Secure Optical Communication using Spreading Codes and Cryptography

Mintas Parveen C. M.

M.Tech Student, Electronics and Communication, KMEA College of Engineeering, Ernakulam, India

Abstract: Fiber optic communication uses several multiple access schemes. Among them Optical Code Division Multiple Access (OCDMA) is one of the multiple access schemes that are widely used because of their advantages such as the flexibility in the allocation of channels, ability to operate asynchronously, enhanced privacy and increased in burst networks. This paper deals with the security enhancement of an OCDMA system. Network security has three major security goals: confidentiality, availability and message integration between senders and receivers. To overcome the drawback of existing OCDMA system cryptography is applied. Cryptography can be used by everyone to protect the confidentiality of their information transmitted over insecure channels as well as to provide privacy, authenticity and data integrity. To provide more confidentiality two cryptographic techniques are incorporated into the system. The proposed technique is based on cryptography which includes the encryption and decryption of the information with the employment of a random key. This paper also discusses the comparison of the above two cryptographic techniques in the OCDMA system to find the best suited encryption technique for OCDMA system that provides strong security.

Keywords: Optical Code Division Multiple Access, Spreading codes, Cryptography, Advanced Encryption Standard, Blowfish.

I. INTRODUCTION

Internet traffic has been growing promptly for many years. There is also a strong relationship between the increase in demand and the cost of bandwidth. Therefore bandwidth taken by each user has been a major factor. Optical network communication is such a technology that full fills this kind of requirements. These networks are also progressively becoming capable of delivering bandwidth in a flexible manner whenever needed. Fiber optic communication uses several multiple access schemes. Among them Optical Code Division Multiple Access (OCDMA) is one of the multiple access schemes that are widely used because of their advantages such as the flexibility in the allocation of channels, ability to operate asynchronously, enhanced privacy and increased in burst networks OCDMA is becoming popular for its low loss and wide bandwidth. OCDMA employs spread spectrum technology which is employed using spreading codes. Here a type of spreading code (gold code) has been generated by using pseudo noise sequence as the basic sequence. Gold codes are selected based on the Autocorrelation and Cross-correlation properties. The objective of the work is the security enhancement of an OCDMA system. Network security has three major security goals: confidentiality, availability and message integration between senders and receivers. To overcome the drawback of existing OCDMA system cryptography is applied. Cryptography can be used by everyone to protect the confidentiality of their information transmitted over insecure channels as well as to provide privacy, authenticity and data integrity.

As an enhancement to provide more confidentiality two cryptographic techniques are incorporated into the system. The proposed technique is based on cryptography which includes the encryption and decryption of the information with the employment of a random key. Based on the encryption and decryption throughput calculated the best suited cryptographic technique suited for the OCDMA system is found. Also the BER vs SNR graph of the OCDMA system is plotted. The gold codes with good correlation properties and the cryptographic techniques incorporated provide more security, and prevention from interference and jamming. So by combining the wide advantages of OCDMA and cryptographic technique a strict security can be ensured and thereby the confidentiality can be improved.

II. TECHNICAL OVERVIEW

In an existing OCDMA system each data is transmitted using unique spreading codes. For providing more security these coded data is again encrypted and decrypted using two cryptographic techniques and throughput of both techniques are compared based on encryption and decryption time.

A. Generation of Gold codes

Gold sequences have been suggested by Gold in 1967 and 1968. Gold sequences form an important class of periodic sequences that provides larger set of sequences with good periodic cross-correlation. These are generated by XOR-ing two PN sequences of the same length with each other. Inotherwords the modulo-2 addition of two Maximum Length Sequences (M-sequences) having same length generates Gold codes. The code sequences are added chip by chip by clock synchronization. The created codes are of the same length as the two M-sequence is added together [6]. Gold codes are selected based on the correlation properties. These codes have good autocorrelation properties and are the pairs with low cross-correlation values. So gold codes will perform better in an OCDMA system and also prevent the Multiple Access Interference (MAI).

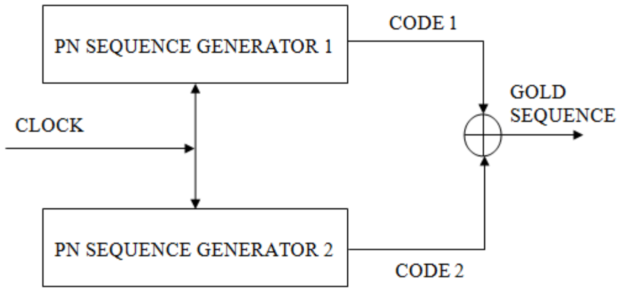

Fig. 1 Gold sequence generator

B. Generation of cryptographic algorithms

- Advanced Encrytion Standard (AES)

AES is a symmetric block cipher. 128 bit blocks of data are encrypted and decrypted using AES. AES comprises of a number of rounds; in which each round performs number of transformations on a state, and it also makes use of a round key which is generated from the encryption key. The number of rounds is based on the block and key sizes. An encryption of a block begins with a conversion 'AddRoundKey', which is followed by a number of ordered rounds, and ends up with a special final round. Special final round differs from the regular rounds. This alteration in the final round has nothing to do with security, but do the reverse encryption and makes the decryption possible. Each transformation in AES is executed in a state that can be pictured as a rectangular array of bytes. The state comprises of four rows and a number of columns which is defined by the block size in bytes divided by four.

A state of four rows is required for a block size of 128 bits.

The four transformations in one round are:

- 1. AddRoundKey
- 2. SubBytes
- 3. ShiftRows
- 4. MixColumns

10 numbers of rounds are required for 128 key sizes. All the nine rounds would execute all the four transformations but the final round contains only three steps. In the final round MixColumn transformation is not present. The Roundkeys are generated by expanding the key used for encryption into a group holding the RoundKeys one after the other. The expansion functions on words of four bytes. The Rijndael proposal for AES defined a cipher that can operate on various block lengths and key lengths. They are 128, 160, 192, 224, and 256 bits [7]

- Blowfish

Blowfish is a symmetric encryption algorithm, that is both encryption and decryption of messages are done using the same secret key. Blowfish is also a block cipher that is during encryption and decryption it divides a message into fixed length of blocks.

The block length of Blowfish is 64 bits; data's that aren't a multiple of eight bytes in size should be padded. Key-expansion and data encryption are the two important parts of Blowfish. During the key expansion stage, the key inputted is converted into several sub key arrays total 4168 bytes. There is the P array, which has eighteen 32-bit boxes, and the S-boxes, that are four 32-bit arrays with 256 entires each. The first 32 bits of the key are XORed by P1 that is the first 32-bit box in the P-array after the string initialization. Then the second 32 bits of the key are XORed by P2, and so on, until all 448, or fewer, by returning to the beginning of the key the key bits have been XORed cycle through the key bits, till the entire P-array has been XORed with the key.

Encrypt all the zero string by means of the Blowfish algorithm, using the modified Permutation array (P-array) above, to obtain a 64 bit block output. P1 is replaced with the first 32 bits of output, and P2 is replaced with the second 32 bits of the output. By making use the 64 bit output as input, back into the Blowfish cipher, can yield a new 64 bit block. The next values in the P-array are replaced with the block. Repeat this for all the values in the P-array and all the S boxes in order [8].

III.PROPOSED SYSTEM

The proposed system is shown in the below figure.

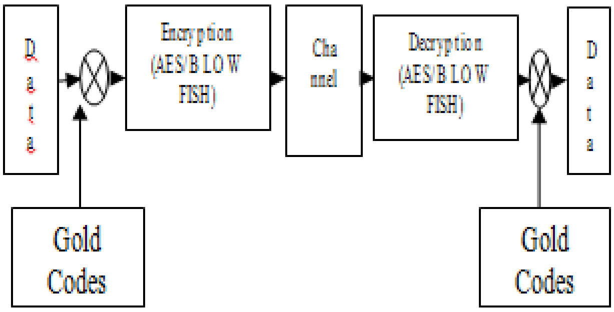

Fig. 2 Proposed system

In the proposed system two cryptographic techniques are used in this OCDMA system and their performance are evaluated by estimating the encryption and decryption throughput by calculating the encryption time and decryption time of two algorithms to find the best suited cryptographic technique for an OCDMA system. The Gold codes are generated and cryptography is applied using the MATLAB. The code is multiplied with the input data, then modulated and encrypted using Advanced Encryption Standard and Blowfish cryptographic method. After the encryption, the encryption times of both algorithms are calculated. Then the data is transmitted through a Rayleigh channel and also noise is added by passing it through an Additive White Gaussian Noise (AWGN) channel. At the receiving end the data is demodulated, then decrypted again using AES and Blowfish. After the decryption, the decryption times of both algorithms are calculated and then the throughput of encryption and decryption of both AES and Blowfish are evaluated. After that the original data is retrieved from the Gold code at the receiver.

Finally the transmitted bit is received. Also the comparative study of the above cryptographic techniques are made to find the best suited algorithm for an OCDMA system to avoid several kind of attacks and thereby making the OCDMA system more secure.

IV. RESULTS AND DISCUSSIONS

The OCDMA system with gold code and cryptographic techniques are implemented. In the proposed system, the performance metrics estimated are encryption time, decryption time and throughput. The encryption time is defined as the time the encryption algorithm consumes to produce a cipher text from a plain text. Encryption time is used to estimate the throughput of an encryption scheme that indicates the speed of encryption. The throughput of the encryption scheme is estimated as the total plaintext in bytes encrypted divided by the encryption time. The decryption time is defined as the time the decryption algorithm consumes to produce plain text from the cipher text. Decryption time is used to estimate the throughput of a decryption scheme that indicates the speed of decryption. The throughput of the decryption scheme is estimated as the total cipher text in bytes decrypted divided by the decryption time [9, 10].

The throughput of the encryption process is calculated using the following formula.

$$Throughput = \frac{Tp}{Et}$$

where *Tp* is the Total Plain text and *Et* is the Encryption time. Similarly, the throughput of the decryption process is calculated using the following formula.

$$Throughput = \frac{Tc}{Dt}$$

where *Tc* is the Total Cipher text and *Dt* is the Decryption time. Along with the encryption and decryption output of AES and Blowfish the BERvs SNR performance of an OCDMA sytem incorporating the cryptographic techniques are plotted. The simulated outputs are shown below.

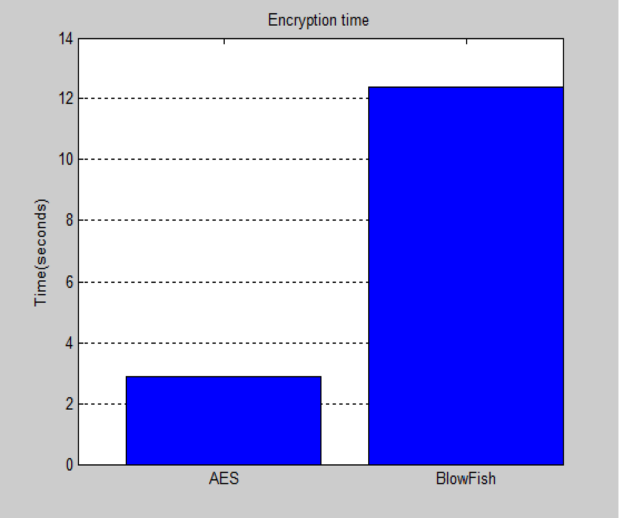

Fig. 3 Encryption time of AES and Blowfish

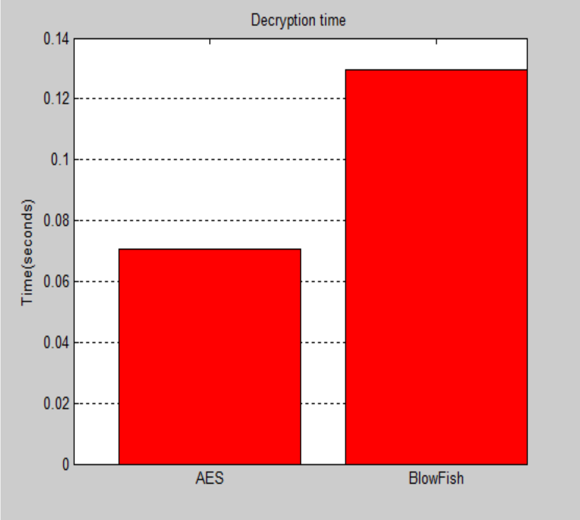

Fig. 4 Decryption time of AES and Blowfish

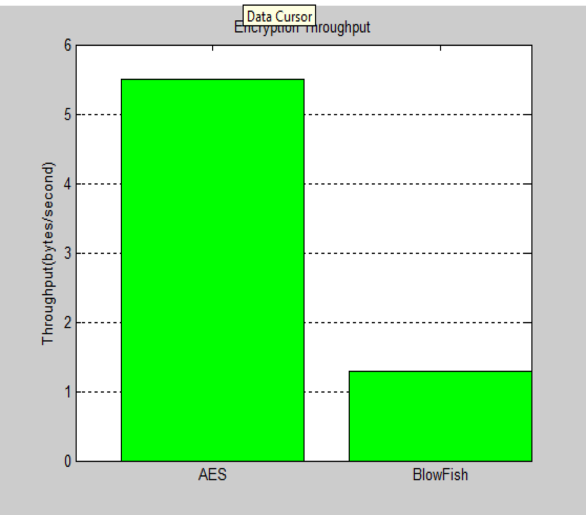

Fig. 5 Encryption throughput of AES and Blowfish

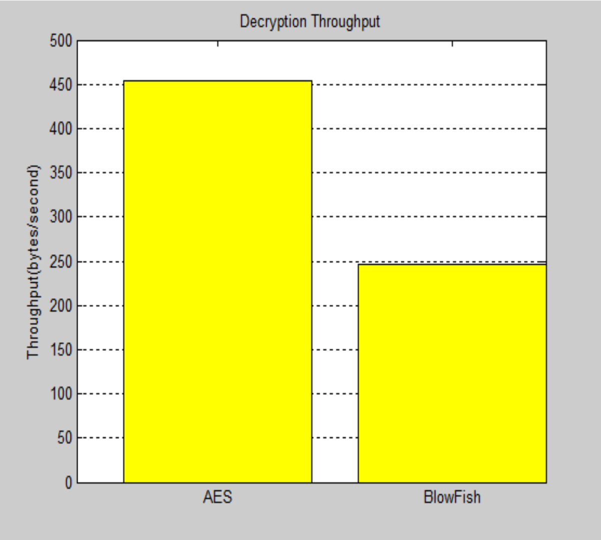

Fig. 6 Decryption throughput of AES and Blowfish

DOI 10.17148/IJARCCE.2015.41080

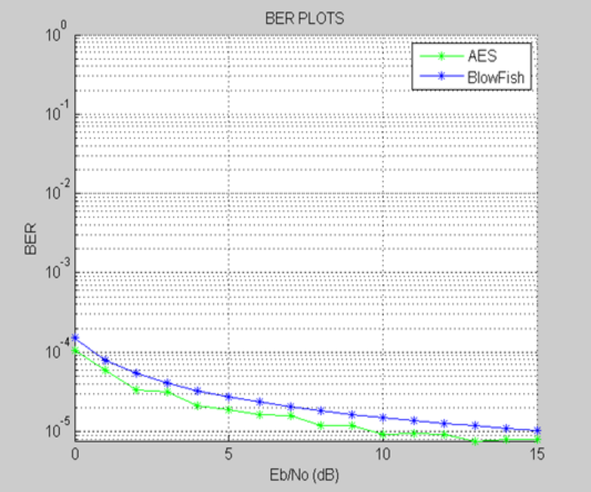

Fig. 7 BER vs SNR graph of OCDMA system

V. CONCLUSION

For the security enhancement of OCDMA system the two cryptographic techniques like AES and Blowfish are incorporated into the existing OCDMA system. The performances of both algorithms in OCDMA system are compared and evaluated. And as a result the AES cryptographic technique which has small encryption and decryption time and also higher encryption and decryption throughput than Blowfish are found to have better performance.

The BER performance of OCDMA system using AES and Blowfish are also evaluated. From the BER performance of OCDMA system it is clear that AES incorporated OCDMA system performs better than Blowfish. And from the above shown results it is concluded that AES is the best suited cryptographic technique for OCDMA system and also the cryptography incorporated OCDMA system performs better than the existing OCDMA system. So by combining the wide advantages of OCDMA and cryptographic technique we can ensure a strict security and thereby the confidentiality can be achieved.

REFERENCES

[1] Snehal Iranna Upwar , Abhishek Shevde , " Performance analysis of OCDMA system using Gold Code " , Proc on IJECE , Vol. 7 , pp.1 – 5 , 2014

[2] Thomas H.Shake," Security Performance of Optical CDMA Against Eavesdropping " , Journal of Lightwave Technology, VOL.23, pp. 655-670, 2005

[3] Vishav Jyoti, Rajinder Singh Kaler, " Simulation Analysis of security Performance of DPSK OCDMA network via virtual user scheme ", Maejo International Journal of Science and Technology , Vol.2 , pp. 238-248 , 2012

[4] Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader, and et .al , " Evaluating the Performance of Symmetric Encryption Algorithms " , International Journal of Network Security, Vol.10, pp. 213 – 219 , 2010

[5] M. Anand Kumar and Dr. Karthikeyan ,"Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms",I. J. Computer Network and Information Security,Vol-2,pp.22-28,2012

[6] S. M. Jahangir Alam, M.Rabiul Alam," Bit Error Rate Optimization in Fiber Optic Communication ,International Journal of Machine Learning and Computing, Vol. 1, pp .435-440 , 2011

[7] Poonam Jindal and Brahmjit Singh , " Study and Performance Evaluation of Security - Throughput Tradeoff with Link Adaptive Encryption Scheme ", International Journal of Security ,Privacy and Trust Management, Vol – 1, 2012

[8] Anirudh Sharma, Tariq Anwar, "Simulation of Gold Code Sequences for Spread Spectrum Application " , International Journal of Engineering and Technical Research (IJETR) , Vol.2, pp. 129-132, 2014

[9] S. Pavithra and Mrs. E. Ramadevi , " Performance Evaluation of Symmetric Algorithms " , Journal of Global Research in Computer Science, Vol-3,pp 43-45, 2012

[10] Rishabh Arora and Sandeep Sharma , " Performance Analysis of Cryptography Algorithms " , International Journal of Computer Applications, Vo l- 48 , pp.35- 39,2012

BIOGRAPHY

Mintas Parveen C. M. received the B.Tech degree in Electronics and Communication Engineering in 2009 from KMCT college of Engineering under Calicut University, and is at final stage of M.Tech in Communication Engineering at KMEA Engineering College, Mahatma Gandhi University, Kerala. Her research interest includes optical fiber communication, network security and cryptography.

DOI 10.17148/IJARCCE.2015.41080