Secure Optical Links in the Next-Generation DWDM Optical Networks

STAMATIOS V. KARTALOPOULOS
Williams Professor in Telecommunications Networking
ECE Depertment, TCOM graduate program
The University of Oklahoma
4502 E. 41st Street, Tulsa, OK 74135, USA

Abstract: - Wavelength Division Multiplexing (WDM) is currently the preferred photonic technology capable to transport more than 1 Tbit/s aggregate traffic over a single fiber. In the optical network, each fiber link consists of segments, each several kilometers long. However, the connecting points of the fiber are amenable to tapping. Even a small amount of optical signal extracted from a tap, when properly amplified can be monitored by unauthorized personnel, Since each WDM channel carries traffic from one customer, it is not difficult for the connoisseur to demultiplex a channel from the mix, isolate a specific payload and attempt to break the encryption code in the datagram. Therefore, data security should not rely only on the end-to-end encryption algorithm but also on link or physical layer. In this paper, we present a WDM link security algorithm that renders channel monitoring by unauthorized personnel virtually impossible. In addition, we examine the applicability of the method to various optical network topologies.

Key-Words: - Optical link security, Physical layer security, DWDM security,

1 Introduction

Wavelength Division Multiplexing (WDM) is a physical-layer technology that multiplexes many optical signals, each at different wavelength, for data transport over a single optical fiber, synchronous or asynchronous, SONET/SDH, IP or gigabit Ethernet. [1]. Tributaries to this network come from a variety of technologies, wireless, wired or fiber-to-the-x (FTTx). However, wireless and optical technologies are increasingly deployed at the edge of the network which is optical and it conforms to one of three major topologies, metro (ring), point-to-point and mesh. With recent advances in optical networking technology as many as 160 channels in the C and in the L spectral bands (1520-1620nm), and bit rates up to 40 Gbps per channel are reality.

The current trend in *Wavelength Division Multiplexing* (WDM) is to utilize each wavelength as a separate channel and at the same fixed rate. However, the number of recommended wavelengths per spectral band (and per fiber) defined by ITU-T [2, 3] is finite and limited and so is the number of users per fiber.

1.1 Aggregate channel capacity per fiber

In general, a spectral band Δf is expressed in terms of the maximum number of channels N that fit in it, and the channel spacing and width C_S and C_W, respectively:

$$\Delta \mathbf{f} = (\mathbf{C_W})\mathbf{N} + \mathbf{C_S}(\mathbf{N-1}) \qquad \mathbf{1}$$

Thus, the maximum number of channels per band is:

$$\mathbf{N} = (\Delta \mathbf{f} + \mathbf{C_S})/(\mathbf{C_W} + \mathbf{C_S}) \qquad \mathbf{2}$$

This relationship implies that the number of channels may be increased as the channel spacing and width are decreased. For interoperability purposes, ITU has recommended specific center frequencies (wavelengths) and channel separation at 12.5, 25, 50, 100, 200, and 400 Ghz.

1.2 Data and network security

Thus, since the number of channels per fiber is large, and since the amount of information per channel is large, it is critically important that not only each tributary is secured but also each optical link in the network. Currently, the telecommunications security is on two levels, data, network access, and network administration.

- Data security or cryptography is left up to end users. Data security uses sophisticated hidden messages within a text, codewords within a text, ASCII character scrambling according to a proprietary algorithm, or text watermarking.
- Network access is predominantly used in wireless and in asynchronous packet networks as

part of the connectivity protocol during user authentication.

▫ Network security relies on access identification codewords and passwords to enter into a node. Typically, this is accomplished by the network management port which provides access to the node for OA&M, node provisioning, and so on, but not for customer traffic.

The focus of this paper is on security of physical optical links. We describe a link security level that takes advantage of a transmission method known as wavelength-bus [4-6].

2 The WDM Wavelength-Bus

2.1 The WDM Wavelength-bus

Our secure link is based on a recent DWDM technology called WDM Wavelength-Bus. Therefore, in this section we provide a brief introduction.

In DWDM, the fiber is a transporting medium of a large number of channels (wavelengths) not all necessary modulated at the same rate; it is only for practical reasons that the modulation rate is the same. Thus, consider that while each channel is in the electronic regime acts upon an optical modulator to generate an optical serial bit stream, each stream at different wavelength; for simplicity of description, consider a group of eight streams, λ1 to λ8, Fig.1.

λ_1: a10 a11 a12 a13 a14 a15 a16 a17 b10 b11 …
λ_2: k20 k21 k22 k23 k24 k25 k26 k27 … a20 a21
λ_3: m30 m31 m32 m33 m34 m35 m36 m37 ... a31
.. : ....
λ8: p80 p81 p82 p83 p84 p85 p86 p87 … a80 a81

Fig.1: DWDM multi-channel data organization

Assume also that the *serial channels* are *byte-synchronized* and while they are still in the electronic regime. This is a typical case for most data and communications systems. Consider that bytes of each serial channel are converted to parallel. We call this a *parallel channel*. Also for simplicity of description, assume 8 bits per byte, although this is not a limiting factor.

Let bytes from several parallel data streams be multiplexed in an orderly fashion. For 8-bit bytes this constructs an 8-bit wide bus which in the optical layer consists of 8 different wavelengths or rails. Each rail of this 8-bit bus is transmitted serially at the same bit-rate with the other seven rails. We call this a WDM *wavelength-bus*. The end result of eight serial channels (of Figure 1) converted to an eight-rail λ-bus is illustrated in Fig.2.

Rail λ1: a10 k10 m30 … p80 b10 ...
Rail λ2: a11 k11 m31 … p81 b11 ...
Rail λ3: a12 k12 m32 … p82 b12 ...
Rail λ4: a13 k13 m33 … p83 b13 ...
Rail λ5: a14 k14 m34 … p84 b14 ...
Rail λ6: a15 k15 m35 … p85 b15 ...
Rail λ7: a16 k16 m36 … p86 b16 ...
Rail λ8: a17 k17 m37 … p87 b17 ...

Fig.2: The wavelength-bus

2.2 Merits of the Wavelength-bus

The wavelength-bus has a bandwidth capacity C equal to the data rate per rail D times the number of rails N on the bus:

$$\mathbf{C = N{\times}D\ \ (GHz)} \qquad 3$$

The only rule that applies is that the sum of all serial data streams (in Figure 2) to be transported by the wavelength bus is equal or less than C. As a consequence, if the serial data streams is a fraction of the bandwidth capacity C, then,

C = or < $\mathbf{\Sigma n_j C}$, over all j 4

where n_j is between 0 and 1, and Σn_j over all j is less or equal to 1.

The elasticity of the wavelength-bus is demonstrated with an 8-rail wavelength bus, each rail at 10 Gbps. Then:

1. 5 channels at 10 Gbps each, and 2 channels at 2.5 Gbps each, and 4 1GbE channels. Notice that this is impossible in a typical 8-channel DWDM system.
2. 1 channel at 40 Gbps, and 2 channels at 10 Gbps each, and 4 channels at 2.5 Gbps. Notice that this is impossible in a typical 10 Gbps DWDM system.

Example #2 has an important implication. Although 40 Gbps channels are uneconomical and they cannot travel over very long links due to a number of non-linear phenomena, transporting 40 Gbps with a wavelength-bus (each rail at 5 Gbps) over very long fiber links is possible and without amplification..

Thus, since a wavelength-bus consists of rails at the same bit rate, it becomes clear that the physical layer of a wavelength bus allows for traffic elasticity, it reduces hardware and software resources at the physical layer, and it reduces system design complexity and cost. In [5] we have addressed data synchronization, delay compensation, continuous data, bursty data [7] and other transmission issues, and therefore we do not repeat it here. In the next section we describe the inherent security features of the wavelength-bus.

3 Secured optical links

An optical link based on the WDM wavelength-bus is secured in several dimensions. Here we describe two, the multiplexer random scheduler and the temporal wavelength-bus randomizer.

3.1 Multiplex random scheduler

At the layer above the physical, the multiplexer layer is in the electronic regime. The multiplexer model assumes a variety of payloads at a variety of data rates. We distinguish two cases of multiplex random scheduler: customer traffic at each channel is at the same rate, and customer traffic is at different rates.

3.1.1 Same data rate

Consider eight data streams {A, B, C, …, H} all at the same data rate, each having a buffer of 2 to 8 bytes deep. We consider an interleaver that multiplexes bytes according to a random algorithm. An example after interleaving is ABBACDDFEFFAC… and so on. The random algorithm is known to the receiving end only for effective de-interleaving. Moreover, assume that this algorithm does not remain the same but it also varies at random intervals according to a program. Information concerning which algorithm is in use in each interval is transmitted to the receiving end over a secure supervisory channel using encrypted codewords that only the receiving end recognizes. These codewords are stored in semipermanent memory during node provisioning.

3.1.2 Different data rate

For simplicity assume two channels A and B, and that channel B is at twice the data rate of A; in fact, more channels are present as described in section 2, Then a typical interleaver multiplexes bytes from A and B as ABBAB. Similarly, assuming three data streams A, B and C, B twice the data rate of A and C thrice, then the typical interleaver multiplexes as ABBCCCABBCCC and so on. Now, if we consider that at each electrical channel has a buffer of 2 to 8 bytes deep, then the multiplexing sequence according to a random algorithm already described. In certain cases, when the aggregate traffic is less than the wavelength-bus capacity, the interleaver uses "empty" of idle bytes to fill the capacity.

Fig.3 illustrates the multiplex section of many tributaries including a buffer that multiplexes parallel bytes according to an algorithm. The buffer allows for a 2:1 aggregation (the equivalent of a TDM 2:1 concentration) as well as to smooth out the random arrival of bursty packets, whereas the electrical to optical conversion and modulation is at the output physical layer. Aggregation, buffer size and optimization algorithms is the subject of a subsequent paper. Fig.4 illustrates the receiver with reverse functionality and de-aggregation.

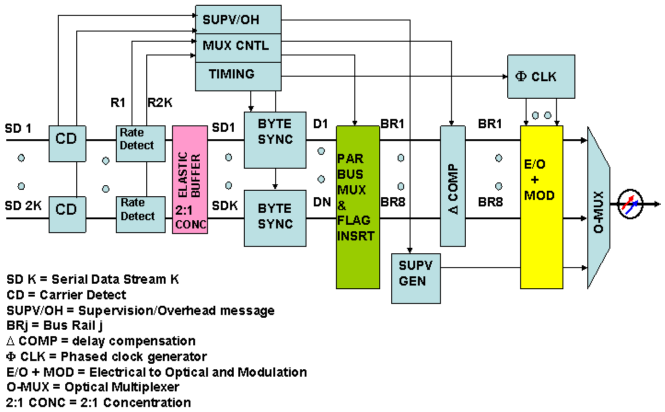
SUPV/OH
MUX CNTL
TIMING
Φ CLK
R1
R2K
SD 1
SD 2K
CD
CD
Rate Detect
Rate Detect
ELASTIC BUFFER
2:1 CONC
SD1
SDK
BYTE SYNC
BYTE SYNC
D1
DN
PAR BUS MUX & FLAG INSRT
BR1
BR8
Δ COMP
BR1
BR8
E/O + MOD
O-MUX
SUPV GEN
SD K = Serial Data Stream K
CD = Carrier Detect
SUPV/OH = Supervision/Overhead message
BRj = Bus Rail j
Δ COMP = delay compensation
Φ CLK = Phased clock generator
E/O + MOD = Electrical to Optical and Modulation
O-MUX = Optical Multiplexer
2:1 CONC = 2:1 Concentration

Fig.3: Circuit for converting a multiplicity of tributaries in a wavelength bus in the transmit direction.

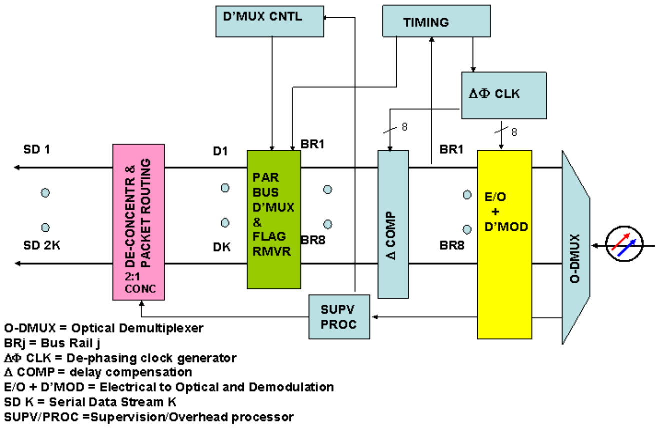
D'MUX CNTL
TIMING
ΔΦ CLK
8
8
SD 1
SD 2K
DE-CONCENTR & PACKET ROUTING
2:1 CONC
D1
DK
PAR BUS D'MUX & FLAG RMVR
BR1
BR8
Δ COMP
BR1
BR8
E/O + D'MOD
O-DMUX
SUPV PROC
O-DMUX = Optical Demultiplexer
BRj = Bus Rail j
ΔΦ CLK = De-phasing clock generator
Δ COMP = delay compensation
E/O + D'MOD = Electrical to Optical and Demodulation
SD K = Serial Data Stream K
SUPV/PROC =Supervision/Overhead processor

Fig.4: De-aggregation and reconstruction of tributaries in the receive direction.

3.2 Temporal wavelength-bus randomizer

Consider a set of parallel data streams $\mathfrak{D}(t)$ generated by the wavelength-bus while it is in the electronic regime. This set undergoes a bit-ordering transformation $\mathfrak{F}(x, t)$, producing a new data stream $\mathfrak{D}(x(t), t)$:

$$\boldsymbol{\mathfrak{D}(x(t), t) = \mathfrak{F}(x, t)\times\mathfrak{D}(t)} \qquad \mathbf{5}$$

For brevity, we describe this algorithm with an analog illustrated in Fig.5. Consider two wheels with aligned axis, one above the other and both divided in eight 45^o sectors, {S0A to S7A} and {S0B to S7B}. Consider that initially the two wheels have sectors aligned and that they are stationary. Each sector corresponds to a rail from the 8-bit wide bus in the electrical regime. Wheel A receives the data set $\mathfrak{D}(t)$. It performs the transformation $\mathfrak{T}(x, t)$ and it transfers the product to wheel B which feeds the O-E output physical layer.

This transformation is quantitatively explained. Consider that while wheel B remains stationary, wheel A above it rotates in increments of k45^o, where k is a random integer equal to or less than |8|. Thus, as k varies randomly between -8 and +8 (and according to an algorithm), the bit order on the wavelength bus is temporally randomized. We call this mechanism *temporal wavelength bus randomizer*. Thus, if the fiber is tapped, it is virtually impossible to isolate a particular client stream and decode it. Only the receiver is able to demultiplex it based on instructions received over the secure supervisory channel. The only vulnerable place is within the node; however, this is considered a secure area as it is non-accessible by unauthorized personnel.

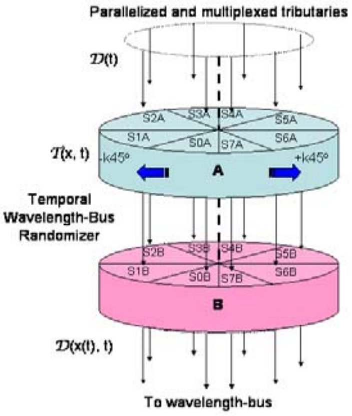

Fig.5. The analog of temporal wavelength-bus randomizer.

3.3 Wavelength-bus and network topology

DWDM technology currently defines 320 optical channels (with 25Ghz spacing) in the C and L bands. If the S and the water-peak regions are also included, then the number of channel approaches 1000. Such a large number of channels may be partitioned to several buses as well as to individual wavelengths for supervision and private "lines". Thus, if a set of channels consists of subsets, and each subset of sub-subsets, a wavelength-bus represent a unit of a sub-subset. This organization helps to treat each wavelength-bus individually and to manage routing in a mesh network or in ring network with optical add-drop multiplexers, as they do today with individual channels.

4 Conclusion

Privacy of traffic is important to communications networks. In this paper we reviewed the wavelength-bus as an efficient method to transmit very high data rates with lower optical data rates, as well as the transmitting and receiving circuitry for a general case. It has become apparent that, in addition to end-to-end encryption algorithms and call initiation authentication algorithms, it is necessary to secure the optical links between nodes so that intruders tapping the light stream from a fiber become unable to decipher the content of the information signals. We have presented a secure method that is based on the wavelength-bus. According to it, optical links are secured on multiple levels by randomizing the multiplexer schedule as well as the temporal mapping of multiplexed data onto the wavelength-bus. Thus, all three security mechanisms, including data encryption, establish an unbreakable code for a reasonably safe period, if ever.

References:

[1] S.V. Kartalopoulos, *DWDM: Networks, Devices and Technology*, IEEE/Wiley, New York, 2003

[2] ITU-T Rec. G.694.1, "Spectral Grids for WDM Applications: DWDM Frequency Grid", 2002.

[3] ITU-T Rec. G.694.2, "Spectral Grids for WDM Applications: CWDM Wavelength Grid", 2002.

[4] S.V. Kartalopoulos, "Ultra-high bandwidth data transport for DWDM short, medium-haul and metro using low bit rates", APOC 2002 Conference, in *SPIE Optical Switching and Optical Interconnection* II, pp. 100-107, October 2002.

[5] S.V. Kartalopoulos, "On the Performance of Multiwavelength Optical Paths in High Capacity DWDM Optical Networks", To be published in *SPIE Optical Engineering*, May 2004

[6] S.V. Kartalopoulos, "Add/Drop Capability for Ultra-High Speed Dense Wavelength Division Multiplexed Systems Using a Wavelength Bus", patent 6,493,118, 12/10/2002.

[7] M. Dueser, E. Kozlovski, R.I. Killey, P. Bayvel, "Design trade-offs in optical burst switched networks with dynamic wavelength allocation", Proc. ECOC 2000, pp. 23-24