Research article Available online www.ijsrr.org ISSN: 2279–0543

International Journal of Scientific Research and Reviews

Data Security in Fiber-Optic CDMA Networks Using Multiclass Optical Orthogonal Codes

Saini Sanjay*[1] and Sharma Anil Kumar [2]

[1]Department of Electronics, Sunrise University, Alwar, Rajasthan
[2]Principal, Institute of Engineering & Technology, Alwar
E Mail - ssainialwar@gmail.com

ABSTRACT:

This paper evaluate data security in Fiber-Optic CDMA network using Multiclass Optical Orthogonal Codes. Security is estimated in terms of data confidentiality. The probability of error free codeword detection vs. fraction of theoretical capacity is plotted for three classes of Multiclass Optical Orthogonal Codes.

KEYWORDS: OCDMA, OOCs, QoS, MWSL, SWML, MWML

***Corresponding Author:**

Sanjay Saini

Research Scholar,

Department of Electronics, Sunrise University, Alwar, Rajasthan

E Mail - ssainialwar@gmail.com

INTRODUCTION

When evaluating the security of a communications technique, it is important to define the type of security issues under consideration. Security such as protection against jamming and transmission covertness may be provided by some types of Optical CDMA encoding scheme[1], it is data confidentiality which is most important for "secure" OCDMA. There are varieties of Optical CDMA encoding schemes such as 1-D OOCs, 2-D OOCs, Multiclass OOCs and 3-D OOCs[2] they share a common strategy of distinguishing data channels not by wavelength or time slot, but by distinctive spectral or temporal code[3] (or signature) impressed onto the bits of each channel. Suitably designed receivers isolate channels by code-specific detection. Optical orthogonal codes such as Multiclass OOCs are basically 2-D codes[4] with variable length and weight are used recently as signature codes.

MULTI CLASS OPTICAL ORTHOGONAL CODES (OOCs)

Optical Orthogonal Codes (OOCs) are limited to single class or multi class with restricted weight and length properties. Therefore, there exists a lack of flexibility in the existing OOCs to support arbitrary rate and Quality of Service (QoS). Multi Class OOC Codes are multi weight multi length strict OOCs. The generated code set fulfills the conditions of strictly OOCs, namely, the maximum nonzero shift autocorrelation and the maximum cross correlation constraints . We can consider three cases of a strict Multiclass OOC by using multiple searches for each code set[5]. These three cases are Multiweight Single-Length OOCs (MWSL-OOCs),Single-Weight Multilength OOCs (SWML-OOCs) and Multiweight Multilength OOCs (MWML-OOCs)

Multiweight Single-Length OOC (MWSL-OOC)

The code set is characterized by (1000, 7), (1000, 5), and (1000, 3) and satisfies the autocorrelation and cross correlation properties of the strict OOCs. For the (1000, 7) single-class OOC, the number of codes is upper bounded by 23 since $K \le (N-1)/W(N-1)$, similarly, the (1000, 5) and (1000, 3) are upper bounded by 49 and 166, respectively.

Single-Weight Multilength OOC (SWML-OOC)

This is applicable to systems with equal QoS and supporting variable data rate. Three-class SWMLOOC code set is characterized by (300, 5) for the high rate users, (1000, 5) for the medium rate users, and (1500, 5) for the low rate users.

Multiweight Multilength OOC (MWML-OOC)

In this case, the weights and lengths of the multi class OOC is selected arbitrarily. The selected parameters of the multi class code are such that high rate users get high QoS and low rate users get low QoS. The set is characterized by (550, 7), (930, 5), and (1300, 3) for the high, medium, and low rate QoS, respectively.

DATA CONFIDENTIALITY

Generally OCDMA encoder is modeled as a linear time-invariant (LTI) system. When driven by an optical input waveform $s_i(t)$, the output of the encoder can be modeled as the convolution of the impulse response of the encoder $h(t)$, with $s_i(t)$. If an eavesdropper can observe the transmitted waveform $s_o(t)$, in the channel, and if someone knows the form of the input waveform $s_i(t)$, he can use standard linear system analysis to solve for the impulse response of the encoder (or its Fourier transform, the transfer function). This reveals the code being used. Even if a transmitter's code is reconfigured frequently, the encoder can still be modeled as a piecewise LTI system, with linear analysis techniques being applicable during the period between code changes. Using LTI transfer function to encode data thus presents a fundamental security problem[6].

For the purposes of security performance calculations assuming that the eavesdropper is able to synchronize to the transmitted signal. The eavesdropper can then locate the beginning and end of a data bit, and can sample the detector output precisely at the end of each code chip time. The figure of merit that will be used here for code interception performance calculations is the probability that the eavesdropper can detect the user's entire code word with no errors, denoted by $P_{correct}$. The probability of missing a transmitted pulse in a given time bin, P_M, and the probability of falsely detecting a pulse in a bin where none was transmitted, P_{FA}. If the code interceptor makes a code word decision based on observing the transmitted signal for a single data bit interval, the overall probability of error-free code word detection as calculated by Thomas H. Shake[7] is given by:

$$P_{correct} = (1 - P_M)^W (1 - P_{FA})^{(n_c \times n_\lambda - W)} \quad \text{.....(1.0)}$$

The first term represents the probability of not missing any of the W pulses that are transmitted during a data bit. The second term is the probability of not falsely detecting pulses in any of the

$n_c \times n_\lambda - W$ time bins where pulses are not transmitted during a data bit. P_M and P_{FA} are determined by the SNR at the eavesdropper and by the eavesdropping detector's performance in noise.

$$P_{FA} = \exp\left(-\frac{\gamma}{N_O}\right) \qquad \text{.....(1.1)}$$

and

$$P_M = Q\left(\sqrt{2E/N_O}, \sqrt{2\gamma/N_O}\right) \qquad \text{.....(1.2)}$$

Where E/N_O is the ratio of peak pulse energy to the noise power spectral density, γ the detection threshold and $Q(a,b)$ the Marcum Q-function defined as:

$$Q(a,b) = \int_b^\infty xI_0(x)\exp\left(-\frac{x^2+a^2}{2}\right)dx \qquad \text{.....(1.3)}$$

where $I_0(x)$ denotes a zeroth order modified Bessel function of first kind.

An authorized receiver's BER performance will be a function of the received SNR. The authorized receiver's SNR is given by following equation:

$$\frac{E_u}{N_{0u}} = \frac{E_u}{(N_{0M} + N_{0\tau})} \qquad \text{.....(1.4)}$$

where N_{0M} represent the total noise spectral density contribution of the MUI and $N_{0\tau}$ represents the spectral density of the receiver noise. N_{0M} is proportional to both the number of active transmitters and to the transmitted power of each user[8].

The eavesdropper's available SNR per code chip is given by

$$\frac{E_{ed}}{N_{0ed}} = \left(\frac{e_t n_u}{\alpha_{ed} e_u W}\right)\left(\frac{M_T - 1}{M_T - M_A}\right)\left(\frac{E_u}{N_{0u}}\right)_{spec} \qquad \text{.....(1.5)}$$

where e_t the eavesdropper's fiber tapping efficiency, n_u the number of taps in the broadcast star coupler that distributes user signals, α_{ed} the ratio of the eavesdropper's receiver noise density to the authorized user's receiver noise density, e_u the authorized user receiver's multichip energy combining efficiency, M_T the maximum theoretical number of simultaneous users at a specified

maximum BER, $\left(\frac{E_U}{N_{0u}}\right)_{spec}$ the required user SNR (per data bit) to maintain the specified BER, M_A the actual number of simultaneous users supported, $\frac{E_{ed}}{N_{0ed}}$ is the eavesdropper's effective SNR per code chip[9].

SYSTEM EVALUATION AND RESULTS

The required user's SNR for a particular BER is different for the different types of optical CDMA encoding schemes from this eavesdropper's effective SNR can be calculated, which is used to plot probability of error-free code detection vs. fraction of theoretical capacity,

Fixing BER = 10^{-4} the required SNR of the authorized user is calculated. This value of SNR is used to obtain eavesdropper's SNR. The probability of error free codeword detection vs. fraction of theoretical capacity for Multiclass OOCs are plotted. Which are as following :

System capacity and data confidentially for MWSL-OOCs

Fig. 1.1 shows that probability of error free codeword detection at 0.5 fraction of theoretical capacity is 10^{-52} for High QoS (1000, 7), 10^{-21} for Medium QoS (1000, 5) and 10^{-2} for Low QoS (1000, 3). Security is high for high code weight because as code weight increases, the probability of bit error reduces and the available SNR for the eavesdropper reduces.

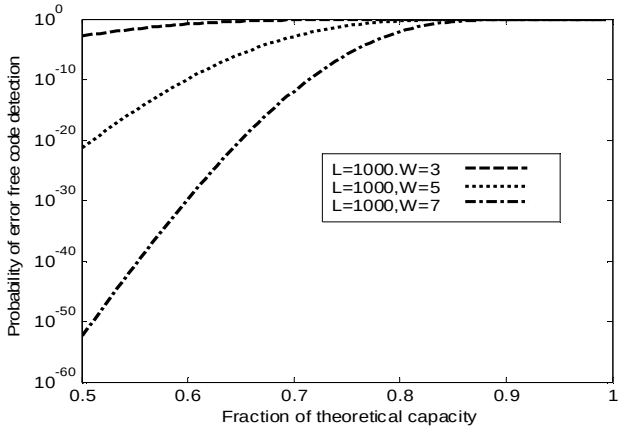

Figure 1.1: "Theoretical capacity and data confidentially for MWSL-OOC Code Set"

System capacity and data confidentially for SWML-OOCs

In Fig. 1.2 we can see that the Probability of error free codeword detection at 0.5 fraction of theoretical capacity is 10^{-7} for High Rate (300, 5), 10^{-22} for Medium Rate (1000, 5) and $10^{-32.5}$ for Low Rate (1500, 5). Security is high for long code length because as code length increases the number of theoretical users increases.

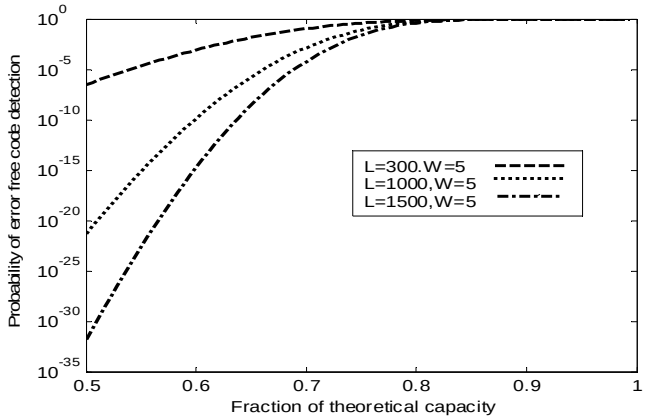

Figure 1.2: "Theoretical capacity and data confidentially for SWML-OOC Code Set"

System capacity and data confidentially for MWML-OOCs

In Fig.1.3 probability of error free codeword detection at 0.5 fraction of theoretical capacity is 10^{-4} for Low Rate Low QoS (1300, 3), 10^{-21} for Medium Rate Medium QoS (930, 5) and 10^{-29} for High Rate High QoS (550, 7). This reflects that security is high for high code weight, because the impact of higher code weight is more than the longer code length.

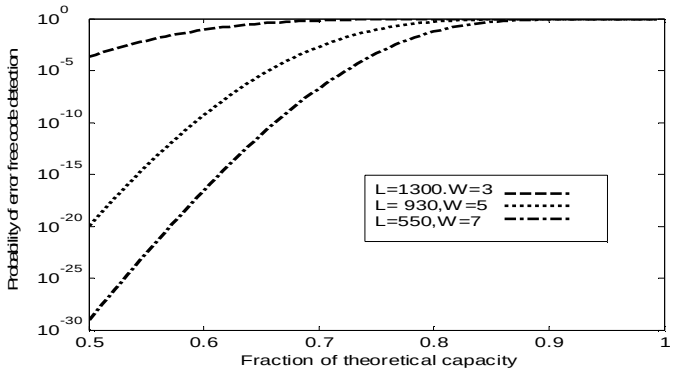

Figure 1.3: "Theoretical capacity and data confidentially for MWML-OOC Code Set"

CONCLUSION

1. Probability of error free codeword detection is high for High QoS (1000, 7), medium for Medium QoS (1000, 5) and low for Low QoS (1000, 3). Security is high for high code weight because as code weight increases probability of bit error reduces and this will reduce the users SNR.
2. Probability of error free codeword detection is low for High Rate (300, 5), medium for Medium Rate (1000, 5) and high for Low Rate (1500, 5). Security is high for long code length because as code length increases the number of theoretical users increases because multi access interference is low and as the number of theoretical users increases this will reduce the users SNR.
3. Probability of error free codeword detection is low for Low Rate Low QoS (1300, 3), medium for Medium Rate Medium QoS (930, 5) and high for High Rate High QoS (550,7). Security is high for high code weight because as code weight increases probability of bit error reduces and this will reduce the users SNR. Impact of higher code weight is more than the longer code.

REFERENCES

1. J.A. Salehi, "Code division multiple-access techniques in optical fiber networks-Part I: Fundamental principles," IEEE Trans. Commun. August 1989; 37:824–833.
2. Jos´e Ortiz-Ubarri, "Three-dimensional periodic Optical Orthogonal Code for OCDMA systems." IEEE Information Theory Workshop 2011.
3. M. Azizoglu, J. Salehi, and Y. Li, "Optical CDMA via temporal codes,"IEEE Trans. Commun. July 1992; 40: 1162–1170.
4. E. S. Shivaleela, A. Selvarajan, "Two-Dimensional Optical Orthogonal Codes for Fiber-Optic CDMA networks Journal of Lightwave Technology", February 2005; 23(2): 647-654.
5. Naser G. Tarhuni, "Multiclass Optical Orthogonal Codes for Multiservice Optical CDMA Networks" Journal of Lightwave Technology, February 2006; 24 (2): 694-704.
6. L.Tancevski, I.Andonovic, and J. Budin, ''Secure optical network architectures utilizing wavelength hopping/time spreading codes," IEEE Photon. Technol. Lett. May 1995; 7: 573–575.
7. Thomas H. Shake, "Security performance of Optical CDMA against eavesdropping," Journal of Lightwave Technology, February 2005; 23(2): 655–670.
8. A.Srivastava, Subrat Kar, V.K.Jain "Performance evaluation of PIN+OA and APD receivers in

multi-wavelength CDMA and WaCDMA Networks," Optics Communication, February 2001; 191:55–66.

9. A.Srivastava, Subrat Kar, V.K.Jain "Performance evaluation of PIN+OA and Avalanche Photodiode receivers in Optical CDMA Networks," *Optical Communication,* 2001; 22: 67–73.