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 WiMAX-VPON, a novel framework for establishing layer-2 virtual private networks (VPNs) over the integration of WiMAX and Ethernet passive optical networks, which has lately been considered as a promising candidate for next-generation fiber-wireless backhaul-access networks. With WiMAX-VPON, 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 and should be fulfilled by a suite of effective bandwidth management solutions. To achieve this, we propose a novel VPN-based admission control and bandwidth allocation scheme that provides per-stream quality-of-service protection and bandwidth guarantee for real-time flows. The bandwidth allocation is performed via a common medium access control 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 networks (EPONs) and WiMAX has been presented as an attractive broadband access network (BAN) solution [1–3]. The complementary features of these networks have motivated interest in using EPON as a backhaul to connect multiple dispersed WiMAX base stations (BSs) [1,4]. 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) [5]. On average, each ONU accesses \( \sim 70 \) Mbps bandwidth, which matches the total capacity offered by a WiMAX BS over a 20 MHz channel as well [6]. The integration can take advantage of the bandwidth benefit of fiber communications and the non-line-of-sight (NLOS) features of wireless communications. In addition, it enables integrated resource allocation and packet scheduling paradigms that help better support the emerging quality-of-service (QoS) services, as well as to improve the overall network throughput. Finally, the integration can help realize fixed-mobile convergence (FMC) by supporting mobility in the broadband access, thereby significantly reducing network operational costs [1].

The EPON-WiMAX integration has been well reported in the past few years [1,2]. Nonetheless, building up virtual private networks (VPNs) directly on the integration has never been investigated in the literature to our knowledge. In addition, the already presented upstream bandwidth allocation schemes are too trivial [2,7–9] 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 [10].

VPNs over EPON-WiMAX could be deployed to support mission-critical (police, health care, fire-fighting) governmental or corporate systems in order to achieve...
Building up layer-2 VPNs is most suitable when an EPON-WiMAX integrated network is installed. This is due to their support for premium services with custom-designed control, diverse QoS requirements, and security assurance, features that can be intrinsically provided by the layer-2 medium access control (MAC) protocols [11]. Such VPNs are referred to as layer-2 VPNs in the sense that they are built upon the layer-2 protocols. Compared with layer-3 [12], layer-2 VPNs can do a better job in resolving the complications due to network dynamics, communication media heterogeneity, and fast-changing channel status. This can be at the expense of a more complicated design that considers any possible layer-2 issue. In other words, when a layer-3 VPN is installed, a specialized software that forms a control plane (e.g., multiprotocol label switching (MPLS)) has to be in place instead of simply deploying standard IP protocol stacks on top of layer-2. Alternatively, deploying layer-1 VPNs over the integration cannot be achieved due to the physical media heterogeneity of both networks and because it requires complex hardware-dependant VPN solutions that can operate over both networks simultaneously [13].

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-VPON.

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 gives rise to the following 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 traffic, 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, to the best of our knowledge, the first framework for supporting layer-2 VPNs over the EPON-WiMAX integration. Layer-2 VPNs act as a cost-effective, secure, and flexible link between the underlying fiber-wireless infrastructure and higher-level mission-and business-critical services.

2) This paper presents a new VPN-based QoS provisioning framework that enables a robust bandwidth and QoS assurance for each wireless registered VPN user in the uplink/upstream shared media. From a user perspective, once a VPN tunnel is established, it is definite that the proper resources are reserved for this tunnel and that its bandwidth is allocated by means of the DBA.

3) Our work differs from previous related work [2–9] in that we offer a novel joint VPN-based AC and DBA scheme that enables an end-to-end (from SS to OLT) QoS guarantee while taking into consideration the different wireless channel conditions. In other words, our scheme offers a robust bandwidth allocation with a MAC-PHY cross-layer consideration so that the physical layer (PHY) burst profile is taken into account rather than relying solely on MAC requests [14].

4) The proposed AC scheme is implemented on a three-stage system, which is involved in the collaboration among the SS, 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-VPON provides a per-flow QoS protection and bandwidth guarantee for admitted traffic. Our simulation results 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-VPON 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 briefly overviews the different possible EPON-WiMAX architectures that can be installed to support our framework. Related challenges such as bandwidth allocation and admission control are also
discussed while demonstrating how existing schemes are not able to provide any QoS guarantees and hence are not suitable for the support of layer-2 VPNs.

A. EPON-WiMAX Architectures

Several architectures were proposed for the EPON-WiMAX integration [1,2], with a point-to-multipoint (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, the ONU and BS are mounted in one box, a 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 an 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 microcell. Here, an optical subcarrier and another wireless subcarrier are used to transfer signals from the wireless to the optical domain.

5) Virtual: Here, a different approach is proposed for designing the ONU-BS communication while preserving the current EPON and WiMAX standards [2]. Namely, a VOB (i.e., a virtual ONU-BS) is built by installing a network bridge between the ONU and the BS.

Note that a mesh-based EPON-WiMAX architecture may alternatively be installed to take advantage of the multihop routing and delaying capabilities of wireless mesh networks. Nonetheless, routing and the related challenges are far from the scope of this study. More details on how to perform routing in fiber–wireless mesh-based networks can be found in [15].

One of the powerful advantages of WiMAX-VPON (as we will see later) is that it is designed to be architecture independent. 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 as detailed in [1–3].

B. Bandwidth Allocation and Admission Control

The integration of EPON and WiMAX networks 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 AC schemes. This property has been widely investigated in EPON [5,16,17] and WiMAX [18] separately, but little work that considers their integration has been done. 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., [2,7–9]). Nevertheless, none of the proposed schemes were able to provide bandwidth guarantees or QoS protection for the incoming flows, properties that are required for the support of VPNs. In addition, these schemes did not consider the underlying PHY burst profiling applied on each wireless link, and so the allocation was based on MAC requests only, which makes such an arbitration less meaningful [14]. Therefore adopting any of these mechanisms is not a viable solution in the context of layer-2 VPNs over the integrated network. Conversely, our proposed framework addresses these issues and provides effective resource allocation solutions.

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 much more efficient and lightweight network management, which is necessary
to support a multiservice and multicustomer 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 service 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 multiplaned VPNs over EPON-WiMAX is illustrated in Fig. 1.

With the current heterogeneous 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) control; however, this paper emphasizes 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 the scope of this 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 [6]. Furthermore in EPON, incoming IP datagrams are encapsulated in Ethernet frames according to the IEEE 802.3 standard [19], whereas they are launched as IEEE 802.16 protocol data units (PDUs) in the case of WiMAX [6]. 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 [1]. 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 for the bandwidth allocation and network control in the optical domain.

2) **Wireless Channel Model**: The wireless channel is modeled as a Rayleigh fading channel [20] that is suitable for flat-fading channels as well as frequency-selective fading channels encountered with optical frequency division multiplexing (OFDM). The received signal of an SS $n$ is computed as follows:

$$r_n = h_n(t) \times ts(t) + b_n(t),$$  

(1)

where $ts(t)$ is the transmitted signal and $b_n(t)$ 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 [21]:

![Layer-2 VPNs over EPON-WiMAX](image-url)
where $D_n$ is the distance between SS $n$ and the connected ONU-BS, $c$ is a constant including the transmission and receiving multi-input–multi-output (MIMO) antenna gain [21], and $\gamma$ 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 $P_n$ 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 ($SNR_n^{\text{max}}$) 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 channel state information (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 in Table I.

The target of our study is the VPN setup by taking WiMAX networks as an extension to EPON networks in order to offer high-speed wireless access in the last mile [1]. Since EPON is based on time division multiple access (TDMA) and for simplicity, we adopt the OFDM-TDMA air interface for the wireless channel access. OFDM-TDMA is supported by the IEEE 802.16 standard and is very suitable for fixed wireless users (i.e., using the IEEE 802.16d standard that is widely deployed in both Europe and Asia) [2]. As a result, 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 [22] with specific SNR$^{\text{max}}$ and bits/symbol [23]. Let $N_d$ be the total number of OFDM data subcarriers and $T_{\text{sym}}$ be 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:

$$R_n^x = \frac{N_d \times W_{sc} \times CR^x}{T_{\text{sym}}}.$$ (3)

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-real-time polling service (nrtPS) and best effort (BE) [6]. On the other hand, an IEEE 802.13ah ONU is allowed to support and report up to eight queues [19]. 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 [5], 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 [2]. Hence we will have a total of five queues for UGS, rtPS, nrtPS, ertPS, and BE classes of service. 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 [6,19] 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 granting in a GPC

**TABLE I**

**ADAPTIVE MODULATION AND CODING MODES**

<table>
<thead>
<tr>
<th>Modulation</th>
<th>BPSK</th>
<th>QPSK</th>
<th>16 QAM</th>
<th>64 QAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmission mode (X)</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Coding rate (CR)</td>
<td>1/2</td>
<td>1/2</td>
<td>3/4</td>
<td>1/2</td>
</tr>
<tr>
<td>Receiver SNR (dB)</td>
<td>6.4</td>
<td>9.4</td>
<td>11.2</td>
<td>16.4</td>
</tr>
<tr>
<td>Bits/symbol ($\phi$)</td>
<td>0.5</td>
<td>1</td>
<td>1.5</td>
<td>2</td>
</tr>
<tr>
<td>Coded bits/subcarrier ($W_{sc}$)</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>

Authorized licensed use limited to: University of Waterloo. Downloaded on June 17,2010 at 21:47:06 UTC from IEEE Xplore. Restrictions apply.
fashion [6]. 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 because 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 multipoint control protocol (MPCP) [19], each ONU is allowed to request bandwidth for up to eight 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 the 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 VPON cycle $T_{\text{cycle}}^{\text{VPON}}$ is divided into two sub-cycles. The first subcycle $\beta T_{\text{cycle}}^{\text{VPON}}$ is shared among all the $K$ VPNs. The second subcycle $(1-\beta)T_{\text{cycle}}^{\text{VPON}}$ is shared among non-VPN services. Let $B_{\text{min}}^k$ 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 $R_N$ is the transmission speed of the PON in Mbps. In addition, let each $V_k$ be given a weight $w_k$ to determine its paid/committed bandwidth. Therefore, $B_{\text{min}}^k$ (in bytes, thus divide by 8) is given as follows:

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

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 a reserved quota for BE traffic takes a portion of $\alpha^k B_{\text{min}}^k$, while the real-time flows will share the remaining bandwidth, that is, $(1-\alpha^k)B_{\text{min}}^k$.

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 noted, 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 will allow it to operate over mobile networks [e.g., IEEE 802.11 (WiFi) and IEEE 802.16e networks] as well.

D. Traffic Characteristics and QoS Requirements

CBR traffic (such as UGS) is nonbursty and can be simply characterized by its mean data rate ($\mu$) in 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 ($\sigma$) in bps.
- Maximum burst size ($\rho$) in bits.

![Fig. 2. (Color online) Proposed VPON QoS provisionning framework.](image-url)
• Delay bound \( (\theta) \), 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 \( (L_{\text{max}} \text{ and } L_{\text{min}}) \). 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 guarantee.

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 [24], 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 [24]:

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

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 [17,24]:

\[
g_i^k = \frac{\rho_i}{\theta_i + \frac{\rho_i}{\sigma_i}}. \tag{7}
\]

In the wireless domain, transmissions are error prone due to fluctuating channel conditions. Thus, the sense of per-flow-based bandwidth guarantees becomes tricky. A common method is to pursue a statistic sense of bandwidth guarantees. By assuming a frame error probability \( P_{\text{error},i} \) for stream \( i \), the transmission rate in the wireless domain, such that a VBR stream perceived bandwidth can be statistically guaranteed, is obtained as follows:

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

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

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

\[
g_i^k = \frac{\mu_i}{1 - P_{\text{error},i}}. \tag{9}
\]

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

\[
g_i^{k+1} \leq B_k^G, \tag{10}
\]

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 the OLT collaboratively perform AC in order to satisfy the conditions defined in Eqs. (8) and (9).

IV. VPN-BASED ADMISSION CONTROL

This section describes the proposed three-stage 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).

Fig. 3. (Color online) Guarantee bandwidth derivation graph.
A. SS-Based Admission Control

Let $M_k$ be the number of ONU-BSs that provision $V_k$ and share the total allocated bandwidth $\alpha^k B_{\text{min}}^k$ 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, $\alpha^k B_{\text{min}}^k / |M_k|$. This information is broadcast by the OLT to all the ONU-BSs in the registration phase. Let $R_{j,\text{BE}}^k$ denote the rate reserved for BE traffic of $V_k$ at each ONU-BS $j$, which can be expressed as

$$R_{j,\text{BE}}^k = \frac{\alpha^k B_{\text{min}}^k \times 8}{|N_k| \times |M_k| \times \beta T_{\text{VPON}}}.$$

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 $\text{gn}_n^k$, can be expressed as

$$R_{j,\text{BE}}^n = \frac{\alpha^k B_{\text{min}}^k \times 8}{N_k \times \beta T_{\text{VPON}}}.$$

According to Eq. (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:

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

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

Using SS-based AC, 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 $R_n^k$; 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

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:

$$\frac{g_{n,i+1}^k}{R_n^k} + \sum_k \sum_i g_{n,i}^k \leq \text{NBR} - \sum_k \sum_i R_{n,\text{BE}}^k.$$

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. $g_{n,i}^k / R_n^k$ is the ratio of the channel rate required to transmit flow $i$ of $V_k$ in a 1 s 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

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:

$$g_{i+1}^k + \sum_i g_i^k \leq \frac{(1-\alpha^k) B_{\text{min}}^k \times 8}{\beta T_{\text{VPON}}},$$

In summary, VPN-AC is used to achieve an 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 building up layer-2 VPNs over EPON-WiMAX integration while at the expense of longer decision making delay at each SS on an order of milliseconds during the next polling interval. Nonetheless, a delay within the maximum OFDM frame length (i.e., 20 ms [6]) is considered tolerable.

V. VPN-BASED DYNAMIC BANDWIDTH ALLOCATION

As a complement to the AC scheme in the course of a per-flow QoS guarantee, we provide a VPN-based dynamic bandwidth allocation (VPN-DBA) scheme that is installed at both the 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 the 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 $G_j = \sum_k \sum_i g_i^k$) and the total reserved VPN BE rates (denoted as $R_{j,\text{BE}}$) using the following equation:

$$R_{j,\text{BE}} = \sum_k R_{j,\text{BE}}^k \times \Gamma_k,$$

where
To protect RT traffic from being shared with BE traffic, in our scheme, each cycle/frame is divided into $K + 1$ subcycles, where subcycle 1 is for real-time flows, while the remaining $K$ subcycles are for all the VPNs' BE traffic. The size of each subcycle 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 subcycle assigned to real-time flows) and $T_{802.16}^k$ (i.e., the subcycle assigned to $V_k$’s BE traffic) can be computed as follows:

\[
T_{802.16}^{RT} = \frac{G_j \times T_{802.16}^{cycle}}{G_j + R_{j,BE}},
\]

\[
T_{802.16}^k = \frac{R_{j,BE}^k \times T_{802.16}^{cycle}}{G_j + R_{j,BE}},
\]

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 that only have BE flows. For a real-time SS $n$, the time share in the real-time subcycle $T_{802.16}^{n,RT}$ is expressed by

\[
T_{802.16}^{n,RT} = \frac{(1/R_n^x) \times T_{802.16}^{n,RT}}{\left[1/\left(\sum_n R_{n,RT}^x\right)\right]},
\]

where $R_n^x$ is the computed transmission rate for SS $n$, and $\sum_n R_{n,RT}^x$ is the sum of transmission rates for all real-time SSs. The inverse of the transmission rate is used because an SS with a lower transmission rate requires more time share to transmit an admitted flow rate. Similarly, the time share allocated to SS $n$ for the $V_k$ BE subcycle, $T_{802.16}^{n,k}$, is expressed by the following:

\[
T_{802.16}^{n,k} = \frac{(1/R_n^x) \times T_{802.16}^{n,k}}{\left[1/\left(\sum_n R_{n,k}^x\right)\right]},
\]

where $\sum_n R_{n,k}^x$ 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 $B_{i,n}^{g}$ for real-time flow $i$ launched by SS $n$ in each polling interval is determined as

\[
B_{i,n}^{g} = \frac{g_i^k \times R_n^x \times T_{802.16}^{n,RT}}{G_j \times 8}.
\]
B. VPN-DBA at the 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

$$R_{BE} = \sum_k \sum_j R_{j, BE}^k.$$  \hspace{1cm} (26)

Same as in the case of VPN-DBA at the ONU-BS, the OLT divides each transmission cycle into two subcycles (real-time and BE), and each BE subcycle is further subdivided into $K$ subcycles. Consequently, the VPON's upstream real-time flow subcycle $T_{RT}^{VPON}$ and a $V_k$ subcycle $T_{k}^{VPON}$ are computed as follows:

$$T_{RT}^{VPON} = \frac{G \times \beta T_{cycle}^{VPON}}{G + R_{BE}},$$  \hspace{1cm} (27a)

$$T_{k}^{VPON} = \frac{\sum_j R_{j, BE}^k \times \beta T_{cycle}^{VPON}}{G + R_{BE}},$$  \hspace{1cm} (27b)

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

$$T_{j, RT}^{VPON} = \frac{\beta T_{cycle}^{VPON} \times R_{N}}{|M| \times 8}.$$  \hspace{1cm} (28)

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

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 $\Sigma_{k=1}^{K} w_k = 1$. 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 $\forall k$, $\alpha^k = 0.1$).

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., $R_n = R_n^x$.
- **Scenario B**: Here, various channel conditions are considered for different SSs. The transmission mode of each SS is randomly generated [$x = \text{random}(1,7)$].

We realize that scenario A (which is applied in most of the related work in the literature [2,7-9]) is not realistic in the presence of the powerful AMC function provided by the IEEE 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 in case other types of wireless air interfaces are employed, such as IEEE 802.11.

In 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 [20]. Alternatively, 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 [24]. Similarly, nrtPS traffic is generated at a guaranteed rate of 500 Kbps and a packet size of 600 bytes [20]. BE traffic is highly bursty, and we use self-similar traffic (Pareto distribution with a Hurst parameter $H=0.8$) for modeling it [5]. 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 [20]. 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 the NBR that is needed to apply the AC rules [Eq. (14)]. The NBR is computed as follows:

$$NBR = \frac{\text{Total Throughput}}{\text{Transmission Rate}} = \frac{59.0976 \text{ Mbps}}{64.8 \text{ Mbps}} = 0.912.$$  \hspace{1cm} (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. Figures 4–6 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 [2].

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 that 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 all 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 ~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., ≤100 ms).

As for rtPS and nrtPS traffic, Figs. 5 and 6 demonstrate that VPN-DBA maintains their delay performance to meet the specified target QoS requirements of the stream (i.e., ≤150 ms) while the delay wit-
nesses 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. 7 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 (see Figs. 8 and 9) with AC maintain their derived 5 Mbps and 500 Kbps throughputs, respectively, throughout the simulation, even after the system saturation. 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 starts 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 admit-
sesses, 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 [20], 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 ≈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 subcycles portion of one SS might be smaller than the head-of-line (HOL) packet in its BE queue. As a result, not only can those packets not be transmitted, but they could also be successively blocked from being transmitted, and therefore, the throughput is suppressed. On the other hand, with a larger frame length, each VPN BE subcycle will be large enough to accommodate most packet sizes for all SSs, and hence the throughput can reach as high as ≈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 subcycles 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 for all CoS, with multiple BE traffic VPN portions (i.e., with multiple α values). As noted, real-time traffic (i.e., UGS, rtPS, and nrtPS) maintain an overall average delay ≤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 throughput agreed upon in the SLA. 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 guaran-

<table>
<thead>
<tr>
<th>TABLE III</th>
<th>VPN 4 TRAFFIC STATISTICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoS</td>
<td>UGS</td>
</tr>
<tr>
<td>Scenario</td>
<td>A</td>
</tr>
<tr>
<td>Number of generated flows</td>
<td>59</td>
</tr>
<tr>
<td>Number of admitted flows</td>
<td>59</td>
</tr>
<tr>
<td>Number of rejected flows</td>
<td>0</td>
</tr>
<tr>
<td>Admission rate (%)</td>
<td>100%</td>
</tr>
<tr>
<td>Expected throughput (Mbps)</td>
<td>3.776</td>
</tr>
<tr>
<td>Monitored throughput (Mbps)</td>
<td>3.76376</td>
</tr>
</tbody>
</table>
This article has been accepted for inclusion in a future issue of this journal. Content is final as presented.

VII. CONCLUSIONS

This paper has presented the first work to our knowledge to establish layer-2 VPNs over the EPON-WiMAX integration. A novel framework, namely, WiMAX-VPON, was proposed for providing per-service QoS protection and assurance. This work first defined layer-2 VPNs over EPON-WiMAX networks and then highlighted a number of important issues such as QoS mapping and traffic characteristics. The proposed framework implements a new joint VPN-based three-stage AC and DBA paradigm to achieve an end-to-end bandwidth guarantee. To validate the effectiveness and the robustness of our framework, extensive simulations were conducted, which demonstrated that the lack of an efficient AC or DBA mechanism could not preserve the QoS requirements of various types of flows. On the other hand, WiMAX-VPON 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 backhaul-access networks.

ACKNOWLEDGMENT

Preliminary results of this work appeared in ICC’10 [25].

REFERENCES

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. He 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 toward his Ph.D. degree in electrical and computer engineering at the University of Waterloo. He 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 Engineering Department of the National Taiwan University in 1993 and 1995, respectively, and his Ph.D. degree from Queens University at Kingston in 2002. He is now an associate professor in the Department of Electrical and Computer Engineering, University of Waterloo, Canada. Professor Ho is the author/co-author of more than 150 refereed technical papers, several book chapters, and a book on optical networking and survivability. His current research interests cover a wide range of topics in broadband wired and wireless communication networks, including survivable network design, wireless metropolitan area networks such as IEEE 802.16 networks, fiber–wireless (FiWi) network integration, and network security. He is the recipient of the Distinguished Research Excellent Award in the Department of Electrical and Computer Engineering of the University of Waterloo; the Early Researcher Award (Premier Research Excellence Award) in 2005; the Best Paper Award in SPECTS'02, ICC'05 Optical Networking Symposium, and ICC'07 Security and Wireless Communications 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 at the Future University-Hakodate, Japan. Before joining the Future University, Dr. Jiang was an Associate Professor at 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 Japan Society for the Promotion of Science (JSPS) Postdoctoral Research Fellow at JAIST from Oct. 1999 to Oct. 2001. He was a research associate in the Department of Electronics and Electrical Engineering of the University of Edinburgh from Mar. 1999 to 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 refereed technical papers in these areas. He is a senior member of IEEE.