Security Enhanced SPECTS O-CDMA with Four-State Encoded Data Modulation

Chunxin Yang[1], Nicolas K. Fontaine[2], Ryan P. Scott[2], David J. Geisler[2], J. P. Heritage[2], and S. J. B. Yoo[2]
[1]Department of Applied Science, University of California, Davis, One Shields Ave., Davis, California 95616 USA
[2]Department of Electrical and Computer Engineering, University of California, Davis, One Shields Ave., Davis, California 95616 USA
Email: sbyoo@ucdavis.edu

Abstract: We demonstrate a security enhancement mechanism based on four-state temporal optical coding which protects a SPECTS O-CDMA upstream link against eavesdropping including DPSK detection. The FPGA-based code-hopping implementation facilitates future encryption by optical codes.

OCIS codes: (060.4250) Networks; (060.4785) Optical security and encryption.

1. Introduction

In recent years, the realization of fiber-to-the-premise (FTTP), along with increasing penetration of broadband access, has renewed interest in optical code-division multiple-access (O-CDMA) technology that provides flexibility and physical layer security to optical access networks [1]. Spectral phase encoded time-spreading (SPECTS) O-CDMA is a coherent O-CDMA scheme which applies a unique code to the spectral phase of each user's data modulated pulses, spreading the time-domain waveform. Among several O-CDMA schemes, the SPECTS O-CDMA method provides relatively high multiple-access-interference (MAI) suppression and 32 user x 10 Gb/s/user (320 Gb/s) SPECTS O-CDMA networking has been reported [2]. However, investigations have revealed certain security vulnerabilities for SPECTS O-CDMA systems. Particularly for the case of an individual upstream link where only one user is present, an eavesdropper can extract the user data without knowledge of the O-CDMA codes. For example, SPECTS O-CDMA using on–off keyed (OOK) data modulation can be intercepted by a power detector [3]. To remedy this security vulnerability, a bright/dark code data modulation scheme is adopted, in which two distinct waveforms generated by two O-CDMA codes that represent the "1"s and "0"s, each with nominally the same total energy [4]. Nevertheless, Jiang *et al.* have shown that such a scheme is still vulnerable to eavesdroppers equipped with a differential phase shift keying (DPSK) receiver which can detect the phase difference between the different spectral phase codes used for "1" and "0" data bits [5]. To enhance security against DPSK eavesdropping, a new data modulation scheme based on a finite-state Markov chain was proposed by Du *et al.* [6]. Following a three-state trellis, the user *binary* data stream is converted into a new sequence of *three* different states corresponding to three different waveforms, two of which are time spread by distinct OCDMA codes while the third is the null energy state. This approach can be generalized to more than three states and we employ a four-state version here to maintain energy balance in the data stream. As long as the state transition does not directly correspond to the binary data sequence, DPSK eavesdroppers cannot recover the user data without knowledge of the O-CDMA codes [6].

For the first time, we present a field-programmable gate array (FPGA) implementation of such a multi-state encoded data modulation technique following a four-state trellis and demonstrate error-free single user performance in a SPECTS O-CDMA testbed at 1.25 Gb/s and 2.5 Gb/s. Our fiber-optic DPSK detector intercepts the bright/dark code modulated data stream with BER as low as 10^{-7}, but the BER rises to ~ 0.5 with the four-state encoded data stream indicating that the user data is effectively obscured. Furthermore, this technique is readily extended to achieve a higher level of link security by alternating between several different trellis state definitions with a previously agreed upon key sequence established through public key encryption.

2. Four-state encoded data modulation

The modulation scheme proposed in [6] adds a null transmission in addition to the "bright" and "dark" O-CDMA encoded waveforms. The odd number of states results in unbalanced rate of "1"s and "0"s in the data so that an additional DC-balance technique is required. In this work, we introduce four-state encoded data modulation to avoid DC-balance issues. Fig. 1(a) shows the finite-state transition diagram (FSTD) which maps the transformation of the binary data to four states and Fig. 1(b) is the corresponding SPECTS O-CDMA transmitter. The four states are labeled as N (null), C1 (code 1), C2 (code 2) and C1C2 (both O-CDMA code 1 and code 2 are used). The state transitions follow the arrows driven by the incoming user data bit labeled on the arrow. The next state is specified by the current state and the new user data bit. Each state is represented by a 2-digit binary number so the four-state encoder has two outputs corresponding to the 2 digits. Each output drives a modulator and an O-CDMA encoder. The combined signal is the four-state encoded user data. Null state means no transmitted energy; C1 state transmits waveform 1 created by applying code 1 to a pulse in O-CDMA encoder 1; C2 state transmits waveform 2 from O-CDMA encoder 2; on C1C2 state, the two waveforms are transmitted simultaneously. The four-state encoded data modulation scheme requires the same O-CDMA code space as the three-state version and is more amenable to dynamic reconfiguration. However, the two waveforms on C1C2 states coherently interfere which contributes to reduced BER performance as compared to the three-state version. The best performance is obtained when OCDMA codes C1 and C2 are chosen with the greatest degree of orthogonality.

We implement the four-state encoder using a Xilinx FPGA equipped with high-speed serial transceivers. Each transceiver includes a transmitter and a receiver operating at up to 3.125 Gb/s. The receiver deserializes the data to a 20-bit parallel data block which is converted to the four-state sequence (two digits) by 20 parallel four-state encoders. Two transmitters send out the serialized four-state data. The corresponding four-state decoder is implemented in the FPGA which converts the four-state sequence back to the original user data bit sequence.

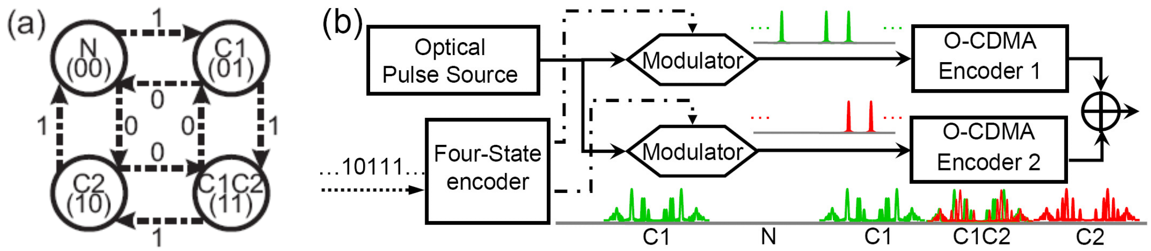

Fig. 1. Security enhanced SPECTS O-CDMA through four-state encoding. (a) Finite-state transition diagram (b) SPECTS O-CDMA transmitter with four-state encoded data modulation.

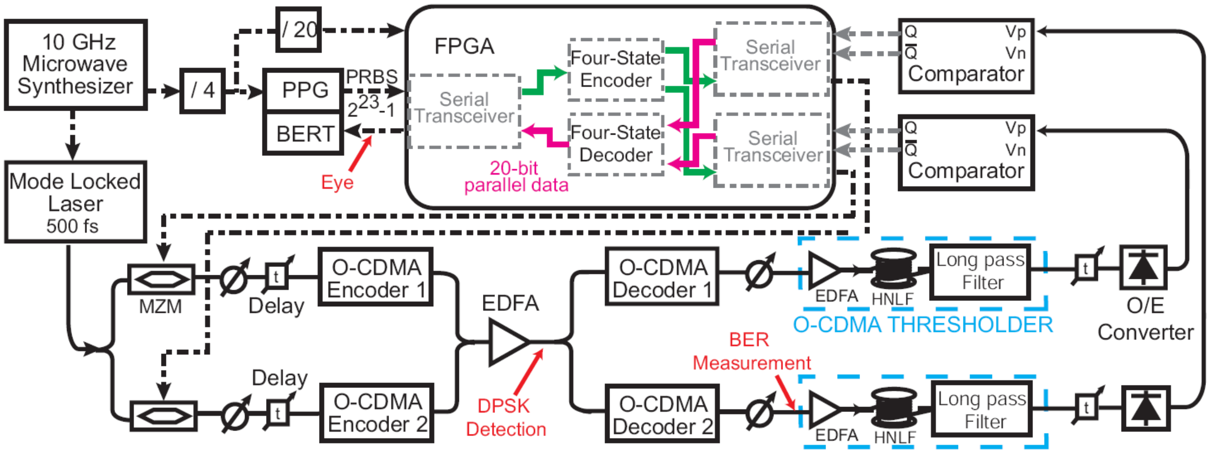

Fig. 2. Single user SPECTS O-CDMA testbed with four-state encoded data modulation. PPG (programmable pattern generator), BERT (bit-error-rate tester), MZM (Mach-Zehnder modulator), HNLF (highly nonlinear fiber)

3. Experiment results and discussion

Fig. 2 shows the experiment arrangement. The original user data is a 2^{23}-1 PRBS from programmable pattern generator (PPG) and it is converted to four-state encoded sequence by the FPGA. The 10 GHz, 500-fs optical pulse train is split and modulated by two Mach-Zehnder modulators (MZM) and go through two O-CDMA encoders applying 128-chip Walsh codes. The combined signal is the transmitted data of a single user. To detect the user data, two O-CDMA decoders apply the conjugate codes of the corresponding O-CDMA encoders. The correctly decoded pulses are short while the incorrectly decoded pulses (interferers) remain spread in time. The O-CDMA thresholder, based on filtering of spectral spreading by self phase modulation, distinguishes the short pulses from the interferers. After optical to electrical conversion, two comparators provide electrical thresholding and differential inputs to the serial transceivers on the FPGA. The FPGA converts the four-state sequence to the original PRBS for BER analysis.

Fig. 3(a) shows the BER and eye diagrams of the four-state encoded data modulation experiment. The received power is recorded before the O-CDMA thresholder. The BER group “O-CDMA encoder 1” (or “O-CDMA encoder 2") is the measured performance of O-CDMA encoder-decoder 1 (or encoder-decoder 2) without four-state encoding, while the other O-CDMA encoder is blocked. The power penalty between the O-CDMA encoder 1 and encoder 2 is mainly from the different amplifiers and nonlinear fiber scrolls used in the two O-CDMA thresholders. The BER group labeled as "four-state encoded" is the measured performance of the single user SPECTS O-CDMA link with four-state encoded data modulation, which achieves BER better than 10^{-11} at both 1.25 Gb/s and 2.5 Gb/s. The power penalty on the four-state encoded data modulation reflects the interference arising from the C1C2 state.

We use a fiber-optic delay interferometer as a DPSK detector operating at 2.50375 Gb/s to test the four-state data modulation scheme. The pulse train source is a stable optical frequency comb generator. First, the FPGA transmits two complimentary data streams in the experimental arrangement depicted in Fig. 2 to implement bright/dark code modulation. The DPSK detection achieves BER better than 10^{-6} as shown in Fig. 3(b). When the FPGA applies four-state encoding, the BER collapses to 0.4995±0.0005, when accumulated over a 30 s interval, as shown in Fig. 3(b). This result indicates that the four-state data modulation scheme has effectively enhanced security against DPSK detection.

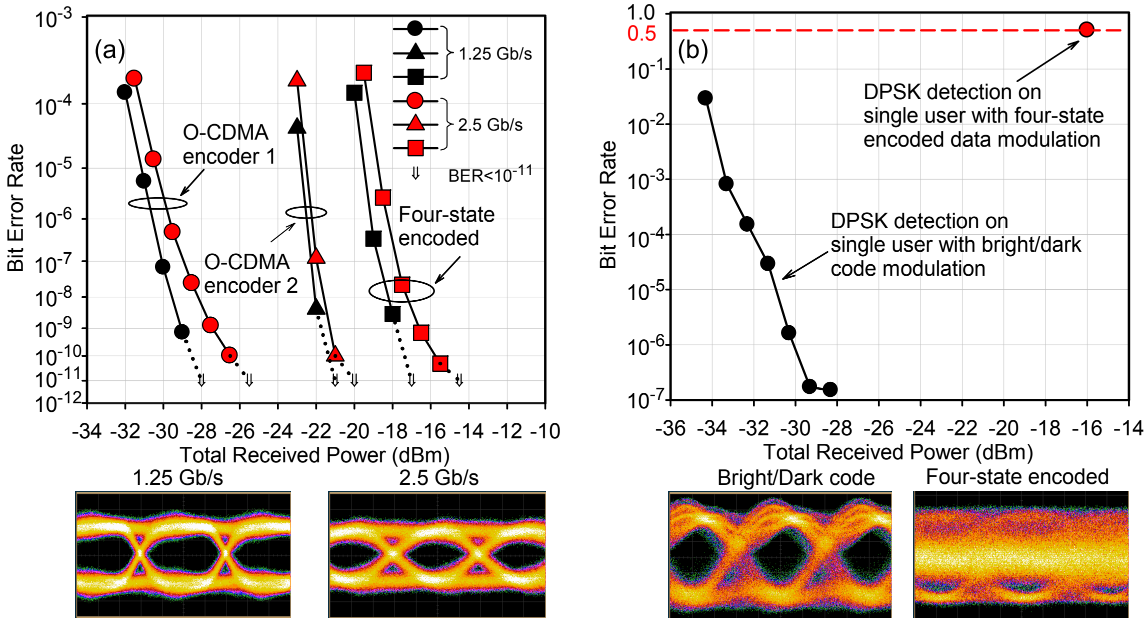

Fig. 3. BER results of the security enhanced SPECTS OCDMA testbed. (a) Single user of SPECTS O-CDMA with four-state data modulation at 1.25 Gb/s and 2.5 Gb/s. (b) DPSK detection on single user with bright/dark code modulation and four-state modulation

4. Conclusions

We implemented a security enhanced data modulation technique based on a finite-state Markov chain which follows a four-state trellis encoding. We present the first demonstration of SPECTS O-CDMA with four-state encoded data modulation at 1.25 Gb/s and 2.5 Gb/s and show the security enhancement against DPSK eavesdropping.

5. References

[1] A. Stok and E. H. Sargent, "The role of optical CDMA in access networks," IEEE Communications Magazine **40**, 83-87 (2002)
[2] V. J. Hernandez, W. Cong, J. Hu, C. Yang, N. K. Fontaine, R. P. Scott, B. H. Kolner, J. P. Heritage, and S. J. B. Yoo, "A 320-Gb/s capacity (32-user × 10 Gb/s) SPECTS O-CDMA network testbed with enhanced spectral efficiency through forward error correction," J. Lightw. Technol. **25**, 79-86 (2007)
[3] T. H. Shake, "Confidentiality performance of spectral-phase-encoded optical CDMA," J. Lightw. Technol. **23**, 1652-1663 (2005)
[4] D. E. Leaird, Z. Jiang, and A. M. Weiner, "Experimental investigation of security issues in OCDMA: A code-switching scheme," Electron. Lett., **41**, 817–818 (2005)
[5] Z. Jiang, D. E. Leaird, and A. M. Weiner, "Experimental investigation of security issues in O-CDMA," J. Lightw. Technol. **24**, 4228–4234 (2006)
[6] Y. Du, F. Xue, S. J.B. Yoo and Z. Ding, "Security enhancement of SPECTS O-CDMA through concealment against upstream DPSK eavesdropping", J. Lightw. Technol. **25**, 2799-2806 (2007)

This work was supported in part by DARPA and SPAWAR under agreement number N66001-02-18937 and by the AFOSR through the UC Davis Center for Digital Security.