A REVIEW ON SECURITY CONCERNS OF OPTICAL CODE DIVISION MULTIPLEXING SYSTEMS

Sajad nabi[1]

[1]M-Tech student, Department of ECE, Arya Institute of Engineering & Technology, kukas, jaipur, India.

Abstract* – *Security as well as capacity in optical transmission link could become a critical issue for some applications such as military networks or enterprise networks. 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 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 technology is an attractive solution for these applications since it provides format-independent security in physical layer while guaranteeing appreciably wide bandwidth. Enhanced information security is often said to be inherent in OCDMA technology due to its coded nature.

Keywords* – *security, optical transmission, information security, optical communication system.

I. INTRODUCTION

Twenty first century is era of Information technology. The phenomenal growth in the internet traffic has increased the bandwidth demand on the telecommunication industry. As the demand for data bandwidth rises steadily, an optical networking is the focus of new technologies, because of immense potential bandwidth of fiber optic technology [1]. Optical communication plays a vital role in the development of high speed and high quality telecommunication system. The optical fiber makes possible to transmit the data at very high data rates in excess of terabits per second and beyond over distance of thousands of kilometres [2]. Optical fiber has been deployed very successfully in long haul communication. These long-haul links serve as the backbone of worldwide communication networks [3].High bit rate and higher bandwidth is the main requirements fulfilled by optical fiber communication. As the capacity of the backbone increases, bandwidth demanding applications have emerged [4].

Optical communication system has revolutionized the telecommunication industry and played a major role in the advent of information age. Today's telecommunication networks have widely adopted optical fiber as the backbone transmission medium. Optical communication is a method of transmitting information from one place to another by sending light through the optical channel [5]. The main advantages of optical communication are the high speed, large capacity and high reliability by the use of the broadband of the optical link [6]. Because of its advantage over electrical transmission, the use of optical channel has largely replaced copper wire in the communication world. The main benefits of optical channel are its exceptionally low loss, allowing long distance between amplifiers or repeaters and its inherently large data carrying capacity; such that thousand of electrical links are required to replace a single high bandwidth optical channel [7].A schematic depiction of the organization of optical system is given in Figure 1. Therefore, 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.

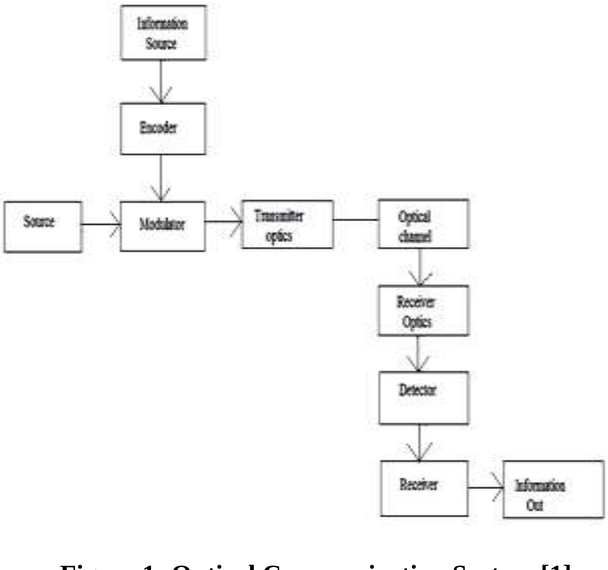

Figure 1: Optical Communication System [1]

II. OCDMA SYSTEM

OCDMA is a multiple access technology which allows multiple users to access the network asynchronously and simultaneously. Every user has access to the entire spectrum all the time. OCDMA technique has received a growing interest because neither time management nor frequency management at the transmitting nodes is necessary [8]. The roots of OCDMA are found in spread spectrum communication techniques. OCDMA can operate asynchronously, without centralized control, and does not suffer from packet collision.

The block diagram of OCDMA system is shown in Figure 2. On transmitter side, data bits obtained in electrical form are converted in to narrow optical pulses by narrow band electrical to optical converters and then fed into an encoder to generate the optical sequences which are then coupled into the fiber [9]. Each receiver is given a unique address code from orthogonal set of codes. Since each receiver is fixed tuned to a unique code, CDMA encoder must be tunable to talk to any of the users in the system. On the receiver side, a fixed tuned match filters recovers the signal in the presences of multiple user interference. The output of the decoder is threshold detected and then converted to electrical form by an optical-to-electrical (O/E) converter.

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 [10]. 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.

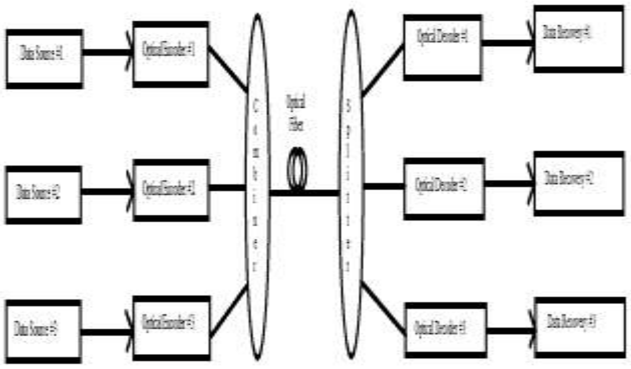

Figure 2: Block Diagram of OCDMA Network [9]

III.BENEFITS AND LIMITATIONS OF OCDMA

OCDMA system is suitable for high speed, large capacity supporting different bit rate and enhanced privacy. OCDMA system does not require bandwidth reservation like WDM system and any user at any time can access the network without prior permission. Thus the OCDMA system has the advantage of flexibility of user allocation in asynchronous mode and secured transmission with different signature codes [11]. Asynchronous incoherent OCDMA systems should be able to operate in the worst case scenario without any timing coordination. The photo detector noise (dark current and thermal noise) is ignored, as the received signal power is sufficient enough to override the photo detector noises.

In addition, the main limitation of OCDMA system is multiple user interference 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 [12]. 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. 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 [13]. As the number of simultaneous users increases, the bit error rate degrades because the effect of MUI increases. An eavesdropper in an OCDMA network may tap signals from various locations within the network. He may commandeer an authorized user terminal, or may tap signals from network.

IV. BACKGROUND

Prucnal *et al.* [14] showed the wide bandwidth channel required by CDMA for asynchronous access to a local area network which can be provided by fiber optic channel. The fiber optic spread spectrum CDMA was proposed and demonstrated with newly designed CDMA sequences and its performance was compared with the conventional CDMA. It was shown that the capacity of CDMA LAN can be increased using all optical processing.

Salehi *et al*. [15] examined fiber optic code-division multiple-access ,a technique in which low information data rates are mapped into very high rate address codes for the purpose of achieving random, asynchronous communication free of network control among many users. The need for a special class of signature sequences to achieve the multiple-access capability using fiber-optic signal processing techniques was discussed. A class of signature sequences called optical orthogonal codes (OOCs) that provide the auto- and cross-correlation properties required for FO-CDMA was also introduced and used in an experiment to show the principles of FO-CDMA. The experiment demonstrated the auto- and cross-correlation properties of the codes. The concept of optical disk patterns, an equivalent way of representing the OOCs, was also introduced. The patterns are used to derive the probability density functions associated with any two interfering OOCs. A detailed study of different interference patterns was presented, and the strongest and the weakest interference patterns were determined.

Shake *et al.* [16] 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.

Shake *et al.* [17] 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. One of them, an optical beat detector, was quantitatively analyzed to determine the probability of correctly detecting user code words. The confidentiality of user signals was shown to be vulnerable to such a detector if an eavesdropper can isolate a single user signal with a sufficiently high signal-to-noise ratio .It was shown that at lower SNRs, combining multiple bits dramatically increase the probability of an eavesdropper correctly detecting user code words, even for codes long enough to strain implementation capabilities, the probability of correct detection was shown to rise from negligibly low values to very high by the combining of less than hundred transmitted bits at the eavesdropper's receiver.

Leaird *et al.* [18] 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 On Off Keying-OCDMA. It was demonstrated that code switching eliminates the vulnerability to eavesdropping based on a simple energy detector. It was shown that 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. However, work did not preclude the possibility of vulnerability to eavesdropping strategies that exploit other structures in the coding and signalling scheme.

Wang *et al.* [19] proposed and theoretically investigate an optical code division multiple access system with coherent coding and code shift keying data modulation. A balanced detection technique is proposed and theoretically investigated. A multiuser CSK-OCDMA system with fiber Bragg gratings and a multiport encoder/decoder (E/D) pair was experimentally demonstrated. The multiport E/D was used in a novel configuration to process multidimensional optical codes .It was shown that the proposed scheme has better multiuser capability, simpler threshold setting in the receiver, and particularly, enhanced security compares with conventional OCDMA systems. A multiuser CSK-OCDMA system with a multiport encoder/decoder (E/D) pair was experimentally demonstrated. A bit-error-rate of less than 10^{-9} was achieved with up to ten and eight active users at data rates of 1.25 and 10.7 Gb/s, respectively, without any forward-error-correction or optical thresholding. The multiport E/D was used in a novel configuration to process multidimensional optical codes.

Chung *et al.* [20] 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. He further demonstrated a security improved incoherent optical CDMA scheme based on incoherent broadband light source and bipolar coding with modified PN code. Improved security was confirmed in 1.25 Gb/s signal transmission over 20 km of conventional single mode fiber. Eavesdropper holing a band-limited photo-detector could not intercept information data because the encoded data remained true noisy waveform. The relationship between a chip's spectral width and the transmission security was also analyzed. All results demonstrated that incoherent optical CDMA scheme based on incoherent broadband light source and bipolar coding provide more security in physical transmission link. Furthermore, it was demonstrated that bipolar coding enhances security in physical transmission link.

Wang *et al.* [21] 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 that the confidentiality of a CSK and DPSK OCDMA can be easily compromised by a differential eavesdropper.

Jiang *et al.* [22] 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 demodulator even without knowing the codes used. Further, it was shown that it is possible to block this vulnerability by adding an additional layer of phase modulation to the transmitter; however, the eavesdropper may still be able to determine characteristics of the data stream by adjusting the bias of the DPSK demodulator. In response, the transmitter could employ analog rather than digital phase modulation in order to better confound the eavesdropper, who would then be required to construct a variable bias DPSK demodulator with tracking ability in order to observe the data stream. If enhanced information security is a critical component of the OCDMA system, the results indicate that care must be taken to evaluate the structure present in the data stream to evaluate the level of complexity required for an eavesdropper to determine the character of the data stream.

Dai *et al.* [23] 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. It was shown that in the systems without proper decoding, error free BER performance and clear open eye diagrams indicate the eavesdropping possibility for both systems. The details of coding scheme were shown and security issues had been investigated by measuring eye diagrams and bit error rates for various cases. The analytical and numerical simulation results were presented for secure transmission of spectrally encoded incoherent optical CDMA signal. The principle of DPSK demodulation attack was also discussed. Also it was shown that confidentiality of data transmission can be increased using phase masking scheme.

Xue *et al.* [24] proposed a phase-masking scheme for O-CDMA security enhancement, and evaluates its confidentiality performance. The proposed scheme is compatible with the operational principles of spectral-phase-encoded OCDMA, and is consistent with the group key concept in secure group communications. Analytical results indicate that phase-masking effectively reduces the probability of interception and achieves low interception rates. It was also observed that a complex phase-mask provides a high level of confidentiality. By selecting a suitable phase-mask structure, the achievable confidentiality was tailored to suit applications with different security requirements. Different levels of phase shifts were also analyzed and it was shown that a complex phase-mask provides a high level of confidentiality.

Emadi *et al.* [25] introduced and modelled three types of jammers which are Pulse Jammer, Partial band Jammer, and Follower Jammer. The effects of these jammers on the performance of the spectral OCDMA systems that use On-Off keying modulation scheme were mathematically analyzed. To ensure the availability of information, real-time optically processed anti-jamming technique was used to hop the signal frequency in a pattern that is unknown to the hostile transmitter. It was shown that the jammer cannot identify and inject a powerful interfering signal containing the spectral characteristics of the data signal. The wavelength of the encrypted signal in OCDMA system can be changed by simply controlling the wavelength of the encryption key. It was shown that jamming signals can degrade the performance of the OCDMA system drastically under certain conditions.

V. CONCLUSION

OCDMA technology is not as secure as it was initially perceived to be. The potential risk of security of the valuable information also increases as tapping of the optical signal from a fiber can be easily done by using inexpensive equipment. 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. Also, the main degradation factor of an OCDMA system is multiple user interference, caused by the asynchronous transmission between the users and the superposition of the transmitting data in the fiber. It is the dominant source of BER in an OCDMA system.

REFERENCES

[1]. John M. Senior, “Optical Fiber Communications Principles and Practice,” Second Edition, Pearson Education, India, 2006.

[2]. Barnoski M.K. “Fundamentals of Optical Fiber Communications”, Academic Press , New York ,1981 .

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

[4]. G.P. Aggrawal, “Fiber Optic Communication System”, John Wiley and Sons, New York, 1997.

[5]. D.J.G. Mestdagh, “Fundamentals of Multi access Optical Fiber Networks,” Artech House, London, 1995.

[6]. 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.

[7]. Ivan p. Kaminow and Thomas l. Koch, “Optical fiber telecommunications”, academic Press, New York, 1997.

[8]. 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.

[9]. 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, 2000.

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

[11]. 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

[12]. Bernard Everett, “Tapping into fiber optic cables,” Network Security, vol. 2007, no. 5, pp. 13- 16, May 2007.

[13]. 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, vol.23, no-4,pp. 2401 – 2406, 2007.

[14]. 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.

[15]. 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.

[16]. Thomas H.Shake, “The Quantitative Impact of Survivable Network Architectures on Service Availability,” IEEE Communications Magazine, vol. 36, no. 5, pp. 122-126, May 1998.

[17]. 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.

[18]. 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.

[19]. 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.

[20]. 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.

[21]. 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.

[22]. 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.

[23]. 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,Shangai,China ,vol.14,no.7, pp. 427-428, Dec 2010.

[24]. 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 ,vol.12,no-3,pp-315-318 ,March 2006.

[25]. Mohammed J. Emadi, and Jawad A. Salehi, “Jamming Resistance Capabilities of the Spectrally Phase Encoded OCDMA Systems with Optimum and Suboptimum (Nonlinear 130 Two-Photon-Absorption) Receiver Structures,” IEEE Journal of Lightwave Communication, vol. 27, no. 22, pp. 5010-5021, Nov. 2009.