Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 94 (2016) 240 – 247

Procedia
Computer Science

The 11th International Conference on Future Networks and Communications
(FNC 2016)

Illustrative signature keys reconfiguration to combat with eavesdroppers in wavelength-coded optical access networks

Jen-Fa Huang*, Kai-Sheng Chen, Ting-Ju Su

Advanced Optoelectronic Technology Center, Institute of Computer and Communications Engineering, Department of Electrical Engineering, National Cheng Kung University, Tainan, Taiwan.

Abstract

In order to enhance data transmission security within internet network, this paper consider a signature reconfiguration scheme over wavelength-coded network coder/decoders (codecs). We propose the reconfiguration scheme of composite signatures in which optical network codecs reconfigure their signature keys in a tractable way to enhance system confidentiality for coded wavelength-division multiplexing (WDM) transmissions. Based on conventional maximal-length sequence (M-sequence) codes over arrayed-waveguide-grating (AWG) codecs, composite signatures of relative prime-length M-sequence codes are structured to identify network node users. Network codecs change their signatures dynamically such that eavesdroppers cannot keep up with the speed of code changing, and thus unable to detect the channel waveform to descramble the code. Evaluated results show the effectiveness of the proposed approach via composite signatures reconfiguration against practical eavesdropping.

Keywords: Composite signature keys; maximal-length sequence (M-sequence) codes; wavelength-division multiplexing (WDM), network confidentiality, arrayed-waveguide grating (AWG).

1. Introduction

Coded wavelength-division multiplexing (WDM) is an attractive multi-user technique in local area networks (LANs) and the first mile[1]. Interest in coded-WDM has been steadily growing in recent decades. This trend, as a pragmatic solution for residential access, is accelerating due to the maturity of the optical fibre in the first mile and the establishment of passive optical network (PON). Coded-WDM is a promising technique for next-generation broadband access networks as it provides the following advantages: Asynchronous access capability, accurate arrival time

* Corresponding author. Tel.: +886-6-2757575 ext. 62370; fax: +886-6-234-5482.
E-mail address: huajf@ee.ncku.edu.tw

doi:10.1016/j.procs.2016.08.037

measurements, user allocation flexibility and the ability to support variable bit rates[2-4]. However, weaknesses, including susceptibility to eavesdropping, have recently reported in coded-WDM systems[5-7].

As respectively noted by Prucnal[8.9] and Shake[10], coded-WDM techniques suffer from inherent security disadvantages. In such systems, an eavesdropper can use a simple energy detector to detect whether energy is present or not in each bit interval. In such cases, there is no security at all because the energy detector output contains the user's data stream. Also, a coded-WDM encoder uses the same fixed code repeatedly over a large number of bits. Consequently, an eavesdropper equipped with a sophisticated detector on the path to an isolated single user may be able to tap into the network and recover specific code, under sufficient signal-to-noise ratio (SNR). Thus, to ensure the network security in the physical layer, enhanced confidentiality mechanisms incorporating composite signature codecs is proposed in coded-WDM data systems.

Data network confidentiality can be enhanced by optical signal processing. Among these methods, three main approaches are adopted: Increasing code-space size[10], reducing subscriber transceiver power and frequently changing signature codes[11]. By employing the third approach, eavesdroppers cannot keep up with the speed of code changing, and thus fail to detect the channel waveform to descramble the code. Early incoherent wavelength-coded multiple-access networks used pseudo-orthogonal sequences to encode signals in the time domain. However, the length of the resulting codes was considerable, and multiple-access interference limited the number of users simultaneously accessing the system. Huang[12] proposed a reconfiguration scheme based on conventional maximal-length sequence (M-sequence) codes over arrayed-waveguide-grating (AWG) codecs. The most significant advantage of composite M-sequences is its cycle characteristics. This property can be used in data security mechanisms to secure network communications, as well as increasing the capacity by adding users to a common channel and eliminating interferences and crosstalk.

In this paper, we adopt a dynamically reconfigurable mechanism over the spectral-amplitude-coding (SAC) scheme of coded-WDM to counter eavesdropping. Relative prime-length M-sequences are composed of composite code sets to govern a reconfigurable network that protects users from tapping by changing signatures. Furthermore, we structure AWG codec pairs, along with the corresponding switches, to implement complex coding in the proposed system. By exploiting linear cyclic, periodic, and virtually orthogonal characteristics of M-sequence codes, we exemplify signature reconfiguration over AWG-based network codecs in this work.

The remainder of this paper is organised as follows: Section 2 briefly outlines the dynamic reconfiguration scheme consisting of composite signatures of M-sequence codes. Section 3 describes how the proposed reconfigurable scheme operates to prevent eavesdroppers from solving the user's code, resulting in improved security. Section 4 analyses the security performance of the proposed signature coding and reconfiguration scheme. Section 5 quantifies the probability intercepting into the degree of network confidentiality. Finally, Section 6 summarizes and presents our conclusions.

2. Structure of composite signature codecs for coded-WDM network

To enhance network confidentiality, the proposed codec dynamically changes its signature keys by cyclically right-shifting one chip in a fixed period. The change is based on the assumption that the upper layers of the network can effectively detect the eavesdroppers. The reconfiguration command changes the signature code to a new one. If a tapper attacks the network frequently, the change time becomes short, making the optical switch operate faster to reconfigure the codes so that the tapping process is blocked. On the other hand, if the network is mostly in a secure environment, the frequency of signature code changing is less. The detailed specifications for the central controller node are considerably complex and are beyond the scope of this paper. Interested reader can refer to the article[13] for more information. Figure 1 shows how the composite signature codecs are reconfigured to enhance coded-WDM network confidentiality.

At the transmitter, the downlink signal is modulated by a broadband light source (BLS). The sending signal is encoded by two AWGs to achieve coding encryption. Then encrypted signals are integrated by a star coupler and transmitted to a fiber channel. When the center node receives an abnormal eavesdropping message, it sends a synchronous control signal to the receiving ends to change the codes. At the receiver, two groups of AWGs including the identical and complementary codes are used to decode the received signals. The central node monitors all network traffic in real-time, which may has a heavy burden since all traffic must pass through it.