Experimental Investigation on Using Phase Mask in Spectral-Phase-Encoded O-CDMA for Security Enhancement

C. Yang[(1)], W. Cong[(1)], F. Xue[(2)], V. J. Hernandez[(2)], R. P. Scott[(1)],
J. P. Heritage[(2)], B. H. Kolner[(1)], Z. Ding[(2)] and S. J. B. Yoo[(2)]
1: Department of Applied Science, 2: Department of Electrical and Computer Engineering
University of California, Davis, One Shields Ave, Davis, California 95616, email: sbyoo@ucdavis.edu

Abstract *This paper experimentally investigates the plausibility of a phase masking scheme for SPECTS O-CDMA security enhancement. Implementation of the phase mask is demonstrated with experimental results showing the improvement in security.*

Introduction

Inherent security has often been cited as a potential benefit of Optical Code Division Multiple Access (O-CDMA) [1]. Recent security analyses [2] have shown that the confidentiality protection offered by the spectral phase encoded time spreading (SPECTS) O-CDMA is relatively weak. Feasible SPECTS solutions are limited to several well-known code families of relatively small code set size; thus an eavesdropper can use brute-force searching in the known sets to easily determine the applied code. Our previous work [3] proposes a time-varying phase-masking scheme for security enhancement by applyling a time-varying *phase mask* to all authorized users within a network. On top of the phase shifts based on the applied phase-code, the encoder adds a new layer of phase shifts based on the *phase mask* and achieves phase encoding according to both the phase code and the *phase mask*. The *phase mask* poses additional difficulty to eavesdroppers if they are unaware how this mask is generated. This phase-mask serves as a *group key* to support secure group communications; only authorized users with the correct key are able to recover the data information using the corresponding inverse phase shift. Analytical results [3] indicate that this scheme increases the difficulty of intercetption and achieves low data interception rates.

In this paper, we implement the *phase mask* in our SPECTS O-CDMA testbed by imposing randomly generated phase shifts onto a liquid-crystal spatial light phase modulator (LC-SLPM) which is part of the encoders/decoders. These phase shifts are additive on to the 127 chip *m*-sequence O-CDMA phase code that are already applied onto the LC-SLPM. 3-user error free performance is achieved when encoding and decoding with the *phase mask* on all the encoders and decoder. We imitate the case where an eavesdropper successfully deciphers the phase code but fails in guessing the *phase mask* by decoding with the correct *m*-sequence while equipped with no *phase mask* on the decoder. The corresponding experimental results show the enhanced security offered by the *phase mask*.

Experimental Setup

Fig. 1 shows the system diagram of the 3-user SPECTS O-CDMA network testbed. The optical source emits 500-fs laser pulses centered at 1550 nm with a repetition rate of 9.95328 GHz (OC-192). After modulation with FEC-encoded data, the 10-Gb/s signal is split into 3 encoders. The combined encoded data streams are amplified and sent to the decoder. The output of the decoder goes to the nonlinear thresholder, which detects the intended user signal at the presence of the interfering signals [4]. The 10-Gb/s optical receiver converts the output of thresholder into an electronic signal that goes to the FEC decoder. The bit-error-rate tester (BERT) receives the FEC-decoded signal and measures BER.

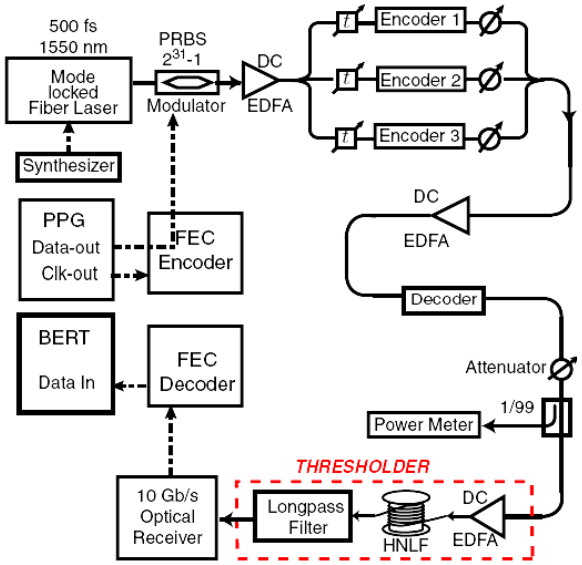

Fig. 1. SPECTS O-CDMA network testbed

Suppose all the encoders are authorized users in the network. A unique 127 chip *m*-sequence is assigned to each encoder as the O-CDMA phase code, and an identical 127 chip *phase mask* is additionally imposed to all the encoders as a group key for authorized users. When the *phase mask* is on, the total phase shift of each chip imposing on the LC-SLPM is the summation of the phase shift from the *m*-sequence (0, or π) and the phase shift from the *phase mask* (a random value from 0 to 0.5 π). The range of phase shift from the *phase mask* is limited to within 0.5π by

the total phase modulation range of the LC-SLPM (0-1.8π). The decoder adds the conjugate of the *phase mask* and the *m*-sequence used by Encoder 1 to correctly decode signal from Channel 1.

Results and Discussion

Fig. 2 shows the cross-correlation traces of the decoded signals. All traces show the encoders with the *phase mask* on. Trace (a) shows decoding with the correct *m*-sequence phase code and the matched *phase mask*, representing the case of decoding by an authorized user. The short pulse is reconstructed at time=0, rising above the multi-access interference. Trace (b) shows decoding with the correct *m*-sequence phase code but without the *phase mask*, representing an eavesdropper who succeeds in determining the O-CDMA phase code but fails in guessing the *phase mask*. A peak with low intensity appears because the net phase shift after decoding is from the *phase mask*, which is smaller than that from the phase code, and it does not spread the pulse as flat as the phase code. Nevertheless, the peak is largely diminished and the trace is similar to trace (c), which is the incorrectly decoded signal obtained using an incorrect *m*-sequence, but with the phase-mask. It is apparent from the traces that it is difficult to distinguish the intended user signal from the interfering users without knowing the *phase mask*,.

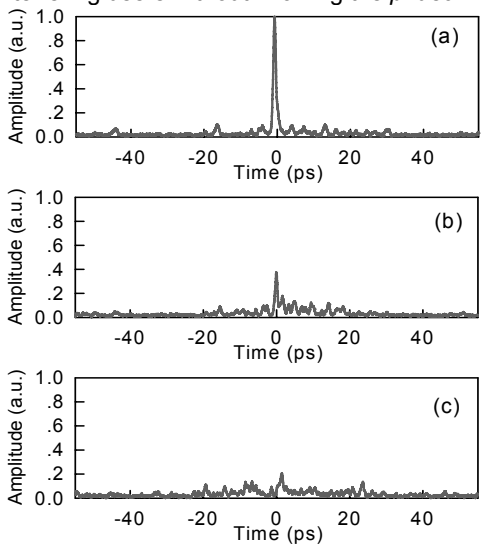

Fig. 2. Cross-correlation traces of the decoded signals (a) with correct phase code and phase-mask, (b) with correct phase code but no phase-mask, and (c) with phase-mask but incorrect phase code.

The bit-error-rate (BER) of the network testbed is taken with respect to the total received optical power at the input to the thresholder. Fig. 3 shows two groups of BER curves. The first group is encoding and decoding without the *phase mask*. The second group is encoding and decoding with the *phase mask*. BER performances of 1-user and 3-user cases are shown in each group. In the 1-user case, only the correctly-decoded intended user is present in the system, while in the 3-user case, 2 interfering users are added. In each case, the testbed achieves error-free performance (BER<10^{-11}). The comparison between the two groups shows that, with the *phase mask*, the testbed still has high performance with some power penalty arising from the mismatch of multi-level phase shifts between the encoder and decoder due to limited resolution within the LC-SLPM.

With the *phase mask* on the encoders, decoding with correct m-sequence but no *phase mask* on the decoder results in measured **BER of 0.5** with appearance of any interfering user. But when there is only one user, by energy detection, error-free detection can still be achieved without knowing the O-CDMA code and *phase mask*, with a ~13 dB power penalty as shown on Fig. 3. Such security vulnerability can be eliminated using a code-switching scheme as discussed in [3, 5].

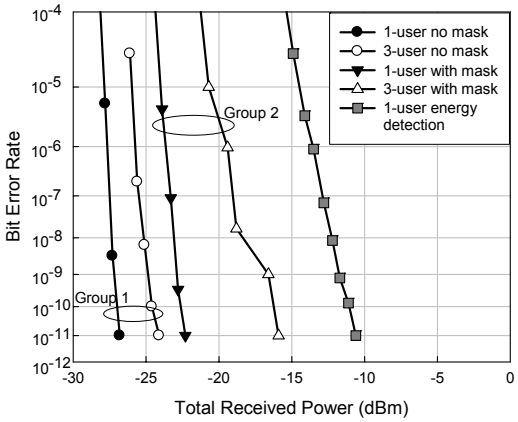

Fig. 3. BER performance of the SPECTS O-CDMA network testbed with and without random phase mask

Conclusions

We have demonstrated the implementation and error-free performance of 3-user SPECTS O-CDMA network testbed with *phase mask*. Cross-correlation and BER measurements prove that confidentiality protection of SPECTS O-CDMA can be improved by applying phase-masking to prevent code exposures to eavesdroppers.

References

1 A. Stok *et al.*, *IEEE Communication Magzine*, **40** (2002), pp 88-87.

2 T. H. Shake, *et al.*, *IEEE Journal of Lightwave Technology*, **23** (2005), pp 1652-1663.

3 F. Xue, *et al.*, *OFC' 06*, (2006), OThT3.

4 R. P. Scott, *et al., IEEE photonics Technology Letters*, **23** (2004), pp 2186-2188.

5 Z. Jiang, *et al., OFC' 06*, (2006), OThT2.

This work was supported in part by DARPA and SPAWAR under agreement number N66001-02-1-8937 and by the AFOSR through the UC Davis Center for Digital Security.