IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 8, Issue 6 (Nov. - Dec. 2013), PP 70-74
www.iosrjournals.org

Security Based Performance Analysis in Optical CDMA Network Systems

Mohamed Mansour Shukra[1], Arvind Kumar Jaiswal[2], Mukesh Kumar[3]
[1]*M.Tech. in optical fibre Communication Engineering in Department of Electronics and Communication Engineering in SHIATS, Allahabad, India.*
[2]*Prof. and Head of ECE Dept at SHIATS-Allahabad, India.*
[3] *Asst. Prof. in the Department of Electronics & Communication Engineering in SHIATS, Allahabad, India.*

Abstract: *(OCDMA) is an alternative method, which performs encoding and decoding through an optical signature code, in order to allow the selection of a desired signal so that different users can share the same bandwidth. In such a systems, data signal overlap both in time and wavelength.*
Tradeoffs between security and performance in optical CDMA are presented. Confidentiality against eavesdropper interception strategies for optical CDMA is considered. Coherent detection and combining signals shows better confidentiality than the incoherent one. Spectral amplitude optical CDMA based on Modified Double Weight (MDW) systems, with different code dimension, is investigated. Increasing the network system capacity or maximizing authorized specified SNRs will lead to eavesdropper to detect high SNRs.

I. Introduction

Communication network system provides data transfer service for customers. Further requirement such as performance, security, and reliability characterize the quality for the transfer service. However, these requirements affect each other such that a decision has to be made for cases in which all or some of the requirements are desired but cannot be fulfilled.

The research activities in secure communication networks have paid little attention to the tradeoffs between security and other quality requirements of the communication service. While security is of prime concern in secure group communicating systems in both wireless and optical networks, security mechanisms employed often have implication on the performance of the system

Optical code-division multiple access (OCDMA) is a multiplexing technique adapted from the successful implementation in wireless networks. 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.

Compared to OCDMA the other multiplexing techniques and 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. Another approach to enhance security has been proposed using optical encoding techniques such as fiber Bragg gratings (FBG) to implement optical CDMA systems, Their degree of security depends on code dimensions being used.

There are five classes of security services in the field of secure data communication system: Authentication, access control, confidentiality, integrity and non-repudiation services. Table 1 shows the classification of the security service according to the OSI security Architecture

Table 1: Classification of the OSI Security Service

Security Services	Subclasses
Authentication	Peer entities Data origin
Access control	Communication services, Hosts, Networks, Subnets, etc.
Confidentiality	Data (connection-oriented, less, selective field) Traffic-related data
Integrity	Data (connection-oriented, less, selective field)
Non-repudiation	Data (origin and/or delivery)

II. Confidentiality In Optical Cdmasystems

The security services of a network have four fundamental objectives designed to protect the data and the network's resources. 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.

The degree of security in any security investigation can be powerfully affected by many assumptions. These assumptions include that eavesdropping at locations shown in figure 1 carried out with proper tools that are simple to realize using commercially available technologies and components, and attackers (eavesdroppers) are technologically intelligent with knowledge about signals being transmitted in optical CDMA networks (i.e. architecture of networks, types of signals, data rates, type of encoding, structure of codes, synchronization, ...etc). According to the well-known Kerckhoffs' principle in cryptography, one should assume that eavesdropper knows everything about cryptographic algorithm except for the key.

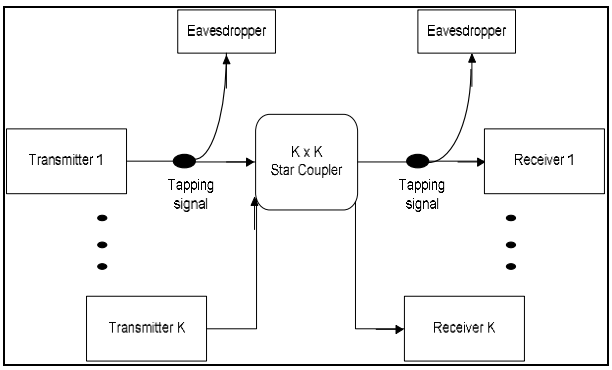

Fig.1. Places for an eavesdropper to intercept signals

Figure 1 shows the potential places to tap a signal from the user. However, when only one user is active in the network, optical CDMA scheme cannot guarantee physical layer security any more. In this case, an eavesdropper may intercept and extract information data simply by applying a band limited photodetector (PD), without the detailed knowledge of the code. The band-limited PD integrates energy within a bit period and converts noise-like OCDMA waveform into clean data signals. Even in a multi-user active OCDMA network, there can be a single user link as reported in recent systemic theoretical analyses.

III. Eavesdropping (Attacker)

The degree of security in any security investigation can be powerfully affected by many assumptions; these assumptions include that Eavesdropping at locations. Attackers (eavesdroppers) are technologically intelligent with knowledge about signals being transmitted in optical CDMA networks

IV. Security And Performance Tradeoffs

In security environments, it is believed that an inherent tradeoffs between networks performance and security exist 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, 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. Ensuring confidentiality against eavesdropper interception strategies for optical CDMA is conducted to investigate limitations and tradeoffs between security and performance.

Modified Double Weight (MDW) code has been proposed for spectral amplitude coding optical COMA system. MDW is the modified version of Double weight code and its code weight can be any even number that is greater than two. The MDW code possesses ideal cross-correlation properties and exists for every

natural number n. As a family of spectral amplitude code, MDW can be represented by (N, W, λ) notation where N is the code length, W is the code weight, and λ is the in-phase cross correlation. Increasing these code dimensions has good impact on confidentiality, because eavesdropper would need to detect higher SNRs.
Using the modeling approximations of, 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:

$$\frac{E_{ed}}{N_{0ed}} = \sigma\left(\frac{1}{w}\right)\left(\frac{1}{1-\frac{M_A}{M_T}}\right)\left(\frac{E_u}{N_{ou}}\right) \qquad (1)$$

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, $\frac{E_u}{N_{ou}}$ is the required user SNR (per data bit) to maintain the specified BER, M_T is the actual number of simultaneous users supported, and $\frac{E_{ed}}{N_{0ed}}$ is the eavesdropper's effective SNR per code chip. Where σ represents several system design parameters as following:

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

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 2 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, 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, coherent detection with combining signals shows better confidentiality than the incoherent one.

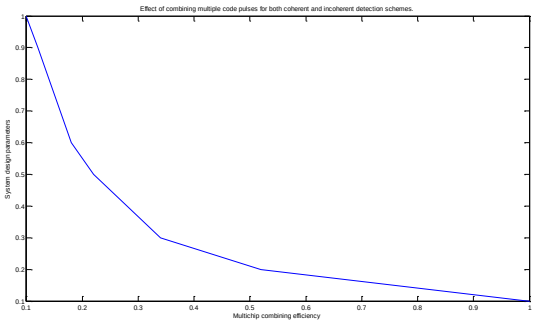

Fig. 2. Effect of combining multiple code pulses for both coherent and incoherent detection schemes.

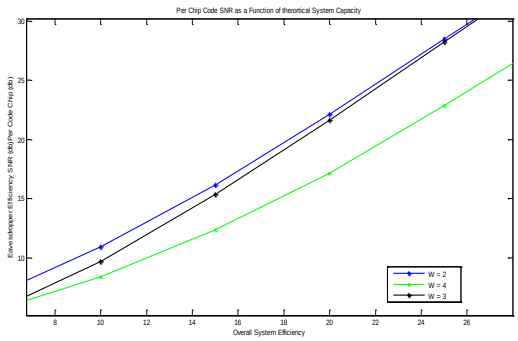

Fig.3. Per chip code SNR as a function of theoretical system capacity

The figure 3 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 4, where high SNRs are specified

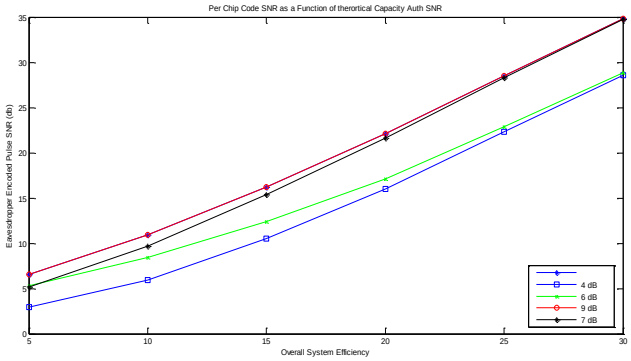

Fig.4. Per chip code SNR as a function of theoretical system capacity for different specified authorized SNRs.

Due care has taken to these limitations under consideration. If 50% of the system capacity is provided, specified authorized SNRs between 6 dB to 7 dB are Suitable for eavesdropper to get encoded pulse SNRs between 6 dB And 7 dB, respectively. Their corresponding bit error rates BERs are nearly 10^{-2}and10^{-1}, respectively as shown in figure 5.

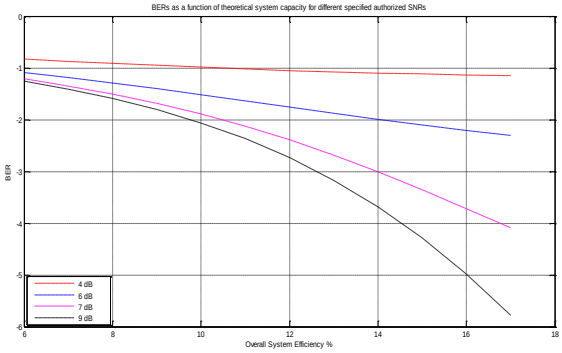

Fig.5. BERs as a function of theoretical system capacity for different specified authorized SNRs

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 6.

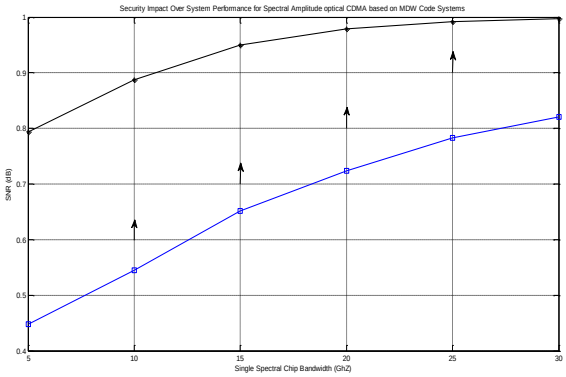

Fig.6. Security impact over system performance for spectral amplitude optical CDMA based on MDW code systems

To improve the degree of security, it has been to necessary to reduced the bandwidth of the encoding chip. This reduction has not affected the system performance. By reduction in spectral chip from 50 GHz to 25 GHz, the authorized user and eavesdropper could obtain SNRs of 22 dB and 16 dB respectively. These values are corresponding to bit error rate BERs of nearly $10^{-12}$and 10^{-5} respectively. The maximum acceptable system BER is assumed to be 10^{-9}. Decreasing spectral chip, below than 25 GHz, has affected the authorized performance forcing to use error correction codes techniques used in commercial optical communications.

V. Conclusions

Simulated design has been investigated for evaluation of system performance. Following are summarized observation:

Coherent detection with combining signals shows better confidentiality than the incoherent one, In the network system if one user is active, the optical CDMA scheme cannot guarantee physical layer any more, If the network capacity is increased, that will lead to eavesdropper to detect high SNRs, Higher SNRs will increase the eavesdropper possibility of attack, Wide bandwidth enhances SNRs for authorized user and eavesdropper, To detect the information data from the eavesdropper the signal to noise ratio SNRs must be reduced without effecting the system performance

References

[1] B. R Mahafza, *Radar Systems Analysis and Design Using MATLAB*. Boca Raton, FL: Champan Hall/CRC, 2005, ch. 4

[2] D. R. Stinson, *Cryptography: Theory and Practice*, Second Edition, 2000 N.W Corporate Blvd, Boca Raton, FL 33431: CHAPMAN & HALL/CRC, CRC Press LLC, (2002).

[3] E. A. Fisch and G. B. White, Secure Computers and Networks: Analysis, Design, and Implementation, Boca Raton, FL: CRC Press LLC, (2000).

[4] H. A. Bakarman, S. Shaari, M. Ismail, "Security Performance of Spectral Amplitude Coding OCDMA Systems," *International Conference on Electronic Design, ICED*, pp.1 - 4 (2008).

[5] H. A. Bakarman, S. Shaari, M. Ismail, "Security performance of spectral amplitude code OCDMA: spectrally encoded pulse bandwidth effects," *J. Opt. Commun.* 30, 242-247 (2009).

[6] J. A. Salehi, "Code division multiple access techniques in optical fiber network-Part I: Fundamental principles," *IEEE Trans. Commun* vol. 37, pp. 824-833 (1989).

[7] J. A. Salehi and C. A. Brackett, "Code division multiple access techniques in optical fiber network-Part II: System performance analysis," *IEEE Trans. Commun* vol. 37, pp. 834-842 (1989)

[8] J. M. Castro, I. B. Djordjevic, and D. F. Geraghty,"Novel Supper Structured Bragg Gratings for Optical Encyption," *J. Lightwave Technol*,vol. 24, pp. 1875–1865, 2006.

[9] N. Ferguson, and B. Schneier, *Practical Cryptography*, Indianapolis, IN: Wiley, (2003)

[10] S. A. Aljunid, A. R. Ramli, M. A. Borhanuddin, K. A. Mohamad, "A new family of optical code sequences for spectral-amplitude coding optical CDMA systems," *IEEE photonics technology letters* 16, 2383– 2385 (2004).

[11] T. H. Shake, "Security performance of optical CDMA against eavesdropping," *J.* Lightwave *Technol*,vol. 23, pp. 655–670, 2005.

[12] T. H. Shake, "Confidentiality performance of spectral-phase-encoded optical CDMA," *J. Lightwave Technol*, vol. 23, pp. 1652-1663, 2005.

[13] V. Zorkadis, "Security versus performance requirements in data communication systems," *Third European Symposium on Research in Computer Security Proceedings, Computer Security – ESORICS*, pp. 19-30 (1994).

AUTHOR'S PROFILE

Mohamed Mansour Shukra

Received his higher diploma of Electronic & Auto control from Higher Center for comprehensive Professions Sebha in LIBYA. M.Tech. in optical fibre Communication Engineering in Department of Electronics and Communication Engineering in SHIATS, Allahabad in India. Email: MM_SH2404@yahoo.com

A.K. Jaiswal is Prof. and Head of ECE Dept at SHIATS-Allahabad. He Obtained M.Sc. (TECH.) in Electronic & Radio Engg. from J. K. Institute Allahabad University in1967. He guided various projects & research at undergraduate &postgraduate level. He has more than 35years Industrial, research & Teaching experience and actively involved in research and publications. His area of interest includes Optical Networks and satellite communication.

Mukesh Kumar is working as a Asst. Prof. in the Department of Electronics & Communication Engineering in SHIATS, Allahabad. He received his M.Tech. Degree in Advanced Communication System Engineering from SHIATS, Allahabad in 2010. His research is focused on Signal processing, Wireless Sensor Network and Computer Networks ,Microwave Engineering, as well as Optical fiber communication