.3.1 Wavelength Conversion through FWM in SOA

In wavelength converters, basically the physical properties of a nonlinear element are used to perform the conversion function [83]. 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 [83,85,86]. The FWM in semiconductor optical amplifier for wavelength conversion is taken into account for the first time with OCDMA.

Semiconductor optical amplifiers are essentially semiconductor lasers with anti reflection coating on the chip facets to reduce light reflections into the circuit. In SOA, three physical mechanisms which are carrier density modulation, dynamic carrier heating and spectral hole burning form a grating which leads to the generation of new frequency components due to the interaction of injected waves with these grating. Carrier density modulation is a inter-band process which relates to the transitions between the conduction and the valence band where as dynamic carrier

heating and spectral hole burning are the intra-band process which refer to carrier–carrier and carrier–phonon scattering changing the carrier distribution within one band [87].

The nonlinear gain dynamics in SOA are responsible for the process of four wave mixing. FWM arises from a nonlinear optical response of the medium when more than one wave is present [88,89]. The outcome of FWM is the generation of a signal at a further frequency whose intensity is proportional to the product of the interacting wave intensities as shown in (4.1) [90,91]

$$\omega_c = 2\omega_p - \omega_s, \tag{4.1}$$

where, ω_c is converted frequency, ω_p is the pump frequency and ω_s is the signal frequency.

The converters based on SOA have the advantages of compactness and low energy requirements to trigger their nonlinearity. Moreover, FWM based conversion process is non inverting and transparent to bit rate and modulation format [88]. They allow conversion over a wide range of wavelengths and provide amplifying regenerative wavelength conversion [88,92,93]. They have high conversion efficiency (η).

Conversion efficiency is defined as the ratio of the converted signal power at output to the signal power at input to SOA as shown in (4.2) [87],

$$\eta = \frac{P_C(L)}{P_S}, \tag{4.2}$$

where, $P_C(L)$ is the converted signal power at SOA output after FWM and P_S is the input signal power.

FWM in SOA has a high intrinsic efficiency as compared to Bi-NLF converters which suffer from two kinds of losses, propagation loss and splice loss [82]. SOA based wavelength converter requires moderate pump power and short lengths as compared to previously proposed PPLN based converters [83]. Therefore, based on the above discussion, it is clear that SOA based wavelength conversion is more beneficial than other wavelength conversion methods.

However, one limitation of using SOA based wavelength conversion is the amplified spontaneous emission (ASE) noise. In order to quantify the noise performance of an SOA, Signal

to background ratio (SBR) is a useful parameter. It is the ratio of converted signal power (Pc(L)) to the noise power of converted signal ($P_N(L)$) at SOA output after FWM as defined in (4.3) [87]

$$SBR = \frac{P_C(L)}{P_N(L)}, \tag{4.3}$$

This drawback is counterbalanced by the compactness of SOA based devices, which enables integration. Hence, the FWM in SOAs is attractive as a wavelength conversion technique, despite the added ASE.

4.3.2 Proposed System Model

Figure 4.2 shows the same OCDMA network as figure 4.1 but with the proposed anti-jamming technique. In the proposed scheme, a wavelength converter is incorporated in the network after the encoder. To achieve anti-jamming, the transmitted signals are passed through an SOA based wavelength converter.

The wavelengths of the transmitted signals are transformed to a different set of wavelengths due to FWM in the SOA. The jammer is not aware of the wavelength converter and keeps transmitting at the authorized user's wavelengths at high power. Due to its high power the attacker will try to superimpose its signal on the legitimate user message but in vain. This is because the wavelength converter has already converted the user's wavelengths to some other set of wavelengths. Now the data will be carried at the converted wavelengths. Unlike figure 4.1, figure 4.2 clearly shows two sets of wavelengths being transmitted through the system, out of which one is the transmitted information and the other is the jammer signal.

The signal received at the OCDMA decoder consists of jammer signal (original wavelengths) and the transmitted signal (converted wavelengths). Here, a band pass filter (BPF) is incorporated to remove the jammer signal and retain the converted signal. Since, the decoder is not aware of the wavelength conversion process; it is incapable of decoding the received information at the converted wavelengths. To convert back the signal at the output of BPF, a wavelength deconverter is used. It will translate the data from the converted wavelengths to the original set of wavelengths which was used for encoding at the transmitter side.

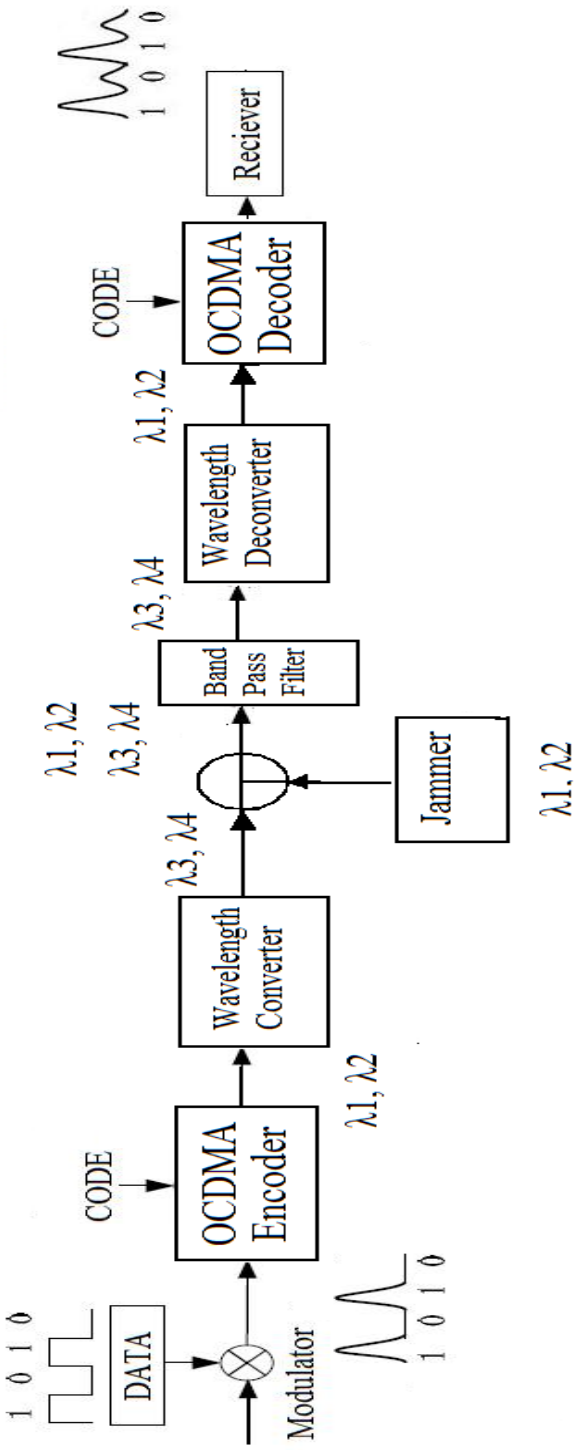


Figure 4.2: OCDMA network with wavelength converter to avoid jamming

Then, the signal is fed to the decoder to retrieve the original data according to the unique code shared by a particular transmitter and receiver pair. For further processing a photodiode is used after decoder for optical to electrical conversion.

Moreover, a wavelength converter based on FWM in SOA can be used for conversion of many wavelengths simultaneously, known as waveband converter. This attribute indicates that a single SOA based waveband converter can replace a number of wavelength converters based on previously proposed techniques, reducing the component count in an optical communication network [94]. Since, a single SOA can achieve waveband conversion as opposed to multiple existing wavelength converters, the overall system cost and complexity will be lower as compared to the previously proposed techniques.

4.3.3 Wavelength Converter as Anti-jammer

The wavelength conversion right after the transmitter in an OCDMA network helps to avoid jamming attack. The detailed block diagram of SOA based wavelength converter is shown in figure 4.3. This will translate the input signal out of jamming window according to the pump wavelength. The converter's optical pump source is a tunable, continuous wave Lorentzian laser. By changing the pump wavelength of SOA, the output wavelength can be changed easily. The pump and OCDMA encoded signal are then combined by an 80/20 coupler which is further amplified in a high power erbium-doped fiber amplifier (EDFA), with an output power of about 21 dBm.

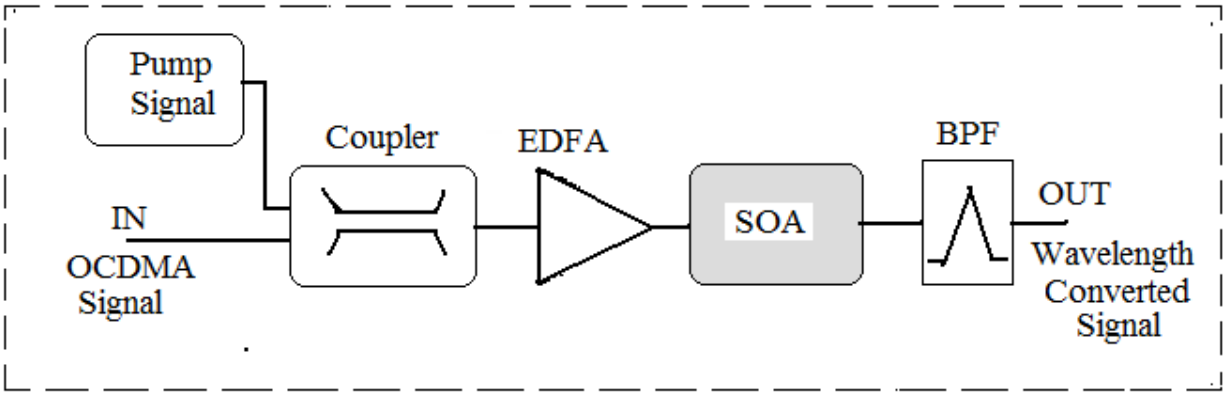


Figure 4.3: Wavelength converter setup based upon FWM in SOA

Then the amplified signal is launched into SOA where FWM takes place and generates the converted signal. The pump wave scatters in SOA to generate the two waves, one at the original frequency and one at a new frequency [95]. At the output of SOA, the pump and the original signal are suppressed using tunable band pass filter centered on the converted signal [96].

4.4 Simulation Setup for OCDMA System with Proposed Anti-jamming Technique

The simulation model for OCDMA system using SOA as a wavelength converter for anti-jamming is shown in figure 4.4. The continuous wave lasers (with input power 0.01 mW) having wavelength range 1548 nm to 1552.8 nm are used to create the carrier signal with wavelength spacing of 0.8 nm. The carrier signal is then spectrally encoded using the optical orthogonal codes. The construction of OOC codes is given in reference [97]. The use of OOCs enables a large number of asynchronous users to transmit information efficiently and reliably. The OCDMA encoder of a particular user uses the wavelengths 1548 nm and 1551.2 nm for encoding. The NRZ data is pseudo random binary sequence with word length of 2^5-1 at a bit rate of 2.5 Gbps. The data to be transmitted is modulated on an optical CDMA sequence at the modulator. The modulated data is then sent to the wavelength converter before being combined with jammer signal in the optical fiber.

The wavelength converter first combines the input encoded data signal with the optical pump source. The converter's optical pump source is a tunable, continuous wave Lorentzian laser operates at wavelength 1555 nm with the input power of 0.1 mw. All the wavelengths of the encoded input signal are demultiplexed before being combined in the SOA. Each wavelength of the encoded signal is multiplexed with the pump signal and then amplified by an EDFA. The amplified signal is launched into SOA where FWM takes place and the converted signal is obtained at wavelengths 1558.8 nm and 1562 nm.

The standard InGaAlAs traveling wave SOA is taken as the amplifier model. The simulation parameters of SOA as a wavelength converter in FWM mode are given in Table 4.1. At the output of SOA, BPF tuned to the converted wavelengths is placed to filter out the wavelengths 1558.8 nm and 1562 nm.

Along with this, a jammer is incorporated in the network. The jammer is transmitting in the same waveband as the authorized user (1548 nm and 1551.2 nm) with a signal power of 1 mW.

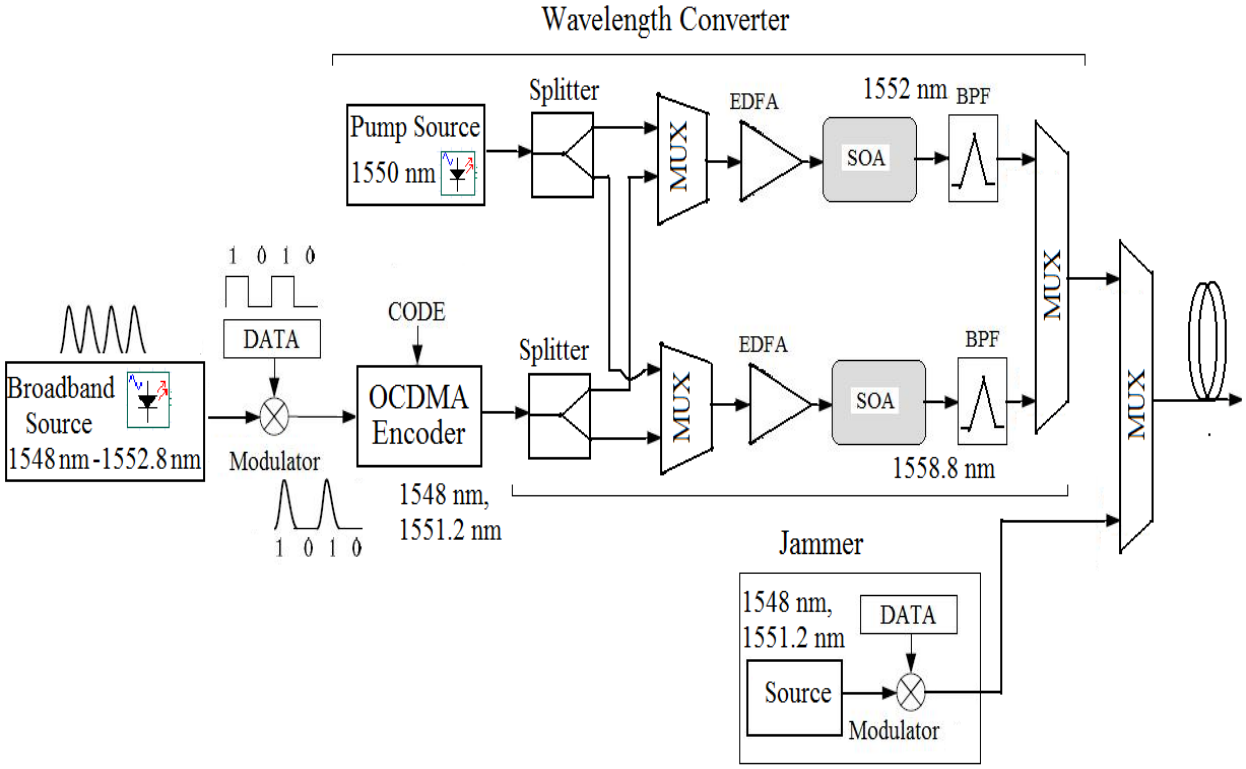


Figure 4.4: Simulation setup of OCDMA transmitter with proposed anti-jamming technique

Table 4.1: Simulation parameters of SOA for FWM

Parameter	Value
Volume of Active layer	210 μm^3
Confinement factor	0.3
Transparency carrier Density	1×10^{18} cm^{-3}
Material Gain Constant	3×10^{-16} cm^2
Bias Current	450 mA
Spontaneous Carrier Lifetime	0.3 ns
Line width Enhancement Factor	3
Material Loss	10.5 cm^{-1}
Input/Output Insertion Loss	3 dB

As shown in figure 4.5, both the original signal (transmitted at 1558.8 nm and 1562 nm) and the jammer signal (at 1548 nm and 1551.2 nm) are received at the band pass filter. The BPF blocks the jammer wavelengths and lets the converted wavelengths pass through to the wavelength deconverter. The wavelength deconverter setup is same as the wavelength converter setup shown in figure 4.3 with the same pump wavelength used at transmitter side. The wavelength deconverter will translate the data on the received wavelengths to the original set of wavelengths which were used for encoding at the transmitter side. These wavelengths are then fed to the decoder which uses the same codeword as the encoder, to decode the signal. Hence, the message is successfully retrieved even in the presence of the hostile jammer.

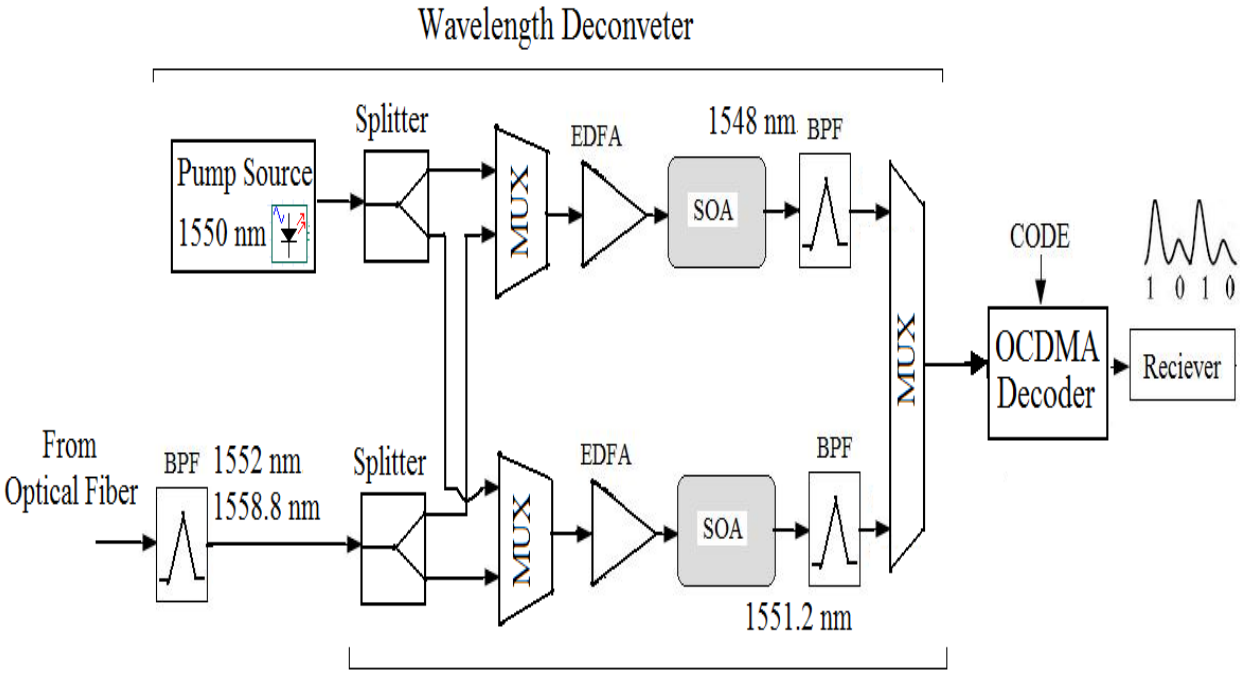


Figure 4.5: Simulation setup of OCDMA receiver with proposed anti-jamming technique

Moreover, the pump in the proposed wavelength converter is tunable, which means that the converted wavelengths can be easily changed at anytime by changing the pump wavelength. Tunable pump is especially useful in the case when jammer changes its wavelengths. Hence, it adds flexibility in the proposed system by making it more resistant against the flexible jammer.

4.5 Optimization of SOA for Effective Wavelength Conversion

The optimization of SOA is done for effective four wave mixing in order to improve the efficiency of wavelength converter. The various parameters of SOA considered for its performance optimization as a wavelength converter are optical confinement factor (OCF), injection current and active region length.

Firstly, the optimization of optical confinement factor is done by keeping other parameters of SOA fixed while varying the OCF. It is found that with the increase in OCF, the four wave mixing effect becomes more pronounced. This happens due to gain variations in SOA. But further increase in OCF value can lead to increase in SOA induced crosstalk. Hence gain saturation of SOA occurs. On the other hand, when OCF is low then the four wave mixing effect

is also low, causing insufficient wavelength conversion. The simulation setup employing wavelength converter setup for anti-jamming in OCDMA system is simulated for different values of OCF. It is observed that the variation of confinement factor from 0.2 to 0.35 produces high quality FWM signal at the output of wavelength converter and minimum BER at receiver. It is best suited for wavelength conversion in an OCDMA network. When OCF is below 0.2, the four wave mixing effect is weak as observed at wavelength converter's output and poor eye diagram is observed at receiver. On the other hand when OCF is greater than 0.35, the four wave mixing effect increases but SOA induced crosstalk also increases. Due to this poor eye diagram with high BER is observed at receiver.

Secondly, the injection current is optimized. Keeping the OCF value between 0.2 to 0.35 and other parameters fixed, injection current is varied. The increase in injection current leads in increase in power levels of FWM signal. At low current values below 250 mA, the FWM effect is weak causing insufficient wavelength conversion. Hence poor eye pattern is observed at low values of injection current. With the increase in input current from 250 mA to 550 mA, FWM effect improves leading to high quality wavelength converted signal. Therefore, this range of injection current is optimal for effective wavelength conversion in OCDMA. At higher current values above 600 mA, gain saturation occurs due to more fluctuations in gain. Hence, a poor eye pattern is observed at the output of wavelength converter.

Further, the injection of light into an SOA varies the carrier density and carrier distribution within the energy bands which results in a modulation of gain and refractive index in the active region of the amplifier. Hence the FWM phenomenon also depends on the length of the active region of the SOA. The optimization of active region length can be done using FWM conversion efficiency. With the increase in active region length above 700μm the conversion efficiency decreases, due to insufficient converted signal power at the output of SOA. At short lengths of 400μm and below, conversion efficiency is high but with poor quality of signal. Hence, at moderate lengths of around 500μm, a clear eye diagram with good conversion efficiency can be obtained.

Based on the above discussion, the OCDMA system with anti-jamming technique is simulated with optimum values of SOA parameters for effective wavelength conversion.

4.6 Results and Discussion

Firstly jammer's performance has been analyzed in OCDMA network. To study the effect of jamming, an ideal receiver is considered and all sources of noise are neglected except MAI. The jammer considered here is pulse band jammer which sends its pulses over entire code wavelengths of the targeted user but for a short period of time. The jammer's performance is analyzed by plotting the BER against jammer's transmission probability as shown in figure 4.6. It shows that as the jammer's transmitting probability increases (i.e. number of jamming pulses increases) then BER at receiver decreases. This is due to the fact as the number of jamming pulses increases then transmitted power per jamming pulse decreases because of constant average jammer power. Further, figure 4.6 shows that high jammer power leads to high BER, increasing the attacking performance of a jammer that causes the original signal to become unreadable by the receiver. Therefore, to maximize the BER at receiver, the jammer should transmit its jamming pulses over a fraction of time with high power rather than sending the pulses all the time.

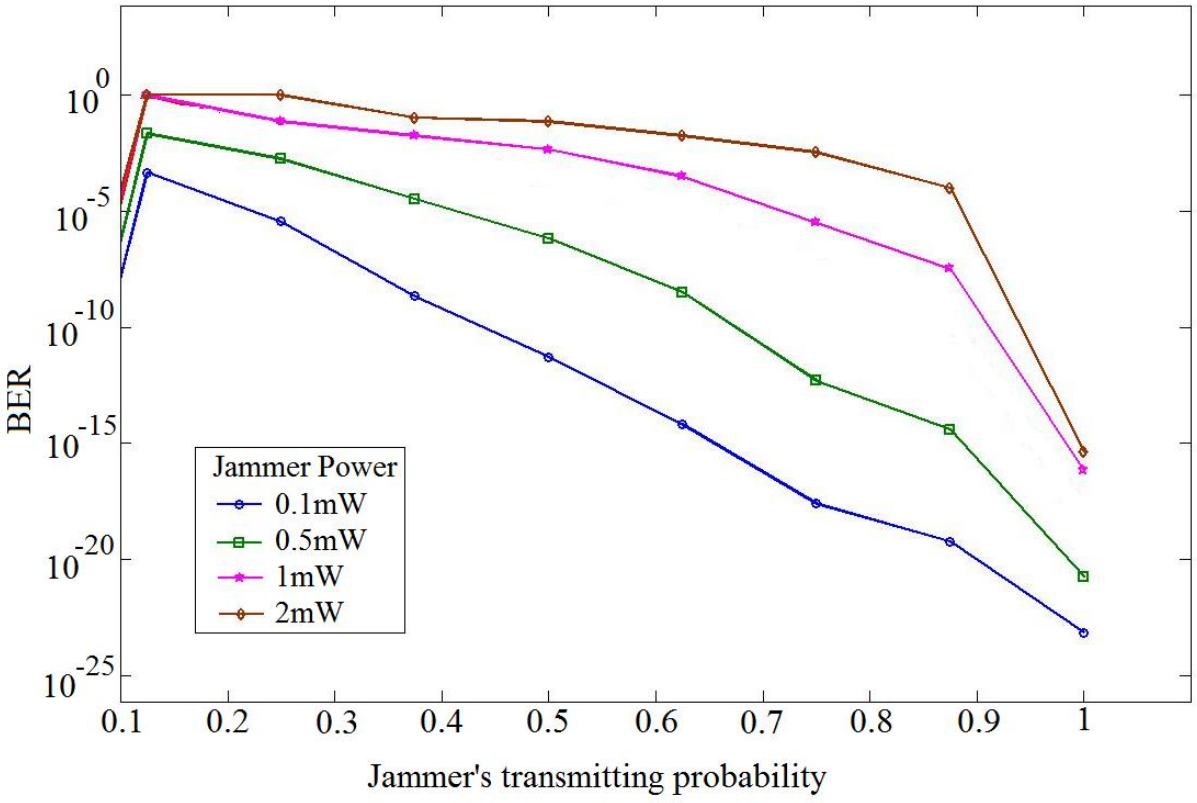


Figure 4.6: BER versus pulse jammer's transmitting probability

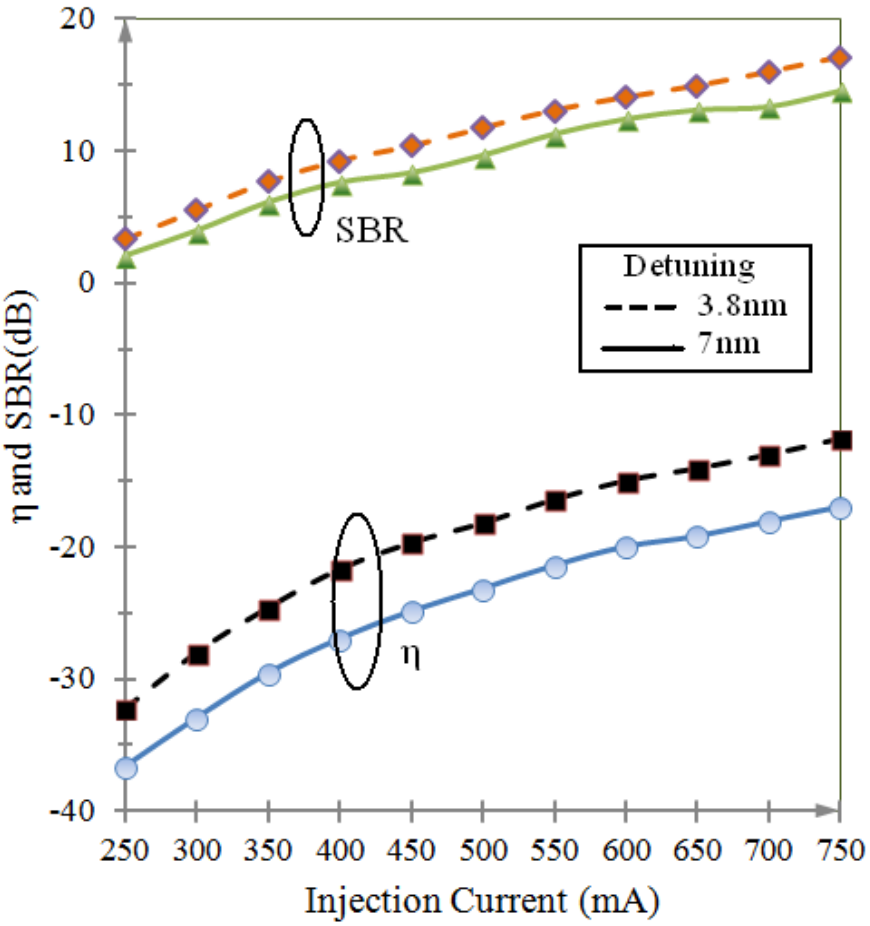


Figure 4.7: Conversion efficiency and SBR versus injection current

After analyzing the jammer effect, the proposed anti-jamming technique based on wavelength conversion using FWM in SOA is simulated with OCDMA. Firstly, the performance parameters of SOA based wavelength converter are considered are conversion efficiency (η) and signal to background ratio. Both, conversion efficiency and SBR are plotted as functions of the injection (bias) current and amplifier length as shown in figures 4.7 and 4.8 respectively. Results show that with increase in bias current, the power level of the FWM signals increases rapidly which leads to increase in its conversion efficiency. However, increasing the injection current also leads to an enhancement of the ASE noise power, whereas increase in FWM signal leads to an increased SBR. On the contrary, the conversion efficiency and SBR decrease with the increase in active region length. Figure 4.7 and figure 4.8 also show the dependence of conversion efficiency and SBR on wavelength detuning between the pump and the input signal. It can be

seen that both the conversion efficiency and SBR decrease with the increase in detuning. High values of η and SBR are observed at detuning of 3.8 nm as compared to 7 nm.

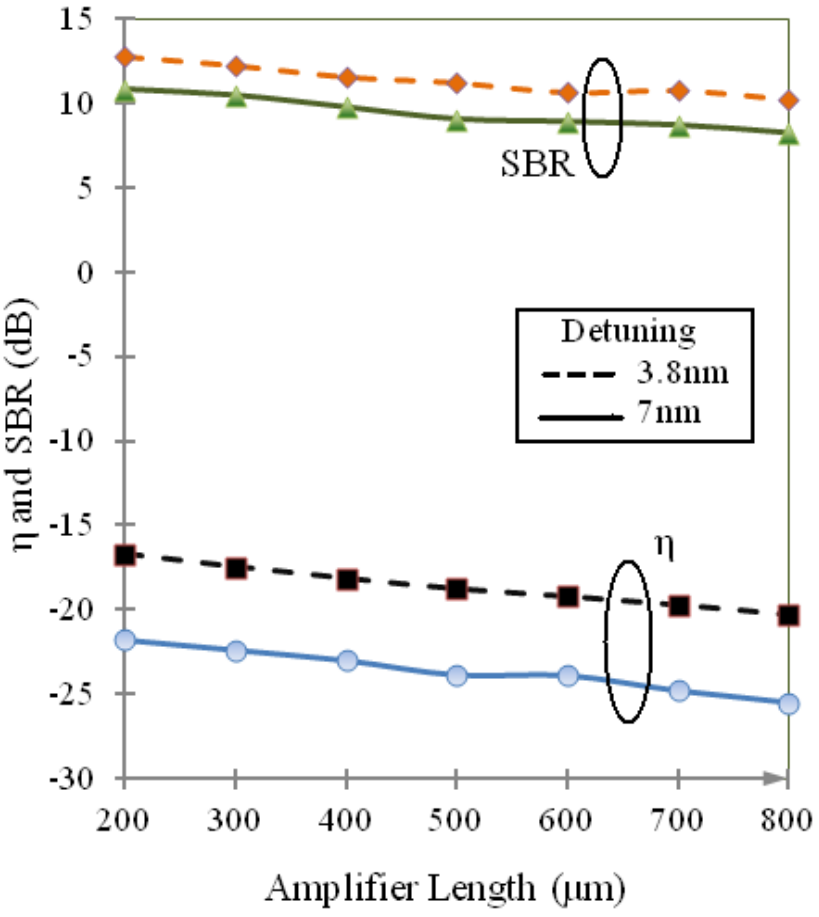


Figure 4.8: Conversion efficiency and SBR versus amplifier length

Further, using the simulation setup, wavelength spectrum, eye diagrams, input signal and received signal are measured for both the jammed OCDMA system and proposed anti-jamming system. The results obtained for anti-jamming optical CDMA systems are evaluated in terms of BER, eye diagrams and signals measured at eavesdropper and receiver.

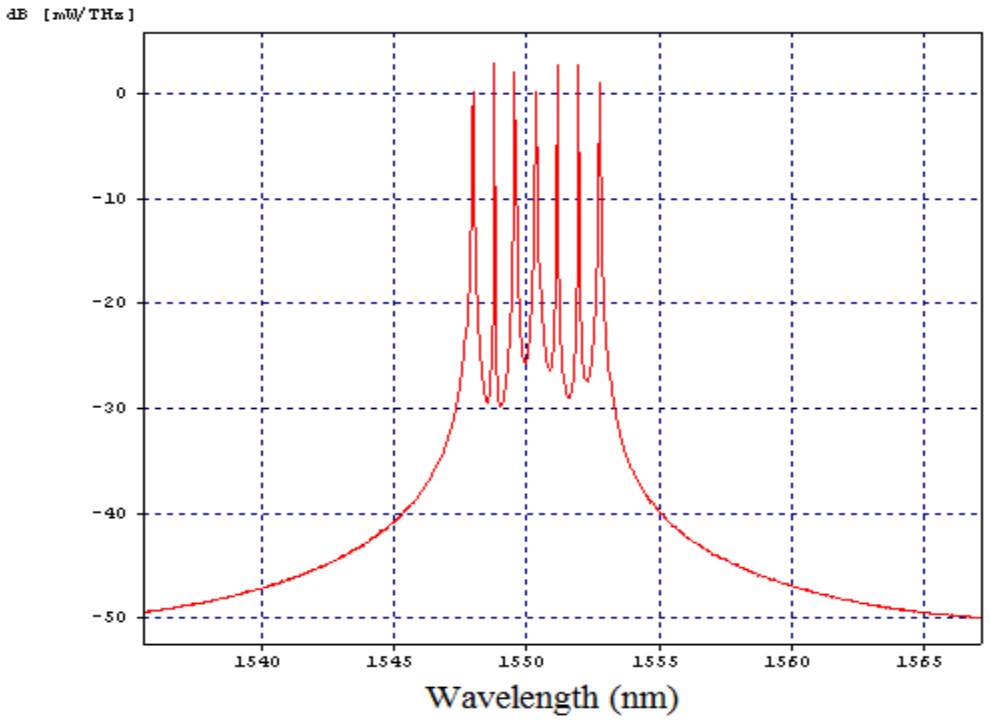


Figure 4.9: OCDMA input spectrum

To study the performance of SOA based wavelength converter as an anti-jammer in OCDMA network, the wavelengths throughout the network are observed. The input spectrum is shown in figure 4.9 consists of 7 wavelengths. The OCDMA encoded sequence consists of two wavelengths 1548 nm and 1551.2 nm (in figure 4.10) which are converted to wavelengths 1562 nm and 1558.8 nm respectively (in figure 4.11) through FWM in SOA using the pump wavelength at 1555nm. The jammer spectrum is same as the OCDMA encoder spectrum as shown in figure 4.12. Figure 4.13 shows the all multiplexed wavelengths from authorized user, jammer and other users present in the network which are transmitted through the optical fiber. All other active users contribute to the multiple access interference (MAI) in the network. At receiver side, the BPF will filter the converted signal out of the incoming waveband as shown in figure 4.14. Then, the filtered out signal is converted back to its original wavelengths through wavelength de-conversion before decoding the signal as shown in figure 4.15.

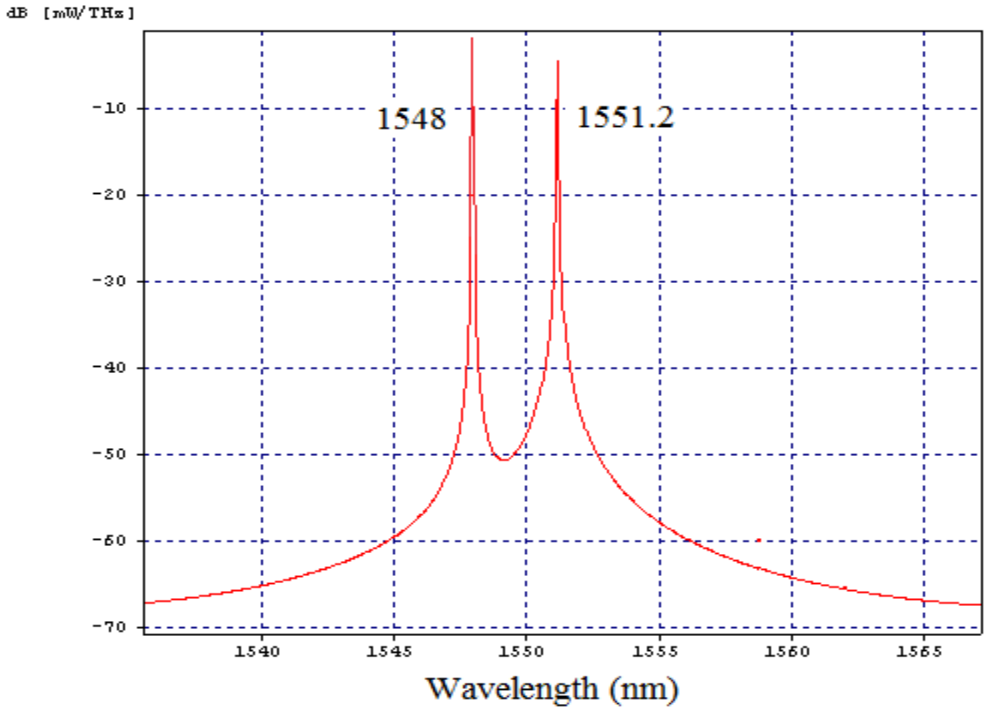


Figure 4.10: OCDMA encoder spectrum

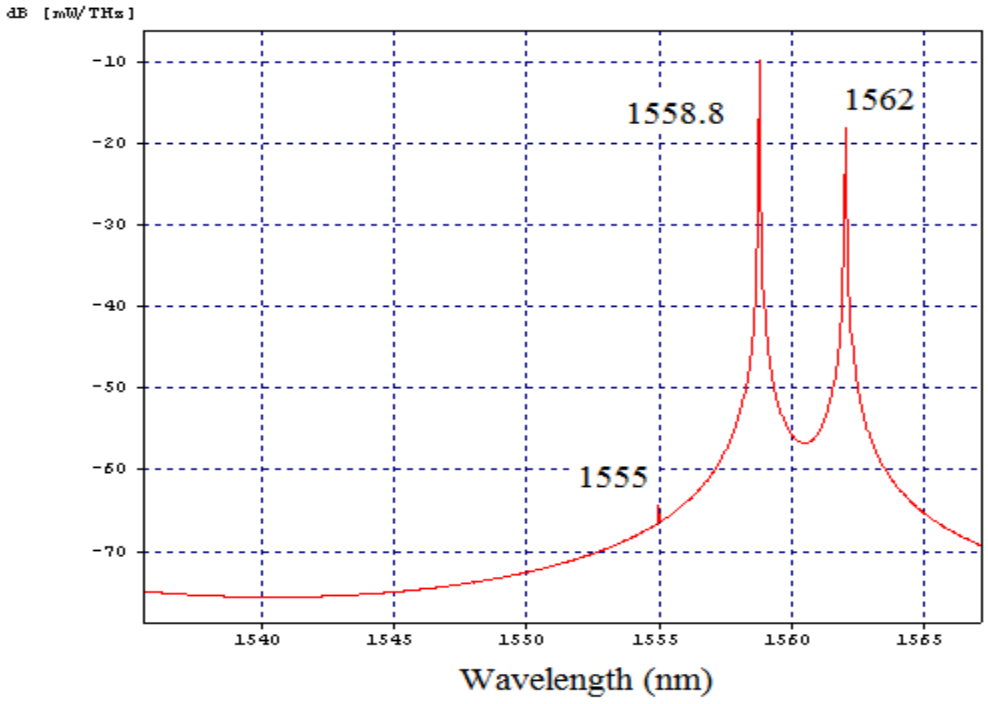


Figure 4.11: Encoded spectrum after wavelength conversion

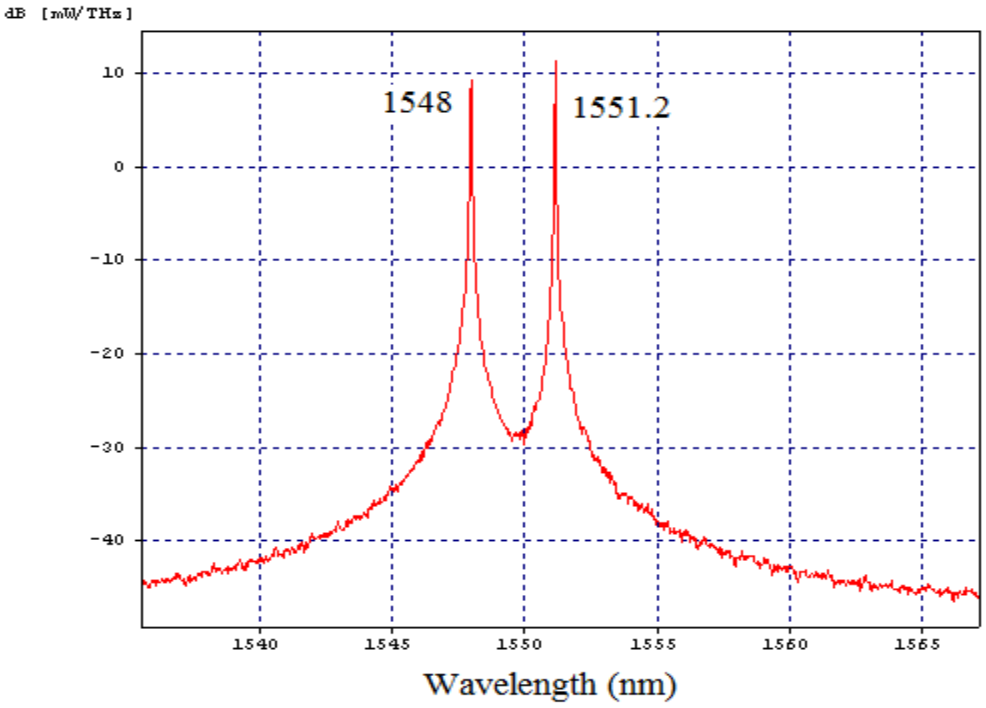


Figure 4.12: Jammer spectrum

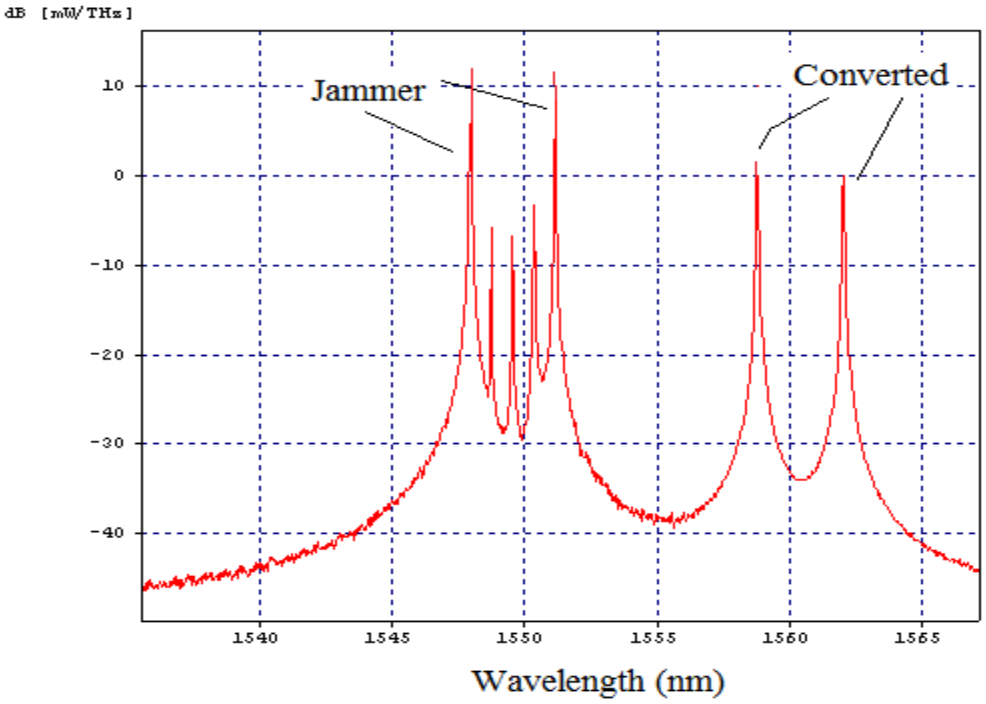


Figure 4.13: Multiplexed spectrum of all signals along the fiber

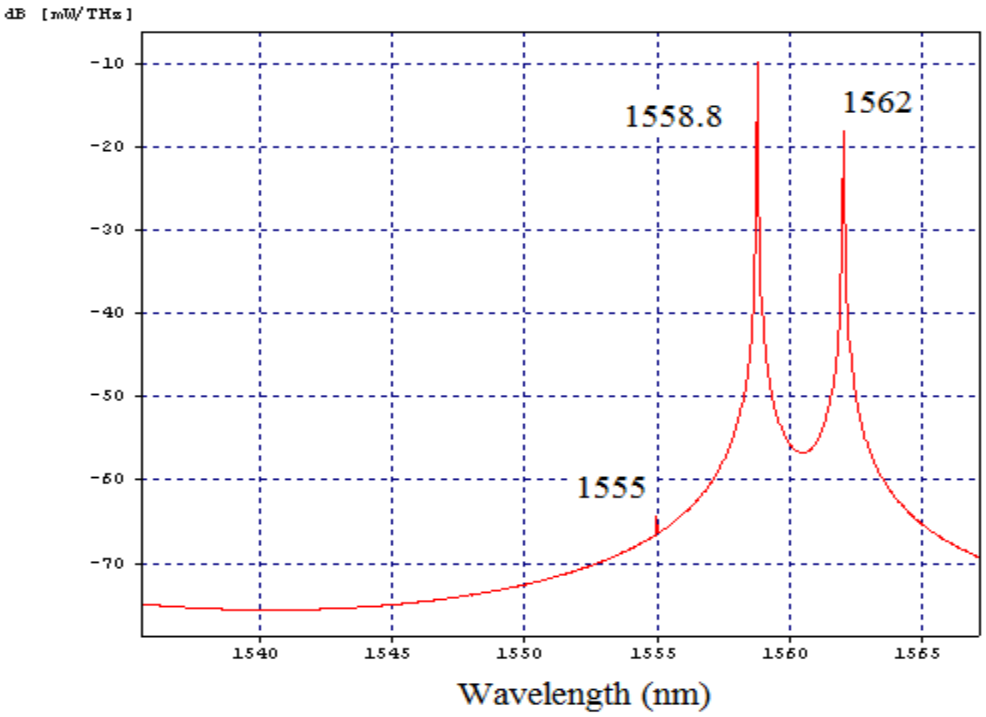


Figure 4.14: Output spectrum after band pass filter

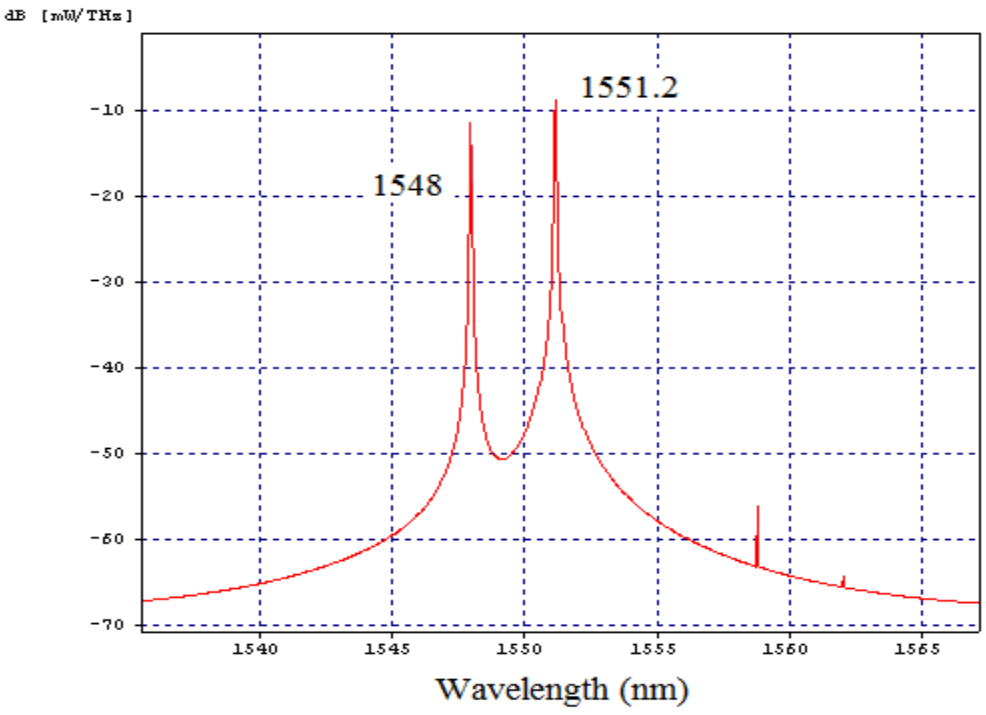


Figure 4.15: Spectrum after wavelength deconverter

Next, the jammer signal and the user input signal are shown in figures 4.16 and 4.17 respectively. The figure 4.18 shows the received signal in presence of jammer. It can be seen that the received signal is different from the input message signal which means high power jammer is disrupting the communication successfully. It is shown that the jammer has completely overshadowed the original message signal with its own, making the originally transmitted data unreadable at receiver.

In order to mitigate the effect of jammer, FWM in SOA is used for wavelength conversion to translate the data from encoder wavelength to other wavelengths which are out of the jamming window. The received signal using wavelength converter in the OCDMA network is shown in figure 4.19. It is observed that the message signal received is same as the user input signal even when the jammer is on. Therefore, if the jamming signals are injected to block the channels of the original signal with the aim of denying service, the data can still be transmitted securely to the receiver after successful wavelength conversion.

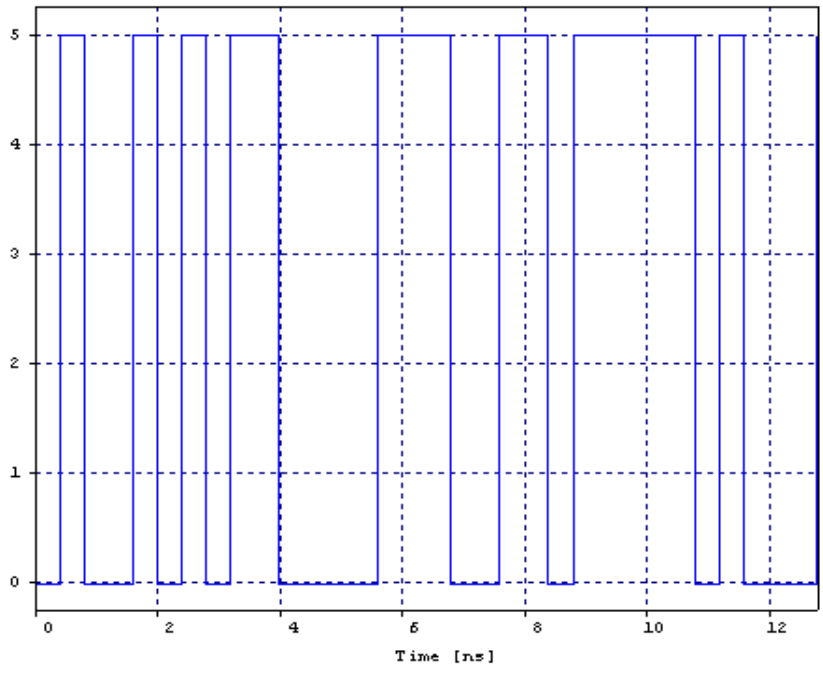


Figure 4.16: Jammer signal

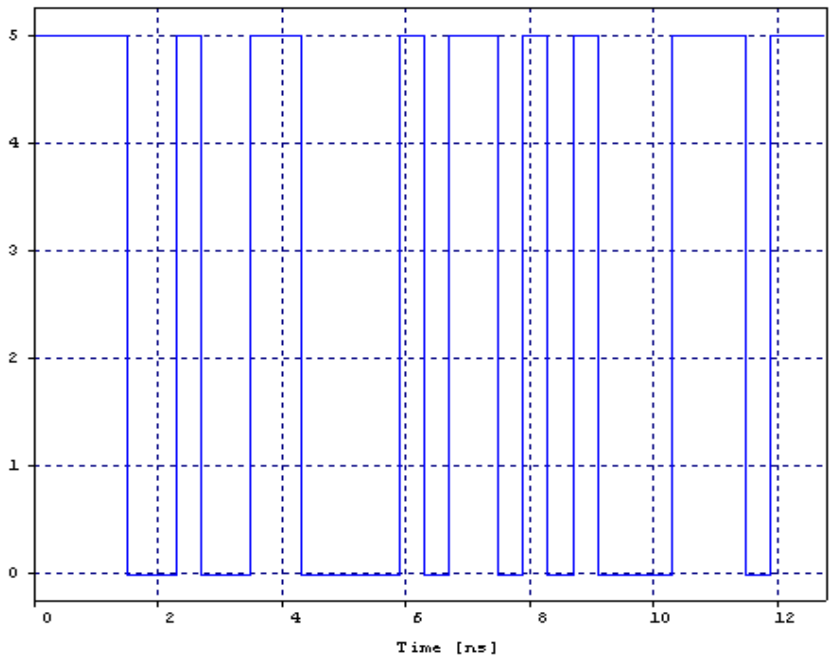


Figure 4.17: User input data signal

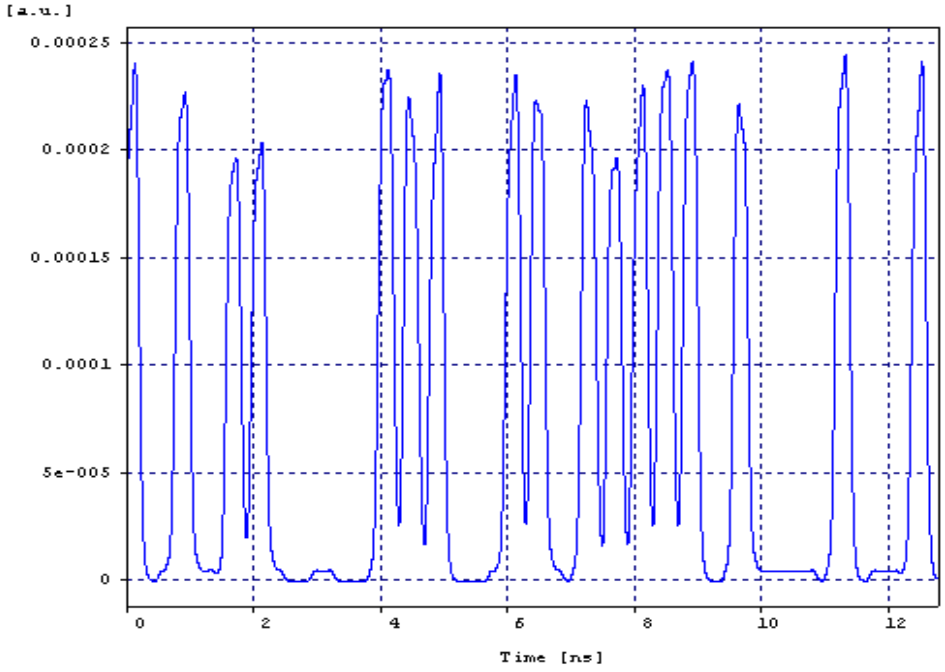


Figure 4.18: Received signal when jammer is on

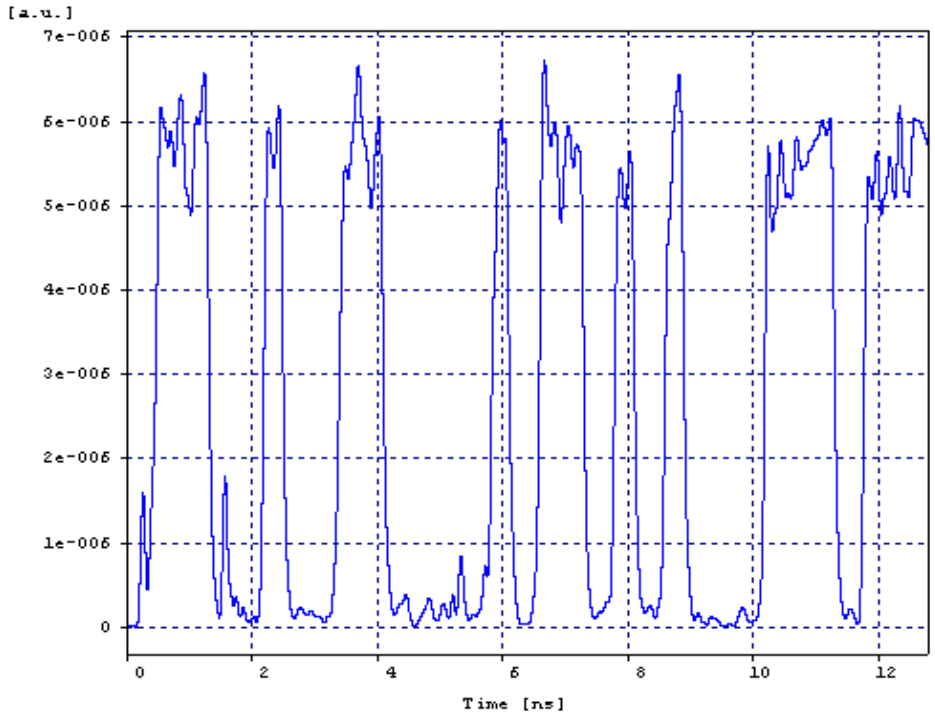


Figure 4.19: Received signal with anti-jamming

Further, BER at receiver for both the systems (with and without anti-jamming) is measured at different jammer powers as shown in figure 4.20. It is observed that BER increases with increase in jammer power for both the cases. But, the value of BER remains below than 10^{-12} at all the power levels for the proposed SOA based wavelength converter system. This means that the BER at the receiver is acceptable 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.

A clear eye diagram can also be observed at receiver as shown in figure 4.21. The results imply that jammer has no effect on this proposed model as it gives resistance to jamming at low as well as high jammer powers. If jamming signals are injected to block the channels of the original signal with the aim of denying service, the data can still be transmitted securely to the receiver by the use of the proposed SOA based wavelength conversion. Moreover, the proposed wavelength converter is compact, transparent and has large conversion bandwidth. Hence, the FWM in SOA based OCDMA system has improved capability of anti-jamming and additional advantages over other converters.

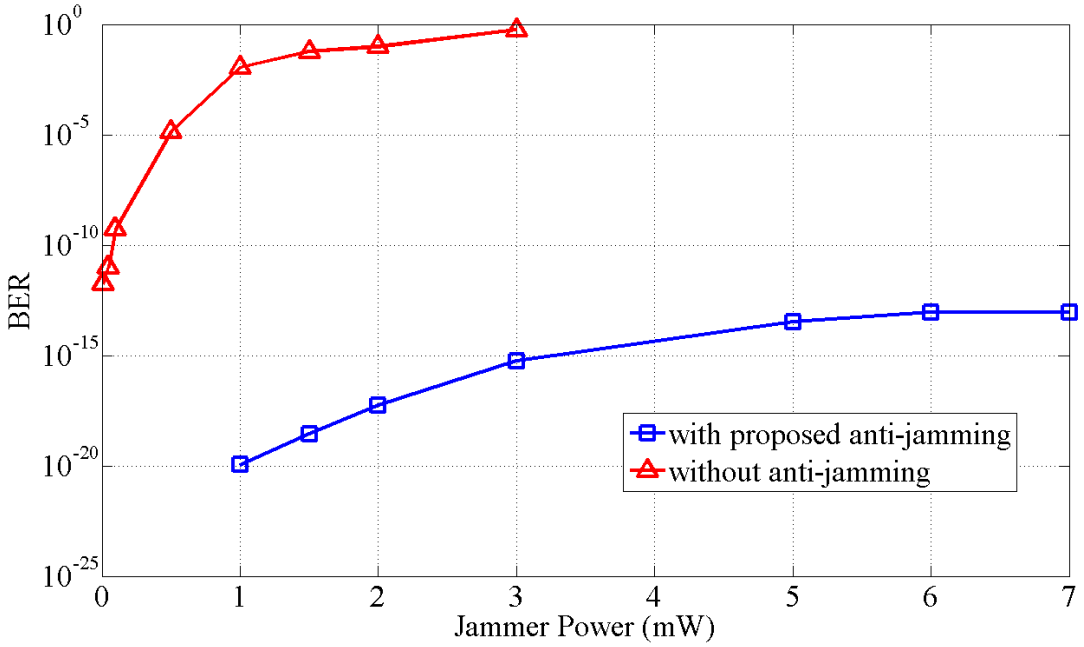


Figure 4.20: BER versus jammer power

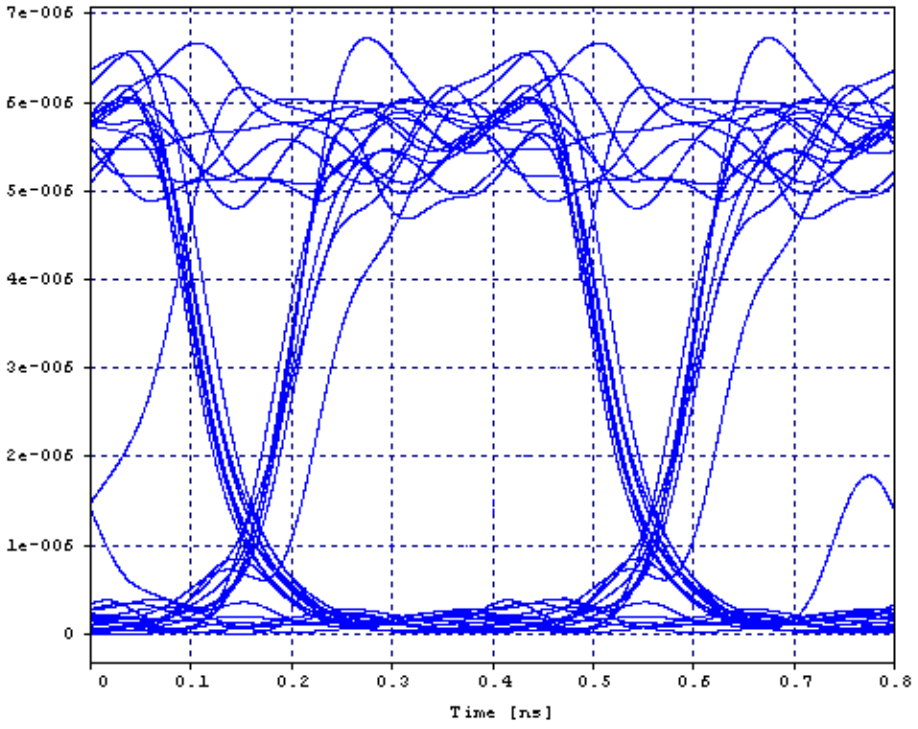


Figure 4.21: Eye diagram at receiver with proposed anti-jamming technique

4.7 Conclusion

OCDMA signal can be easily jammed with high power jamming signal. In this chapter, we propose a novel anti-jamming technique for OCDMA network through four wave mixing in semiconductor optical amplifier based wavelength converter. The wavelength conversion at the transmitter negates the jamming attack by moving the user's wavelengths out of jamming window. It is shown that wavelength conversion through four wave mixing in SOA has improved capability of jamming resistance. The tunable pump used in wavelength converter adds flexibility in the proposed technique, which is useful in obtaining the different converted wavelengths in the case of jammer with varying wavelengths. It is observed that jammer has no effect on OCDMA network even at high jamming powers by using the proposed technique.

Chapter 5

Validation of Proposed Security Techniques against Eavesdropping and Jamming

This chapter deals with the third objective of the thesis which is to validate the techniques proposed in the previous chapters for improved security against eavesdropping and jamming.

5.1 Introduction

Novel security techniques against eavesdropping and jamming are proposed in chapter 3 and chapter 4 respectively, where the theoretical system models are proposed and simulated. The validation of the proposed techniques is carried out in this chapter in order to verify their effectiveness. The effectiveness of these novel methods is validated by both through mathematical analysis and by simulation them on different software. Firstly, the technique proposed for security against eavesdropping is analyzed mathematically. The results show that confidentiality of the system is effectively increased. Further, the proposed anti-jamming technique is validated using software Optisystem 7.0. Similar results are obtained for the proposed anti-jamming technique using both the softwares.

5.2 Validation of the Proposed Technique for Confidentiality against Eavesdropping

The technique proposed for security enhancement against eavesdropping in OCDMA network is virtual user scheme. VUS exploits the notion that deciphering the data bits becomes more difficult when multiple users are present.

A simple analysis is carried out for OOK-OCDMA and CSK-OCDMA to validate the virtual user scheme for enhanced security against eavesdropping.

5.2.1 Effect of Virtual User Scheme on the Confidentiality Performance of OOK-OCDMA

The confidentiality performance of OOK-OCDMA with VUS is analyzed for both the synchronous and asynchronous transmissions. Consider two simultaneous transmissions, each of which is OCDMA encoded and modulated using OOK. Each operates at a data rate of D bits/s.

a) For synchronous transmissions

When all users transmit synchronously, the beginning and ending time for transmission of each bit is the same for both users as shown in figure 5.1.

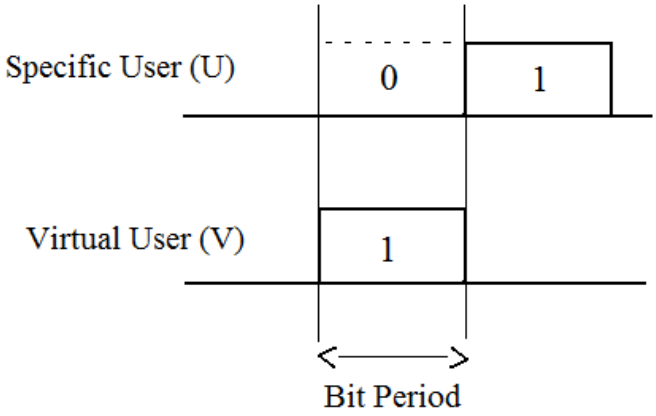


Figure 5.1: Two users transmitting synchronously

In a given bit period, assume equally likely "ones" and "zeros".
The probability that a specific user (U) transmits a '1' or '0' during a given bit period is,

$P_U(1) = ½$ and $P_U(0) = ½$

Similarly, the probability that virtual user (V) transmits a '0' or '1' during the same bit period is,

$P_V(0) = ½$ and $P_V(1) = ½$

Assuming that the value of each data bit is independent of other data bits and independent of other user's bits, the probability that a specific user transmits a '1' while virtual transmit a '0' on any particular bit is simply the product of these two probabilities. Therefore, the probability of both events occurring together is P_{Com} as given in (5.1).

$$P_{Com} = P_U(1) \text{ and } P_V(0) = ½ \times ½ = ¼ \quad (5.1)$$

Depending on various combinations of ‘0’ and ‘1’, there are four cases. All other cases are shown in table 5.1.

Table 5.1: Different combinations of both users transmitting synchronously

Specific User (U) transmits in a bit period	Virtual User (V) transmits in a bit period	Probability of both event occurring together P_{Com}	Detection at **eavesdropper** for specific user U
1	0	¼	True
1	1	¼	True
0	0	¼	True
0	1	¼	False

From the table, it can be seen that if specific user is transmitting a bit ‘1’ then eavesdropper will correctly detect the data irrespective of what is being transmitted at virtual user by a simple energy detector.

However, if the specific user is transmitting a ‘0’ in a bit period then it depends on virtual user whether the eavesdropper will correctly detect the data or not.

Out of the four cases, for one case where specific user transmits a ‘0’ and virtual user transmits a ‘1’, a simple power detector at eavesdropper will falsely detect ‘1’ when actually ‘0’ is being transmitted by the authorized user.

Hence, the proposed virtual user technique will increase the security of OCDMA using on-off keying by 25% when both the users are transmitting synchronously.

b) For asynchronous or non-synchronous transmissions

When all users transmit asynchronously, the starting and ending time for the transmission of each bit is not same for both users. So, when one user transmits a ‘1’, other user may transmit fractions of two consecutive bits during the transmission time of the “one” bit due to the lack of synchronization among users as shown in figure 5.2.

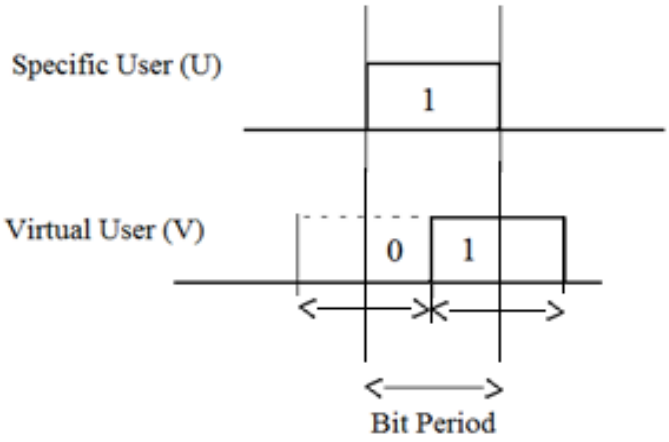


Figure 5.2: Two users transmitting asynchronously

In a given bit period, assume equally likely "ones" and "zeros". The probability that a specific user (U) transmits a '1' or '0' during a given bit period is,

$P_U(1) = ½$ and $P_U(0) = ½$

Similarly, the probability that virtual user (V) transmits fractions of two consecutive bits (00, 01, 10, 11) during the same bit period is,

$P_V(00) = ¼$, $P_V(01) = ¼$, $P_V(10) = ¼$ and $P_V(11) = ¼$.

Assuming that the value of each data bit is independent of other data bits and independent of other user's bits, the probability that a specific user transmits a '1' while virtual user transmits two consecutive '0s' on any particular bit interval is simply the product of these two probabilities.

Therefore, the probability of both events occurring together (P_{Com}) is given by (5.2)

$$P_{Com} = P_U(1) \text{ and } P_V(0) = ½ \times ¼ = 1/8 \quad (5.2)$$

Depending on the various combinations, the total number of cases turns out to be eight. All other cases are shown in table 5.2.

Table 5.2: Different combinations of both users transmitting asynchronously

Specific User (U) transmits in a bit period	Virtual User (V) transmits in a bit period		Probability of both event occurring together P_{Com}	Detection at eavesdropper for specific user U
	V_1 (Bit 1)	V_2 (Bit 2)		
1	0	0	1/8	True
1	0	1	1/8	True
1	1	0	1/8	True
1	1	1	1/8	True
0	0	0	1/8	True
0	0	1	1/8	False
0	1	0	1/8	False
0	1	1	1/8	False

From the table 5.2, it can be observed that if a specific user is transmitting the bit '1' then eavesdropper will correctly detect the data of an authorized user irrespective of what is being transmitted by the virtual user.

If a specific user is transmitting a '0' in the bit period then it depends on virtual user whether an eavesdropper will correctly detect the data or not.

Out of the eight cases, for three cases where specific user transmits a '0' and virtual user transmits any of the other combination except '00' then a simple energy detector will falsely detect '1' when actually '0' is being transmitted by the authorized user.

Hence, the proposed virtual user technique will increase the security of OCDMA using On-Off keying by 37.5% when both users transmit asynchronously.

In the end, it is concluded from the above analysis that the virtual user scheme will decrease the vulnerability to eavesdropping by increasing the security of an OCDMA system by 25% and 37.5% for synchronous and asynchronous cases respectively.

5.2.2 Effect of Virtual User Scheme on the Confidentiality Performance of CSK-OCDMA

In this section, a simple analysis is carried out for code switching scheme to show how the presence of a virtual user will enhance the system's confidentiality. It is already known that this modulation format is vulnerable to differential detection eavesdropper.

For worst case scenario, eavesdropper's capability is overestimated for the security analysis of virtual user scheme in CSK-OCDMA network. It is assumed that eavesdropper is in synchronization with the transmitted data, so that it can easily locate the beginning and ending of a transmitted data bit. Therefore, the confidentiality performance of CSK-OCDMA with VUS is analyzed for synchronous transmissions only. However in reality, there cannot be perfect synchronization between eve and transmitted data, resulting in degraded eavesdropper's performance.

Consider two synchronous transmissions, each of which is OCDMA encoded and modulated using CSK. In a given bit period, assume the probability of '1s' and '0s' to be equal.

The probability that a specific user (U) transmits a '1' or '0' during a given bit period is,

$P_U(1) = ½$ and $P_U(0) = ½$

Similarly, the probability that virtual user (V) transmits a '0' or '1' during the same bit period is,

$P_V(0) = ½$ and $P_V(1) = ½$

Assuming that the value of each data bit is independent of other data bits and independent of other user's bits, the probability that a specific user transmits a '1' while virtual transmits a '0' on any particular bit is simply the product of these two probabilities.

So, probability of both events occurring together is P_{Com} as shown in (5.3).

$$P_{Com} = P_U(1) \text{ and } P_V(0) = 1/2 \times 1/2 = 1/4 \quad (5.3)$$

Table 5.3 shows the codes used for CSK and the data being transmitted after encoding. The encoded data from both users overlaps before being transmitted on an optical fiber after passing through the multiplexer,. So, an eavesdropper which has access to isolated user transmission is basically getting the overlapped encoded data due to the presence of virtual user as shown in figure 5.3. Due to the presence of a virtual user, there are possible four combinations of encoded

bits which can occur in a particular bit period. If we assume, the possibility of occurrence of all the combinations is equally likely, then each combination has the probability of ¼.

Table 5.3: Codes used for CSK

	Specific User (Authorized)	Virtual User
Codes used for encoding	'0' → OC1 '1' → OC2	'0' → OC3 '1' → OC4
Data transmitted after CSK	01101 	10100 

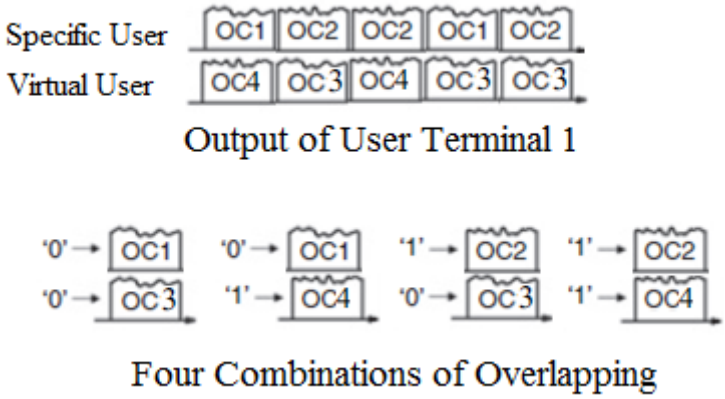


Figure 5.3: Different combinations of encoded bits

It is already known that in differential detection, two consecutive bit periods are compared by using a balanced photodetector. The different combinations of the consecutive bits for single transmitting user are considered in [42].

Similarly, all possible combinations for two consecutive bit periods in virtual user environment are shown in tables 5.4, 5.5, 5.6 and 5.7.

Table 5.4: Specific user is transmitting bit “0” in a bit period (while virtual is transmitting “0”)

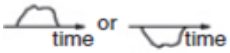
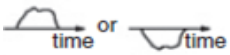
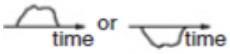
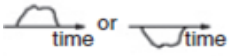
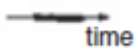
Encoded Data after overlapping		After balanced Photodetector	Probability of both event occurring together	Detection at eavesdropper for specific user U
Current bit	Previous Bit			
‘0’ → OC1 ‘0’ → OC3	‘0’ → OC1 ‘0’ → OC3		¼ × ¼ = 1/16	True
	‘0’ → OC1 ‘1’ → OC4		¼ × ¼ = 1/16	False
	‘1’ → OC2 ‘0’ → OC3		¼ × ¼ = 1/16	False
	‘1’ → OC2 ‘1’ → OC4		¼ × ¼ = 1/16	False

Table 5.5: Specific user is transmitting bit “0” in a bit period (while virtual is transmitting “1”)

Encoded Data after overlapping		After balanced Photodetector	Probability of both event occurring together	Detection at eavesdropper for specific user U
Current bit	Previous Bit			
‘0’ → OC1 ‘1’ → OC4	‘0’ → OC1 ‘0’ → OC3		¼ × ¼ = 1/16	False
	‘0’ → OC1 ‘1’ → OC4		¼ × ¼ = 1/16	True

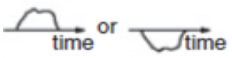
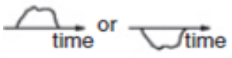
	'1' → OC2 '0' → OC3		¼ × ¼ = 1/16	False
	'1' → OC2 '1' → OC4		¼ × ¼ = 1/16	False

Table 5.6 Specific user is transmitting bit "1" in a bit period (while virtual is transmitting "0")

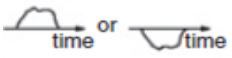
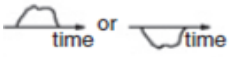
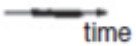
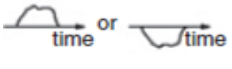
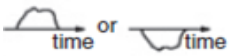
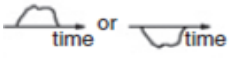
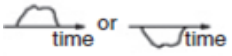
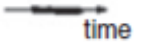
Encoded Data after overlapping		After balanced Photodetector	Probability of both event occurring together	Detection at eavesdropper for specific user U
Current bit	Previous Bit			
'1' → OC2 '0' → OC3	'0' → OC1 '0' → OC3		¼ × ¼ = 1/16	True
	'0' → OC1 '1' → OC4		¼ × ¼ = 1/16	True
	'1' → OC2 '0' → OC3		¼ × ¼ = 1/16	False
	'1' → OC2 '1' → OC4		¼ × ¼ = 1/16	True

Table 5.7 Specific user is transmitting bit “1” in a bit period (while virtual is transmitting “1”)

Encoded Data after overlapping		After balanced Photodetector	Probability of both event occurring together	Detection at eavesdropper for specific user U
Current bit	Previous Bit			
‘1’ → OC2 ‘1’ → OC4	‘0’ → OC1 ‘0’ → OC3		¼ × ¼ = 1/16	True
	‘0’ → OC1 ‘1’ → OC4		¼ × ¼ = 1/16	True
	‘1’ → OC2 ‘0’ → OC3		¼ × ¼ = 1/16	True
	‘1’ → OC2 ‘1’ → OC4		¼ × ¼ = 1/16	False

From all the four tables (5.4 to 5.7), total probability of falsely detecting data at eavesdropper is given by (5.4)

$$P_{False} = 3/16 + 3/16 + 1/16 + 1/16 = 8/16 = ½ \quad (5.4)$$

This means by using virtual environment the probability of falsely detecting the data at eavesdropper (whenever he is able to find a single user transmission) for CSK-OCDMA system increases by 50 %.

Figure 5.4 and table 5.8 show the comparison of security performance of virtual user scheme for both the OOK and CSK. It is seen that the virtual user forces the eavesdropper to falsely detect the transmitted bits. With OOK modulated scheme probability of falsely detecting data increases by 25% for synchronous transmission and 37.5% for asynchronous transmission. Furthermore, the probability increases by 50% for the synchronous transmission with CSK modulation format.

The synchronous case will give the minimum security provided by virtual user CSK-OCDMA system. The asynchronous transmission between an authorized user and the virtual user will further increase the security performance of virtual user scheme. It is shown that even in worst case scenario; the VUS increases the immunity of CSK-OCDMA network against differential detection at least by 50%. Therefore, it is validated that the novel virtual user scheme increases immunity of the OCDMA system against eavesdropping.

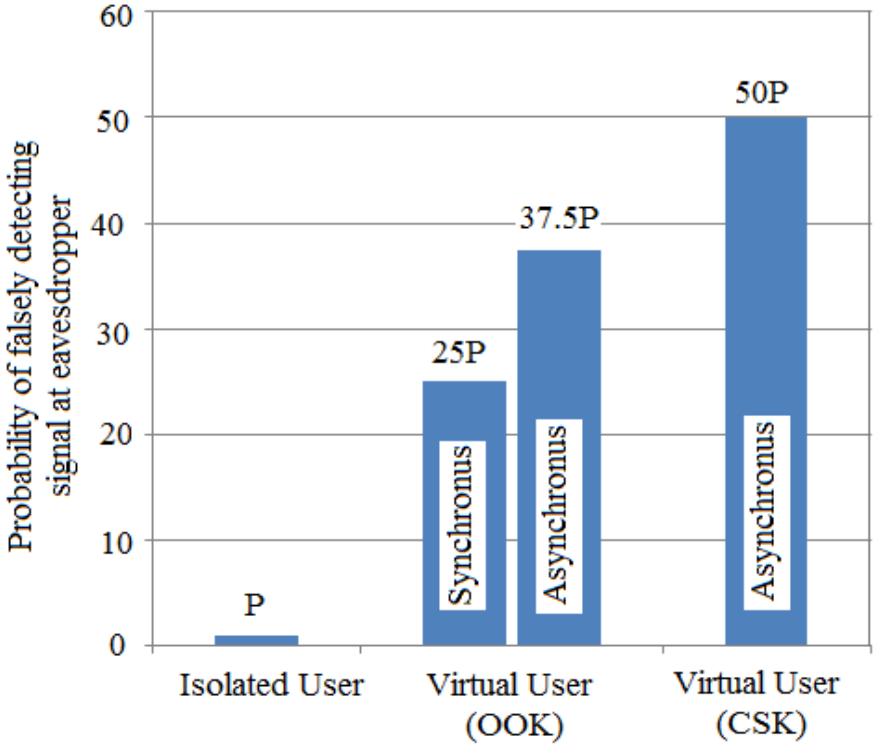


Figure 5.4: Comparision of security performance of virtual user scheme for OOK and CSK

Table 5.8: Percentage increase in security of different OCDMA networks

Proposed scheme	Security increases
Virtual User Scheme with OOK-OCDMA	25% against simple energy detector for synchronous transmission 37.5% against simple energy detector for asynchronous transmission
Virtual User Scheme with CSK-OCDMA	50 % against differential detector

5.3 Validation of the Proposed Technique for Signal Availability against Jamming

The technique proposed to deter the effect of jamming in OCDMA network is based on wavelength conversion process. The process of four wave mixing in SOA is used to translate the information data to a new set of wavelengths. Validation of the proposed technique for signal availability against jamming is done by simulating on multiple softwares. The simulation is performed for all types of codes (1-D, 2-D and 3-D codes) in order to evaluate the effectiveness of proposed technique. Along with OptSim, the other software used to validate the proposed anti-jamming technique is OptiSystem 7.0. It is a comprehensive software design suite that enables users to plan, test, and simulate optical links in the transmission layer of modern optical networks.

5.3.1 Simulation Setup for OCDMA with Proposed Anti-jamming Technique

The simulation is carried out for OCDMA using 1-D, 2-D and 3-D codes with the proposed anti-jamming technique. Continuous wave lasers at different wavelengths are used to create the carrier signal. The logical input data is converted into non return to zero electrical data which modulates the broadband optical carrier signal resulting in the electrical to optical conversion of data bits. The on-off keying is used as modulation format with a bitrate of 1 Gbps. The modulated data is then spectrally encoded using the required codes for each setup. The encoded data is then input to wavelength converter before being transmitted into the optical fiber.

For 1-D codes, the wavelengths range from 1548 nm to 1549 nm with spacing of 0.2 nm used to create a dense carrier signal is shown in figure 5.5. The 1-D encoder uses two wavelengths 1548.6 nm and 1549 nm for encoding which are converted to 1551.4 nm and 1551 nm using the pump wavelength of 1550 nm.

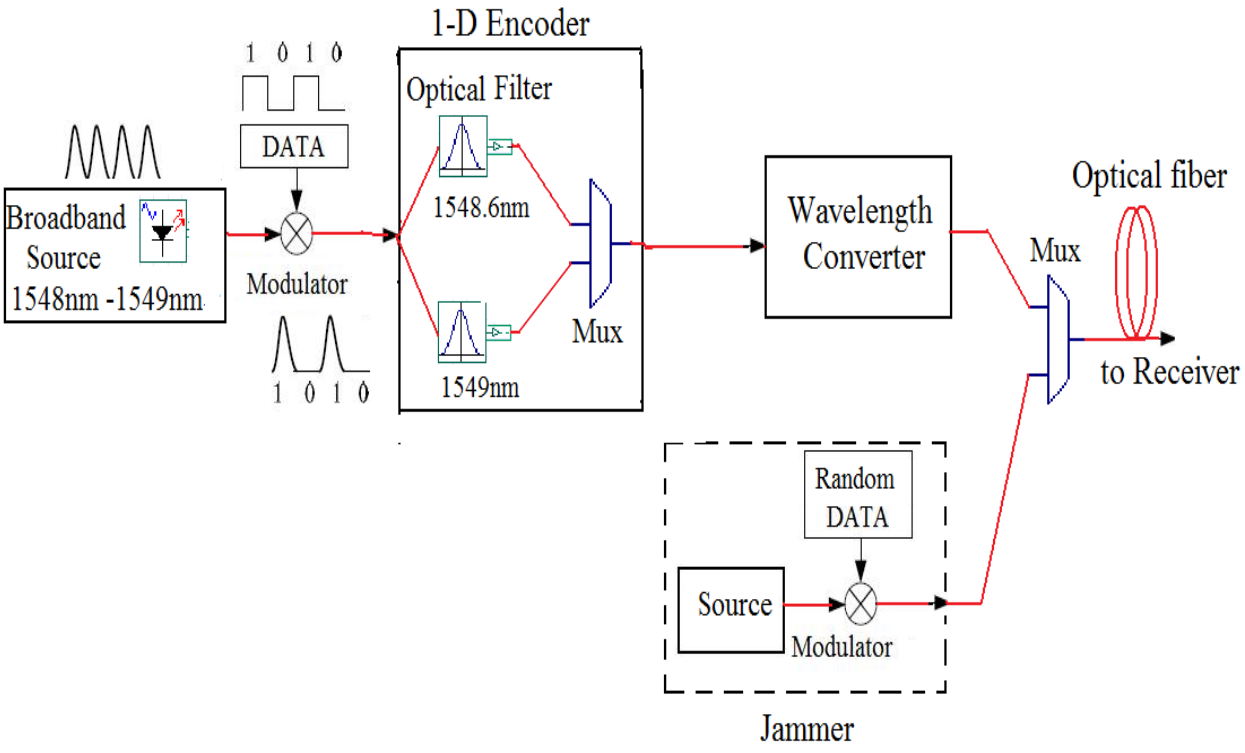


Figure 5.5: Schematic diagram of 1-D OCDMA transmitter with proposed anti-jamming technique

For 2-D OCDMA, the waveband 1548.6 nm to 1549 nm with spacing of 0.4 nm is used for optical carrier signal as shown in figure 5.6. 2-D encoder uses four wavelengths 1550 nm, 1550.4 nm, 1550.8 nm and 1551.2 nm for encoding the input data. In the encoder, each wavelength is given different time delays according to the extracted code from the code set. The encoded data is then converted to 1549.2 nm, 1548.8 nm, 1548.4 nm and 1548 nm respectively using the pump wavelength 1549.6 nm.

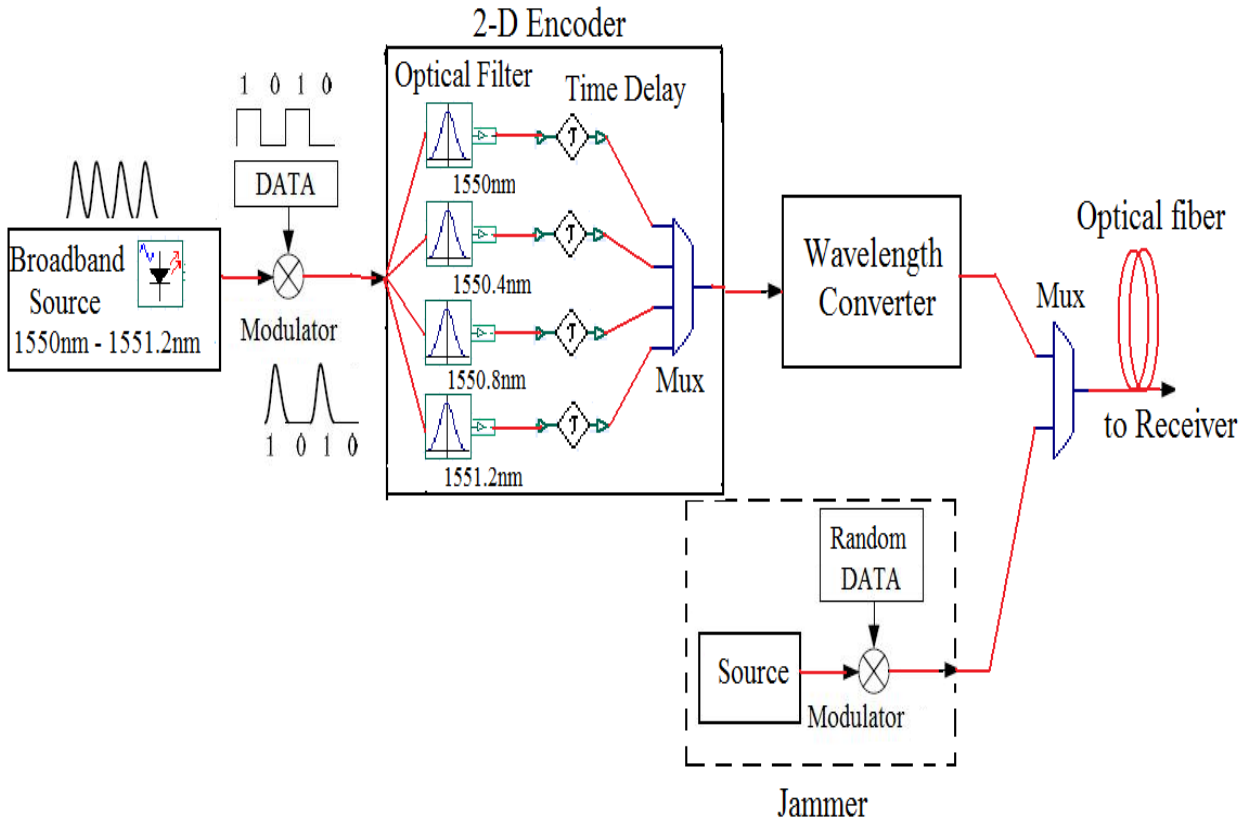


Figure 5.6: Schematic diagram of 2-D OCDMA transmitter with proposed anti-jamming technique

The schematic diagram of 3-D OCDMA with proposed anti-jamming technique is shown in figure 5.7. The two dimensional implementation of 3-D codes is used but tunable filters are used instead of arrayed waveguide gratings [24]. Space × Wavelength × Time codes are implemented by using the wavelengths equal to Space × Wavelength for 2-D implementation with a delay used for each new set of wavelengths. The wavelength range 1548.6 nm to 1552.8 nm with spacing of 0.4 nm is used for 3-D codes. The 3-D encoder uses four wavelengths as one set which are 1550 nm, 1550.4 nm, 1550.8 nm and 1551.2 nm and other time delayed wavelengths 1551.6 nm, 1552 nm, 1552.4 nm and 1552.8 nm are used as second set of wavelengths. The pump wavelength of 1549.6 nm is used to convert the data to 1549.2 nm, 1548.8 nm, 1548.4 nm and 1548 nm for first set and 1547.6 nm, 1547.2 nm, 1546.8 nm and 1546.4 nm for second set.

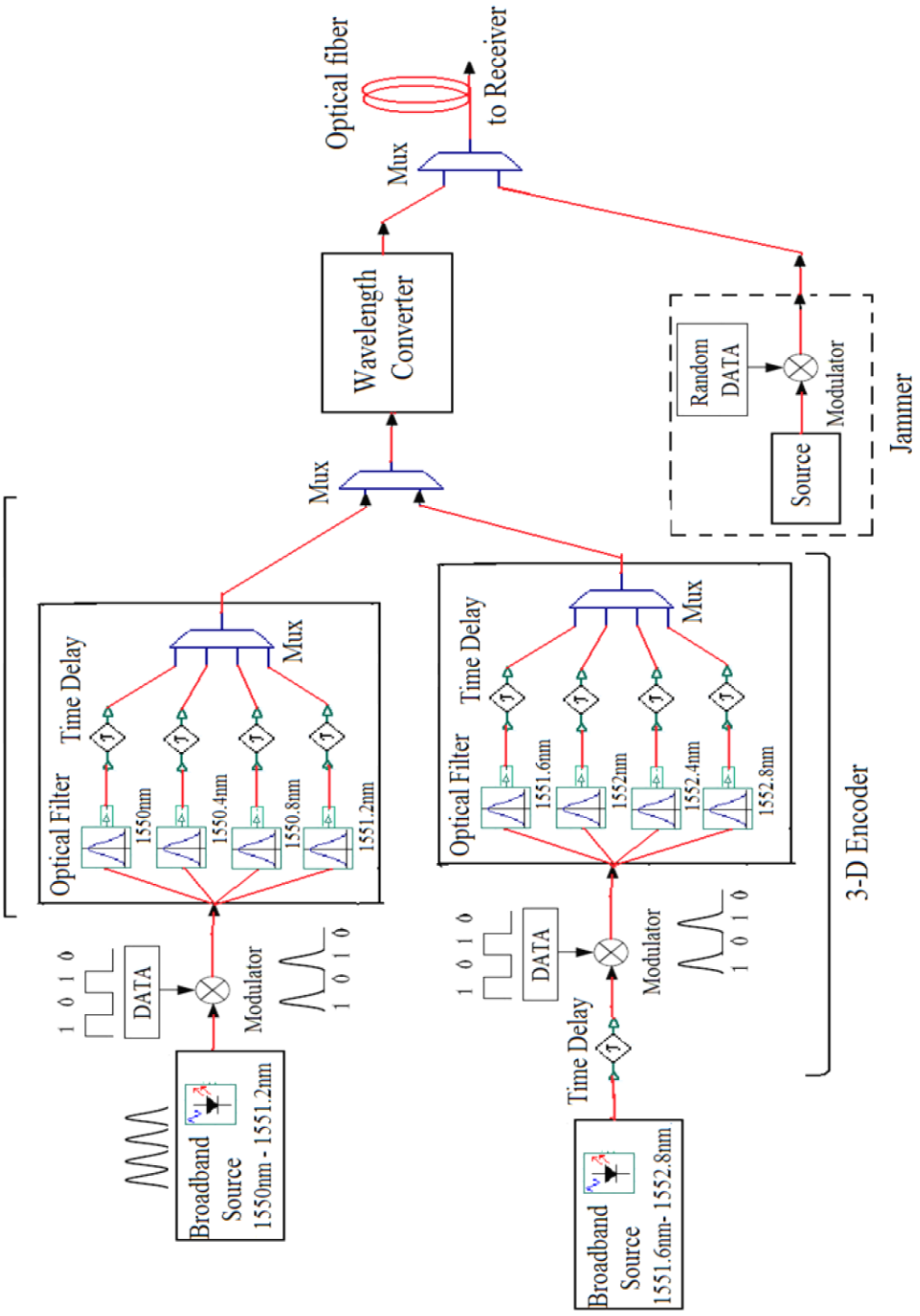


Figure 5.7: Schematic diagram of 3-D OCDMA transmitter with proposed anti-jamming technique

The wavelength converter first combines the input encoded data signal with the optical pump source. The converter's optical pump source is a tunable, continuous wave Lorentzian laser with input power of 0.1mw. All the wavelengths of input encoded signal are demultiplexed before being combined in the SOA. Each wavelength of the encoded signal is multiplexed with the pump signal and then amplified by an EDFA. The amplified signal is launched into the SOA where the pump signal modulates the carrier density and consequently the gain of SOA, which further modulates the input data signal. This is known as four wave mixing and generates the output wavelength containing the information of input signal.

The traveling wave SOA amplifier model is used as a wavelength converter in FWM mode. At the output of SOA, BPF is tuned to the converted wavelengths to filter out only the translated wavelengths. The same wavelength converter is placed before decoder at the receiver side. The combination of band pass filter and wavelength deconverter will translate the data back to its original wavelengths which are being used at the decoder to retrieve the transmitted information.

5.3.2 Results and Discussion

The results are obtained for 1-D, 2-D and 3-D coded OCDMA network and evaluated in terms of BER and eye diagrams at the receiver. Firstly, BER is simulated for OCDMA system in presence of jammer. After that the novel anti-jamming technique proposed in chapter 4 is incorporated into the network and its effect on BER is observed.

Figure 5.8 shows the BER versus jammer power for OCDMA system using 1-D codes. The variations in BER against jamming power are measured for different input powers. It can be seen that BER increases with increase in jammer power. Even at very low jamming powers the recorded BER is very high. The BER observed for 0.1mW input power was close to unity, when jammer power was above 0.1mW. Also, the BER is observed to be low at high input power as compared to the low input power. But the overall system performance degrades even at high input power in presence of jammer. Hence, the jammer further worsens the system performance at low input power levels.

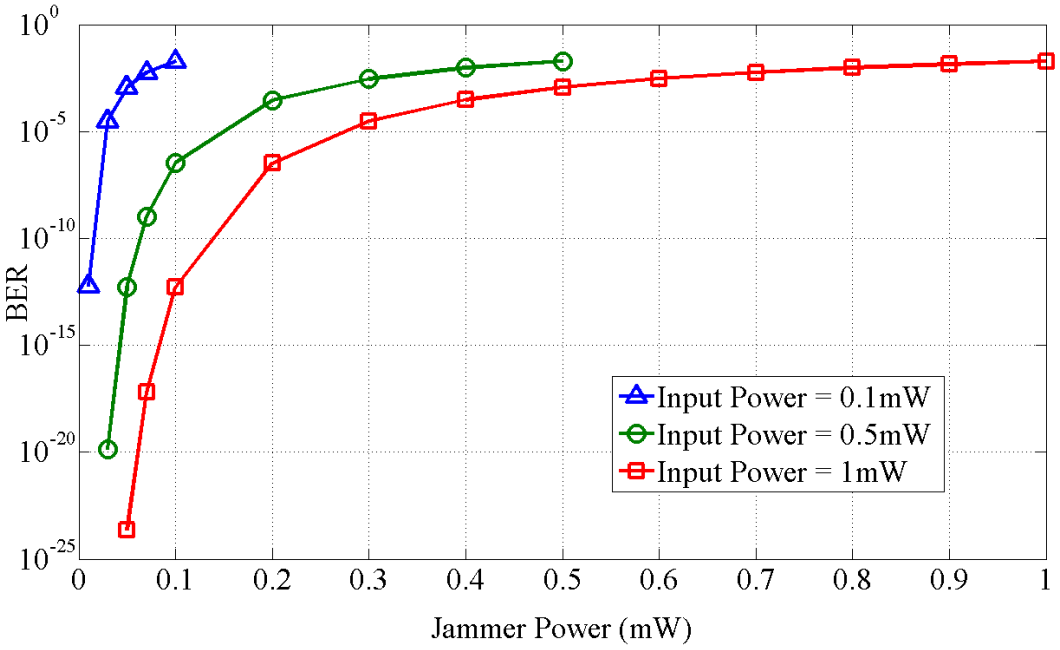


Figure 5.8: BER versus jammer power for 1-D codes

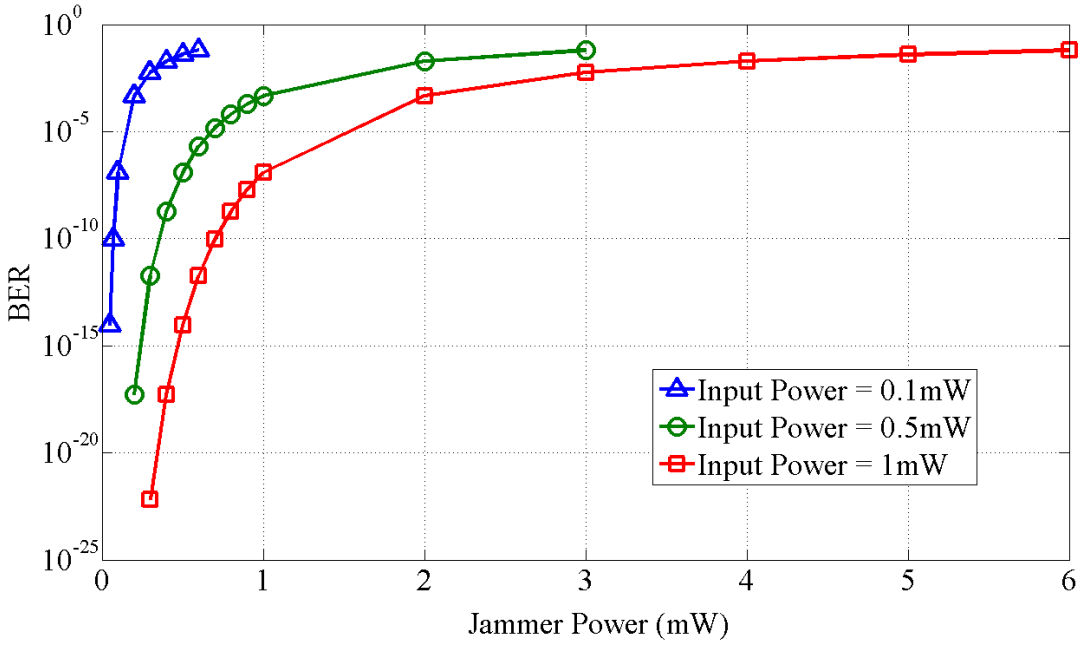


Figure 5.9: BER versus jammer power for 2-D codes

Similar results are observed for OCDMA system using 2-D and 3-D codes as shown in figure 5.9 and figure 5.10 respectively. In both the cases, increase in jammer power leads to increased BER at the receiver and further the BER is higher at lower input power. Hence, it can be seen that jammer transmitting at same waveband as of the authorized user negatively affects the system performance even at low jammer power.

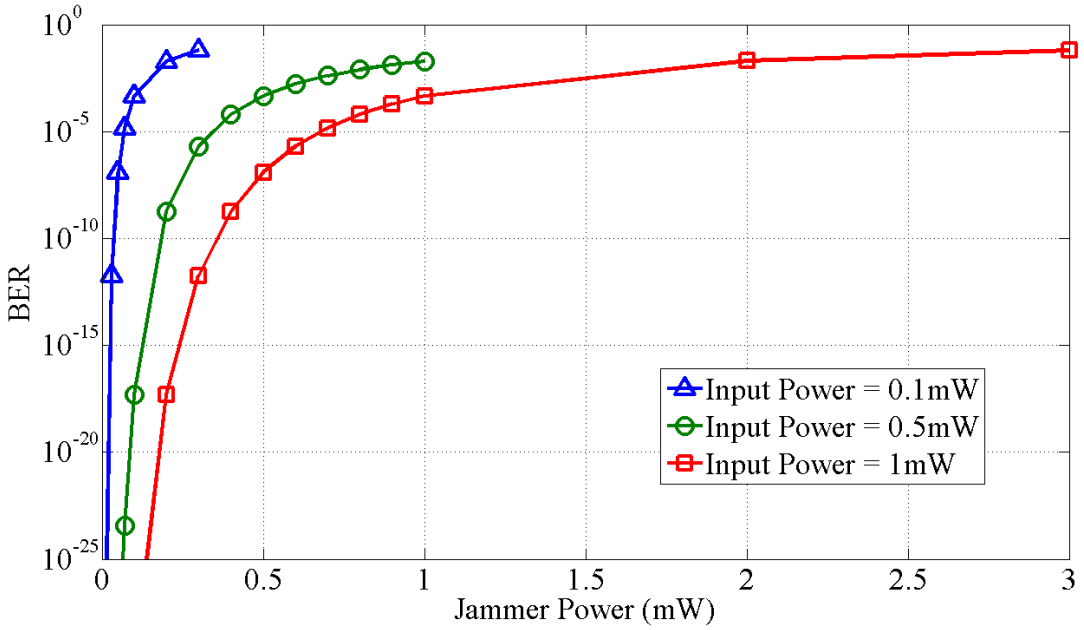


Figure 5.10: BER versus jammer power for 3-D codes

To mitigate the effect of jamming, the wavelength conversion technique proposed in chapter 4 is implemented. The SOA based wavelength converter is used after the encoder to convert the wavelengths out of the jamming window. Figure 5.11 shows the BER versus jammer power for 1-D codes with proposed anti-jamming technique. The variations in BER against jamming power are measured at different pump powers of the wavelength converter. It is observed that the BER at receiver remains constantly below 10^{-9} value at all the jamming powers. The low values of BER at receiver imply that jammer does not degrade the system performance when novel anti-jamming technique is applied. This is due to transfer of information to a new set of wavelengths through four wave mixing in SOA. Similar results are observed for OCDMA with 2-D codes as shown in figure 5.12. Hence, the wavelength conversion technique is an effective solution to provide jamming resistance in OCDMA network.

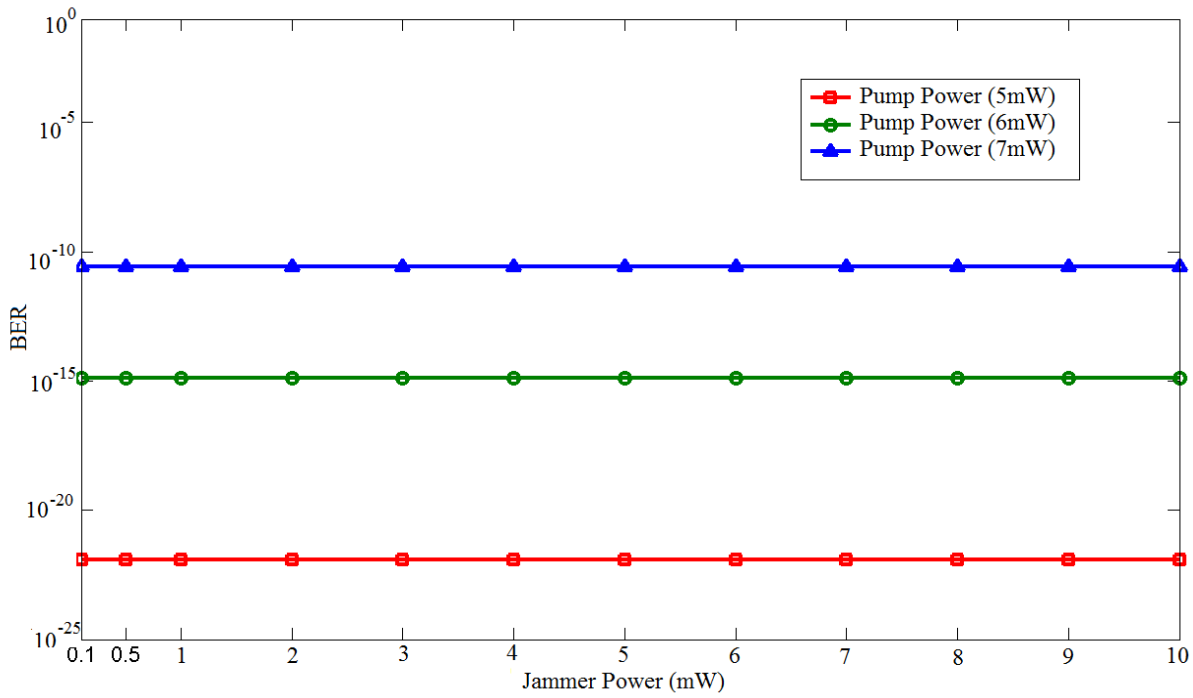


Figure 5.11: BER versus jammer power for 1-D codes with proposed anti-jamming technique

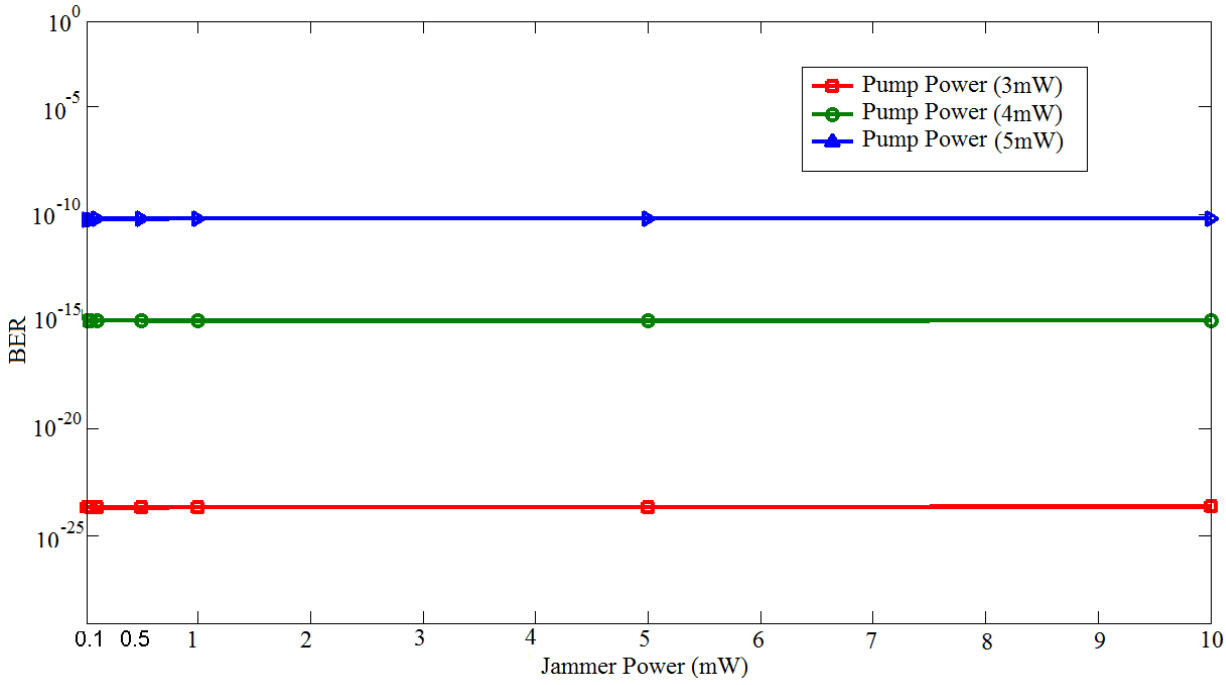


Figure 5.12: BER versus jammer power for 2-D codes with proposed anti-jamming technique

Further, the eye diagrams are also obtained for 1-D and 2-D coded OCDMA as shown in figures 5.13 and 5.14 respectively, when wavelength conversion is applied. A good eye opening with acceptable BER at receiver is found for both the cases. An increased eye opening is observed for 2-D codes with low BER at receiver as compared to 1-D coded OCDMA. Hence 2-D system performs better than 1-D code with the proposed technique.

Also OCDMA with 3-D codes are simulated with the proposed anti-jamming technique. The BER observed was essentially, almost equal to zero. Hence, it could not be plotted. Therefore, only an eye diagram is presented instead. A clear eye diagram is observed as shown in figure 5.15. This means receiver is correctly receiving the information data nullifying the effect of jammer. Hence, information is transmitted securely even in the presence of high power jammer with the use of SOA based wavelength converter. Moreover, 3-D OCDMA performs better than 2-D OCDMA using the wavelength conversion technology. This means that the proposed scheme is compatible with all type of OCDMA with different coding dimensions. The OCDMA system performs as said in the research literature that 3-D has better system performance than 2-D and 2-D has better system performance than 1-D even with the novel technology.

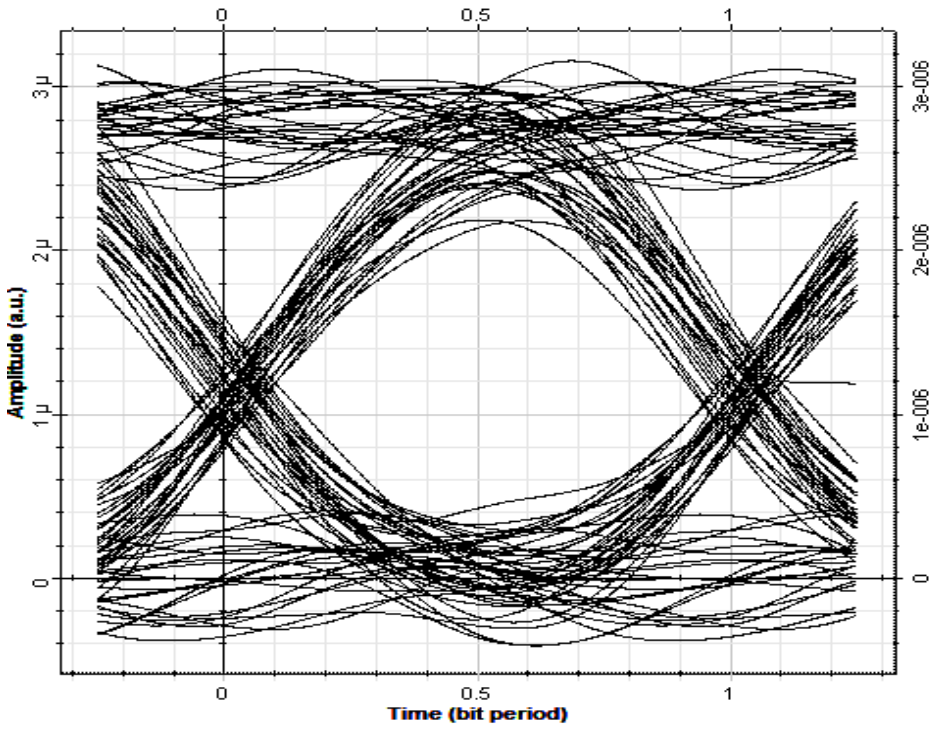


Figure 5.13: Eye diagram for 1-D OCDMA with proposed anti-jamming technique

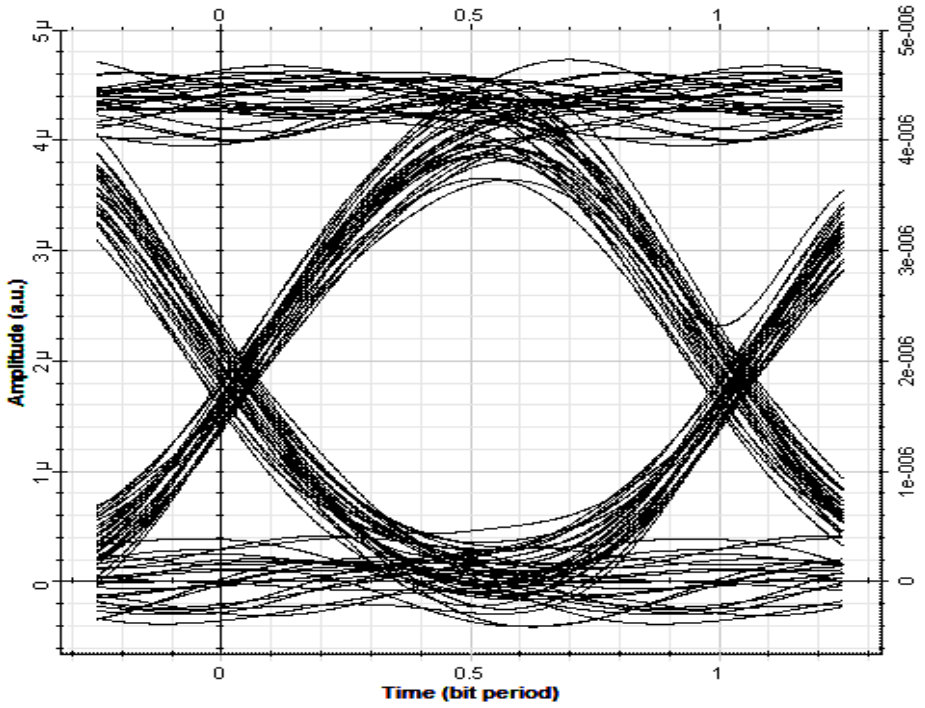


Figure 5.14: Eye diagram for 2-D OCDMA with proposed anti-jamming technique

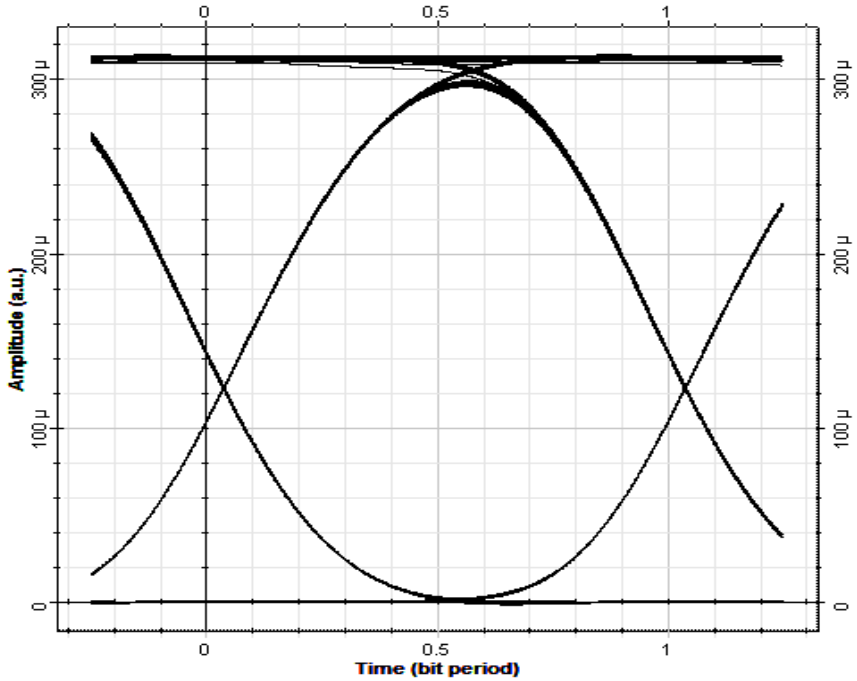


Figure 5.15: Eye diagram for 3-D OCDMA with proposed anti-jamming technique

Therefore, strict security against jamming is achieved using the four wave mixing in SOA for wavelength conversion process for all type of OCDMA technologies.

Furthermore, the input signal power and the pump power are two important parameters for the performance of wavelength converter. The pump is an essential part of wavelength converter. The effective FWM depends upon the pump power. So, to choose the optimal pump power against the particular input power, BER versus pump power curve is plotted. Figure 5.16 and figure 5.17 show the BER variation against different pump powers for 1-D and 2-D codes respectively. In both the cases it can be seen that BER becomes high with the increase in pump power. So, optimal values for pump power are chosen for acceptable BER at receiver in order to enhance FWM effect in SOA. It is further observed that high pump powers are required for high input power to pronounce the four wave mixing effect.

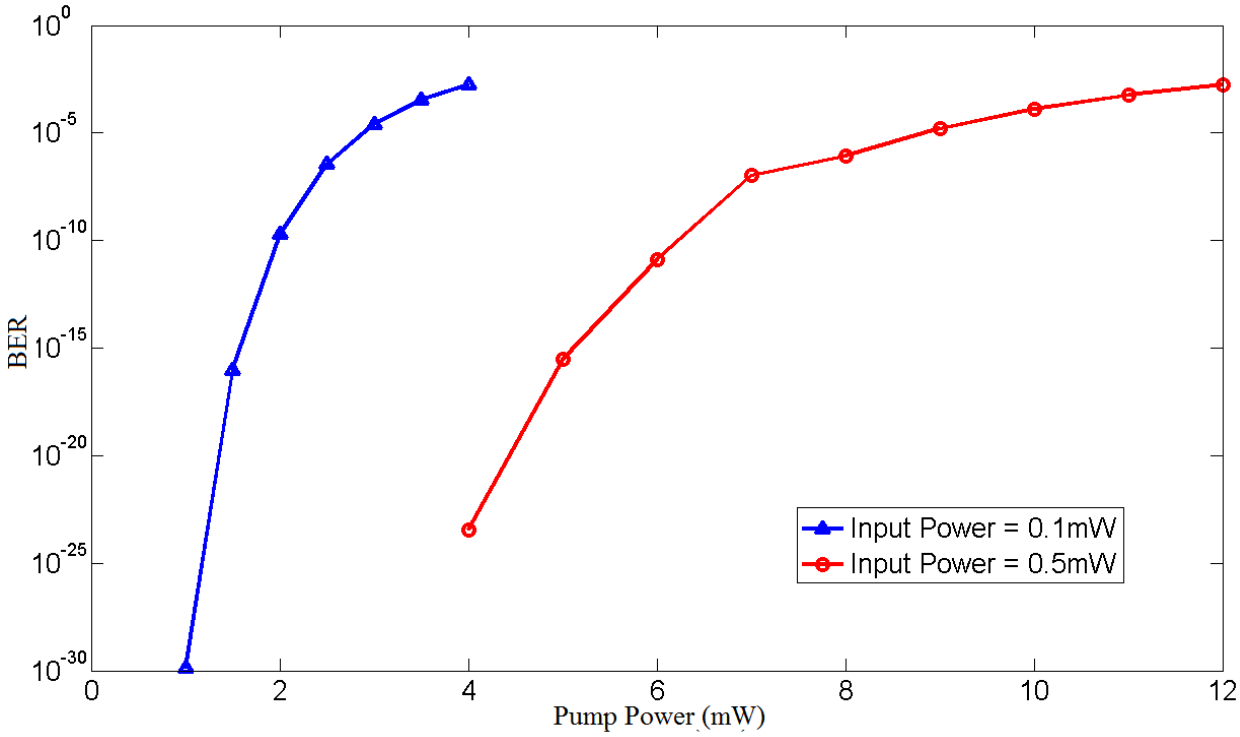


Figure 5.16: BER versus pump power for 1-D codes with proposed anti-jamming technique

However, the results obtained for anti-jamming OCDMA system have shown that the proposed wavelength conversion technique effectively converts the wavelengths and maintains low BER at receiver even at the low input powers. Therefore, the low pump powers can be used against

the low input power. The use of low pump powers makes the system suitable for practical implementation.

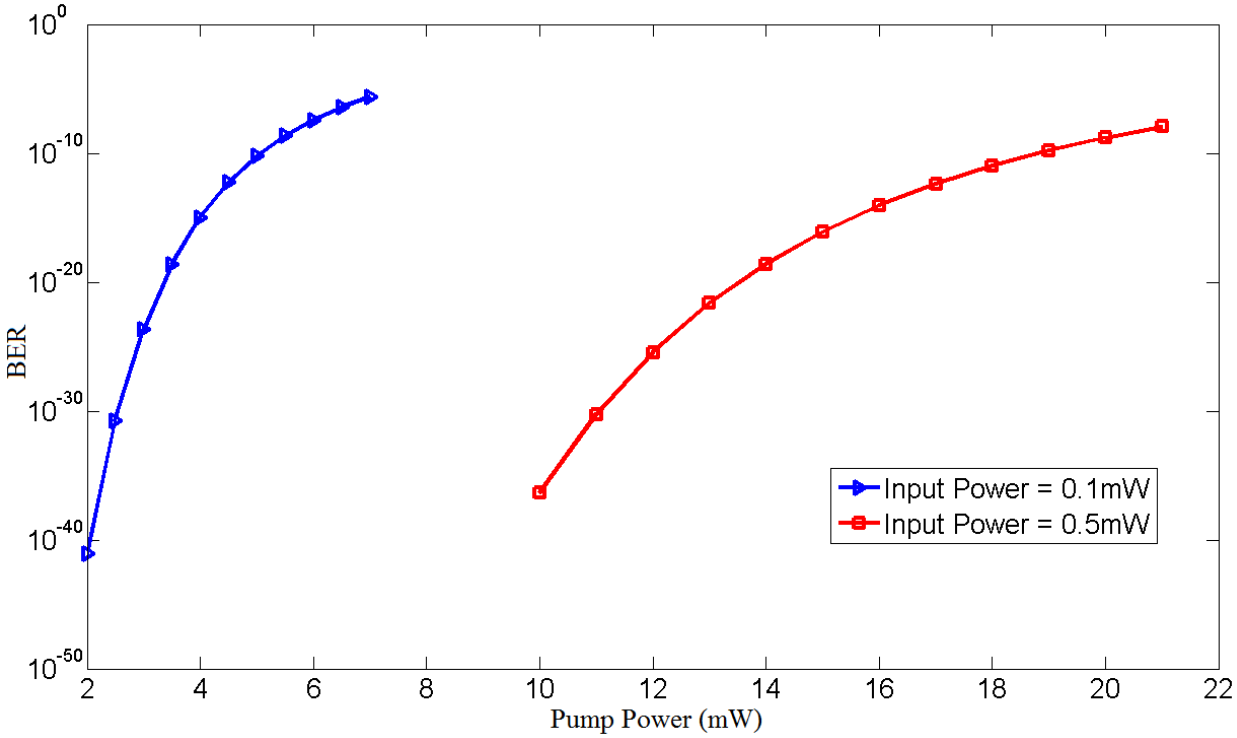


Figure 5.17: BER versus pump power for 2-D codes with proposed anti-jamming technique

5.4 Conclusion

The validation of proposed security enhancement techniques against eavesdropping and jamming is done in this chapter. We validate the novel virtual user scheme by using an analytical model. It is verified that the confidentiality is enhanced by 25% for synchronous transmission and 37.5% for asynchronous transmission in case of OOK-OCDMA against simple energy eavesdropper and 50% in case of CSK-OCDMA against differential eavesdropper. In addition, we have validated the accuracy of proposed anti-jamming approach through simulation experiments on other software using different types of codes. It is found that data availability at the receiver remains unaffected even in the presence of high power jammer using the proposed anti-jamming technique. Hence, information security of an OCDMA system is improved essentially using the virtual user scheme and SOA based wavelength converter.

Chapter 6

Conclusion and Future Scope

This chapter summarizes the main findings of the dissertation. The objectives of research, outlined in chapter 1, are reviewed and the work done towards the achievement of each objective is addressed. Also, in this chapter, the recommendations and scope for further research is given.

6.1 Conclusion

The essence of this research work is well encapsulated by the title of this work, namely "Security enhancement in optical code division multiple access network". Optical code division multiple access technology is not as secure as generally perceived despite its coded nature. The increasing number of ways with added sophistication for extracting and injecting information into a fiber link makes it easy to breach the network security. In this dissertation, the two aspects of security: data confidentiality and signal availability are analyzed. As discussed in previous chapters, data confidentiality is related to security against eavesdropping which is the extraction of information considered private and signal availability refers to the security against jamming which is the intentional injection of the interference to disrupt communication.

The work done towards the achievement of proposed objectives is summarized objective wise below.

- To propose a technique to increase the confidentiality of OCDMA system against eavesdropping.

The confidentiality enhancement against eavesdropping in an OCDMA network is done under this objective. Firstly, the locations in OCDMA network where a user can be isolated are identified. Then the code interception performance of an eavesdropper for single transmitting user is analyzed. The results show the vulnerability of isolated user signal access to simple eavesdropping strategies. It is also seen that 1-D coded OCDMA is easy to eavesdrop as compared to 2-D and 3-D coded OCDMA. Therefore, a novel technique called virtual user technique is proposed to avoid the access to isolated transmitting users having vulnerability to simple eavesdropping strategies. VUS actually causes multiple access interference which makes

it difficult for an eavesdropper to extract the actual message being transmitted without the knowledge of the code used. The eavesdropper's probability of correct bit interception in presence of virtual user is analyzed. The results show that the virtual user degrades the code intercepting performance of an eavesdropper. To make it bandwidth efficient, a modified VUS is proposed where an intelligent feedback control is incorporated into the virtual user environment. The proposed technique is simulated with on-off keying OCDMA, code shift keying OCDMA and differential phase shift keying OCDMA. The results obtained for the proposed technique are compared with the existing schemes. OOK-OCDMA is vulnerable to simple power detector while CSK-OCDMA and DPSK-OCDMA are vulnerable to differential eavesdropping. The results obtained show that the proposed virtual user scheme is immune to both simple energy detector (for OOK-OCDMA) and differential eavesdropper (for CSK-OCDMA and DPSK-OCDMA). Further, it has been reported that use of virtual user scheme does not impose any additional bandwidth penalty by wasting the available codes as the virtual user is active only when a user is isolated. Also, a single active virtual user along with the isolated user signal does not degrade the received signal. Therefore, the confidentiality of an OCDMA system is successfully enhanced using the novel technique without affecting the received signal.

- To propose a technique for security enhancement of OCDMA system in terms of availability of signal against jamming.

In this objective, signal availability is increased against jamming attack in an OCDMA network. An OCDMA network with a jammer transmitting in the authorized user's waveband is considered. The results show that the high power pulse jammer easily overpowers the authorized signal at receiver, resulting in disruption of the communication. Therefore, a novel technique is proposed to combat the intentional interference caused by the jammer. A wavelength conversion technique is used to restore the communication link by translating the information to different wavelengths. Our proposed technique utilizes the four-wave mixing in SOA for wavelength conversion to take the signal wavelength out of the jamming window. Hence, the proposed anti-jamming scheme is based on wavelength conversion. A wavelength converter is placed after the OCDMA encoder, which translates the encoded data to a new set of wavelengths. Similarly, a wavelength de-converter is placed before the OCDMA decoder to convert the translated wavelengths to the original set of wavelengths which were used at encoder. The spectrum

carrying the data bits is measured at different points in the network. The results obtained for the proposed anti-jamming technique in OCDMA network are compared with an OCDMA system without any jamming resistance. It is shown that the transmitted and received signals are the same when the proposed wavelength converter is used with the conventional OCDMA network. The FWM in SOA completely negates the effect of jamming in OCDMA network by shifting the data to wavelengths outside the jamming window. It is seen that the message signal can be successfully transmitted even when the jammer power is very high. Moreover, compactness of SOA enables integration; transparency to bit rates adds flexibility and low power to trigger nonlinearity makes it an attractive choice for practical implementation. Therefore, communication cannot be disrupted when SOA based wavelength converter is used and data can be securely transmitted in the presence of a jammer.

- To validate the proposed techniques for OCDMA system.

Finally, the validation of the novel techniques proposed for security enhancement against eavesdropping and jamming is done. Firstly, the technique proposed for confidentiality enhancement against eavesdropping is validated. A mathematical analysis is carried out for OOK-OCDMA and CSK-OCDMA with the proposed technique. It is shown analytically that the proposed virtual user scheme increases the probability of false detection of data at eavesdropper by 25% for synchronous transmission and 37.5% for asynchronous transmission in case of OOK-OCDMA. For CSK-OCDMA, only synchronous transmission is considered for the worst case scenario. The analysis shows that the probability of falsely detecting the data at differential eavesdropper increases by 50% in case of CSK-OCDMA. Therefore, it is clear that the novel virtual user scheme effectively increases the confidentiality of an OCDMA system.

Also, the validation of novel anti-jamming technique is carried out by simulating the same system on multiple softwares i.e. OptSim and Optisystem. The proposed OCDMA system is simulated and similar results are obtained for the proposed anti-jamming technique using both the software. The results show that information can be successfully transmitted using the proposed scheme, even when a high power jammer is transmitting in the user's waveband. In addition, to see the effectiveness of the proposed approach, it is simulated using different types of codes i.e. 1-D, 2-D and 3-D codes. The results show that the data availability at receiver remains unaffected for 1-D, 2-D and 3-D OCDMA using the proposed anti-jamming technique,

in the presence of a high power pulse jammer. The comparison of the proposed anti-jamming technique with previously proposed techniques in literature shows that it is better in terms of security performance and is free from the limitations of the previous ones.

Hence, information security of an OCDMA system is improved essentially against eavesdropping and jamming using the virtual user scheme and SOA based wavelength converter respectively.

6.2 Recommendations

The techniques are proposed to increase the OCDMA network security against eavesdropping and jamming attack. Hence, the OCDMA system with proposed techniques is recommended for sensitive data transactions such as personal data, financial data, military transactions and intellectual property transactions on the internet where the confidential transmission of data without being jammed is of prime importance. The recommendations on the basis of results obtained in previous chapters are given below.

- The novel virtual user technique proposed in chapter 3 increases data confidentiality in OCDMA network by a simple addition of an active user which mimics the MAI. It increases the security of OOK-OCDMA against both the simple power detector and differential eavesdropper as compared to already proposed code switching scheme which is secure to only simple power detector.
- Our proposed technique based on virtual user scheme further increases the confidentiality of security enhanced schemes such as CSK-OCDMA and DPSK-OCDMA against differential eavesdropping.
- The novel technique to achieve anti-jamming in OCDMA network proposed in chapter 4, exploits the four-wave mixing in SOA for wavelength conversion. Our model is transparent to bit rate and modulation format, has non-inverting output and low energy requirements to trigger their non-linearity. Further, the compactness of SOA based devices enables device integration as compared to converters based on PPLN waveguides with moderate lengths.
- Our proposed model for anti-jamming has an intrinsic high efficiency as compared to the Bi-NLF based wavelength converters which suffers from different losses when spliced

with single mode fiber. Further, bismuth based fibers exhibit large propagation loss due to bismuth oxide.

- The pump used in wavelength converter is tunable which adds the flexibility to attain different converted wavelengths against different jamming wavelengths in OCDMA network by increasing the wavelength conversion range.

6.3 Future Scope

Throughout the thesis, specific topics have been identified which have a potential for further research. The flexibility and variety in OCDMA approaches has a capability to play significant role in near future.

- In this research study, the security concerns of data confidentiality against eavesdropping and signal availability against jamming are addressed to increase the photonic layer security in OCDMA network. However, the potential of OCDMA to provide security functions such as signal integrity and authentication remains an open area of research.
- The design of virtual user scheme in OCDMA network with intelligent feedback control increases network security against eavesdropping but poses the challenge of increased system complexity. Hence, increased security is obtained at the expense of increased system complexity which may increase the cost of network management. Therefore, there is a need to investigate simpler and efficient decentralized OCDMA network with increased network confidentiality.
- The novel virtual user technique increases data confidentiality in OCDMA network by a simple addition of an active user which mimics the MAI. The proposed OCDMA can be used with MAC (media access control) protocol to increase the network throughput to increase the number of successfully received packets in presence of MAI.
- The amplified spontaneous noise generated in SOA limits the performance of SOA as wavelength converter. Hence, further study is required to reduce the effect of ASE on the wavelength conversion capability of anti-jammer in OCDMA network.
- The FWM in SOA can be used to convert the multiple wavelengths simultaneously to the other set of wavelengths known as waveband conversion. The attribute of waveband conversion can reduce the component count in OCDMA network by replacing a set

wavelength converters with a single waveband converter. Hence, the OCDMA system can be modeled with waveband conversion as an anti-jammer with reduced system complexity.

- The new system models to increase security are proposed and simulated. Although validation of the proposed techniques is done using mathematical analyses and multiple software testing, the experimental verification is required to consider its application in practical world.

References

[1] V. K. Jain, J. Franz and F. Matera "Emerging Trends in Fiber Optic Networks," Fiber and Integrated Optics, Vol. 20, No. 2, pp. 95-124, 2001.

[2] John M. Senior, "Optical Fiber Communications Principles and Practice," Second Edition, Pearson Education, India, 2006.

[3] Gerd Keiser, "Optical Fiber Communications," Third Edition, McGraw-Hill, New York, 2000.

[4] D.J.G. Mestdagh, "Fundamentals of Multiaccess Optical Fiber Networks," Artech House, London, 1995.

[5] Izhak Rubin, "Message Delays in FDMA and TDMA channels," IEEE Transactions on Communications, Vol. 27, No. 5, pp: 769-777, May 1979.

[6] Theodore S. Rappaport, "Wireless Communications: Principles and Practice," Second Edition, Prentice Hall, 2007.

[7] www.umtsworld.com/technology/cdmabasics.htm.

[8] Paul R. Prucnal, Mairo A. Santoro and Ting R. Fan, "Spread Spectrum Fiber-optic Local Area Network Using Optical Processing," IEEE Journal of Lightwave Technology, Vol. 4, No. 5, pp. 547-554, May 1986.

[9] A. M. Weiner, J. P. Heritage and J. A. Salehi, "Encoding and Decoding of Femtosecond Pulses," Optics Letters, Vol. 13, No. 4, pp. 300–302, April 1988.

[10] Andrew Stok and Edward H. Sargent, "Lighting the Local Area: Optical Code-Division Multiple Access and Quality of Service Provisioning," IEEE Network, Vol. 14, No. 6, pp. 42-46, Nov/Dec. 2000.

[11] Kerim Fouli and Martin Maier, "OCDMA and Optical Coding: Principles, Applications, and Challenges," IEEE Communications Magazine, Vol. 45, No. 8, pp. 27- 34, Aug 2007.

[12] V. K. Jain and Giancarlo De Marchis, “Hybrid Wavelength and Code Division Multiple Access in Optical Networks,” Fiber and Integrated Optics, Vol. 20, No. 1, pp. 1–19, 2001.

[13] Nikos Karafolas, “Optical Fiber Code Division Multiple Access Networks: A Review,” Optical Fiber Technology, Vol. 2, No. 2, pp. 149–168, April 1996.

[14] Guu Chang Yang and Wing C. Kwang, “Prime Codes with Applications to CDMA Optical and Wireless Networks” Arctech house Boston London

[15] Andreas Karlsson, “Simulation of a CDMA system based on optical orthogonal codes,” Thesis, Linkopings University, 14th April 2004.

[16] Manoj Choudhary, P.K.Chatterjee and Joseph John, “Optical Orthogonal Codes using Error Correcting Codes,” Proceedings of the Eighth National Conferenece on Communications (NCC-2002), IIT Bombay, pp. 65-69, Jan 2002.

[17] Jawed A Salehi, “Code Division Multiple-Access Techniques in Optical Fiber Networks-Part I: Fundamental Principles,” IEEE Transactions on Communications, Vol. 37, No. 8, pp. 824-833, Aug 1989.

[18] F. R. K. Chung and Jawed A. Salehi, “Optical Orthogonal Codes: Design, Analysis and Applications,” IEEE Transactions on Information Theory, Vol. 35, No. 3, pp. 595-604, May 1989.

[19] Jawed A. Salehi and Charles A. Brackett, “Code Division Multiple-Access Techniques in Optical Fiber Networks-Part 11: Systems Performance Analysis,” IEEE Transactions on Communications, Vol. 31, No. 8, pp. 834-842, Aug 1989.

[20] Bin Ni and James S. Lehnert, “Performance of an Incoherent Temporal-Spreading OCDMA System with Broadband Light Sources,” IEEE Journal of Lightwave Technology, Vol. 23, No. 7, pp. 2206-2214, July 2005.

[21] E. Inaty, H. M. H. Shalaby, P. Fortier, and L. A. Rusch, “Multirate Optical Fast Frequency Hopping CDMA System Using Power Control,” IEEE Journal of Lightwave Technology, Vol. 20, No. 2, pp. 166–177, Feb 2002.

[22] K. Yu, J. Shin, and N. Park, "Wavelength-time Spreading Optical CDMA Systems Using Wavelength Multiplexers and Mirrored Fiber Delay Line," IEEE Photonics Technology Letters, Vol. 12, No. 9, pp. 1278–1280, Sept 2000.

[23] Antonio J. Mendez, Robert M. Gagliardi, Vincent J. Hernandez, Corey V. Bennet, and William J. Lennon, "Design and Performance Analysis of Wavelength/Time (W/T) Matrix Codes for Optical CDMA," IEEE Journal of Lightwave Technology, Vol. 21, No. 11, pp. 2524-2533, Nov 2003.

[24] Jaswinder Singh and Maninder Lal Singh, "Design of 3-D Wavelength/Time/Space Codes for Asynchronous Fiber-Optic CDMA Systems," IEEE Photonics Technology Letters, Vol. 22, No. 3, pp. 131-133, Feb. 2010.

[25] Sangin Kim, Kyungsik Yu, and Namkyoo Park, "A New Family of Space/Wavelength/Time Spread Three-Dimensional Optical Code for OCDMA Networks," IEEE Journal of Lightwave Technology, Vol. 18, No. 4, pp. 502-511, April 2000.

[26] J. E. McGeehan, S. M. R. Motaghian Nezam, P. Saghari, T. H. Izadpanah, A. E. Willner, R. Omrani, and P. V. Knmar, "3D Time-Wavelength-Polarization OCDMA Coding for Increasing the Number of Users in OCDMA LANs," Proceedings of Optical Fiber Communication Conference (OFC 2004), Los Angeles, CA, USA. Vol. 2, 2004.

[27] J. E. McGeehan, S. M. R. Motaghian Nezam, P. Saghari, Alan E. Willner, Reza Omrani and P. Vijay Kumar, "Experimental Demonstration of OCDMA Transmission Using a Three-Dimensional (Time–Wavelength–Polarization) Codeset," IEEE Journal of Lightwave Technology, Vol. 23, No. 10, pp. 3282-3289, Oct 2005.

[28] Paul R. Prucnal, "Optical Code Division Multiple Access: Fundamentals and Applications." Taylor & Francis Group, 2006.

[29] Hongxi Yin and David J. Richardson, "Optical Code Division Multiple Access Communication Networks Theory and Applications," Tsinghua University Press, Beijing and Springer-Verlag GmbH Berlin Heidelberg, 2007

[30] Tomoaki Ohtsuki and Iwao Sasase, "Optical Synchronous CDMA, Encyclopedia of Telecommunications," Editor: John Proakis, Wiley, 2002.

[31] Kohki Ohba, Iwao Sasase, and Takaya Miyazawa "A Mitigation Technique of High-Power MAI in the Optical CDMA System with the Optical Power Selector," IEEE Global Telecommunications Conference, (GLOBECOM '07), pp. 2401 – 2406, 2007.

[32] M. Medard, D. Marquis, R. A. Barry, and S. G. Finn, "Security Issues in All Optical Networks," IEEE Network, Vol. 11, No. 3, pp. 42-48, June 1997.

[33] G.V.S. Raju and Rehan Akbani "Mobile Ad Hoc Networks Security," Annual Review of Communications, Vol. 58, pp. 625-628, Nov 2005.

[34] www.rootsecure.net/content/downloads/pdf/fiber_optic_taps.pdf

[35] Bernard Everett, "Tapping into fiber optic cables," Network Security, Vol. 2007, No. 5, pp. 13- 16, May 2007.

[36] Keith Shaneman and Stuart Gray, "Optical Network Security: Technical Analysis of Fiber Tapping Mechanisms and Methods for Detection & Prevention," Proceedings of IEEE Military Communications Conference (MILCOM-2004), Monterey, CA. November 2004.

[37] M. Z. Iqbal, H. Fathallah, and N. Belhadj, "Optical fiber tapping: Methods and precautions," Proceedings of High Capacity Optical Networks and Enabling Technologies Conference (HONET-2011), Riyadh, pp.164-168, Dec. 2011.

[38] Kimberlie Witcher, "Fiber Optics and its Security Vulnerabilities," Sans Institute, GIAC Security Essentials Certification University Mary Washington, Feb 2005.

[39] Thomas H. Shake, "Security Performance of Optical CDMA Against Eavesdropping," IEEE Journal of Lightwave Technology, Vol. 23, No. 2, pp. 655-670, Feb 2005.

[40] Thomas H. Shake, "Confidentiality Performance of Spectral-Phase-Encoded Optical CDMA" IEEE Journal of Lightwave Technology, Vol. 23, No. 4, pp. 1652-1653, April 2005.

[41] A. Stok and E. H. Sargent "The Role of Optical CDMA in Access Networks," IEEE Communication Magazine, Vol. 40, No. 9, pp. 83-87, Nov 2002.

[42] B. Dai, Z. Gao, X. Wang, N. Kataoka and N. Wada, "Demonstration of Differential Detection on Attacking Code-Shift-Keying OCDMA System," IET Electronics Letters, Vol. 46, No. 25, pp. 1680–1682, 2010.

[43] A. Mishra and K. M. Nadkarni, "Security in Wireless Ad Hoc Networks" The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

[44] M. R. Wilson, "The Quantitative Impact of Survivable Network Architectures on Service Availability," IEEE Communications Magazine, Vol. 36, No. 5, pp. 122-126, May 1998.

[45] A. Teixeira, A. Vieira, J. Andrade, A. Quinta, M. Lima, R. Nogueira, P. André, and G. Tosi Beleffi, "Security Issues in Optical Networks Physical Layer," Proceedings of International Conference on Transparent Optical Networks (ICTON'08), Athens, Vol. 4, pp. 123-126, June 2008.

[46] Mohammad J. Emadi and Jawad A. Salehi "Jamming Resistance Capabilities of the Spectrally Phase Encoded OCDMA Systems," Proceedings of International Symposium on Telecommunications (IST-08), Tehran, pp. 204-208, Aug. 2008.

[47] L. Zhou and Z. J. Hass, "Securing Ad Hoc Networks," IEEE Networks: Special Issue on Network Security, Vol. 13, pp. 24-30, Nov/Dec 1999.

[48] Gabriella Cincotti, Valentina Sacchieri, Gianluca Manzacca, Nobuyuki Kataoka Naoya Wada, Naoki Nakagawa and Ken-ichi Kitayama, "Physical Layer Security: All-Optical Cryptography in Access Networks," Proceedings of International Conference on Transparent Optical Networks (ICTON'08), Athens, Vol. 4, pp. 127-130, June 2008.

[49] D.D.Sampson, G.J. Pendock, and R.A. Griffin, "Photonic Code-Division Multiple Access Communications," Fiber and Integrated Optics, Vol. 16, No. 12, pp. 129–157, 1997.

[50] D. E. Leaird, Z. Jiang, and A. M.Weiner, "Experimental Investigation of Security Issues in OCDMA: A Code-Switching Scheme," IET Electronics Letters, Vol. 41, No. 14, pp.817–819, 2005.

[51] X. Wang, N. Wada, T. Miyazaki, G. Cincotti, and K. Kitayama, "Asynchronous Multiuser Coherent OCDMA System with Code-Shift-Keying and Balanced Detection," IEEE Journal of Selected Topics in Quantum Electronics, Vol. 13, No. 5, pp. 1463–1470, 2007.

[52] Hwan Seok Chung, SunHyok Chang, BongKyu Kim, and Kwangjoon Kim, "Security Enhanced OCDMA System Based on Incoherent Broadband Light Source and Bipolar Coding," Proceedings of Optical Fiber Communication and the National Fiber Optic Engineers Conference (OFC/NFOEC 2007), Anaheim, CA, pp. 1-3, March 2007.

[53] Hwan Seok Chung, Sun Hyok Chang, Bong Kyu Kim, and Kwangjoon Kim, "Experimental Demonstration of Security-Improved OCDMA Scheme Based on Incoherent Broadband Light Source and Bipolar Coding," Optical Fiber Technology, Vol. 14, No. 2, pp. 130-133, 2008.

[54] X. Wang, N. Wada, T. Miyazaki, and K. Kitayama, "Coherent OCDMA System using DPSK Data Format with Balanced Detection," IEEE Photonics Technology Letters, Vol. 18, No.7, pp. 826-828, April 2006.

[55] Z. Jiang, D.E. Leaird, and A.M. Weiner, "Experimental Investigation of Security Issues in OCDMA," IEEE Journal of Lightwave Technology, Vol. 24, No. 11, pp. 4228-4234, 2006.

[56] D.E. Leaird, C.-B. Huang, Z. Jiang1, S.-G. Park, and A.M. Weiner, "DPSK Based Eavesdropper Vulnerability in Two-Code Keyed O-CDMA Systems," Proceedings of Optical Fiber communication and National Fiber Optic Engineers Conference (OFC/NFOEC 2008), San Diego, CA, pp. 1-3, Feb. 2008.

[57] B. Dai, Z. Gao, X. Wang, N. Kataoka and N. Wada, "Experimental Investigation on Security of Temporal Phase Coding OCDMA System with Code-Shift Keying and

Differential Phase-Shift Keying," Proceedings of Asia Communications and Photonics Conference and Exhibition (ACP-2010), Shanghai, China, pp. 427-428, Dec 2010.

[58] Fei Xue, Yixue Du, S.J. Ben Yoo and Zhi Ding, "Security Issues on Spectral Phase-Encoded Optical CDMA with Phase-masking Scheme," Proceedings of Optical Fiber Communication Conference and National Fiber Optic Engineers Conference (OFC/NFOEC 2006), March 2006.

[59] Valentina Sacchieri, Pedro Teixeira, Antonio Teixeira, and Gabriella Cincotti, "Secure OCDMA Transmission Using Data Pattern Scrambling," Proceedings of Transparent Optical Networks, Anniversary International Conference (ICTON-08), Athens, Vol. 1, pp. 51-54, June 2008.

[60] Mable P. Fok and Paul R. Prucnal, "All-Optical Encryption for Optical Network with Interleaved Waveband Switching Modulation," Optical Society of America, Vol. 34, No. 9, pp. 1315-1317, March 2009.

[61] Natalie Kostinski, Konstantin Kravtsov, and Paul R. Prucnal, "Demonstration of an All-Optical OCDMA Encryption and Decryption System with Variable Two-Code Keying," IEEE Photonics Technology Letters, Vol. 20, No. 24, pp. 2045-2047, Dec 2008.

[62] Zhenxing Wang, Yue-Kai Huang, Yanhua Deng, John Chang, and Paul R. Prucnal, "Optical Encryption With OCDMA Code Swapping Using All-Optical XOR Logic Gate," IEEE Photonics Technology Letters, Vol. 21, No. 7, pp. 411-413, April 2009.

[63] Mable P. Fok and Paul R. Prucnal, "Optical Steganography Using Chirped Fiber Bragg Grating," Proceedings of Optical Fiber Communications Conference (OFC-2009), San Diego, CA, pp. 1-3, March 2009.

[64] Paul R. Prucnal, Mable P. Fok, Konstantin Kravtsov, and Zhenxing Wang, "Optical Steganography for Data Hiding in Optical Networks," Proceedings of 16th International Conference on Digital Signal Processing, Santorini-Hellas, pp. 1-6, July 2009.

[65] Mohammed J. Emadi, and Jawad A. Salehi, "Jamming Resistance Capabilities of the Spectrally Phase Encoded OCDMA Systems with Optimum and Suboptimum (Nonlinear

Two-Photon-Absorption) Receiver Structures," IEEE Journal of Lightwave Communication, Vol. 27, No. 22, pp. 5010-5021, Nov. 2009.

[66] Mable P. Fok and Paul R. Prucnal, "Low-Latency Nonlinear Fiber-Based Approach for Data Encryption and Anti-Jamming in Optical Network," Proceedings of 21st Annual Meeting IEEE Lasers and Electro-Optics Society (LEOS-2008), Acapulco, pp. 743–744, Nov. 2008.

[67] Mable P. Fok, Yanhua Deng, and Paul R. Prucnal, "Physical Layer Network Security Based on Optical Processing using Compact Passive Devices," Proceedings of 14th OptoElectronics and Communications Conference (OECC-2009), Hong Kong, pp. 1–2, July 2009.

[68] Zhenxing Wang, Aref Chowdhury, and Paul R. Prucnal, "Optical CDMA Code Wavelength Conversion Using PPLN to Improve Transmission Security," IEEE Photonics Technology Letters, Vol. 21, No. 6, pp. 383-385, March 2009.

[69] G. Cincotti, N. Kataoka, N. Wada and K. Kitayama, "Perspectives of Optical Coding/Decoding Techniques in OCDMA Networks," Proceedings of Asia Communications and Photonics Conference and Exhibition (ACP-2009), Shanghai, China, pp.1-2, Nov 2009.

[70] M. Y. Azizoglu, J. A. Salehi, and Y. Li, "Optical CDMA via Temporal Codes," IEEE Transactions on Communications, Vol. 40, No. 7, pp. 1162–1170, 1992.

[71] E. Narimanov, W. C. Kwong, Yang Guu-Chang, and P. R. Prucnal, "Shifted Carrier-Hopping Prime Codes for Multicode Keying in Wavelength-Time O-CDMA," IEEE Transactions on Communications, Vol. 53, No. 12, pp. 2150–2156, 2005.

[72] A. J. Mendez, R. M. Gagliardi, H. X. C. Feng, J. P. Heritage, and J. M. Morookian, "Strategies for Realizing Optical CDMA for Dense, High-Speed, Long Span, Optical Network Applications," IEEE Journal of Lightwave Technology, Vol. 18, No. 12, pp. 1685-1696, Dec 2000.

[73] A. J. Mendez, R. M. Gagliardi, V. J. Hernandez, C. V. Bennet and W. J. Lennon, "High-Performance Optical CDMA System Based on 2-D Optical Orthogonal Codes," IEEE Journal of Lightwave Technology, Vol. 22, No. 11, pp. 2409-2419, Nov 2004.

[74] K.J. Horadam, "Hadamard Matrices and Their Applications," Princeton University Press, 1986.

[75] X. Wang, N. Wada, T. Miyazaki and K. Kitayama, "Demonstration of DPSK-OCDMA with Balanced Detection to Improve MAI and Beat Noise Tolerance in OCDMA System," Proceedings of Optical Fiber Communication Conference and National Fiber Optic Engineers Conference (OFC/NFOEC- 2006), Anaheim, USA, March 2006.

[76] X. Wang, N. Wada, T. Miyazaki, G. Cincotti and K. Kitayama, "Advanced Modulation Techniques in OCDMA System," Proceedings of Optical Fiber Communication and Optoelectronics Conference, Shanghai, Asia, pp.100-102, Oct. 2007.

[77] J. S. Chitode, "Principles of Communication," Technical Publications, Pune, pp.12-18, 2009.

[78] M. S. Anuar, S. A. Aljunid, R. Badlishah, N. M. Saad and I. Andonomic, "Performance Analysis of Optical Zero Cross Correlation in OCDMA System," Journal of Applied Science, Vol. 7, No. 23, pp. 3819-3822, 2007.

[79] Xiaogang Chen, Deyi Chen, and Zonglong Wang, "Performance Improvement of Bandwidth-Limited Coherent OCDMA System," Photonics Networks Communications, Vol. 16, pp.149–154, 2008.

[80] RSoft Design Group, "OptSim Models Reference: Block Mode" Vol. II, pp 320.

[81] Weiwei Fan, Bok Hyeon Kim, Lin Htein and Won-Taek Han, "Linear and Nonlinear Optical Properties of Bi-doped Germano-Silicate Optical Fiber," Journal of Optics, Vol. 14, No. 12, pp. 125201, 2012.

[82] M. Jamshidifar, A. Vedadi, D.S. Govan and M.E. Marhic, "Continuous-wave parametric amplification in bismuth-oxide fibers," Optical Fiber Technology, Vol. 16, No. 6, pp. 458–466, Oct 2010.

[83] C. Politi, C. Matrakidis, and A. Stavdas, "Optical wavelength and waveband converters," Proceedings of International Conference on Transparent Optical Networks (ICTON-2006), Nottingham, pp. 179–182, June 2006.

[84] M. P. Fok, Wang Zhexing, Deng Yanhua and P. R. Prucnal, "Optical Layer Security in Fiber-Optic Networks," IEEE Transactions on Information Forensics and Security, Vol. 6 , No. 3 , pp 725 – 736, Sept. 2011.

[85] Byrav Ramamurthy, and Biswanath Mukherjee, "Wavelength Conversion in WDM Networking," IEEE Journal on Selected Areas in Communications, Vol. 16, No. 7, pp. 1061-1073, Sept 1998.

[86] Cristiano M. Gallep, Harmen J. S. Dorren, and Oded Raz, "Four-Wave-Mixing Based Dual-Wavelength Conversion in a Semiconductor Optical Amplifier," IEEE Photonics Technology Letters, Vol. 22, No. 21, pp. 1550-1552, Nov 2010.

[87] S. Diez, C. Schmidt, R. Ludwig, H.G. Weber, K. Obermann, S. Kindt, I. Koltchanov, and K. Petermann, "Four-wave mixing in Semiconductor Optical Amplifiers for Frequency Conversion and Fast Optical Switching," IEEE Journal of Selected Topics in Quantum Electronics, Vol. 3, No. 5, pp. 1131–1145, Oct. 1997.

[88] Ian White, Richard Penty, Matthew Webster, Yew Jun Chai, Adrian Wonfor, and Sadegh Shahkooh, "Wavelength Switching Components for Future Photonic Networks," IEEE Communications Magazine, Vol. 40, No. 9, pp. 74-81, Sept. 2002.

[89] S. Olonkins, V. Bobrovs, and G. Ivanovs, "Comparison of Semiconductor Optical Amplifier and Discrete Raman Amplifier Performance in DWDM Systems," Electronics and Electrical Engineering (ISSN 1392 – 1215), Vol. 7, No. 123, pp. 133-136, 2012

[90] S. J. B. Yoo, "Wavelength Conversion Technologies for WDM Network Applications," Journal of Lightwave Technology, Vol. 14, No. 6, pp. 955-966, June 1996.

[91] Hiroshi Ishikawa, Shigeki Watanabe, and Haruhiko Kuwatsuka, "Wavelength Conversion Technologies for Photonic Network Systems," Fujitsu Science and Technology, Vol. 35, No.1, pp. 126-138, July 1999.

[92] S. Singh, and R. S. Kaler, "Wide Band Optical Wavelength Converter Based on Four Wave Mixing using Optimized Semiconductor Optical Amplifier," Fiber and Integrated Optics, Vol. 25, No.3, pp. 213–230, 2006.

[93] S. Singh, Xiaohua Ye, and R. S. Kaler, "All Optical Wavelength Conversion Based on Cross Polarization Modulation in Semiconductor Optical Amplifier," IEEE Journal of Lightwave Technology, Vol. 31, No. 11, pp. 1783 – 1792, June 2013.

[94] C. Politi, D. Klonidis, and M. J. O'Mahony, "Waveband Converters Based on Four-Wave Mixing in SOAs," IEEE Journal of Lightwave Technology, Vol. 24, No. 3, pp. 1203–1217, 2006.

[95] S. Singh, and R.S. Kaler, "20-Gb/s and Higher Bit Rate Optical Wavelength Conversion for RZ-DPSK Signal Based on Four-Wave Mixing in Semiconductor Optical Amplifier," Fiber and Integrated Optics, Vol. 26, No. 5, pp. 295-308, 2007.

[96] David F. Geraghty, Robert B. Lee, Marc Verdiell, Mehrdad Ziari, Atul Mathur, and Kerry J. Vahala "Wavelength Conversion for WDM Communication Systems using Four-Wave Mixing in Semiconductor Optical Amplifiers," IEEE Journal of Selected Topics in Quantum Electronics, Vol. 3, No. 5, pp. 1146-1155, Oct 1997.

[97] F. R. K. Chung, M. kerner, M. G. O'Conner, J. A. Salehi, and V. K. Wei, "Encoding and Decoding for Code Division Multiple Access Systems," IEEE Transactions on Communications, Patent No. 4779266, Oct 1988.