English
Research Express@NCKU Volume 2 Issue 3 - November 16, 2007
[http://research.ncku.edu.tw/re/articles/e/20071116/2.html]

Robust Design for Reconfigurable Coder/ Decoders to Protect Against Eavesdropping in Spectral Amplitude Coding Optical CDMA Networks

Yao-Tang Chang[2], Chuan-Ching Sue[*1], and Jen-Fa Huang[2]

[1] Department of Computer Science and Information Engineering, National Cheng Kung University, Corresponding Author

[2] Department of Electrical and Engineering, Institute of Computer and Communication Engineering, National Cheng Kung

Email : suecc@mail.ncku.edu.tw [1], huajf@ee.ncku.edu.tw [2]

IEEE/OSA Journal of Lightwave Technology, vol. 25, no. 8, pp. 1931-1948, August 2007.

Because the Optical Code-Division Multiple-Access (OCDMA) technique provides a burst and asynchronous multiple-access environment in both the time and the spectral domains, it has attracted considerable attention for application in local-area networks (LAN). However, recently various weaknesses of OCDMA systems are identified, in particular their susceptibility to eavesdropping. Therefore, constructing enhanced security mechanisms for optical CDMA systems becomes an important issue when designing the physical layer in the optical LAN network.

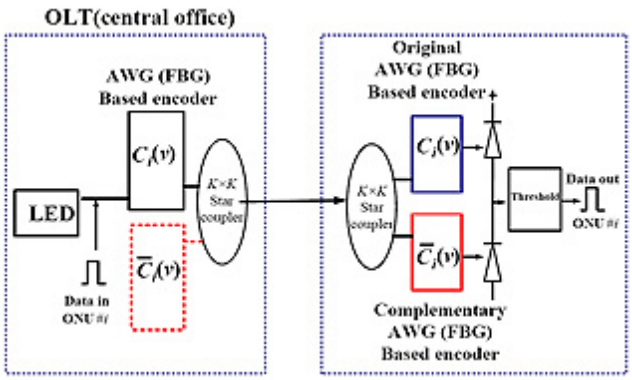

Fig. 1: Block diagram of SAC-OCDMA system.

The concepts of Array Waveguide Grating (AWG)-based or Fiber Bragg Grating (FBG)-based OCDMA encoder/decoders (codecs) are well documented in previous studies and can be illustrated by Fig. 1. Fig. 1 illustrates the use of FBG and AWG routers in a SAC OCDMA scheme. The FBGs and AWGs are prewritten with Walsh-Hadamard code and M-sequence code, respectively, and the scheme is implemented using an Intensity Modulation/Direct Detection scheme based on a low-cost incoherent optical source and balanced photo-detectors. The use of AWG router-based optical network codec pairs for Spectral Amplitude Coding Optical-Code Multiple-Access (SAC-OCDMA) networks integrated with M-sequence code provides a viable means of eliminating lengthy fiber delay lines in the FBG-based design. However, the code matrix assignment is fixed and can not be changed once the connection links between the coupler and the AWG router have been set up.

Two approaches for enhancing network security mechanisms have been suggested in order to protect the network from attack by unauthorized users. The first approach involved increasing the code complexity (i.e., increasing the code space size), while the second involved reducing the subscriber's transceiver power. However, a third approach is for each transmitter to change its code on a frequent basis. In this way, the code is likely to be changed before an eavesdropper has the chance to detect the channel

waveform and solve the code. Although the concept of code-changing is frequently cited as a network security mechanism, the application of this limited-code-complexity reconfiguration approach to SAC-OCDMA networks was not actually demonstrated in the previous studies.

In the current study, the codec design in Fig. 1 is transformed into a reconfigurable scheme by adding an array of 1×2 optical switches and simple electrical shift registers as shown in Fig. 2. The status of each optical switch, i.e., “on” (bar) or “off” (cross), is governed by the state of the electrical shift register, which in turn depends on the current code matrix assignment. This reconfigurable SAC-OCDMA network has the advantages of physical compactness and simplicity since all the network users share a single codec pair. FurthermoreAWG-based encoder and decoder components are centralized at a common location.

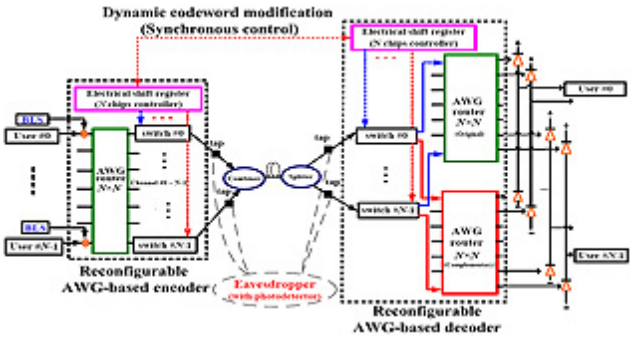

Fig. 2: Dynamic reconfigurable AWG-based SAC-OCDMA network with enhanced eavesdropping protection.

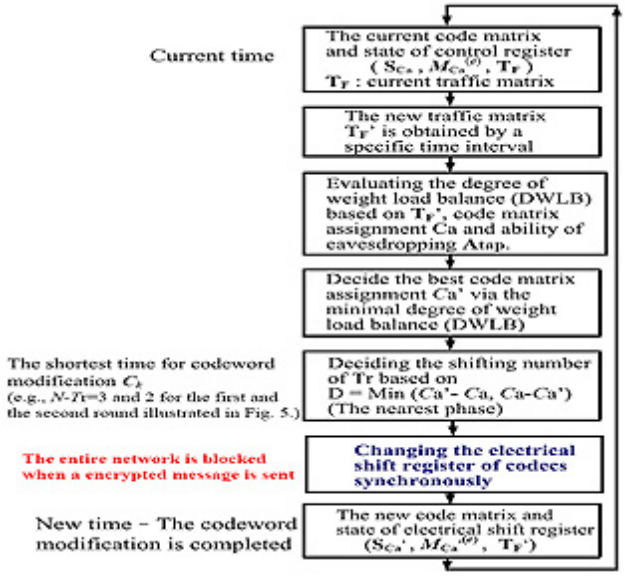

Fig. 3: Proposed reconfiguration policy.

In other words, this study proposes an alternative to huge code space size techniques such as wavelength hopping/time spreading or spectral phase coding for network protection against eavesdropping by using a Spectral Amplitude Coding (SAC) approach in which a unipolar M-sequence is used to generate a specific signature address during the coding process and to retrieve its matching address codeword during the decoding process. A dynamic reconfiguration policy as shown in Fig. 3 is proposed in which the code matrix assignment is changed in response to changing traffic patterns in order to protect the network from attack by unauthorized users. The code matrix assignment is specifically chosen such that it minimizes the degree of weighted load balance (DWLB) and is implemented using simple electrical shift registers.

The performance of the dynamic reconfiguration policy in obtaining the best code matrix assignment when the network is under attack from eavesdroppers of various abilities is investigated as shown in Fig. 4. We also derives the overall signal-to-noise ratio (SNR) of the proposed system based on the phase-induced intensity noise (PIIN), the shot noise and the thermal noise, respectively and show the evaluation result in Fig. 5.

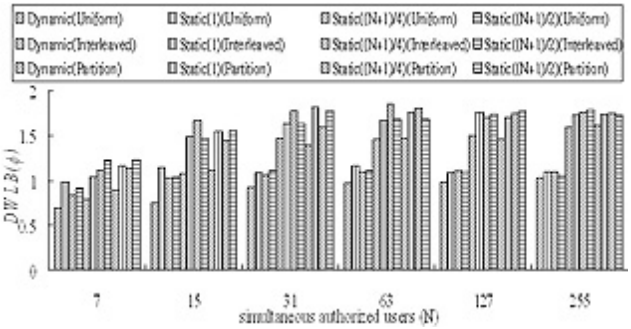

Fig. 4. Comparison of dynamic and static reconfiguration approaches in terms of DWLB for

different ability matrices Atap.

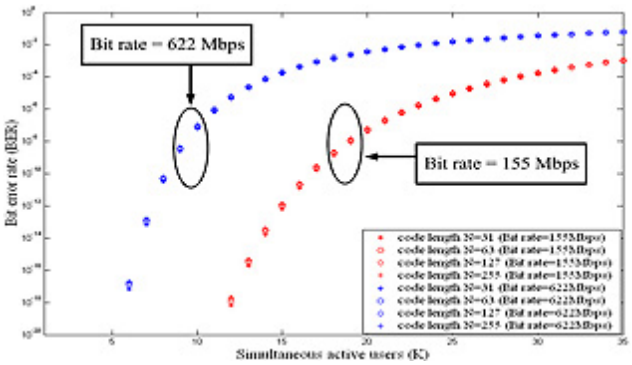

Fig. 5. BER versus number of simultaneous active users for various different code lengths and data bit rates.

In general, the results presented above have shown that the BER increases, i.e., the SNR decreases, at higher data bit rates, e.g., 622 Mbps, and the confidentiality of the network must be reduced at higher data rates. Consequently, in networks characterized by higher data bit rates, the interval at which the proposed scheme should assess the need to reconfigure the code matrix assignment should be reduced to ensure that the network remains adequately protected against eavesdropping attack. Although optical devices (e. g., optical switches) have a shorter processing time than electrical devices (e.g., electrical shift registers), this study additionally uses an electrical shift register to reconfigure the code assignment matrix. To enable the processing time of the current electrical shift registers to approach that of the optical switches, the reconfiguration scheme deliberately adopts a minimum shift-step (Tr) policy. Hence, the time for which the network is blocked during the codeword modification procedure is significantly reduced.

Note that Figs. 2-5 are sourced from Yao-Tang Chang, Chuan-Ching Sue, and Jen-Fa, “Robust Design for Reconfigurable Coder/Decoders to Protect Against Eavesdropping in Spectral Amplitude Coding Optical CDMA Networks”, IEEE/OSA Journal of Lightwave Technology, vol. 25, no. 8, pp. 1931-1948, Aug. 2007.

Copyright 2009 National Cheng Kung University