ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 7, Issue 11, May 2018

# Eavesdropping Detection based on Power-Comparisons to Reconfigure Signature Keys in Optical Coding Access Networks

Chao-Chin Yang[a],Kai-Chun Lin[b],Jen-Fa Huang[b], Chien-Sheng Chen[c]
[a]Department of Electro-Optical Engineering, Kun Shan University, Tainan, Taiwan.
[b]Department of Electrical Engineering, National Cheng Kung University, Tainan, Taiwan.
[c]Department of Information Management, Tainan University of Technology, Tainan, Taiwan.

***Abstract:*** ***In this paper, a scheme of signature code reconfiguration over optical code-division multiple-access (OCDMA) network is proposed to enhance multiple-users data transmission security. The security scheme is devised on the basis of two mechanisms: (1). Eavesdropping detection based on power comparison in local node; (2). Signature codes reconfiguration in each node on command of central control station. On eavesdropping detection, we sense significant power change while communicating nodes pair is suffering malicious attack. On signature reconfiguration, central station sends commands to the communicating transceiver nodes to change their signature keys. We illustrate with maximal-length sequence (M-sequence) codes as signature keys to the network nodes. These signatures are structured over arrayed-waveguide gratings (AWGs) devices. When eavesdropping occurs on aspecific network user, new code sequence is selected for the signature code reconfiguration in order to combat the behavior of eavesdropping. Simulation result shows that the spectral amplitude drops obviously after eavesdropping and the threshold value can be determined in order to detect the eavesdropping effectively.***

*Keywords:* **Maximal-length sequence (M-sequence) codes, Optical code-division multiplexing access (OCDMA), network confidentiality, arrayed-waveguide grating (AWG), eavesdropping detection.**

## I. INTRODUCTION

Optical code-division multiple-access (OCDMA) is an attractive multi-user technique in local area networks (LANs) and in the first mile [1]. Interested in OCDMA 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 fiber in the first mile and the establishment of passive optical network (PON). OCDMA is a promising technique for next-generation broadband access networks as it provides the following advantages: Asynchronous access capability, accurate arrival time measurements, user allocation flexibility and the ability to support variable bit rates. However, weaknesses, including susceptibility to eavesdropping, have been reported in OCDMA systems [2]-[4].

As respectively noted by Prucnal [5] and Shake [6], OCDMA 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, an OCDMA 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).

Data network confidentiality can be enhanced by optical signal processing. Among these methods, three main approaches are adopted: Increasing code-space size, reducing subscriber transceiver power and frequently changing signature codes. 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 OCDMA 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 [7] 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 periodic and cyclic 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 [8], a security-architecture for Software-Defined-Network (SDN) is proposed. This architecture is design to avoid the flow rule attack that can lead severe influence on network. The concept of the scheme is that flow rules are no longer from a single controller, for multiple controllers take part in judging which controller produces valid rules. Therefore, when attackers try to charge numerous controllers simultaneously, the cost and difficulty are increased remarkably. However, we utilize a similar concept, implementing in the OCDMA network as the controller architecture which can detect the abnormity such as tapping of eavesdropper, and selects the corresponding solution to combat the attack.

Existing methods applied to detect tapping attack are: (1) Power detection method, which applies power detection techniques to detect the loss of the power ; (2) Optical spectral analysis method, which using an optical spectrum analyzer (OSA) to measure the drop of channel power when there is an eavesdropping; (3)Pilot tone methods that the pilot tones are signals that travel along the same links as the communications data but which are distinguishable from that data for the purpose to detect transmission disruptions. However, a new method for detecting attacks is presented in [9]. This method is based on the notion that the input and output signals of the detected device behave a mathematical relationship that is known by the central station. Therefore, a comparison of the input and output signals might be able to detect an attack if the some value of the signal parameters does not conform to an a priori known set of parameters. We will investigate such optical signal power degradation due to eavesdropping attack in OCDMA networks.

In this paper, we adopt a dynamically reconfigurable mechanism over the spectral-amplitude-coding (SAC) scheme of OCDMA to combat with eavesdropping. In the proposed reconfiguration scheme, innovative eavesdropping detection based on input/output power-comparisons around the OCDMA receiver decoder is investigated. When an eviltapping is detected on a specific user, that user’s signature code would then be reconfigured to counteract with the behavior of eavesdropping.

The remainder of this paper is organized as follows: Section 2 outlines the proposed mechanism of signature code reconfiguration. In Section 3, we briefly introduce the eavesdropping strategy in OCDMA networks andthe proposed eavesdropping detection scheme based on power comparison and the mathematical derivation of threshold value which determines whether there is an eavesdropping or not. In Section 5, an example is proposed, depicting the reconfiguration scenario before and after eavesdropping. Finally, Section 6 summarizes and presents our conclusions.

## II. SIGNATURE KEYS RECONFIGURATION

The scheme proposed in the previous research [7] described that, to enhance network confidentiality, the codecs from the transmitter and receiver dynamically change their 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. However, we proposed asignature keys reconfiguration scheme with eavesdropping detection where the signature codes change only when an eavesdropping is detected, which can reduce the power consumption of the optical switch by avoiding repeatedly codes change.

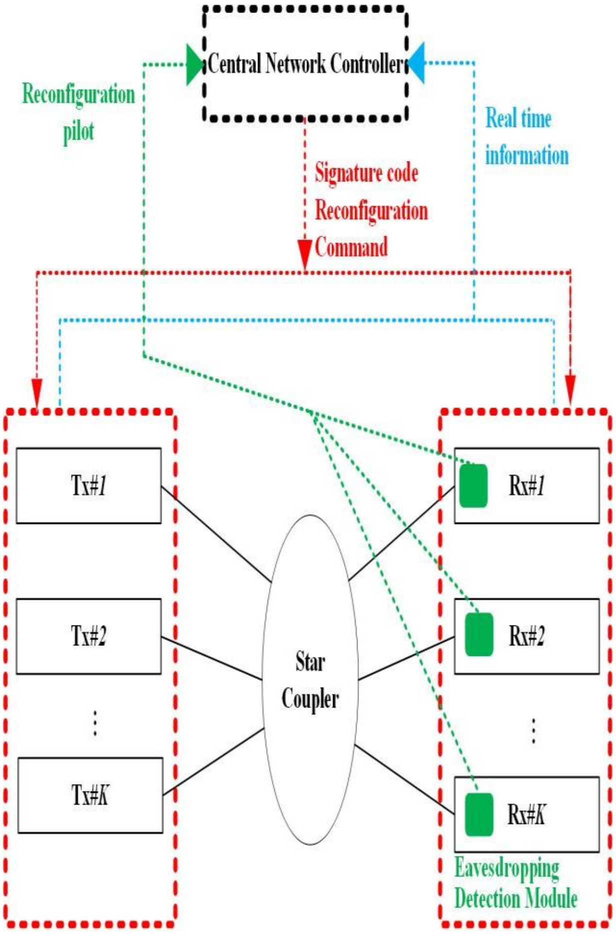
Central Network Controller
Reconfiguration pilot
Real time information
Signature code Reconfiguration Command
Tx#1
Tx#2
Tx#K
Star Coupler
Rx#1
Rx#2
Rx#K
Eavesdropping Detection Module

**Fig. 1: The mechanism of signature code reconfiguration.**

Figure 1 shows the proposed signature keys reconfiguration mechanism and specifies how signature codes being reconfigured when the network is under eavesdropping. Once the eavesdropping detection unitsensesany traffic or power abnormity, a reconfiguration pilot is sent to the network reconfigurationcontroller.Upon receiving the pilot from the eavesdropping detection unit, the reconfiguration controller transmits a reconfiguration command to the communicating users to reconfigure their signature keys. Noted that the controller also collects real-time information of the code sequences to avoid the reconfigured keys been the same as their prior ones.

## III. EAVESDROPPING DETECTION BASED ON POWER COMPARISONS

An eavesdropper in an OCDMA network may tap signals from various locations within the network. Therefore, the eavesdropper can tap on the uplink or downlink which the user transmits data. The eavesdropper can install an interceptor(decoder scheme) on the tapped link which the user transmit data to optical fiber star coupler, in order to recover specific code. If an O-CDMA coding scheme that has a very large number of possible codes could be developed, then an eavesdropper would have to perform a brute-force search through half of them, on average, before finding the proper code to demodulate a given user’s data.

In the eavesdropper aspect, we assume that the eavesdropper knows the “old key”, the original signature code used by the desired user. In this situation, the eavesdropper will use the receiver with the same code sequence of the desired user. At the receiver, the received signal is broadcasted into three parts by splitter. The first and the second copies of the received signal are input into the two blocks for correlation computation between spectral distribution of the local code and its complementary code. Based on the subtracted correlation energy, the received “1” or “0” data bit from transmitter can be accordingly obtained.

The structure of the proposed eavesdropping detection module is as illustrated in Figure 2. Both the input and the output signals are connected into the receiver decoder unit. Both under-monitored optical paths are photo-detected and the corresponding electrical powers are derived from the received optical signals. After that, electronic processing unit calculates the difference of the converted input signal and the recovered outputsignal.The I/O difference will be a null value when there is no eavesdropping and will be a certain magnitude when there exists eavesdropping.

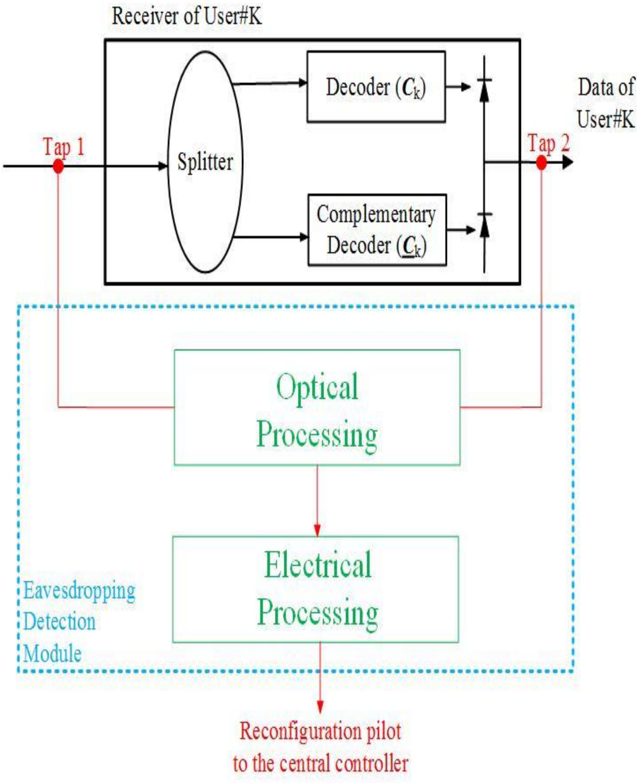
Receiver of User#K
Decoder ($C_k$)
Data of User#K
Tap 1
Splitter
Tap 2
Complementary Decoder ($\bar{C}_k$)
Optical Processing
Electrical Processing
Eavesdropping Detection Module
Reconfiguration pilot to the central controller

**Fig.2: Eavesdropping detection module at the receiver.**

To investigate whether an eavesdropping occurs, we define two parameters. The parameter $F = P_{in}–P_{out}$is defined as the power difference between the input and the output signals on the receiver decoder, which means the degradation degree of the optical signal. The parameter $D = F_{noE}–F_E$ is defined as the difference between parameter $F_{noE}$(when there is no eavesdropping) and parameter $F_E$(when there is an eavesdropping). It shows the degree of being influenced by eavesdropping on the desired user.

When there is no eavesdropping, the electrical powers from the input and output (I/O) taps are:

$P_{in\_noE} \propto K \cdot P_{user}$(1)

$P_{out\_noE} \propto P_{user}$(2)

Where $K$ is the number of active users and $P_{user}$ is the power of single user. The input signal may contain information from $K$ active users, and the power of output signal is approximately equal to the power of one single user due to the reason that the receiver only recovers signal of one single user.

According to the definition of $F$,we can derive the value of $F_{noE}$ when there is no eavesdropping, to be:

$F_{noE} = P_{in\_noE}–P_{out\_noE}$

$=K \cdot P_{\text{user}}–P_{user}$

$= (K–1) \cdot P_{user}$(3)

On the other hand, when an eavesdropping occurs, a part of power$P_x$ from the input signal will be tapped from the eavesdropper, so the value of $F_E$ when there is an eavesdropping becomes:

$F_E = P_{in\_E}–P_{out\_E}$

$=(P_{in\_noE} –P_x)–(1/K)P_{in\_E}$

$= K \cdot P_{user} –P_x - P_{user} + (1/K)P_x$

$= (K–1) \cdot P_{user}+ [(1–K/K)]P_x$ (4)

Notice from Eqs. (3) and (4), if there is no eavesdropping on the specific node user, then the value $D$ is almost 0 when there is no eavesdropping for the reason that there is no change on the value $F_E$, i.e.,$F_{noE} =F_E$. On the other hand, if an eavesdropping occurs, then the $F_E$ changes, so that $F_{noE} \neq F_E$, which means value $D$ is not zero, so the value $D$ when there is eavesdropping is:

$D = F_{noE} - F_E$

$= (K–1) \cdot P_{user} – (K–1) \cdot P_{user} – [(1–K/K)]P_x$

$=[(K–1/K)]P_x$ (5)

Therefore, value D is deemed as the threshold value of eavesdropping detection. In other words, when D is almost 0, then there is no eavesdropping. However, if D≠0, then there is currently an eavesdropping in the local node decoder.

Following the above power-comparisons-based eavesdropping detection in the receiver decoder, network reconfiguration controller commands the change of signature keys to the communicating transceiver upon receiving the reconfiguration pilot.

## IV. SIGNATURE RECONFIGURATIONS UPON EAVESDROPPING DETECTION

First, let us examine the negative situation when eavesdropping detection is sensed be null value ($D$=0) and no signature code reconfigurations is necessary. Consider an OCDMA network with three active transceiver pairs assigned with signature codes$\boldsymbol{C}_{1,pri}$ = (1 1 1 0 0 1 0),$\boldsymbol{C}_{2,pri}$ = (01 1 1 0 0 1), and $\boldsymbol{C}_{3,pri}$ = (101 1 1 0 0), respectively. Also, the transmitted data bits sequences for the three active transceivers are supposed to be $\boldsymbol{d}_1$ = [(1), (1), …],$\boldsymbol{d}_2$ = [(0), (1), …], and$\boldsymbol{d}_3$ = [(1), (0), …], respectively. With these code keys prior to signature reconfiguration,the combined spectral signal is $\boldsymbol{S}_{\boldsymbol{pri}} = \boldsymbol{d}_1\boldsymbol{C}_{1,pri}+ \boldsymbol{d}_2\boldsymbol{C}_{2,pri}+ \boldsymbol{d}_3\boldsymbol{C}_{3,pri}$=[(2,1,2,1,1,1,0), (1, 2,2,1,0, 1, 1), …]. Thissummed spectral signal is then transmitted over fiber link to the optical receivers.

Suppose an eavesdropper is tapping on user#1and has deciphered user #1's signature key. Subtracted correlation output energy from the upper and the lower photodiodes for both user#1 and eavesdropper then are of the same chips power in one data bit. The eavesdropper thus successfully tapsthedata bits sequence transmitted to user#1. In other words, prior to correct eavesdropping detection to make signature reconfiguration, the eavesdropper can steal the data bits transmitted to user#1.

On the other contrary, when eavesdropping detection is sensed and signature code reconfigurations needed. Note that, once the network reconfiguration controller receives reconfiguration pilot from the specific receiver decoder, it sends reconfiguration command to the corresponding transceivers to change their signature keys. Suppose the newly reconfigured signature keys are emerged from random bits-shift to $\boldsymbol{C}_{1,pst}$= (0 1 0 1 1 1 0), $\boldsymbol{C}_{2,pst}$= (0 0 1 0 1 1 1), and $\boldsymbol{C}_{3,pst}$= (1 0 0 1 0 1 1), respectively.Under the same transmitted data bits sequences for the three active transceiver users, the combined spectral signal after signature reconfiguration becomes$\boldsymbol{S}_{\boldsymbol{pst}}= \boldsymbol{d}_1\boldsymbol{C}_{1,pst}+ \boldsymbol{d}_2\boldsymbol{C}_{2,pst}+ \boldsymbol{d}_3\boldsymbol{C}_{3,pst}$=[(1,1,1,2,2,3,2), (0, 1,1,1,2,2,1), …]. This reconfigured spectrally summed signal is then transmitted to the receiver decoders to counteract with the eavesdropper.

Under the situation that an eavesdropper is tapping on user#1, the correlation output energy for the receiver decoder ofuser#1 obtained at the upper/lower photodiodes are respectively $\boldsymbol{S}_{\boldsymbol{pst}}\times\boldsymbol{C}_{1,pst}$and $\boldsymbol{S}_{\boldsymbol{pst}}\times\underline{\boldsymbol{C}}_{1,pst}$. Nevertheless, after signature reconfiguration, the eavesdropper remains with its prior signature key $\boldsymbol{C}_{\mathrm{e}}$ = (1 1 1 0 0 1 0) and the correlation output energy for eavesdropper will result in the detected output energy $\boldsymbol{S}_{\boldsymbol{pst}}\times\boldsymbol{C}_{\mathrm{e}}$ and $\boldsymbol{S}_{\boldsymbol{pst}}\times\underline{\boldsymbol{C}}_{\mathrm{e}}$at the upper/lower photodiodes, respectively. Since the transceiver pair of communicating users can duly reconfigure their signature keys on the thwart of eavesdropping, the communicating users can correctly decode the desired data bits sent from the corresponding transmitter coder. However, the eavesdropper did not know the change of signature key so that it cannot decode the desired data bits while still using the "old key" on the received summed signal spectra.

It is clear that without detecting eavesdropping successfully so that no signature reconfiguration made, an eavesdropper who detects the specific signature code assigned for the corresponding transceiver can easily detect the data bits sequence for that transceiver user. However, when eavesdropping is detected successfully, the risk of being eavesdropped can be reduced significantly.

## V. CONCLUSIONS

In this paper, we propose a scheme of signature keys reconfiguration to combat eavesdropping in OCDMA networks. In this scheme, each user is randomly assigned one M-sequence code that dynamically reconfigured to enhance network confidentiality. When detecting if the network node being eavesdropped or not by the method of power comparison, a value *D* is transmitted to the reconfiguration controller. The controller determines whether to send a signature reconfiguration command depending on the value *D*, if $D \neq 0$ (which means an eavesdropping occurs,) then the decision maker sends reconfiguration commands to transceiver nodes to change the assigned code sequence. Moreover, the real time value of the transponder is to avoid the reuse of code sequence, making the scheduler selects the sequences have not been using. Some of the attractive features of the proposed scheme include asynchronous network coordination, the reduced number of codecs, enhanced system confidentiality and a more complete mechanism in signature keys reconfiguration. The most important feature is the reconfiguration mechanism of signatures that thwarts the attack of code detection from an eavesdropper.

## REFERENCES

[1] K. Kravtsov and P. R. Prucnal, "Ultra short Optical Pulse Detection for High-Speed Asynchronous Optical CDMA Networks," IEEE J. Light wave Technology, vol. 27, no. 18, pp. 4069-4075, Sept. 2009.

[2] Nasaruddin and T. Tsujioka, "Design of Reconfigurable Multiweight Wavelength-Time Optical Codes for Secure Multimedia Optical CDMA Networks," IEEE International Conference on Communications (ICC'08), Beijing, pp. 5437-5442, May.2008.

[3] A. Nirmalathas, N. Nadarajah and E. Wong, "Multiple secure virtual private networks over passive optical networks using electronic CDMA," IEEE/LEOS Summer Topical Meeting (LEOSST '09), pp. 13-14, Newport Beach, CA, July. 2009.

[4] J.F. Huang, S.H. Meng, and Y.C. Lin, "Securing optical Code-Division Multiple-Access Networks with a Post-Switching Coding Scheme of Signature Reconfiguration," Optical Engineering, vol. 53(11), pp. 116101-1 ~ 116101-11, Nov. 2014.

[5] P.R. Prucnal, M.P. Fok, Y. Deng, and Z. Wang, “Physical layer security in fiber-optic networks using optical signal processing,” Optical Transmission Systems, Switching, and Subsystems VII, Proc. SPIE-OSA-IEEE Asia Communications and Photonics, pp. 1-10 Nov. 2009.

[6] T.H. Shake, “Security performance of optical CDMA against eavesdropping,” IEEE J. Light wave Technol., vol. 23, no. 2, pp. 655–670, Feb. 2005.

[7] J.F. Huang, K.S. Chen, Y.C. Lin, and C.Y. Li, “Reconfiguring Waveguide-Gratings-based M-Signature Codecs to Enhance OCDMA Network Confidentiality,” Optics Communications, vol. 313C, pp. 223-230, Feb. 2014.

[8] Chao Qi, Jiangxing Wu, Hongchao Hu, Guozhen Cheng, Wenyan Liu, Jianjian Ai, Chao Yang, "An Intensive Security Architecture with Multi-Controller for SDN," IEEE Conference on Computer Communications Workshops (INFOCOM), pp. 401-402, San Francisco, CA, USA, April. 2016.

[9] Muriel Medard, S. R. Chinn, P. Saengudomlert, “Attack Detection in All-Optical Networks,” Optical Fiber Communication Conference and Exhibit, pp. 272-273, Feb. 1998.