WiMAX-VPON: A Framework of Layer-2 VPNs for Next-Generation Access Networks

Ahmad R. Dhaini, Pin-Han Ho, and Xiaohong Jiang

***Abstract*—This paper proposes a novel framework, WiMAX-VPON, for realizing layer-2 virtual private networks (VPNs) over the integrated IEEE 802.16 Ethernet Passive Optical Network fiber-wireless technology; which has been lately considered as a promising candidate for next-generation backhaul-access networks. With the proposed framework, layer-2 VPNs support a bundle of service requirements to the respective registered wireless/wired users. These requirements are stipulated in the service level agreement (SLA) and should be fulfilled by a suite of effective bandwidth management solutions. For achieving this, we propose a novel VPN-based admission control (AC) and bandwidth allocation scheme that will provide per-stream quality-of-service (QoS) protection and bandwidth guarantee for real-time flows. The bandwidth allocation is performed via a common medium access control (MAC) protocol working in both the optical and wireless domains. An event-driven simulation model is implemented to study the effectiveness of the proposed framework.**

***Index Terms*—Ethernet PON (EPON); IEEE 802.16 (WiMAX); QoS; virtual private network (VPN).**

I. Introduction

The massive increase of broadband access applications with varying QoS requirements, such as Internet Protocol television (IPTV) and video-on-demand (VoD), has significantly contributed to the evolution of next-generation wired and wireless networks.

Lately, the integration of Ethernet Passive Optical Network (EPON) and WiMAX has been presented as an attractive broadband access network (BAN) solution [2]–[4]. The complementary features of these networks has motivated interest in using EPON as a backhaul to connect multiple dispersed WiMAX base stations (BSs) [2], [5]. The integration can take advantage of the bandwidth benefit of fiber communications, and the mobile and non-line-of-sight (NLOS) features of wireless communications. More specifically, EPON and WiMAX perfectly match in terms of capacity hierarchies. EPON for instance, supports a total of $1\ Gbps$ bandwidth in both downstream and upstream directions, shared by typically $N \leq 32$ remote optical network units (ONUs). On average, each ONU accesses $\approx 70\ Mbps$ bandwidth, which matches the total capacity offered by a WiMAX BS over a $20\ MHz$ channel as well. In addition, the integration enables integrated resource allocation and packet scheduling paradigms that help to better support the emerging quality-of-service (QoS) services, as well as to improve the overall network throughput. Finally, the integration can help realizing fixed mobile convergence (FMC) [6] by supporting mobility in the broadband access; thereby significantly reducing network design and operational costs [2].

The EPON-WiMAX integration of has been well reported in the past few years [2], [3]. Nonetheless, building up virtual private networks (VPNs) directly on the EPON-WiMAX integration has never been investigated in the literature. In addition, the already presented bandwidth allocation schemes are too trivial ([3], [9]–[11]) and are neither able to provide per-flow QoS protection nor able to offer end-to-end (from the subscriber station [SS] to the optical line terminal [OLT]) bandwidth guarantee; features that are essential for establishing VPN tunnels over EPON-WiMAX.

A. Supporting VPNs over EPON-WiMAX

VPNs have been known as a superb technology that are provisioned over a public or third party network infrastructure, and are positioned to provide dedicated connectivity to a closed group of users with a strong per-flow QoS guarantee [12].

VPNs over EPON-WiMAX could be deployed to support mission-critical (police, healthcare, fire-fighting), governmental or corporate systems, in order to achieve a secure high-speed and efficient mobile connectivity among private users in rural and urban areas.

Due to its support for premium services with custom-designed control, diverse QoS requirements and security assurance intrinsically provided by the layer-2 medium access control (MAC) protocols [13], building up layer-2 VPNs is considered the best suitable when an EPON-WiMAX integrated network is installed. Such VPNs are referred to as *layer-2 VPNs* in the sense that the VPNs are built upon the layer-2 protocols. Compared with layer-3 and layer-1 VPNs [14], [15], layer-2 VPNs can do a better job in resolving the complications due to network dynamics, communication media heterogeneity, and fast changing channel status, at the expense of a more complicated design

Manuscript received xxx, 2010; revised xxx, xxx.

Preliminary results of this work appeared in ICC'10 [1].

A. R. Dhaini and P.-H. Ho are with the Department of Electrical and Computer Engineering, University of Waterloo, Canada (e-mail: adhaini@uwaterloo.ca).

X. Jiang is with the School of Systems Information Science, Future University-Hakodate, Japan (e-mail: jiang@fun.ac.jp).

that considers any possible layer-2 issue. In other words, a specialized software that forms a control plane has to be in place instead of either simply deploying standard IP protocol stacks on top of layer-2 (in the case of layer-3 VPNs), or deploying hardware-dependant solutions that are specifically designed to operate over EPON and WiMAX networks only (in the case of layer-1 VPNs).

For these reasons in this paper, we investigate the realization of layer-2 VPNs over the EPON-WiMAX integration. To achieve the latter, we propose a novel framework for establishing IEEE 802.16 virtual private passive optical networks, namely WiMAX-V**P**ON.

To the best of our knowledge, this is the first work that considers the support of layer-2 VPNs over EPON or WiMAX networks, or over their integration as well.

B. Contributions of This Work

Supporting layer-2 VPNs entitles the emergence of two main resource management challenges, that will be the focus of our study:

- Meeting the QoS requirements of the supported VPN services.
- Providing guaranteed resources for each service.

To resolve these issues, we propose a new VPN-based admission control (AC) and upstream/uplink dynamic bandwidth allocation (DBA) paradigm that will provide guaranteed bandwidth for each VPN service. This paradigm will ensure and protect end-to-end per-flow QoS (in both the wireless and optical planes) for new and existing traffics, respectively, while maintaining their expected performance as defined in the service level agreement (SLA).

More specifically, the contributions of this paper can be summarized as follows:

1) This paper proposes for the first time to our best knowledge, a novel framework for supporting layer-2 VPNs over the EPON-WiMAX integration. Layer-2 VPNs act as a cost-effective, secure and efficient link between the underlying fiber-wireless infrastructure and higher-level mission-critical, governmental or corporate services.
2) This paper presents a new QoS-provisionning framework that enables a bandwidth and QoS assurance for each wireless registered user with the "freedom" of connecting to any BS. This is achieved by *reserving* the VPN bandwidth for the respective users and allocating it accordingly by means of the DBA. This can ultimately facilitate a smooth handover operation of wireless users between different BSs (the handover operation is not covered in this paper).
3) Unlike the reported related work on EPON-WiMAX [3], [9]–[11], this paper offers a novel joint VPN-based AC and DBA scheme that enables an end-to-end (from SS to OLT) QoS guarantees, while taking into consideration the wireless channel state information (CSI).
4) The proposed AC scheme is implemented on a three-stage system, which is involved in the collaboration among the SSs, ONU-BS, and OLT. Such a decentralized AC design reduces the complexity and "decision time" of the AC scheme, as opposed to installing it at one end (e.g., the OLT).
5) WiMAX-V**P**ON provides a per-flow QoS protection as well as bandwidth guarantee for admitted traffic. Our simulation results will show that in the case where no AC is applied, a drastic performance degradation is witnessed for already admitted and newly admitted VPN services.

The rest of the paper is organized as follows. In Section II, the different EPON-WiMAX architectures that may be used for supporting our framework are summarized, and the research challenges related to QoS and resource management are highlighted. WiMAX-V**P**ON is presented in Section III, and its potential advantages and the related design issues are demonstrated. The proposed three-stage admission control mechanism is described in Section IV, and the VPN-based bandwidth allocation scheme is presented in Section V. Section VI presents the performance evaluation and Section VII concludes the paper.

II. EPON-WiMAX Related Challenges

This section summarizes the EPON-WiMAX architectures that may be deployed to carry the proposed WiMAX-V**P**ON framework. In addition we overview the challenges related to resource allocation and bandwidth management, which are crucial in the design and support of layer-2 VPNs over the integration.

A. EPON-WiMAX Architectures

Several architectures were proposed for the EPON-WiMAX integration [2], [3], with a point-to-multi-point (PMP) topology. The disparity between these architectures is in the mounting procedure of the EPON's ONU and the WiMAX's BS.

1) Independent: In this architecture, EPON and WiMAX work independently. As a result, each ONU would consider a WiMAX BS as an end-user and can interconnect it through Ethernet (a common supported standard interface).

2) Hybrid: In this architecture, ONU and BS are mounted in one box, so called *ONU-BS*.

3) Unified Connection-Oriented: The purpose of this architecture is to handle the connection-oriented bandwidth allocation paradigm offered by the IEEE 802.16 MAC rather than the queue-oriented one offered by the IEEE 802.3ah MAC. This architecture also recommends the installation of ONU-BS as one box.

4) Microwave-over-Fiber (MOF): In this architecture, a "dumb" antenna is connected to the EPON's ONU, responsible for relaying WiMAX radio signals to and from its associated micro-cell. Here, one optical subcarrier and another wireless one are used to transfer signals from the wireless to the optical domain.

5) Virtual: The authors of [3] proposed a different approach for designing the ONU–BS communication while preserving the current EPON and WiMAX standards. This was achieved by proposing the concept of VOB (*Virtual* ONU-BS) where a network *bridge* is deployed in between.

Note that a mesh-based EPON-WiMAX architecture may be alternatively installed, to take advantage of the multi-hop routing capabilities of mesh networks so as to balance the network load over the shared wireless media. Nonetheless, routing and the related challenges are not covered in this paper. More details on how to perform routing in fiber-wireless mesh-based networks can be found in [16].

One of the advantages of WiMAX-PON (as we will see later) is that it is designed to be architecture-independant. Hence, the decision of selecting any of the described architectures is left to the network designer's preferences. Such a decision could be made based on the pros and cons of each architecture; which are detailed in [2]–[4].

B. Bandwidth Allocation & Admission Control

The integrated EPON-WiMAX network is expected to deliver common services with the same level of quality and matching performance behavior. Such features can be achieved by manipulating the bandwidth allocation and admission control schemes. This property has been widely investigated in EPONs [7], [8], [17] and WiMAX [18] separately, but few work has been done in the integration. In general, the efforts of bandwidth allocation and admission control may fall in either one of the following categories: (1) Upstream/Uplink, and (2) Downstream/Downlink.

In the downstream direction, both EPON and WiMAX simply broadcast data packets over the shared media. Previous research efforts on WiMAX scheduling, resource allocation, and admission control in the downstream direction have been extensively reported [18], and the additional consideration of EPON on top of WiMAX has not brought up more issues due to the broadcast-in-nature transmission in both systems. On the other hand, in the upstream direction, the EPON's ONUs and WiMAX's SSs launch packets in the shared media, respectively, and have to be synchronized such that the packets can be successfully transmitted to the corresponding OLT and BS. This is expected to fundamentally change the nature of the problem. Therefore, the paper focuses on solutions pertaining to dynamic bandwidth allocation and admission control for EPON-WiMAX networks in the upstream direction.

In the past couple of years, some related works addressed the upstream resource management problem in EPON-WiMAX (e.g., [3], [9]–[11]). Nonetheless, none of the proposed schemes were able to provide bandwidth guarantee or QoS protection for the incoming flows; properties that are required for the support of VPNs. Therefore adopting any of the proposed mechanisms is not a viable solution in the context of layer-2 VPNs over the integrated network. Conversely, our proposed framework will address these issues and will provide effective uplink resource allocation solutions.

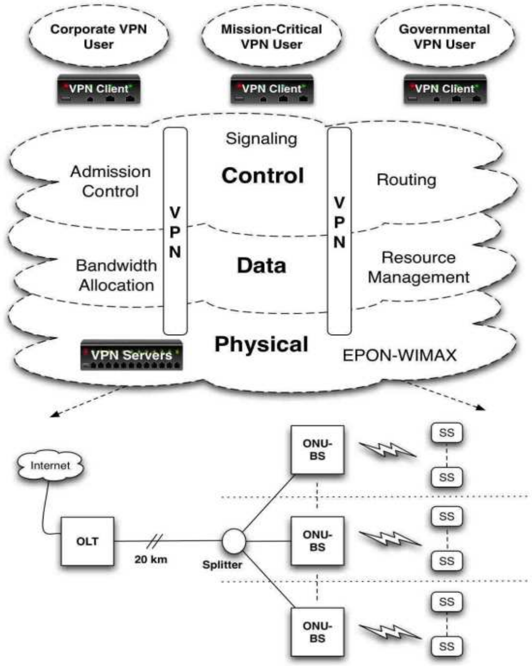


Fig. 1. Layer-2 VPNs over EPON-WiMAX

III. WiMAX-VPON: Layer-2 VPNs over EPON-WiMAX

A. Network Model

To support VPN services on EPON-WiMAX networks, one approach is to deploy VPNs in the network layer (i.e., IP layer) in the ONU-BSs. This is certainly at the expense of higher control and management overhead due to the protocol overlay and potentially longer delay. A layer-2 VPN over the EPON-WiMAX domain is expected to achieve a much more efficient and light-weight network management, which is necessary to support a multi-service and multi-customer environment. In the proposed framework, each VPN serves as a *shim layer* that maps those service requirements and commands to the MAC layer routing, resource allocation, and AC mechanisms, via a suite of service access points (SAPs) and primitives. Thus, each VPN corresponds to a specific service requirement bundle such that the users can dynamically configure their service requirements. This feature is essential to support stringent bandwidth guarantee and possible preemption requests.

Typically, a VPN consists of three planes 1) control, 2) data and 3) physical. The control plane handles operations such as connection establishment, routing and AC. The data plane is concerned with the bandwidth management for VPN services and meeting their SLA-based QoS requirements. The physical plane is basically the underlying network infrastructure (here, EPON-WiMAX). The realization of multi-planed VPNs over EPON-WiMAX is illustrated in Fig. 1.

With the current heterogenous Internet and access network deployment, it is possible that a connection goes through multiple VPNs supported by different technologies at different network layers, or even any data path without any QoS protection and class of service (CoS); however, the paper emphasizes on the implementation of layer-2 VPNs in terms of per-flow QoS protection, custom-design network control, performance parameter selection, and tunneling between nodes at the network boundary. In the context of EPON-WiMAX networks, the network boundary is formed by the end-users and the OLT. A VPN gateway could be deployed at the OLT so as to interface with other VPNs under some agreements/policies. The design of the VPN gateway and related issues are nonetheless out of scope of the paper.

B. System Model

The integration of EPON-WiMAX requires the identification of multiple design and operation themes. In this section, we discern these matters in order to complete the support of layer-2 VPNs over EPON-WiMAX.

1) Principle of Operation: EPON supports differentiated services (DiffServ), whereas WiMAX supports integrated services (IntServ), especially in the case of Grant Per Connection (GPC) mode [19]. Furthermore in EPON, incoming IP datagrams are encapsulated in Ethernet frames according to the IEEE 802.3 standard [20], whereas they are launched as IEEE 802.16 PDUs in the case of WiMAX [19]. Therefore to enable a unified connection-oriented control from the SS to the OLT, and since WiMAX allows for a finer bandwidth allocation than EPON, we propose to modify the MAC protocol in EPON to support connection-oriented requests from the ONU-BS to the OLT. This can be implemented by launching IEEE 802.16 MAC PDUs encapsulating Ethernet frames in the optical domain, rather than directly carrying Ethernet frames in upstream and downstream frames/bursts of EPON [2]. As a result, the whole integrated system will support IntServ, and can be controlled by unified connection-oriented bandwidth management protocols, launching WiMAX PDUs. In addition, no control frames will then be required in the Ethernet frame layer for the bandwidth allocation and network control in the optical domain.

2) Wireless Channel Model: The wireless channel is modeled as Rayleigh fading channel [21] that is suitable for flat-fading channels as well as frequency-selective fading channels encountered with orthogonal frequency division multiplexing (OFDM). The received signal of an SS n is computed as follows:

$$rs_n = h_n(t) \times ts(t) + bn_n(t) \tag{1}$$

where $ts(t)$ is the transmitted signal and $bn_n(t)$ is the background noise at time t. $h_n(t)$ is the total instantaneous channel gain that jointly considers the multipath effect, shadowing effect, and path loss exponent. For fixed users, the average channel gain h_n can be used and is described as follows [22]:

$$h_n = m_n \sqrt{\frac{c}{D_n^{\gamma}} \times S_n} \tag{2}$$

where D_n is the distance between SS n and the connected ONU-BS, c is a constant incorporating the transmission and receiving antenna gain and γ is the path loss exponent. S_n is a random variable for the shadow fading effect and m_n is the multipath fading effect that represents the Rayleigh fading channel. The average signal-to-noise ratio (SNR) for SS n is given by $SNR_n = \frac{P_n}{V_{bn}}$, where V_{bn} is the background noise variance. P_n is the receiving power and is given by $P_n = |h_n|^2 P_t$, where P_t is the total transmitter power of the ONU-BS. Assuming that P_t is fixed, P_n can be allocated by the ONU-BS such that the maximum SNR (SNR_n^{max}) is achieved.

We assume that multiple transmission modes are available, with each mode representing a pair of a specific modulation format and a forward error correcting (FEC) code. Based on the CSI estimated at the receiver, the adaptive modulation and coding (AMC) controller determines the modulation-coding pair/mode, which is sent back to the transmitter through a feedback channel for the AMC controller to update the transmission mode. In our framework we consider the transmission modes tabled in Table I. We also adopt the OFDM-time division multiple access (OFDM-TDMA) air interface for the wireless channel access [3]. Thus, each user/SS will be allocated all the OFDM subcarriers and a time division duplexing (TDD) time-slot (or TDD frame physical slots) for uplink transmission.

Given a bit error rate (BER) less than 10^{-6}, Table I lists the convolutionally coded M-ary rectangular or square QAM modes, adopted from the HIPERLAN/2 or the IEEE 802.11a standards [23] with specific SNR_n^{max} and bits/symbol [24].

Let N_d be the total number of OFDM data subcarriers and T_{sym} the OFDM symbol duration in seconds. For a transmission mode x (table I), SS n's transmission rate R_n^x (bps) is computed as follows:

$$R_n^x = \frac{N_d \times W_{sc}^x \times CR^x}{T_{sym}} \tag{3}$$

Alternatively, orthogonal frequency division multiple access (OFDMA) could be adopted as well. Nonetheless, this will only increase the complexity of the resource management scheme, since the ONU-BS (or OLT) will be required to perform power allocation as well as arbitrate the transmission over the time

TABLE I
ADAPTIVE MODULATION AND CODING (AMC) MODES

Modulation	BPSK	QPSK		16 QAM		64 QAM	
Transmission Mode (X)	1	2	3	4	5	6	7
Coding Rate (CR)	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{3}{4}$	$\frac{1}{2}$	$\frac{3}{4}$	$\frac{2}{3}$	$\frac{3}{4}$
Receiver SNR (db)	6.4	9.4	11.2	16.4	18.2	22.7	24.4
bits/symbol (ϕ)	0.5	1	1.5	2	3	4	4.5
Coded bits/subcarrier (W_{sc})	1	2	2	4	4	6	6

and frequency domains. We favored the OFDM-TDMA access technology to keep the integration ”simple”, as EPON only supports TDMA. This will allow our designed DBA to be adopted in both the optical and wireless domains with minimal changes (as we will see next). Moreover, since the main feature of layer-2 VPNs is ”light-weightness”, we aim at maintaining such a feature in the design of the MAC protocol as well. However, we believe that the operation of WiMAX-V**P**ON over OFDMA networks that can offer an effective NLOS support, is worth investigation; hence, we plan to cover this aspect in the future.

3) QoS Mapping: The IEEE 802.16 standard defines five classes of services, namely Unsolicited Grant Service (UGS), real-time Polling Service (rtPS), extended real-time Polling Service (ertPS, defined in 802.16e), non-realtime Polling Service (nrtPS) and best-effort (BE) [19]. On the other hand, an IEEE 802.13ah ONU is allowed to support and report up to eight queues [20]. Typically, three classes of services are supported in an EPON: (1) Expedited Forwarding (EF) for constant bit rate (CBR) traffic (2) Assured Forwarding for variable bit rate (VBR) traffic, and (3) BE [7]; each assigned one buffering queue. To simplify the bandwidth allocation operation, we perform a one-to-one mapping between the CoS queues in the BS and the ones in the ONU [3]. Hence we will have totally five queues for all UGS, rtPS, nrtPS, ertPS and BE classes of services. Consequently, the users' incoming flows are initially classified at the SS-side using the packet classifier and mapped to the corresponding CoS queue. In case a *VOB* is installed, each transmitted packet is then classified at the BS-side and then mapped to the corresponding ONU CoS queue. Alternatively if a ”one-box” ONU-BS is mounted, incoming packets can be directly mapped to one of the five corresponding buffering queues. Before being buffered, flows can be subject to traffic policing and admission control.

4) Requesting and Granting: Requesting and *granting* are two fundamental operations standardized in EPON and WiMAX [19], [20], and are used to exchange bandwidth allocation control messages. In the wireless plane, the *polling mode* is adopted to achieve better sensitivity in QoS guarantee. The polling mode enables every ONU-BS to poll its SSs in each OFDM frame so as to gather the bandwidth requirement of each SS. Once available, each ONU-BS performs the proper bandwidth allocation and performs the granting in a GPC fashion [19]. Each grant specifies the number of physical slots used for upstream transmission in the next OFDM frame. Typically, each SS reports its requirements using the BW_Request message. Nonetheless, the UGS traffic does not need to request as its rate is constant. Thus, the ONU-BS should reserve the bandwidth for the admitted UGS flows.

In the optical plane and according to the multi-point control protocol (MPCP) [20], each ONU is allowed to request bandwidth for up to 8 queues in each REPORT message. To preserve the REPORT structure, each ONU-BS will report the buffering queue occupancies for real-time flows (i.e., UGS, rtPS, ertPS and nrtPS queues), and will use the remaining four fields to report up to four BE VPN bandwidth needs. If an ONU-BS provisions more than four VPNs, multiple REPORT messages may be used to report the rest of VPNs. The latter can be implemented by having a counter that keeps track of each BE packet buffered in the BE queue. On the other hand, a GATE message includes a grant for each real-time buffer request and an aggregate grant for all the VPN BE traffic requests.

C. VPN-based QoS provisioning

With our QoS provisioning framework, each upstream V**P**ON cycle T_{cycle}^{VPON} is divided into two *sub-cycles*. The first sub-cycle βT_{cycle}^{VPON} is shared among all the K VPNs. The second sub-cycle $(1-\beta)T_{cycle}^{VPON}$ is shared among non-VPN services. Let B_{min}^{k} be the bandwidth reserved for VPN k (denoted as V_k) in each transmission cycle. T_g denotes the guard time that separates the transmission windows of two consecutive ONU-BSs, and R_N the transmission speed of PON in Mbps. In addition, let each V_k be given a weight w_k to determine its *paid/committed* bandwidth. Therefore, B_{min}^{k} (in bytes, thus divide by 8) is given as follows:

$$B_{min}^{k} = \frac{(\beta T_{cycle}^{VPON} - K \times T_g) \times R_N \times w_k}{8} \tag{4}$$

where $\sum_{k=1}^{K} w_k = 1$. An important parameter in the proposed cycle framework is the minimum per-VPN throughput that allows the BE traffic to be free from starvation. Such reserved quota for BE traffic takes a portion of αB_{min}^{k}, while the real-time flows will share

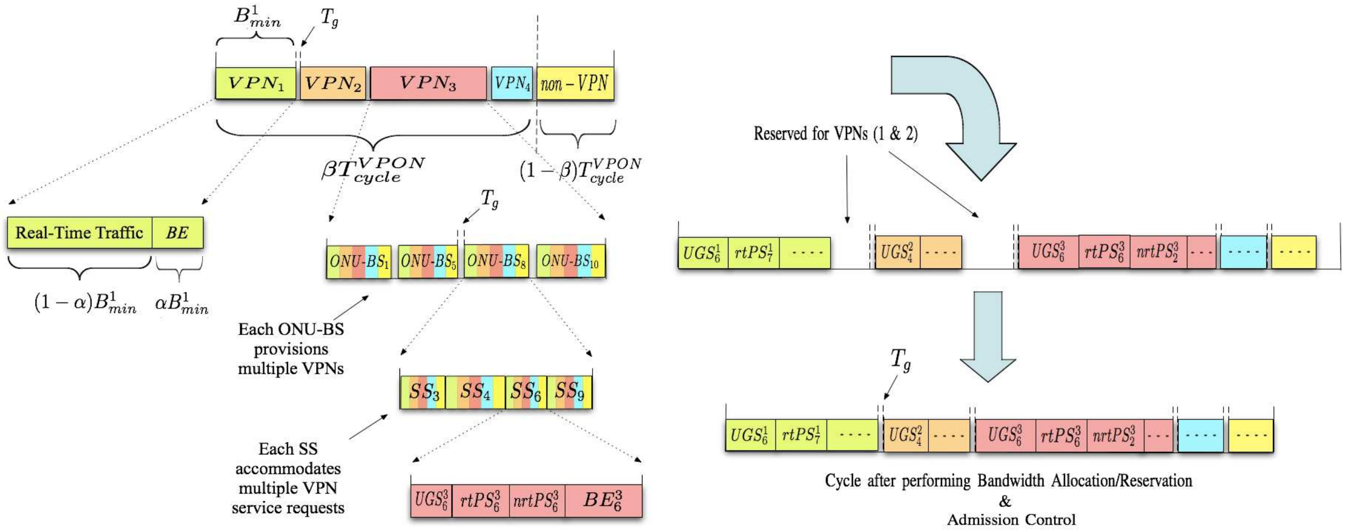


Fig. 2. Proposed VPON QoS-Provisionning Framework

the remaining bandwidth, that is $(1-\alpha)B^k_{min}$. Here, a packet preemption mechanism may be allowed such that the BE traffic is preempted in order to accommodate more real-time flows and/or to maintain the bandwidth requirement for the existing higher prioritized flows that are possibly subject to bad channel conditions. A graphical illustration of the proposed QoS-provisioning framework is given in Fig. 2.

As noticed, our framework is designed to be architecture-independent. Namely, it can operate on top of any of the EPON-WiMAX architectures that were described earlier. In addition, it is designed to allow each SS to access its VPN reserved bandwidth through any ONU-BS; which can ultimately enable a robust handover operation. Yet, handover operations and related issues are outside the scope of this paper.

D. Traffic Characteristics and QoS Requirements

CBR traffic (such as UGS) is non-bursty and can be simply characterized by its mean data rate (μ) in bits per seconds (bps). On the other hand, VBR traffic (such as rtPS and nrtPS) is bursty in nature and is characterized by the following parameters:

- Peak Arrival Data Rate (σ) in bits per second (bps).
- Maximum Burst Size (ρ) in bits.
- Delay Bound (θ) which is the maximum amount of time in units of seconds allowed to transport a traffic stream measured between the arrival of the flow to the MAC layer and the start of transmission in the network.
- MAC service data unit (MSDU) maximum and minimum sizes (L_{max} and L_{min}). For fixed frame size streams of size L, the mean frame size $\bar{L}$ = L.

Finally, BE traffic is bursty and requires neither delay requirements nor bandwidth guaranteed.

Once all these parameters are specified by the end-user, the problem left for the admission control unit (ACU) is simply to determine whether a new stream should be admitted and whether its QoS requirements can be guaranteed while the QoS requirements for already admitted streams can be protected. For CBR traffic, a flow is admitted in case its mean data rate can be supported by the current system. For VBR traffic, the AC may admit a VBR stream according to either its peak rate or its mean data rate [25], which obviously causes a dilemma between the boost of network utilization and a more secured service guarantee, respectively. With the proposed framework, our approach defines a suite of new traffic parameters via a dual-token leaky bucket (DTLB) model for traffic regulation. The DTLB is situated at the entrance of the MAC buffer and is associated with each stream. The bucket size is calculated as follows:

$$S = \rho \times (1 - \mu/\sigma) \tag{5}$$

Accordingly, the arrival process of the stream passing through the filter is computed as follows [25]:

$$A(t, t+\tau) = \min(\sigma\tau, S + \mu\tau) \tag{6}$$

where $A(t, t+\tau)$ is the number of cumulative arrivals during $(t, t+\tau)$. The arrival rate curve could be constructed from the above equation and is shown in Fig. 3. Therefore, the guaranteed rate for every real-time flow i belonging to V_k can be easily derived from Fig. 3 using the distance formula [17], [25]:

$$g^k_i = \frac{\rho_i}{\theta^k_i + \frac{\rho_i}{\sigma_i}} \tag{7}$$

In the wireless domain, transmissions are error-prone due to fluctuating channel conditions. Thus, the sense of per-flow based bandwidth guarantee becomes tricky. A common method is to pursue a statistic sense of bandwidth guarantee. By assuming a frame error probability $P_{error,i}$ for stream i, the transmission rate

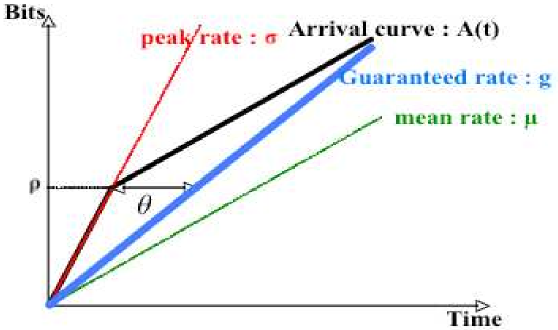


Fig. 3. Guarantee Bandwidth Derivation Graph

in the wireless domain, such that a VBR stream perceived bandwidth can be statistically guaranteed, is obtained as follows:

$$g_i^k = \frac{\rho_i}{(\theta_i^k + \frac{\rho_i}{\sigma_i})(1 - P_{error,i})} \tag{8}$$

Note that $P_{error,i}$ is a function of the channel condition (i.e., the SNR), which is random in nature as described in Section III-B.

Similarly, the transmission rate for statistical guarantee of a CBR stream perceived bandwidth, pertaining to $P_{error,i}$, can be obtained as follows:

$$g_i^k = \frac{\mu_i}{1 - P_{error,i}} \tag{9}$$

With the above computations, a rate-based admission control [17] can be designed as simple as follows: Given the allocated bandwidth for V_k (denoted as B_k^G), a new flow $i+1$ can be admitted if:

$$g_{i+1}^k + \sum_{i=1}^{h_k} g_i^k \leq B_k^G \tag{10}$$

where h_k is the number of real time streams (CBR or VBR) of VPN k. However, there are other restrictions that need to be taken into consideration in VPN-based EPON-WiMAX networks, rather than simply admitting based on such a rule. Due to the fact that V_k could be simultaneously provisioned at multiple ONU-BSs, B_k^G is shared among all the ONU-BSs that provision V_k at a first stage, and meanwhile shared among all the SSs with the same provisioning capability at a second stage. In this case, the AC's decision making needs to further consider the network architecture and SSs' distribution. For this reason, we propose a three-stage AC mechanism, where all the SSs, ONU-BSs and OLT collaboratively perform AC in order to satisfy the conditions defined in Eqs. (8) and (9).

IV. VPN-Based Admission Control (VPN-AC)

This section describes the proposed three-stage admission control (AC) mechanism for real-time flows. Note that the BE traffic requests are always admitted. The admitted flows will be further distinguished according to a dynamic bandwidth allocation algorithm (which will be provided in Section V).

A. SS-based Admission Control (SAC)

Let M_k be the number of ONU-BSs that provision V_k and share the total allocated bandwidth αB_{min}^k for maintaining the minimum BE bandwidth. Each ONU-BS is allocated an equal portion of the currently available bandwidth at the OLT for the BE traffic of V_k, namely $\frac{\alpha B_{min}^k}{|M_k|}$. This information is broadcasted by the OLT to all the ONU-BSs in the registration phase. Let $R_{j,BE}^k$ denote the rate reserved for BE traffic of V_k at each ONU-BS j, which can be expressed as:

$$R_{j,BE}^k = \frac{\alpha B_{min}^k \times 8}{|M_k| \times \beta T_{cycle}^{VPON}} \tag{11}$$

Let N_k denote the number of SSs using the services of V_k via ONU-BS j. Thus, the reserved BE rate for each user/SS n of V_k at ONU-BS j, which is denoted as $R_{j,BE}^{n,k}$, can be expressed as:

$$R_{j,BE}^{n,k} = \frac{\alpha B_{min}^k \times 8}{|N_k| \times |M_k| \times \beta T_{cycle}^{VPON}} \tag{12}$$

According to (10), a new real-time (RT) flow $i+1$ by SS n could be admitted to V_k at ONU-BS j if the following condition is satisfied:

$$g_{n,i+1}^k + \sum_k \sum_i \left(g_{n,i}^k + R_{j,BE}^{n,k} \right) \leq R_n^x \tag{13}$$

where $g_{n,i+1}^k$ is the guaranteed rate (bps) for the flow computed according to either Eq. (8) or Eq. (9).

Using SAC, a new flow is admitted at the SS-side if its guaranteed bandwidth plus the already existing traffic (real-time and best effort) is less than or equal to the SS PHY transmission rate. This condition also implies that SS n's PHY rate (or the adapted AMC) cannot go lower than R_n^x. Otherwise, the bandwidth will no longer be guaranteed. Thus, our system ensures guaranteed bandwidth for admitted flows under the condition that its respective SS maintains a minimum PHY rate that will obey the specified rule.

B. ONU-BS-based Admission Control (OBAC)

Once a flow is conditionally admitted at the SS level, it is reported to its connected ONU-BS j. The ONU-BS then locally performs rate-based AC according to the bandwidth requirement of the arriving flow along with the overall wireless bandwidth availability. The condition for flow $i+1$ of V_k from SS n to be admitted at ONU-BS j is defined as follows.

$$\frac{g_{n,i+1}^k}{R_n^x} + \sum_k \sum_n \sum_i \frac{g_{n,i}^k}{R_n^x} \leq NBR - \sum_k \sum_n \frac{R_{n,BE}^k}{R_n^x} \tag{14}$$

Here, the *nominal bandwidth ratio* is defined as $NBR = (1 - C_o)$, where C_o represents the control overhead ratio caused by the signaling required to perform resource allocation and will be evaluated via simulations. $\frac{g_{n,i}^k}{R_n^x}$ is the ratio of channel rate required to transmit flow i of V_k in one-second time interval at SS

n. If sufficient bandwidth is available to accommodate the flow, it will be reported to the OLT for the final stage of AC in the VPN level.

C. OLT-based Admission Control (OLAC)

After passing the first and second stages, flow $i+1$ is admitted by the OLT if sufficient bandwidth is available in V_k. The condition of admission is defined as follows:

$$g^k_{i+1} + \sum_i g^k_i \leq \frac{(1-\alpha)B^k_{min} \times 8}{\beta T^{VPON}_{cycle}} \tag{15}$$

In summary, VPN-AC is used to achieve end-to-end (from SS to OLT) bandwidth guarantee for each admitted flow. It is designed for the scenario where the users of a VPN may connect to any ONU-BS, but are not allowed to utilize more bandwidth than their predefined bandwidth share in the upstream channel. Such a feature is critical to build-up layer-2 VPNs over EPON-WiMAX integration while at the expense of longer decision making delay at each SS in an order of milliseconds during the next polling interval. Nonetheless, a delay within the maximum OFDM frame length (i.e., $20ms$ [19]) is considered tolerable.

V. VPN-based Dynamic Bandwidth Allocation (VPN-DBA)

As a complement to the AC scheme in the course of per-flow QoS guarantee, we provide a VPN-based dynamic bandwidth allocation (VPN-DBA) scheme that is installed at both OLT and ONU-BSs, in order to arbitrate the transmission of ONU-BSs over the upstream optical channel, and to arbitrate the transmission of SSs over the uplink wireless channel, respectively. Moreover at the ONU-BS, VPN-DBA takes into consideration different channel conditions of each SS reported through the CSI, where the allocated time share is adaptive to the fluctuating channel condition in order to achieve the desired bandwidth guarantee.

A. VPN-DBA at ONU-BS

To determine the time share for a flow, each ONU-BS j calculates the aggregated rates of the admitted real-time flows (denoted as $G_j = \sum_k \sum_i g^k_i$), and the total reserved VPN BE rates (denoted as $R_{j,BE}$) using the following equation:

$$R_{j,BE} = \sum_k R^k_{j,BE} \times \Gamma_k \tag{16}$$

where,

$$\Gamma_k = \begin{cases} 1 & \text{if } \forall i, \exists\ SS_i \text{, such that } |SS_i| \text{ has } V_k \text{ requests} \\ 0 & \text{otherwise} \end{cases} \tag{17}$$

To protect RT traffic from being shared with BE traffic, in our scheme, each cycle/frame is divided into $K+1$ sub-cycles, where sub-cycle 1 is for real-time flows, while the rest K sub-cycles are for all VPNs' BE traffic. The size of each sub-cycle should be determined in each polling interval so as to adapt to the bandwidth request fluctuation of each flow. Thus, $T^{802.16}_{RT}$ (i.e., the sub-cycle assigned to real-time flows) and $T^{802.16}_k$ (i.e., the sub-cycle assigned to V_k's BE traffic) can be computed as follows:

$$T^{802.16}_{RT} = \frac{G_j \times T^{802.16}_{cycle}}{G_j + R_{j,BE}} \tag{18a}$$

$$T^{802.16}_k = \frac{R^k_{j,BE} \times T^{802.16}_{cycle}}{G_j + R_{j,BE}} \tag{18b}$$

where $T^{802.16}_{cycle}$ is the total wireless frame length.

In addition, the proposed AC scheme differentiates the SSs with real-time flows from those who only have BE flows. For a real-time SS n, the time share in the real-time sub-cycle $T^{802.16}_{n,RT}$ is expressed by:

$$T^{802.16}_{n,RT} = \frac{(1/R^x_n) \times T^{802.16}_{RT}}{\left(1/(\sum_n R^x_{n,RT})\right)} \tag{19}$$

where R^x_n is the computed transmission rate for SS n, and $\sum_n R^x_{n,RT}$ is the sum of transmission rates for all real-time SSs. The inverse of the transmission rate is used because an SS with lower transmission rate requires more time share to transmit an admitted flow rate. Similarly, the time share allocated to SS n for V_k BE sub-cycle, $T^{802.16}_{n,k}$, is expressed by the following:

$$T^{802.16}_{n,k} = \frac{(1/R^x_n) \times T^{802.16}_k}{\left(1/(\sum_n R^x_{n,k})\right)} \tag{20}$$

where $\sum_n R^x_{n,k}$ is the sum of transmission rates for all V_k SSs. Next and based on the admitted flow rate and reported frame size, our scheme estimates the amount of bandwidth required to satisfy each admitted flow in each frame. Thus, the estimated guaranteed bandwidth $B^g_{i,n}$ for real-time flow i launched by SS n in each polling interval is determined as:

$$B^g_{i,n} = \frac{g^k_i \times R^x_n \times T^{802.16}_{n,RT}}{G_j \times 8} \tag{21}$$

To explore the bandwidth usage of each frame and avoid any possible resource waste, the number of packets per polling cycle estimated for flow i, denoted as $np_{i,n}$, is first obtained:

$$np_{i,n} = \left\lceil \frac{B^g_{i,n}}{\bar{L}_i} \right\rceil \tag{22}$$

where $\bar{L}_i$ is the average packet size as defined in section III-D. Thus, the allocated bandwidth for flow i in the next cycle/frame, $B^{alloc}_{i,n}$, is then given by:

$$B^{alloc}_{i,n} = \min\left(np_{i,n} \times \bar{L}_i, r_{i,n}\right) \tag{23}$$

where $r_{i,n}$ is the requested bandwidth for real-time flow i (i.e., the buffering queue occupancy) by SS n

in each polling interval. As mentioned, UGS traffic needs not to be requested. Hence, the ONU-BS may periodically grant it the desired bandwidth.
With OFDM, one physical symbol may carry different bits of MAC layer data according to channel condition that in turn affects the modulation scheme employed. Therefore, each ONU-BS has to convert the allocated bandwidth into number of symbols accordingly. The number of OFDM symbols required for flow i by SS n, denoted as $F_{i,n}$, is computed as follows [3]:

$$F_{i,n} = \frac{B^{alloc}_{i,n} \times 8}{\phi_x} \tag{24}$$

For BE traffic, the allocated bandwidth $B^{alloc}_{n,BE}$ is determined in the same approach as follows:

$$B^{alloc}_{n,BE} = \min\left(\frac{R^x_n \times T^{802.16}_{n,k}}{8}, r_{n,BE}\right) \tag{25}$$

where $r_{n,BE}$ is the requested bandwidth for BE traffic in each polling interval.

B. VPN-DBA at OLT

The OLT receives reports from ONU-BS j on the length of its real-time queue m, (i.e., $r_{m,j}$) and a BE VPN counter of V_k (i.e., $r_{k,j}$). Moreover, we have the rate of BE traffic as:

$$R_{BE} = \sum_k \sum_j R^k_{j,BE} \tag{26}$$

Same as in the case of VPN-DBA at the ONU-BS, the OLT divides each transmission cycle into two sub-cycles (real-time and BE) respectively, and each BE sub-cycle is further subdivided into K sub-cycles. Consequently, the VPON's upstream real-time flow sub-cycle T^{VPON}_{RT} and a V_k sub-cycle T^{VPON}_k are computed as follows:

$$T^{VPON}_{RT} = \frac{G \times \beta T^{VPON}_{cycle}}{G + R_{BE}} \tag{27a}$$

$$T^{VPON}_{k} = \frac{\sum_j R^k_{j,BE} \times \beta T^{VPON}_{cycle}}{G + R_{BE}} \tag{27b}$$

where, $G = \sum_{j=1}^{M} G_j$, and $\sum_j R^k_{j,BE}$ is the total requested bandwidth for V_k. Note that for a non-VPN flow, the computation is done with $(1-\beta)T^{VPON}_{cycle}$ instead of βT^{VPON}_{cycle}. As mentioned, in the optical plane all ONU-BSs transmit at the same speed. Thus with a real-time sub-cycle T^{VPON}_{RT}, the time share for each ONU-BS j in the real-time sub-cycle $T^{VPON}_{j,RT}$ is computed as follows:

$$T^{VPON}_{j,RT} = \frac{T^{VPON}_{RT} \times R_N}{|M| \times 8} \tag{28}$$

Finally, the OLT calculates the allocated bandwidth for queue m of ONU-BS j, $B^{alloc}_{j,m}$ in the same manner as the computation done by the ONU-BS. The same logic also applies for the BE computation.

TABLE II
SIMULATION PARAMETERS

EPON	Number of ONU-BSs (M)	16
	Channel Speed (R_N)	1 $Gbps$
	Distance (OLT to ONU-BS)	25 km
	T^{VPON}_{cycle}	2 ms
	T_g	1 μs
	ONU-BS Queue Size	10 $Mbytes$
WiMAX	Channel Bandwidth	20 MHz
	N_d	1440
	T_{sym}	0.1 ms
	Distance (SS to ONU-BS)	5 km
	$T^{802.16}_{cycle}$	$5, 10, 20\ ms$
	SS Queue Size	10 $Mbytes$
VPN	Number of VPNs (K)	4
	β	1
	α	0.1
	SS V_k	$random(1, 4)$

VI. Performance Evaluation

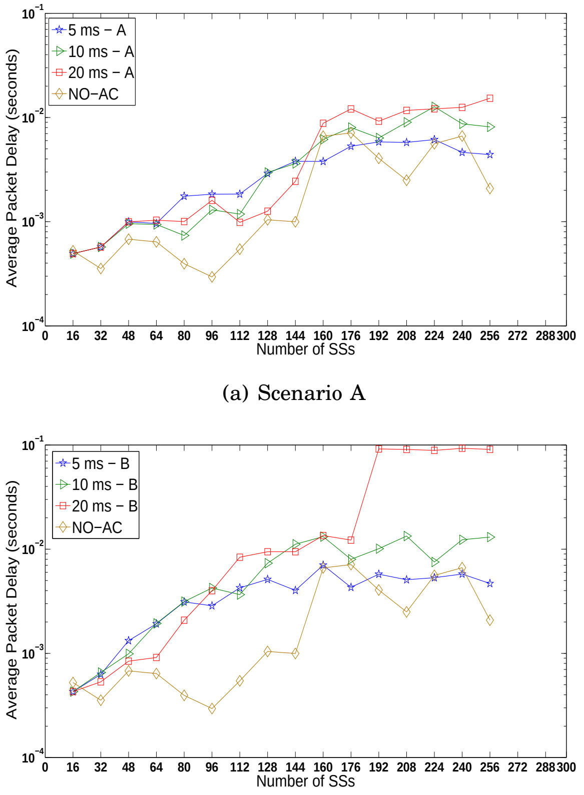
To evaluate the effectiveness of the proposed AC and DBA algorithms, we have developed a simulator using OMNET++. The simulation parameters are shown in Table II. Here, the case of $\beta = 1$ implies that "non-VPN" traffic is NOT considered, and therefore the available VPON bandwidth is divided among $K = 4$ VPNs. Without loss of generality, we assume that all VPNs have equal weights. Thus, $w_k = w = 1/K\ \forall k$, and $\sum_{k=1}^{K} w_k = 1$. As a result, each VPN is reserved a total of 249.5 $Mbps$, out of which, 24.95 $Mbps$ are reserved for BE traffic (since $\alpha = 0.1$).

To test the resilience of our proposed algorithms in handling fluctuating channel conditions, the following two simulation scenarios are investigated.

- *Scenario A*: The highest transmission rate is adopted for every SS n of each ONU-BS; i.e., $R^x_n = R^7_n$.
- *Scenario B*: Here, various channel conditions are considered for different SSs. The transmission mode of each SS is randomly generated ($x = random(1, 7)$).

We realize that scenario A (which is applied in most of the related work in the literature [3], [9]–[11]) is not realistic in presence of the powerful AMC function provided by the 802.16 standard; nonetheless, the result of scenario A is explored and positioned to serve as a benchmark for scenario B, and is expected to provide some insights to the case when other types of wireless air interfaces are employed, such as 802.11.

Under each scenario, we simulate with multiple OFDM frame lengths (5, 10 and 20 ms), in order to show how this affects the overall network performance in terms of end-to-end (from SS to OLT) flow throughput and end-to-end average packet delay. Each incoming SS has four flows (UGS, rtPS, nrtPS and BE). Every UGS flow is generated with a mean/guaranteed rate of 64 $Kbps$ (modeled using the constant distribution) and a packet size equal to 70 $bytes$ [21]. Al-



(a) Scenario A

(b) Scenario B

Fig. 4. UGS Flow Average End-to-End Packet Delay

ternatively, rtPS and nrtPS flows are modeled using the poisson distribution. We generate rtPS traffic at a guaranteed rate of $5\ Mbps$ (which is the average bit rate of a DVD-quality video) and a packet size of $800\ bytes$ [25]. Similarly, nrtPS traffic is generated at a guaranteed rate of $500\ Kbps$ and a packet size of $600\ bytes$ [21]. BE traffic is highly bursty, and we use self-similar traffic (pareto distribution with a hurst parameter $H = 0.8$) for modeling it [7]. Each BE flow is generated at a mean rate of $2\ Mbps$ with packet sizes uniformly distributed between 64 and $1518\ bytes$. The maximum allowable latency for voice traffic is $100\ ms$, and for video traffic is $150\ ms$ [21]. The number of SSs used in the figures increments by $|M|$ with time and reflects the arrival (or request for joining) of a new SS in time (with its CoS flows) to each ONU-BS simultaneously. Hence, every time a new SS wants to join the network, it will be subject to the VPN-AC framework as well as the VPN-DBA computation.

We first start by running scenario A to extract NBR that is needed to apply the AC rules (Eq. (14)). NBR is computed as follows:

$$NBR = \frac{Total\ Throughput}{Transmission\ Rate} = \frac{59.0976\ Mbps}{64.8\ Mbps} = 0.912 \tag{29}$$

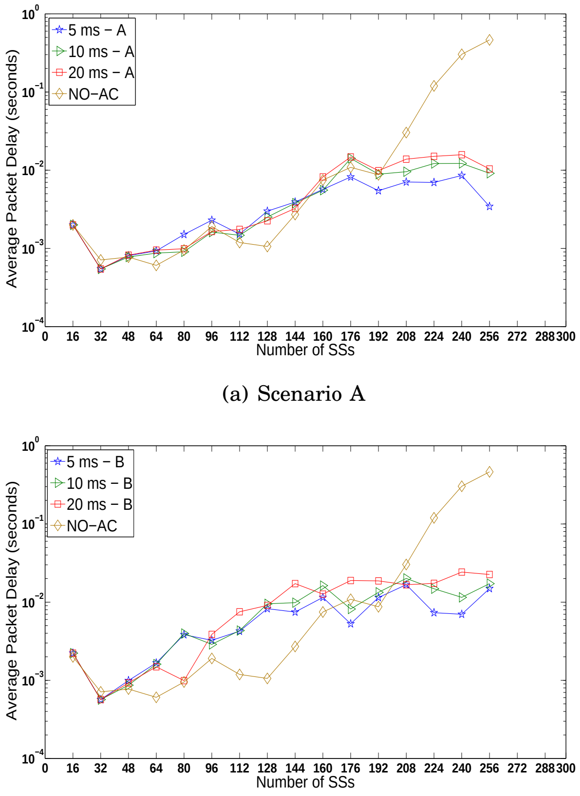
For a more conservative AC, we set $NBR = 0.9$.

To study the performance of real-time traffic, we measure the instantaneous average packet delays of a selected SS's real-time flows. Figs. 4, 5 and 6 show these measurements with AC (i.e., VPN-DBA) and without AC (i.e., NO-AC) under both scenarios. Note that with VPN-DBA, there is no intra-ONU/intra-SS scheduling required since the OLT/ONU-BS allocates bandwidth for each CoS, per each ONU-BS/SS, every cycle/OFDM frame. On the other hand with NO-AC, we apply strict priority (SP) scheduling [3].

Clearly, using the SP scheduler, UGS traffic shows the optimal performance where its average packet delay remains under $2-10\ ms$ even when the number of SSs continuously increases, regardless of the OFDM frame length. This is a direct result of the SP policy which always selects packets from a queue with a higher priority. As for VPN-DBA, it makes sure to satisfy the QoS requirements in terms of delay and throughput by reserving every real-time traffic with appropriate bandwidth in every cycle. Since a UGS flow is admitted only if its guaranteed bandwidth is assured in every cycle, we can see that VPN-DBA maintains a UGS average packet delay of $5-20\ ms$ under scenario A. However, the delay variation is affected by the OFDM frame length; especially in scenario B, where the delay might reach $\approx 90\ ms$ with a $20\ ms$ frame size. This is due to the fact that in this scenario, the bandwidth is allocated to each SS with respect to its transmission rate, and hence the cycle might saturate because some SSs have requested for more OFDM symbols than others to support the admitted flow rate. Nonetheless, VPN-DBA still maintains a UGS packet latency less than the maximum allowable one (i.e., $\leq 100\ ms$).

As for rtPS and nrtPS traffics, Figs. 5 and 6 demonstrate that VPN-DBA maintains their delay performance to meet the specified target QoS requirements of the stream (i.e., $\leq 150\ ms$) while the delay witnesses an exponential increase with NO-AC; especially after system saturation (number of SSs $= 192$). This behavior highlights the need for the application of AC in WiMAX-VPON, because when the system reaches saturation and all the arriving streams are admitted, the performance is no longer maintained. More specifically, no bandwidth is guaranteed for each type of traffic, and the QoS requirements can no longer be met not only for new flows but also for the existing ones. On the other hand, the deployment of AC allows for a bandwidth guaranteed service with protected and guaranteed QoS that will meet the VPN SLA and maintain it.

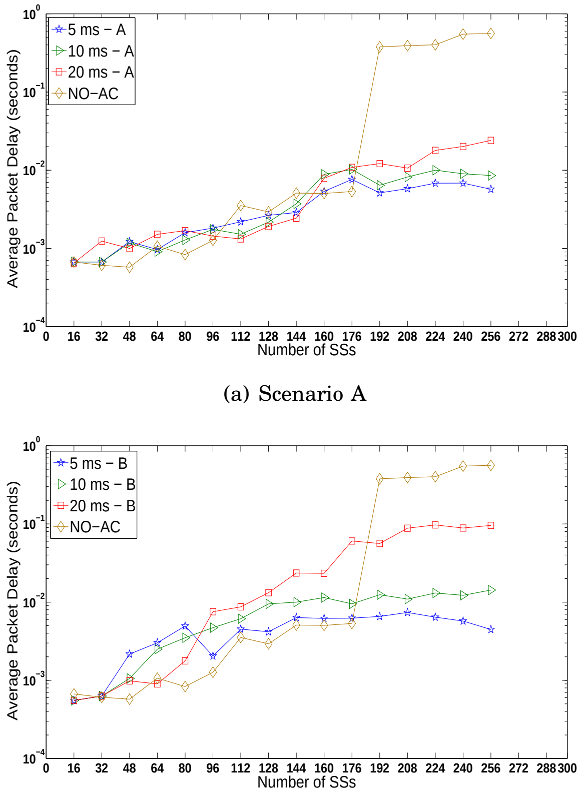
We further evaluate the proposed VPN-AC framework by measuring the throughput of one flow from each CoS of a common SS with AC (i.e., VPN-DBA) and with No-AC. It is demonstrated in Fig. 6 that the selected UGS flow exhibits similar performance behavior to that with NO-AC, whereas the selected rtPS and nrtPS flows show different behaviors. Here, rtPS and nrtPS flows with AC maintain their derived $5\ Mbps$ and $500\ Kbps$ throughputs respectively throughout the simulation, even after the system sat-



(a) Scenario A

(b) Scenario B

Fig. 5. rtPS Flow Average End-to-End Packet Delay



(a) Scenario A

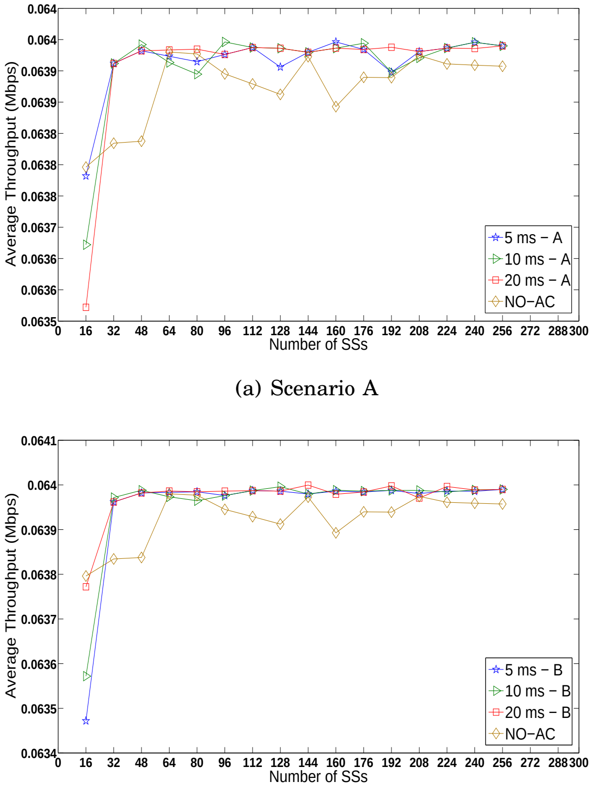
(b) Scenario B

Fig. 6. nrtPS Flow Average End-to-End Packet Delay

uration. On the other hand, when NO-AC is applied, these flows do not show a stable throughput behavior. Moreover, when the system reaches saturation, their throughput start decreasing. This is due to the fact that when more real-time flows are admitted and no AC is applied, the bandwidth that was guaranteed for the already admitted flows (before saturation) is now shared among more flows. Hence, the bandwidth is no longer guaranteed for the already admitted flows as well as for the newly admitted ones. This, again, shows the effectiveness of our AC framework in stabilizing and guaranteeing the throughput for all admitted flows by rejecting the flows that will break this theme. Furthermore, our framework proves that no matter what channel condition each user possesses, it can still provide its flows with the guaranteed bandwidth, which are well demonstrated by the results under scenario B. This is achieved by allocating more OFDM frames to transmit the same flow rate, as described before. In real and practical settings, this will deny all malicious users from monopolizing the bandwidth provided; and at the same time, it will allow for protection to the bandwidth assigned for other well-behaved users, while meeting the QoS requirements for each VPN service as specified in the SLA.

We now study the performance of BE traffic in both scenarios under different OFDM frame lengths. Since BE has no QoS requirement in terms of delay [21], we show the total BE throughput in Fig. 10, which is highly affected by the OFDM frame length. For example, with $5\ ms$ frame length under scenario A, $VPN\ 3$ yields a total throughput of $10\ Mbps$ knowing that its reserved one is $24.95\ Mbps$. The total throughput increases to reach $\approx 25.5\ Mbps$ when the frame length is increased to $20\ ms$. This is due to the fact that with a smaller frame size, the VPN BE sub-cycles portion of one SS might be smaller than the head-of-line (HOL) packet in its BE queue. As a result, not only those packets cannot be transmitted, but they could be successively blocked from being transmitted; and therefore, the throughput is suppressed. On the other hand, with a larger frame length, each VPN BE sub-cycle will be large enough to accommodate most packet sizes for all SSs, and hence the throughput can reach as high as $\approx 24.95\ Mbps$ (i.e., the reserved one). Nonetheless, using an OFDM frame length of $10\ ms$ also meets the expected throughput under both scenarios and produces a throughput equivalent to the reserved one. This shows that WiMAX-VPON can achieve the desired/expected performance for all types of traffic, if the network parameters are set properly.

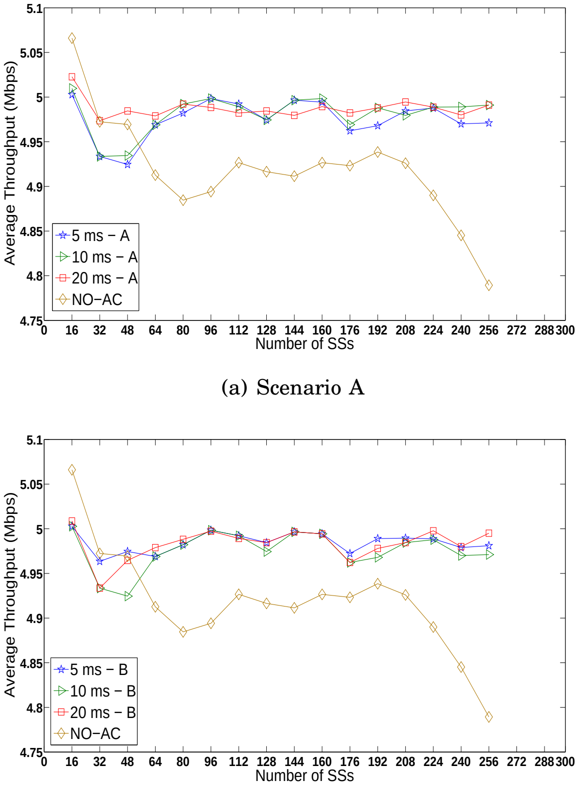
As mentioned before, our proposed VPN-DBA divides each transmission cycle into multiple sub-cycles in order to protect real-time traffic from being shared with BE traffic. To highlight this advantage, we plot in Fig. 11 the overall average end-to-end packet delay



(a) Scenario A

(b) Scenario B

Fig. 7. UGS Flow Average End-to-End Throughput



(a) Scenario A

(b) Scenario B

Fig. 8. rtPS Flow Average End-to-End Throughput

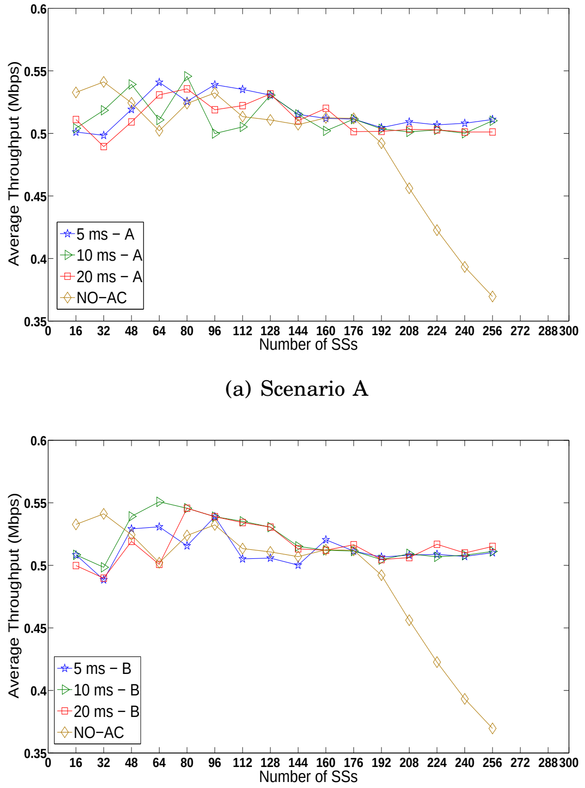
for all CoS, with multiple BE traffic VPN portions (i.e., with multiple α values). As noticed, real-time traffic (i.e., UGS, rtPS and nrtPS) maintain an overall average delay $\leq 10\ ms$ regardless of the assigned BE portion for each VPN. On the other hand, BE traffic witnesses a delay decrease as its reserved portion increases, which is under our expectations. This shows how VPN-DBA can efficiently preserve the QoS requirements for real-time flows while satisfying BE traffic with the "agreed-upon in the SLA" throughput. Finally, Table III summarizes the statistics collected from our simulations about a particular VPN (here, $VPN\ 4$). These results show that 100% and 52% of the generated $VPN\ 4$ UGS traffic is admitted, while its overall QoS and bandwidth requirements are guaranteed, under scenarios A and B respectively. $\approx 64\%$ and 24% of its rtPS flows are also admitted under both scenarios; and $\approx 82\%$ and 38% of its nrtPS flows are admitted as well; whereas all BE flows are admitted. The difference of admission rates between scenarios A and B is caused by OBAC (i.e., Eq. (14)), where the overall wireless system capacity is proportional to each SS's transmission rate. Thus, the admission rule becomes more conservative if more SSs have lower transmission rates. The table also shows that the monitored/measured throughput for each CoS traffic meets the expected/calculated one. This again demonstrates the effectiveness of our proposed framework in providing the expected performance under various channel conditions. Note that with no AC, all traffic is admitted; however, their QoS requirements are not guaranteed (except for UGS traffic). Note also that these collected results are traffic model dependent. In other words, more flows can be admitted or rejected, depending on all of the required guaranteed throughput for real-time and BE traffic, the generated flows mean rates, and the number of flows/SSs generated.

VII. Conclusions

This paper serves as the first research effort in exploring layer-2 VPNs over the EPON-WiMAX integration. This work presented a novel framework for providing bandwidth guarantee and QoS protection for VPN services via upstream dynamic bandwidth allocation (DBA) and admission control (AC), which are critical issues in the course of fixed-mobile convergence (FMC). The paper first defined layer-2 VPNs over EPON-WiMAX networks, and highlighted a number of important issues such as QoS mapping and traffic characteristics. The proposed framework implements a novel three-stage AC mechanism and a VPN-based DBA scheme, in order to achieve end-to-end bandwidth guaranteed. To validate the effectiveness and the robustness of our framework, extensive simulations were conducted, which demonstrated that the lack of AC

TABLE III
VPN4 Traffic Statistics

VPN	4					
CoS	**UGS**		**rtPS**		**nrtPS**	
Scenario	**A**	**B**	**A**	**B**	**A**	**B**
Number of Generated Flows	59	50	59	50	59	50
Number of Admitted Flows	59	26	38	12	48	19
Number of Rejected Flows	0	24	21	38	11	31
Admission Rate (%)	100%	52%	≈ 64%	24%	≈ 82%	38%
Expected Throughput (Mbps)	3.776	1.664	190	60	24	9.5
Monitored Throughput (Mbps)	3.76376	1.66151	189.815	58.6636	23.7408	9.51106



(a) Scenario A

(b) Scenario B

Fig. 9. nrtPS Flow Average End-to-End Throughput

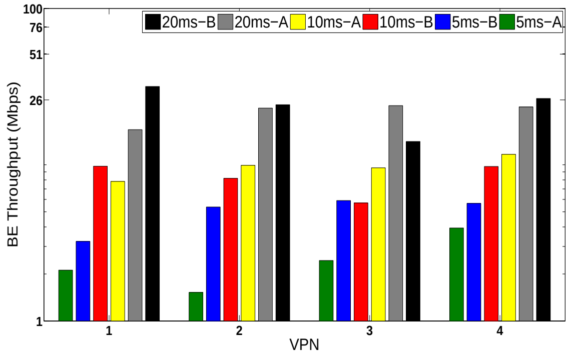


Fig. 10. Per-VPN BE End-to-End Throughput

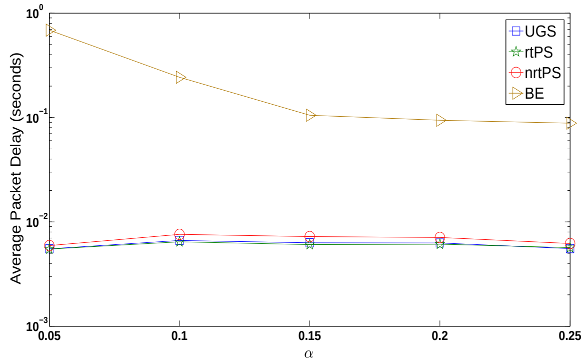


Fig. 11. Average End-to-End Packet Delay vs. α

and an effective DBA mechanism, the QoS requirements of various types of flows could not be protected. On the other hand, our framework has shown much improved performance in terms of maintaining the QoS requirements of the existing flows while providing an overall per-VPN acceptable minimal throughput for BE traffic. We conclude that the proposed framework is a promising candidate for the operation of future EPON-WiMAX access networks.

References

[1] A. R. Dhaini, P.-H. Ho, and X. Jiang, "QoS-Aware Layer-2 VPNs over EPON-WIMAX," in *Proceedings of IEEE International Conference on Communications (ICC'10)*, Cape Town, South Africa, May 2010.

[2] G. Shen, R. S. Tucker, and C.-J. Chae, "Fixed Mobile Convergence Architectures for Broadband Access: Integration of EPON and WiMAX," *IEEE Communications Magazine*, vol. 45, no. 8, pp. 44–50, Aug. 2007.

[3] K. Yang, S. Ou, G. Ken, and H.-H. Chen, "Convergence of Ethernet PON and IEEE 802.16 Broadband Access Networks and its QoS-Aware Dynamic Bandwidth Allocation Scheme," *IEEE JSAC*, vol. 27, no. 2, pp. 101–116, Feb. 2009.

[4] N. Ghazisaidi, M. Maier, and C. M. Assi, "Fiber-Wireless (FiWi) Access Networks: A Survey," *IEEE Communications Magazine*, vol. 47, no. 2, pp. 160–167, February 2009.

[5] S. Sarkar, S. Dixit, and B. Mukherjee, "Hybrid Wireless-Optical Broadband-Access Network (WOBAN): A Review of Relevent Challenges," *IEEE/OSA Journal of Lightwave Technology (JLT)*, vol. 25, no. 11, pp. 3329–3340, Novemeber 2007.

[6] M. Vrdoljak, S. I. Vrdoljak, and G. Skugor, "Fixed-Mobile Convergence Strategy: Technologies and Market Opportunities," *IEEE Communications Magazine*, vol. 38, no. 2, pp. 116 – 121, Feb. 2000.

[7] G. Kramer, B. Mukherjee, and G. Pesavento, “IPACT A Dynamic Protocol For An Ethernet PON (EPON),” *IEEE Communications Magazine*, vol. 40, no. 2, pp. 74–80, February 2002.

[8] M. P. McGarry, M. Maier, and M. Reisslein, “Ethernet PONs: A Survey of Dynamic Bandwidth Allocation (DBA) Algorithms,” *IEEE Communications Magazine*, vol. 42, no. 8, pp. S8–15, August 2004.

[9] M. Luo, H. Li, Y. Lu, and Y. Ji, “QoS-Aware Scheduling in Emerging Novel Optical Wireless Integrated Networks,” in *Challenges for Next Generation Network Operations and Service Management*. Springer Berlin / Heidelberg, October 2008, pp. 445–448.

[10] Y. Yan, H. Yu, H. Wang, and L. Dittmann, “Integration of EPON and WiMAX Networks: Uplink Scheduler Design,” in *Proceeding of Asia-Pacific Optical Communications (APOC 2008)*, Hangzhou, China, October 2008.

[11] Y. Luo, S. Yin, T. Wang, Y. Suemura, S. Nakamura, N. Ansari, and M. Cvijetic, “QoS-Aware Scheduling over Hybrid Optical Wireless Networks,” in *Proceedings of Optical Fiber Communication and the National Fiber Optic Engineers Conference (OFC/NFOEC’07)*, March 2007, pp. 1–7.

[12] R. Venkateswaran, “Virtual Private Networks,” *IEEE Potentials*, vol. 20, no. 1, pp. 11–15, Feb. 2001.

[13] W. Luo, C. Pignataro, A. Y. H. Chan, and D. Bokotey, “Layer-2 VPN Architecture,” *CISCO Press*, 2005.

[14] N. Nadarajah, E. Wong, and A. Nirmalathas, “Implementation of Multiple Secure Virtual Private Networks Over Passive Optical Networks Using Electronic CDMA,” *IEEE Photonics Technology Letters*, vol. 18, no. 3, pp. 484–486, February 2006.

[15] W. Wei, J. Hu, D. Qian, P. N. Ji, T. Wang, X. Liu, and C. Qiao, “PONIARD: A Programmable Optical Networking Infrastructure for Advanced Research and Development of Future Internet,” *IEEE/OSA Journal of Lightwave Technology (JLT)*, vol. 27, no. 3, pp. 233–242, Feb. 2009.

[16] A. S. Reaz, V. Ramamurthi, S. Sarkar, D. Ghosal, S. Dixit, and B. Mukherjee, “CaDAR: An Efficient Routing Algorithm for a Wireless–Optical Broadband Access Network (WOBAN),” *IEEE/OSA Journal of Optical Communications and Networking (JOCN)*, vol. 1, no. 5, pp. 392–403, Oct. 2009.

[17] A. R. Dhaini, C. M. Assi, M. Maier, and A. Shami, “Per-Stream QoS and Admission Control in Ethernet Passive Optical Networks (EPONs),” *IEEE/OSA Journal of Lightwave Technology (JLT)*, vol. 25, no. 7, pp. 1659–1669, July 2007.

[18] C. So-In, R. Jain, and A.-K. Tamimi, “Scheduling in IEEE 802.16e Mobile WiMAX Networks: Key Issues and a Survey,” *IEEE Journal of Selected Areas in Communications (JSAC)*, vol. 27, no. 2, pp. 156–171, February 2009.

[19] “IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Inteface for Fixed Broadband Wireless Access Systems,” Online, 2004.

[20] IEEE 802.3ah Task Force Home Page. [Online]. Available: http://www.ieee802.org/3/efm

[21] J. G. Andrews, A. Ghosh, and R. Muhamad, *Fundamentals of WIMAX: Understanding Broadband Wireless Networking*. Prentice Hall, 2007.

[22] S. Catreux, P. F. Driessen, and L. J. Greenstein, “Data Throughputs using Multiple-Input Multiple-Output (MIMO) Techniques in a Noise-Limited Cellular Environment,” *IEEE Transactions on Wireless Communications*, vol. 1, no. 2, pp. 226–234, April 2002.

[23] A. Doufexi, S. Armour, M. Butler, A. Nix, D. Bull, and J. McGeehan, “A Comparison of the HIPERLAN/2 and IEEE 802.11a Wireless LAN Standards,” *IEEE Communications Magazine*, vol. 37, no. 12, pp. 172–180, May 2002.

[24] Q. Liu, S. Zhou, and G. B. Giannakis, “Queuing With Adaptive Modulation and Coding Over Wireless Links: Cross-Layer Analysis and Design,” *IEEE Transactions on Wireless Communications*, vol. 4, no. 3, pp. 1142–1153, May 2005.

[25] C.-T. Chou, S. S. N, and K. G. Shin, “Achieving Per-Stream QoS with Distributed Airtime Allocation and Admission Control in ieee 802.11e Wireless LANs,” in *Proceedings of IEEE INFOCOM’05*, April 2005, pp. 1584 – 1595.

Ahmad R. Dhaini received his B.Sc. in computer science from the American University of Beirut (AUB) in 2004, and his M.App.Sc. in Electrical and Computer Engineering from Concordia University, Montreal, with a best thesis award nomination in 2006. Ahmad worked as a software consultant at TEKSystems, Montreal, in 2006-2007; and as a software designer at Ericsson, Montreal, in 2007-2008. He is currently working towards his Ph.D. degree in Electrical and Computer Engineering at the University of Waterloo. Ahmad has authored a book and published several papers in major journals and conferences related to his area of expertise. He has also been assigned as a technical program committee member, technical reviewer and member of the editorial board in major conferences and journals. His research interests focus on access networks; more specifically on optical/wireless broadband access networks.

Pin-Han Ho received his B.Sc. and M.Sc. degrees from the Electrical and Computer Engineering, Department of National Taiwan University in 1993 and 1995, respectively. He started his Ph.D. studies in 2000 at Queen’s University, Kingston, Ontario, Canada, focusing on optical communications systems, survivable networking, and QoS routing problems. He finished his Ph.D. in 2002, and joined the Electrical and Computer Engineering Department at the University of Waterloo as an assistant professor in the same year. He is the author/coauthor of more than 100 refereed technical papers and book chapters, and the co-author of a book on optical networking and survivability. He is the recipient of the Distinguished Research Excellence Award in the ECE Department at the University of Waterloo, the Early Researcher Award in 2005, the Best Paper Award at SPECTS’02 and the ICC’05 Optical Networking Symposium, and the Outstanding Paper Award in HPSR’02.

Xiaohong Jiang received his B.S., M.S. and Ph.D degrees in 1989, 1992, and 1999 respectively, all from Xidian University, Xian, China. He is currently a full professor of Future University Hakodate, Japan. Before joining Future University, Dr. Jiang was an Associate professor, Tohoku University, from Feb. 2005 to Mar. 2010. He was an assistant professor in the Graduate School of Information Science, Japan Advanced Institute of Science and Technology (JAIST), from Oct.2001 to Jan.2005. Dr. Jiang was a JSPS (Japan Society for the Promotion of Science) postdoctoral research fellow at JAIST from Oct.1999-Oct. 2001. He was a research associate in the Department of Electronics and Electrical Engineering, the University of Edinburgh from Mar. 1999-Oct. 1999. Dr. Jiang’s research interests include optical switching networks, routers, network coding, WDM networks, VoIP, interconnection networks, IC yield modeling, timing analysis of digital circuits, clock distribution and fault-tolerant technologies for VLSI/WSI. He has published over 150 referred technical papers in these areas. He is a senior member of IEEE.