# Reconfiguring Composite Signature Labels over Optical MPLS Network Codecs to Secure Data Packets Routing

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

*Advanced Optoelectronic Technology Center*, *Institute of Computer and Communications Engineering*,
*Department of Electrical Engineering*, *National Cheng Kung University*, *Taiwan*.
*Tel*.: +886-6-2757575 ext. 62370; *Fax*: +886-6-234-5482;
*E-mail: huajf@ee.ncku.edu.tw, q38024016@mail.ncku.edu.tw, Q36034497@mail.ncku.edu.tw*

***Abstract*—This paper proposes a network security scheme in which optical network coders/decoders (codecs) reconfigure signature label codes to enhance system confidentiality for optical multi-protocol label switching (OMPLS) transmissions. In the proposed codec labels reconfiguration, we structure composite signatures from maximal-length sequence (M-sequence) codes to identify both data packet labels and network node codecs. Each core node can dynamically change its signature label to combat eavesdroppers for a reliable data packets routing. The results verify that the proposed approach via signature labels reconfiguration is effective against eavesdropping.**

***Keywords-Composite signature key, Maximal-length sequence (M-sequence) codes, Network confidentiality.***

## I. INTRODUCTION

Optical Multi-Protocol Label Switching (OMPLS) is a swiftly emerging technology that plays a significant role in next generation networks by delivering quality of service (QoS) and traffic engineering features. Interest in OMPLS has been steadily growing in recent decades. One of the most promising advances in packet-switching systems in recent years has been the development of MPLS, where the separation of routing and forwarding procedures enables high-speed optical packet transmission [1]. Great processing delays can be shortened at each node due to the avoidance of label de-composition in the network layer. In other words, OMPLS simplifies the forwarding function of routers. Without abandoning the basics of IP network, OMPLS is considered an extension protocol because it provides a more flexible and efficient packet switching.

Within the OMPLS network, signature labels assignment and decomposition on data packets can follow from Optical Code-Division Multiple-Access (OCDMA) techniques. Orthogonal coding labels can stack on data packets and correlate with the corresponding label codes at each successive routing node. However, weaknesses, including susceptibility to eavesdropping, have recently been reported in OCDMA [2][3] and hence in OMPLS systems. As respectively noted by Prucnal [4] and Shake [5], OCDMA techniques suffer from inherent security disadvantages in the signature decoding. In each routing node, an eavesdropper can use a simple energy detector to detect whether energy is present or not. In such cases, there is no routing security at all because the energy detector output contains the user's data stream. In addition, an OMPLS encoder uses the same fixed code repeatedly over a large number of bits. Consequently, an eavesdropper equipped with a sophisticated detector on the data node may be able to tap into the network and recover specific code, if he/she can obtain a sufficient signal-to-noise ratio (SNR). Thus, to ensure network routing confidentiality when designing physical transport layer, enhanced security mechanisms must incorporate appropriate signature codecs to enhance secure packets routing over OMPLS networks.

Data network confidentiality can be enhanced by methods based on optical signal processing. The three main approaches are: increasing code-space size [5], reducing subscriber transceiver power, and frequently changing signature code [6]. By employing the third approach, it is difficult for eavesdroppers to keep up with the speed when the code is changed. Thus, the code cannot be descrambled by simply detecting the channel waveform. In addition, multiple-access interference (MAI) limits the number of users simultaneously accessing the system. The most significant advantage of composite M-sequences is its cyclic property. Other characteristics include achieving enhanced communication with data security mechanisms, increasing system capacity by adding additional users to the same channel and eliminating MAI.

In this paper, we adapt a dynamically reconfigurable mechanism over the spectral-amplitude coding scheme of OMPLS to counter eavesdropping. We compose relatively prime-length M-sequence codes into sets of complex codes that govern reconfigurable network codecs by changing signature codes. Furthermore, we structure codec pairs based on arrayed-waveguide gratings (AWGs), along with the corresponding reconfiguration switches, to implement complex signature coding in the proposed network. By exploiting linear cyclic, periodic, and virtually orthogonal characteristics of M-sequence codes, we exemplify signature

 ISBN: 978-1-61208-509-8 

reconfiguration over AWG-based network codecs in this work.

The remainder of this paper is organized as follows. Section II briefly outlines the dynamic reconfiguration scheme consisting of the proposed composite signatures. Section III describes how the reconfigurable scheme operates to prevent eavesdroppers from solving the user's code, resulting in improved security. Section IV explains the perspectives on eavesdropper before and after reconfigurations. Finally, Section V summarizes and presents our conclusions.

## II. STRUCTURING COMPOSITE SIGNATURE CODECS FOR OPTICAL-MPLS NETWORK

Label stacking is used in MPLS systems by attaching one or more labels to a single packet to support hierarchical addressing, reducing the number of labels detected at each node. The core nodes only need to check an optical label matching to their label set to determine whether the packet should be forwarded or not. They do not need to remove the previous labels and swap a new one. It avoids the function of optical swapping at the expense of having a large number of stacked labels.

In the proposed MPLS network, the labels are encoded by spectral-amplitude-coding (SAC) because it has consentience with label stacking, fast recognition, and low system cost. Due to its inherent nature, all SAC labels occupy the same optical band, regardless of the wavelength used for the optical payload in our system. The payload is coded by a laser whose spectrum is outside the band of labels. Thus, label and payload can be combined as an optical packet and be transmitted simultaneously. Figure 1 shows such a scheme of an optical packet with label stacking.

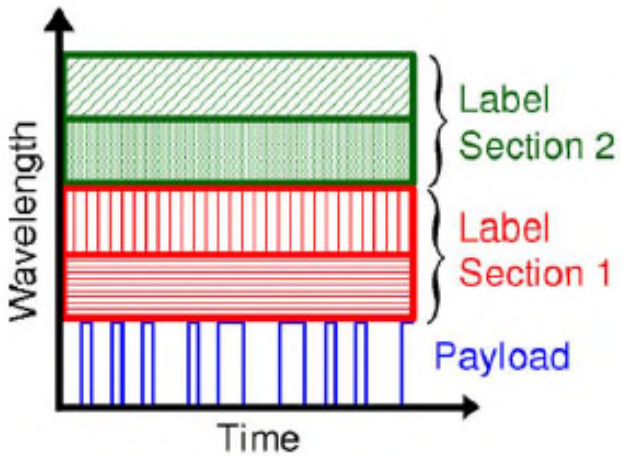


Fig. 1. Optical packet with stacked SAC labels.

As shown in Figure 2, the MPLS network is composed of many different types of nodes. According to the role of the label switching router (LSR) in the MPLS network, they can be divided into three different kinds: Ingress node, Core node, and Egress node. Figure 2 shows the optical packet switching in the MPLS network. There are six nodes in total, (*A*, *B*, *C*, *D*) are the core nodes and (*E*, *F*) are edge nodes. The label switching path (LSP) of this packet is assumed to be *E* (Ingress)-*A*-*D*-*F* (Egress). Later, we will verify the situation of the composite label code packet that we propose.

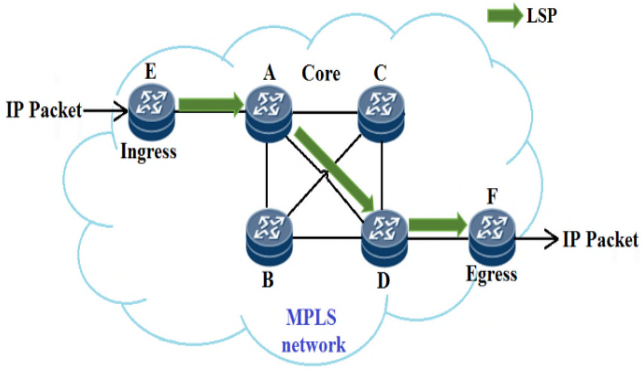


Fig. 2. The diagram of label switching in MPLS network.

In the proposed network, the reconfiguration has two mechanisms. The first one is, each core node changes its label at a fixed frequency by cyclic shifting signature code. This scheme is based on the assumption that the upper layers of the network effectively detect the threat of eavesdropping. The other way is, the reconfiguration command changes the signature code to a new one at the transceiver. If a tapper attacks the network frequently, the changing time becomes short, making the optical switch operate faster to reconfigure the code 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 lowered. The detailed design of the specifications for the central controller is very complex and beyond the scope of this paper. In this paper, we use the first mechanism.

## III. SUMMED SPECTRL LABELS ON RECONFIGURATIONS

At the ingress node, composite SAC-labels are implemented by two AWGs, two multiplexers, one BLS, and several optical switches, as shown in Figure 3. By using the cyclic properties of AWG routers and M-sequence codes, the codecs pair can encode/decode multiple labels simultaneously. Thus, all labels share the same hardware for the coding process. A modulo-2 operation combines M-sequences from two AWGs into a composite code. Optical switches are used for selecting composite codes for label stacking, in accordance with the number of pass nodes determined by label switching path (LSP). The optical

 ISBN: 978-1-61208-509-8 

modulator is used to modulate the payload bits onto the optical coded carrier. The Mach-Zehnder modulator (MZM) modulates the payload bits onto the coded optical carrier. Then, the SAC labels are combined with the payload bits to form a packet.

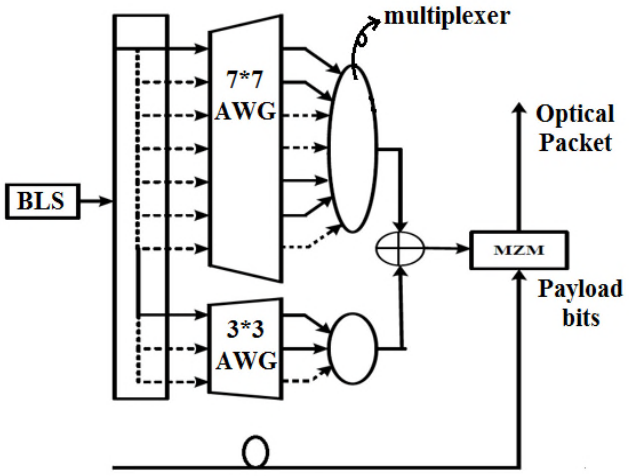


Fig. 3. The mechanism of labels encoding.

In the discussed composite label signatures reconfiguration, the core node will change the label dynamically. Let us consider an example optical-MPLS network with three nodes to illustrate composite signature codes reconfiguration. The three nodes are node #A, #D, and #F. We represent the operation of the network codecs prior to and subsequest to code reconfiguration using numerical coding data. Reconfiguration switches will switch on corresponding M-sequence codes to compose a set of composite signature codes. The setup for packets with SAC labels is illustrated in Figure 4. In our illustration, we select a 3×3 AWG and a 7×7 AWG for nodes to compose their label codes.

By combining each of the upper codes ($T^0C_1$, $T^1C_1$ and $T^2C_1$) in Table I (a) with the 1st lower code $T^0\boldsymbol{C}_2$ in Table I (b), we can get a subset label codes $T^iC_1 \oplus T^0\boldsymbol{C}_2$, $i$=0, 1, 2. Similarly, we can combine each of the upper codes with the 2nd lower code $T^1\boldsymbol{C}_2$ to get another subset label codes $T^iC_1 \oplus T^1\boldsymbol{C}_2$, $i$=0, 1, 2. In this way, we can combine each of the upper M-sequence codes $T^iC_1$ in Table I (a), $i$=0, 1, 2, with either of the lower M-sequence codes $T^j\boldsymbol{C}_2$ in Table I (b), $j$=0, 1, …, 6, to get the subset composite label codes $T^iC_1 \oplus T^j\boldsymbol{C}_2$ in Table I (c). We can have 7 yards groups in total, and each group can provide 3 label codes for the network labels assignment.

From the point of view of eavesdroppers, if a M-sequence code $T^i\boldsymbol{C}_1$ of period length $n_1$=3 (Table I (a)) is adopted in the network, the eavesdropper will have a 1/3 probability of detecting the signature code correctly. On the other hand, if an M-sequence code $T^j\boldsymbol{C}_2$ of period length $n_2$=7 (Table I (b)) is utilized, the eavesdropper will have a 1/7 probability of correctly detecting the signature code. However, if a composite code $\boldsymbol{S}^{(i,j)} = T^i\boldsymbol{C}_1 \oplus T^j\boldsymbol{C}_2$ of period length $n$=21 is used (Table I(c)), the probability of interception by the eavesdropper can be lowered to 1/21. This makes the eavesdropping more difficult and causes the eavesdropper to spend more time trying to guess the correct code.

TABLE I. STRUCTURING COMPOSITE SIGNATURE $\boldsymbol{S}^{(i,j)}(X)$ FROM M-SEQUENCES $T^i\boldsymbol{C}_1(X)$ AND $T^j\boldsymbol{C}_2(X)$. (a). 7 BLOCKS OF $T^i\boldsymbol{C}_1(X)$ SEQUENCES; (b). 3 BLOCKS OF $T^j\boldsymbol{C}_2(X)$ SEQUENCES; (c). COMPOSITE SIGNATURES $\boldsymbol{S}^{(i,j)}(X) = T^i\boldsymbol{C}_1(X) \oplus T^j\boldsymbol{C}_2(X)$.

(a).

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $\boldsymbol{C}_1$ | 110 | 110 | 110 | 110 | 110 | 110 | 110 |
| $T\boldsymbol{C}_1$ | 011 | 011 | 011 | 011 | 011 | 011 | 011 |
| $T^2\boldsymbol{C}_1$ | 101 | 101 | 101 | 101 | 101 | 101 | 101 |

(b).

| | | | |
|---|---|---|---|
| $\boldsymbol{C}_2$ | 1110010 | 1110010 | 1110010 |
| $T\boldsymbol{C}_2$ | 0111001 | 0111001 | 0111001 |
| $T^2\boldsymbol{C}_2$ | 1011100 | 1011100 | 1011100 |
| $T^3\boldsymbol{C}_2$ | 0101110 | 0101110 | 0101110 |
| $T^4\boldsymbol{C}_2$ | 0010111 | 0010111 | 0010111 |
| $T^5\boldsymbol{C}_2$ | 1001011 | 1001011 | 1001011 |
| $T^6\boldsymbol{C}_2$ | 1100101 | 1100101 | 1100101 |

(c).

| Node #A | |
|---|---|
| $\boldsymbol{C}_1 \oplus \boldsymbol{C}_2$ | 001111101010011000100 |
| $T\boldsymbol{C}_1 \oplus \boldsymbol{C}_2$ | 100010000111110101001 |
| $T^2\boldsymbol{C}_1 \oplus \boldsymbol{C}_2$ | 010100110001000011111 |

| Node #D | |
|---|---|
| $\boldsymbol{C}_1 \oplus T^3\boldsymbol{C}_2$ | 100001111101010011000 |
| $T\boldsymbol{C}_1 \oplus T^3\boldsymbol{C}_2$ | 001100010000111110101 |
| $T^2\boldsymbol{C}_1 \oplus T^3\boldsymbol{C}_2$ | 111010100110001000011 |

| Node#F | |
|---|---|
| $\boldsymbol{C}_1 \oplus T^5\boldsymbol{C}_2$ | 010011000100001111101 |
| $T\boldsymbol{C}_1 \oplus T^5\boldsymbol{C}_2$ | 111110101001100010000 |
| $T^2\boldsymbol{C}_1 \oplus T^5\boldsymbol{C}_2$ | 001000011111010100110 |

 ISBN: 978-1-61208-509-8 

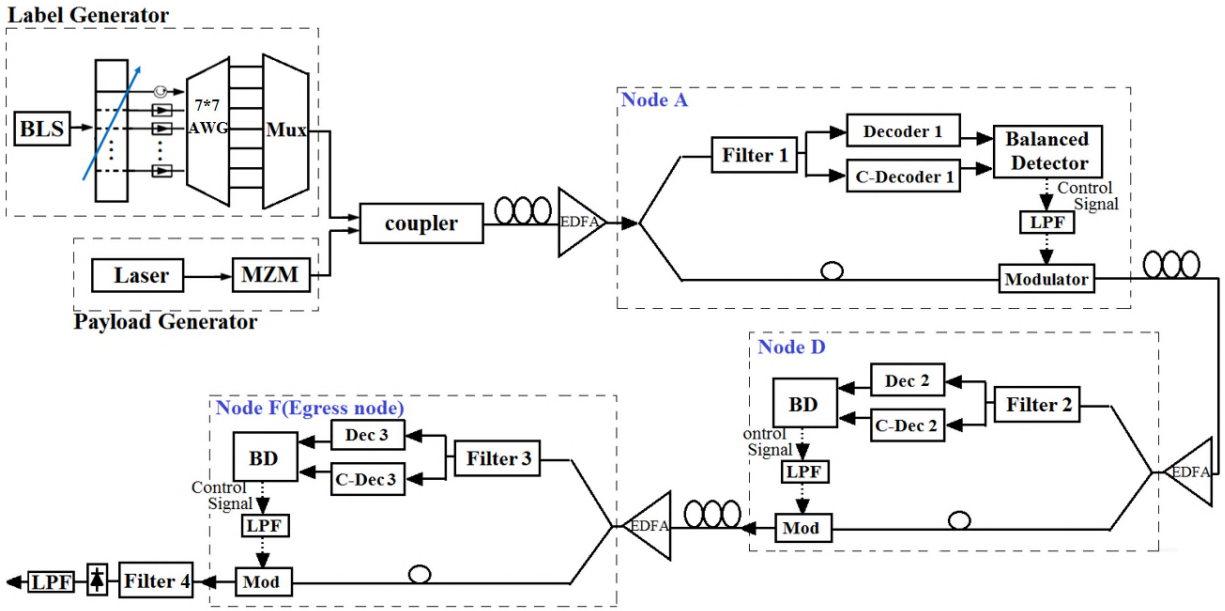


Fig. 4. Schematic optical-MPLS network with reconfigurable composite signature codecs.

Before signature reconfiguration, we suppose that the composite code for the node #A is combined from M-sequence codes $\boldsymbol{C}_1(X)$ = (110, …) and $\boldsymbol{C}_2(X)$ = (1110010, …):

$$\boldsymbol{S}_1^{(0,0)}(X) = T^0\boldsymbol{C}_1(X) \oplus T^0\boldsymbol{C}_2(X)$$
$$= (001\ 111\ 101\ 010\ 011\ 000\ 100).$$

As for the node #D, we suppose that the composite code is combined from M-sequence codes $T^1\boldsymbol{C}_1(X)$ = (011, …) and $T^3\boldsymbol{C}_2(X)$ = (0101110, …):

$$\boldsymbol{S}_2^{(1,3)}(X) = T^1\boldsymbol{C}_1(X) \oplus T^3\boldsymbol{C}_2(X)$$
$$= (001\ 100\ 010\ 000\ 111\ 110\ 101).$$

Further, we suppose the composite signature code for node #F is constructed from M-sequence codes $T^1\boldsymbol{C}_1(X)$ = (011, …) and $T^5\boldsymbol{C}_2(X)$ = (1001011, …):

$$\boldsymbol{S}_3^{(1,5)}(X) = T^1\boldsymbol{C}_1(X) \oplus T^5\boldsymbol{C}_2(X)$$
$$= (111\ 110\ 101\ 001\ 100\ 010\ 000).$$

The stacked label prior to signature reconfiguration thus takes the form $\boldsymbol{Y}_{(pri)}(X) = \boldsymbol{S}_1^{(0,0)}(X) + \boldsymbol{S}_2^{(1,3)}(X) + \boldsymbol{S}_3^{(1,5)}(X)$, the label coded signature chips will combine together to result in a label stack signal prior to signature reconfiguration:

$$\boldsymbol{Y}_{(pri)}(X) = \boldsymbol{S}_1^{(0,0)}(X) + \boldsymbol{S}_2^{(1,3)}(X) + \boldsymbol{S}_3^{(1,5)}(X)$$
$$= (001\ 111\ 101\ 010\ 011\ 000\ 100)$$
$$+ (001\ 100\ 010\ 000\ 111\ 110\ 101)$$
$$+ (111\ 110\ 101\ 001\ 100\ 010\ 000)$$
$$= (113\ 321\ 212\ 011\ 222\ 120\ 201).$$

Subsequest to signature reconfiguration, each core node changes its label by state shifting of the signature code. The resulted label codes allocated for each routing node are then stacked over the newly generated data packets. Other possible combinations of logic "ON" and logic "OFF" information on stacked label decoding can be similarly deduced.

## IV. PERSPECTIVES ON EAVESDROPPER BEFORE AND AFTER RECONFIGURATIONS

The objective of secure OMPLS routing is to ensure that an unauthorized individual does not gain access to data in the network. We assume that an eavesdropper is technologically intelligent with knowledge about signals being transmitted in the network (i.e., the architecture of the network, types of signals, data rates, encoding rules, structure of codes, etc.). In other words, the eavesdropper is supposed to know everything about the network operations and signatures coding scheme except for the specific signature key in the network node.

Figure 5 depicts a general configuration of OMPLS label decoder at each routing node. A pair of AWGs with signature label $\boldsymbol{S}_u^{(i,j)}$ and complementary key $\underline{\boldsymbol{S}}_u^{(i,j)}$ is adopted here for the $u$-th receiver decoder. The stacked label $\boldsymbol{Y}$ from the optical fiber channel is directed to the ($i$+1)-th and the ($j$+1)-th input ports of the 3x3 and 7x7 AWG decoders. Then the label is decoded by executing balanced detection of correlation subtraction. Only when the label code of the incoming packet matches that of the core node, a "matched" indication signal is generated, and

the modulator stays in an "ON" state. In contrast, when the packet label does not match that allocated in the passing node, no matched indication signal exists, and the modulator stays in an "OFF" state.

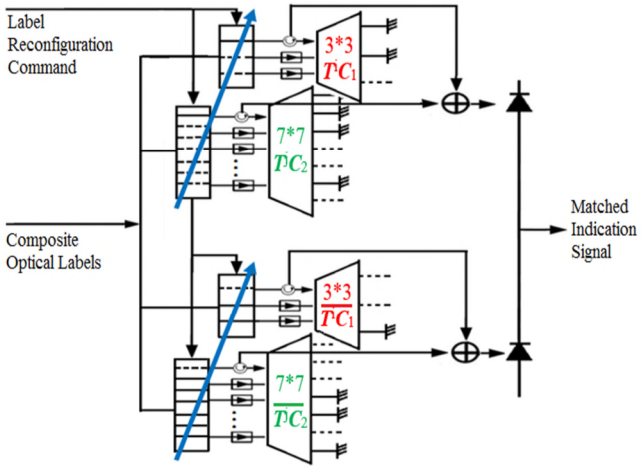


Fig. 5. Composite signature decoder with complementary subtraction scheme.

In the illustrative OMPLS data packets routing, an eavesdropper is supposed to tap on node #D. As we have mentioned, the eavesdropper may bear the same decoder structure as those in the tapped routing nodes, but with different signature label codes. Since an eavesdropper is assumed to tap on node #D, both node #D and eavesdropper will bear the same label code $\boldsymbol{S}_2^{(1,3)}$ = (001 100 010 000 111 110 101) just prior to signature reconfiguration. Correlation outputs on node #D and also on eavesdropper before signature reconfiguration will be

$$\boldsymbol{Y}_{(\text{pri})} \times \boldsymbol{S}_2^{(1,3)} = (003\ 300\ 010\ 000\ 222\ 120\ 201)$$
$$\boldsymbol{Y}_{(\text{pri})} \times \underline{\boldsymbol{S}}_2^{(1,3)} = (110\ 021\ 202\ 011\ 000\ 000\ 000).$$

The above correlation magnitudes on the upper and the lower photodiodes of balanced decoder will subtract to result in a net photo-energy of $|\boldsymbol{Y}_{(\text{pri})}\boldsymbol{S}_2^{(1,3)}| - |\boldsymbol{Y}_{(\text{pri})}\underline{\boldsymbol{S}}_2^{(1,3)}|$ = 19-11 = 8 units, indicating a label switching state of 'ON' and is able to route the packet data into eavesdropper.

The network will dynamically reconfigure signature labels allocated to each routing node, either by local node codecs or globally-controlled state machine. Let us examine the situation on labels decoding after signature reconfiguration. With reference to Table I(c), assume that node #A changes its signature label from $\boldsymbol{S}_1^{(0,0)}$ to $\boldsymbol{S}_1^{(1,0)}$, node #D changes from $\boldsymbol{S}_2^{(1,3)}$ to $\boldsymbol{S}_2^{(2,3)}$ and node #F changes from $\boldsymbol{S}_3^{(1,5)}$ to $\boldsymbol{S}_3^{(0,5)}$. We therefore have a stacked label signal after signature reconfiguration:

$$\boldsymbol{Y}_{(\text{pst})}(X) = \boldsymbol{S}_1^{(1,0)}(X) + \boldsymbol{S}_2^{(2,3)}(X) + \boldsymbol{S}_3^{(0,5)}(X)$$
$$= (221\ 031\ 100\ 321\ 112\ 212\ 113).$$

This reconfigured and stacked label signal then cascade with payload data to route the resulted data packets to the corresponding nodes in the network.

Figure 6 depicts schematic diagram on data packets routing to node #D while an eavesdropper taps there to "steal" the information that is sent to the node. Since node #D can duly reconfigure its label code dynamically, node #D can correctly decode the information sent into node #D. However, the eavesdropper would not know the change of label code and would not decode information correctly while it still uses "old key" on the decoded summed signal spectra.

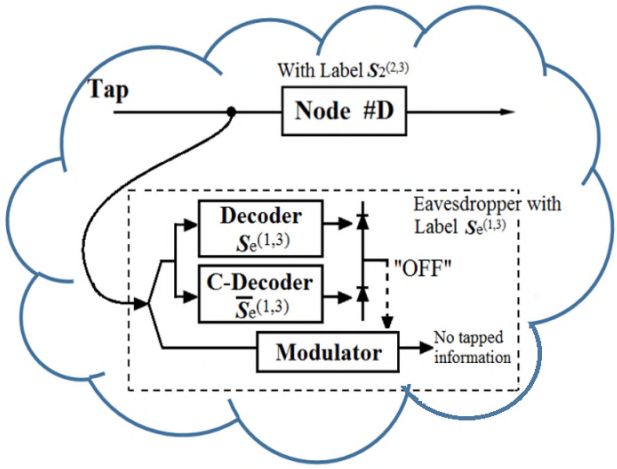


Fig. 6. Schematic of eavesdropper tapping on Node #D.

Specifically, for node #D with new label code $\boldsymbol{S}_2^{(2,3)}$ = (111 010 100 110 001 000 011) and the newly stacked label $\boldsymbol{Y}_{(\text{pst})}$ = (221 031 100 321 112 212 113), correlation output energies obtained at the decoding side for node #D are

$$\boldsymbol{Y}_{(\text{pst})} \times \boldsymbol{S}_2^{(2,3)} = (221\ 030\ 100\ 321\ 002\ 000\ 013),$$
$$\boldsymbol{Y}_{(\text{pst})} \times \underline{\boldsymbol{S}}_2^{(2,3)} = (000\ 001\ 000\ 001\ 110\ 212\ 100).$$

The above correlation magnitudes will subtract at the balanced photo-detector in the node #D to result in a net photo-energy of $|\boldsymbol{Y}_{(\text{pst})}\boldsymbol{S}_2^{(2,3)}| - |\boldsymbol{Y}_{(\text{pst})}\underline{\boldsymbol{S}}_2^{(2,3)}|$ = 21-10 = 11 units, indicating a label switching state of 'ON' and is able to route the packet data into node #D.

Nevertheless, even after label signature reconfiguration, the eavesdropper remains with its prior label code $\boldsymbol{S}_e^{(1,3)} = \boldsymbol{S}_2^{(1,3)}$ = (001 100 010 000 111 110 101). Correlation with the received stacked label $\boldsymbol{Y}_{(\text{pst})}$ at the photodiodes will result in detected output energy for the eavesdropper;

$$\boldsymbol{Y}_{(\text{pst})} \times \boldsymbol{S}_e^{(1,3)} = (001\ 000\ 000\ 000\ 112\ 210\ 103),$$
$$\boldsymbol{Y}_{(\text{pst})} \times \underline{\boldsymbol{S}}_e^{(1,3)} = (220\ 031\ 100\ 321\ 000\ 002\ 010).$$

 ISBN: 978-1-61208-509-8

Correlation subtraction at the balanced photo-detector in the eavesdropper will result in a net photo-energy of $|\boldsymbol{Y}_{(pst)}\boldsymbol{S}_e^{(1,3)}| - |\boldsymbol{Y}_{(pst)}\underline{\boldsymbol{S}}_e^{(1,3)}| = 12\text{-}18 = -6$ units, indicating a label switching state of 'OFF' and is unable to route the packet data to the eavesdropper.

Table II summarizes the numerical results on the decoded subtracted correlation for node #D and the eavesdropper, subsequent to signature reconfiguration. It is clear that, if the label code is not changed, the eavesdropper who detects the label code assigned for the corresponding transceiver user can easily detect the information for that user. That is the reason we employ a dynamic code reconfigurations scheme to change labels allocated to the nodes.

TABLE II. EAVEDROPPER'SPERSPECTIVES CONSEQUENT TO SIGNATURE RECONFIGURATION

| | Correlation subtraction | Subtracted correlation energy |
|---|---|---|
| For Node #D | $\boldsymbol{Y}_{(pst)}\times\boldsymbol{S}_2^{(2,3)}$ = (221 030 100 321 002 000 013) $\boldsymbol{Y}_{(pst)}\times\underline{\boldsymbol{S}}_2^{(2,3)}$ = (000 001 000 001 110 212 100) | $\lvert\boldsymbol{Y}_{(pst)}\boldsymbol{S}_2^{(2,3)}\rvert - \lvert\boldsymbol{Y}_{(pst)}\underline{\boldsymbol{S}}_2^{(2,3)}\rvert = 21\text{-}10 = 11$ ➔ Label 'ON' |
| For Eavesdropper tapped at #D | $\boldsymbol{Y}_{(pst)}\times\boldsymbol{S}_e^{(1,3)}$ = (001 000 000 000 112 210 103) $\boldsymbol{Y}_{(pst)}\times\underline{\boldsymbol{S}}_e^{(1,3)}$ = (220 031 100 321 000 002 010) | $\lvert\boldsymbol{Y}_{(pst)}\boldsymbol{S}_e^{(1,3)}\rvert - \lvert\boldsymbol{Y}_{(pst)}\underline{\boldsymbol{S}}_e^{(1,3)}\rvert = 12\text{-}18 = -6$ ➔Label 'OFF' |

The dynamic code reconfiguration mechanism significantly reduces the probability of correct information being obtained by attackers via interception, and hence significantly enhances system confidentiality. By changing the label code of the nodes, the eavesdroppers have less chance of intercepting the correct code. Simulation results show that the degree of network security is significantly improved when dynamic signatures reconfiguration are implemented over the composite M-sequence codes.

## V. CONCLUSIONS

In this paper, we proposed a scheme based on reconfigurable signatures to combat eavesdropping in optical-MPLS networks. In the proposed scheme, each user is randomly assigned one set of prime-lengths M-sequence codes, and then these signature codes get dynamically reconfigured to enhance network confidentiality. Each core node changes its label at a fixed frequency by cyclic shifting one or two chips of signature code to change the code sets assigned for each node to enhance confidentiality.

When the number of signature codes increases, detection of the unique user code by an eavesdropper becomes more difficult; thus, network confidentiality is significantly increased. The most important feature is the signature codes reconfiguration mechanism that thwarts an eavesdropper's code detection attack. Further work is required in order to implement fast optical switching and to get lower SNR transmissions. Nevertheless, the proposed scheme can considerably improve simple composite coding techniques to provide superior security.

## REFERENCES

[1] M.J. O'Mahony, D. Simeonidou, D.K. Hunter, and A. Tzanakaki, "The application of optical packet switching in future communication networks," *IEEE Commun. Mag.*, vol. 39, no. 3, pp. 128–135, Mar. 2001.

[2] B.B. Wu and E.E. Narimanov, "A method for secure communications over a public fiber-optical network," *Optics Express*, vol. 14, no. 9, pp. 3738-3751, May 2006.

[3] 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.

[4] P.R. Prucnal, M.P. Fok, Y. Deng, and Z. Wang, "Physical layer security in fiber-optic networks using optical signal processing," in *Optical Transmission Systems, Switching, and Subsystems VII,* edited by Dominique Chiaroni, Proc. of SPIE-OSA-IEEE Asia Communications and Photonics, 2009.

[5] T.H. Shake, "Security performance of optical CDMA against eavesdropping," *J. Lightwave Technol.*, vol. 23, no. 2, pp. 655–670, Feb. 2005.

[6] M.L.F. Abbade, L.A. Fossaluzza Jr., C.A. Messani, G.M. Taniguti, E.A.M. Fagotto, and I.E. Fonseca, "All-Optical Cryptography through Spectral Amplitude and Delay Encoding," *Journal of Microwaves, Optoelectronics and Electromagnetic Applications*, vol.12, no.2, São Caetano do Sul, Dec. 2013.

 ISBN: 978-1-61208-509-8 