Introducing a soa based cmux and cdemux for ocdma system

Technology, Internet

OCDMA Technology is one of the promising technologies to implement all-optical networks. Optical networks are used in multiple access technique to reach the demand for large capacity and high speed communication.

Presently communication demand is extremely high because of research and production of various new communication methods. All-optical communication, offering security amid transmission, and being proficient in transfer speed use are the cases of the properties that are produced because innovative work of OCDMA network. OCDMA has turned out to be vital piece of the computerized communication framework for long haul, fast LAN and MAI networks.

For OCDMA systems, the performance matrices like bit error rate and quality factor depends upon the number of users accessing the bandwidth at a time and number of users also depends upon the types of codes used. As a result, many code algorithms, many methods and many techniques have been proposed. In this research a two code keying encryption technique is used to design the proposed OCDMA technique. In this paper OCDMA system is designed using Semiconductor Optical Amplifiers (SOAs). SOA is very attractive nonlinear elements for the realization of different logic functions, since they can exhibit a strong change of the refractive index together with high gain. Due to tremendous growth in the volume of information exchange and strong demands in security and privacy, the issues and degree of physical-layer confidentiality potentially supported by O-CDMA have become an interesting research topic.

From the concept of multi code keying encription the two code keying encriiption is used in this research to enhance the confidentiality and security of the user.

In this research an optical code word multiplexer (CMUX) is designed using two code keying encryption to multiplex the user data as well as an optical code word de-multiplexer is designed to de-multiplex the CMUX to get the user data. A two code keying encryption is a technique where two unique optical code words and a unique key are multiplexed with a user data. Finally in this paper an optical data is multiplexed with CMUX and transmitted through an optical fiber varying different fiber length and finally CDEMUX is used in the receiver side to get the original data. The whole system is designed in the optical domain and it is called OCDMA system.

The software implementation of the proposed two code-keying encryption techniques, which relies on all-optical exclusive-or (XOR) gate and codeword multiplexer (CMUX) are also investigated. The new all optical design is scalable and integrable and also able to handle both data bits and encryption keys in the optical and non-return to-zero (NRZ) format. In the NRZ format, the signal to the CMUX can provide large enough (time) window to switch optical codewords, without the need of any pulse duplicator (if RZ format is used) [10]. To gate the data at the receiver side a code word de-multiplexer (CDEMUX) is also introduced which is designed for the first time in this paper with the help of all optical logic gates.

Design structure

This figure shows the overall concept of proposed OCDMA system. From the figure it can be understood that CMUX is consist of SOA (semiconductor optical Amplifier) based optical combinational logic circuit which multiplex the user data with two optical codes and unique key. On the other hand, at the receiver side CDEMUX (code word de-multiplexer) is used to get the user data. CDEMUX also consist of SOA based optical combinational circuit.

The 2 × 1 CMUX is designed with the all optical logic gates made with SOAs which is polarization independent. This CMUX is actually 2 × 1 code word multiplexer where two code words are multiplexed and passed through a single line. The encrypted key Ei found from the XOR gate is used as input of the CMUX as shown in Fig. 2. The principle of CMUX is when encryption key Ei = 0 , Cj will pass on the other hand when encryption key Ei = 1 and the lower SOA pass the optical codeword Cj+1 . The center SOA can invert the optical signal. Where CW laser beam is injected in forward and Ei is injected in backward. Both outputs are combined with the help of 2×1 optical combiner. As a result, the final logic of the all-optical 2×1 CMUX is Cj (E_i)̅ + CjE_i.

A two input XOR gate design

The two XOR gate is designed with SOA so that it can only deals with optical signals. It can work with the date bits of up to 10 Gb/s. In this all optical XOR gate there are two inputs. One is key stream Ki and another is data stream Di. In principle, at the top SOA the Ki (which is optical NRZ pulse) is injected in backward and simultaneously Di is also injected in forward which is also

NRZ format. As a result, the output from the top SOA will be D_i (K_i)̅. So, the D_i pulse can pass through SOA when the Ki pulse is absent.

Ki (which is optical NRZ pulse) is injected in forward and simultaneously Di is also injected in backward which are also NRZ format. As a result, the output from the top SOA will be (D_i)̅Ki. Ki pulse can pass through SOA when the Di pulse is absent. Similarly, two outputs are combined together help of optical 2×1 passive combiner to get the final output D_i (K_i)̅+(D_i)̅Ki. which is all optical XOR operation and also the XOR output is denoted as encryption key E to the CMUX.

Codeword De-Multiplexor (CDEMUX)

TABLE1: Truth table of the CMUX logic circuit

E	C0	C1	o/p= C0E+C1 E̅
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Table1 shows truth table of the CMUX logic circuit. From the truth table, CDEMUX logic circuit can be designed. It is observed that by making NOR gate of CMUX output and codeword C1 we can get E which was XOR output. Then making XOR of E and KEY finally we can get the user data. After designing the CMUX and CDEMUX different data can transmit thorough a fiber over the OCDMA system to observe the performance of the whole designed system.

Simulation

In this section the simulation of all XOR gate, CMUX, CDEMUX, OCDMA with WDM system are simulated in optisystem and the results are discussed.

XOR gate design

Here,

UDBS = User Defined Bit Sequence

NRZPZ= NRZ Pulse Generator

MZM= Mach-Zehnder Modulator

2×1 Power Combiner

1×2 Power Splitter

SOA = Semiconductor Optical Amplifier

GOF= Gaussian Optical Filter

Here two User Define Bit Sequence(UDBS) are used to represent the user data stream and key stream. The Mach-Zehnder Modulator used to modulate the bit sequence and convert the it into optical signal. Here two input power combiners are used to combine two optical signals. On the other hand, power splitter is used to split the signal. SOAs are optical amplifiers are also used to maintain the logic function (discussed in design structure chapter). Also, optical amplifier is used to make the signal stronger. At last GOF is used to eliminate the unwanted signal and get the original signal.

For two input XOR logic gate, if two bits are presented together and two bits are absent together the XOR output will be 0 (no bits). On the other hand, any one bit is absent and another bit is present together the output will be 1.

In the optical format, a stream of NRZ data bits D = 01011011 and a stream of NRZ encryption keys K= 11010110 are applied to the XOR gate. XOR output is a steam of NRZ cipher bits E0 = D0 ⊕ K0 = 10001101which is same as the simulation (shown in Fig. 8)

CMUX design

The simulation set-up of the all-optical 2 × 1 CMUX has been presented in Fig. 9. From the design structure section, it can be observed that the CMUX output will be C0E+C1 $\overline{E}$. For E= 0, C0 will be selected as output as well as for E= 1, C1 will be selected as output. Here C0= 01101101 , C1= 10010010 and XOR output, E= 10001101

The CMUX output should be 00011111. In this Section the Bit Error rate and Quality factor(Q) are investigated and the result is analyzed for the proposed OCDMA System.

Q factor Vs Fiber length

In optical communication, the acceptable BER (without the application of any error correcting schemes) can be considered less than □10□^(-12) and the corresponding value of quality factor is, Q ≥6 [18], [19]. The system performs better up to 70 km. After 70Km the log(BER) increased (grater than -12) which is not acceptable. At fiber length 70 km the Q factor of the User is 6. 6(shown in Fig. 14). After 70 Km the Q factor falls to below 6 which is not acceptable [22]. So, from the two graphs it can be observed that the proposed OCDMA system performs well up to 70 km of Fiber length.

To enhance physical-layer confidentiality SOA (semiconductor optical Amplifier) based Optical CMUX and a SOA based optical CDEMUX is designed and implemented in the software for OCDMA system using two code keying encryptions. From graphs and results it can be observed that the designed system has the best transfer rate of 1. 25 Gb/s for each user that achieved along a 70km long fiber. (without application of any error correcting schemes and amplifier). The concept of multi code keying is used in this paper which is best for security and confidentiality enhancement [19].