Manuscript received Nov. 12, 2007; revised Dec. 22, 2007

Vulnerabilities and Security Strategy for the Next Generation Bandwidth Elastic PON

STAMATIOS V. KARTALOPOULOS, DI JIN
ECE Department, TCOM graduate program
The University of Oklahoma
4502 E. 41st Street, Tulsa, OK 74135
USA
kartalopoulos@ou.edu, di.jin@ou.edu

Abstract - The next generation WDM/TDM-PON is scalable and delivers elastically ultra-high data rates to many thousands of end-users, and therefore network security becomes of particular importance. We identify different levels of security and responsibilities in the communications network, we identify vulnerabilities in the optical access network and we describe the security features, monitoring and detecting of the next generation PON network.

Keywords: - Optical Networks, PON, FTTH, Network Security

1 Introduction

Wavelength division multiplexing (WDM) technology is delivering huge data rates per channel and unprecedented aggregate traffic per fiber. As such, WDM has been established as the technology of choice for long haul fiber networks as well as fiber to the home (FTTH). In long haul networks, this technology utilizes dense WDM (DWDM) for which the aggregate bandwidth has far exceeded the Tbps mark [1]. The success of fiber and WDM networks in long haul is being applied in residential and enterprise network applications to address the well-known "first/last mile" bandwidth bottleneck with fiber-optic solutions. In the latter case, in order to meet the access network requirements of high-efficiency and low-cost, passive optical technology is contemplated, and hence this network has been dubbed *passive optical network* (PON). Thus, both FTTH and PON terms refer to a fiber-optic access network; the first term indicates the method of delivery (that is, fiber-optic as compared to wired or wireless) and the second refers to the implementation technology indicating the type of optical components, that is, passive and not active.

Passive optical technology in access networks was selected to provide a cost-efficient transport and delivery mechanism, which is

- interference-free,
- bandwidth-scalable,
- distance independent between the premises (NT) and head-end (ONU), and
- security.

In addition, to allow for low-cost laser technology, such as:

- directly NRZ modulated and un-cooled VCSELs or high-speed LEDs with a center frequency that can swing several nanometers (as compared with fraction of nanometer in DWDM), and
- passive optical components with relaxed specifications (filters with 13 nm trapezoidal bandwidth, splitters, mux/demux), and
- semiconductor optical amplifiers (SOA), and perhaps low gain erbium doped fiber amplifiers (EDFA).

In response to this, the CWDM grid with 20 nm channel separation (compare with ~0.20 nm or 25 Ghz for DWDM) was specifically developed to meet the required relaxed specifications for lower cost.

The FTTH is applicable to residential or home as well as to enterprise applications, each with different needs, traffic type, bandwidth demands, quality of service and security.

For example, the bandwidth, cost-efficiency and security needs of the fiber to the premises (FTTP) are different than those of the FTTH, and different than those of the fiber to multi-dwelling units (FTTmdu) with high density residential complexes or campus-settings.

For example, fiber distribution, type of service and traffic, time of day peak demand, and security needs all differ. As a consequence, there are two FTTH and PON variants.

- The Ethernet PON (EPON) adopts the Ethernet protocol and data rates, the gigabit PON (GPON) adopts the GbE (and more recently the 10GbE) and it is a variant of the EPON, and
- The broadband PON (BPON) delivers broadband rates.

As the FTTH and PON are defined, standards are being developed by IEEE, ITU-T, Telcordia and other entities for interoperability purposes, recommending protocols, equipment housing, connector requirements and installation practices [2-8]. In sort, xPON represents any PON whereas FTTx any market that it addresses; occasionally, a more generic term that is used is fiber to the user (FTTU).

The passive optical network technology in the access space is a technology that is characterized by cost-efficiency, interference-free transmission, bandwidth scalability, payload and protocol transparency, and distance independence between premises and network head-end. Thus, a general PON topology consists of single mode fiber that links the network optical line terminal (OLT) with the optical network unit (ONU), for a link distance that can be up to 40 km without amplification. Additionally, fibers that link the ONU with each optical network terminating unit (NT) located at the premises, or at the curb; or at the neighborhood; this depends on the first/last mile medium selection and transmission method. The link ONU-NT may be up to several kilometers covering all loop lengths (in the US, some rural loops lengths can exceed 28 Kft). At the NT the optical signal is converted into electric and thence, the electric signal is transmitted over very short copper TPs to end-devices using fast digital transmission technology such as xDSL.

Among the PON architectures two topologically different are distinguished, the time division EPON (TDM-EPON) and the coarse wavelength division multiplexing EPON (CWDM-EPON).

- The TDM-EPON uses a single wavelength and also an elaborate timing protocol necessary to time multiplex packets of information, as they arrive at different and random instances.
- The CWDM-EPON takes advantage of the standard coarse wavelength grid and of the water-free fiber so that it can utilize all channels.

A close analysis of these two architectures reveals that each one has complementary advantages and disadvantages [9]. The number of end-users in TDM-EPON is based on a single wavelength and therefore it is a combination of data rate and number of time slots in the unit of time. Thus, in order to be able to reach a large number of end-users and deliver large bandwidth to each, a very high data line rate is required (such as 10 Gbps, or perhaps 40 Gbps) which thusly reduces cost-efficiency since ultra fast modulators, photodetectors and lasers need to be used. Conversely, the ITU-T CWDM grid defines eighteen (18) optical channels, Table 1, and thus the CWDM-EPON, although it delivers high data rates to end-users, has a very limited number of optical channels.

In response to this, a hierarchical CWDM/TDM next-generation PON has been proposed, briefly called hCT-PON [10]. The hCT-PON may also be engineered for standard single mode fiber applications using the DWDM grid in the C and L bands with 100 or 200 Ghz channel separation. The hCT-PON is characterized by:

- elastic bandwidth that expands upon end-user request ranging from DS0 to Gbps in small increaments.
- network scalability that can serve from few hundreds to 16,000 end-users or more.
- network topology flexibility that accommodates one or two topologies simultaneously.
- future-proofing.
- protocol transparency, and
- triple-play and multi-play as it is able to deliver any type of payload (voice, video and data).

Moreover, the hCT-PON adopts well-known network protection strategies [11], as well as excellent security features for intruder detection and source authentication.

When the hCT-PON network employs the CWDM standard grid, then we allocate 16 optical channels for data and two for supervision. Each channel is time division multiplexed and with a granularity of 2.5 Mbps (or less) per user, and at a data rate of OC-48 per optical channel, an aggregate

16x2.5 Gbps=40 Gbps is achieved; each Gbps corresponds to 15 million DS0s or to more than 500 compressed simultaneous video channels.

Table 1. ITU-T CWDM optical channel grid

λ (nm)	f (Thz)	λ (nm)	f (Thz)
1271	232.6	1451	206.5
1291	230.1	1471	203.6
1311	227.7	1491	200.9
1331	225.1	1511	198.2
1351	221.8	1531	195.6
1371	218.5	1551	193.1
1391	215.4	1571	190.7
1411	217.3	1591	188.2
1431	209.3	1611	185.9

Additionally, this bandwidth may be elastically distributed up to 16,000 end-users with protocol transparency to meet true multimedia needs. Because the hCT-PON is highly scalable, as more optical channels are added, either by doubling the CWDM to 36 channels, or by using a coarse DWDM, more bandwidth can be delivered to potentially 40,000 end-users. However, as the number of users in the network increases, the opportunities for network attacks increase. Such attacks may be eavesdropping, source mimicking, flooding to cause denial of service and many more.

In this paper we investigate the vulnerabilities, type of attacks and security issues of the general FTTx PON, and specifically of the FTTx hCT-PON, from the premises to the network access point, security measures, monitoring and detecting.

2 Overview of the hCT-PON

The hCT-PON employs a WDM grid of ITU-T defined channels that are coupled onto single mode fiber between the OLT and the ONU of the PON network and thus it conforms to a multiwavelength point-to-point topology. It also conforms to an optical tree topology at the ONU, which consists of two major functions, a single ONU optical (de)multiplexer and a set of ONU optical TDM. Finally, the topology between each ONU optical TDM and NT conforms to a point-to-multipoint.

The hCT-PON may adopt the CDWM or the DWDM grid in the C and/or L bands with 200 Ghz channel separation to meet low-cost objectives. As capacity need increases, the hCT-PON may be retrofitted using either a dense CWDM with twice as many channels or the DWDM with 100 Ghz channel spacing. In this paper for simplicity, we overview the standard CWDM case.

Sixteen of the eighteen CWDM optical channels are used for client data and two for supervision. Because the supervisory channels carry much lower data rate, the two most degraded channels of the spectrum are selected; these may be the two end channels of the grid or (depending on fiber specifications) two channels in the 1400 nm range.

At the OLT, the sixteen data and the two supervisory channels are multiplexed and transmitted in single mode water-free fiber to the optical network unit (ONU), Figure 1. Based on simulation results for OC-48 data rate and performance better than 10^{-12} BER, the fiber can be up to 40 km. The two supervisory channels are at OC-3, OC-12 or GbE to support high data rates and multi-services.

The ONU consists of an optical demultiplexer, hence ONU-d, 16 optical time division demultiplexing network units (ONU-t), SOA amplifiers, and two splitters for two supervisory channels. Each unit contains an optical switch which deflects packets in time slots to their corresponding fiber.

The sixteen (16) data channels from the ODemux are separated in two groups (group A and group B) 8 channels each, and each channel is connected with an ONU-t. One supervisory channel is assigned to group A, and the other to group B; each data channel is accompanied by the supervisory channel which is split into 8.

The ONU-t time demultiplexes packets of equal length and each demultiplexed packet is routed to a fiber in a cluster of fibers; each fiber in the cluster connects the ONU-t with a network terminating unit (NT), where each NT may serve one or more end-users. The length of each fiber in the cluster is the same in order to eliminate group delay variation and facilitate synchronization.

Each NT receives supervisory control messages that provide information regarding time reference (it is the same for all NTs in the same group), time slot location and slot length, payload type, testing, and other control messages, from which each NT determines its own time slot.

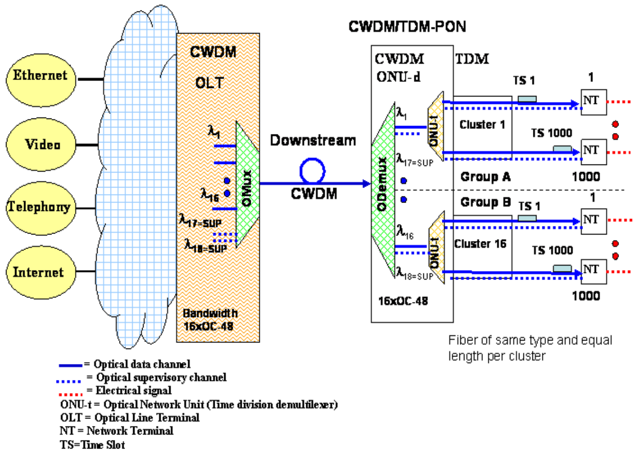

Figure 1: The hCT-PON access network (downstream direction).

Supervisory messages are kept simple. To illustrate this, assume a pragmatic data rate of OC-48 (2.5 Gbps) per optical data channel. For bandwidth scalability, the minimal time slot granularity is set to 125μs/1000 or 125 ns, which corresponds to a data granularity of 2.5 Mbps, Figure 2, and therefore, 2.5 Gbps data rate is distributed to 1,000 NTs. Thus, the number of all NTs supported by hCT-PON is 16,000, each receiving a respectable minimum bandwidth of 2.5 Mbps able to support triple-play (voice, compressed video, data). As such, the hCT-PON is transparent of data protocol because information is carried in logical segments over consecutive time slots.

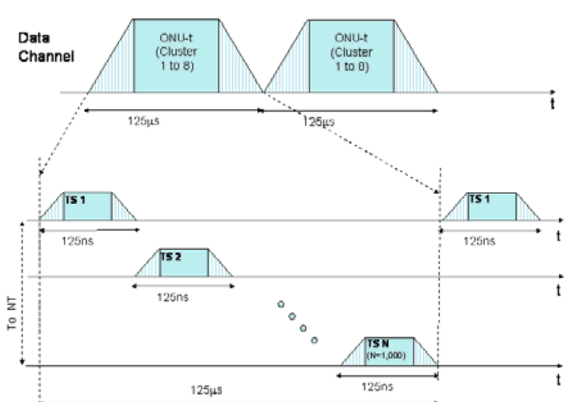

Figure 2: Time Division Demultiplexing of one optical data channel for a cluster of NTs.

In the supervisory message two bytes are used for addressing NTs. The latter corresponds to a large potential address space of 2^{16} which may be useful for future proofing, despite the fact that in the current generation 8,000 NTs per group are addressed. Thus, 16,000 messages/second per supervisory channel correspond to one message per 500 milliseconds per NT; this is considered sufficient in most access applications. Similarly, a cluster of NTs is addressed within 1/16 second or 62.5 msec, a cluster twice per second, and each of the 8,000 NTs in a cluster is addressed with a 62.5 μsec time slot. At OC-3 and for a generous 360 octets per message, approximately a 20 μsec window per NT is centered within the 62.5 μsec window leaving 42.5 μsec for guard band and for future-proofing, Figure 3. The guard band is set to zero or to a fixed pattern such as 01010101. The structure of the supervisory messages consists of a header, a data field and a CRC trailer.

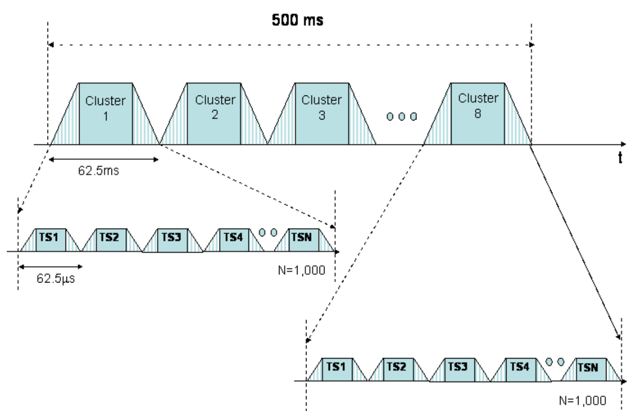

Figure 3: TDM for one optical supervisory channel and eight clusters of NTs.

In the upstream direction, the hCT-PON works in reverse, Figure 4. Each NT receives traffic from end-users, it packetizes it and it transmits each packet within its allotted time slot. Similarly, supervisory messages are time multiplexed onto the supervisory channel. Since the data channel and the supervisory channel are on different wavelengths, the NT wavelength-multiplexes the two and couples onto an optical time division multiplexing unit (OTDM).

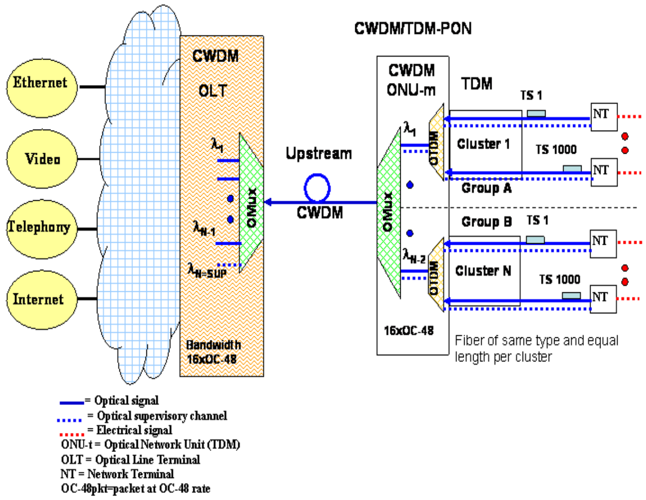

Figure 4: The hCT-PON access network (upstream direction).

Each OTDM time multiplexes packets from their corresponding cluster and transmits them to the optical multiplexer (OMux). The OTDM in this case is simple and it consists of a coupler for time division multiplexing, and a wavelength division multiplexer for the data and the supervisory channels. The OMux time division multiplexes messages from the two groups onto the two supervisory channels, and it couples all 18 CWDM channels onto the fiber, which are transmitted to the OLT.

The hCT-PON, in addition to the topology already discussed, supports the open ring physical topology, Figure 5. Moreover, the hCT-PON also supports bidirectional transmission in full hybrid mode using a circulator at each fiber end.

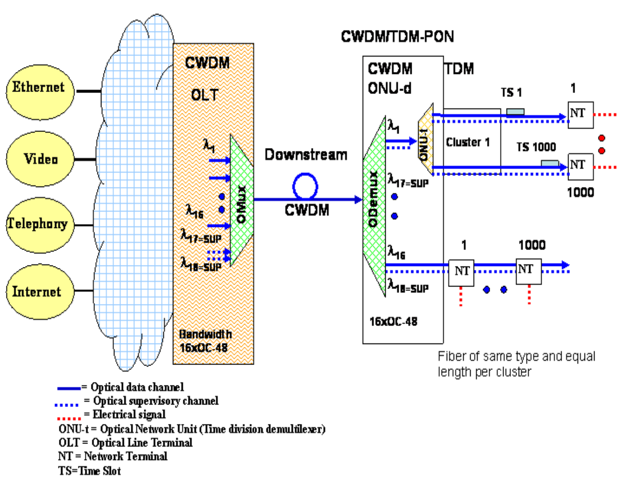

Fig. 5. The hCT-PON supports simultaneously two different topologies.

3 Levels of security in networks

Communication security is a fundamental problem for both the service provider and the end-users and recently it has received increasing attention. The reason is that recently the access network has become an entry point of sensitive information such as bank accounts, credit card numbers, trade secrets, personal information and more that trigger the appetite to bad actors. Therefore, it is very important that the communications system meets robust security requirements that protect end-user data that flow in communication links from network malicious attacks. Therefore, it is important that one examines the communication networks from the security viewpoint at various levels as each one has its own vulnerabilities.

3.1 Security Requirements

When designing a robust communication system with good security and attack-resistant attributes, one should consider the following questions:

- Will the system still be available to serve the customers in case of security attacks?
- Will the data transferred between the customers and the networks be kept secret and untouched from the attackers?
- Will the malicious attackers be recognized and be kept out of the system?

The answer to these questions leads directly to the security requirements of the communications system, which are as follows:

Availability: Availability is an important and it directly affects the level of customer satisfaction. Whenever the customers need the agreed upon QoS, the network must able to provide it despite its operational condition and attacks.

Data confidentiality: Data transmitted from an end user to another over the network are transparent or unintelligible to a third unauthorized party.

Data integrity: Assures that the data transmitted between the network and the customers has not been altered or deleted (in part) or added by the malicious attackers. The data should keep its authenticity and be genuine.

Authentication: Authentication assures that the transmitting party communicates with its intended receiving party and not a masqueraded party. Authentication is used to thwart several types of attacks such as impersonation, theft of service, denial of service (DoS) and so on.

Non-repudiation: Non-repudiation assures that the sender can not deny that the message has been sent by it, or that the recipient can not disavow that the transmitted message by the sender has not being received.

3.2 End-user data

Security of end-user data is most vulnerable to attacks as bad actors attempt to harvest personal data, gain access of bank accounts and other records or attempt to impersonate a user. The protection of end-user data is typically the responsibility of the end-user who uses encryption algorithms and secret keys to create the ciphertext. However, the secret key needs to be distributed to the rightful recipient(s) so that they can recover the data from the ciphertext. In this case, there are the following vulnerabilities:

- A bad actor may capture or copy the ciphertext, break the code and recover the data.
- A bad actor may copy the key during its distribution process.
- A bad actor may intercept and compromise the key distribution process and cause denial of service.
- A bad actor may mimic one the receiver during the key distribution process.

As a consequence, the key-type and its distribution method are very critical in secure communications. The key may be symmetric, asymmetric, continuous, timed, or one-pad.

- The symmetric key is the same for both ciphering and deciphering. Symmetric keys are known by the transmitter and the receiver and thus the secrecy of the key may be compromised at either side, transmitter or receiver.
- The asymmetric key is different for ciphering than the one for deciphering, although the latter is capable to produce the original text. The asymmetric key enhances secrecy as each side does not know of the key of the other side.
- A continuous key is used over and over again. This method lends itself to breaking the code easier using a supercomputer.
- A timed key is used for a predetermined duration of time, after which it changes to another key. This method enhances secrecy but if the duration is long then it too becomes vulnerable.
- A one-pad key is used only once; and it changes from text to text. This method is very robust if the key is truly random and as long as the text. However, if the text is too long and the key of limited length, then the key may be repeated over the length of the text in which case it may be vulnerable.

Although data ciphering is the responsibility of the end-user and it must be transparent to the network providers, the integrity of the key distribution method is a shared responsibility between user and network provider.

3.3 Link/node security

Security of the link pertains to securing the transmission paths throughout the network. The user trusts the network and expects that data and key are transported safely from unauthorized intrusions. Therefore, communication links should have sensing and detecting mechanisms to detect possible intrusions and to also employ fast protection and countermeasures strategies. Therefore, link security is viewed as being the responsibility of the network provider.

3.4 Network security

Network security is associated with node access security. Nodes are accessed for testing, management and provisioning by authorized network personnel; typically, this is done remotely over the Ethernet, Intranet or Internet and thus it may fall victim to bad actors.

Unauthorized node access may disable the node, flood the network to cause congestion, harvest user information, destroy or alter user data information, deflect traffic to other destinations, cause denial of service, or mimic a source. In telecommunication networks, such user data information may be calling numbers, traffic profiles, and so on, but no client data. In data networks, in addition to network data, harvested information may be client data such as credit card numbers, bank accounts, client records and files, connectivity maps, and so on.

Typically, network security and data delivery assurance is the responsibility of the network provider.

4 Vulnerabilities of the PON

Optical access networks such as PONs have an open structure, serve many end users and they may become the target of bad actors who look for vulnerable points. The PON structure is open because the ONU is located outside the central office (CO) and most likely in the vicinity of neighborhood, whereas the NT is often placed right at the customer premises or near it. Although these two components, ONU and NT, are under the control of the network operator, it is possible that an intruder may penetrate the ONU or the NT enclosure. In addition, sophisticated attackers may gain access to the fiber medium between components and tap it. Therefore, the hCT-PON may also be a target as it serves many thousands of end-users, some of which may be non-cooperative.

In this section, we investigate possible vulnerabilities and we attempt to assess the degree of vulnerability for the hCT-PON.

4.1 Eavesdropping

Eavesdropping is a familiar method of attack. However in hCT-PON it is not easily to achieve because in the downstream direction the primary distribution method is not the typical broadcasting as is in typical PONs and EPONS. In hCT-PON, although the NT contains a splitter/combiner and it may seem as an opportunity for attacks, the attacker must have thorough knowledge of both data time slot assignment and supervisory time slot assignment for each end-user in order to access a user channel. Conversely, because every data packet has a unique destination at the NT, ONU and OLT, and because there is no power splitter but only a passive time slot multiplexer, eavesdropping is hard to accomplish in the upstream direction. This is an important feature because in asymmetric transmission, security is more significant in the upstream than the downstream direction.

4.2 Interception

There are three possibilities for interception in the hCT-PON. If the open ring topology is employed, the NT nearest to ONU is more vulnerable to interception because data packets destined to all NTs in this group pass through it. Interception may take place by tapping a waveguide, or fiber inside the cabinet. However, this is extremely difficult to accomplish due to physical and technological constraints as sensors in the cabinet may trigger alarms that hinder attacks. If optical splitters are employed, then information may be extracted from an unused splitter port. This again implies that the attacker is able to gain access inside the cabinet, which is not an easy job.

4.3 Source mimicking, theft of service, and denial of service

In the upstream and downstream direction, NTs with the same wavelength share the upstream and downstream bandwidth with each other using TDM technology. Every NT has its specific length of time slot, and within the assigned time slot the NT sends and receives data. In fact, the duration of assigned time slot to each NT may change dynamically upon user bandwidth request. Now, if a bad actor who wants to impersonate another user must have knowledge of the bandwidth and service level agreement that were requested by that user and also knowledge of the NT identification. Additionally, the bad actor should be able to defeat the authentication protocol when service is granted to a NT.

4.4 Supervisory channel attack

In hCT-PON, the supervisory channel transports operation, administration and maintenance (OAM) control messages. It may also carry scrambling parameters and encryption keys to NTs, user identifier, and username/password, or it may contain important NT configuration data, and so on.

Thus, attacking the supervisory channel may be more serious than attacking the data channel in terms of denial of service. In view of this, the NT and OLT exchange periodically encrypted control messages that are embedded in the data packet, which confirm their proper operation. In addition, more sophisticated countermeasure mechanisms may be employed that can readily detect intruders by monitoring the channel signature [12].

5 Security measures

Reports of malicious attacks such as eavesdropping, data theft, identity theft, bank account theft, and so on, in wired, wireless and data networks are not uncommon [13]. The FTTH PON is relatively a new optical network that requires sophistication and expertise. However, bad actors are also sophisticated and with the proper know-how. Therefore, FTTH PONs should have built-in security and countermeasure features from the outset so that they do not become victims of attack, such as:

5.1 End user terminal authentication

Upon activation of the end terminal, a terminal code is sent to the network which authenticates it and grants service. In view of possible attack, the data time slot may be reassigned; that is, the hCT-PON OLT may dynamically reassign the time slot to NT upon activation and authentication such that it is almost impossible for a malevolent actor to track the data and the time slot association with the end user.

5.2 NT authentication

As the network expands and new NTs are added to the network, a self-discovery takes place to validate the NT type and assign an ID code to it. For security purposes, the NT ID code may be randomly change thus diminishing the probability of NT impersonation or mimicking.

5.3 Fiber monitoring against bad actors and countermeasure strategies.

This is addressed with well known methods that may be incorporated in the OLT so that it can detect eavesdroppers and bad actor attacks [12, 14].

When an eavesdropper is detected, then the OLT activates a countermeasure strategy whereby it sends client data over a different link whereas it continues transmitting decoy messages over the attacked link.

5.3 Key Renewal and Key Distribution

Key renewal and key distribution are important to maintain a system with high security level. The keys (public, private or secret key) are updated frequently so that the attacker can not get enough information to decrypt the ciphertext.

Key distribution protocols may also be employed in hCT-PON, and with frequently renewed keys the possibility of successful security attacks is reduced to a negligible level.

6 Conclusions

We presented a versatile, resilient and scalable passive optical network for fiber to the premises application. This optical network combines the WDM and TDM methods, hence called hCT-PON. The hCT-PON has a hierarchical tolerant topology; a WDM point-to-point between OLT and ONU, a tree topology within the ONU, and a TDM point-to-multipoint or open ring topology between ONU and NTs.

Employing the CWDM standard grid, 16 optical channels are allocated for data and two for supervision, and at OC-48 per optical channel, an aggregate 40 Gbps is achieved, which is elastically distributed up to 16,000 end-users (at 2.5 Mbps per user) with protocol transparency meeting true triple play services. The hCT-PON is highly scalable such that as more optical channels are added, more bandwidth is delivered to potentially 40,000 end-users.

We identified different levels of security and responsibilities in the communications network. We identified possible vulnerabilities in the optical access network and we examined the security features of the hCT-PON network. In conjunction with encryption methods, robust protocols, intruder identification methods, channel signature monitoring, dynamic time-slot assignment and reassignment methods, and cabinet alarms, the possibility of eavesdropping, service theft, source mimicking and denial of service becomes either non-existent or negligible. Work continues in algorithmic encryption key distribution as well as in intruder detection and countermeasures strategies.

References

1. S.V. Kartalopoulos, *DWDM Networks, Devices, and Technology*, (IEEE Press/Wiley, NJ, 2003).
2. Telcordia GR-13, "*Generic requirements for Pedestal Terminal Closures*", (Sept 2002).
3. Telcordia GR-902, "*Generic requirements for Non-Concrete Splice Enclosures*", (1988).
4. Telcordia GR-3120, "*Generic requirements for Hardened Fiber Optic Connectors*", (2004).

5. Telcordia GR-3121, "*Generic requirements for Below Ground Cabinets*", (2004).
6. Telcordia GR-3122, "*Generic requirements for FITS (Factory Installed Termination System*)", (2004).
7. Telcordia GR-3123, "Generic requirements for Indoor Fiber Distribution Hubs", (2004).
8. ITU-T recommendation G.694.2, "*Spectral grids for WDM applications: CWDM Wavelength grid*", (6/2002).
9. Andres Sierra and S.V. Kartalopoulos, "Evaluation of Two Prevalent EPON Networks Using Simulation Methods", Proceedings of the Advanced International Conference on Telecommunications 2006, Guadeloupe, French Caribbean, (2/19-22/06), session AICT-3, CD-ROM product: E2522, ISBN: 0-7695-2522-9.
10. S.V. Kartalopoulos, "Next Generation Hierarchical CWDM/TDM-PON Network with Scalable Bandwidth Deliverability to the Premises", *Optical Systems and Networks*, **2**, 164-175 (2005).
11. N. Kolothody, A. Sierra, and S.V. Kartalopoulos, "Network Protection on Next Generation PON", NOC 2005, 10th European Conference on Networks and Optical Communications, University College London, July 5-7, 107-114 (2005).
12. S.V. Kartalopoulos, "Optical Channel Signature in Secure Optical Networks", *WSEAS Transactions on Communications*, **4**, 494-504, (2005).
13. S.V. Kartalopoulos, "A Primer on Cryptography in Communications", *IEEE Communications Magazine*, **44**, 146-151 (2006).
14. S.V. Kartalopoulos, "Distinguishing between Network Intrusion and Component Degradations in Optical Systems and Networks", *WSEAS Transactions on Communications*, **4**, 1154-1161, (2005).