Received August 21, 2019, accepted August 31, 2019, date of publication September 9, 2019,
date of current version September 25, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2940057

Design and Investigation on Image Transmission in Multi-User Cross-Layer Security Network

JIANHUA JI[1], WENJUN LI[2], BING WU[1], KE WANG[1], MING XU[1], AND LU SUN[3]

[1]Shenzhen Key Laboratory of Communication and Information Processing, College of Electronics and Information Engineering, Shenzhen University, Shenzhen 518060, China
[2]China Mobile International Company, Shenzhen 518060, China
[3]School of Electronics, Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

Corresponding author: Bing Wu (wb799475497@foxmail.com)

This work was supported in part by the NSFC under Grant 61671306, and in part by the Fundamental Research Project of Shenzhen under Grant 20160328145357990.

ABSTRACT A multi-user cross-layer security network based on optical code division multiple access (OCDMA) and algorithmic cryptography is proposed, and its security performance is analyzed quantitatively for the first time. In this scheme, eavesdroppers have to not only intercept the optical code of OCDMA in physical-layer, but also break the algorithmic cryptography in data-layer. Thus, the information security will be enhanced effectively. Synchronous transmission system and asynchronous transmission system are analyzed respectively. It can be seen that the cross-layer security of asynchronous transmission is far greater than that of synchronous transmission when the number of users is large enough. OptiSystem simulation is used to investigate the image transmission in cross-layer security system. The transmission distance of single mode fiber is 100 km, and transmission rates are 10 Gbit/s and 1 Gbit/s respectively. It can be seen that legitimate user can recover original image correctly with matched decoder and correct encryption algorithm. However, eavesdroppers cannot recover the image correctly with matched decoder/wrong encryption algorithm or unmatched decoder/correct encryption algorithm. Therefore, our scheme can greatly enhance the security of image transmission system.

INDEX TERMS Image transmission, image processing, cross-layer security network, optical code division multiple access, algorithmic cryptography, physical-layer security.

I. INTRODUCTION

Fiber-optic networks have been employed in commercial and military communication system for image transmission. The issue of security is important in fiber-optic networks due to the huge sensitive information. As a result, there are three types of security schemes including quantum key distribution (QKD), algorithmic cryptography and physical-layer cryptography [1]. Algorithmic cryptography is implemented in Layer 3 or the upper layers. However, its security is not entirely free from constant threats. For example, it is reported that the 768-bit RSA cryptosystem was broken in December 2009. The speed and distance of QKD are the price for realizing the unconditional security. The maximum key generation rate at present is around 1 Mb/s. Physical-layer cryptography can be an intermediate scheme with provable security, and has recently received more and more attention as an additional security layer in transmission systems. Optical code division multiple access (OCDMA) has been considered as a good candidate to provide physical-layer security [2]–[4]. Quantitative analysis of data confidentiality for OCDMA encoding can be evaluated as a function of several parameters, including signal-to-noise ratio (SNR) and fraction of total available system capacity [5],[6]. The physical-layer security of OCDMA-based optical fiber communication system is analyzed in [7], and the authors use security leakage factor to evaluate the physical-layer security level. By establishing the eavesdropping model of the FSO/CDMA wiretap channel, the performance of physical-layer security and reliability are evaluated simultaneously in [8]. OCDMA based hybrid FSO/fiber wiretap channel is proposed in [9], and the physical-layer security is analyzed theoretically, using the conditional secrecy outage probability as the performance metric.

However, with the development of detecting technology, an eavesdropper (Eve) could use some strategies to eavesdrop

The associate editor coordinating the review of this manuscript and approving it for publication was Guitao Cao.

on an optical fiber, such as energy detection, differential detection and code interception. Those strategies can threaten the inherent security of OCDMA. For example, in conventional on-off keying (OOK) OCDMA, data bits can be easily recovered by Eve using a simple energy detector in the uplink side of a user, since the energy levels of bit "1" and "0" are different and can be easily distinguished by a photodetector, without the use of optical decoders [10]. OCDMA can adopt two code-keying, which uses two different codes to represent bit "1" and "0" respectively, making the energy levels equal for all bits [11]–[13]. However, differential detection can be used to recover user data in this scheme.

As for data-layer security, algorithmic cryptography is one of the most widely used data-layer security methods. Cryptanalysis is defined as the process of attempting to find a shortcut method–not envisioned by the designer–for decrypting an enciphered message when the key used to encrypt the message is not known [14]. The methods of cryptanalysis used are the chosen-plaintext attack, known-plaintext attack, and ciphertext-only attack. The chosen-plaintext attack allows a choice of which messages the cryptanalyst can encrypt under the unknown secret key. The known-plaintext attack limits the messages to whatever plaintext and corresponding ciphertext the cryptanalyst can gather. Both of them are to find the key because the plaintext is known. The ciphertext-only attack requires the least difficult form of data collection, and the primary goal of this attack is to determine the plaintext because no plaintext is available to the cryptanalyst.

Although there are many complex methods being used for security analysis of physical-layer and data-layer respectively, few papers present any quantitative analysis of the degree of security that can be expected from cross-layer security which combines physical-layer security with data-layer security. We introduce a single-user optical communication system with cross-layer security in [15], which can enhance the security performance. However, for single-user OCDMA system, Eve can recover user data directly by energy detection without an optical decoder, so the physical-layer security of the system does not exist.

In this paper, for the first time, we propose and investigate a multi-user cross-layer security scheme based on OCDMA and algorithmic cryptography. It then presents a detailed theoretical evaluation of cross-layer security that is provided by certain types of OCDMA and algorithmic cryptography. This evaluation includes quantitative results on the degree of confidentiality. The degree of confidentiality obtainable by cross-layer security scheme is also compared with the degree of confidentiality in algorithmic cryptography. Simulation results show that, to recover the image correctly, Eve has to not only intercept the OCDMA code in the physical-layer, but also break the encryption algorithm in the data-layer. Hence, our scheme can enhance the security of image transmission system greatly.

The rest of this paper is organized as follows. In Section II, we introduce our system model of multi-user cross-layer network based on OCDMA and Advanced Encryption Standard (AES). In Section III, we analyze the security performance of multi-user cross-layer network under synchronous transmission and asynchronous transmission respectively. In Section IV, secure image transmission in cross-layer security system is simulated by OptiSystem. The paper concludes in Section V.

II. SYSTEM MODEL

Fig.1 shows the system model of multi-user cross-layer security network based on OCDMA and algorithmic cryptography. Legitimate users Alice and Bob transmit images securely through optical fibers, and Eve uses known-plaintext attack to eavesdrop on information. In the transmitter, the user's data is first encrypted by AES in the data-layer. After that, the physical-layer encryption is implemented by optical encoder. At the receiver, after the corresponding optical decoding process, Bob uses the decryption algorithm to recover data.

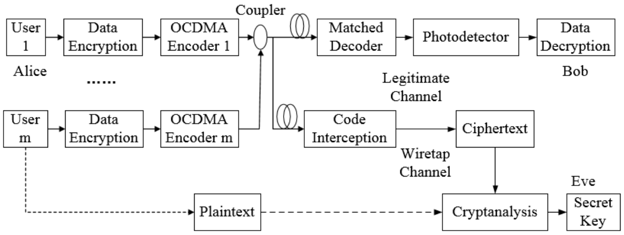


FIGURE 1. System model of cross-layer security network.

In this scheme, we can employ any type of optical encoder and optical code, such as time-spreading code, time spreading/wavelength hopping code, spectral amplitude code, spectral phase code and time phase code. For example, if we use time-spreading code, one-dimensional optical encoder can be constructed by couplers and optical delay lines (ODL). Encoder is implemented by connecting ODLs of different lengths with different ports of couplers. At the decoder, the delay of each port is complementary to the delay of the corresponding port of the encoder.

If Eve can detect the single-user signal, code interception can be performed to detect the optical code [5], [6]. The probability that Eve can detect the user's entire code with no errors is denoted by P_C. It can be calculated from two quantities (i.e. the probability of missing a transmitted pulse in a given time bin, P_M, and the probability of falsely detecting a pulse in a bin where none was transmitted, P_{FA}). The overall probability of error-free code detection is given by

$$P_C = (1 - P_M)^W \, (1 - P_{FA})^{(L \times \lambda - W)} \tag{1}$$

where W is the code weight, L is the code length, λ is the number of wavelengths. P_M and P_{FA} are determined by the SNR at Eve and by the eavesdropping detectors performance in noise.

$$P_M = 1 - Q\left(\sqrt{2E/N}, \sqrt{2\gamma/N}\right) \tag{2}$$

$$P_{FA} = \exp\left(-\frac{\gamma}{N}\right) \tag{3}$$

where E/N is the ratio of the peak pulse energy to the noise power spectral density, γ is the detection threshold [16], and *Q(a, b)* is the Marcum Q-function defined as

$$Q(a,b) = \int_b^\infty x I_0(ax) \exp\left(-\frac{x^2+a^2}{2}\right) dx \tag{4}$$

where $I_0(x)$ denotes a zeroth order modified Bessel function of the first kind.

Linear cryptanalysis method is essentially a known-plaintext attack that utilizes the output ciphertexts [17]. If Eve uses linear cryptanalysis method to attack the AES of cross-layer security system, Eve has to intercept the OCDMA code to get the output ciphertexts. Hence, the expected time complexity of cross-layer security system against Eve is given by

$$\bar{T} = \sum_{n=1}^{\infty} n\,(T_e + T_i) P_{cin} \tag{5}$$

Here, T_e is the time required to operate the encryption on AES once. T_i is the time required to intercept the entire code once. P_{cin} is the probability that Eve correctly detects the user's code till the *n-th* code interception.

$$P_{cin} = (1 - P_C)^{n-1} P_C \tag{6}$$

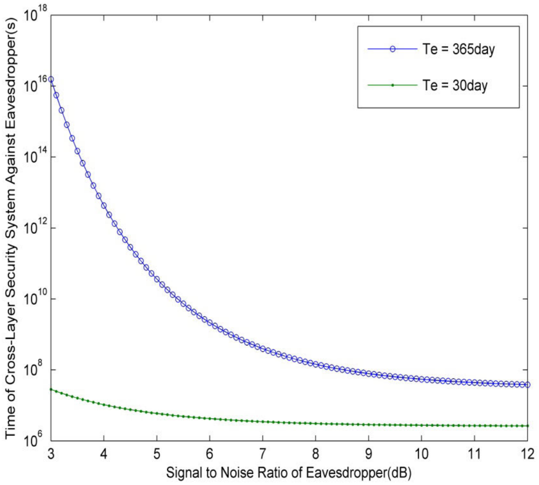


FIGURE 2. Relationship of cross-layer security with SNR.

Fig.2 shows the relationship between the expected time complexity of cross-layer security system and the SNR of Eve. Here, we use the optical orthogonal code (80,5,2,1) and $T_i = 60s$. Optical orthogonal code can be represented as $(n, w, \lambda_a, \lambda_b)$, where n is the code length, w is the code weight, λ_a is the maximum value of shifted auto-correlation and λ_b is the maximum value of cross-correlation. It can be seen that with the increase of SNR, the expected time complexity of cross-layer security system for Eve decreases gradually and tends to be stable. Under the same SNR, the security of the system will be higher if the code interception time is longer.

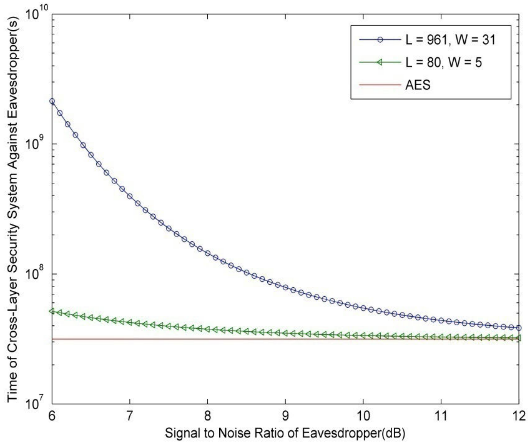


FIGURE 3. Security performance with different codes.

Fig.3 shows the expected time complexity with different codes. The straight line represents AES security. The other two curves represent the cross-layer security with prime code (961,31,30,2) and optical orthogonal code (80,5,2,1) respectively. With the decrease of SNR of Eve, the expected time complexity of cross-layer security system for Eve is also increasing. Meanwhile, the expected time complexity of prime code (961,31,30,2) increases faster than that of optical orthogonal code (80, 5, 2, 1). Hence, the complex code can improve cross-layer security. Especially in the case of low SNR, the cross-layer security is much higher than the algorithmic cryptography security.

III. CROSS-LAYER SECURITY WITH MULTIPLE USERS

In multi-user cross-layer security system, Eve must be forced to detect multiple signals simultaneously. We consider two transmission schemes: synchronous system and asynchronous system.

A. SYNCHRONOUS SYSTEM

Considering N simultaneous users, each of which is OCDMA encoded and modulated using OOK. Each user operates at data rate D bits/s, and all users transmit synchronously. In this case, the probability that a specific user transmits "1" during a given bit period is 1/2, and the probability that all $N-1$ users transmit "0" during the same bit period is $1/2^{N-1}$. Assuming that the value of each data bit is independent of other data bits and independent of other users' data bits, the probability that one user transmits "1" while all other users transmit "0" during a given bit period is $N/2^N$. Therefore, the expected amount of time that Eve must wait for single-user transmission is $2^N/(D \times N)$.

When Eve can detect the single-user transmission, code interception can be used to break the user's optical code. Employing the intercepted code, Eve can decode the received signal, and the information of ciphertexts can be obtained. Finally, Eve can access the information according to the prescribed ciphertexts, and then decipher the key of the encryption algorithm. In this case, the expected value of the time for

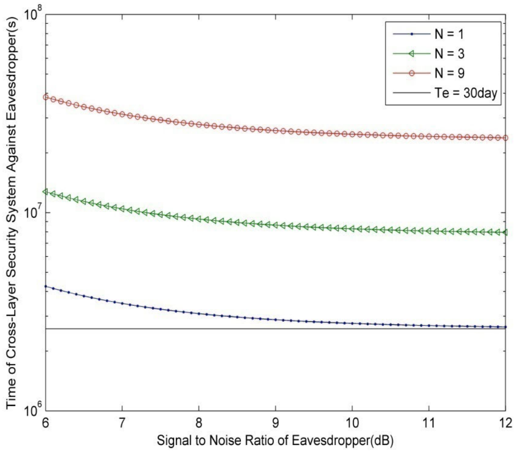


FIGURE 4. **Performance of cross-layer security with different users (synchronous system).**

Eve to successfully break the cross-layer security system is

$$\bar{T}_s = \sum_{n=1}^{\infty} n\left(T_e + T_o + \frac{2^N}{D \times N}\right) P_{cn} \tag{7}$$

Here, T_e is the required time for Eve to successfully attack the encryption algorithm. T_o is the required time for Eve to successfully intercept the address code. P_{cn} is the probability that Eve correctly detects the user's code till the *n-th* interception.

$$P_{cn} = \frac{(1 - P_C \,/\, N)^{n-1}\, P_C}{N} \tag{8}$$

Performance of cross-layer security with different users (synchronous system) is shown in Fig.4. Here, $T_o = 60$ s, data rate is 1 Gbit/s. The straight line represents AES security. It can be seen from Fig.4 that, the security performance of cross-layer security decreases with the increase of the SNR of Eve. When the SNR is greater than 11 dB, the security of the system is almost unchanged. Moreover, in the case of the same SNR, the cross-layer security will be enhanced with the increase of the number of simultaneous users.

B. ASYNCHRONOUS SYSTEM

In this case, when one user transmits "1," all other $N - 1$ users may transmit fraction of two consecutive bits during the transmission time of the "1" bit period. For Eve to isolate a single user, the other $N - 1$ users must transmit two consecutive "0" during the period of overlap with the single user's "1" bit. The probability that a specific user transmits "1" during a given bit period is 1/2, and the probability that all $N - 1$ users transmits "0" for the two overlapping bits is $1/2^{2N-2}$. Therefore, the expected amount of time that Eve must wait for single user transmission is $2^{2N-1}/(D \times N)$.

The expected value of the time for Eve to successfully break the cross-layer security system is

$$\bar{T}_a = \sum_{n=1}^{\infty} n\left(T_e + T_o + \frac{2^{2N-1}}{D \times N}\right) P_{cn} \tag{9}$$

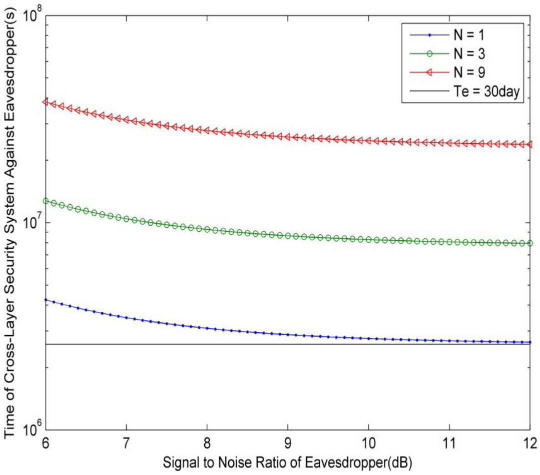


FIGURE 5. **Performance of cross-layer security with different users (asynchronous system).**

Performance of cross-layer security with different users (asynchronous system) is shown in Fig.5. Also, the straight line represents AES security. It can be seen that, the security performance of the cross-layer security decreases with the increase of the SNR of Eve. When the SNR is greater than 11 dB, the security of the system is almost unchanged. In addition, in the case of the same SNR, the cross-layer security is higher with the increase of the number of users.

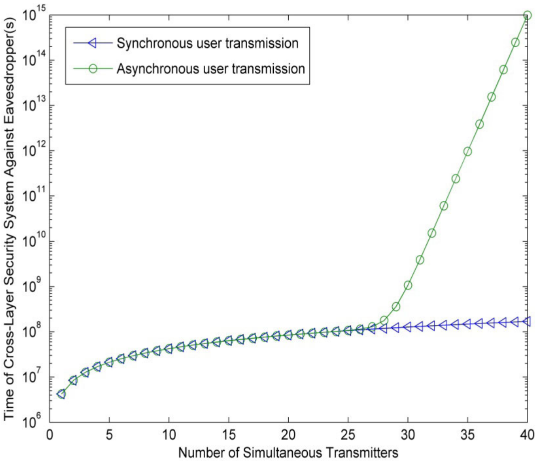


FIGURE 6. **Comparison of cross-layer security performance between synchronous system and asynchronous system (SNR = 6 dB).**

Fig.6 shows the comparison of cross-layer security performance between synchronous system and asynchronous system ($SNR = 6$ dB, $T_e = 60$ minutes). As can be seen from Fig.6, when the number of users is less than 26, the cross-layer security of synchronous transmission is almost the same as that of asynchronous transmission. However, when the number of users is greater than 26, the cross-layer security of synchronous transmission system still increases slowly with the number of users, but the cross-layer security of asynchronous transmission system security increases greatly.

The reason is that when the number of users is small, there is no significant difference in the expected time of isolating a single user between synchronous transmission system and asynchronous transmission system. However, when the number of users is large enough, the expected time to isolate a single user in the asynchronous transmission system is much larger than that of the synchronous transmission system.

IV. SIMULATION AND DISCUSSION

In some cases, if Eve can't detect the number of simultaneous users, code interception should be implemented during each bit period. For a synchronous transmission system, the probability that Eve correctly detects the user's code till the *n-th* interception is

$$P_{cns} = \frac{\left(1 - P_C / 2^N\right)^{n-1} P_C}{2^N} \tag{10}$$

For an asynchronous transmission system, the probability that Eve correctly detects the user's code till the *n-th* interception is

$$P_{cna} = \frac{\left(1 - P_C / 2^{2N-1}\right)^{n-1} P_C}{2^{2N-1}} \tag{11}$$

According to Equations (5), (10), (11), the expected time complexity of cross-layer security system against Eve can be evaluated for the synchronous system and asynchronous system respectively.

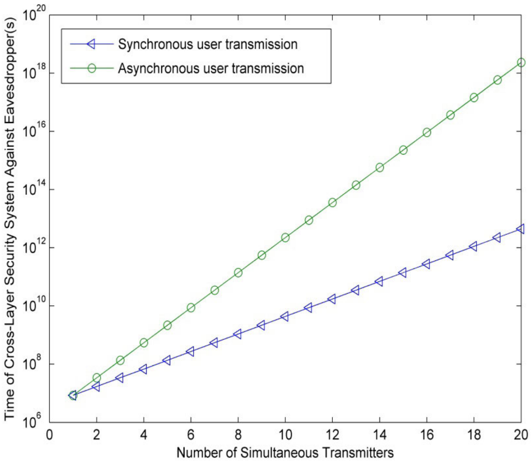


FIGURE 7. Comparison of cross-layer security performance without detecting the number of users (SNR = 6 dB).

Fig.7 shows the comparison of the cross-layer security performance between synchronous system and asynchronous system (SNR = 6 dB), where Eve can't detect the number of simultaneous users. As can be seen from Fig.7, the cross-layer security is proportional to the number of users, and the cross-layer security of asynchronous transmission is greater than that of synchronous transmission. Furthermore, the cross-layer security will be degraded if Eve can detect the number of simultaneous users, as shown in Fig. 8.

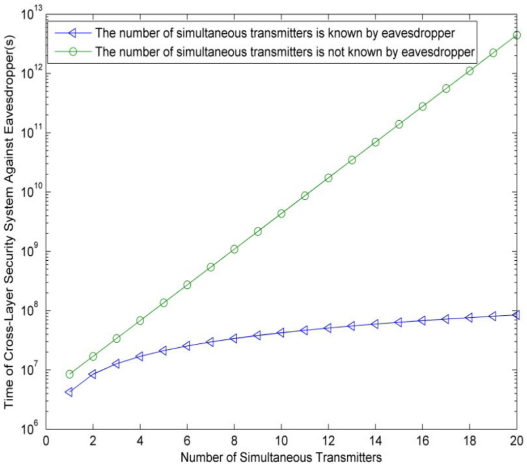
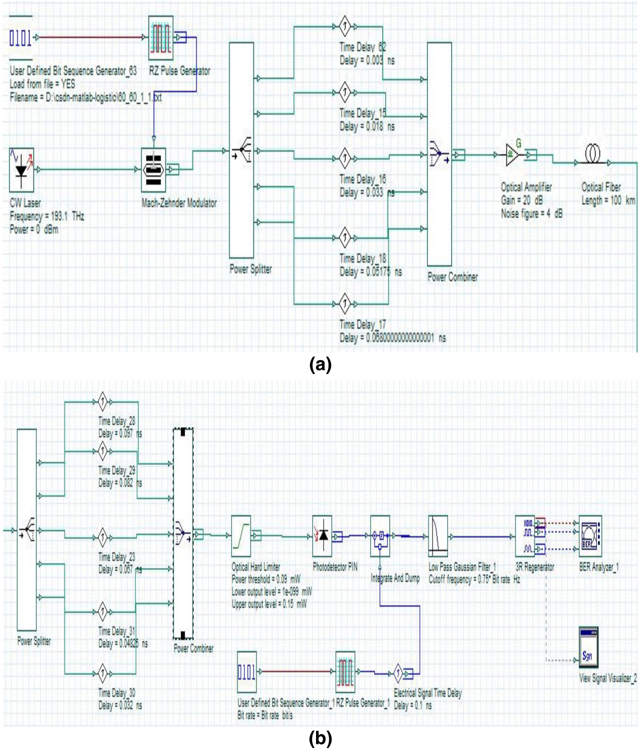


FIGURE 8. Comparison of cross-layer security performance w/o detecting the number of users (SNR = 6 dB, synchronous transmission).



(a)

(b)

FIGURE 9. OptiSystem simulation of cross-layer security system. (a)Transmitter. (b) Receiver.

Image transmission has been widely applied for image processing [18]–[21]. Next, OptiSystem is employed to simulate the image transmission in the cross-layer security system, as shown in Fig.9. ODLs are used to construct the optical encoder/decoder with the optical orthogonal code. Code length is 80 and code weight is 5. At the transmitter, user data is encrypted by AES, and then OOK modulated by 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

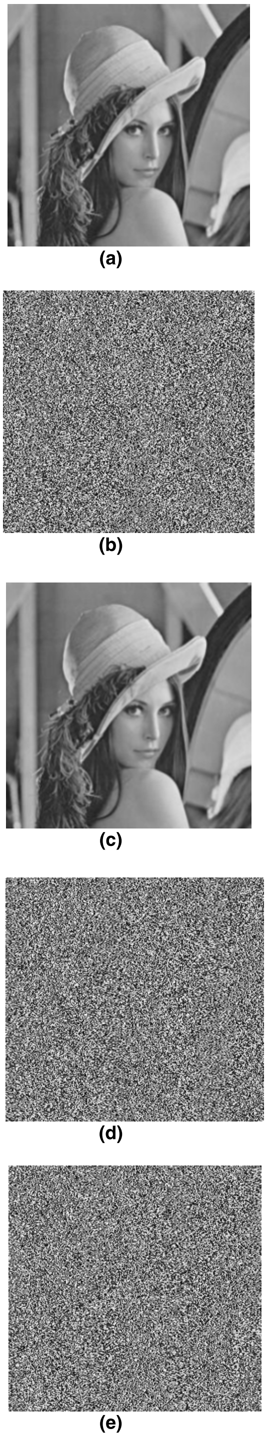


FIGURE 10. Image transmission of cross-layer security system. (a) Original image (b) image after data encryption (c) matched decoder/ correct AES (d) matched decoder/wrong AES (e)unmatched decoder/ correct AES.

optical orthogonal code {1,13,25,40,53}. The relative delays of encoder are 3 ps, 18 ps, 33 ps, 51.7 ps, 68 ps, respectively.

Then, the signal is amplified by an erbium doped fiber amplifier (EDFA) and transmits through a 100 km single mode fiber link. The dispersion compensation fiber (DCF) is used to compensate for the fiber dispersion. At the receiver, optical signal is decoded by a matched decoder for the legitimate user. The relative delays of the decoder are 97 ps, 82 ps, 67 ps, 48.3 ps and 32 ps respectively.

According to *Kerckhoffs*'s principle, Eve knows what types of OCDMA signals are being sent, but does not know the optical code of the legitimate user. Hence, we assume that the optical code of the legitimate user should not be available for Eve. Therefore, Eve can employ unmatched optical decoder. Then, decoded signal is recovered by the photodetector and decrypted by AES.

Fig.10 shows that when Eve attacks a cross-layer security communication system, Eve can successfully crack the system only after successfully intercepting the OCDMA code and deciphering the key of the encryption algorithm simultaneously. However, Eve cannot recover the image correctly with the matched decoder/wrong AES encryption algorithm or the unmatched decoder/correct AES encryption algorithm. Hence, this scheme can enhance the security performance of the image transmission system.

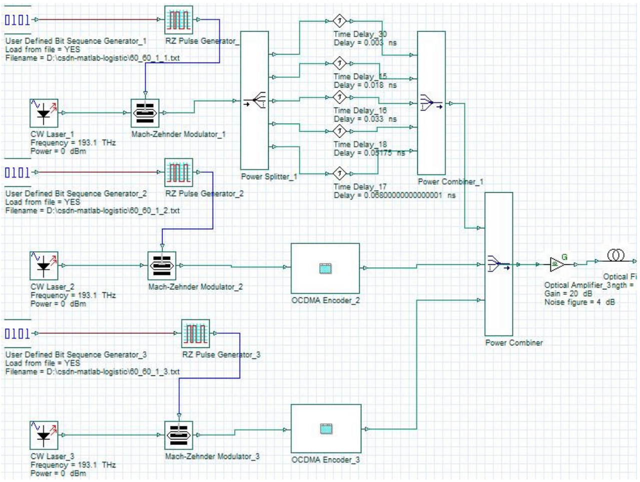
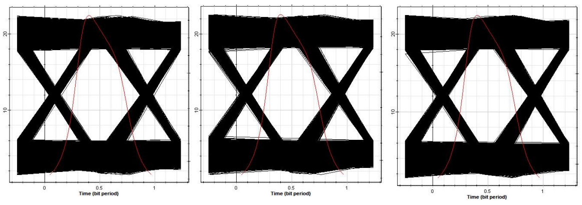


FIGURE 11. Cross-layer security system with three users.

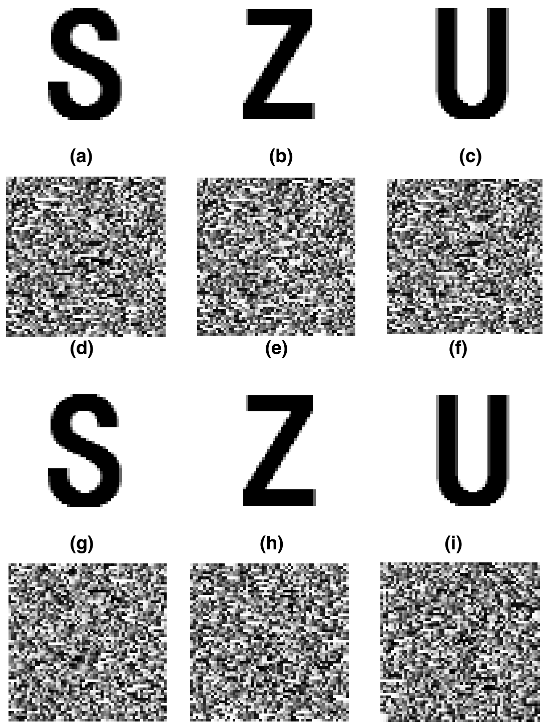
Fig.11 shows the cross-layer security system with three users. Each user employs different optical encoders with optical orthogonal codes {1,13,25,40,53},{1,11,21,32,43} and {1,9,17,26,35} respectively. The delay settings of the optical encoder are similar to those of Fig.9. The transmission rate is 1 Gbit/s and the transmission distance of single mode fiber is 100 km. Fig.12 shows eye diagrams of three users at the receiver. It can be seen that the encrypted images are error-free transmitted in the physical-layer of multi-user cross-layer security system.

Fig.13 shows the image transmission of three-user cross-layer security system. In Fig.13, (a), (b) and (c) are three original images for three users, and (d), (e) and (f) are three images after encryption respectively. It can be seen that legitimate users can recover images correctly with matched decoder and correct AES encryption algorithm, as shown in (g), (h) and (i). However, as shown in (j) and (k), Eve cannot recover user data correctly with matched decoder/wrong



(a) (b) (c)

FIGURE 12. Eye diagrams of users. (a) User 1 (b) user 2 (c) user 3.



(a) (b) (c) (d) (e) (f) (g) (h) (i) (j) (k) (l)

FIGURE 13. Image transmission of three-user cross-layer security system. (a) Original image 1 (b) original image 2 (c) original image 3 (d) image 1 after encryption (e) image 2 after encryption (f) image 3 after encryption (g) matched decoder 1/ correct AES (h) matched decoder 2/ correct AES (i) matched decoder 3/ correct AES (j) matched decoder 1/ wrong AES (k) unmatched decoder 1/ correct AES (l) energy detection 2, correct AES.

AES encryption algorithm or unmatched decoder/correct AES encryption algorithm. On the other hand, as shown in (1), Eve cannot recover user data correctly with energy detection, which can also enhance the physical-layer security. Therefore, our scheme can enhance the security of image transmission system greatly.

V. CONCLUSION

In this paper, we introduce a multi-user cross-layer security system that combines the OCDMA with algorithmic cryptography. In this system, Eve has to not only intercept the optical code of OCDMA in physical-layer, but also break the algorithmic cryptography in data-layer. It can be seen that our scheme can improve the image confidentiality of the optical networks. Furthermore, under the large number of simultaneous users, the cross-layer security of asynchronous transmission is far greater than that of synchronous transmission. OptiSystem simulation is investigated on the secure image transmission over 100 km single mode fiber. It can be seen that Eve can recover images only when the matched decoder and the correct encryption algorithm are used simultaneously. Therefore, the multi-user cross-layer security system proposed in this paper can be a good candidate for secure image transmission systems.

For cross-layer security system, how to achieve more in-depth cross-layer security convergence will be one of the future research directions. In addition, the security performance evaluation of cross-layer security system is also worth studying. In the future research, we will experimentally study image transmission in cross-layer security system.

REFERENCES

[1] M. Sasaki, M. Fujiwara, R.-B. Jin, M. Takeoka, T. S. Han, H. Endo, K.-I. Yoshino, T. Ochi, S. Asami, and A. Tajima, "Quantum photonic network: Concept, basic tools, and future issues," *IEEE J. Sel. Topics Quantum Electron.*, vol. 21, no. 3, May/Jun. 2015, Art. no. 6400313.

[2] A. Stok and E. H. Sargent, "The role of optical CDMA in access networks," *IEEE Commun. Mag.*, vol. 40, no. 9, pp. 83–87, Sep. 2002.

[3] W. C. J. Zhenxing and P. R. Prucnal, "Theoretical analysis and experimental investigation on the confidentiality of 2-D incoherent optical CDMA system," *J. Lightw. Technol.*, vol. 28, no. 12, pp. 1761–1769, Jun. 15, 2010.

[4] Z. Wang, L. Xu, J. Chang, T. Wang, and P. R. Prucnal, "Secure optical transmission in a point-to-point link with encrypted CDMA codes," *IEEE Photon. Technol. Lett.*, vol. 22, no. 19, pp. 1410–1412, Oct. 1, 2010.

[5] T. H. Shake, "Confidentiality performance of spectral-phase-encoded optical CDMA," *J. Lightw. Technol.*, vol. 23, no. 4, pp. 1652–1663, Apr. 2005.

[6] T. H. Shake, "Security performance of optical CDMA Against eavesdropping," *J. Lightw. Technol.*, vol. 23, no. 2, pp. 655–670, Feb. 2005.

[7] J. Ji, G. Zhang, W. Li, L. Sun, K. Wang, and M. Xu, "Performance analysis of physical-layer security in an OCDMA-based wiretap channel," *J. Opt. Commun. Netw.*, vol. 9, no. 10, pp. 813–818, Oct. 2017.

[8] J. Ji, X. Chen, and Q. Huang, "Performance analysis of FSO/CDMA system based on binary symmetric wiretap channel," *IET Commun.*, vol. 13, no. 1, pp. 116–123, 2018.

[9] J. Ji, Q. Huang, X. Chen, and L. Sun, "Performance analysis and experimental investigation of physical-layer security in OCDMA-based hybrid FSO/fiber wiretap channel," *IEEE Photon. J.*, vol. 11, no. 3, Jun. 2019, Art. no. 7903420.

[10] Z. Jiang, D. E. Leaird, and A. M. Weiner, "Experimental investigation of security issues in O-CDMA," *J. Lightw. Technol.*, vol. 24, no. 11, pp. 4228–4234, Nov. 2006.

[11] I. Glesk, Y.-K. Wang, C.-S. Brès, and P. R. Prucnal, "Design and demonstration of a novel optical CDMA platform for avionics applications," *Opt. Commun.*, vol. 271, no. 1, pp. 65–70, 2007.

[12] N. Kostinski, K. Kravtsov, and P. R. Prucnal, "Demonstration of an all-optical OCDMA encryption and decryption system with variable two-code keying," *IEEE Photon. Technol. Lett.*, vol. 20, no. 24, pp. 2045–2047, Dec. 15, 2008.

[13] Z. Wang, Y.-K. Huang, Y. Deng, J. Chang, and P. R. Prucnal, "Optical encryption with OCDMA code swapping using all-optical XOR logic gate," *IEEE Photon. Technol. Lett.*, vol. 21, no. 7, pp. 411–413, Apr. 1, 2009.

[14] C. de Canniere, A. Biryukov, and B. Preneel, "An introduction to block cipher cryptanalysis," *Proc. IEEE*, vol. 94, no. 2, pp. 346–356, Feb. 2006.

[15] W. Li, J. Ji, G. Zhang, and W. Zhang, "Cross-layer security based on optical CDMA and algorithmic cryptography," in *Proc. IEEE Optoelectron. Global Conf.*, Sep. 2016, pp. 1–2.

[16] P. A. Humblet and M. Azizoglu, "On the bit error rate of lightwave systems with optical amplifiers," *J. Lightw. Technol.*, vol. 9, no. 11, pp. 1576–1582, Nov. 1991.

[17] A. Biryukov and J. Großschädl, ''Cryptanalysis of the full AES using GPU-like special-purpose hardware,'' *Fundam. Inform.*, vol. 114, nos. 3–4, pp. 221–237, 2012.

[18] W. Cao, Q. Lin, Z. He, and Z. He, ''Hybrid representation learning for cross-modal retrieval,'' *Neurocomputing*, vol. 35, pp. 45–57, Jun. 2019.

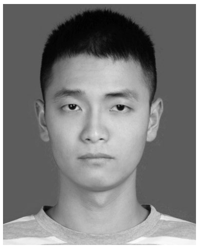
[19] R. Wang, Y. He, C. Huang, X. Wang, and W. Cao, ''A novel least-mean kurtosis adaptive filtering algorithm based on geometric algebra,'' *IEEE Access*, vol. 7, pp. 78298–78310, 2019.

[20] R. Wang, W. Zhang, Y. Shi, X. Wang, and W. Cao, ''GA-ORB: A new efficient feature extraction algorithm for multispectral images based on geometric algebra,'' *IEEE Access*, vol. 7, pp. 71235–71244, 2019.

[21] W. Cao, J. Yuan, Z. He, Z. Zhang, and Z. He, ''Fast deep neural networks with knowledge guided training and predicted regions of interests for real-time video object detection,'' *IEEE Access*, vol. 6, pp. 8990–8999, 2018.

JIANHUA JI was born in Jiangsu, China, in 1970. He received the Ph.D. degree from Shanghai Jiao Tong University, China. He is currently a Professor with the College of Electronics and Information Engineering, Shenzhen University. His research interests include optical fiber communication and free-space optical communication.

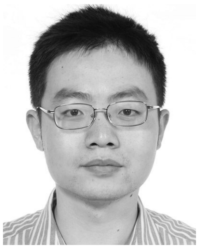
WENJUN LI graduated from Shenzhen University, in 2017. Since 2017, he has been a Senior Project Manager with China Mobile International Company. He takes charge of international telecommunication service and provides professional, high-quality, and full-scale transnational communication solutions for international operators and enterprises.



BING WU received the B.E. degree from the Anhui University of Technology, Anhui, China, in 2017, where he is currently pursuing the M.E. degree with the Shenzhen Key Laboratory of Communication and Information Processing, College of Electronics and Information Engineering. His research interests include optical fiber communication and free space optical.

KE WANG is currently pursuing the Ph.D. degree in optical engineering with Shenzhen University, where he is currently an Assistant Professor. He has published more than ten journal articles. His current research interests include optical fiber communication and 2D materials.

MING XU received the M.S. and Ph.D. degrees in physical electronics and optoelectronics from the University of Electronic Science and Technology of China, in 1998 and 2002, respectively. He is currently an Associate Professor with Shenzhen University, China. He is the author of more than 40 journal articles. His current research interests include photon coding and calculation, high-speed micro–nano photonic components, and next-generation communication switching networks.



LU SUN received the B.S. and Ph.D. degrees from Shanghai Jiao Tong University, Shanghai, China, in 2010 and 2016, respectively, where he is currently an Assistant Professor. His research interests include quantum electrodynamics, nano-optics, and 2D materials.