NET2 Groupwork: Lecture

OCDMA

Group 1: Marc Amay, Daria Ri, Regina Ochonu, Xiaohui Zhao

I. What is OCDMA and how does it compare to other multiple access techniques?
   - Differentiate TDMA, FDMA, CDMA
   - What are the spread spectrum techniques?

II. How CDMA works and what are the system parameters involved?

III. How does it affect the existing Optical Access Networks in terms of performance? What are the value add?
   - Advantages
   - Limitations

IV. How does it affect the existing Optical Access Networks in terms of Security? What are the value add?
   - How to increase security using OCDMA?

I. What is Multiple Access? Why do we do it and what are the different techniques to do it?

In communication system, Multiple Access allows several transmitters to send information simultaneously over a single communication channel and allowing several users to share a band of frequencies

There are three common types of multiple access systems:

i. Wavelength division multiple access (WDMA)
ii. Time division multiple access (TDMA)
iii. Code division multiple access (CDMA)

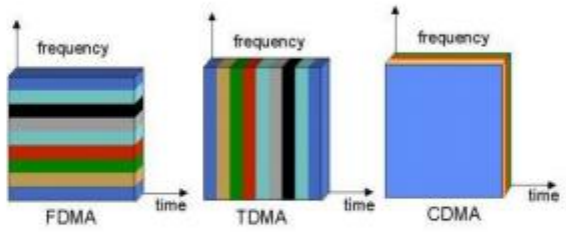


Fig 3: Multiple Access Methods [15]

A. Wavelength division multiple access (WDMA) In WDMA systems, each channel occupies a narrow optical bandwidth (≥100 GHz) and each channel is transmitted at a different wavelength respectively. Each channel is independent in terms of modulation format and speed for a particular wavelength

B. Time division multiple access (TDMA) In TDMA systems, each channel is allocated a time slot during which it can transmit. So the bandwidth is just single channel which is time shared by different stations. The main problem with TDMA lies in achieving synchronization between different stations.

C. Code Division Multiple Access (CDMA)
CDMA is where single channel carries all transmission simultaneously. We transmit multiple signals over the same frequency band, using the same modulation techniques at the same time [8]. CDMA is a form of spread spectrum transmission which uses spreading codes to spread the signal out over a wider bandwidth the would normally be required.

! CDMA differs from FDMA because only one channel occupies the entire bandwidth of the link.

! CDMA differs from TDMA because all stations can send data simultaneously; there is no timesharing

Spread spectrum techniques:

Frequency hopping spread spectrum (FHSS)
In frequency hopping spread spectrum, the signal is broadcast over a random series of radio frequencies, hopping from frequency to frequency at split interval. The receiverhoppe between frequencies in synchronization with the transmitter [8]**.**

Direct sequence spread spectrum (DSSS)
In direct sequence spread spectrum, users are differentiated by spreading code. Each bit of the information signal is combined with the bits of pseudorandom bit stream using an exclusive OR, thus each bit in the original signal is represented by multiple bits in the transmitted signals (Chip). The chipping code spread the signal across a wider frequency band in direct proportion to the number of bits used. In today scenario of communication, DSSS is the most commonly used spread spectrum.

OCDMA stands for Optical code-division multiple access combines the large bandwidth of the fiber medium with the flexibility of the CDMA technique to achieve high-speed connectivity

II. How CDMA works?

Each user on the O-CDMA system has a unique signature sequence. The encoder of each transmitter represents each "1" bit by sending the signature sequence whereas the binary "0" bit is represented by all zero sequence. Since each bit of the original signal is represented by a pattern of lit and unlit chips, the bandwidth of the data stream is increased [6]. Optical CDMA is therefore a spread spectrum technique. The optical CDMA encoded data is then sent to the N x N star coupler in a local area network or 1 x N coupler in an access network and broadcast to all nodes as shown in fig.4

In optical CDMA, different users whose signals may be overlapped both in time and frequency share common communication medium; multiple access is achieved by assigning unlike minimally interfering code sequence to different transmitter, which must subsequently be detected in the presence of multiple access interference from the users. The crosstalk between different users sharing the common fiber channel known as the multiple access interference is usually the dominant source of bit errors in an O-CDMA system. The intelligent design of the code word sequence is important to reduce the contribution of MAI to the total

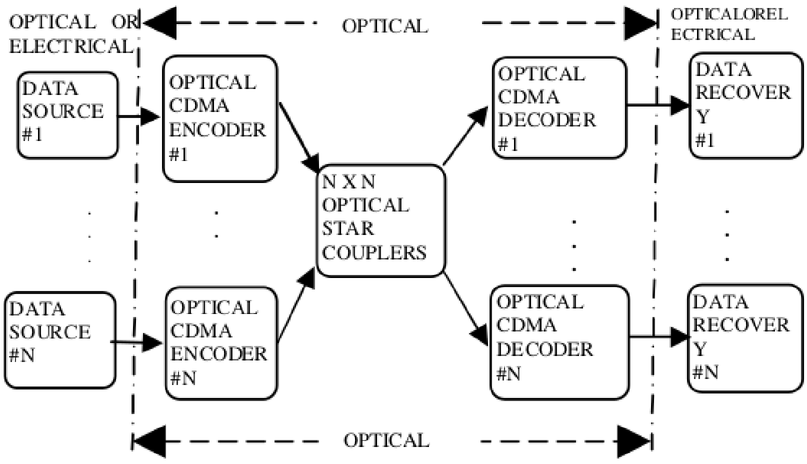


Fig. 4 Block diagram of an OCDMA communication system with a star architecture

received signal. Performance of O-CDMA communications is clearly dependent on the Multiple User Interface, the type of modulation used and the receiver topology

A. Coherent and Incoherent OCDMA

OCDMA system can be classified as *coherent* and *incoherent* depending on the nature of superposition of the optical signal. Incoherent systems use intensity-modulation/direct-detection (IM-DD) receivers that detect the power of the optical signal but not the instantaneous phase variations of the optical signal. Thus uses the presence of light signal energy or no light signal energy to represent the binary “1” and “0”. Incoherent OCDMA systems use only uni-polar codes.

In coherent OCDMA system, the phase information of the optical carrier is crucial for the dispreading process. It increases the complexity of receiver. However the performance of the coherent system is superior to the incoherent since the receiver is more sensitive to signal to noise ratio, which makes the overall system performance better [9]. Early O-CDMA networks were developed based upon code sequences of incoherent pulses and intensity modulation. The signals were therefore uni-polar with no negative components due to the incoherent nature of the system. Each user had a unique spreading sequence: coded transmission was sent to represent data bit “1” and null was used for a “0” bit. Nevertheless, the signature codes used, i.e. optical orthogonal codes (OOCs), generally had much poorer correlation properties than their bipolar counterparts, and their availability was severely restricted.

Later coherent systems often relied on phase coding of the optical signal field and coherent detection. Bipolar signaling was used in the form of ‘+1’ or ‘-1’, which could be obtained by manipulating the polarization or phase of the optical coherent carrier signal.

B. Synchronous and Asynchronous OCDMA

The optical CDMA system may be synchronous or asynchronous. In a synchronous OCDMA (S-OCDMA) the bit and chip are synchronized and the receiver examines the correlator output only at one instant in the chip interval. The codeset for S-OCDMA are described by the (N, w, λ). S-OCDMA dramatically improves efficiency by trading off between code length, MAI and address space. In the asynchronous OCDMA the bit are not synchronized but the chips may be transmitted synchronously. The codeset for A-OCDMA are described as (N, w, λ_a, λ_c). The cardinality of /C a / for A-OCDMA can be used as a codeset of C s with (N, w, max (λ_a, λ_c)) and cardinality /C s / = n. /C a / for S-OCDMA, since each of the n time shifts of each code sequence of C a can be used as a unique code sequence in C s with the same correlation properties

System parameters

a) *Bit rate*:

The OCDMA communication system must be optimized for bit rate in 4 Giga bps or higher.

b) *Chip rate*

The chip rate is the chips per second at which the code is transmitted. Chip is a sequence of numbers (+1, -1) in bipolar OCDMA or (1, 0) in uni-polar OCDMA that constitute the code assigned to each user, which is multiplied by a data sequence. The chips are therefore just the bit sequence out of the code generator; they are called chips to avoid confusing them with message bits. The chip rate is larger than the bit rate.

c) *Power handling (≤1)*

In optical CDMA systems physical channel corresponds to a particular spreading code, hence the received signal code power (RSCP) denotes the power measured by a receiver on a particular physical communication channel. It is used as a representation of signal strength and to calculate path loss [20].

d) *Processing gain*

The ratio of chip rate to the symbol rate is called the spreading factor or processing gain. It determines to a certain extent the upper limit of the total number of users supported simultaneously by a base station.

e) Multiple access interference

Multiple Access Interference (MAI) is a type of interference caused by multiple users who are using the same frequency allocation at the same time. The multiple-access interference can present a significant problem if the power level of the desired signal is significantly lower (due to distance) than the power level of the interfering user.

f) Shot Noise

Shot noise is a type of electronic noise which originates due to the quantized character of light radiation.

g) Beat Noise

Beat noise is due to interference, if fields of partially coherent light source are added.

E. Performance Parameters

The performance of OCDMA communication systems are evaluated in terms of:-

a) *Bit error rate*

BER is the most important parameter of the performance analysis disclosing the occurrence of errors when the system allocates the increasing number of simultaneous users.

It is desirable to optimize the OCDMA systems for BER of up to one error out of 10^{-9} or lower [15].

b) *Quality of services*

Quality of service is the ability of network to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow for providing multimedia services, video Conference and Internet etc.

c) *Eye Diagram:*

It is an experimental tool for the evaluation of the combined effects of channel noise and inter-symbol interference on the performance of a baseband pulse-transmission system. It is the synchronized

superposition of all possible realizations of the signal of interest viewed within a particular signaling interval.

III. The advantages / drawbacks / limits of the OCDMA

3.1 Advantages

a). Fair Division of Bandwidth

Explanation: Optical CDMA provides a way for many active users to share optical bandwidth in a fair manner.

- ➢ The bandwidth of the fiber medium is partitioned into a number of virtual channels, one for each station on the network. The large number of parallel channels eliminates channel contention.
- ➢ Crosstalk increases with the addition of each active user. All users on the network have access to an equal portion of the shared bandwidth, and one user cannot block access to the channel for any other user (if we ignore contention for a common receiver)
- ➢ Therefore, O-CDMA networks achieve the ideal in network fairness.

b). Flexibility

- ➢ Two-dimensional O-CDMA codes that use both time and wavelength domain encoding have been developed. It has favorable cross-correlation and autocorrelation characteristics.

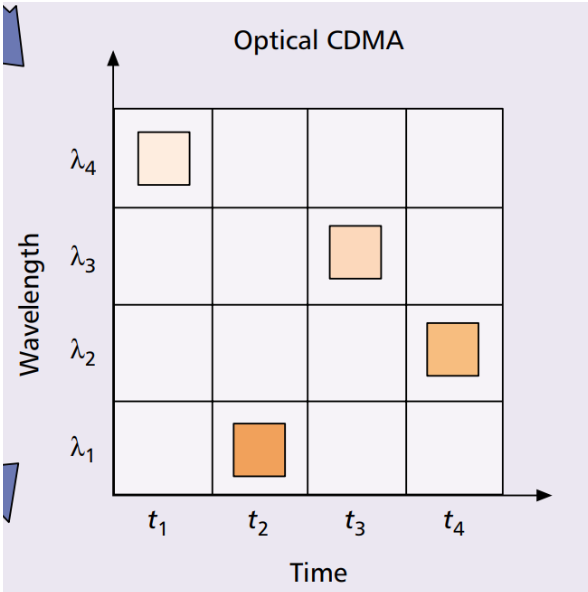


Fig1: OCDMA codes use both time and wavelength domain encoding

- ➢ Two-dimensional codes allow a network designer to tailor the spreading to the particular system under design.
- ➢ The aspect ratio of the 2D codewords is not fixed; therefore, to achieve a specified BER more wavelength spreading may be desirable in a system with a high channel count while additional time-domain spreading may be performed in a system with a low channel count.
- ➢ In O-CDMA, performance can also be traded for robustness. By sacrificing capacity, in terms of the maximum number of users that can be supported, the wavelength drifts due to temperature fluctuations could be controlled entirely through the use of robust codes. This eliminated the need for complex, expensive frequency control loops to manage wavelength drift.

flexibility
simplified network control and management
service differentiation
increased security.

3.2 Drawbacks
The technical
economic
perception barriers

III. OPTICAL ACCESS NETWORK PERFORMANCE IMPROVEMENTS USING OCDMA

1. OCDMA-WDM-PON - Using Hyperchaotic sequences

The high cost of provision of dedicated fibers and the requirement of a wavelength specific laser source at each ONU are the major limitations in the realization of high speed broadband access network infrastructure especially for the Next-Generation PON system requiring more than 64 optical network units (ONUs). To solve this problem, optical code division multiple access (OCDMA) over wavelength division multiplexed (WDM) Passive optical network (PON) has been proposed to provide sufficient subscribers and reduce the cost of PON systems.

The experimental setup of the proposed OCDMA-WDM PON system is shown in the Figure below;

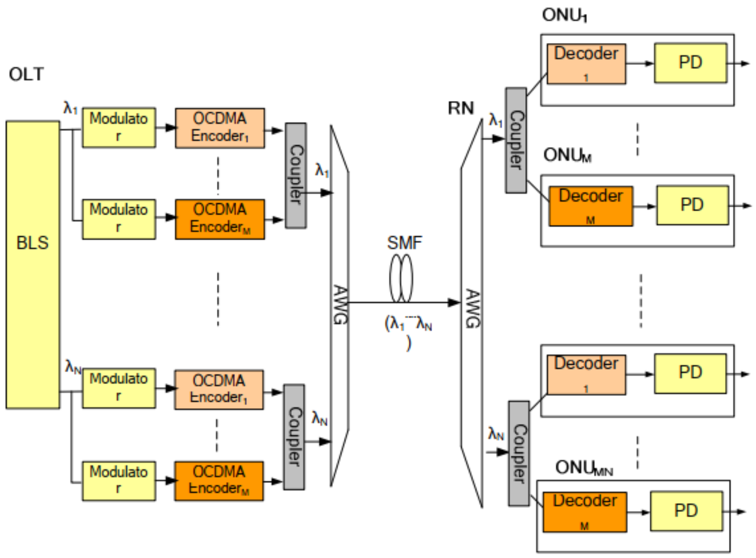


Fig 3.1: OCDMA-WDM-PON system architecture[1]

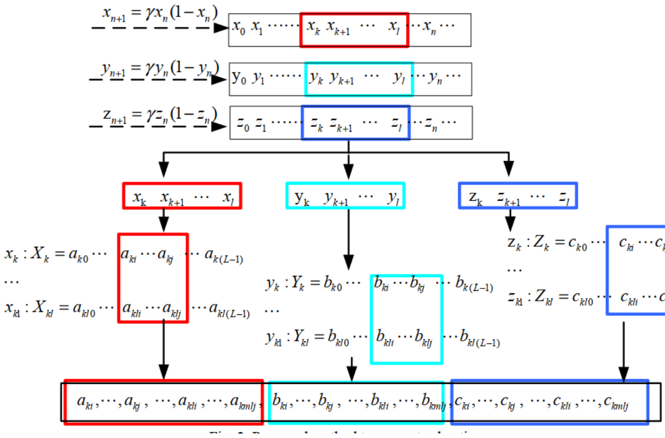
In the optical line terminal (OLT), the light source has to be replaced with a BLS which establishes p2p connections to each ONU. The number of ONU depends on the number of codewords and wavelengths. ONU extracts the desired signal through a decoder. Different wavelengths are multiplexed by arrayed waveguide grating (AWG) to send along the fiber. Encoded signals are broadcast to all nodes with the same wavelength. Each subscriber is assigned a distinguishable signature code. Only the receiver with a matching code can decode and convert the signals.

<u>To further improve the transmission efficiency</u>, an important problem for OCDMA is to generate a powerful sequence with **good correlation properties** and **large cardinality**. **Chaotic sequences** are investigated here to break a new path for spread spectrum sequences. The main advantages of the chaotic sequence are **ease of generation** of a great number of sequences, can offer favorable correlation characters, high capacity and good transmission performance.

<u>The design of chaotic sequences</u> is illustrated in Fig.3.2 below. Logistic-map function, given by;

$$\mathbf{x_{n+1} = \gamma x_n\,(1-\ x_n\,)}\ , \qquad \text{where } 1 < \gamma \leq 4$$

is used to generate real valued chaotic sequences $\{x_n\}$,$\{y_n\}$ and $\{z_n\}$ with the same control parameter (γ) and different initial values of $\{x_0\}$, $\{y_0\}$ and $\{z_0\}$. Then part of the sequences $\{x_n\}$,$\{y_n\}$ and $\{z_n\}$ are used to generate the new sequence and converted to binary sequences. The output sequence is the final one.



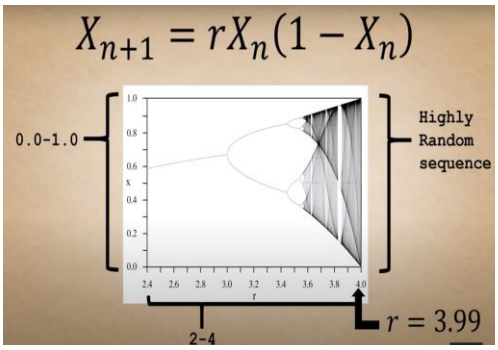


Fig. 3.2a: Proposed method to generate chaotic sequences[1] b)When $3.57 < \gamma \leq 4$, the Logistic-map enters a chaotic state.

$$x_{n+1} = f(x_n) = \frac{a}{2}\left(\frac{\gamma}{2}-1\right) - \frac{\gamma}{a}x_n^2, \quad x_n \in \left(-\frac{a}{2}, \frac{a}{2}\right) \quad (1)$$

$$y_{n+1} = f(y_n) = \frac{a}{2}\left(\frac{\gamma}{2}-1\right) - \frac{\gamma}{a}y_n^2, \quad y_n \in \left(-\frac{a}{2}, \frac{a}{2}\right) \quad (2)$$

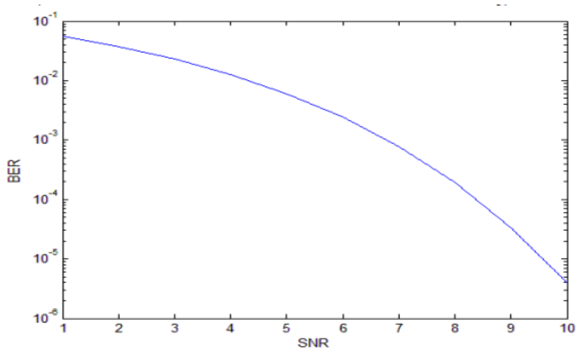
$$z_{n+1} = f(z_n) = \frac{a}{2}\left(\frac{\gamma}{2}-1\right) - \frac{\gamma}{a}z_n^2, \quad z_n \in \left(-\frac{a}{2}, \frac{a}{2}\right) \quad (3)$$

$$X_n = \sum_{i=0}^{L-1} a_i 2^{(L-1)-i} = (a_0 a_1 a_2 \cdots a_i \cdots a_{L-1}), a_i = 0,1 \quad (4)$$

$$Y_n = \sum_{i=0}^{L-1} b_i 2^{(L-1)-i} = (b_0 b_1 b_2 \cdots b_i \cdots b_{L-1}), b_i = 0,1 \quad (5)$$

$$Z_n = \sum_{i=0}^{L-1} c_i 2^{(L-1)-i} = (c_0 c_1 c_2 \cdots c_i \cdots c_{L-1}), c_i = 0,1 \quad (6)$$

<u>The system performance</u> was investigated in terms of **BER** as a function of **optical received power**. The BER performance depends mainly on the correlation properties of sequences. BER versus SNR simulation is as shown in Figure 3.3 below. The BER can be calculated from equations (7) and (8).



$$BER = Q\left(\sqrt{SNR}\right) = Q\left(\sqrt{\frac{\varphi_{xx}^2(0)N}{\left(12\sigma^6 + 14\sigma^4 + \frac{9}{2}\sigma^2\right)}}\right) \quad (7)$$

Where,

$$Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-\frac{z^2}{2}}dz = 1 - \varphi(x) \quad (8)$$

Fig 3.3: BER performance[1]

The BER varies from 10^{-1} to 10^{-5} when SNR changes from 1 to 10. It can be observed that 10^{-5} BER is obtained when SNR is near 10 dB. These simulation results suggest that the use of chaotic sequences for spectral spreading in OCDMA system provides several advantages over conventional methods while still preserving the same BER performance.

OCDMA Communications - Using Orthogonal Codes with Negative Auto-Correlation

In asynchronous DS/CDMA (direct sequence/code division multiple access) systems, BER can be reduced by using spreading codes with appropriate negative auto-correlation compared to the conventional uncorrelated spreading codes. Such spreading codes with negative autocorrelation can be generated by linear/nonlinear feedback shift registers (LFSRs/NFSRs) based on chaos theory. On the other hand, in synchronous DS/CDMA communications, multiple access interference (MAI) can be zero by using orthogonal spreading codes, such as Walsh codes and OVSF (orthogonal variable spreading factor) codes. Orthogonal codes can also be generated by NFSRs.

For optical OCDMA communications, OOC (optical orthogonal code) codes are proposed, where their cross-correlations depend on the number of collisions of 1's between the unipolar codes. However, using SIK (sequence inversion keyed) CDMA technique, which is another type of OCDMA communications with unipolar codes, correlation properties including negative auto-correlation and orthogonality of corresponding bipolar codes can be utilized.

Here, we discuss BER performance of orthogonal spreading codes with negative auto-correlation in particular OCDMA communications, where SIK technique is used.

<u>Generating the spreading codes</u> with negative auto-correlation (Figure 3.4 below), is based on a k-stage NFSR and a combinational logic circuit with 4 inputs. The NFSR generates a maximal-period sequence, called de Bruijn sequence of period 2k. Though de Bruijn sequences are uncorrelated ones, the output of the combinational logic circuit with 4 inputs a0, a1, a2, a3 can be a sequence with negative auto-correlation.

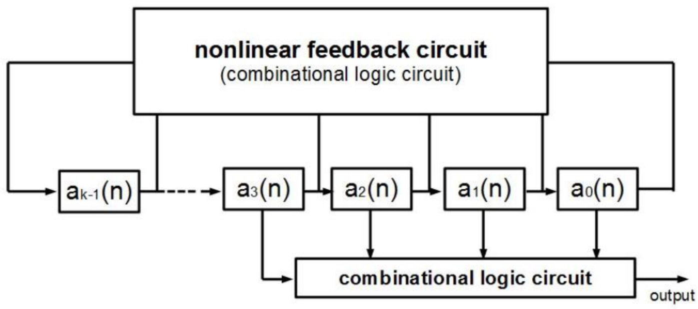


Fig 3.4: Generator of orthogonal spreading codes with negative auto-correlation based on k-stage NFSR[4]

Since a k-stage NFSR can be regarded as a finite-bit (k-bit) approximation of Bernoulli chaotic map, the combinational logic circuit is designed by using chaos theory for Bernoulli map. In the chaos theory, we can generate binary sequences with a normalized auto-correlation function C(ℓ) given by;

$$C(\ell) = 1(\ell = 0),\ -1/4(\ell = 1),\ 0(\ell \geq 2). \qquad (1)$$

Many binary (logic) functions for generating such sequences with negative auto-correlation given by eq.(1) can be obtained. Here, 6 logic functions where usedand are given by;

$$b_n = \begin{cases} 1 & a_0a_1a_2a_3 \in P_i \\ 0 & \text{otherwise}, \end{cases} \qquad (2)$$

$$\begin{aligned}
P_0 &= \{0010,\ 0011,\ 0100,\ 0110,\ 1000,\ 1010,\ 1110,\ 1111\},\\
P_1 &= \{0010,\ 0011,\ 0100,\ 0101,\ 0110,\ 0111,\ 1100,\ 1101\},\\
P_2 &= \{0010,\ 0011,\ 1000,\ 1001,\ 1010,\ 1011,\ 1100,\ 1101\},\\
P_3 &= \{0001,\ 0011,\ 0100,\ 0111,\ 1010,\ 1011,\ 1100,\ 1110\},\\
P_4 &= \{0001,\ 0011,\ 0100,\ 0101,\ 1000,\ 1001,\ 1101,\ 1110\},\\
P_5 &= \{0001,\ 0010,\ 0110,\ 0111,\ 1001,\ 1010,\ 1101,\ 1110\}.
\end{aligned}$$

Each of the six logic functions can generate a binary sequence with negative auto-correlation of eq.(1). Furthermore, the six binary sequences generated by a common de Bruijn sequence are orthogonal to each other.

Simulated Performance - For the CDMA scheme considered, each user transmits *f*-bit information simultaneously by using *f* orthogonal spreading codes with negative auto-correlation obtained from a de Bruijn sequence. Different users use different de Bruijn sequences for generating *f* orthogonal spreading codes. We assume the users transmit their information signal at different timing, that is, the CDMA system is asynchronous between different users. On the other hand, the *f* spread-spectrum signals of one user are transmitted simultaneously, that is, the CDMA system is synchronous and there is no MAI since the *f* spreading codes are orthogonal to each other.

Computer simulations of SIK optical CDMA communication where performed with the following simulation conditions;

- Number of information bits: 500bit/user/set
- Spreading code length $N = 128$ ($k = 7$)
- $f = 2 \sim 6$
- Number of users: $K = 2 \sim 32$
- Total number of channels ($f \times K$): 12∼64bits
- Channel noise: none

2,000 sets of simulations were performed by changing initial values of random numbers for generating information bits and inter-user delays. Thus, the average BERs were calculated and the BER versus total number of channels for *f* = 6 is as shown in Figure 3.5.

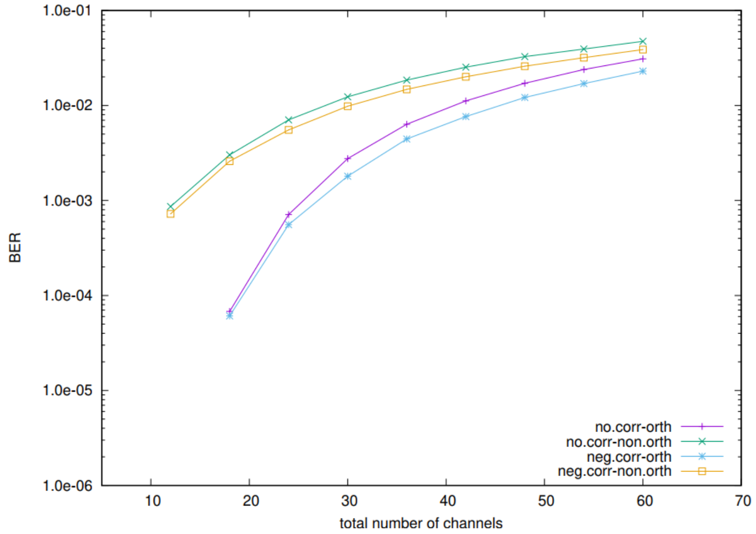


Fig. 3.5: BER versus the total number of channels (f = 6)[4]

orthogonal codes with negative auto-correlation is denoted by “neg.corr-orth” are proposed codes, and uncorrelated orthogonal codes (“no.corr-orth”), uncorrelated non-orthogonal codes (“no.corr-non.orth”), and non-orthogonal codes with negative auto-correlation (“neg.corr-non.orth”) are also shown for comparison.[4]

From Fig 3.5, we can see that the proposed orthogonal codes with negative auto-correlation achieve the lowest BER.

Ⅳ. Application (Security Performance)

4.1 How to improve the security of communication by using OCDMA?

To enhance security in the physical layer of an optical network, several approaches have been investigated, such as Quantum Private Communication, Optical Encryption, and Optical Steganography.

4.2 What’s Optical Encryption

- ➢ Optical CDMA (OCMDA) technology directly encrypts optical transmission links at the physical layer, which can improve the security of communication systems against fiber-optic eavesdropping attacks.
- ➢ OCDMA systems can achieve physical-layer encryption by using optical encoding and decoding technologies.
- ➢ Optical en/decoding technologies are the core technologies of OCDMA systems, which is one of the key issues to determine the security of OCDMA systems. The performances of optical encoder and decoder are mainly determined by the cross-correlation characteristics of the address codes, so it’s important to study the effects of the cross-correlation characteristics on the physical-layer security of OCDMA systems.

4.3 How to achieve Optical Encryption?

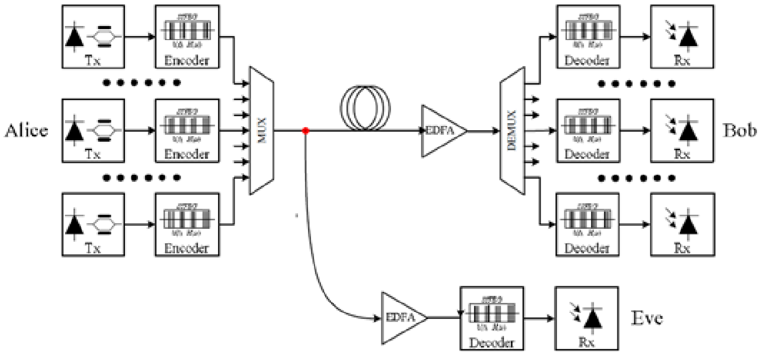


Fig4.1 The wiretap channel model of multiuser OCDMA system

The wiretap channel model of OCDMA systems is illustrated in Fig.1, assuming that both sides of secret communication are Alice and Bob, and there is an eavesdropper named Eve who can extract the transmission signal in the fiber-optic channel. According to pre-assigned address code, the sender named Alice carried out spread-spectrum coding of transmission signal in OCDMA systems. After multi users code division multiplexing, the optical signal appears to have broadband noise's characteristics, and only the receivers with matched decoder can recover specific signals from multi-user signals. When the legitimate users take security enhancement strategies (e.g. the code words switching, the code words reconstruction and multi-user transmission, etc.), the eavesdropper can't decipher the user's address code. So, the eavesdropper can't recover the original signals from the multi-user signals by an unmatched decoder, but the noise-like signals.

In the legitimate channel, the signals S sent by Alice is encoded by an optical encoder, then are coupled to the fiber channel together with the coded signals from other users and transmit. At the receiving end, the original signals sent by Alice are recovered from the multi-user signals through the matched decoder of Bob, and the datum is generated after the receiver.

4.4 What's the results of "secrecy capacity"?

Based on information-theoretic security, "secrecy capacity" is employed to evaluate the effects of the system parameters (the type of code words and the length of code words) on the physical-layer security of OCDMA systems, which provides theoretical guidance for OCDMA technology to be applied gradually. Secrecy capacity is the largest rate at which eavesdroppers gain no information from the message and can evaluate the physical-layer security of the secure communication systems quantitatively [6]. Its expression can be represented as:

$$\begin{aligned} C_S &= C_M - C_W \\ &= \max_{P(x)} \{ I(X;Y) - I(X;Z) \} \\ &= [I(X;Y) - I(X;Z)]_{P(X=0)=P(X=1)=0.5} \\ &= \left[\sum_{X,Y} P(xy) \log \frac{P(y|x)}{P(y)} - \sum_{X,Z} P(xz) \log \frac{P(z|x)}{P(z)} \right]_{P(X=0)=P(X=1)=0.5} \\ &= H_2(p_m) - H_2(p_w) \end{aligned} \tag{12}$$

The physical-layer security of OCDMA systems mainly depend on the following key system parameters: the type of code words and the length of code words related to the cross-correlation characteristics.

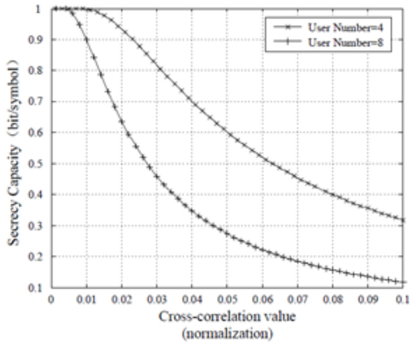


Fig4.2 Secrecy capacity vs. cross-correlation value

Fig.2 shows the relationship between the secrecy capacity and the normalized cross-correlation value, and the numbers of users are 4, 8 respectively. With the increasing normalized cross-correlation value, the secrecy capacity decreases, in other words, it helps for the security of OCDMA systems to choose the code words whose cross-correlation characteristics are better.

The main factors that cause the difference of cross correlation characteristics include the type of codeword and the length of codeword.

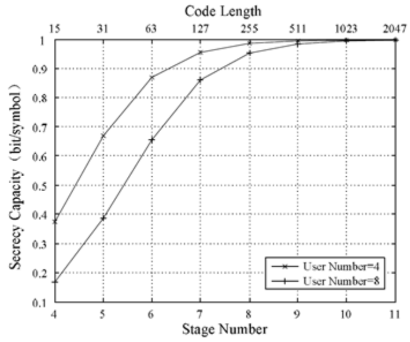


Fig4.3 Secrecy capacity vs. the length of code words

In Fig.3, we plot the secrecy capacity as functions of the length of Gold codes for the case of user numbers are 4, 8 respectively. It can be shown that with increasing the length of code words (the stage of shift register), the secrecy capacity of OCDMA systems increases. This is because the cross-correlation characteristics of code words will be better with the increase of the length of code words, which will lead to the increase of the secrecy capacity. Therefore, increasing the length of code words can help to improve the security of OCDMA systems.

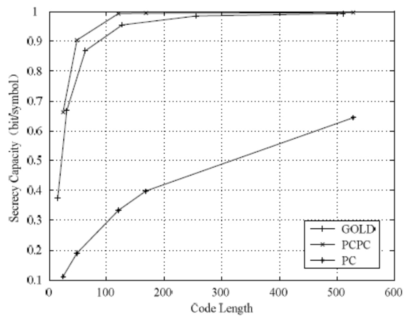


Fig4.4 Relationship between the secrecy capacity and the type of code words (user number is 4)

Fig.4 is the relationship between the secrecy capacity and the type of code words (user number is 4), and the types of code words are PC code, Gold code and PCPC code respectively. As can be seen from Fig.4, the secrecy capacity of OCDMA systems using PCPC code is in turn larger than that using Gold code and PC code, i.e., the safety level deteriorates in turn. This is because the cross-correlation characteristics of these three address codes are different, cross-correlation value of PCPC code < that of Gold code < that of PC code. Therefore, the secrecy capacity of OCDMA systems using PCPC code is larger than that using Gold code and PC code using the 2-D address codes or the bipolar address codes whose cross-correlation characteristics are better can improve the security of OCDMA systems.

4.5 How to evaluate Optical Encryption?

Based on Wyner's wiretap channel model, the wiretap channel model of OCDMA systems has been established, "secrecy capacity" is employed to evaluate the physical-layer security of OCDMA systems. The influences of the cross-correlation characteristics of code words, the type and length of code words related to the cross-correlation characteristics on the security of OCDMA systems are analyzed quantitatively. The results show that the secrecy capacity decreases with the increase of the cross-correlation value of code words. With the increase of the length of code words, the secrecy capacity increases as well. The secrecy capacity of OCDMA systems using PCPC code is in turn larger than that using Gold code and PC code.

4.6 What's Optical Steganography?

- Steganography is one of the methods that have received attention in recent years. The word steganography, which is derived from Greek, literally means "covered writing".

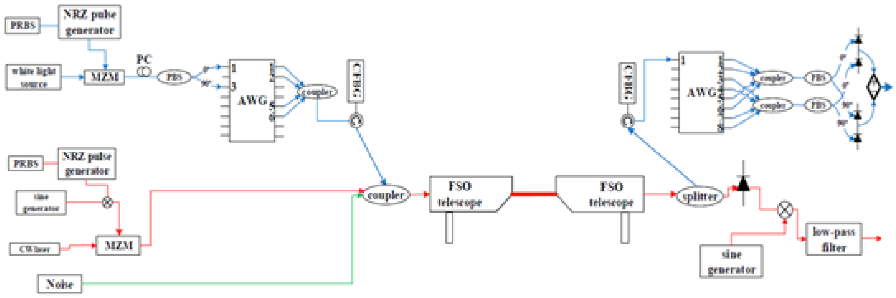
  For example, optical encryption allows a signal to be encrypted with low latency; thus, the recipient requires a key to read the information. However, each person notices the information by seeing the coded signal; that is, the method cannot prevent the signal from being detected. In some cases, the system is already in danger of being decrypted if an eavesdropper knows about the existence of the signal. Steganography provides an additional layer of security by hiding the data transmission underneath the steganographic medium.

- The physical layer security has become an important issue of communication security technique because it is cost-efficient without sacrificing much data rate. It takes the advantages of channel randomness nature of transmission media to achieve communication confidentiality and authentication.

4.7 What's the main difference between Optical Steganography and Optical Encryption?

The main goal of steganography is to hide information sufficiently well such that any unintended recipients do not suspect that the steganographic medium contains hidden data. This is a major distinction between steganography and the other methods of improving security.

4.8 What's the Proposed Optical Steganography System Setup?



The stealth signal is first encoded and then transmitted into the public channel. To simulate the system noise in a real optical network, a noise source is introduced to generate noise and couple it to the public and stealth signals. This enables convenient investigation of the impact of system noise on the stealth signal.

We transmit a BPSK signal in the public channel to make the signal always exist irrespective of the data bit transmitted. The stealth signal is not exposed because of the disappearance of the public signal.

On–off keying (OOK) data are generated using a white light source, and the MZM is driven by a pseudorandom binary sequence (PRBS). A polarization controller is placed between the modulator and the PBS to adjust the SOP. The modulated signal is divided into mutually orthogonal SOPs by the PBS and then input into the AWG-based OCDMA encoder. The encoded stealth signals are combined using a coupler and passed through a CFBG for further pulse broadening to lower the peak power for effectively concealing the stealth channel beneath the public channel.

To restore the stealth signal, the received signal is first passed through a CFBG, which is the same as that at the transmitter except with opposite dispersion. The stretched stealth signal is then compressed back into the original profile. Thereafter, the mutually orthogonal SOP components from the encoded spectrum are input to the AWG router for OCDMA decoding. The output ports of the AWG couple with the upper and lower couplers depending on the signature code Ck and its complementary code Ck. With the PBS, the same SOPs of spectra are extracted for balanced detection. Furthermore, the detected electrical signal from the lower branch is subtracted from the corresponding signal from the upper branch. Finally, the stealth signal is obtained using the decoding mechanism.

4.9 How to evaluate Optical Encryption?

This method transforms the stealth signal into a noise-like signal so that it can be buried in the public channel. The results indicate that the security of the system is enhanced because no one except the intended recipient knows the existence of the stealth signal in either the spectral or time domain.

The power of the public noise is proportional to the security of the system and inversely proportional to the performance of the stealth channel. That is, with larger public noise, the stealth signal can be hidden more efficiently but the BER is higher.

An eavesdropper needs the correct dispersion compensator to detect the stealth signal. Even if the correct dispersion is obtained by using a tunable dispersion compensator, the eavesdropper cannot recover the data without the corresponding receiver. The results show that the stealth signal is favorably hidden in the public channel and that our proposed optical steganography system provides high security when the average power of the stealth signal, public signal, and public noise are -5, 0, and -3 dBm, respectively.

REFERENCES

1. Yang, L., Shi, S., & Zhang, W. (2018, October). Performance analysis of OCDMA-WDM-PON system with hyperchaotic sequences. In *2018 Asia Communications and Photonics Conference (ACP)* (pp. 1-3). IEEE.

2. Chih-Ta Yen, Jen-Fa Huang, and Wen-Zong Zhang. Hiding Stealth Optical CDMA Signals in Public BPSK Channels for OpticalWireless Communication. *Appl. Sci. 2018, 8, 1731; doi:10.3390/app8101731.*

3. Yeteng Tan, Tao Pu, Jilin Zheng, Hua Zhou, Guorui Su, and Haiqin Shi. Study on the Effect of System Parameters on Physical-Layer Security of Optical CDMA Systems. *International Conference on Optical Communications and Networks, 2019.*

4. Yoshioka, T., & Tsuneda, A. (2019, October). Study on Optical CDMA Communications Using Orthogonal Codes with Negative Auto-Correlation. In *2019 International Conference on Information and Communication Technology Convergence (ICTC)* (pp. 1234-1236). IEEE.