Opt Quant Electron (2018) 50:215
https://doi.org/10.1007/s11082-018-1481-5

Improvement of physical-layer security and reliability in coherent time-spreading OCDMA wiretap channel

Jianhua Ji[1] · **Guirong Zhang**[1] · **Ke Wang**[1] · **Ming Xu**[1]

Received: 13 December 2017 / Accepted: 24 April 2018 / Published online: 26 April 2018

Abstract Optical code division multiple access (OCDMA) can enhance the physical-layer security performance of optical fiber communication systems. In asynchronous coherent time-spreading OCDMA employing *m* sequence and Gold code, the reliability, capacity and physical-layer security of the system will degrade due to multiple access interference and beat noise. In order to enhance the physical-layer security and reliability of coherent OCDMA systems, a quasi-synchronous coherent time-spreading OCDMA wiretap channel is proposed in this paper. The influences of the extraction location, the extraction ratio, the number of active users on the physical-layer security are analyzed quantitatively. System performances are characterized by bit error rate, secrecy capacity as well as security leakage factor. The numerical results prove that the proposed scheme can improve the physical-layer security and reliability simultaneously.

Keywords Optical code division multiple access · Bit error rate · LA code · Secrecy capacity · Security leakage factor

1 Introduction

The issue of security is pivotal in fiber-optics network when it comes to huge amount of sensitive information. However, there are detrimental safety issues in fiber-optics transmission system, e.g., the eavesdropper (Eve) can get access to a small portion of optical signals by bending the optical fiber, which is not easy to be discovered by legitimate users (Shaneman and Gray 2004). At present, there are three types of security schemes including quantum key distribution (QKD), algorithmic cryptography and physical-layer cryptography. The traditional optical network security adopts data encryption of network upper layer protocol, and assumes that physical layer provides unblocked and error-free transmission. However, all

✉ Jianhua Ji
jjh@szu.edu.cn

[1] College of Information Engineering, Shenzhen University, Shenzhen 518060, China

algorithm-based encryption methods have been proven to be crackable (Zhou and Tang 2011). For example, it has been reported that the 768-bit RSA cryptosystem was broken in December 2009. QKD ensures the unconditional security in the sense that Eve can have unlimited physical abilities and computational power (Shields et al. 2012; Shimizu et al. 2014). The maximum key generation rate at present is around 1 Mb/s over a 50 km installed fiber (Sasaki et al. 2015). This performance, however, still falls short of the level for practical deployment in wide area public infrastructures. There is still a big gap between QKD and photonic network. Physical-layer cryptography can be an intermediate scheme to fill this gap (Jiang et al. 2006).

As an important merit of OCDMA technology, physical-layer security can improve the ability of optical fiber system to prevent eavesdropper from attack. Physical-layer security is measured by the probability that Eve could detect the user's entire code (Shake 2005a, b). In the case of brute-force search, code cardinality is usually used to analyze the physical-layer security of the system (Wang et al. 2010). In Leaird et al. (2005), the eavesdropper uses energy detection for code interception, and physical-layer security is evaluated by code interception time and eye diagram. Three types of secrecy capacities are analyzed in Tan et al. (2016). Secrecy capacity is the largest rate at which eavesdropper gains no information from the message. Therefore, legitimate users need to select the appropriate channel coding to achieve the secrecy capacity. However, if the transmitter chooses to communicate at the channel capacity, the secrecy capacity is not sufficient to evaluate physical-layer security. In Ji et al. (2017), the security leakage factor is used to evaluate the physical-layer security level. However, due to the multiple access interference (MAI) and beat noise, the reliability and capacity of the system will be reduced, as well as the physical-layer security.

To further enhance the physical-layer security and reliability of coherent OCDMA systems, a quasi-synchronous coherent time-spreading OCDMA wiretap channel employing LA code is proposed in this paper. The influences of the extraction location, the extraction ratio, the number of active users on the physical-layer security are analyzed quantitatively.

This paper is organized as follows. In Sect. 2, we will introduce the quasi-synchronous coherent OCDMA wiretap channel model. In Sect. 3, performance of the quasi-synchronous coherent OCDMA wiretap channel will be analyzed. In Sect. 4, we will discuss the results of this security performance. The conclusions are drawn in Sect. 5.

2 Quasi-synchronous coherent OCDMA wiretap channel model

LA code is a kind of $\{0, \pm 1\}$ sequence, which can be represented as LA (N, K, M). Here, N is the code length, K is the basic pulse number, and M is the length of the zero correlation zone (Fan et al. 1999). The normalized cross-correlation function of LA code is

$$C_{x,y}(\tau) = \begin{cases} 0 & 0 \le \tau \le \mathrm{M}-1 \\ \frac{1}{N} \sum_{i=0}^{N-1-\tau} a_{i-\tau}^{x} a_{i}^{y} & \mathrm{M} \le \tau < N-1 \end{cases}. \tag{1}$$

Here, $a_i^{x(y)} (i = 0, 1, \ldots, N-1)$ is the LA code for $x(y)$ users, and τ is the relative delay.

For LA (156, 8, 16), the length of is 156, the zero correlation zone is 16, and the code cardinality is 8. One of the basic LA codes is

$$a^1 = \Big\{ \underbrace{1,0,\ldots,0}_{16}, \underbrace{1,0,\ldots,0}_{17}, \underbrace{1,0,\ldots,0}_{18}, \underbrace{1,0,\ldots,0}_{20}, \underbrace{1,0,\ldots,0}_{19}, \underbrace{1,0,\ldots,0}_{22}, \underbrace{1,0,\ldots,0}_{23}, \underbrace{1,0,\ldots,0}_{21} \Big\}.$$

If the relative delays between all LA codes are within the zero correlation zone, i.e., quasi-synchronization, the value of the code cross-correlation is zero. Therefore, the influence of MAI and beat noise in coherent OCDMA can be eliminated.

Figure 1 shows the quasi-synchronous coherent OCDMA wiretap channel model based on LA code, where legitimate users (Alice) wants to send a message to another user (Bob). An eavesdropper (Eve) intends to obtain useful information at extraction location with an extraction ratio x. Quasi-synchronous coherent OCDMA uses on–off keying (OOK) modulation. The system has $k+1$ users, and each user data is encoded by different LA encoder. The relative delay between the users is controlled by the tunable optical delay line within the zero correlation zone. At the receiver, Bob will use matching decoder to decode the received optical signals, while Eve can only use non matching decoder. The receiver consists of an erbium-doped fiber amplifier (EDFA) with gain G and noise index F_n, an optical filter with bandwidth B_o, a p-i-n detector with responsivity R, and a low pass filter with an equivalent bandwidth B_e (San and Vo 2000). We assume all users have the same transmit power P (Decoded chip signal power). The optical signal power at the Bob's receiver is $P_S = (1-x)\frac{P}{10^{\alpha L/10}}$. Here, L is the total transmission distance of legitimate users, and α is the fiber attenuation coefficient. When the target user sends data "1" and "0", the received average signal power can be represented as $P_1 = P_S$, $P_0 = 0$.

Eve intends to obtain useful information at extraction location l with an extraction ratio x, and the signal power of extracting the target signal is $P_{Eve} = x\frac{P}{10^{\alpha l/10}}$. When Eve uses non matching decoder for decoding the optical signals, the cross-correlation peak of LA code is 1. Therefore, the received average optical power for data "1" is

$$P_{E1} = \xi k P_{Eve} + (1/K^2) P_{Eve}. \tag{2}$$

The received average optical power for data "0" is

$$P_{E0} = \xi k P_{Eve}. \tag{3}$$

Here, ξ is average normalized crosstalk value, i.e., $\xi \equiv \langle P_i \rangle / P_d$. P_i and P_d are the optical intensity of the decoded signal from inference users and targeted users.

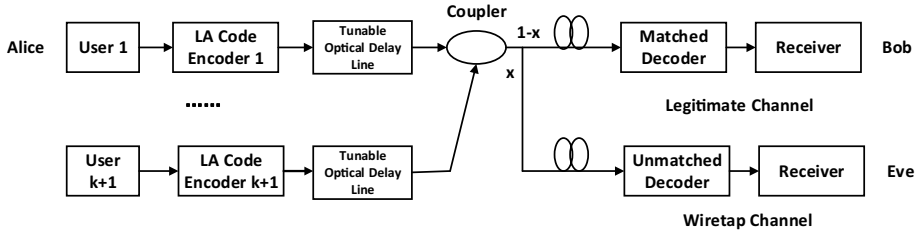

Fig. 1 Quasi-synchronous coherent OCDMA wiretap channel model based on LA code

3 Performance analysis

In quasi-synchronous coherent OCDMA wiretap channel, the relative delays between the users are controlled within the zero correlation zone of the LA code. Therefore, for legitimate user, the cross-correlation values are 0, and MAI and beat noise can be completely eliminated.

When the signal passes through the photodiode, the mixing of the target signal with the interfering signal causes signal-spontaneous beat noise σ_{s-sp}, and spontaneous–spontaneous beat noise σ_{sp-sp}. The shot noise σ_{sh}, thermal noise σ_{th} and dark current noise σ_{d} will also be considered here.

Hence, for legitimate user, the total noise variance for data "1" is

$$\sigma_1^2 = \sigma_{sh1}^2 + \sigma_{s-sp1}^2 + \sigma_{sp-sp}^2 + \sigma_{th}^2 + \sigma_d^2 . \tag{4}$$

The total noise variance for data "0" is

$$\sigma_0^2 = \sigma_{sh0}^2 + \sigma_{s-sp0}^2 + \sigma_{sp-sp}^2 + \sigma_{th}^2 + \sigma_d^2 \tag{5}$$

where $\sigma_{sh1}^2 = 2e\left\{RG\,P_1 + R\,F_{\mathrm{n}}\,h\nu(G-1)\,B_0\right\}B_e$, $\sigma_{sh0}^2 = 2e\left\{RG\,P_0 + R\,F_{\mathrm{n}}\,h\nu(G-1)\,B_0\right\}B_e$, $\sigma_{s-sp1}^2 = 2\frac{B_e}{B_0}R^2\,G\,P_1\,P_{ASE}$, $\sigma_{s-sp0}^2 = 2\frac{B_e}{B_0}R^2\,G\,P_0\,P_{ASE}$, $\sigma_{th}^2 = \frac{4\,k_B\,T}{R_L}B_e$, $\sigma_d^2 = 2e\,I_d\,B_e$, $\sigma_{sp-sp}^2 = \frac{B_e}{{B_0}^2}\left(R\,P_{ASE}\right)^2(2B_0 - B_{\mathrm{e}})$.

Here, e is the electron charge, h is Planck's constant, ν is the incident light frequency, k_B is Boltzmann constant, T is temperature, R_L is load resistance and I_d is dark current, P_{ASE} is the spontaneous emission noise power generated by EDFA.

The average signals current for data "1" and "0" are

$$I_{m1} = RG\,P_1 + R\,F_{\mathrm{n}}\,h\nu(G-1)\,B_0 \tag{6}$$

$$I_{m0} = R\,F_{\mathrm{n}}\,h\nu(G-1)\,B_0 . \tag{7}$$

Therefore, BER can be calculated by

$$BER = \frac{1}{2}erfc\left(\frac{Q}{\sqrt{2}}\right) \approx \frac{\exp\left(-Q^2/2\right)}{Q\sqrt{2\pi}}. \tag{8}$$

Here, $Q = \frac{I_{m1} - I_{m0}}{\sigma_1 + \sigma_0}$. $erfc(\,)$ is complementary error function.

Assuming that Alice sends data "0" and "1" with the same probability, BER of Eve can be represented as

$$BER = \frac{1}{2}\left[p(0/1) + p(1/0)\right]. \tag{9}$$

Here, $p(0/1)$ indicates the error probability that the transmitted signal is "1" and the received signal is "0", and $p(1/0)$ indicates the error probability that the transmitted signal is "0" and the received signal is "1".

For eavesdropper using non matching decoder, the cross-correlation value equals 1. Therefore, beat noise and MAI will exist in the receiver. For LA (N, K, M) code, it can be seen that

$$\xi = ((K \times K)/N)\big/K^2 = 1/N. \tag{10}$$

The beat noise for data "1" is

$$\sigma_{beat-1}^2 = 2k\xi \left(GR_{P_{Eve}}\right)^2. \tag{11}$$

The beat noise for data "0" is

$$\sigma_{beat-0}^2 = k(k-1)\,\xi^2 \left(GR_{P_{Eve}}\right)^2. \tag{12}$$

For coherent OCDMA based on LA (N, K, M), q_1 and q_0 are used to denote the probability that the cross-correlation values of the codes are "1" and "0" respectively, $q_1 = K^2/2N$, $q_0 = 1 - q_1$. The cross-correlation mean μ and variance σ^2 are

$$\mu = K^2/2N \tag{13}$$

$$\sigma^2 = \left(1 - \left(\frac{K^2}{2N}\right)\right)\left(\frac{K^2}{2N}\right). \tag{14}$$

Therefore, the variance of MAI is

$$\sigma_{MAI}^2 = k\,\sigma_{MAI-0}^2 \left(GR_{P_{Eve}}\right)^2. \tag{15}$$

Here, σ_{MAI-0}^2 is the variance of a single interfering signal, $\sigma_{MAI-0}^2 = \left(1 - \left(\frac{K^2}{2N}\right)\right)\left(\frac{K^2}{2N}\right)$.

For user data "1" and "0", the total noise variance for Eve is

$$\sigma_{E1}^2 = \sigma_{sh1}^2 + \sigma_{s-sp1}^2 + \sigma_{sp-sp}^2 + \sigma_{th}^2 + \sigma_d^2 + \sigma_{MAI}^2 + \sigma_{beat-1}^2. \tag{16}$$

$$\sigma_{E0}^2 = \sigma_{sh0}^2 + \sigma_{s-sp0}^2 + \sigma_{sp-sp}^2 + \sigma_{th}^2 + \sigma_d^2 + \sigma_{MAI}^2 + \sigma_{beat-0}^2. \tag{17}$$

Similarly, according to Eq. (8), BER of Eve can be calculated.

For coherent OCDMA based on 127 Gold code, there are also MAI and beat noise. The ξ value of 127 Gold code is $\xi \approx 1/N_{chip} = 1/127$. The calculation method of MAI for 127 Gold code was elaborated in Wang and Kitayama (2004).

4 Results and discussion

4.1 Bit error rate

In quasi-synchronous coherent OCDMA wiretap channel employing LA (156, 8, 16), simulation parameters for Matlab is listed in Table 1.

Figure 2 is the BER performance of the coherent OCDMA system based on LA (156, 8, 16) code and 127 Gold code, when the eavesdropper extraction ratio is 0.1% and the extraction distances are 5, 20, 50 km respectively. It can be seen from Fig. 2 a–c that, for legitimate user, BER of LA code is independent of the number of users and the extraction distances, and is only related to the extraction ratio of Eve. However, BER of 127 Gold code is dependent on the number of users, and it deteriorates as the number of users increases. For eavesdropping user, when extraction ratio is 0.1%, regardless of the system

Table 1 Simulation parameters

λ	1550 nm	Wavelength
F_n	5 dB	Noise index
G	30 dB	Gain
L	100 km	Transmission distance
α	0.2 dB/km	Attenuation coefficient
υ	1 Gbit/s	Transmission rate
R	0.8 A/W	Responsivity
P	1 mw	Power
I_d	2 nA	Dark current
T	300 K	Temperature
R_L	50 Ω	Load resistance
k + 1	8	Users

using LA (156, 8, 16) code or 127 Gold code, BER of Eve increases as the number of users increases. Compared with 127 Gold code, BER of LA (156, 8, 16) code is higher than that of Gold code. For example, when extraction distance is 50 km and the number of users is 3, BER of LA (156, 8, 16) code is 0.4963, while BER of 127 Gold code is 0.4931. Therefore, LA code can improve the physical-layer security and reliability simultaneously.

4.2 Secrecy capacity

The secrecy capacity is defined as the difference between main channel capacity and eavesdropping channel capacity. Secrecy capacity is the largest rate at which an eavesdropper gains no information about the message. If the non-zero security capacity exists, the main channel is superior to the eavesdropping channel.

Assuming that Alice sends data "0" and "1" with the same probability and the optimal decision threshold is used, the eavesdropping channel model can be simplified as a binary symmetric discrete channel. Assuming that ε is the eavesdropping channel transition probability, Eve's channel capacity can be calculated by

$$C_{XZ} = 1 - \left[-(1-\varepsilon)\log(1-\varepsilon) - \varepsilon \log \varepsilon\right]. \tag{18}$$

Similarly, assuming that τ is BER of legitimate user, channel capacity of the main channel is

$$C_{XY} = 1 - \left[-(1-\tau)\log(1-\tau) - \tau \log \tau\right]. \tag{19}$$

Secrecy capacity can be obtained by

$$C = \upsilon \times (\mathrm{k}+1)\left\{C_{XY} - C_{XZ}\right\}. \tag{20}$$

Here, $\upsilon = 1$ Gbit/s, is the single-user transmission rate.

Figures 3, 4 and 5 is secrecy capacity of LA (156, 8, 16) code and 127 Gold code at different extraction ratio and same extraction distance. As can be seen from Figs. 3, 4 and 5, when the number of users is small, the secrecy capacity of the LA code and the Gold code are almost the same. But when the number of users is more than 4, the secrecy capacity of LA code is obviously better than that of Gold code. For example, when the extraction ratio of eavesdropper is 1%, extraction distance is 5 km and the number of users is 4, the secrecy capacity of LA (156, 8, 16) code is 3.99×10^9 bit/s, and the secrecy capacity of 127 Gold code is 3.98×10^9 bit/s. When the number of users

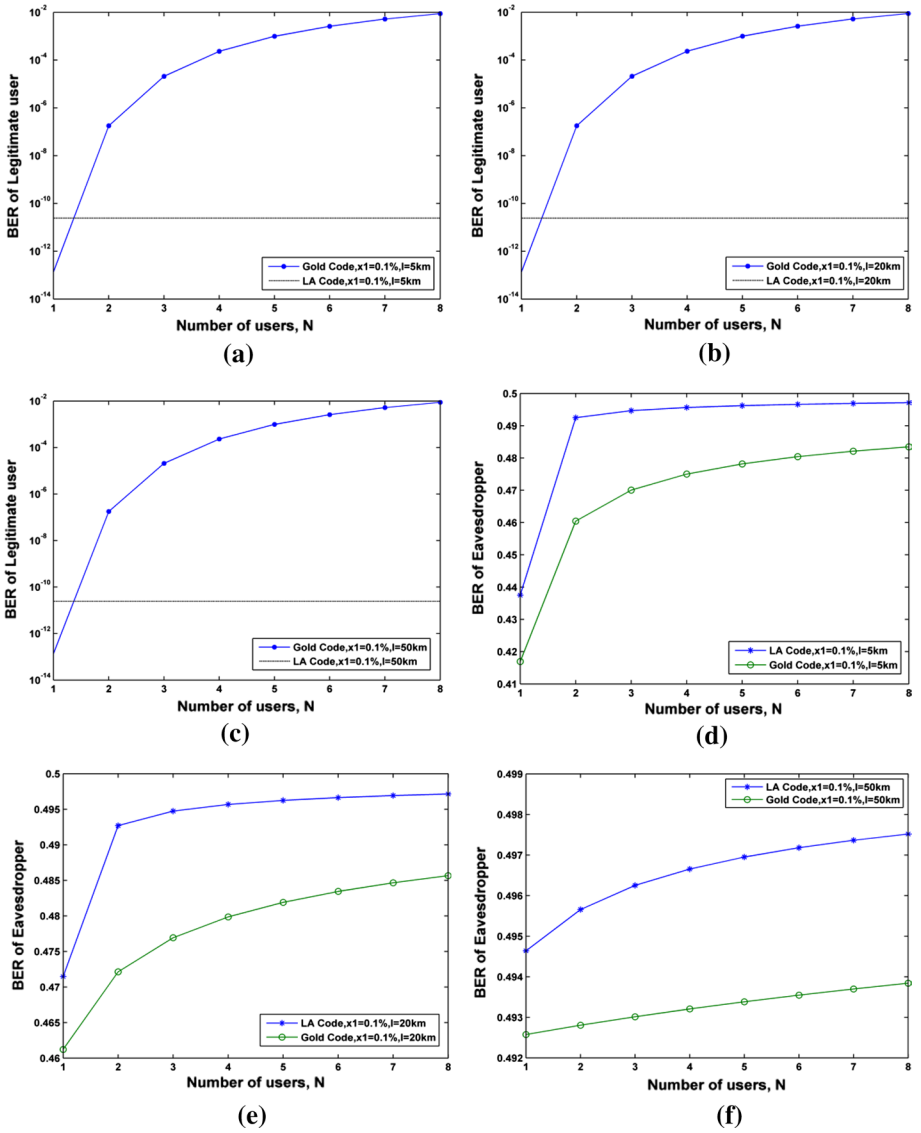

Fig. 2 BER performance with extraction ratio 0.1%. **a** BER of legitimate user (5 km), **b** BER of legitimate user (20 km), **c** BER of legitimate user (50 km), **d** BER of eavesdropper, extraction location 5 km, **e** BER of eavesdropper, extraction location 20 km, **f** BER of eavesdropper, extraction location 50 km

is 8, the secrecy capacity of LA (156, 8, 16) code is 8×10^9 bit/s, and the secrecy capacity of 127 Gold code is 7.4×10^9 bit/s. The reason is that, as long as the relative delay between users is controlled in the range of the zero correlation zone, BER of legitimate user with LA code is independent of the number of users. That is, the single legitimate channel remains unchanged. However, BER of legitimate user with Gold code is related to the number of users. When the number of users increases, the BER of legitimate users becomes larger, and the legitimate channel capacity becomes smaller.

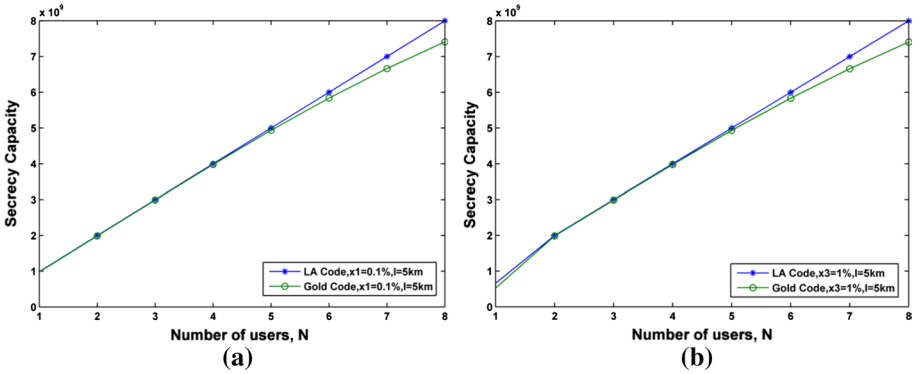

Fig. 3 Secrecy capacity of LA code and Gold code at different extraction ratio (5 km). **a** Extraction ratio 0.1% and extraction location 5 km, **b** extraction ratio 1% and extraction location 5 km

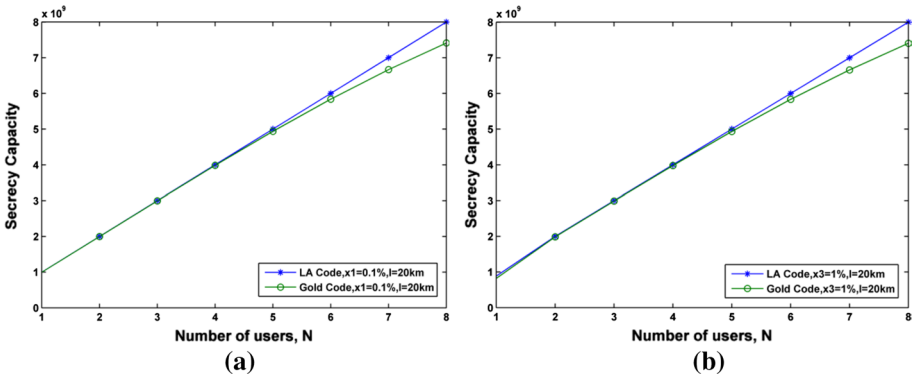

Fig. 4 Secrecy capacity of LA code and Gold code at different extraction ratio (20 km). **a** Extraction ratio 0.1% and extraction location 20 km, **b** extraction ratio 1% and extraction location 20 km

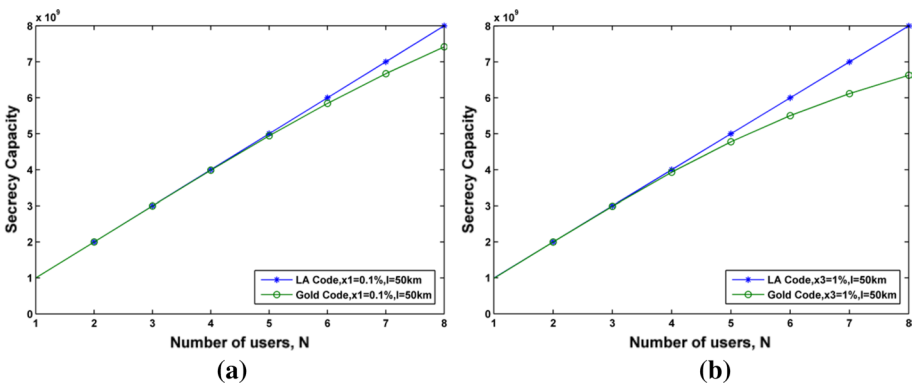

Fig. 5 Secrecy capacity of LA code and Gold code at different extraction ratio (50 km). **a** Extraction ratio 0.1% and extraction location 50 km, **b** extraction ratio 1% and extraction location 50 km

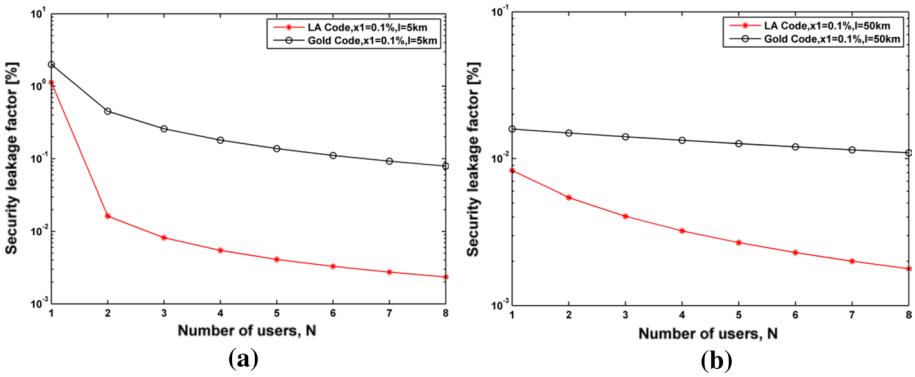

Fig. 6 Security leakage factor of LA (156, 8, 16) code and 127 Gold code (extraction ratio 0.1%). **a** extraction location at 5 km, **b** extraction location at 50 km

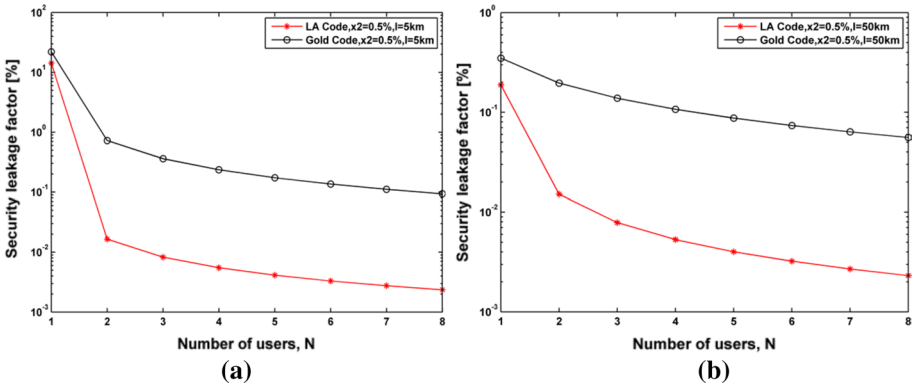

Fig. 7 Security leakage factor of LA (156, 8, 16) code and 127 Gold code (extraction ratio 0.5%). **a** extraction location at 5 km, **b** extraction location at 50 km

4.3 Security leakage factor

When the transmitter chooses to communicate at the main channel capacity, the secrecy capacity cannot be evaluated as a parameter for physical layer security. Here, we use security leakage factor to evaluate the physical-layer security of OCDMA system. Security leakage factor η is defined as the ratio of the Eve's channel capacity to the source entropy $H(X)$

$$\eta = \frac{C_{XZ}}{H(X)} \times 100\%. \tag{21}$$

According to the definition of security leakage factor, the smaller the security leakage factor is, the better the security performance of the system's physical layer.

Figures 6, 7 and 8 are the security leakage factors for LA (156, 8, 16) code and 127 Gold code, when extraction ratios of the Eve are 0.1, 0.5 and 1% respectively, and extracts distances from 5 to 50 km respectively. The security leakage factor is reduced as the number of users increases. However, the security performance of LA code is

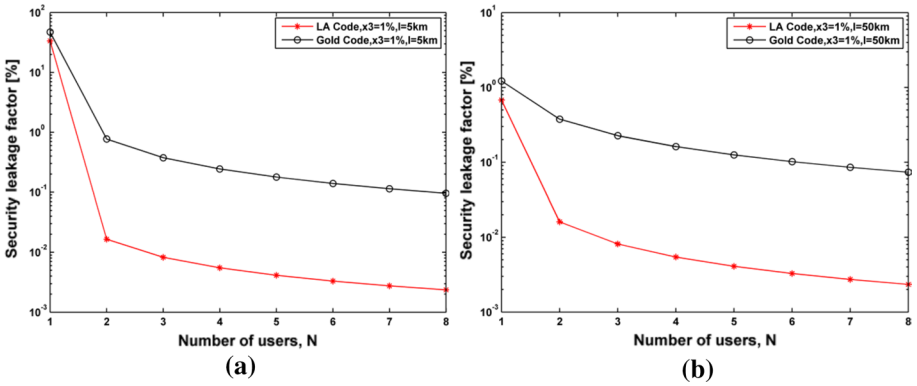

Fig. 8 Security leakage factor of LA (156, 8, 16) code and 127 Gold code (extraction ratio 1%). **a** extraction location at 5 km, **b** extraction location at 50 km

always better than that of Gold code. For example, when the extraction ratio of Eve is 1%, the extraction distance is 5 km and the number of users is 3, the security leakage factor of the LA (156, 8, 16) code is 0.0083%, while the security leakage factor of 127 Gold code is 0.375%.

5 Conclusion

Because of the MAI and beat noise, the reliability, capacity and physical-layer security of asynchronous coherent time-spreading OCDMA system will degrade. To further enhance the physical-layer security and system capacity of coherent OCDMA systems, a quasi-synchronous coherent time-spreading OCDMA Wiretap Channel is proposed. The influences of the extraction location, the extraction ratio, the number of active users on the physical-layer security are investigated quantitatively.

For legitimate users employing LA (156, 8, 16) code and 127 Gold code, BER of LA code is lower than that of Gold code. However, for eavesdropping user, the BER of LA code is higher than that of Gold code. When the number of users is small, the secrecy capacity of LA code and the Gold code is almost identical. But when the number of users exceeds 4, the secrecy capacity of LA code is obviously higher than the secret capacity of Gold code. The security leakage factor decreases slowly with the increase of the number of users, with the security leakage factor of LA code lower than the security leakage factor of Gold code. Therefore, the proposed scheme can improve the physical-layer security and reliability simultaneously.

Acknowledgement This work was supported by NSFC 61671306 and JCYJ 20160328145357990.

References

Fan, P.Z., Suehiro, N., Kuroyanagi, N., Deng, X.M.: Class of binary sequences with zero correlation zone. Electron. Lett. **35**, 777–779 (1999)

Ji, J., Zhang, G., Li, W., Sun, L., Wang, K., Xu, M.: Performance analysis of physical-layer security in OCDMA-based wiretap channel. J. Opt. Commun. Netw. **9**, 813–818 (2017)

Jiang, Z., Leaird, D.E., Weiner, A.M.: Experimental investigation of security issues in O-CDMA. J. Lightwave Technol. **24**, 4228–4234 (2006)

Leaird, D.E., Jiang, Z., Weiner, A.M.: Experimental investigation of security issues in OCDMA: a code-switching scheme. Electron. Lett. **41**, 817–819 (2005)

San, V.V., Vo, H.V.: Accurate estimation of receiver sensitivity for 10 Gb/s optically amplified systems. Opt. Commun. **181**, 71–78 (2000)

Sasaki, M., Fujiwara, M., Jin, R.B., Takeoka, M.: Quantum photonic network: concept, basic tools, and future issues. IEEE J. Sel. Top. Quant. **21**, 49–61 (2015)

Shake, T.H.: Confidentiality performance of spectral-phase-encoded optical CDMA. J. Lightwave Technol. **23**, 1652–1663 (2005a)

Shake, T.H.: Security performance of optical CDMA against eavesdropping. J. Lightwave Technol. **23**, 655–670 (2005b)

Shaneman, K., Gray, S.: Optical network security: technical analysis of fiber tapping mechanisms and methods for detection and prevention. Mil. Commun. Conf. (Milcom) **2**, 711–716 (2004)

Shields, A.J., Dixon, A.R., Sharpe, A.W., Choi, I., Dynes, J.F.: Stability of high bit rate quantum key distribution on installed fiber. Opt. Exp. **20**, 16339–16347 (2012)

Shimizu, K., Honjo, T., Fujiwara, M., Ito, T., Tamaki, K.: Performance of long-distance quantum key distribution over 90-km optical links installed in a field environment of Tokyo Metropolitan Area. J. Lightwave Technol. **32**, 141–151 (2014)

Tan, Y., Pu, T., Xiang, P., Fang, T., Zheng, J., Wu, W., Zhu, H.: Secrecy capacities of optical CDMA communication systems based on gold codes. In 15th International Conference on Optical Communications and Networks (ICOCN), pp. 24–27 (2016)

Wang, X., Kitayama, K.: Analysis of beat noise in coherent and incoherent time-spreading OCDMA. J. Lightwave Technol. **22**, 2226–2235 (2004)

Wang, Z., Chang, J., Prucnal, P.R.: The oretical analysis and experimental investigation on the confidentiality of 2-D incoherent optical CDMA system. J. Lightwave Technol. **28**, 1761–1769 (2010)

Zhou, X., Tang, X.: Research and implementation of RSA algorithm for encryption and decryption. In: The 6th International Forum on Strategic Technology, pp. 1118–1121. IEEE (2011)