Confidential Enhancement with Active Reconfigurable AWG-Based Codecs over Fiber-to-the-Home Network

1Jen-Fa Huang, 2Philippe Gallion, 3Yao-Tang Chang, and 1Gallion Li-Wei Chou  
1Institute of Computer and Communications, Department of Electrical Engineering  
National Cheng Kung University, Taiwan, ROC.  
2Group des Ecole Nationale Superieure des Telecommunications, France.  
3National Tainan University of Technology, Taiwan, ROC.  
Phone: (866-6)2757575 ext 62370, FAX: 06-2345482, huajf@ee.ncku.edu.tw

ABSTRACT
By extending a protecting mechanism called anticipative warning time policy to improve previous reconfigurable SAC-OCDMA (i.e., coded WDM) scheme, the active reconfigurable arrayed waveguide grating based (AWG-based) encoder/decoder (codec) architecture is presented to enhance the more data confidentiality in fiber-to-the-home (FTTH) networks. To avoid the huge code space requirements of conventional wavelength-hopping, time-spreading or spectral phase coding approaches, this study applies a spectral amplitude coding (SAC) technique and constructs the signature address codes using unipolar maximal-length sequence (M-sequence) code. Exploiting the inherent cyclic properties of AWG routers, the additional anticipative-warning-time policy is integrated to previous degree of weighted load balance (DWLB) policy and performs the changing codeword algorithm to thwart network attacks by eavesdroppers. Furthermore, the qualitative and quantitative evaluations of the system’s network protection performance are first investigated by assessing the attained degree of confidentiality (DOC). Under the assumption of the brute-force searching attacking, the proposed active changing codeword scheme show that for a system capacity of $N = 127$, the proposed system enhances the data confidentiality in the network by a factor of 8063 times compared to that provided by a conventional wavelength division multiplexing PON (WDM-PON) scheme.

KEY WORDS
Arrayed-waveguide grating (AWG), Fiber-to-the-home (FTTH), Code-division multiplexed passive optical network (CDM-PON), Reconfigurable AWG codecs, Degree of confidentiality (DOC).

1. Introduction
Ethernet Passive Optical Network (EPON) schemes are widely viewed as an ideal solution for first (last) mile access networks. Traditionally, broadband, high-speed transmission schemes such as Time-Division-Multiplexing (TDM) and Wavelength-Division-Multiplexing (WDM) have been applied for Fiber-to-the-Home (FTTH) access networks [1]. However, the transmission characteristics of conventional EPON networks render the network vulnerable to eavesdropping and impersonation when such transmission schemes are employed [2]. Therefore, improving the confidentiality of access networks has emerged as a critical problem in recent years. It has been shown that optical code-division multiple-access (OCDMA) schemes significantly improve the robustness of local area networks (LANs) toward malicious attack [3-4]. However, it is well-known that a sophisticated eavesdropper can utilize various policies such as brute-force searching [5-6] to detect a particular transmitted signal or can use a simple energy detector to detect the presence of energy in a particular bit interval.

Shake [6, 7] suggested two potential strategies for enhancing the robustness of OCDMA networks toward attack by unauthorized users, namely increasing the code complexity (i.e. increasing the code space size) and reducing the subscriber’s transceiver power. However, an alternative, limited-code-complexity approach is to change the code used by each transmitter on a frequent basis such that it is likely to change before an eavesdropper has sufficient time to detect the channel waveform and solve the code. It is assumed that the eavesdropper commences by employing a simple, low-cost energy detector to sense the presence of energy in a particular bit interval and then applies a brute-force searching algorithm to attack the targeted user [5-7].

Following the previous work done the current author [8], the same codec design is transformed into a reconfigurable scheme by adding an array of $1 \times 2$ optical switches and simple electrical shift registers. 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 (i.e., coded WDM) network has the advantages of physical compactness and simplicity since all the network users share a single codec pair.

In this current study, the additional anticipative-warning-time (i.e., the expected time for which an eavesdropper must wait between isolations for the targeted user) policy [7] is investigated and integrated with degree of previous weighted load balance (DWLB) policy [8] and then performs the changing codeword algorithm to thwart network attacks by eavesdroppers. Hence, the active reconfigurable network configured by AWG-based codec at a centralized common location is constructed to provide more enhanced security for authorized users.
The remainder of this paper is organized as follows. Section 2 provides an overview of the AWG-based codecs and discusses the merits of the active reconfigurable CDM-PON system. Section 3 describes the detailed design concepts and mechanisms of the active reconfigurable AWG-based codecs for FTTH networks. Sections 4 integrate the anticipative warning time and previous degree of weighted load balance (DWLB) policy to perform active changing codeword algorithm in against eavesdropping. Section 5 investigates the ability of the proposed scheme to protect the network from attackers using a brute-force attacking strategy. Moreover, section 5 compares the performance of the proposed reconfigurable CDM-PON scheme in enhancing data confidentiality within the network with that of conventional TDM-PON and WDM-PON schemes. Finally, Section 6 presents some brief conclusions and indicates the intended direction of future research.

2. Active Reconfigurable Coded WDM-PON over FTTH

It presents a schematic illustration of the active reconfigurable AWG-based SAC-OCDMA network with enhanced eavesdropping protection shown in Fig. 1. In this network, each authorized ONU shares the same AWG router, but is assigned its own optical switch. The output spectrum of the AWG encoder generated when an incoherent broadband light source (BLS) enters the AWG is characterized by an inherent cyclic property. As shown in Fig. 1, \( N \times 2 \) optical switches are set up at the decoder in front of the original and complementary AWGs. The states of these switches, i.e. “on” or “off” are determined by the elements in an electronic shifting control register, i.e. “1” or “0”, where “1” turns the switch “on” and “0” turns the switch off.

By integrating the optical switches with a control register and an appropriate code matrix assignment policy (i.e. an active codeword modification policy), this study accomplishes an active reconfigurable AWG-based codec with an enhanced ability to protect the network from attack by unauthorized users.

In Fig. 1, the permutable codeword key, which determines the required number of register shifts in accordance with the minimal degree of weighted load balance (DWLB) or anticipative warning time policy, requires the implementation of a synchronous control mechanism at the encoder and decoder. Here, the changing codeword algorithm is employed to thwart network attacks by eavesdroppers. In the same way as previous study [8], it is assumed that a protocol is used to block the entire network temporarily while the control registers at the encoder and decoder are updated synchronously.

3. Active Reconfigurable AWG-based Codec

Following the previous work done by current author [8, 9], this study applies a spectral amplitude coding (SAC) technique and constructs the signature address codes using unipolar maximal-length sequence (M-sequence) code. By exploiting the inherent cyclic properties of AWG routers, a control register state \( \mathbf{S} \) is written as M-sequence code pattern to control individual \( 1 \times 2 \) optical switch and code matrix \( \mathbf{M} \) (i.e., M-sequence code family) is then appeared in output port of coded AWG routers.

Simplicity, given a network with seven ONUs (\( N = 7 \)) and a control register state of \( \mathbf{S}_i = (1110010) \) (designated as Initial State #1), \( \mathbf{M} \) has the form shown in Fig. 2. As described above, the \( k \)-th row of \( \mathbf{M} \) denotes the \( k \)-th channel originating from the output port of the active reconfigurable AWG-based encoder.

The first column of \( \mathbf{M}_1 \) (enclosed by a red rectangle in Fig. 2) is encoded as \((\lambda_1^{(1)}, \lambda_2^{(1)}, 0, 0, 0, 0, 0)\) and is assigned as the codeword for ONU #1 originating from the first input port of the AWG. Similarly, the second column of \( \mathbf{M}_2 \) is encoded as \((0, \lambda_2^{(2)}, \lambda_3^{(2)}, 0, 0, 0)\) (and is assigned as the codeword for ONU #2 originating from the second input port of the AWG). In the same way, the sixth column of \( \mathbf{M}_6 \) (also enclosed by a red rectangle) is encoded as \((0, 0, 0, 0, 0, \lambda_7^{(6)})\) and is assigned as the codeword for ONU #6 coming from the sixth input port of the AWG.

At the decoder end, the Fig. 3 presents an illustrative example of the active reconfigurable AWG-based decoder. For a state \( \mathbf{S}_i = (1110010) \), input ports #1, #2, #3 and #6 of the original active reconfigurable AWG-based decoder are unimpeded, but the other input ports are closed. Meanwhile, input ports #4, #5 and #7 of the
complementary active reconfigurable AWG-based decoder are unimpeded, but the other input ports are closed. For each ONU, a pair of photo-detectors is employed to perform the correlation subtraction of the output port signals of the original and complementary active reconfigurable AWG-based decoders in order to recover the data bit of each ONU.

4. Evaluation of anticipative-warning-time for Anti-Attacking

Adopting the same definition of the combinations per second as that given in Fig. 1 of Ref. [5], this study evaluates the anti-attacking ability of the proposed scheme when the eavesdropper applies a brute-force attacking strategy. Subsequently, by considering the expected time for which an eavesdropper is constrained to wait between isolations for a particular user [6] (i.e. the so-called anticipative warning time), the study investigates the effectiveness of the active codeword modification policy in enhancing the confidentiality of the proposed scheme.

When the simultaneous active users are active at any time, the reconfigurable SAC-OCDMA policy based on DLWB strategy have been demonstrated in the previous done work [Fig 6, 8]. Since the simultaneous active users may decrease to only one as the eavesdropper is attacking, this section further estimates the time for which the proposed scheme suffers a threat of confidentiality based on the expected time for which an eavesdropper has to wait between isolations for a particular user [6] (referred to hereafter as the anticipative warning time).

Combining the DLWB and below-mentioned policy based on anticipative warning time, the changing codeword mechanism is shown as Fig. 4. If the anticipative warning time is up, it decides an optimum shifting number of $T_r$ [Fig 5, 8] immediately to carry out the changing codeword mechanism. Otherwise, the DWLB is used as an index to change the codewords of all the users simultaneously at a specified trigger time. Following the [8], the degree of weighted load balance (DWLB) characterizes the efficiency of the code matrix assignment $C_a$ in meeting the traffic matrix demands, denoted by $T_F$, weighted by the ability of the eavesdropper, $A_{tap}$. The degree of weighted load balance (DWLB, $\phi(C, T_F)$) can be used to evaluate the distance between the maximal element $w_i$ of the weighted deviation feature $W$ and the average $\sum_{i=1}^{N}w_i/N$. Subsequently, a minimum shift-step ($T_r$) value [8] is determined by the best code matrix assignment $C_a$ when the current active reconfiguration policy is triggered to further minimize the time required to change the codeword.

In practical, the implementation of current active changing codeword mechanism requires the use of a synchronous mechanism to communicate the trigger time at which to carry out the changing codeword process and update the electrical shift register, respectively, from the encoder to the decoder. Hence, the total time for which the network is blocked, as the user codewords are modified, is considerably reduced.

![Fig. 3. Active reconfigurable AWG-based decoder controlled by state registers: (1110010)](image)

![Fig. 4. the active reconfigurable algorithm extending from Fig.6 of reference [8]](image)

Regarding the anticipative-warning-time situation under which the network confidentiality faces the greatest threat (referred to as the “weakest scenario”) is that in which only the targeted ONU (i.e., the ONU whose signal the eavesdropper wishes to obtain) is transmitting a data bit one, while the other ONUs are silent.

For an ONU capacity of $N$, an assumption is made that the transmitted data bits of the various ONUs are equally likely to be “one” or “zero”. Furthermore, it is assumed that the ONUs all transmit at a data rate of $B$ bits/s. Hence, the probability that only $K$ ONUs transmit a data bit of one while the other ONUs (i.e. $N-K$ ONUs) simultaneously transmit data bit zero is given by:

$$P = C_K^N \times \left(\frac{1}{2}\right)^K \times \left(\frac{1}{2}\right)^{N-K}$$

(1)

Substituting $K = 1$ into Eq. (1) to reflect the weakest scenario in which only one ONU transmits a data bit of one, this probability becomes:

$$P = N^2 \times \left(\frac{1}{2}\right)^N$$

(2)
Accordingly, the anticipative warning time of the proposed active reconfigurable coded WDM-PON is given by:

\[ 2^N / (N^2 \times B) \]

(3)

where \( B \) denotes the bit rate and is a constant for each of the ONUs in the network.

Figure 5 illustrates the variation of the anticipative warning time with the number of simultaneous active users as a function of the bit rate, \( B \). It is observed that the required anticipative warning time increases with an increasing number of simultaneous active ONUs or with a decreasing bit rate. Regarding the confidentiality of the proposed scheme, Fig. 5 shows that a trade off exists between the anticipative warning time and the bit rate when the number of simultaneous active ONUs is fixed. As a consequence, for a constant number of simultaneous active ONUs, the codeword must be modified more frequently as the bit rate increases.

Figure 5 also provides the means of determining an appropriate codeword modification policy, i.e. the DWLB policy or a constant anticipative warning time policy, on the basis of the current number of simultaneous ONUs. In the particular example shown in Fig. 5, the network supervisor specifies a time of 10 minutes as a tolerable attacking time, i.e. he or she feels that the network is capable of resisting an eavesdropper’s attack for 10 minutes.

Accordingly, for \( K \geq 45 \), the network is secure since the anticipative warning time is higher than the specified value. Hence, the codeword modification procedure can be triggered using the anticipative warning time policy. Conversely, when \( K < 45 \), the network is less secure since the actual anticipative warning time may be less than the tolerable attacking time. To avoid the risk of the eavesdropper successfully accessing the network, the codeword is therefore modified in accordance with the DWLB policy.

From the discussions above, it is clear that the choice of an appropriate codeword modification policy depends on the number of currently active ONUs. In the example above, \( K = 45 \) represents the critical number of active ONUs. However, if the network supervisor were to specify a tolerable attacking time of 1 hour rather than 10 minutes, the critical number of simultaneous active ONUs would increase to approximately 50.

In the proposed OCDMA-EPON scheme, each ONU is assigned a unique signature address code such that packets from/to different ONUs can be easily identified. The proposed scheme not only reduces the processing time, but also resolves the collision problem arising from the simultaneous arrival of multiple active packets at the OLT or ONUs. In addition, since the functionality of the AWG-based codec used to implement the OCDMA-EPON scheme is based on the correlation property of the underlying coding pattern, the scheme requires the use only of a straightforward wavelength-selective filter rather than sophisticated wavelength controllers such as those used in WDM schemes. Furthermore, in the proposed SAC-OCDMA scheme, the signals of all the active users are mixed via an optical coupler prior to transmission, and therefore the network confidentiality is considerably enhanced.

As a result, the proposed SAC-OCDMA scheme provides a more promising solution for FTTH access networks than conventional WDM-EPON schemes [10-11].

5. Confidentiality Performance of Proposed Scheme

Although robust data confidentiality is frequently cited as an advantage of conventional coded WDM signaling, this technique is susceptible to eavesdropping since energy is present when a data bit one is transmitted, but is absent when a data bit zero is transmitted. Furthermore, many of the studies relating to coded WDM schemes presented in the literature neglect the issue of network confidentiality. Accordingly, the present study performs a qualitative analysis of the enhanced confidentiality provided by the proposed active reconfigurable coded WDM scheme, and calculates the degree of confidentiality afforded against an eavesdropping attack executed using a simple photodetector.

5.1 Eavesdropping protection mechanism

Figure 6 illustrates the scenario where an eavesdropper attempts to tap into a desired signal by using a simple energy detector to sense whether or not energy is present in a particular bit interval. Note that an assumption is made here that the eavesdropper selects the most cost-efficient attack strategy in attempting to attain the power distribution pattern \( E \) in each tapped channel.

The enhanced confidentiality provided by the active reconfigurable coded WDM-PON scheme proposed in this study arises in part because the AWG-based codecs are centralized at a common location. As stated in the Introduction, Shake [6] advocated frequent changes of the individual ONU codewords in order to limit the time available for an eavesdropper to break the code. As described in Section 3, the current coded WDM-PON employs a spectral amplitude coding (SAC) approach using a unipolar M-sequence code matrix to generate a
specific signature address (coding) for each ONU and to retrieve its matching address codeword (decoding). The confidentiality of the current system is enhanced by adopting Shake’s recommendation in [6] to modify the codewords on a frequent basis by integrating the active reconfigurable AWG-based codecs with the active codeword modification algorithm presented by the current authors in [9].

As illustrated in Fig. 2, and reported in previous studies of AWG-based codecs by the current authors [8], the mapping power distribution pattern E of the codec output ports depends both on the settings of the optical switches and the nature of the data bits (i.e. “1” or “0”). Note that the states of the two shifting control registers vary strictly in accordance with the current M-sequence patterns, i.e. 1110010, 0111001, 1011100, 0101110, 0010111, 1001011, and 1100101. For a system capacity of N = 7, a power distribution pattern of E₁ = [K, K, K, 0, 0, 0, 0] is obtained when the control register is in a state of S₁ = [1, 1, 1, 0, 0, 1, 0]. Note that in E₁ the value of element K indicates the number of simultaneous active ONUs, i.e. the number of ONUs transmitting a data bit of one. Similarly, when the control register has a state of S₂ = [0, 1, 1, 1, 0, 0, 1], a power distribution pattern of E₂ = [0, K, K, K, 0, 0, K] is obtained, i.e. a right shift of one place with respect to E₁. The power distribution patterns E₁ to E₇, corresponding to control register states S₁ to S₇ are derived in a similar manner. From the eavesdropping perspective, when the power distribution pattern of E₂ = [0, K, K, K, 0, 0, K] is obtained, the eavesdropper knows that a total of K ONUs are simultaneously transmitting data bits one, but, crucially, is uncertain which of the N ONUs are active. In other words, in the current case of N=7, and assuming that K=2 in the power distribution pattern, the eavesdropper must test a total of C₇² = 21 combinations to establish exactly which two ONUs are transmitting data.

As implied above, when K ONUs transmit a data bit of one, the eavesdropper must test a total of Cᴺᴷᴺ = N!/K!(N-K)! combinations in order to achieve a correct detection result. Hence, in practice, the eavesdropper has no idea which K ONUs (i.e. users) are currently transmitting a data bit of one (or equivalently, which N-K ONUs are transmitting a data bit of zero). Furthermore, since the codewords employed in the proposed scheme are reconfigured in accordance with the state of the register controller, the number of combinations which the eavesdropper must test increases to N×Cᴺᴷᴺ = N×N!/K!(N-K)!], where N=7, 13, …, 127 in the current M-sequence code.

In other words, the probability of achieving a correct detection result, i.e. establishing the nature of the data bit transmitted by the targeted user, Pₑ, in the current active reconfigurable coded WDM PON scheme is given by:

\[ Pₑ = 1/(N×Cᴺᴷᴺ) \]  

(4)

Figure 6 shows the situation where the same power distribution pattern of E = [2, 2, 2, 0, 0, 2, 0] is obtained for two different transmitted data bit distributions of [1, 0, 1, 0, 0, 0, 0] and [0, 0, 0, 0, 1, 0, 1], respectively. The elements in the power distribution pattern correspond to the summed energies of the individual wavelengths in each channel. In this case, it is clear that even when tapping into each channel using a simple energy detector, the eavesdropper will most likely fail to identify the data bit of the targeted ONU using an inverse function operation. In this particular example, the eavesdropper has a probability of 1 in 21 (i.e. C₂¹) of achieving a correct detection result.

5.2 Degree of confidentiality of proposed scheme

Figure 7 illustrates the ability of the eavesdropper to successfully detect a specific power distribution pattern E for different numbers of simultaneous active ONUs (i.e. users) in systems of different capacities. It is clear that the eavesdropper’s ability is dependent on the number of simultaneous active ONUs, i.e. K. When each ONU simultaneously transmits a data bit of one, there is a 100% probability of the eavesdropper achieving a correct detection result, i.e. Cᴺᴷᴺ = 1. However, as the number of active ONUs (K) reduces toward one half of the total system capacity (N), the ability of the eavesdropper to acquire the desired user’s signal is significantly impaired. Consider the case of N=127. When the number of active ONUs is approximately half the total system capacity, the probability of a correct detection reduces to 10⁻³⁸ (i.e. Pₑ = 1/N×Cₑ₆³¹₂⁷).
In general, Fig. 7 shows that network confidentiality is higher in systems with larger total capacities in which approximately half of the ONUs are active at any one time. The degree of confidentiality (DOC) of the system is defined as the reciprocal of the average probability of correct detection, $P_C$, i.e.,

$$\text{DOC} = \frac{1}{\left(\sum P_C\right)/(N+1)}$$

(5)

Since in TDM-PON and WDM-PON schemes, the data bits of each ONU are broadcast to every ONU in the network, and furthermore each ONU is assigned a unique wavelength, the WDM-PON scheme achieves a DOC of $N$, while the TDM-PON scheme achieves a DOC of 1 ($C_N^N = 1$).

As shown in Fig. 8, in the proposed active reconfigurable SAC-OCDMA-PON (coded WDM-PON) scheme, the DOC increases significantly with an increasing system capacity $N$. The evaluation results show that the DOC of the proposed WDM-PON scheme is improved by a factor of 111 times compared to that of a conventional WDM-PON for a system capacity of $N = 7$ and by a factor of 8063 times for an ONU capacity of $N = 127$.

6. Conclusion

By extending a protecting mechanism called anticipative warning time policy to improve previous reconfigurable SAC-OCDMA scheme, the active reconfigurable arrayed waveguide grating based (AWG-based) encoder/decoder (codec) architecture is demonstrated.

The evaluation results have shown that the proposed active reconfigurable coded WDM-PON scheme achieves a higher degree of data confidentiality than conventional TDM- and WDM-PONs. Specifically, the proposed scheme improves the DOC by a factor of 8063 times compared to a conventional WDM-PON for a system capacity of $N = 127$.

To thwart eavesdropper attacks, the proposed scheme is integrated with an active codeword modification policy in which the requirement to modify the codeword is triggered either by the DWLB codeword modification policy proposed by the current authors or the anticipative warning time depending on the number of simultaneous active users. A more sophisticated mechanism for active determining the appropriate codeword modification policy will be addressed in a future study.

Acknowledgements

This study was supported by the Advanced Optoelectronic Technology Center, National Cheng Kung University, under NTP-GET projects from the National Science Council (96-2219-E-006-010-) of Taiwan.

References

