Designing a Wireless Broadband IP System with QoS Guarantees

Juha Ala-Laurila[1], Lorraine Stacey[2], Neda Nikaein[3], Jukka Seppälä[4]

[1,4] Nokia Mobile Phones, P.O. Box 68, FIN-33721, Tampere, Finland
email: juha.ala-laurila@nmp.nokia.com

[2] Lucent Technologies, Swindon, United Kingdom
[3] Eurecom Institute, France

Abstract: *The growth of the Internet community and the trend towards multimedia services changes the Internet Protocol (IP) suite. Simultaneously, users desire to have a high speed wireless access to the Internet. To meet the increased service and mobility needs the traditional IP protocol has been enhanced with advanced mobility and Quality of Service (QoS) features. This paper proposes a concept which seamlessly integrates these modern IP techniques with wireless broadband radio access technology. The defined wireless IPv6 based radio access network supports real-time applications in mobile IP environment utilising specific radio flows for QoS management. The ACTS WAND wireless ATM access system was considered as a starting reference point which was extended to provide efficient native IP support. The depicted system architecture covers the mobile terminal, radio access network and the necessary interworking functions.*

Introduction

The Internet is changing from a best-effort services model to an integrated services model with a wide range of applications and different traffic characteristics. The introduction of new innovative Quality of Service (QoS) aware Internet Protocol techniques, such as integrated services and differentiated services has significantly improved the usability of multimedia and real-time applications in the Internet. The integrated mobility features of IPv6 and mobile IP increase the suitability and attractiveness of the IP protocol suite even more in mobile networks. Many experts foresee that instead of ATM, IP will maintain its position as the leading access network technology in fixed Local Area Networks (LANs). Consequently, in the future wireless Internet extensions should offer native IP access over high speed indoor radio link and reliably maintain IP QoS characteristics over the air interface.

The original target of the ACTS Magic WAND project was to design 20 Mbit/s, 5 GHz radio access to ATM backbone as it was globally expected that ATM will become de-facto networking technology also in LANs. In the WAND reference design IP services are provided using LAN Emulation (LANE) which does separate IP packets with different QoS requirements but handles all IP traffic as best-effort data [Mik98]. CLassical IP (CLIP) technology, where IP packets are directly encapsulated into ATM Adaptation Layer (AAL5) frames was not deployed as it will not provide any QoS mechanisms. Furthermore, neither CLIP nor LANE support delay sensitive multimedia.

To provide an efficient wireless access to the Internet backbone the WAND project has started to specify a new mechanism which is optimised for transmitting native IP traffic over the 5 GHz radio link. The target is to minimise the IP protocol overhead in the wireless interface and to seamlessly support IPv6 and state-of-the-art IPv6 QoS mechanisms. The proposed concept enables full exploitation of real-time IP applications in mobile environment thus increasing the applicability of the developed 5GHz WAND radio modem.

This paper describes how the wireless ATM system was changed into the native IP access system. The first part describes the design framework and system architecture focusing on the QoS and IP flow management scheme. The latter part of the document briefly introduces the outlines of the mobility management and optimised wireless multicast delivery which are also essential parts of the wireless IP broadband network.

IP Design Framework

Wired networks are gradually being upgraded to support the new IPv6 protocol suite which solves the existing problems related to IPv4 routing and addressing schemes [Dee95]. An important IPv6 feature is the introduction of flow labels which offers an easy way of separating various IP packet streams. In the context of service quality the advanced IPv6 flow identification mechanism allows to assign different priority characteristics for each packet stream. An additional benefit of IPv6 is the integrated standard network level mobility management scheme which enables the terminal mobility within and between IP domains. Mobile IP services include IP address auto-configuration and seamless packet routing which are necessary also in the wireless environment. Due to its virtues and future potential IPv6 was selected as a protocol framework for the proposed native broadband IP network architecture.

System Architecture

The reference wireless Internet access architecture, depicted in Figure 1, is composed of Mobile Terminal (MT), Access Point (AP) and Mobility enhanced IP router (M-router). Compared to the wireless ATM network (WAND) the main architectural changes concern the network part in which the mobility enhanced ATM switch is replaced with the IP-router.

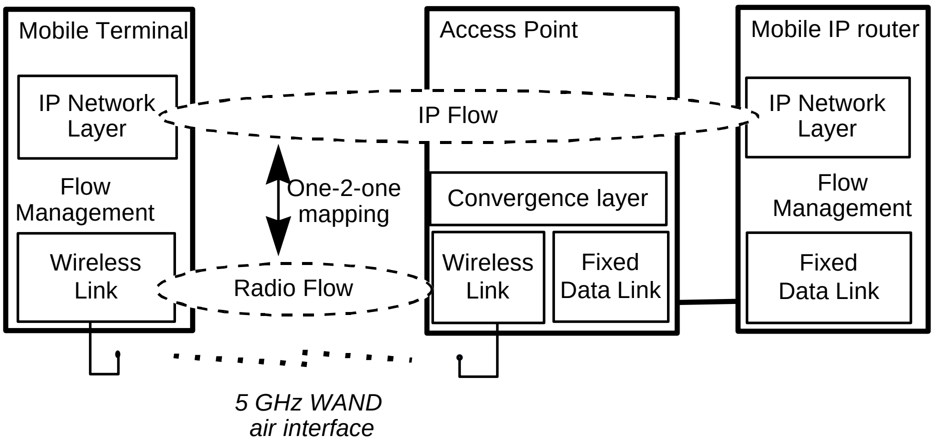

Figure 1: Wireless broadband IP system architecture

The Mobile Terminal is the user device for accessing wireless Internet services. The terminal will be the end point of the Internet and radio access network control protocols.

The Access Point implements all of the radio dependent control functionality, such as radio resource management, setup and release of radio flows. It has an embedded IP stack for control and configuration purposes. Neighbouring access points attached to the same M-router belong to the same IP subnet making intra-router handovers transparent to the network layer (here IP).

The M-router creates the wireless IP subnet managing one or more access points. It will provide mobility services, such as Dynamic Host Configuration Protocol (DHCPv6) functionality, home agent services, and mobile terminal location management database. DHCP is used for allocating IP addresses for the terminals (stateful address auto-configuration) while home agent is needed to provide mobility between wireless IP subnets.

In the proposed architecture the ATM control signalling is replaced with a specific IP flow management protocol which classifies IP flows in the core network interface. By default all IP packets are transmitted as best-effort data. As the mobility enhanced IP router detects an IP flow it marks the IP packets belonging to the flow with a dedicated flow identifier and establishes a new radio flow to which the IP packets will be switched. The flow identifiers map the radio flows and IP flows together. The IP QoS parameters of a certain flow define the packet (flow) scheduling priority in the radio link, which guarantees that time-critical data flows are always handled first. Figure 1 shows the flow mapping principle.

The defined concept follows the outlines of the theoretical General Radio Access Network (GRAN) reference model [ES21]. In theory the same WAND radio access network could be connected to both IP and ATM backbones simply by defining the necessary interworking functions for the terminal and the network side. Reference points for interoperability are assumed to exist in two places. The first one is in the radio interface. This is intended to follow the BRAN HIPERLAN/2 standardisation outlines. The second reference point is in the radio access network - core network interface, i.e. between AP and M-router. This will make the radio access networks of different manufacturers compatible with each other. In addition the latter reference point defines the interoperability of the core and radio access networks, e.g. implementation of mobility features.

Control and User Plane

In IP networks all communication is packet based relying on a connectionless transmission scheme. Although the small fixed size cell nature of ATM works well in terms of efficient multiplexing and forwarding speeds, ATM connection-oriented control protocols are not appropriate for native IP traffic. Therefore, ATM control is replaced with a Wireless Flow Management Protocol (WFMP) similar to the Ipsilon Flow Management Protocol (IFMP) which classifies IP flows in the core network interface and establishes IP flows between terminals and the core network in the proposed wireless IP system [New96]. The defined lightweight WFMP signalling minimises the wireless overhead and decreases implementation complexity. A significant difference between WFMP and traditional ATM signalling is that ATM creates virtual channels (VCs) end-to-end. In contrast WFMP creates dedicated VCs on a hop-by-hop basis between MTs and IP routers. Moreover, ATM control must create VCs before the traffic flows. In contrast WFMP uses the flow of traffic to trigger the creation of dedicated VCs.

Figure 2 illustrates the resulting data and control plane architecture. The radio resources are managed by Radio Resource Manager (RRM) which locates in each access point. In this concept RSVP protocol is used for making explicit bandwidth and delay reservations in the radio interface.

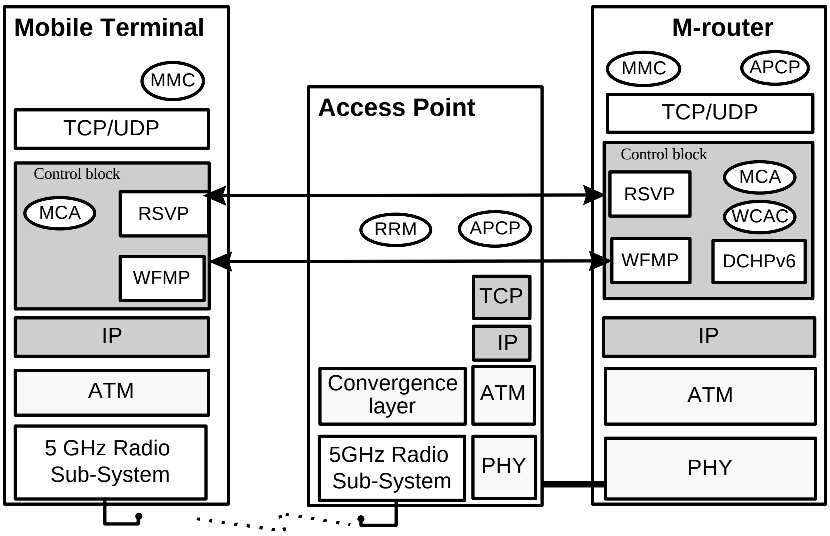

Figure 2: Data and control plane architecture

Wireless Call Admission Control (WCAC) inside the M-router handles RSVP reservation messages and sends a query to RRM which checks the available capacity. RRM communicates with the M-router using Access Point Control Protocol (APCP). The radio level mobility management, such as terminal registration and radio access network handovers are handled by Mobility Management Control (MMC) blocks which reside in the M-router and the terminal. The MMC functionality

resembles. the original WAND implementation [Mik98]. The wireless optimised multicasting, is managed by MultiCast Agents (MCA) in terminals and in the M-router.
The wireless IP system retains ATM in the user plane where ATM creates a convergence layer between the IPv6 flows and the radio link flows offering an easy way of identifying IP flows between the access points and the core network. IP packets belonging to a specific flow are transmitted with a dedicated virtual channel identifier to the access point, which sends the data to the mobile terminal using a radio flow identifier that corresponds to the VC value thus mapping IP QoS parameters into the radio link. By default all IP traffic is carried on a default best-effort VC and forwarded hop-by-hop by intermediate IP routers. However, long-lived or real-time IP traffic is detected in M-router and switched through the network via dedicated VCs created by WFMP. Furthermore, to save scarce radio resources the IP packets are compressed. For instance, sending a complete IP header with full IP address (128 bit) is not necessary for all packets. Instead of transmitting complete IP headers over the radio link, the reference IP system proposes the use of IP header compression scheme which is discussed later in this paper.

QoS Management Scheme

The QoS approach can be divided into two parts: radio access network QoS and core network QoS services. IETF has specified two competing QoS approaches: integrated and differentiated services. RSVP, which is part of integrated services, maintains QoS state end-to-end and requires state reservations in each router in the Internet while the differentiated services separate each service into traffic classes which require only different queues in each router. The Internet society considers the latter as a more scaleable option which may become the de-facto standard in wired networks.

The defined wireless IP network should be compatible with the fixed IP network state-of-the-art QoS solutions. Therefore, the proposed QoS approach is independent of the backbone QoS technique and provides only a mechanism for mapping the fixed network QoS parameters into the air interface. In this scheme the radio flow identifiers are always mapped with a certain QoS value which are derived from the IP QoS parameters. The network level QoS parameters are input to the DLC scheduler entity which maintains the guaranteed QoS in the radio link. RSVP and real-time traffic are handled with the highest priority. Flows which are not delay sensitive (e.g. WWW connections) are scheduled as medium priority traffic while all the packets without any flow are handled as best-effort traffic which is transmitted as there are free slots left in the radio link. The differentiated service can be adopted into different radio access priority classes.

IP Flow Detection

Here it is assumed that the MT and the M-router are WFMP peers (i.e. VCs are created between MTs and the M-router). The M-router will establish a dedicated VC for a traffic flow and request the neighbouring MT to use this VC. This process occurs when the M-router’s flow detector is triggered (i.e. if the number of packets seen for that flow exceeds a threshold). The ATM connection identifiers are always allocated by the M-router. WFMP classifies flows on the basis of a matching combination of header field values. In addition RSVP reservation messages trigger the flow classification process.

IFMP defines different flow types only for IPv4 systems. In the case of IPv6 two other scenarios have to be considered: the first is if IPv6 packets contain a non-zero flow label. In this case the IPv6 source address and flow label have to be utilised for detecting a flow. Thus this combination is a valid flow identifier. Furthermore, [Dee95] states that all packets belonging to the same flow must be sent with the same source address, destination address, flow label, and hop-by-hop options header contents. If the packet contains a routing header, each packet in that flow must have the same contents in all extension headers and include the routing header (note the hop-by-hop and destination extension headers are usually placed before the routing header). Hence, if the flow label is zero, two other valid flow identifiers are the combination of the fields described above. It is possible to take into account also additional criteria for detecting flows, such as transport protocol port numbers. In addition the extension header format of IPv6 should be considered. Significant processing time may be required to access some header fields (e.g. the TCP or UDP port number) since all preceding headers will need to be parsed first. Hence in the Wireless IP platform we assume the following IPv6 flow identifiers:

Table 1: Specified IPv6 Flow Identifiers

Flow Type	IPv6 Header Fields
I	Source Addr; Flow Label
II	Source Addr; Dest Addr; Flow Label; Hop-by-Hop Options
III	Source Addr; Dest Addr; Flow Label; Hop-by-Hop Options; Destination Options; Routing Header

As discussed earlier, the flow detection process is independent of the resource reservation process which in the future could be based on RSVP, differentiated services or some other resource reservation protocol. As a result we do not support the case where RSVP flows directly trigger the system to create a dedicated flow. Instead, all flows are detected on the basis of data traffic flowing through the M-router.

IP Header Compression Scheme

Efficient transmission of data is particularly important in a wireless environment, because the available bandwidths tend to be lower, and the loss rates higher. Several encapsulation schemes are proposed to make the transmission of IP traffic more efficient, by not transmitting unnecessary IP header fields [Deg93]. However, the current IP switching encapsulation types are defined for IPv4 networks only. These encapsulation types are linked to the flow identifiers. All packets in a given flow must have the same values for several header fields. Thus there is no need to transmit these header fields in each packet. Instead, they can be reinserted into the packet at the end-point of the dedicated VC. For IFMP compression the savings per packet are 8, 24 and 16 bytes depending on the IP flow type. The same concept is applied for the IPv6 based wireless IP system. Three flow identifiers are proposed, I for use with non-zero flow labels and II and III for flows with zero flow labels (see table 1). For type I and II flows all packets belonging to the flow must have the same values for the following fields: source address, destination address, flow label, and hop-by-hop options. These fields can be ignored in the wireless link, which causes significant resource savings. As stated above, for type III flows, all extension headers up to the routing header must have the same value. All fields in these headers can be removed from each packet. Thus for type III flows even greater bandwidth savings can be made.

To summarise, the encapsulation schemes in IPv6 can offer even greater bandwidth savings than in IPv4 networks. However, it is important to note that the proposed encapsulation can only be employed for dedicated flows which are marked with specific VCs. For the best effort data we have to transmit also IP headers since multiple traffic flows are carried on the same VC.

Mobility Management

Mobility is an inherent part of the system specification. The specified mobility management scheme provides full terminal mobility within the M-router and between routers. Both radio access network and IP domain mobility are supported. The radio access network mobility scheme deploys the handover mechanism developed for the wireless ATM approach while the core network mobility management utilises IPv6 mobility functions. Unlike in wireless ATM, the handovers can be hard and lossy due to the connectionless nature of the IP network. If the user moves within the same IP subnet the mobility is transparent to the network layer and the system tries to maintain IP flows and IP QoS parameters. In the case of inter IP domain mobility the reservations are re-created due to which a few packets may be transmitted as best-effort traffic. The M-router maintains a database of the mobile terminals that are registered into the particular access network while the IP home agent keeps track of the IP level mobility routing packets into the correct M-router. The detailed mobility management scheme is described in[HaPas98].

Wireless Optimised Multicasting

The wireless interface causes specific requirements also for the multicasting scheme. To avoid the waste of bandwidth, multicast packets must be forwarded only to the APs with active members of the specified group. Therefore, a multicast management agent is added to the M-router which has to keep a location list of MTs per group. The location list contains all APs having at least one registered terminal of that group. The multicast management agent processes all join/leave messages transmitted by MTs and updates the group location lists. The multicasting agent is also responsible for updating the groups' location lists in case of handover. Host mobility will cause an update in a group location list if a MT, which is the last member of a group in its AP, makes a handover or if a MT enters a cell in which it is the first member of a group.

Local multicast delivery is done in each AP using the native broadcasting capability of the radio interface. A multicast group is identified by a link layer address in an AP. This address is allocated by AP whenever there is a join demand for a group that does not have any members in that AP. The AP uses this address as long as it has at least one member of the group in its cell. This address is communicated by the AP to its local group members that use this address for multicast packet reception. As a consequence, multicast communication requires modifications to both the network layer and the radio link layer.

Conclusions

The depicted architecture follows the BRAN reference model introducing native IP into the 5 GHz radio access network. The presented QoS and mobility management schemes are compatible with the fixed IPv6 network techniques. Modern IPv6 mobility functions are combined with previously defined radio access network mobility management (target WAND) functionality, which provides a flexible and efficient addressing and handover scheme. The ATM signalling is replaced by the light-weight WFMP protocol which improves performance. As the radio flow management is independent of the deployed IP protocol suite, the reference IP system can be enhanced to support alternative IP techniques, such as differentiated services in the future. The reference architecture creates design outlines for the 5 GHz wireless native IP access system maximising the synergy with the WAND wireless ATM access system. The final system specification is to a great extent dependent on the development of the IP protocols and QoS services in fixed LANs. However, native IP system creates a fascinating alternative for the conventional wireless data networks.

Acknowledgements

This work has been performed in the framework of the project ACTS AC085 The Magic WAND, which is partly funded by the European Community and the Swiss BBW (Bundesamt für Bildung und Wissenschaft). The authors would like to acknowledge the contributions of his colleagues from Nokia Mobile Phones, Lucent Technologies, Tampere University of Technology, Technical Research Centre of Finland, Ascom Tech AG, University of Lancaster, Robert Bosch GmbH, University of ULM, Compaginie IBM France, IBM Zürich Research Laboratory, Eurecom Institute, ETH Zürich, Intracom Hellenic Telecommunications and University of Athens.

References

[Dee95] S. Deering, R. Hinden, "Internet Protocol, version 6 (IPv6) specification", IETF RFC 1883, Dec 1995.

[ES21] Draft ES 21.01, "Universal Mobile Telecommunication Systems (UMTS); System concepts and reference model for the UMTS", ETSI, v1.0.0, February 1997.

[New96] P. Newman et. al., 'Ipsilon Flow Management Protocol Specification for IPv4 Version 1.0', RFC1953, May 1996.

[Mik98] Mikkonen et. al., The Magic WAND—Functional Overview. To appear in IEEE JSAC, special issue on Wireless Access Broadband Networks, August 1998.

[Deg93] M. Degenmark et.al.; " IP Header Compression, INTERNET DRAFT, Networking group"

[HaPas98] Stathes Hadjiefthymidiades, Sarantis Paskalis et. al. “Mobility Management in an IP-based Wireless ATM Network”, ACTS Mobile Summit 98, Greece