Demonstration of differential detection on attacking code-shift-keying OCDMA system

B. Dai, Z. Gao, X. Wang, N. Kataoka and N. Wada

In this reported work, differential detection to eavesdrop the encoded information in the temporal phase coding code-shift-keying OCDMA system, is proposed and experimentally demonstrated. Differential detection can be used to distinguish the discrepancy in the two encoded signals.

Introduction: Security is often considered as an attractive advantage in the optical code-division multiple access (OCDMA) system [1, 2]. In the OCDMA system, each user is assigned a unique code for data encryption and the encoded data is broadcast to the whole network. On the receiving side, only the authorised user can recover the original data, using the same code sequence. However, the vulnerability of the single-user on-off-keying OCDMA (OOK-OCDMA) system has been demonstrated, which can be easily attacked by the energy detection [3]. Compared to the OOK-OCDMA system, the differential phase-shift keying OCDMA (DPSK-OCDMA) system ensures security against simple energy detection [4], but eavesdroppers can still detect the data from the encoded signals using a DPSK demodulator [5]. As a distinctive modulation format in the optical coding system, code-shift keying (CSK), where data bit '0' and '1' are encoded by two different codes, was introduced into the OCDMA system to improve security against energy detection [6]. Nevertheless, researches have revealed that a DPSK demodulator followed by a balanced photodetector (BPD) can also directly detect the data in the CSK-OCDMA system [5, 7]. The DPSK demodulator is an interferometer with one-bit delay in one arm. Using the DPSK demodulator to detect CSK data is based on the interference between two optical signals, which may not work properly under the condition of the incoherent coding or the existence of other phase information. In this Letter, we propose a novel eavesdropping scheme using differential detection, which has a simple structure with a tunable optical delay line (TOLD) and a BPD. The differential detection is independent of the coherence of the signals, and it can be used in situations of incoherent coding and the existence of other phase information. We also carry out an experimental demonstration of the differential detection to attack the CSK-OCDMA system.

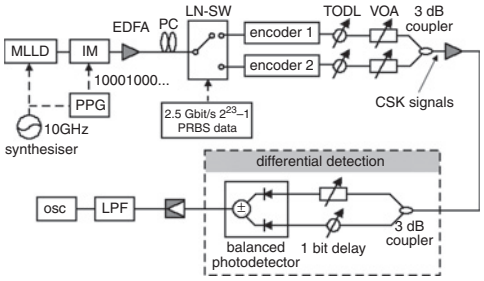

Fig. 1 *Experimental setup of CSK-OCDMA system with differential detection*

Principle of differential detection: Differential detection compares two encoded signals and distinguishes the difference between them. The schematic diagram of the differential detection module is shown in Fig. 1. The 3 dB coupler divides the encoded signal into two arms. In one arm, a TODL is added to generate 400 ps (one-bit) delay. In another arm, a variable optical attenuator (VOA) is used to balance the power in both arms. At the BPD, the optical signals from two arms are converted into electrical signals by the two photodetectors (PDs), followed by the subtractor to detect the difference between the two signals. According to the different combinations of the consecutive bits, the resultant waveforms from the BPD are illustrated in Fig. 2. If the symbols of consecutive bits are the same, they are encoded by the same code, resulting in cancellation between each other in the differential detection and no output; while if the symbols of consecutive bits are different, it leads to either positive or negative output. According to Fig. 2, the symbol of each data bit can then be derived one by one from the output of the differential detection: a null output indicates that the current data bit is the same as the previous one, and nonzero outputs hint at the difference between current and previous data bits. Furthermore, by adjusting the TODL to generate multiple bits delay, we are able to compare any two encoded bits at any two different time slots, which is very flexible.

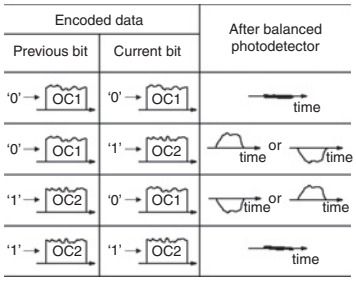

Fig. 2 *Look-up table for differential detection*

Experiment and results: The experimental setup of the CSK-OCDMA system with the differential detection is shown in Fig. 1. A 10 GHz optical pulse train with pulse width of 2 ps is generated by the modelocked laser diode (MLLD). An intensity modulator, driven by the pulse pattern generator (PPG) with the data pattern of 10001000..., is used to convert the data rate to 2.5 Gbit/s. The optical pulses are then separated into two branches by means of a lithium niobate optical switch (LN-SW), according to the data bit '0' and '1' of the $2^{23}-1$ pseudorandom bit sequence (PRBS) data. The optical pulses in two branches are encoded with two different 31-chip Gold codes by two 640 Gchip/s superstructured fibre Bragg gratings (SSFBGs) encoders, respectively. The TODLs and VOAs are used to align the pulses and balance the power in both branches. The signals from two branches are than combined using a 3 dB coupler generating the CSK signal, where the bits '0's and '1's present as noise-like waveforms with equal power.

In the receiving side, the differential detection is implemented directly without the decoding. In our experiment, the response rate of the BPD is 45 GHz. Fig. 3 shows the original data sequence, the detected waveform from the differential detection, and the measured eye diagram. We can attempt to extract the data sequence from the detected waveform in Fig. 3*b*. First, we assume the first bit at t_0 is '1' (assuming its '0' will only result in a complementary data sequence). Then, we can derive the second bit based on the look-up table in Fig. 2. Nonzero output at t_1 exposes that the second bit is different from the first one, so the second bit is '0'. The third bit is '0' as well owing to the null output at t_2. The negative output at t_3 hints that the fourth bit is '1'. The following data sequence can be similarly derived one by one. Finally, the whole data sequence can be extracted from the detected waveform from the differential detection. The extracted data sequence is exactly the same as the original data sequence, as shown in Fig. 3*a*. Fig. 3*c* shows the measured eye diagram after the differential detection. In the eye diagram, three levels, null and nonzero (positive and negative) outputs, can be clearly distinguished, which accords with the analysis and verifies the feasibility of the proposed scheme.

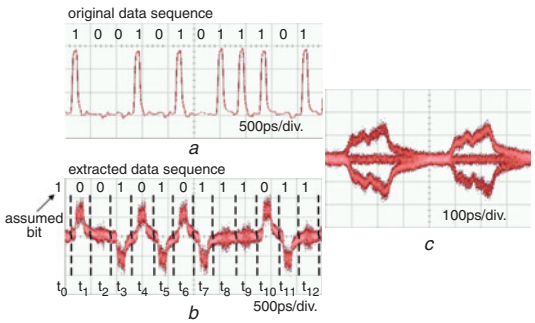

Fig. 3 *Data sequence and eye diagram*

a Original electrical data sequence
b Extracted data sequence using differential detection
c Eye diagram after differential detection

Conclusion: We propose differential detection to attack the single-user CSK-OCDMA system. In the experiment, we extracted the data sequence successfully from the detected waveform without the

decoding. It means that with the help of the differential detection, eavesdroppers do not need to know anything about the code and can easily intercept the information from the single-user CSK-OCDMA system. The differential detection offers a simple way to distinguish the difference between two encoded signals. Because of the flexibility of the bit-to-bit comparison, the differential detection has the potential to be implemented in other complex systems.

29 October 2010
doi: 10.1049/el.2010.3061
One or more of the Figures in this Letter are available in colour online.

B. Dai, Z. Gao and X. Wang (*Joint Research Institute for Integrated Systems, EPS, Heriot-Watt University, Edinburgh, EH14 4AS, United Kingdom*)

E-mail: x.wang@hw.ac.uk

N. Kataoka and N. Wada (*National Institute of Information and Communications Technology (NICT), 4-2-1 Nukui-Kitamachi, Koganei, Tokyo, Japan*)

References

1 Shake, T.H.: 'Security performance of optical CDMA against eavesdropping', *J. Lightwave. Technol.*, 2005, **23**, (2), pp. 655–670
2 Torres, P., Valente, L.C.G., and Carvalho, M.C.R.: 'Security system for optical communication signals with fiber Bragg gratings', *IEEE Trans. Microw. Theory Tech.*, 2002, **50**, (1), pp. 13–16
3 Jiang, Z., Seo, D.S., Yang, S.D., Leaird, D.E., Roussev, R.V., Langrock, C., Fejer, M.M., and Weiner, A.M.: 'Four user, 2.5 Gb/s, spectrally coded O-CDMA system demonstration using low power nonlinear processing', *J. Lightwave. Technol.*, 2005, **23**, (1), pp. 143–158
4 Wang, X., Wada, N., Miyazaki, T., and Kitayama, K.: 'Coherent OCDMA system using DPSK data format with balanced detection', *IEEE Photonics Technol. Lett.*, 2006, **18**, (7), pp. 826–828
5 Dai, B., Gao, Z., Wang, X., Kataoka, N., and Wada, N.: 'Experimental investigation on security of temporal phase coding OCDMA system with code-shift keying and differential phase-shift keying'. 2010 Asia Communications and Photonics Conf. and Exhibition, (ACP'10), Shanghai, China (Paper FO1)
6 Wang, X., Wada, N., Miyazaki, T., Cincotti, G., and Kitayama, K.: 'Asynchronous multiuser coherent OCDMA system with code-shift-keying and balanced detection', *J. Sel. Top. Quantum Electron.*, 2007, **13**, (5), pp. 1463–1470
7 Jiang, Z., Leaird, D.E., and Weiner, A.M.: 'Experimental investigation of security issues in OCDMA'. 2006 Optical Fiber Communication Conf., (OFC'06), Anaheim, CA, USA (Paper OThT2)