中文

成大研發快訊　第二卷 第三期 - 2007年十一月十六日
[http://research.ncku.edu.tw/re/articles/c/20071116/2.html]

在頻譜振幅編碼的光分碼多工網路中設計一個可防止竊聽而且具穩健特性的可重組態的編解碼器

張耀堂[2]，蘇銓清*[1]，黃振發[2]

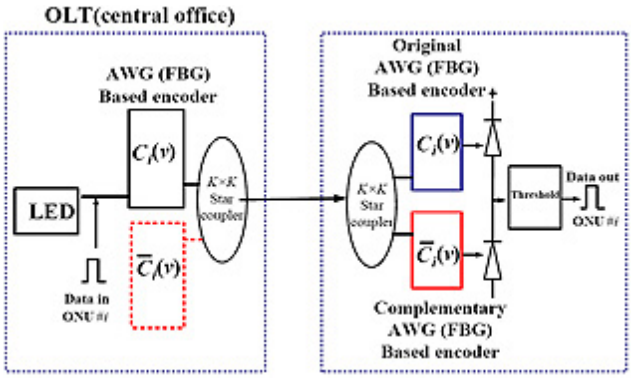
[1] 國立成功大學 資訊工程系, 通訊作者

[2] 國立成功大學 電機工程系暨電腦與通訊工程研究所

電子信箱 : 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.

光分碼多工技術(OCDMA)由於可以在時域(time domain)及頻域(spectral domain)上達到巨量(burst)及非同步(asynchronous)的多重存取(multiple access)環境，非常適合應用在區域網路(local area networks)領域，因此吸引了學者在光分碼多工技術投入相當的研究。然而有研究學者指出光分碼多工網路在面對竊聽者(eavesdropper)的竊聽(eavesdropping)攻擊仍然存在許多的缺點。因此建立一個具更佳安全性的光分碼多工系統於實體層上是一個極重要的課題。

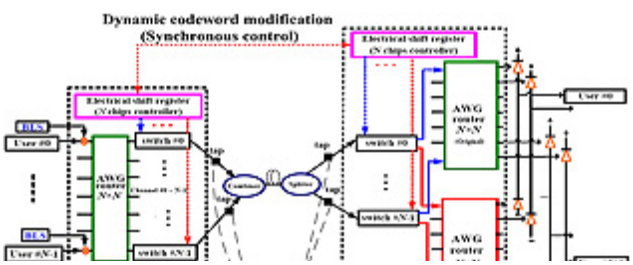


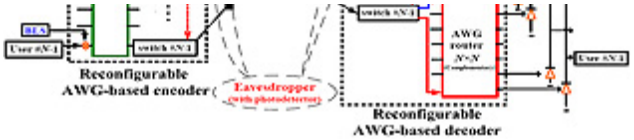
圖一: 頻譜振幅調變光分碼多工系統區塊圖

以陣列波導柵欄(Array Waveguide Grating)或光纖布拉格柵欄(Fiber Bragg Grating)來實作光分碼多工的編解碼器(encoder/decoder)的觀念在之前的研究已被大量實現，我們可以利用圖一來說明。圖一顯示以陣列波導柵欄(AWG)或光纖布拉格柵欄(FBG)來實作頻譜振幅編碼(spectral amplitude coding)的機制。陣列波導柵欄(AWG)或光纖布拉格柵欄(FBG)分別以預先設計的最大順序碼(M-sequence code)及Walsh-Hadamard 碼來設計。而且這種機制一般都是以低成本的incoherent光源及balanced光感測器實作強度調變(Intensity Modulation)及直接偵測(Direct Detection)來完成。值得注意的是使用陣列波導柵欄(AWG)結合最大順序編碼(M-sequence code)的實作可以消除在以光纖布拉格柵欄(FBG)的實作上所使用大量光纖延遲線路。然而以陣列波導柵欄(AWG)為主的光分碼多工網路的碼矩陣分配是固定無法更動的，因此只要選定一組編碼，則所有在光耦合器及陣列波導柵欄(AWG)間的所有光纖連結也會跟著固定下來。

針對光分碼多工網路實體安全性(security)如何來避免被未經授權(unauthorized)的使用者攻擊，研究學者曾建議了二個方法來加強。第一種是增加碼的複雜度，也就是增加碼的空間度(code space)，其次是減少傳送所使用的能量，使攻擊者無法取得足夠的資訊以供解碼。然而，還有一個方法是讓每一個傳送器經常地改變編碼的碼型。藉由這種方式，碼型便可以在竊聽者偵測並解出碼型前作改變。這種變碼的觀念雖然已有學者提過，但如何將一個有限的編碼複雜度的最大順序編碼實作在可變碼的光分碼多工的網路上並沒有任何學者進行過研究及探討。

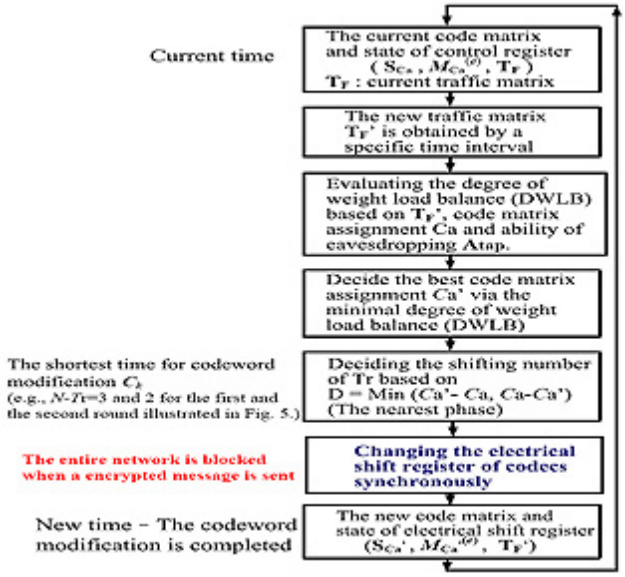
目前這個研究便是將圖一中的編解碼器轉換成一個可重組態(Reconfigurable)的編解碼器。這個可重組態(Reconfigurable)的編解碼器主要是增加一列的1x2的光切換器(optical switch)及簡單的移位暫存器(electrical shift register)，我們以圖二來表示。值





圖二:動態可重組陣列波導光柵為主的頻譜振幅調變光分碼多工系統區塊圖

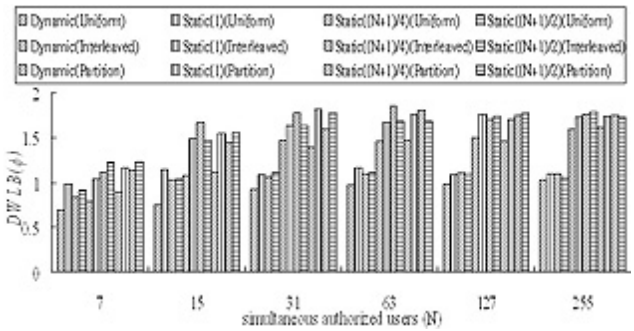
得注意的是每個光切換器(optical switch)的狀態不管是開或關(“on” (bar) or “off” (cross))都是由移位暫存器(electrical shift register)來控制,而移位暫存器(electrical shift register)的值則是決定於目前設定的編碼矩陣。這樣設計的可重組態(Reconfigurable)的編解碼器有一些優點，如實體上所有的網路使用者都共用同一個編解碼單元使得實體層的設計更加簡化，也因為所有的編解碼器都位於同一個地方，對於網路安全性可以提供一個更佳的保密性



圖三: 提出的可重組態策略

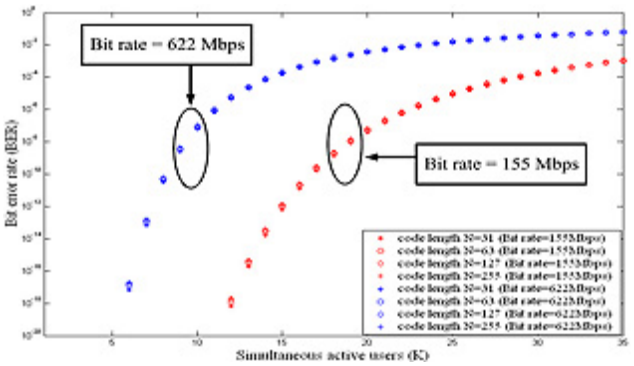
事實上，我們的研究是提出另一種不同於利用大量碼空間的技術如波長跳頻加上時間展頻，或是利用頻譜相位編碼，而是利用簡單的頻譜振幅編碼加上最大順序編碼來產生特定的識別位址(signature address)，並且於解碼過程中利用簡單的比對技術(matching)取出相對應識別位址(signature address)上的資料。為了避免遭到未經授權的使用者利用竊聽來攻擊，我們實作了一個動態可重組態的策略，並將其呈現在圖三中。這個策略主要是說明我們的變碼時機是根據網路上所傳播的資訊的安全性來作出變碼的決定。而網路上所傳播的資訊的安全性在這篇研究中是以具權重性的負載平衡性(Degree of weighted load balance)來評估。所以動態可重組態的策略是動態地改變編碼矩陣使其權重性的負載平衡性最小化，並以最少的時間來完成變碼的動作。

在圖四中，我們將各種竊聽者能力考量下的所有方法所得到的權重性的負載平衡性(DWLB)的值作一個比較，發現在interleaved及partition的竊聽模型下，我們所提的動態可重組態策略的改善幅度是比另一種uniform的竊聽模型還大。我們也推導了所提的光分碼多工系統的訊號雜訊比(signal-to-noise ratio (SNR))，共考慮了三種雜訊因子包含相位雜訊(the phase-induced intensity noise (PIIN))，發射雜訊(the shot noise) 及 熱雜訊(the thermal noise)。而其結果以圖五的訊號錯誤率(BER)來呈現。



圖四: 比較動態及靜態的可重組態策略於不同的竊聽者能力模型下的權重性的負載平衡性

圖五中顯示訊號錯誤率(BER)在較高的傳送速率如622 Mbps時是會比低傳送速率155Mbps時來得高，也就是整體網路的私密度在高傳輸率時是會比較小的。因此在標榜高傳輸率的網路中愈需要作安全性的提昇，也就是愈需要重組態編碼矩陣使整體網路免於被竊聽。因為光切換器比起移位暫存器有比較小的處理時間，因此我們為了使得整體處理時間最小，我們的目標即是最小化移位暫存器的移位動作時間(a minimum shift-step (Tr) policy)。所以網路因為變碼所需的暫停時間便會大幅減少。



圖五:訊號錯誤率在不同的碼長度，傳輸速率及不同使用者下的大小

本文中的圖二至六的來源是取自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.