International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 06 | Jun 2022 www.irjet.net p-ISSN: 2395-0072

PERFORMANCE EVALUATION OF CROSS LAYER SECURITY SYSTEM FOR SECURE OPTICAL TRANSMISSION

Narmatha J[1], I. Muthumani[2]

[1]*Student, Dept. of ECE, GCE, Tirunelveli, Tamil Nadu, India*
[2]*Professor, Dept. of ECE, GCE, Tirunelveli, Tamil Nadu, India*

Abstract - *Cross layer security network is used to improve the security of image transmission over optical fiber and Image confidentiality is increased by means of this method. To evaluate the Security performance of cross layer security network, encoding schemes is performed at the different network layers. It is difficult for the eavesdropper to intercept the code as it provide cross layer security for both physical and datalink layer. The original image is recovered if user use correct decoder and encryption algorithm. Hence it achieves higher confidentiality than other network.*

Key Words: Image transmission, Security, Encryption, Confidentiality

1. INTRODUCTION

Fiber optic network is used in many applications for image transmission. As user information is more sensitive, it is important to maintain security in image transmission. Eavesdropper use some of the techniques like differential detection, Energy detection and Code interception to eavesdrop the signal. Two level of security is implemented by means of cross layer security network. Cross layer security is the combination of both physical layer security and data layer security. To improve the security, transmitted data is encrypted at both physical layer and data layer. To evaluate the Security performance of cross layer security network AES encryption is used in data layer and CDMA technique is used in physical layer.

1.1 Physical layer security

To enhance the security of communication channel physical layer security is important. OCDMA is employed to enhance physical layer security. Optical code-division multiple access (O-CDMA) technique has a advantage of providing large bandwidth of the fiber medium and flexibility. Hence it achieve high-speed connectivity, fairness, flexibility, simplified network control and management, service differentiation, and increased security.

1.2 Data layer security

Algorithmic cryptography is employed to enhance data layer security. Algorithmic cryptography is classified as two types

- Symmetric key cryptography
- Asymmetric key cryptography

The technique used here is symmetric key encryption.

AES encryption technique is employed to enhance the security at data layer.

2. PROPOSED METHODOLOGY

The block diagram for cross layer security network is depicted in Fig.1. cross layer security system is designed with the help of optisystem. optical encoder and optical decoder is constructed by means of optical delay lines with the optical orthogonal code. At the transmitter, user data is encrypted by means of AES encryption, and then modulated by means of M-Z modulator. The transmission power is 0 dBm and the central wavelength is 1550 nm. The transmission rate is 10 Gbit/s. The modulated signal is encoded by the optical encoder using optical orthogonal code . Then, the signal is amplified by an erbium doped fiber amplifier (EDFA) and transmits through a single mode fiber link. The dispersion compensation fiber (DCF) is used to compensate for the fiber dispersion.

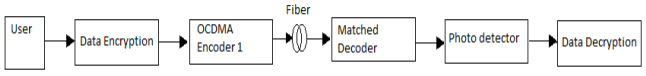

Fig-1: Block diagram of Cross layer security network

At the receiver, optical signal is decoded by a matched decoder for the user. Cross layer security network for secure optical transmission is designed with the help of Optisystem simulation software

2.1 Transmitter

The transmitter block designed in Optisystem is shown in Fig-2. The AES encrypted image is fed as input to User defined bit sequence generator by enabling load from file option. The AES encrypted data is then modulated by means of MZ modulator. The modulated signal is encoded by optical encoder using optical orthogonal code {1,13,25,40,53}. The delays introduced to encode the signal are 3 ps, 18 ps, 33 ps, 51.7 ps, 68 ps,

respectively. The signal is then modulated by optical amplifier and then transmitted via an optical fiber.

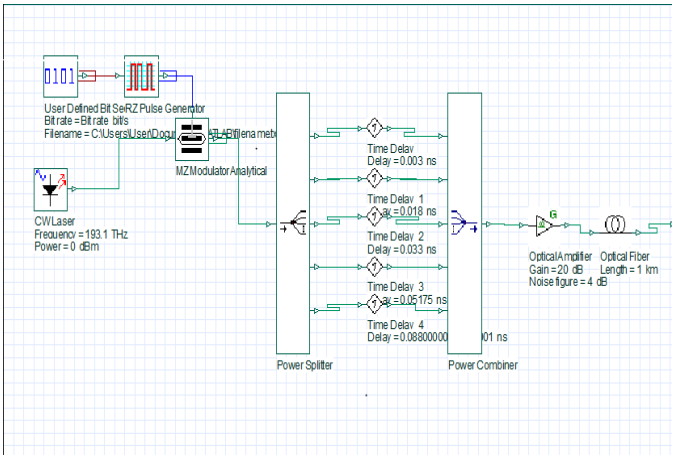

Fig -2: Transmitter of cross layer security network

2.2 Receiver

At the receiver, optical signal is decoded by a matched decoder for the user. The relative delays of the decoder are 97 ps, 82 ps, 67 ps, 48.3 ps and 32 ps respectively.

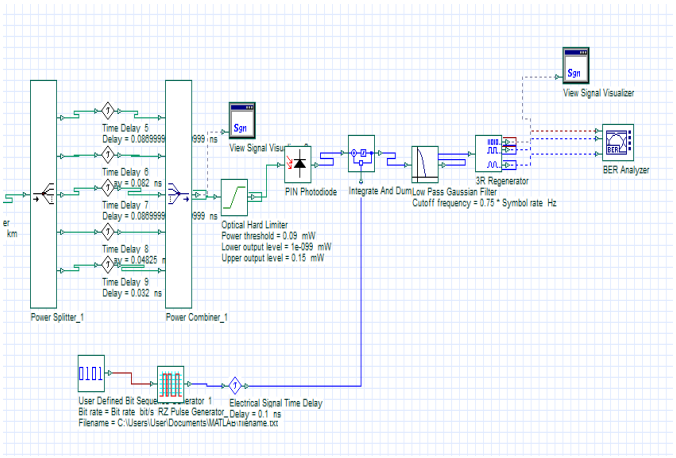

Fig 3: Receiver of cross layer security network

3. RESULTS AND DISCUSSION

3.1 Encryption

The encryption is performed at both physical layer and data layer of optical network. Fig -4 depicts the original image transmitted via optical fiber.

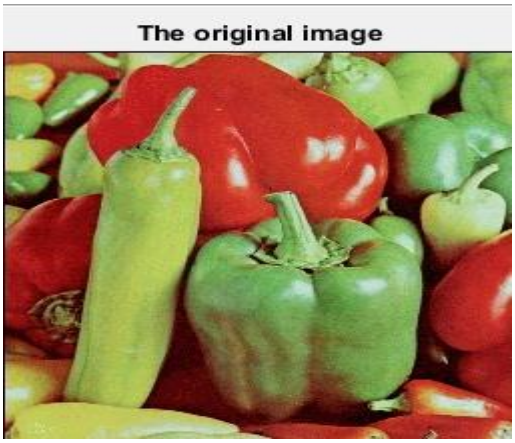

Fig -4: Original image

The transmitted image is first AES encrypted to enhance data layer security. Fig -5 depicts the AES encrypted image which is load as input to user defined bit sequence. The AES data is again encrypted by means of optical delay lines which acts as optical encoder which enhance the security at physical layer. Fig -6 a depicts the encrypted image received at the end of receiver.

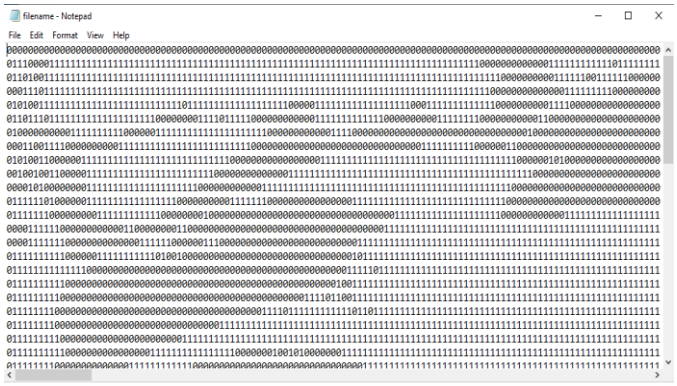

Fig-5: AES encrypted image

3.2 Decryption

The signal is collected via view signal visualizer and again decrypted with correct decoder to retrieve the original image. Fig -6b depicts corresponding decrypted image

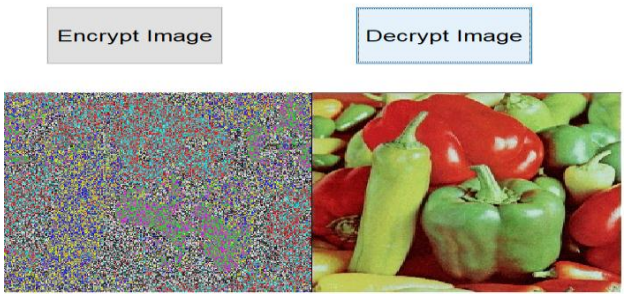

Fig -6 a)Encrypted image b)Decrypted image

3. CONCLUSION

Cross layer security network enhance the security at both physical layer and data layer. The transmitted image is retrieved at the receiver only user use correct decryption algorithm and correct decoder that exactly matches the encryption algorithm and encoder at the transmitter side. It enhance the security and it is impossible for the eavesdropper to eavesdrop the signal. The future scope of this paper to introduce different encoding schemes to improve the security further.

REFERENCES

[1] Jianhua ji, wenjun li, bing wu, ke wang, ming xu, lu sun, " Design and Investigation on Image Transmission in Multi-user Cross-Layer Security Network", IEEE access, vol. 7, pp. 132066-132073, 2019.

[2] Masahide sasaki, mikio fujiwara et al, "quantum photonic network: concept, basic tools, and future issues", IEEE journal of selected topics in quantum electronics, 21(3): 6400313, 2015.

[3] A. Stok, E. H. Sargent, "The role of optical CDMA in access networks", IEEE Communications Magazine, 40(9): 83–87, 2002.

[4] Zhenxing Wang, Chang J, Prucnal P.R, "Theoretical Analysis and Experimental Investigation on the Confidentiality of 2-D Incoherent Optical CDMA System", Journal of Lightwave Technology, 28(12): 1761-1769, 2010.

[5] Zhenxing Wang, Lei Xu, Chang J, Ting Wang, Prucnal P.R, "Secure Optical Transmission in a Point-to-Point Link With Encrypted CDMA Codes", IEEE Photonics Technology Letters, 22(19): 1410 – 1412, 2010.

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

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

[8] J. Ji, G. Zhang, W. Li, et al, "Performance analysis of physical-layer security in an OCDMA-based wiretap channel", IEEE/OSA J. Opt. Commun. Netw, 9(10): 813-818, 2017.

[9] Jianhua J, Xuemei C et al, "Performance analysis of FSO/CDMA system based on binary symmetric wiretap channel" , IET Communications. 13(1),116-123, 2018.

[10] Jianhua Ji, Qian Huang, Xuemei Chen, Lu Sun, "Performance Analysis and Experimental Investigation of Physical-Layer Security in OCDMA-Based Hybrid FSO/Fiber Wiretap Channel", IEEE Photonics Journal, 11(3), 7903420, 2019.

[11] Z. Jiang, D. E. Leaird, A. M. Weiner, "Experimental investigation of security issues in O-CDMA" ,Journal of Lightwave Technology, 24(11): 4228–4234, 2006.

[12] GleskI , Huang Y K , Camille S. Bres, et al, "Design and demonstration of a novel optical CDMA platform for use in avionics applications", Optics Communications, 271(1):65-70, 2007.

[13] N. Kostinski, K. Kravtsov, and P. R. Prucnal, "Demonstration of an All-Optical OCDMA Encryption and Decryption System With Variable Two-Code Keying", IEEE Photonics Technology Letters, 20(24): 2045–2047, 2008.

[14] Z. Wang, Y.-K. Huang, Y. Deng, J. Chang, P. R. Prucnal, "Optical Encryption With OCDMA Code Swapping Using All-Optical xor Logic Gate", IEEE Photonics Technology Letters, 21(7): 411–413, 2009.

[15] De Canniere C, Biryukov A, Preneel B, "An Introduction to Block Cipher Cryptanalysis", Proceedings of the IEEE, 94(2): 346–356, 2006.

[16] Wenjun Li, Jianhua Ji, Guirong Zhang, Wenlin Zhang, "Crosslayer security based on optical CDMA and algorithmic cryptography", IEEE Optoelectronics Global Conference,1-2, 2016.

[17] P. A. Humblet, M. Azizoglu, "On the bit error rate of lightwave systems with optical amplifiers" ,Journal of Lightwave Technology, 9(11): 1576-1582, 1991.

[18] Biryukov A, Grobschadl J, "Cryptanalysis of the Full AES Using GPU-Like Special-Purpose Hardware. Fundamental Informaticae", 2011(3-4):710,2012.

[19] Simarpreet Kaur, Simranjit Singh, "Security Enhancement of 2-D DIM Codes using 4 x 1NOR Logic based on FISO", Optical and Quantum Electronics,53, Article number: 434 (2021)

[20] Valarmathimarudhai, Shanthi Prince, Shayna Kumari, "Design and Simulation of Physical Layer Security for Next Generation Intelligent Optical Networks", research review, preview article.