Secrecy Capacities of Optical CDMA Communication Systems Based on Gold Codes

Yeteng Tan, Tao Pu, Peng Xiang, Tao Fang, Jilin Zheng, Weijiang Wu, and Huatao Zhu*

College of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, China
*E-mail: nj_putao@163.com

ABSTRACT

Optical CDMA transmission systems can not only increase system capacity, but also achieve physical- layer security against fiber tapping attacks. In this paper, we examine the information-theoretic security of optical CDMA systems by evaluating the tradeoff between the achieved information capacity and the confidentiality. Moreover, we also evaluate the impacts of key system parameters, such as the number of users M, the number of stages of shift-register r (or code lengths L=2r-1) and the input optical power P, on the secrecy capacity and the interception probability. Our results indicate that key system parameters play an important role in enhancing the secrecy capacities, thus choosing suitable values of these system parameters will be helpful to improve the secure performance of optical CDMA systems to some degree.

Keywords: *Optical Code Division Multiple Access (OCDMA), wiretap channel model, secrecy capacity, interception probability, Gold codes*

1. INTRODUCTION

Fiber-optic communication systems are vulnerable to various types of physical-layer attacks, for example, an eavesdropper can extract the transmission signal by bending the fiber and detecting the evanescent optical field coupled out of the fiber at the bend [1, 2]. Optical CDMA communication systems address this issue by using optical encoding and decoding technologies. Enhanced security has often been cited as an important benefit of optical CDMA communication technology. However, the quality and degree of security enhancement have not been closely examined in the literature [3]. Most of the literature discussing optical CDMA security relies on rather intuitive and imprecise notions of the degree of security.

In this paper, the security of optical CDMA based on Gold codes from information theory viewpoint is evaluated. Information-theoretic security is a widely accepted notion of secrecy in a classical communication system. When a communication system is operated under secrecy conditions, even an eavesdropper can observe the channel output, he can only guess the transmitted data. The secrecy capacity then quantifies the maximum achievable transmission capacity that can be transmitted to a legitimate receiver, provided that an eavesdropper cannot receive any useful information [4]. We examine the information-theoretic security of optical CDMA systems, using three types of secrecy capacities: guaranteed capacity, outage capacity and average capacity.

2. MODEL AND SIMULATION

Fig.1 illustrates the wiretap channel model. In the model, a legitimate user named Alice wants to send message to another legitimate user named Bob, but there is an eavesdropper named Eve who can extract the transmitted signal. The message D sent by Alice is firstly encoded by optical encoder, then coupled into the fiber channel and transmitted. At the receiver end, the coded data from both targeted and un-targeted users come into the decoder, which leads to multi-access interference (MAI). Because photodiode is a square-law device, optical signals from different sources will produce cross terms when optical signals are converted into electronic signals. Cross terms between D and I are called prime beat noise (PB) and cross terms between each parts of I are called secondary beat noise (SB). There will also be thermal noise N_T induced by photodiode in the system at the same time [5].

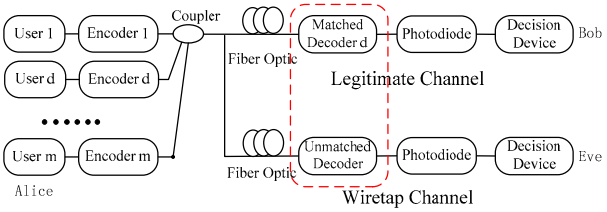

Fig.1 Wiretap Channel Model of Optical CDMA Systems

It is generally assumed that eavesdropper is aware of some of the optical CDMA signal parameters (such as data rate, coding type and code word structure, etc.), but he or she doesn't know the specific code words that legitimate users used [6]. So, the eavesdropper can only choose some codes from random sequences with the period n =2^r-1 as decoder's code word, then the decoder is unmatched. According to Shannon's theorem [7, 8], the legitimate channel capacity C_M and wiretap channel capacity C_W can be represented as separately:

$$C_M = \log_2(1+SNR_M) = \log_2\left(1+\frac{\langle i_P^2\rangle}{\langle i_T^2\rangle+\langle i_{MAI}^2\rangle+\langle PB^2\rangle+\langle SB^2\rangle}\right) \quad (1)$$

978-1-5090-3491-8/16/$31.00 ©2016 IEEE

$$C_W = \log_2(1+SNR_W) = \log_2\left(1+\frac{\langle i_{P'}^2\rangle}{\langle i_{T'}^2\rangle+\langle i_{MAI'}^2\rangle+\langle PB'^2\rangle+\langle SB'^2\rangle}\right) \quad (2)$$

If $C_M > C_W$, We can get the secrecy capacity of Optical CDMA systems as follow [4]:

$$C_S = C_M - C_W \quad (3)$$

The legitimate and wiretap channels are both random because the users and the eavesdropper choose code words randomly. So, the channel capacities and the secrecy capacities are also both random. We can't predict which of the code words will be chosen. As a result, the secrecy capacity of Optical CDMA channel is randomly distributed. Here, we will study three types of secrecy capacities:

1). Guaranteed Secrecy Capacity. We can refer to the maximum communication rate achieved in perfect secrecy as guaranteed secrecy capacity [9], which can be defined as

$$C_S^{grt} = (C_M - C_W)_{\min} \quad (4)$$

2). Average Secrecy Capacity. For random choices of code words, the channel capacities and secrecy capacities are random distributed. We can average the secrecy capacity for many random code words choices by which a secrecy capacity can be achieved. We refer to this capacity as average secrecy capacity, which is given by:

$$C_S^{avg} = E(C_M - C_W) \quad (5)$$

3). Outage Secrecy Capacity. If the transmitter chooses to communicate at a rate R higher than the guaranteed secrecy capacity, there is a finite probability that the eavesdropper can get a portion of the secret information. We refer this probability as the interception probability $p_{int}(R)$, which is given by:

$$p_{int}(R) = P(C_M - C_W < R) \quad (6)$$

We also can refer to the maximum achievable secrecy rate such that the interception probability is less than ε as the outage secrecy capacity with interception probability ε [10]. That is,

$$P(C_M - C_W < C_S^{out}) \le \varepsilon \quad (7)$$

3. RESULTS AND DISCUSSION

The previous section shown that the secrecy capacities of optical CDMA communication systems depend on several system parameters, such as the number of users M, the number of the stages of shift-registers *r* and the input optical power P, etc. Here, we evaluate the impact of each of these system parameters, based on numerical approach. For a given set of parameters, we run a simulation that generates 10^5 random choices of code words. Then, we calculate the secrecy capacities based on statistics generated by these random choices. The simulation parameters are set as follow: extinction ratio ext=10dB, responsivity of PD R=0.65, bandwidth of PD Be=2×10^7Hz, equivalent load impedance Re=1000Ω, absolute temperature T=290K.

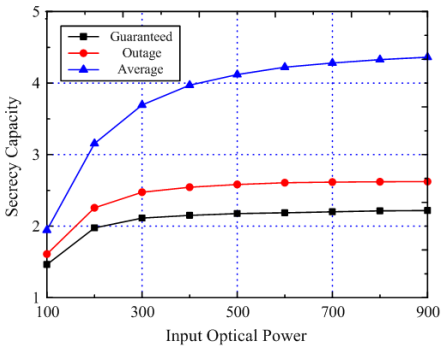

Fig.2 Secrecy capacities vs. input optical power P, with M=8 and *r*=9

In Fig.2 we plot the average, outage (with $p_{int}=10^{-3}$) and guaranteed secrecy capacities as functions of the input optical power P for the case of M=8, *r*=9. We observe that when the input power is small (<300nW), all the three types of secrecy capacities increase quickly, then when the input power increases, the secrecy capacities increase slower, and finally (>700nW) they become almost constant with the input optical power P increasing. This is because the user signals and noises (MAI, PB and SB) in the channel will both increase when the power P gets larger, but the augmenter of the user signals is larger relative to the noises. So, the SNRs and capacities of the legitimate and wiretap channels will both increase. And because the augmenter of the legitimate channel capacity is larger than that of the wiretap channel, the secrecy capacities of optical CDMA systems will get larger. When the input optical power P increases to some values, the systems will be saturated and the secrecy capacities won't increase.

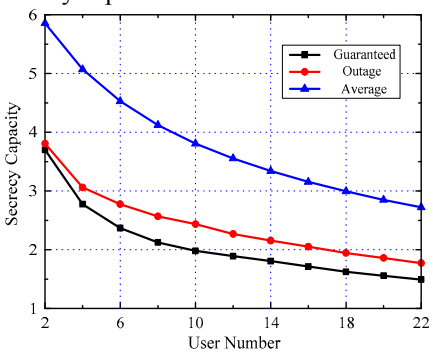

Fig.3 Secrecy capacity vs. number of users M, with P=500nW and r=9

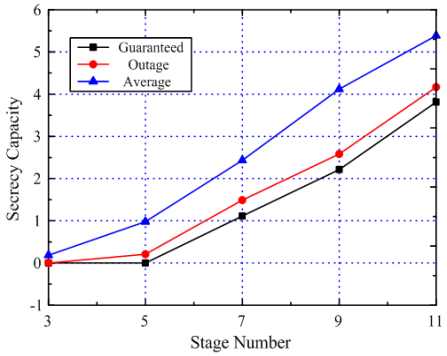

Fig.4 Secrecy capacity vs. number of stages of shift-registers *r*, with M=8 and P=500nW

For the case of P=500nW, *r*=9, Fig.3 shows that the average, outage (with $p_{int}=10^{-3}$) and guaranteed secrecy capacities decrease along with the increase of the number of users M, but the reductive rates of them are getting slower. This is because the noises (MAI, PB and SB) in the channels are getting larger as the number of users M increases, the SNRs and channel capacities of the legitimate and wiretap channels will be smaller. So, the secrecy capacities will reduce due to the larger reduction of the legitimate channel.

In Fig.4, we plot the capacities as a function of the number of stages *r*, for M=8 and P=500nW, which shows that as the number of stages *r* increases, the average, outage (with $p_{int}=10^{-3}$) and guaranteed secrecy capacities will also increase. This is because the normalized cross-correlations of code in the legitimate channel words decrease with the increase of the number of stages *r*, which will lead to the decrease of MAI, PB and SB and the increase of SNR of the legitimate channel. So, the legitimate channel capacity will also increase. But, for the wiretap channel, the number of stages *r* has no influence on the user signals and noises, and then the SNR and channel capacity of the wiretap channel is independent of the number of stages *r*. So, the secrecy capacities of optical CDMA systems will increase with the increase of the number of stages *r*.

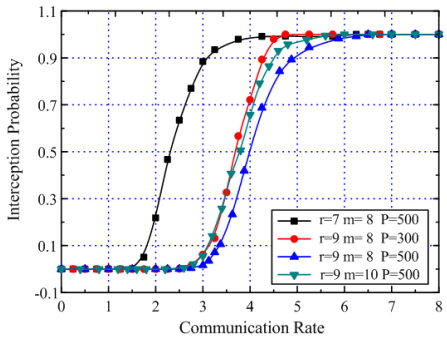

Fig.5 Interception probability vs. communication rate under different system parameters

We plot the interception probability as functions of communication rate for the case of r={7, 9}, P={300nW, 500nW}, M={8, 10}. In Fig.5, we observe that increasing stage number *r*, input optical power P or decreasing user number M are in favor of reducing the interception probability when the communication rate is definite. In other words, it's helpful to improve the secure performance of the systems. As analyzed above, the secrecy capacities of optical CDMA communication systems are larger when the stages number r, the input optical power P are bigger or the users number M is smaller. Then, the interception probability $p_{int}(R) = P\{C_S<R\}$ is smaller when the communication rate R is fixed. So, this result shows that the system parameters *r*, P and M play an important role in reducing the interception of the secret information by the eavesdroppers.

4. CONCLUSION

In conclusion, we evaluated the secure performance of optical CDMA systems quantitatively by using interception probability and secrecy capacities from information theory viewpoint. And, we also assessed the impact of key system parameters on the security of optical CDMA systems. Our results show that the systems parameters play an important role in improving secure performance of optical CDMA communication systems. The proper values of the number of users M, the input optical power P and the number of stages of shift-registers *r* will help to enhance the secrecy capacities of the systems and decrease the interception probability of secure information at the same communication rate. This will provide theoretical guidance for further improving the secure performance of optical CDMA communication systems.

5. ACKNOWLEDGMENTS

The work was supported in part by the National Natural Science Foundation of China under Grant No. 61475193, No.61174199, and the Jiangsu Province Science Foundation under Grant No. BK20120058 and BK20140069.

6. REFERENCES

[1] K. Shaneman and S. Gray, "Optical network security: Technical analysis of fiber tapping mechanisms and methods for detection & prevention" IEEE Military Communications Conference, 2004, 2:711-716 Vol. 2

[2] M. Medard, D. Marquis, R. A. Barry, and S. G. Finn, "Security issues in all-optical networks" Srii Global Conference, 2011, 11(3):42-48

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

[4] A.D. Wyner, "The wire-tap channel" The Bell System Technical Journal, 1975, 54(8):1355-1387

[5] T Pu, H Zhang, Y Guo, M Xu, and Y Li, "Evaluation of beat noise in OCDMA system with non-Gaussian approximated method" Journal of Lightwave Technology, 2006, 24(10):3574-3582

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

[7] C.E. Shannon, "A mathematical theory of communication" The Bell System Technical Journal, 1948, 27: 379–423, 623–656

[8] C.E. Shannon, "A mathematical theory of communication2" The Bell System Technical Journal, 1948, 27(3):3-55

[9] K Guan, A.M. Tulino, P.J. Winzer, and E Soljanin, "Secrecy Capacities in Space-Division Multiplexed Fiber Optic Communication Systems" IEEE Transactions on Information Forensics & Security, 2015, 10(7):1-1

[10] J Barros, M.R.D. Rodrigues, "Secrecy Capacity of Wireless Channels" IEEE International Symposium on Information Theory, 2006:356-360