ACCEPTED FROM OPEN CALL

A Potential Evolution of the Policy and Charging Control/QoS Architecture for the 3GPP IETF-Based Evolved Packet Core

Stéphane Ouellette, Ericsson Research and École Polytechnique de Montréal
Laurent Marchand, Ericsson Research
Samuel Pierre, École Polytechnique de Montréal

ABSTRACT

The 3rd Generation Partnership Project (3GPP) Release 8 defines the specifications of a low latency, high-data rate all-IP Core Network (CN) capable of supporting real-time packet services over multiple access technologies, including the new Long-Term Evolution (LTE) access network. The mobile communications industry is maturing. In order to remain competitive many operators now focus on reducing their capital and operational expenditures (CAPEX and OPEX), by outsourcing some of their business activities and/or by sharing some network infrastructures. This article presents a possible evolution of the 3GPP Policy and Charging Control (PCC) and Quality of Service (QoS) architecture to better support Fixed-Mobile Convergence (FMC) and more flexible CN sharing solutions. This goal is achieved with a clearer separation of the business roles (e.g. access and network providers) and the introduction of a Network Policy Function (NPF) for the management of the CN.

INTRODUCTION

The 3GPP Release 8 specifications define the Evolved Packet System (EPS) as an evolution of the General Packet Radio Service (GPRS). It features a flat radio access network (RAN) architecture compared to a 3rd generation (3G) packet switched domain. As such, the functionalities of the radio network controller (RNC) were split between the LTE base station (eNodeB), the serving gateway (S-GW) and the mobility management entity (MME).

As depicted in Fig. 1, only eNodeBs are found in the RAN; all of the other nodes compose the Evolved Packet Core (EPC). Two network architecture solutions are defined for the EPC:
- The first one [1] is based on the GPRS Tunneling Protocol (GTP) and supports all 3GPP access technologies.
- The second solution [2] is based on the IETF Proxy Mobile IP (PMIP) protocol and defines some enhancements for non-3GPP access technologies.

This work derives from a research project that explores possible evolutions to the 3GPP network architecture beyond Release 8. Although most aspects of our proposal could be applied to the GTP-based architecture, we focused our efforts on the IETF-based solution.

The rest of this article is organized as follows. We discuss the ongoing transformation of the communications industry. We describe the policy control and QoS architectures proposed by 3GPP and the Telecommunications and Internet-converged Services and Protocols for Advanced Networks (TISPAN) organization. We list the requirements we believe should be fulfilled by the PCC and QoS architecture in order to better support FMC and more flexible CN sharing solutions. We then detail our proposal and evaluate our solution based on the requirements listed. Finally, we conclude and discuss future work.

CHANGES IN THE INDUSTRY

As the communications industry matures, many operators are focusing more on reducing costs rather than bringing innovation to the market [3]. In the future, the industry will be characterized by an increased specialization of the network operators (Fig. 2a) toward more specific market segments (e.g. teenagers, retired).

As part of this transformation, operators running both fixed and mobile accesses realized that they could further reduce costs by connecting their access network (AN) to a single, multiaccess CN. Additionally, the emergence of multimode terminals allows the operators to provide their subscribers with either the best or the most cost effective available connection on all accesses.

The design of the EPC is in line with the rise of FMC, which is a trend that aims to provide telephony and Internet access with a single device that can switch between local (e.g. WiFi) and wide-area (e.g. cellular) networks (Fig. 2b). As there are many business advantages resulting from FMC, pure fixed or mobile-only operators are urged to build alliances to stay competitive.

Based on this transformation of the industry, we foresee that it will progressively migrate from its vertical integration model to a disaggregated value chain in which the players focus on key business activities.

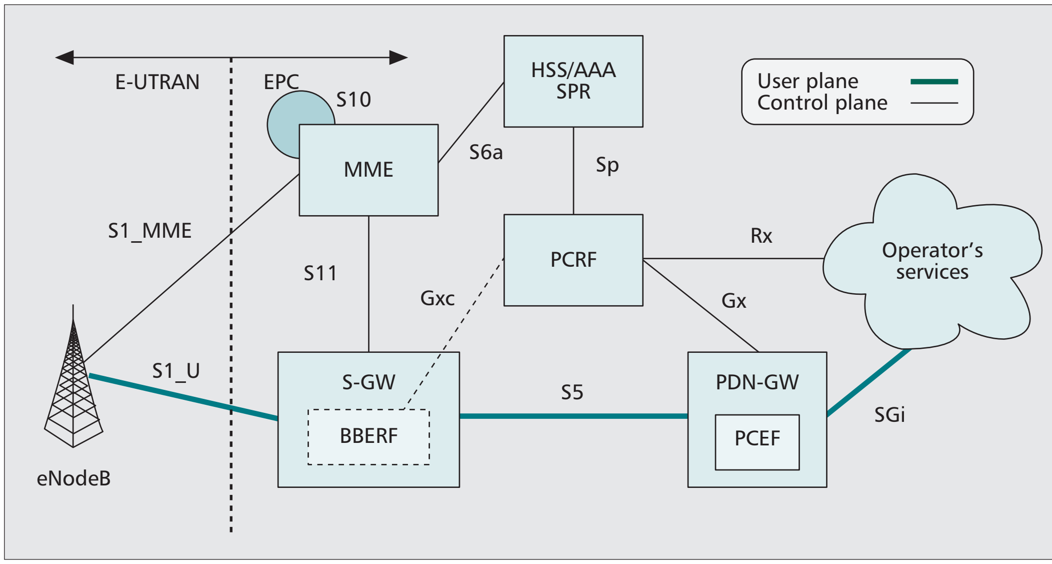


Figure 1. *Main nodes of the EPS showing the LTE access (dotted elements are specific to [2]).*

To reduce their costs, many operators restructure themselves by outsourcing parts of their network management activities or by sharing infrastructures with other operators [4]. The average revenue per user is the main driver for these reorganizations because it has remained constant in the past years, although voice and data traffic volumes per user are steadily growing.

Because of the fierce competition, the only way operators can increase their profits is to reduce their costs by focusing on "key assets" and "critical success factors" [5], i.e. their most profitable business activities or assets. As such, services are now being considered, beyond branding and coverage, as the prime differentiator between operators. Consequently, more advanced infrastructure sharing scenarios will emerge in the future.

There are potential benefits to infrastructure sharing. First, a country's regulations can force operators to cover areas that are unattractive from a business point of view. Second, a "greenfield" operator could offer coverage to its customers in a previously uncovered region without having the burden to deploy a full-scale RAN; in return the operator already present has the opportunity to leverage its RAN to generate more revenues [5]. Finally, because network dimensioning mostly depends on the peak demand, there are incentives for operators that have different subscriber bases (e.g. teenagers and business users that have disjoint traffic peaks) to share the RAN. This allows the average traffic level to increase without any significant increase in peak demand level because the traffic peaks occur at different times for the operators. Sharing infrastructures often leads to cost reductions.

Based on this transformation of the industry, we foresee that it will progressively migrate from its vertical integration model to a disaggregated value chain (Fig. 2c) in which the players focus on key business activities. Moreover, an increasing number of operators will offer services using several access technologies. These realities must be reflected by the logical CN architecture.

3GPP and TISPAN Policy Control/QoS Architectures

This section presents the key features of the 3GPP PCC and TISPAN Resource and Admission Control Subsystem (RACS) architectures. TISPAN is a Next Generation Network (NGN) architecture focusing on fixed networks and Internet convergence. This section concludes with a list of issues regarding FMC and CN sharing support for both architectures.

The 3GPP PCC Architecture

The PCC architecture [6] implements the policy and charging control functions of an EPC. For a detailed description of the PCC architecture, its procedures and QoS management, refer to [7, 8].

The Policy and Charging Rules Function (PCRF) decides how a service data flow (SDF) shall be treated by the Policy and Charging Enforcement Function (PCEF). A SDF is a set of packet flows that matches a SDF template. A SDF template is a set of filters containing header parameters/ranges used to identify the packet flows constituting a SDF. The PCRF provides network control regarding SDF detection, QoS, gating and SDF-based charging, with the exception of credit management.

The PCRF takes policy decisions based on the session information received from the Application Function (AF) and on the user profile stored in the Subscription Profile Repository (SPR). It authorizes QoS resources defined by the QoS class indicator (QCI), allocation and retention priority (ARP), guaranteed/maximum bitrates (GBR, MBR). When an AF request is granted, the PCRF sends a QoS rule to the Bearer Binding and Event Reporting Function (BBERF) and a PCC rule (basically a QoS rule with gating and charging informations) to the PCEF.

The PCEF encompasses SDF detection and measurement, gate and QoS enforcement, online and offline SDF-based charging functionalities and event reporting to the PCRF. The PCEF is implemented into the PDN Gateway (P-GW).[1]

[1] *The PCEF can also be implemented into the evolved Packet Data Gateway (ePDG) but untrusted non-3GPP networks are out of scope.*

The BBERF is implemented into the access edge gateway (AEG) for each type of access. Its main tasks are event reporting to the PCRF and bearer binding.[2] The BBERF exists because IETF mobility protocols focus on routing only and carry no information about the bearers' QoS properties.

Mobility is supported within 3GPP/3GPP2 accesses but session continuity that involves non-3GPP accesses is still under development. The non-roaming architecture is presented in Fig. 3a while Fig. 3b illustrates two roaming cases:

- The *home-routed* case forces all user traffic to be tunneled back to the home network.
- The *local breakout* case allows the UE to be connected to a P-GW in the visited network.

Infrastructure sharing is possible in both the RAN and parts of the CN. RAN sharing involves not only sharing the RAN nodes but also frequency pooling. Two basic scenarios for infrastructure sharing are defined for the EPC [9]:

- Multi-operator core network (MOCN) in which only the RAN nodes are shared.
- Gateway core network (GWCN) configuration where RAN and S-GW are shared.

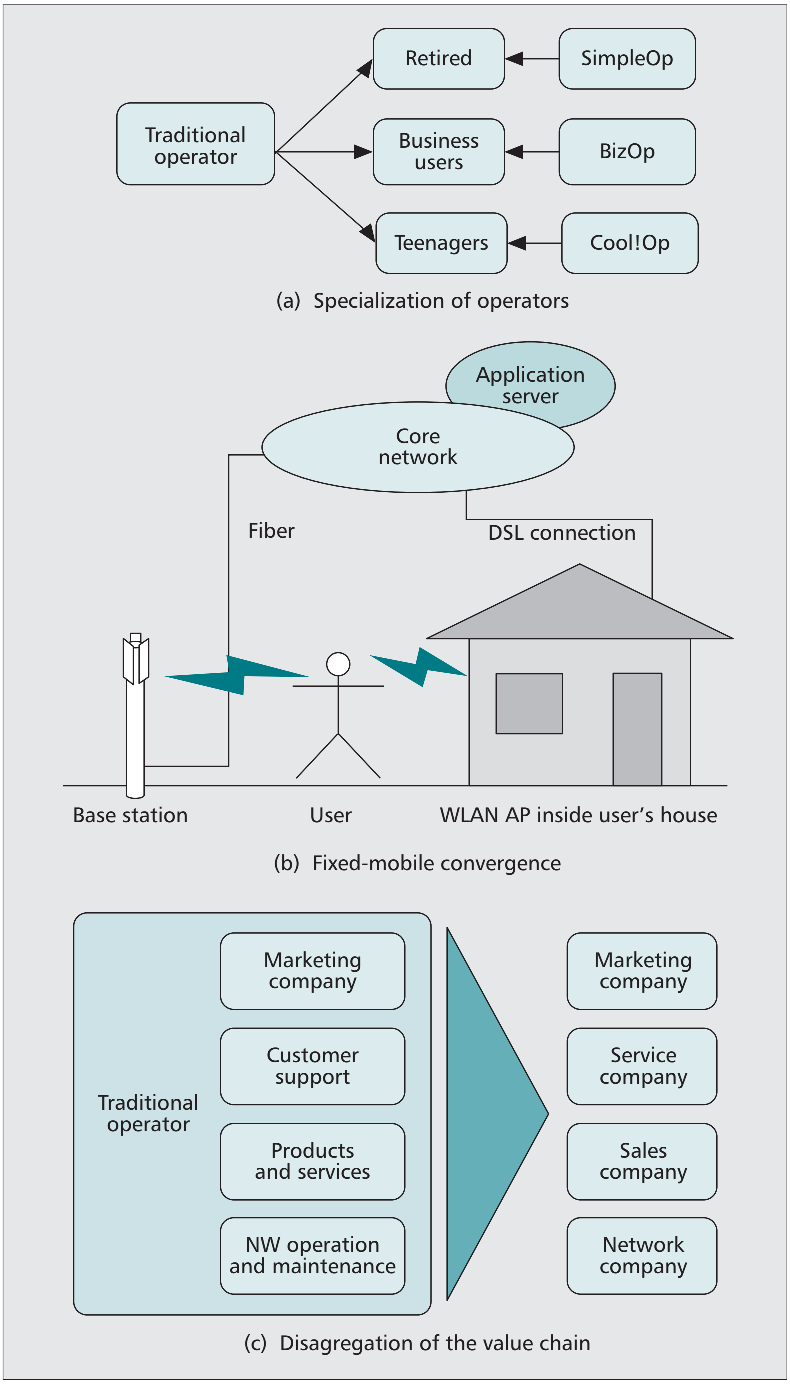


Figure 2. *Transformations of the communications industry.*

The TISPAN RACS

The RACS [10] offers to AFs a mechanism to reserve resources from the network. Figure 4 shows the logical architecture of the RACS (only a subset of the interfaces are visible and the charging aspect is left out of scope) and of the user plane nodes. Refer to [11] for an overview of the TISPAN Release 2 architecture.

The Resource Control Enforcement Function (RCEF) supports a number of elementary functions: opening and closing gates, packet marking, policing of incoming traffic, and resource allocation for upstream and downstream traffic.

The Border Gateway Function (BGF) interfaces two IP domains. It encompasses the functionality of the RCEF and also supports additional elementary functions: usage metering, network address translation (NAT), hosted NAT traversal, etc. The TISPAN BGF is very similar to a 3GPP PCEF.

The Network Attachment SubSystem (NASS) is responsible of authentication and authorization based on the user identity, IP address allocation, and configuration of the user's device via the e1 reference point. In case the user device is a customer network gateway (CNG), the e3 reference point is used to configure it. At last, the NASS supports roaming with the help of two reference points:

- The e5 interface is used to proxy user authentication requests to the home network.
- The e2 reference point enables AFs to retrieve information about the characteristics of the IP-connectivity session used to access such applications (e.g. network location information) from the connectivity session location and repository function (CLF), a sub-component of the NASS.

The RACS itself is composed of two primary function blocks:

- The Access-Resource and Admission Control Function (A-RACF) is a functional entity that manages resources in the AN and performs admission control, taking into account the user's access profile retrieved from the NASS through the e4 reference point. A core RACF (C-RACF) is also defined to manage the aggregation network's resources (but it is user-unaware).
- The Service Policy Decision Function (SPDF) is a functional entity acting as a policy decision point for service requests received from an AF. It applies operator-defined policy rules that specify a service's resource needs, NAT, and firewall traversal rules, etc. It doesn't consider the user identity as it has no direct access to the NASS. The SPDF performs a coordination func-

[2] *A bearer is a logical IP data path between the User Equipment (UE) and the network with specific QoS properties. Bearer binding is the association between a SDF and the IP-CAN bearer (also known as a PDP context for GPRS).*

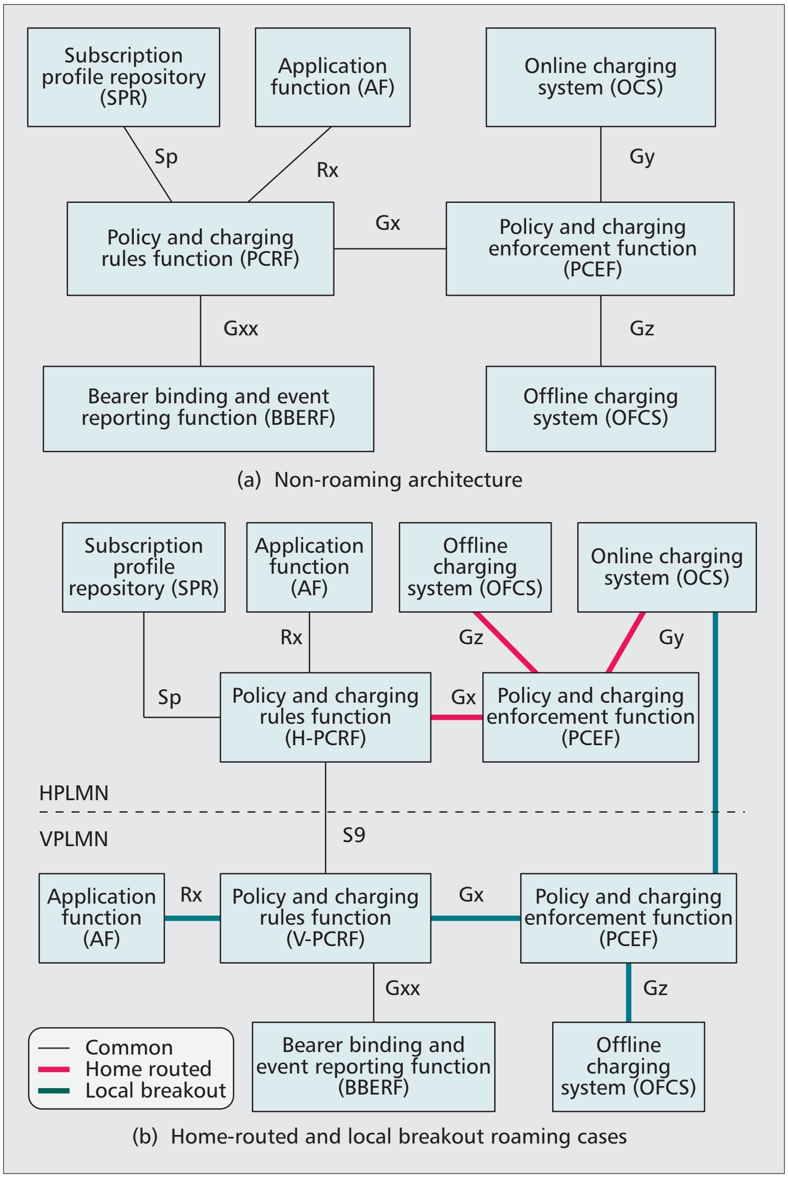


Figure 3. *Logical PCC architecture for the IETF-based EPS (*roaming *and* non-roaming *cases).*

tion between the AF, A-RACF, and BGF. It also supports charging. Roaming is supported over the Ri' interface that links the SPDF in the home network to the one in the visited network. As of TISPAN Release 2, only nomadism is supported, not mobility.

FMC and CN Sharing Issues in 3GPP and TISPAN Networks

When one considers the transformation of the communications industry as seen earlier, some issues appear for both architectures.

Suppose that two operators share a 3GPP CN. Because the operators want to offer their own applications to their users, both need a policy server that takes service requests and user profiles as inputs to the policy decision process, independently of the CN conditions. In addition to taking user- and service-related policy decisions, the 3GPP PCRF directly controls the policy enforcement points (PCEF, BBERF), maps QCIs to DiffServ code points (DSCPs), and determines the charging rules. Clearly, two operators can't control the network resources independently nor decide the network policies to enforce.

On the other hand, the TISPAN architecture is handicapped regarding global mobility, FMC, and roaming because the user is tied to the AN. This also makes it more difficult to integrate mobile virtual network operators (MVNOs).[3]

[3] *A MVNO has no network infrastructures nor spectrum license but it has a subscriber base and can offer applications to its subscribers.*

[4] *An example of network policy could be to keep a minimum of the total bandwidth for best-effort traffic.*

[5] *Note that traditional operators play all roles.*

Requirements on the Policy Control and QoS Architecture to Support CN Sharing/FMC

A number of concepts must be respected to ensure that a PCC/QoS architecture meets current and future needs of the CN. These concepts shall maximize an operator's flexibility to follow any evolution path desired, such as broadening the palette of accesses that a user can choose from, or growing into elaborate network sharing scenarios to reduce costs. FMC and flexible CN sharing have no relationship *a priori* but an evolution of the 3GPP architecture that satisfies the requirements below will improve both aspects. The following four requirements consider FMC and infrastructure sharing in general.

First, the network architecture must clearly separate the services from the network. This implies a separation of policy control applied to the service requested and the user's profile on one side, from the network policies[4] and resource management on the other side. Therefore, this approach would allow service convergence to take place because the users can invoke the services they subscribed to from any AN. Moreover, potential service duplication is avoided because many services are common to all accesses.

Second, the PCC and QoS architecture must separate the subscriber management (service and user policies, IP address allocation, authentication) from the network management. As a consequence, this separation facilitates the integration of a MVNO on top of an existing CN.

The third requirement stipulates that each business/network entity should directly control its assets, especially when they are shared between multiple "clients." For example, a CN operator sharing its assets between two network service providers (NSPs) must ensure that the service level agreements (SLAs) are respected. As a result, the NSPs cannot directly reserve the resources of the CN; they must send a request to a resource manager in the CN for prior approval.

The last requirement applies to FMC support of roaming users. The visited network should be involved in AEG selection because the home network is rarely aware of the visited network's conditions. Also, the visited network should be able to move the UE between accesses based on the evolution of the visited network's conditions.

A Potential Solution

First, we define the following business roles[5] to support network sharing scenarios:

• The network service provider (NSP) hosts

AFs (IMS[6] and non-IMS) and bills the user (by volume, duration, QoS requested, etc). It defines user- and service-related policies (hosts a PCRF), owns the subscriber base, authenticates the user (hosts a HSS), and controls the BGFs in the P-GW. It interacts with other NSPs for roaming.
- The IP aggregation network (IPAN) provider sets up SLAs with the NSPs to which it offers transport services. It owns the edge nodes (e.g. S-GW, P-GW) and interacts with the underneath transport architecture. It links access network providers (ANPs) to the NSPs and offers infrastructure services (e.g. anti-virus DPI[7] engine, traffic localization) to the supported NSPs.
- The access network provider (ANP) manages the access network resources according to a set of local policies and enforces the SLAs made with the IPAN operator(s).

Second, this article builds on top of [12], which has previously described possible enhancements to the mobility architecture. For roaming users it introduced a local mobility anchor in the visited P-GW to clearly separate local and global mobility. This anchor allows the visited network to play a role in the selection of the AEG because it can track the network conditions and move the UE between accesses. The proposed roaming architecture is illustrated in Fig. 5a.

Figure 5b shows a hypothetical network's control plane that focuses on the separation of the business roles and involves two NSPs and two ANPs. The data plane is similar to the one from Fig. 1, except that the IPAN can offer some infrastructure services to the NSPs. Their location is intentionally unspecified as some (notably the location-based) services should be implemented close to the UE to maximize their efficiency.

Infrastructure services can be considered as advanced value-added functions that are shared by numerous applications. They are a generalization of the concept of BGF (which are only implemented into a P-GW) and can benefit both IMS and non-IMS applications.

Each NSP hosts a P-GW that belongs to the IPAN but yields some of its border gateway functions to the NSP. The PCEF functions under IPAN control are QoS enforcement and gating while the others are under NSP control.

The Network Policy Function (NPF) was introduced to manage the IPAN resources and the infrastructure services it offers to the NSPs. Its main purpose is to completely separate the underlying transport network from the NSPs. As a result, NSPs are considered as MVNOs. The NPF enforces the SLAs between itself, the ANPs, and the NSPs. The NPF applies network policies[8] according to the IPAN conditions regardless of the user or service requested. It can modify the network policies based on the situation or time of the day (normal, overload, emergency situation). The NPF is access-agnostic to the PCRF but relies on access-specific mechanisms to perform QoS and admission control in the AN. As such, the NPF is a mediator between the 3GPP CN and the policy infrastructure that might exist for any given access technology. For scalability reasons the NPF only

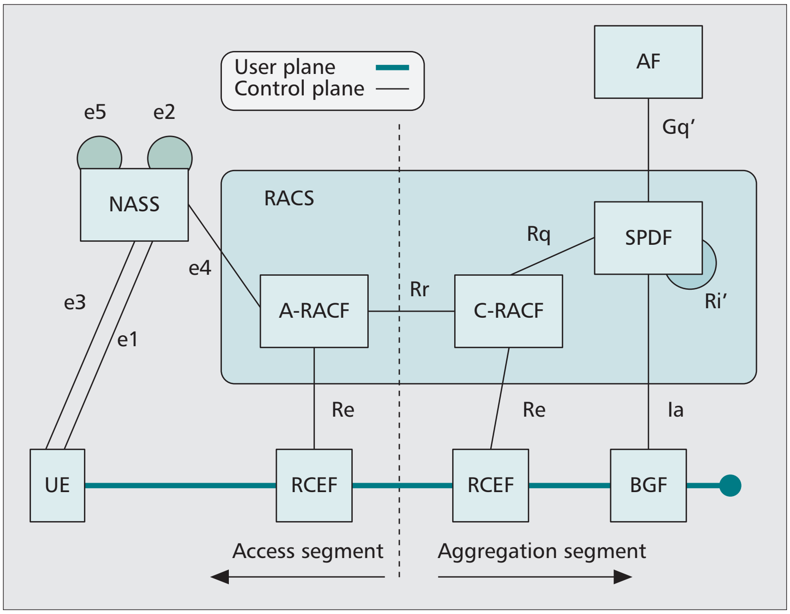


Figure 4. *TISPAN RACS logical architecture.*

performs coarse-grained resource management based on pre-congestion notifications received from the AEGs or P-GWs. This allows the NPF to assist the UE during inter-AEG handovers, by telling the UE, for example, not to switch to the new AEG because the latter notified the NPF of an imminent congestion situation. At least two options for pre-congestion notifications must be studied:
- If the IPAN is a plain DiffServ domain, marking each packet with congestion informations may be appropriate.
- If the IPAN operates on top of virtual circuits (e.g. IP-MPLS, MPLS-TP, PBB-TE), the tunnel ingress node can easily determine when a tunnel is about to become congested.

In both cases, when the ingress node experiences congestion, the NPF is notified so that it will reject any new resource reservation for the congested GBR QoS class until further notice.

Finally, the NPF maps the 3GPP QCIs to L3 QoS classes (DSCP codes) and coordinates the mappings if multiple QoS domains exist in the IPAN. The NPF supports priority services based on the ARP of the resource reservation.

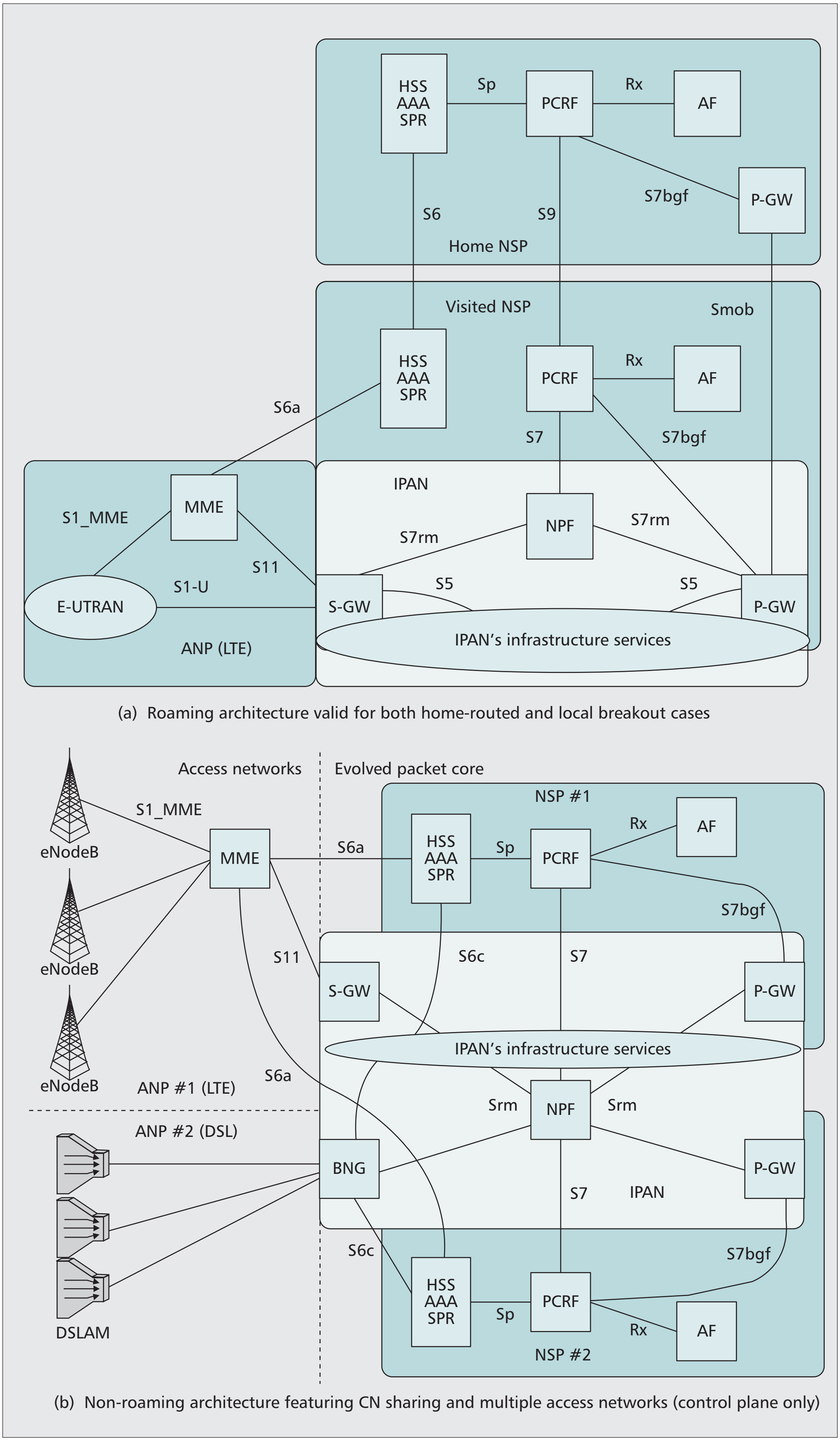
Three Diameter-based reference points are defined in our solution:
- S7 carries the SDF QoS parameters and supports infrastructure service invocation. S7 is based on Gxx and will include the yet to be defined attribute-value pairs (AVPs) to announce and invoke infrastructure services.
- S7bgf controls the border gateway functions and specifies the charging rules to the P-GW for each SDF. S7bgf is based on Gx but doesn't specify the SDF QoS parameters.
- Srm carries the QoS rules of each SDF to the AEGs and P-GWs for QoS rate enforcement and QCI mapping. Srm is based on Gxx.

[6] *The IP Multimedia Subsystem (IMS) is an architectural framework for delivering IP multimedia services.*

[7] *Deep Packet Inspection (DPI) implies that the protocol headers as well as the data traffic are inspected.*

[8] *For example, a network policy could be that the sum of bandwidths of some L3 QoS classes must not exceed a given total because they are mapped to a single L2 class.*

Infrastructure services can be considered as advanced value-added functions that are shared by numerous applications. They are a generalization of the concept of BGF (which are only implemented into a P-GW) and can benefit both IMS and non-IMS applications.



(a) Roaming architecture valid for both home-routed and local breakout cases

(b) Non-roaming architecture featuring CN sharing and multiple access networks (control plane only)

Figure 5. *Proposed evolution of the 3GPP PCC and QoS architecture.*

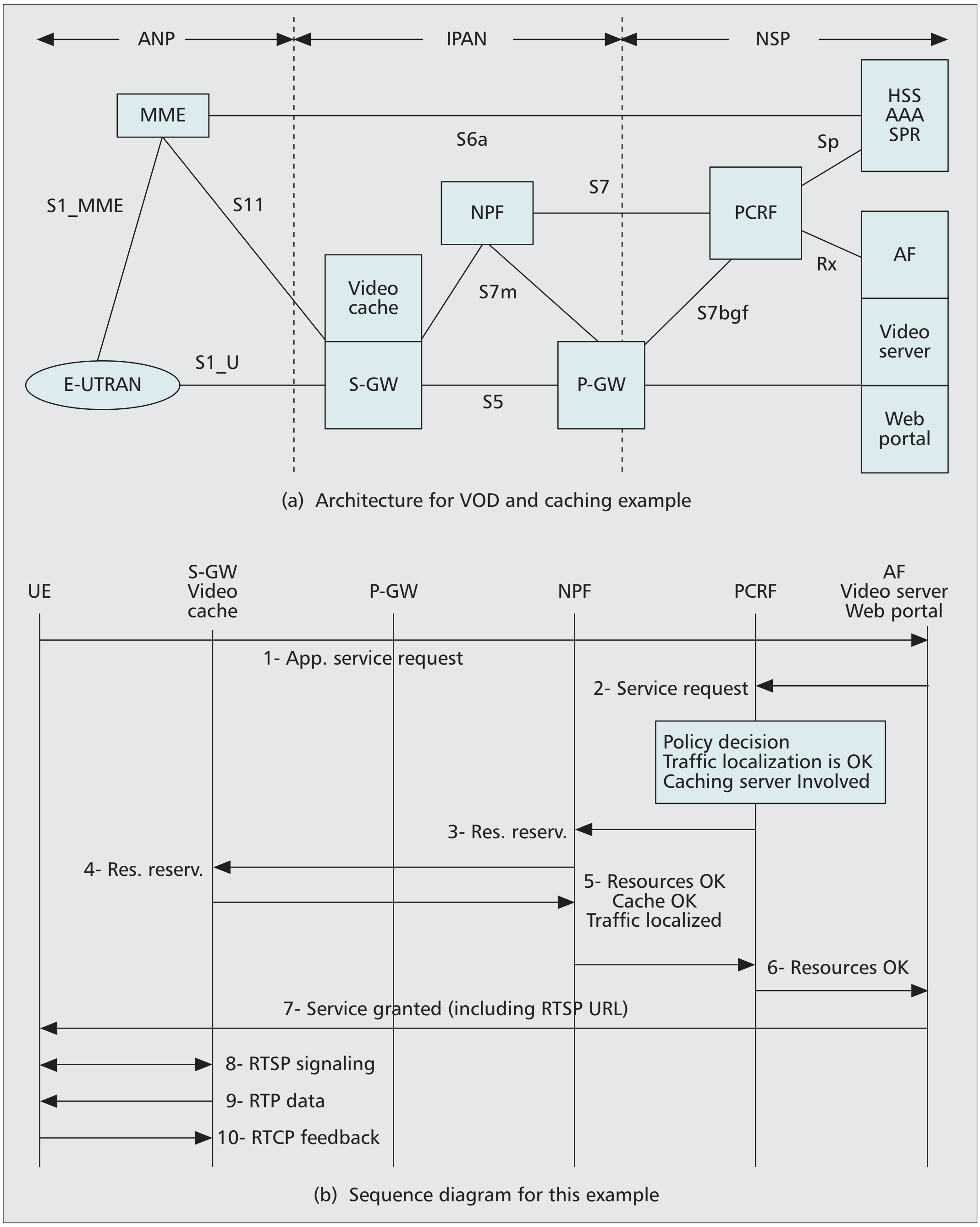


Figure 6. *Infrastructure service example featuring video caching collocated with the S-GW.*

Our solution explicitly defines the NPF to take network policy decisions and perform high-level resource management. In the 3GPP model, static network policies can be defined into the P-GW, but this depends on node configuration.

Figure 6 depicts an example of infrastructure service in which a video on demand (VOD) server uses a cache (collocated with the S-GW) in order to store the most popular movies. This example also features traffic localization which prevents user traffic from being tunneled back to the P-GW unless required. Step 1 shows the application service request sent by the UE to the AF. Step 2 is the service request sent by the AF to the PCRF, describing the resource needs and infrastructure services to invoke. The PCRF decides that the service is entitled to use traffic localization and the video cache, then sends a resource reservation request to the NPF (Step 3). The NPF takes a network policy decision, then sends the resource reservation request to the S-GW in order to set up the resources in the AN and bind the caching server to the corresponding GTP tunnel (Step 4). A positive answer is returned to the AF (Steps 5 and 6). In Step 7, the AF returns a Real-Time Streaming Protocol (RTSP) universal resource locator (URL) to the UE that actually points to the S-GW. Finally, the UE connects to the video caching server and exchanges Real-Time Protocol (RTP) traffic and Real-Time Control Protocol (RTCP) feedback.

Discussion

This section discusses how the requirements from earlier are met by TISPAN, 3GPP, and our proposal. Table 1 summarizes the results.

Concept	TISPAN	3GPP	Suggested evolved 3GPP PCC architecture
Separation of services from the AN.	Full (Gq' interface between the RACS and AF).	Full (Rx interface between the PCRF and AF).	Full (Rx interface between the PCRF and AF).
Separation of user and network management.	AN authenticates user, allocates IP address. A-RACF takes user policy decisions.	User auth., IP addr. alloc. and user-/service-based policy decisions done by CN. No clear separation with IP transport.	User auth., IP addr. alloc. and user-/service-based policy decisions done by CN. Network mgmt. done by the NPF in the IPAN.
Separation of the business roles. Distinct domains for policy and resource mgmt.	Separation of aggregation and AN resource mgmt. and policy control. No distinction between IP transport and NSP.	Distinguishes RAN and CN operators. CN sharing not standardized beyond S-GW.	Clear separation of NSP, ANP and IPAN provider business roles. Flexible network sharing solution.
Local mobility anchor in visited network.	N/A	In S-GW for home routed scenario.	In the P-GW in all cases.

Table 1. *Brief comparison of PCC and QoS architectures: 3GPP, TISPAN, and our solution.*

Separation of AN from Services

From the AF's point of view, all three architectures fully separate the services from the AN. The architectures are access-agnostic and use generic QoS parameters (QCIs are used for 3GPP and our proposed evolution) to specify the packet forwarding treatment. Our proposal and 3GPP use the Rx reference point to link an AF to the PCRF. Similarly, this functionality is achieved by TISPAN with the Gq' reference point that links an AF to the RACS.

Separation of User Management from Network Management

The 3GPP PCC architecture and the evolution we propose feature a Home Subscriber Server (HSS) to store subscriber credentials and service profiles. Both own a PCRF that takes user and service-based policy decisions, for roaming and non-roaming cases, regardless of the network policies and resource management. However, our solution explicitly defines the NPF to take network policy decisions and perform high-level resource management. In the 3GPP model, static network policies can be defined into the P-GW, but this depends on node configuration.

On the other hand, TISPAN doesn't meet this requirement because the AN is user-aware. The NASS retrieves the subscriber profile from the authentication, authorization and accounting (AAA) server, then forwards it to the A-RACF over the e4 interface. Note that the TISPAN network architecture presents serious handicaps for FMC, roaming, and eventually for mobility support. As a result, the A-RACF admission control is based on resource availability, AN policies, and on the subscriber profile.

Separation of Business Roles into Independent PCC/QoS Domains

The 3GPP architecture partially meets this requirement because Universal Mobile Telecommunications System (UMTS) was originally built under the principle of "one operator, one radio access network" [13], and as a result the standard lacks some functionalities that facilitate network sharing. In fact, the only business roles identified by 3GPP are RAN and CN (grouping the NSP and IPAN roles) operators. CN node sharing isn't standardized beyond the S-GW.

TISPAN partially meets this requirement because it considers the access and core networks as two distinct domains. Additionally, it defines the C-RACF which provides a separation of resource management between the access and aggregation networks. However, as with 3GPP, there is no distinction between the entity that provides IP transport and the one that owns the user database and offers application services.

Our proposal specifically introduces the NPF to manage the IPAN and share the CN resources in multiple NSP scenarios. Each AN is responsible for its own resource management, but the NPF relies on access-specific mechanisms to determine if there are available resources in both the aggregation and AN. It is worth noting that most access technologies do not define a central AN policy server and resource manager.

AEG Selection when Roaming

This requirement is not met in the 3GPP Release 8 specifications for the home-routed case. The UE's traffic is tunneled between the visited S-GW and the home P-GW. The visited network cannot move the UE to another AEG. This does not apply to TISPAN because only nomadism is supported in Release 2. Finally, our solution inherited a local mobility anchor in the home-routed and local breakout cases.

Conclusion

This article suggested possible enhancements to the 3GPP PCC architecture to ease the design of advanced infrastructure sharing scenarios and better support FMC. These are built on top of the following concepts:

- *Separation of the services from the AN* that is essential to full service convergence.
- *Separation of user/network management* to simplify the roaming support and facilitate the creation of MVNOs.

- *Separation of business roles into independent PCC/QoS domains* that simplifies the design of complex sharing scenarios that not only cover networks that were designed with sharing in mind but also those that introduce it later on as an evolution path that follows a NSP's change of business strategy.
- *Local mobility anchor in visited network* for roaming scenarios. The UE can move to another AEG based on network conditions.

The next steps of this work are to fully specify the reference points and network nodes affected. Two additional work items are the support of infrastructure services and inter-AEG handovers.

Our proposal specifically introduces the NPF to manage the IPAN and share the CN resources in multiple NSP scenarios. Each AN is responsible for its own resource management, but the NPF relies on access-specific mechanisms to determine if there are available resources in both the aggregation and AN.

ACKNOWLEDGEMENTS

The authors would like to thank Reiner Ludwig for reviewing this article. This work was funded in part by the Natural Sciences and Engineering Research Council (NSERC) of Canada under grant agreement 341116.

REFERENCES

[1] 3GPP Tech. Spec. 23.401, "General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access," v8.4.1.
[2] 3GPP Tech. Spec. 23.402, "Architecture Enhancements for non-3GPP Accesses," v8.4.1.
[3] G. Smith and C. Beckman, "Shared Networks: More Than Making Wireless Communications Affordable," *IEEE 61st Vehicular Tech. Conf.*, vol. 5, 2009, pp. 2984–88.
[4] W. Webb, Ed., *Wireless Communications — the Future*, Wiley, 2007.
[5] T. Frisanco *et al.*, "Infrastructure Sharing and Shared Operations for Mobile Network Operators From A Deployment and operations view," *NOMS 2008 — IEEE/IFIP Network Operations and Management Symp.: Pervasive Management for Ubiquitous Networks and Services*, 2008, pp. 129–36.
[6] 3GPP Tech. Spec. 23.203, "Policy and Charging Control Architecture," v8.4.0.
[7] J-J. Pastor Balbás, S. Rommer and J. Stenfelt, "Policy and Charging Control in the Evolved Packet System," *IEEE Commun. Mag.*, vol. 47, no. 2, Feb. 2009.
[8] H. Ekström, "QoS Control in the 3GPP Evolved Packet System," *IEEE Commun. Mag.*, vol. 47, no. 2, Feb. 2009.
[9] 3GPP Tech. Spec. 23.251, "Network Sharing; Architecture and Functional Description," v8.0.0.
[10] ETSI Standard 282 003, "TISPAN; Resource and Admission Control Sub-System (RACS): Functional Architecture," v2.0.0.
[11] ETSI Standard 282 001, "TISPAN; NGN Functional Architecture," v2.0.0.
[12] S. Krishnan, L. Marchand and G. N. Cassel, "An IETF-based Evolved Packet System Beyond the 3GPP Release 8," CTIA — The Wireless Association, 2008. [13] 3GPP Tech. Spec. 22.951, "Service Aspects and Requirements for Network Sharing," v8.0.0.

BIOGRAPHIES

STÉPHANE OUELLETTE (stephane.ouellette@ericsson.com) received his B.Eng. and M.S. degrees in computer engineering, respectively in 1999 and 2006, from Ecole Polytechnique, Montreal, Canada. He is currently doing his Ph.D. in collaboration with Ericsson's Broadband and Systems Research group located in Montreal. His research interests include QoS and policy control in converged networks. He is also a teaching assistant at Ecole de Technologie Supérieure (affiliated with University of Quebec in Montreal, Canada). He is a graduate student member of the IEEE.

LAURENT MARCHAND (laurent.marchand@ericsson.com) received his B.Eng. and M.S. degrees from Ecole Polytechnique, Montreal, Canada. He is the technical director of the Corporate Ericsson Research Unit in Montreal. Prior to joining the Research Unit, he was Systems Manager and technical member in the Ericsson TDMA Business Unit where he contributed to the successful development and deployment of the Digital AMPS cellular network product. Before joining Ericsson in 1991, he was head of research and development for a telecom equipment supplier in Ottawa, where he worked on the development of a new generation of digital switches and on Network Management applications.

SAMUEL PIERRE [SM] (samuel.pierre@polymtl.ca) received the B.Eng. degree in civil engineering in 1981 from Ecole Polytechnique, Montreal, Canada. He obtained his B.S. and M.S. degrees in mathematics and computer science in 1984 and 1985, respectively, from University of Quebec in Montreal, Canada. He also received the M.S. degree in economics in 1987 from the University of Montreal, Canada, and his Ph.D. in electrical engineering in 1991 from Ecole Polytechnique. He is currently a professor of computer engineering at Ecole Polytechnique, where he is also the director of the Mobile Computing and Networking Research Laboratory (LARIM) and the holder of the NSERC/Ericsson chair in next generations fixed and mobile networking systems. His research interests include wireline and wireless networks, mobile computing, artificial intelligence, and telelearning. He is a fellow of the Engineering Institute of Canada (EIC). He is a regional editor of the *Journal of Computer Science*, an associate editor of *IEEE Communications Letters*, *IEEE Canadian Journal of Electrical and Computer Engineering*, and *IEEE Canadian Review*, and serves on the editorial board of *Telematics and Informatics* (Elsevier Science).