International Journal of Research (IJR)

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Vol. 9 Issue 05
May 2022

Investigation of Eavesdropping and Error Detection of OCDMA-Free Code

Mohamed Mansour Shukra[1],Alsanossi M. Aboghrara[2],Ahmed Imsaeri Omar Imsaeri[3]
Moh.Shukra@Fezzanu.Edu.Ly,als.abdulhafid@sebhau.edu.ly, Ahm.Imsaeri@Fezzanu.Edu.Ly
Fezzan university, Faculty of Education, Physics Department
Sebha University,Renwable Energy ,Engineering Department

Abstract. *This paper presents the security performance of spectral amplitude code OCDMA systems. We examine factors affecting data security such as system capacity and its influents on the eavesdropped SNR. The eavesdropper probability of error-free code detection for Modified Double Weight (MDW) OCDMA scheme is investigated. The eavesdropper performance is based on observing the authorized transmitted signal based on classical detection theory. For probability of correct detection of 0.5, an eavesdropper receiver would need to detect SNRs of 8, 9.3 and 10 dB for MDW (9, 4), MDW (18, 6) and MDW (30,8) Respectively*

I .Introduction

Security as well as capacity in optical transmission link could become a critical issue for some applications such as military networks or enterprise networks. Optical code-division multiple-access (OCOMA) technology is an attractive solution for these applications since it provides format-independent security in physical layer while guaranteeing appreciably wide bandwidth.

The potential provided by a COMA for enhanced information security is frequently mentioned in addition to other possible advantages, such as simplified and decentralized network control, improved spectral efficiency, and increased flexibility in the granularity of bandwidth that can be provisioned. This is plausible at first glance considering that frequently mentioned in addition to other possible advantages, such as simplified and decentralized network control, improved spectral efficiency, and increased flexibility in the granularity of bandwidth that can be provisioned. This is plausible at first glance considering that frequently the OCDMA encoded signal manifests itself as a noise- like waveform that may not be accessible to an eavesdropper without knowledge of the applied code. Studies has previously demonstrated there is no security at all in most coded OCDMA for a single-user system employing on-off keying (OOK) modulation.

Recently, to solve this problem, a code switching scheme (or 2-code keying) was proposed and its performance was evaluated theoretically [1] and [2]. Experimental demonstration of the code switching scheme was carried out by employing coherent optical COMA with a short coherent optical pulse [3]. However, a bandwidth-limited PO was assumed for eavesdropping and the degree of security was only investigated by measuring eye-diagrams at back-toback configuration.

An M-code keying Acdma system with parallel encoders/decoders presented by [4], and quantitatively analyzed its security performance. The results show that the security performance is slightly improved which does not have greatly enhancement in security performance compared with the two-code keying OCOMA system. Even though both the switching code keying has better security compared to the OOK OCOMA system, their costs should be taking into account. The increase in codes will increase multiuser interference which may reduce the number of users and many codes are needed.

In this paper, security performance of spectral amplitude coding aCDMA is presented. The eavesdropper probability of error-free code detection for Modified Double Weight (MDW) aCDMA scheme is investigated. The eavesdropper performance is based on observing the transmitted signal and then calculate signal to noise ratio (SNR).

2. MODIFIED DOUBLE WEIGHT (MDW) OCDMA SCHEME

Many codes have been proposed for spectral amplitude code aCOMA. Among the popular ones are Hadamard [5], Prime codes, Optical Orthogonal codes [6], and MFH codes [7]. However these codes suffer from various limitations one way or another. The codes constructions are either complicated (e.g. OOC and MFH codes), the cross-correlation are not ideal (e.g. Hadamard and Prime codes), or the code length is too long (e.g. DOC and Prime code). Long code lengths are considered disadvantageous in its implementation since either very wide band sources or very narrow filter bandwidths are required.

A new code structure based on Oouble-Weight (OW) code families has been proposed for spectral amplitude coding aCOMA system. MOW is the modified version of OW code and its code weight can be any even number that is greater than two [8]. The MOW code possesses ideal cross-correlation properties and exists for every natural number n. As a family of spectral amplitude code, MOW can be represented by (N, W, A) notation where N is the code length, W is the code weight, and A is the in-phase cross

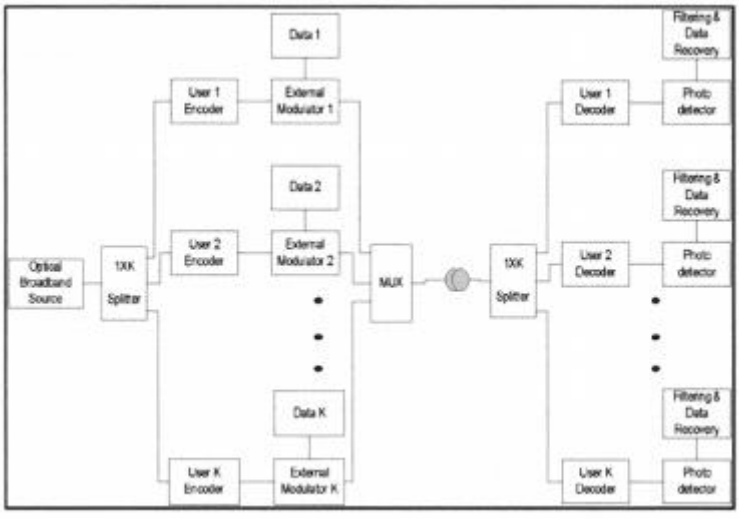

Figure 1. The system architecture of spectral amplitude code OCDMA system network

International Journal of Research (IJR)
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Vol. 9 Issue 05
May 2022

A simple schematic block diagram consists of K users is illustrated in figure 1. In most spectral amplitude code OCDMA systems, when the data bit is "1," a spectrally encoded pulse is sent, while nothing is sent for data bit "0".

1. EAVESDROPPER CODE INTERCEPTOR

The analysis in this paper assumes that potential intruders are technologically sophisticated, have significant resources, and know a great deal about the signals being transmitted [9]. In particular, the eavesdropper knows what types of O-CDMA signals are being sent: the data rate, the type of encoding, and the structure of the codes—but not the particular code that an individual user employs. These same principles are applied in the analysis of cryptographic systems, and are often stated in the form of Kerckhoffs' principle, which essentially states that one should assume that the eavesdropper knows everything about the cryptographic algorithm except for the key that each user employs

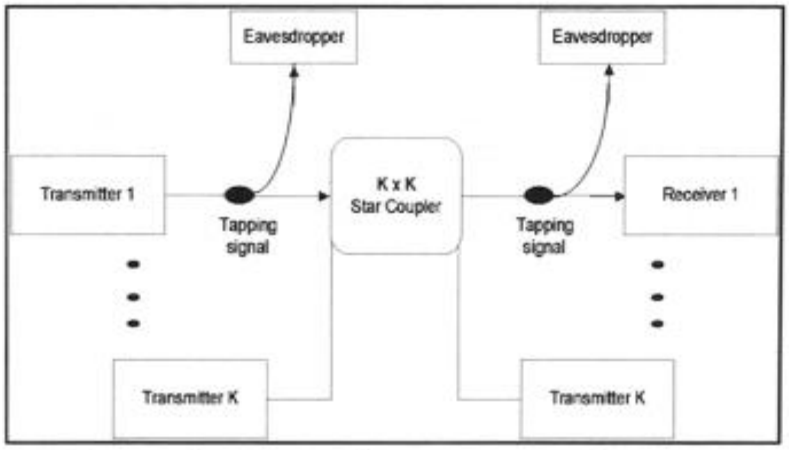

Figure 2. Places for an eavesdropper to intercept signals

The analysis presented here treats the eavesdropper's code interception problem as a problem in classical detection theory [1] and assumes idealized transmission components (e.g., fiber, couplers, and receiver components). Receiver implementation losses are also not considered. The eavesdropper taps a coded transmission of a particular user and performs the necessary calculations to derive the transmitter's code word from these transmissions. Figure 2 shows the potential places to tap a signal from the user. However, when only one user is active in the network, aCOMA scheme cannot guarantee physical layer security any more.

An intelligent eavesdropper can design a listening device to detect this code word as shown in figure 3. Once a user's code word is detected by the eavesdropper, the eavesdropper has free access to the user's data until the user's code is changed.

International Journal of Research (IJR)
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Vol. 9 Issue 05
May 2022

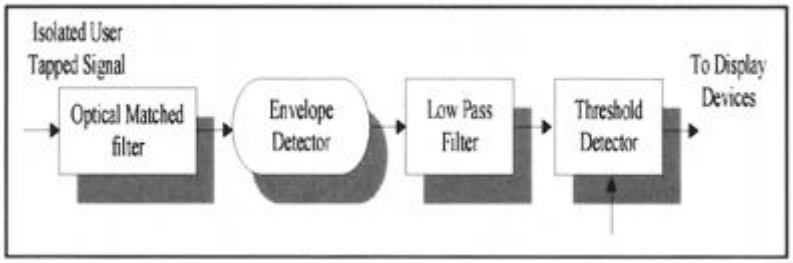

Figure 3. Eavesdropper code interceptor structure

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. This probability will depend on the type of detection processing and on the amount of time the eavesdropper observes the user's signal for each detection; it can be calculated from two quantities that are staples of classical detection analysis—the probability of missing a transmined pulse in a given time bin, (pM), and the probability of falsely detecting a pulse in a bin where none was transmitted, (F).

If the code interceptor makes a code word decision based on observing the transmitted signal for an encoded spectral amplitude coding OCDMA data bit interval, the overall probability of error-free code word detection is given by:

$$P_{correct} = (1 - P_M)^W (1 - P_F)^{(N-W)}, \quad (1)$$

$$P_F = \exp(-\frac{\gamma}{N_o}), \quad (2)$$

(*r*is the detection threshold and *No* is the noise power spectral density). Since, *PM* is the probability of missing a transmitted pulse in a given time bin, then the probability of not missing a transmitted pulse is denoted as *PD*, sometimes referred as the probability of detection.

$$P_D = (1 - P_M), \quad (3)$$

$$P_D = Q(\sqrt{2E/N_o}, \sqrt{-2\ln P_F}), \quad (4)$$

$$Q(\alpha, \beta) \cong \int_{\beta}^{\infty} z \exp(-\frac{z^2 + \alpha^2}{2}) I_0(\alpha z) dz \quad (5)$$

Equation (1) can be written as:

$$P_{correct} = [Q(\sqrt{2E/N_o}, \sqrt{(2\gamma/N_o)})]^W [1 - \exp(\gamma/N_o)]^{(N-W)} \quad (6)$$

Where, *E* / *No* is the single pulse signal to noise ratio and *r* is detection threshold. W and *N* represent code weight and code length of a spectral am code aCOMA, respectivel

4. RESULTS AND DISCUSSIONS

been employed. Figure 4 is obtained which shows th eavesdropper probability of correct detection as function of signal to noise ratio for a single detecte code pulse. For probability of correct detection of 0.5 an eavesdropper receiver would need to detect SNRs o 8, 9.3 and 10 dB for MOW (9, 4), MOW (18, 6) an MOW (30, 8) respectively. As the figure shows, the difference in performance of the optical matched filt with envelope detection is getting small, especially a higher SNRs. For these particular MOW cod dimensions, the eavesdropper would have the ability detect the code without errors with a probability of t virtually one at SNRs higher than 14 dB.

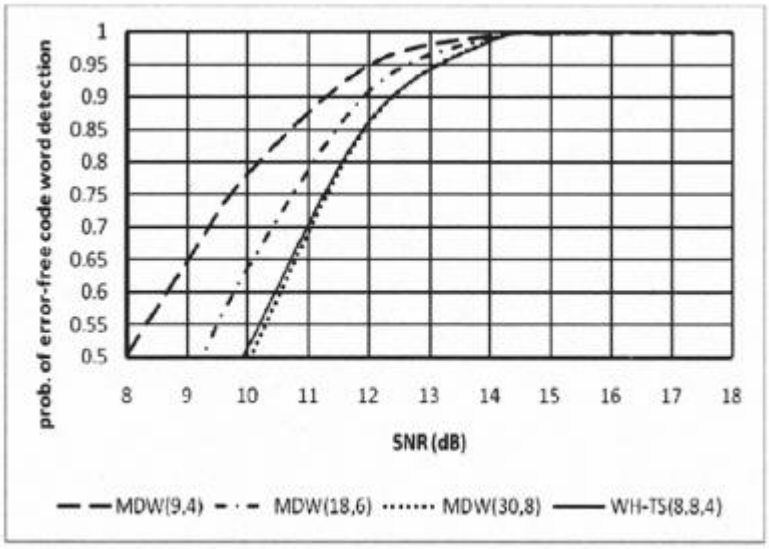

Figure 4. Code intercepting detector performances

TS(*nt* ,*nA*, ,*W*), where *nt*, *nA*, and *ware* time slots, wavelengths and code weight, respectively. WH-TS (8, 8, 4) has better security than MOW (9, 4) even they have same code weight. It is clear that MDW aCDMA with code weight $W = 8$ has slightly the same security performance as WH-TS (8, 8,4). The higher the code space size the better the security performance available from aCOMA encoding. Using the modeling approximations of [1], per signature chip SNR of the eavesdropper is related to the per data bit signal-to-noise ratio (SNR) of the user by the following relationship

$$\frac{E_{ed}}{N_{0ed}} = \left(\frac{e_t n_u}{\alpha_{ed} e_u W}\right)\left(\frac{1}{1-\frac{M_A}{M_T}}\right)\left(\frac{E_u}{N_{0u}}\right)_{spec} \qquad (7)$$

In this equation, *et* is the eavesdropper's fiber tapping efficiency, *nu* is the number of taps in the broadcast star coupler that distributes user signals, *aed* is the ratio of the eavesdropper's receiver noise density to the authorized user's receiver noise density, *e u* is the authorized user receiver's multichip energy combining efficiency, *M T* is the maximum theoretical number of simultaneous users at a specified maximum BER, *Eu* / *NOu* is the required user SNR (per data bit) to maintain the specified BER, *M A* is the actual

number of simultaneous users supported, and *Eed* / *NOed* is the eavesdropper's effective SNR per code chip. The per code chip eavesdropper's SNRs as a function of the theoretical system capacity are shown Figure 5. If the authorized users transmit sufficient power so that 50%, 65% and 75% of the theoretical system capacity is attained for code weights W of 4, 6 and 8 respectively, the eavesdropper has SNR of 15 dB. An optical matched filter receiver followed by envelope detection theoretically requires a (peak) SNR f approximately 15 dB to produce the required raw detector BER of 10-4 [11]. Error correction codes used in commercial high-rate optical telecommunication equipment can produce the maximum acceptable system BER 10-9•

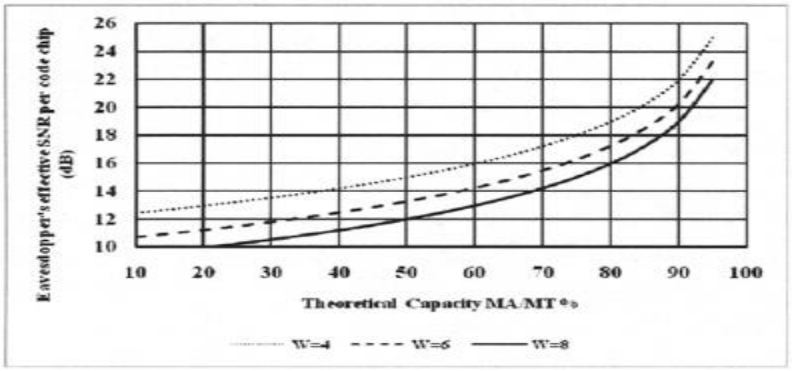

Figure 5. Per chip code SNR as a function of theoretical system capacity

5.CONCLUSION

The assumptions used in a security analysis can strongly affect the degree of security that the analysis shows. The eavesdropper probability of error-free code detection for Modified Double weight (MDW) OCDMA scheme is investigated. This probability is dependent on many design parameters of the communication system that affect the amount of signal power available to the eavesdropper such as code dimensions being used for OCDMA system encoding and system capacity. Wavelength hopping —time spreading and spectral phase codes appear to be the two of the most promising code types for generate code spaces that are large enough prevent successful brute- forc code search attacks

.

REFERENCES

[1] T.H. Shake, "Security performance of optical CDMA against eavesdropping", J. Lightwave Technology, 23 (2), February 2005, pp. 655—670.
[2] T.H. Shake, "Confidentiality performance of spectral- phase-encoded optical CDMA", J. Lightwave Technology, 23 (4), April 2005, pp. 1652—1663.
[3] D.E. Leaird, Z. Jiang, and A.M. Weiner, "Experimental investigation of security issues in OCDMA: A code- switching scheme", IEE Electron. Lett, 41 (14), July 2005.
[4] Liqiao Qin, Hongxi Yin, Wei Liang, Ziyu Wang, and Anshi Xu, "Security performance

analysis of an M-code keying OCDMA system", Photon Netw Commu, 23 July 2007.
[5] Smith, E. D. J., Blaikie, a R. J., and Taylor, D. P., "Performance Enhancement of Spectral-Amplitude- Coding Optical CDMA Using Pulse-Position Modulation," IEEE Trans. Commun., 46, 1998, pp. 1176-1185.
[6] Salehi, J. A., "Code Division Multiple Access Techniques in Optical Fiber Network-Part I: Fundamental Principles," IEEE Trans. Commun., 1989, 37, pp. 824-833.
[7] Zou Wei, and Ghafouri-Shiraz, H., "Codes for Spectral- Amplitude-Coding Optical CDMA Systems," J. Lightwave Technology", 20, 2002, pp.1284-1291.
[8] Aljunid, S. A., Ramli, A. R., Borhanuddin, M. A. & Mohamad K. A., "A new family of optical code sequences for spectral-amplitude-coding optical CDMA systems", IEEE photonics technology letters, 16 (10), 2004, pp. 2383-2385.
[9] N. Ferguson and B. Schneier, *Practical Cryptography. Indianapolis, IN: Wile y*, 2003.
[10] Harry L. Van Trees, *Detection, Estimation, and Modulation Theory, Part I, John* ***Wile y & Sons,*** 2001.
[11] P. A. Humblet and M. Azizoglu, "On the bit error rate of lightwave systemswith optical amplifiers," J. Lightw. Technol., (9) 11, 1991, pp. 1J76—1J82.