5

Security Limitations of Spectral Amplitude Coding Based on Modified Quadratic Congruence Code Systems

Hesham Abdullah Bakarman, Shabudin Shaari and P. Susthitha Menon
University Kebangsaan Malaysia
Malaysia

1. Introduction

Generally, communication network systems provide data transfer services for customers. Further requirements such as performance, security, and reliability characterize the quality of the transfer service. Network and information security refer to confidence that information and services existing on a network cannot be accessed by unauthorized users (eavesdropper). However, these service requirements affect each other such that a decision has to be made for cases in which all or some of these requirements are desired but cannot be fulfilled (Zorkadis 1994).

In secure communication networks, tradeoff considerations between system performance and security necessities have not been mentioned widely in many researches. Actually, it has been known that security is of main concern in both wireless and optical communications networks, security mechanisms employed often have implication on the performance of the system (Imai et al. 2005). For some application environments, such as military or enterprise networks, security and system capacity in communications transmission media could become a critical issue. Optical code-division multiple-access (optical CDMA) technology, a multiplexing technique adapted from the successful implementation in wireless networks, is an attractive solution for these applications because it presents security in the physical layer while providing significantly wide bandwidth (Chung et al. 2008).

Optical CDMA systems are getting more and more attractive in the field of all optical communications as multiple users can access the network asynchronously and simultaneously with high level of security (Salehi 1989, Salehi & Brackett 1989) compared to other multiplexing techniques such as Wavelength Division Multiplexing WDM and Time Division Multiplexing TDM.

The potential provided by optical CDMA for enhanced security is frequently mentioned in several studies using different techniques and approaches such as quantum cryptography and chaotic encryption systems (Castro et al. 2006). Other approaches to enhance security have been proposed using optical encoding techniques such as fiber bragg gratings (FBG) to implement optical CDMA systems (Shake 2005a,2005b). Their degree of security depends on code dimensions being used.

In this chapter, security limitations of spectral amplitude coding Optical CDMA are presented and investigated. The tradeoffs between security and system performance have been investigated for a specific eavesdropper interception situation. Section II briefly presents some network security services and assumptions required for optical CDMA confidentiality analysis in the physical layer. Security and performance tradeoffs, based on MQC code system, are presented in section III. Performance analysis is given in section IV. Finally, a conclusion is given in section V.

2. Optical CDMA physical layer networks

Due to the transparency increment in optical communications network components and systems, network management and maintenance have been faced additional security challenges. An evaluation on several existing physical security violates on optical communications network is presented in (Teixeira et al. 2008).There are four main threats that can be described in terms of how they affect the normal flow of information in the network, as shown in figure (1),they are: denial of service, interception, modification and creation. Table 1 summarized some of these attacks.

Attack method	Realizes	Means
In-Band Jamming	Service Disruption	An attacker injects a signal designed to reduce the ability of the receiver to interpret correctly the transmitted data
Out-of-Band Jamming	Service Disruption	An attacker reduces communication signal component by exploiting leaky components or cross-modulation effects
Unauthorized Observation	Eavesdropping	An attacker listens to the crosstalk leaking from an adjacent signal through a shared resource in order to gain information from the adjacent signal, the collection of signals by an attacker for whom they were not intended).

Table 1. Optical networks attack methods

The security services of a network have four fundamental objectives designed to protect the data and the network's resources (Fisch & White 2000). These objectives are:

- Confidentiality: ensuring that an unauthorized individual does not gain access to data contained on a resource of the network.
- Availability: ensuring that authorized users are not unduly denied access or use of any network access for which they are normally allowed.
- Integrity: ensuring that data is not altered by unauthorized individuals. Related to this is authenticity which is concerned with the unauthorized creation of data.
- Usage: ensuring that the resources of the network are reserved for use only by authorized users in appropriate manner.

In this chapter, ensuring confidentiality against eavesdropper interception strategies for optical CDMA aims to investigate the limitations and tradeoffs between security and performance.

There are various fiber optic tapping methods, of which fall into the following main categories (Oyster Optics 2008): splice (involves literally breaking the cable at some point and adding a splitter), splitter or coupler (involves bending the cable to a certain radius, which allows a small amount of the transmitted light to escape) and non-touching methods (passive and active), involve highly sensitive photo-detectors that capture the tiny amounts of light that emerge laterally from the glass fiber owing to a phenomenon known as Rayleigh scattering.

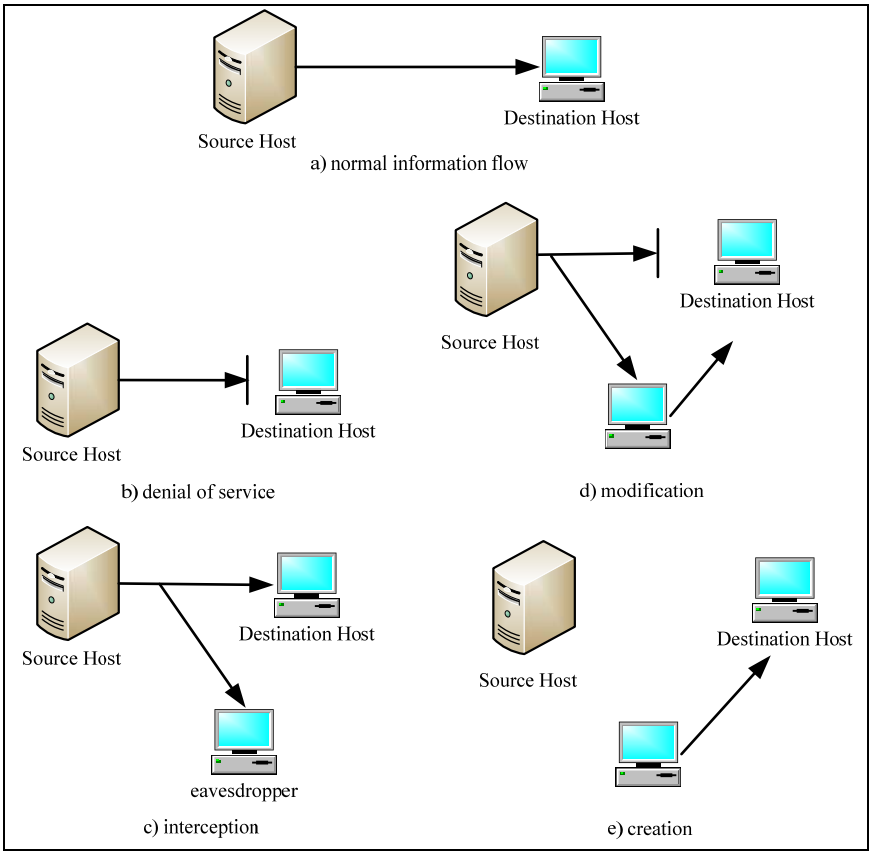


Fig. 1. Pattern of network attacks

Communication between authorized users in a network can be implemented by two approaches; point-to-point and broadcast. In the point-to-point, approach each user transmits to another specific one whereas in a broadcast approach users transmit in common to the medium accessible to all other users. Figure (2) shows a common topology found in point-to-point networks. Figure (3) shows two topologies established in broadcast networks.

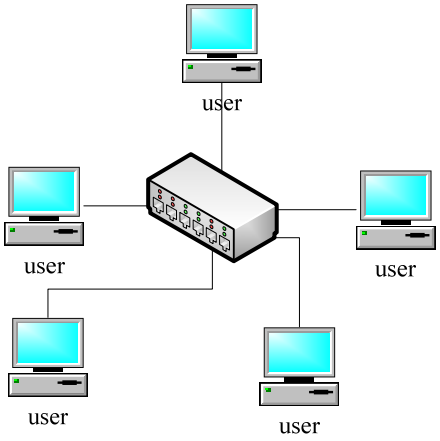


Fig. 2. Point to point star topology

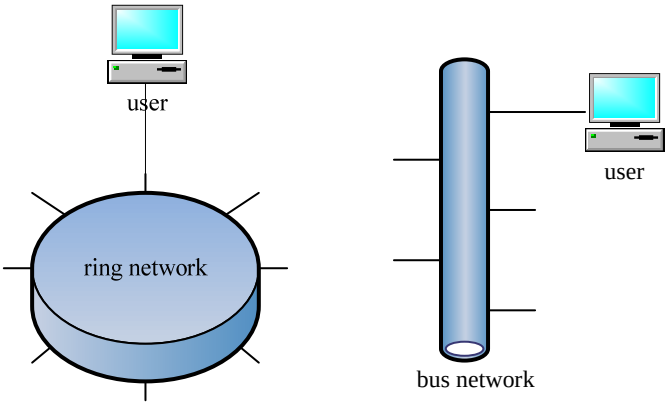


Fig. 3. Broadcast network topologies

Topology is an important architectural consideration, and different topologies have different security properties. Ring topologies allow attacks to be relatively easily localized, because of the structured interconnectivity of nodes. Star topologies make attack detection nominally easier than other topologies, because any propagating attacks are commonly received at many stations. Optical CDMA has many advantages such as sharing bandwidth, controlling and high security compared to other access technologies such as TDMA and WDMA. Recently, studies discovered that Optical CDMA systems suffer from weakness against eavesdropping and jamming attacks.

Figure (4) shows the possible positions, within the network, to tap a signal from the user. Therefore, when just a single user is active, optical CDMA system cannot guarantee physical layer security any more. In certain time, this situation can be existed even in a multiuser active optical CDMA network as reported in current theoretical analyses (Shake 2005a,2005b).

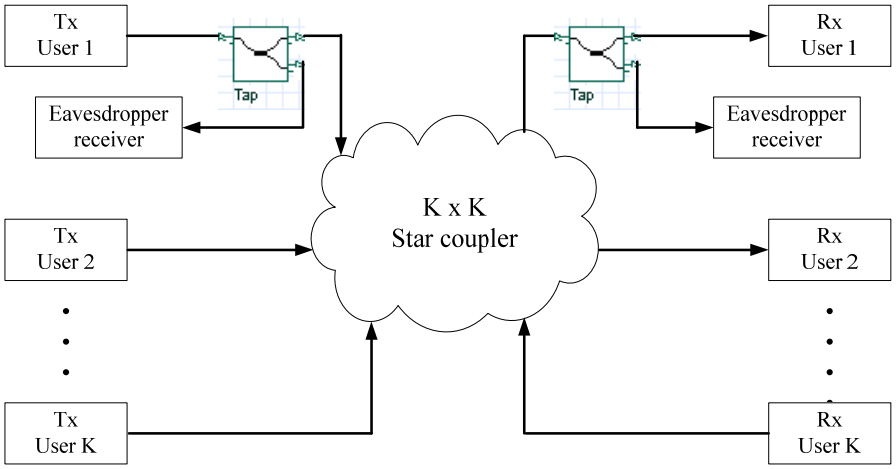


Fig. 4. Places for an eavesdropper to attack and tap optical CDMA encoded pulses

3. Security and performance tradeoffs

In security environments, it is believed that an inherent tradeoffs between networks performance and security are existed which lead many network designers to seek a balance between both of them. Depending on the confidentiality measurement required between communicating networks, different sets of optimizations can be considered (Jin-Hee & Ing-Ray 2005). In (Wolter & Reinecke 2010), the relationship of performance and security has been investigated in model-based evaluation. Their approach is illustrated based on the premise that there are significant similarities between security and reliability.

The combination of security and performance poses interesting tradeoffs that have high relevance especially in modern systems that are subject to requirements in areas, performance and security. In this chapter, ensuring confidentiality against eavesdropper interception strategies for optical CDMA is conducted to investigate limitations and tradeoffs between security and performance.

Using the modeling approximations of (Shake 2005b), 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:

$$\frac{E_{ed}}{N_{0ed}} = \sigma\left(\frac{1}{W}\right)\left(\frac{1}{1-\frac{M_A}{M_T}}\right)\left(\frac{E_u}{N_{0u}}\right)_{spec} \tag{1}$$

W is the code weight of the code being used, M_T is the maximum theoretical number of simultaneous users at a specified maximum BER, E_u / N_{0u} is the required user SNR (per data bit) to maintain the specified BER, M_T is the actual number of simultaneous users supported, and E_{ed} / N_{0ed} is the eavesdropper's effective SNR per code chip. Where σ represents several system design parameters as following:

$$\sigma = \left(\frac{e_t n_u}{\alpha_{ed} e_u} \right) \tag{2}$$

In this equation, e_t is the eavesdropper's fiber tapping efficiency, n_u is the number of taps in the broadcast star coupler that distributes user signals, α_{ed} 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. Figure (5) shows the effect of combining multiple code pulses for both coherent and incoherent detection schemes. The eavesdropper is assumed to use a receiver that is equal in sensitivity to the authorized user's receiver (α_{ed} = 1). It is assumed that the total number of taps in the star coupler, shown in figure (4), is n_u = 100 with a tapping efficiency of e_t = 0.01. Since, e_u is equal to one and between zero and one for coherent and incoherent detection respectively (Mahafza & Elsherbeni 2003), coherent detection with combining signals shows better confidentiality than the incoherent one.

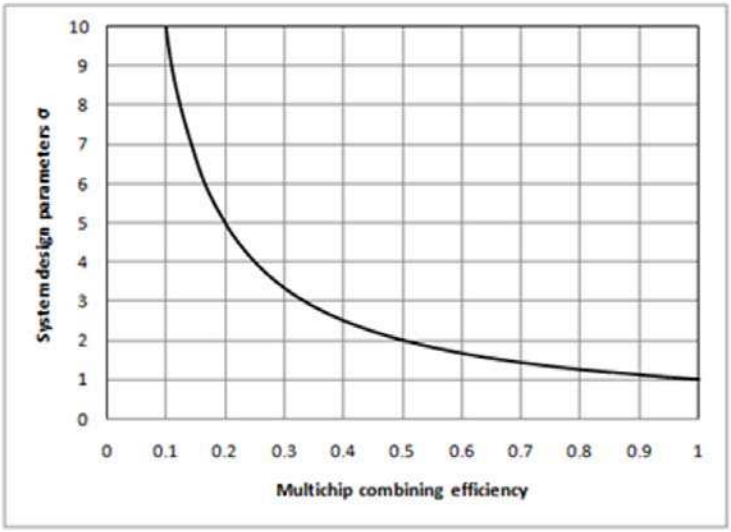


Fig. 5. Effect of combining multiple code pulses for both coherent and incoherent detection schemes

4. Performance analysis

Spectral amplitude coding optical CDMA systems using codes, which have code properties with low in-phase cross correlation, can eliminate the interference signals such as M-sequence (Peterson et al. 1995), Hadamard (Zou,Ghafouri-Shiraz et al. 2001), modified double weight (MDW) (Aljunid et al. 2004), and modified quadratic congruence (MQC) (Zou,Shalaby et al. 2001) codes. However, as broad-band thermal sources are used in such system, the phase-induced intensity noise (PIIN) that is due to the intensity fluctuation of thermal source severely affects the system performance (Smith et al. 1998). Commonly, these codes are represented by (N, w, λ) notation where N, w, and λ are code length, code weight, and in-phase cross correlation, respectively.

The establishment of MQC codes was proposed in (Zou,Shalaby et al. 2001). The proposed code families with the odd prime number p > 1 and represented by (p2+p, p+1, 1), have the following properties:

i. there are p2 sequences.
ii. each code sequence has N = (p2+p) chip component that can be splitted into w = (p+1) sets, and each set consists of one "1" and (p-1) "0 s".
iii. Between any two sequences cross correlation λ is exactly equal to 1.

According to (Zou,Shalaby et al. 2001), MQC code families can be constructed in two steps as following:

Step 1: Let GF (p) represents a finite field of p elements. A number sequence $y_{\alpha,\beta}(k)$ is assembled with elements of GF (p) over an odd prime by using the following expression:

$$y_{\alpha,\beta}(k) = \begin{cases} d[(k+\alpha)^2+\beta](\mathrm{mod}\, p), k=0,1,...,p-1 \\ [\alpha+b](\mathrm{mod}\, p), k=p \end{cases} \tag{3}$$

where d ∈ {0, 1, 2, …, p-1} and b, α, β ∈ {0, 1, 2, …, p-1}.

Step 2: a sequence of binary numbers $s_{\alpha,\beta}(i)$ is constructed based on each generated number sequence $y_{\alpha,\beta}(k)$ by using the following mapping method:

$$s_{\alpha,\beta}(i) = \begin{cases} 1, if i=kp+y_{\alpha,\beta}(k) \\ 0, otherwise \end{cases} \tag{4}$$

where i = 0, 1, 2, …, p2+p-1, k = $\lfloor i/p \rfloor$. Here, $\lfloor x \rfloor$ defines the floor function of x.

Table 2 shows MQC basic code matrix for p = 3. Thus, the code length N = 12, code weight w = 4, and in-phase cross correlation is 1. The upper bound of the number of codes that can be produced is p2 = 9 code sequences.

In the analysis of spectral-amplitude coding system, PIIN, shot noise and thermal noise are three main noises that should be taken into consideration. To simplify the analysis, the distribution of intensity noise and shot noise are approximated as Gaussian for calculating the bit-error-rate (BER). The analysis performance of optical CDMA system based on MQC codes in the existence of PIIN, the photodiode shot noise and the thermal noise are presented in (Zou,Shalaby et al. 2001). Based on the complementary detection scheme the average signal to noise ratio has been expressed as:

$$SNR = \frac{I^2_{Data}}{\left\langle I^2_{Total\,noise} \right\rangle} \tag{5}$$

$$I^2_{Data} = \frac{\Re^2 P_{sr}^2}{p^2} \tag{6}$$

P_{sr} is the effective power of a broadband source at the receiver and $\Re$ is the photodiode responsivity.

And

$$\left\langle I^2_{Total\,noise} \right\rangle = \langle I^2_{shot} \rangle + \langle I^2_{PIIN} \rangle + \langle I^2_{thermal} \rangle \tag{7}$$

		Code spectral chips											
		C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12
Code sequences (users)	1	1	0	0	0	1	0	0	1	0	0	0	1
	2	0	1	0	0	0	1	0	0	1	0	0	1
	3	0	0	1	1	0	0	1	0	0	0	0	1
	4	0	1	0	0	1	0	1	0	0	1	0	0
	5	0	0	1	0	0	1	0	1	0	1	0	0
	6	1	0	0	1	0	0	0	0	1	1	0	0
	7	0	1	0	1	0	0	0	1	0	0	1	0
	8	0	0	1	0	1	0	0	0	1	0	1	0
	9	1	0	0	0	0	1	1	0	0	0	1	0

Table 2. MQC basic code matrix for p = 3

Then,

$$SNR = \frac{\frac{\Re^2 P_{Sr}^2}{p^2}}{\frac{P_{Sr}\, e\, B\, \Re}{N}\left[p-1+2K\right] + \frac{P_{Sr}^2\, B\Re^2 K}{2\,\Delta\upsilon\; wp^2}\left[\frac{(K-1)}{p}+p+K\right] + \frac{4K_b T_n B}{R_L}} \tag{8}$$

Where e is the electron's charge, B is the noise-equivalent electrical bandwidth of the receiver, $\Delta\upsilon = 3.75$THz is the optical source bandwidth in Hertz, K_b is the Boltzmann's constant, $T_n = 300K$ is the absolute receiver noise temperature, and $R_L = 1030\,\Omega$ is the receiver load resistor.

Using Gaussian approximation, BER can be expressed as:

$$BER = P_e = \frac{1}{2}\, erfc\left(\sqrt{\frac{SNR}{8}}\right) \tag{9}$$

The system performance is shown in figure (6) for different MQC code size for two data rates. Data rate of 155 Mb/s shows good performance compared to 622 Mb/s. In communication systems, there is a trade-off between data bit rate and the provided system number of channels. Data bit rate x sequence code length = encoded chip rate. Generally, in optical CDMA analysis, in order to reduce the MAI limitations the data bit rate should be reduced. Increasing the bit rate will decrease the required average SNRs to maintain low BERs values, making the signal to be more sensitive to fiber dispersion and receiver circuitry noise.

The per code chip eavesdropper's SNRs as a function of the theoretical system capacity are shown in figure (7). If the authorized users transmit sufficient power so that 50%, 75%, 82%, and 85% of the theoretical system capacity is attained for MQC codes that have prime number p of 3, 7, 11, and 13 respectively, the eavesdropper has SNR of 15 dB. An optical matched filter receiver followed by envelope detection theoretically requires a peak SNR of approximately 15 dB to produce the required raw detector BER of 10^{-4}. Error correction codes used in commercial high-rate optical telecommunication equipment can produce the maximum acceptable system BER 10^{-9}.

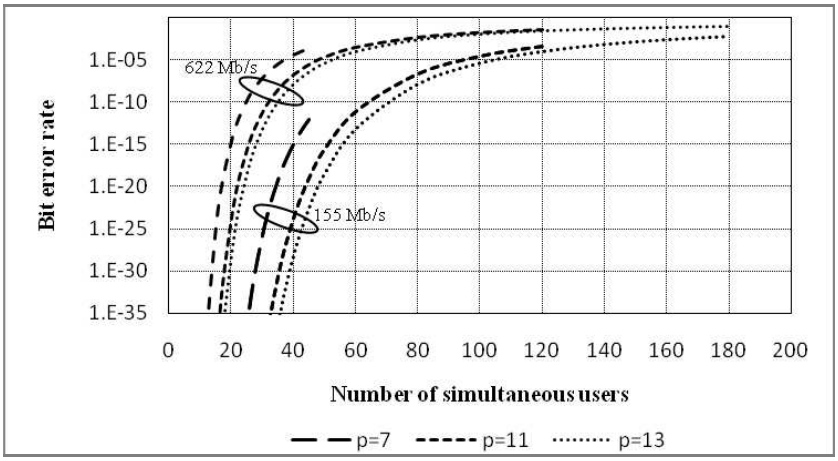


Fig. 6. BER versus number of simultaneous users. $P_{sr} = -10$ dBm.

The figure above shows a contradiction between network system performance and security. Increasing the network system capacity will lead the eavesdropper to detect high SNRs. Another limitation can be shown in figure (8), where high specified SNRs will increase the eavesdropper possibility of attacks.

Thus, for secure firms, a network designer should take these limitations under consideration. If 50% of the system capacity is provided, specified authorized SNRs between 10 dB to 15 dB are suitable for eavesdropper to get encoded pulse SNRs between 10 dB and 15 dB, respectively. Their corresponding bit error rates BERs are nearly 10^{-5} and 10^{-2}, respectively as shown in figure (9).

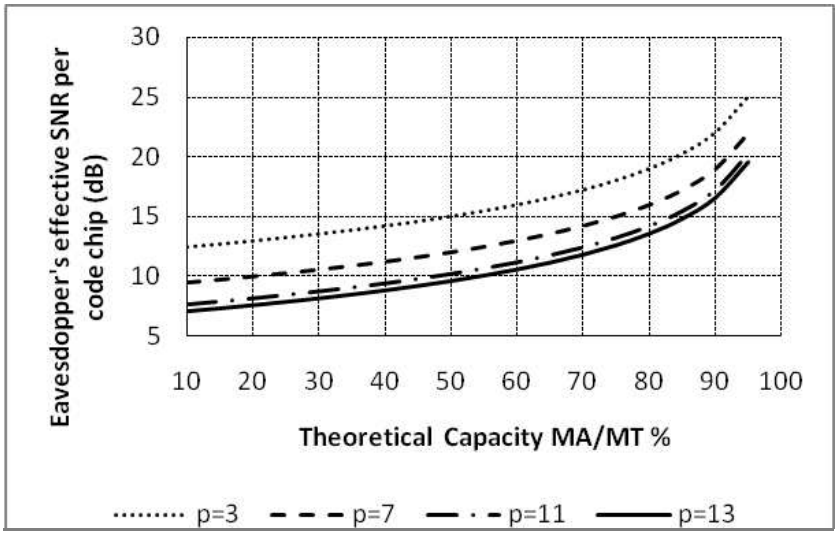


Fig. 7. Per chip code SNR as a function of theoretical system capacity

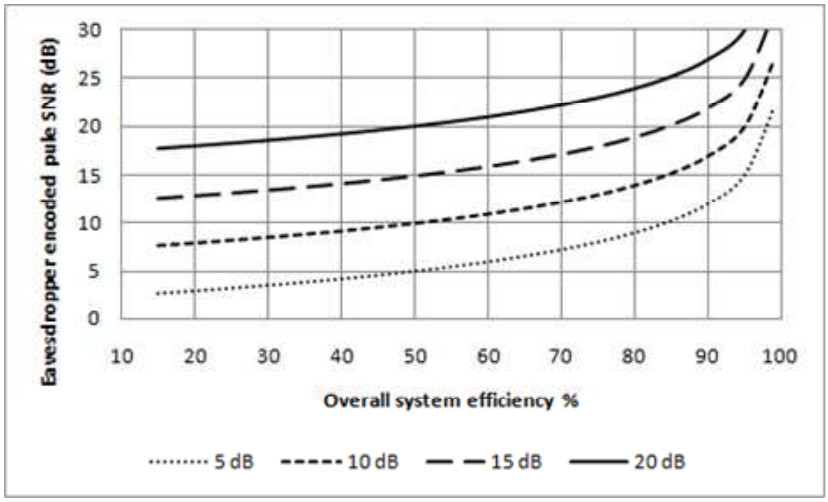


Fig. 8. Per chip code SNR as a function of theoretical system capacity for different specified authorized SNRs

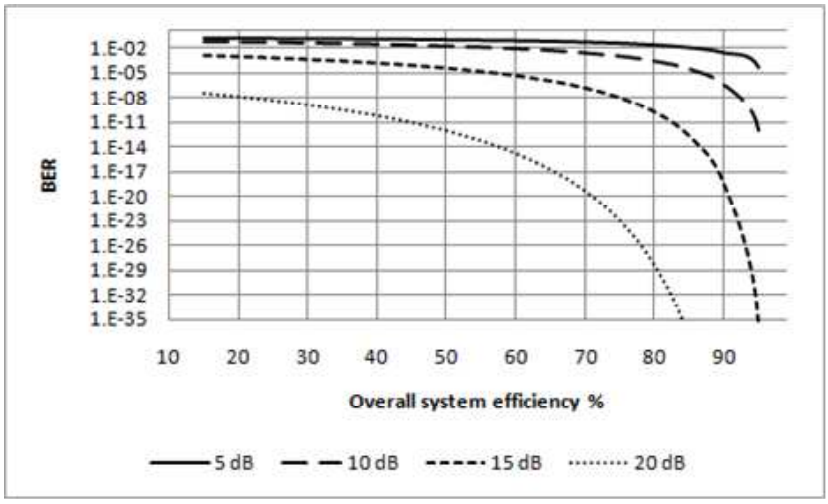


Fig. 9. BERs as a function of theoretical system capacity for different specified authorized SNRs

The eavesdropper performance of detecting spectral encoding chip bandwidth pulses form spectral amplitude optical CDMA code word that has been investigated in (Bakarman et al. 2009). The basic MQC code denoted by (12, 4, 1), has been considered to demonstrate the performance for both authorized user and eavesdropper.

Wide bandwidth enhances SNRs for both authorized user and eavesdropper, which increases the possibility of eavesdropping. Therefore, from the security viewpoint, one

should minimize the eavesdropper ability to detect code word pulses by controlling the authorized performance to reasonable throughput. This leads to security impact over system performance as shown in figure (10). The solid and dashed lines represent theoretical results for authorized user and eavesdropper, respectively using MQC (12, 4, 1). Whereas, triangle and rectangle symbols represent results for authorized user and eavesdropper, respectively using M. sequence code (7, 4, 2).

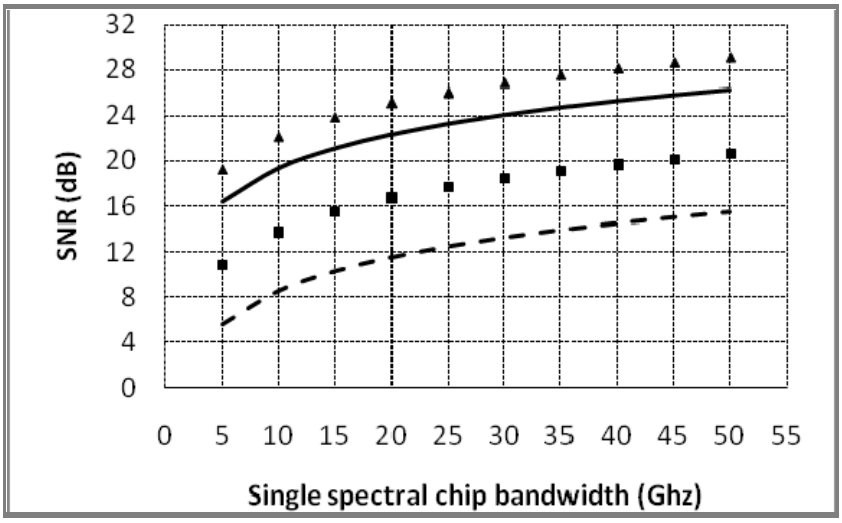


Fig. 10. Security impact over system performance for MQC code system

Thus, to improve the degree of security, we have to reduce the bandwidth of the encoding chip bandwidth pulses. This reduction should not affect the system performance. For example, if a spectral chip is reduced from 50 GHz to 25 GHz, the authorized user and eavesdropper could obtain SNRs of 23 dB and 12 dB respectively. These values correspond to bit error rate BERs of nearly 10^{-12} and 10^{-4} respectively. The maximum acceptable system BER is assumed to be 10^{-9}. Decreasing spectral chip, below than 25 GHz, will affect the authorized user performance forcing him to use error correction codes techniques used in commercial optical communications.

The results show that using unipolar optical CDMA codes schemes based on MQC and modified double weight MDW (Aljunid et al. 2004) code system enhance the security with a low cost implementation in comparison to the bipolar ones based on modified pseudorandom noise (PN) code (Chung et al. 2008), see also figure (10). MQC (12, 4, 1) code has 5 dB security preferences over PN (7, 4, 2) code. For the authorized users, bipolar codes would show high performance in comparison to unipolar codes because the bipolar signaling has a 3-dB signal-to-noise ratio (SNR) advantage over the on-off keying system with high cost implementation because each transmitter sends energy for both "0" and "1" bit (Nguyen et al. 1995). From the security viewpoint, one should minimize the eavesdropper ability to detect code word pulses by controlling the authorized performance to reasonable throughput.

Further security enhancement can be obtained by increasing the code dimension as shown in figure (11). With large value of prime number p, the main parameter to construct MQC codes, the eavesdropper ability to detect single encoded pulses becomes difficult even with wideband spectral chip. The eavesdropper BER will be higher than 10^{-3}.

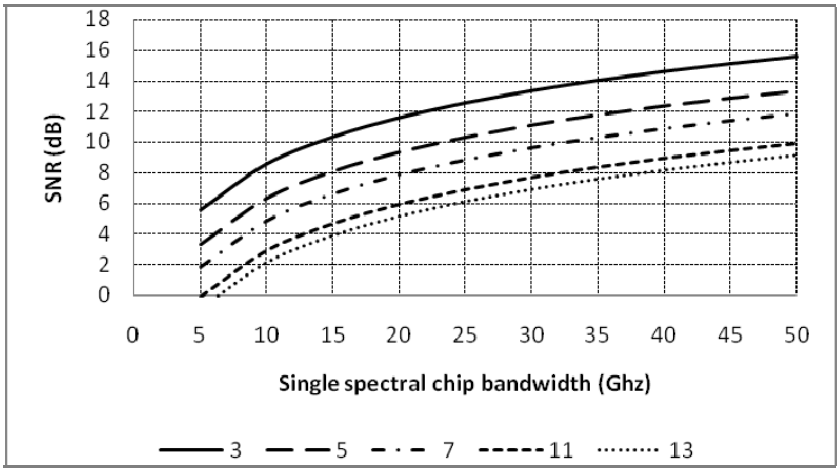


Fig. 11. Code dimension effects on eavesdropper performance

In communication systems, there is a tradeoff between data bit rate and the provided system number of channels. Data bit rate x sequence code length = encoded chip rate. Generally, in optical CDMA analysis, in order to reduce the MAI limitations, the data bit rate should be reduced. Figure (12) shows the impact of data bit rates on the eavesdropper performance. Increasing the bit rate will decrease the eavesdropper SNR, making the signal to be more sensitive to fiber dispersion and receiver circuitry noise.

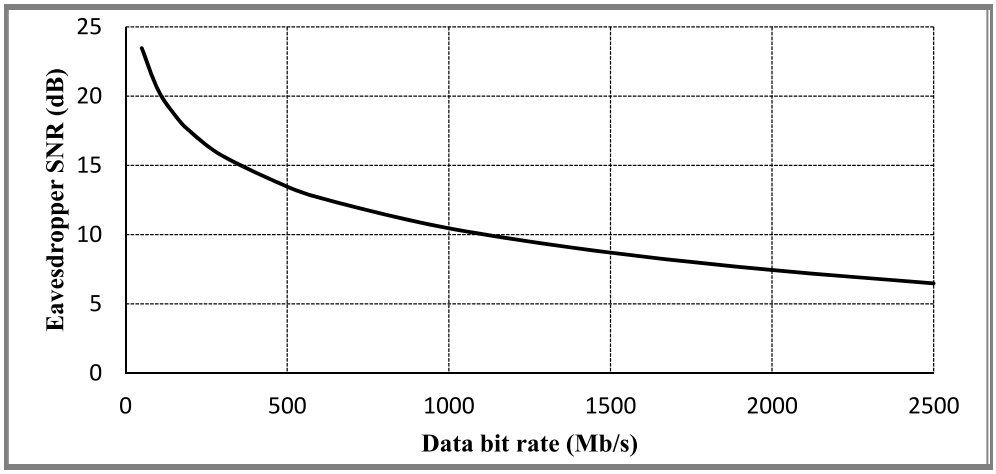


Fig. 12. Eavesdropper SNR vs bit rates

5. Conclusion

Improving the degree of security or enhancing the performance of optical CDMA networks have their impacts on each other such that a decision has to be made for cases in which all or some of these requirements are desired but cannot be fulfilled. The tradeoffs between security and the performance in optical CDMA, based on Modified Double Weight (MQC) system, are presented. From the security viewpoint, optical CDMA designer should minimize the eavesdropper ability to detect code word pulses by controlling the authorized performance to reasonable throughput. Otherwise, error correction codes techniques used in commercial optical communications would be the solution to obtain the maximum acceptable system BER.

6. Acknowledgment

This work was carried out at the Photonics Technology Laboratory (PTL), Institute of Micro Engineering and Nanoelectronics (IMEN),Universiti Kebangsaan Malaysia (UKM), under the supervision of professor Sahbudin Shaari. I would like to express my gratitude to him for providing a conductive enviroment for performing this research at this institute.

7. References

Aljunid, S. A., Ismail, M., Ramli, A. R., Ali, B. M. & Abdullah, M. K. 2004. A new family of optical code sequences for spectral-amplitude-coding optical CDMA systems. *Photonics Technology Letters, IEEE* 16 (10): 2383-2385.

Bakarman, H. A., Shaari, S. & Ismail, M. 2009. Security Performance of Spectral Amplitude Code OCDMA: Spectrally Encoded Pulse Bandwidth Effects. *J. Opt. Commun.* 30 (4): 242-247

Castro, J. M., Djordjevic, I. B. & Geraghty, D. F. 2006. Novel super structured Bragg gratings for optical encryption. *Lightwave Technology, Journal of* 24 (4): 1875-1885.

Chung, H. S., Chang, S. H., Kim, B. K. & Kim, K. 2008. Experimental demonstration of security-improved OCDMA scheme based on incoherent broadband light source and bipolar coding. *Optical Fiber Technology* 14 (2): 130-133.

Fisch, E. A. & White, G. B. 2000. *Secure Computers and Networks: Analysis, Design, and Implementation*. Boca Raton, FL: CRC Press LLC.

Imai, H., Rahman, M. G. & Kobara, K. 2005. *Wireless Communications Security*: Artech House Universal Personal Communications.

Jin-Hee, C. & Ing-Ray, C. On design tradeoffs between security and performance in wireless group communicating systems, at. *Secure Network Protocols, 2005. (NPSec). 1st IEEE ICNP Workshop on*: 13-18. 6 Nov. 2005

Mahafza, B. R. & Elsherbeni, A. 2003 *MATLAB Simulations for Radar Systems Design* Boca Raton: CHAPMAN & HALL/CRC.

Nguyen, L., Aazhang, B. & Young, J. F. 1995. All-optical CDMA with bipolar codes. *Electronics Letters* 31 (6): 469-470.

Oyster Optics, I. 2008. *http://www.oysteroptics.com/index_resources.html*.

Peterson, R. L., Ziemer, R. E. & Borth, D. F. 1995. *Introduction to Spread Spectrum Communications*. Englewood Cliffs: Prentice Hall.

Salehi, J. A. 1989. Code division multiple-access techniques in optical fiber networks. I. Fundamental principles. *Communications, IEEE Transactions on* 37 (8): 824-833.

Salehi, J. A. & Brackett, C. A. 1989. Code division multiple-access techniques in optical fiber networks. II. Systems performance analysis. *Communications, IEEE Transactions on* 37 (8): 834-842.

Shake, T. H. 2005a. Confidentiality performance of spectral-phase-encoded optical CDMA. *Lightwave Technology, Journal of* 23 (4): 1652-1663.

Shake, T. H. 2005b. Security performance of optical CDMA Against eavesdropping. *Lightwave Technology, Journal of* 23 (2): 655-670.

Smith, E. D. J., Blaikie, R. J. & Taylor, D. P. 1998. Performance enhancement of spectral-amplitude-coding optical CDMA using pulse-position modulation. *Communications, IEEE Transactions on* 46 (9): 1176-1185.

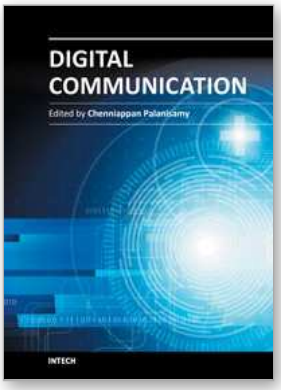
Teixeira, A., Vieira, A., Andrade, J., Quinta, A., Lima, M., Nogueira, R., Andre, P. & Tosi Beleffi, G. Security issues in optical networks physical layer, at. *Transparent Optical Networks, 2008. ICTON 2008. 10th Anniversary International Conference on*: 123-126. 22-26 June 2008

Wolter, K. & Reinecke, P. 2010. Performance and Security Tradeoff. In. Aldini, A., Bernardo, M., Di Pierro, A. & Wiklicky, H. (eds.). *Formal Methods for Quantitative Aspects of Programming Languages*: 135-167 Springer Berlin / Heidelberg.

Zorkadis, V. 1994. Security versus performance requirements in data communication systems. In. Gollmann, D. (eds.). *Computer Security — ESORICS 94*: 19-30 Springer Berlin / Heidelberg.

Zou, W., Ghafouri-Shiraz, H. & Shalaby, H. M. H. 2001. New code families for fiber-Bragg-grating-based spectral-amplitude-coding optical CDMA systems. *Photonics Technology Letters, IEEE* 13 (8): 890-892.

Zou, W., Shalaby, H. M. H. & Ghafouri-Shiraz, H. 2001. Modified quadratic congruence codes for fiber Bragg-grating-based spectral-amplitude-coding optical CDMA systems. *Lightwave Technology, Journal of* 19 (9): 1274-1281.



Digital Communication

Edited by Prof. C Palanisamy

ISBN 978-953-51-0215-1
Hard cover, 208 pages
Publisher InTech
Published online 07, March, 2012
Published in print edition March, 2012

All marketing is digital and everyone should have a digital strategy. Everything is going mobile. "The world has never been more social" is the recent talk in the community. Digital Communication is the key enabler of that. Digital information tends to be far more resistant to transmit and interpret errors than information symbolized in an analog medium. This accounts for the clarity of digitally-encoded telephone connections, compact audio disks, and much of the enthusiasm in the engineering community for digital communications technology. A contemporary and comprehensive coverage of the field of digital communication, this book explores modern digital communication techniques. The purpose of this book is to extend and update the knowledge of the reader in the dynamically changing field of digital communication.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Hesham Abdullah Bakarman, Shabudin Shaari and P. Susthitha Menon (2012). Security Limitations of Spectral Amplitude Coding Based on Modified Quadratic Congruence Code Systems, Digital Communication, Prof. C Palanisamy (Ed.), ISBN: 978-953-51-0215-1, InTech, Available from: http://www.intechopen.com/books/digital-communication/security-limitations-of-spectral-amplitude-coding-based-on-modified-quadratic-congruence-code-syste1

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821