Review of Advanced Mobility Solutions for Multimedia Networking in IPv6

József Kovács[†], László Bokor[‡], Zoltán Kanizsai[‡], Sándor Imre[‡]

[†]Computer and Automation Research Institute, Hungarian Academy of Sciences, Systems and Control Laboratory, Pervasive Networks Research Group. Kende u. 13-17, H-1111, Budapest, Hungary. jk@sztaki.hu

[‡]Budapest University of Technology and Economics, Department of Telecommunications, Multimedia Networks and Services Laboratory. Magyar Tud. krt. 2, H-1117, Budapest Hungary. {bokorl | kanizsai | imre}@hit.bme.hu

ABSTRACT

IPv6 is the new version of the Internet Protocol (IP), which is expected to be introduced for the wide audience in the forthcoming years. IPv6 comes with a huge amount of improvements compared to the currently widespread IP version (IPv4), while it keeps the same conceptual basics. For instance, IPv6 has a comprehensive and built-in scheme for mobility management with a great set of additional functionality, while IPv4 has only an extension for this purpose (and it is usually not implemented). Considering the evolution of telecommunication architectures toward a heterogeneous all-IP fixed-mobile convergent multimedia-provisioning system, it is now obvious that only the appearance of IPv6 could extend the infrastructure to cope with the emerging scenarios and use-cases. This chapter will provide a broad introduction of the advanced IPv6 features and will guide the readers from the basics of the new IP protocol family to its complex feature set and power to support multimedia communications in the mobility-centric Future Internet. Optimization techniques to further increase the adequacy of IPv6 for mobile multimedia are also presented along with the description of several research directions.

INTRODUCTION

The vision of "anytime and anywhere" has become a powerful concept for voice telephony, where it has been widespread as a global phenomenon and an essential infrastructure. However, nowadays mobile telecommunications aim to emerge beyond individualized voice services and converge to a much more complex system by having mass media content (text, voice, sound, images, video, etc.) within integrated service platforms such creating the phenomenon of mobile multimedia. Newspapers, magazines, books, Internet radio and TV channels, web-sites, portable music (e.g., in MP3 format) or portable/on-line electronic games, text and rich (incorporating voice/picture/video material) messages, real-time and on-demand video materials (e.g., video phone) and photos are taking part from the emerging new medium of ubiquitous mobile networking which also continuously creates new types of content, initiates new technologies and allows people to interact in novel ways.

In order to make all the above advanced mobile media applications available for the wide audience, network operators are taking the challenge of combining mobile communications and the Internet.

The convergence is not only observable in networks but also in devices and services, and also amplifies the essential need of networked information provisioning for users anytime and anywhere. Current trends place mobile Internet architectures into the focus point of the whole technological progress. With the development of various wireless network technologies such as WiFi, WiMAX, UMTS, HSPA, LTE, LTE-A, more and more users want to enjoy the benefits of seamless connectivity and ubiquitous Internet access. Vendors prognosticate that mobile networks will suffer an immense multimedia traffic explosion in the packet switched domain up to year 2020 (UMTS Forum, June, 2010), (Cisco VNI, Feb. 2011). In order to accommodate the future Internet to the anticipated demands and requirements, technologies applied in the radio access and core networks must become scalable and appropriate to advanced future use cases. Network operators not only have to take care of the growing traffic volumes and mass of users, the heterogeneous, overlapping wireless access, and

secure communication, but they have to enforce certain policies in order to provide the necessary Quality of Service (QoS) to consumers, all considering the fact that majority of mobile traffic consists of multimedia content (Bokor, Faigl, & Imre, 2011).

The increasing number of consumers, the complexity of mobility scenarios, the technological convergence in telecommunication and information technology present a great challenge for the architecture of the Internet we use today, as such things were not envisioned in the 70's, when the still used IP protocol was designed: IPv4 does not allow the mobility of hosts, works with relatively small address space and lacks support for QoS. To address all problems and serve the evolving trends of mobile communication, IPv6, a new version of the protocol was developed (Hinden & Deering, 2006), (Deering & Hinden, 1998). In terms of multimedia requirements, IPv6 has a number of features that not only optimize current networking techniques for multimedia content transmission, but tries to keep up with the growing demand for services, especially in mobile environments.

Future generations of mobile and wireless technologies will provide virtually unlimited possibilities to the community of multimedia users all over the world. Network technology innovations and architecture evolution will create the convergent environment in which every media is available, and networked resources are accessible anytime and anywhere, via any kind of connected device in any number. IPv6 – as the common language of the Future Internet both in the fixed and mobile domains – could be one of the most important tools for mobile content service delivery, in which enlarged address space, advanced security, multicast and QoS capabilities are naturally integrated with efficient and extendable mobility management in order to support mobile multimedia services for every possible application scenario.

In this chapter we summarize the feature set of IPv6 for enabling seamless, transparent and secure transmission of multimedia content over mobile IPv6 networks, then the authors, as result of their research, introduce a new handover technique which intends to increase networking performance of mobile multimedia services.

IPV6 ESSENTIALS: THE BACKGROUND OF MOBILE EVOLUTION

Content delivery is shifting towards peer-to-peer networks, while the majority devices are becoming mobile. This is intensified by Machine-to-Machine (M2M) communications which also accommodate end-to-end communicating devices without human intervention for remote controlling, monitoring and measuring, road safety (e.g., traffic avoidance, enforcement, and control systems), security/identity checking, video surveillance, electronic healthcare delivery, personal locator services, etc. Predictions state that there will be 225 million cellular M2M devices by 2014 with little traffic per node but resulting significant growth in total, mostly in uplink direction (Dohler, Watteyne, & Alonso-Zárate, Dec. 2010). Therefore we can say that one of the most obvious features of IPv6 for future mobile multimedia is the large address space.

With a four times increase in address length compared to IPv4, any IPv6 enabled mobile device will be reachable via a globally routable unique address, eliminating the need for address space saving techniques, such as NAT (Network Address Translation). There are 2^{128} different IPv6 addresses, as opposed to the 2^{32} possible addresses in IPv4, which opens up new possibilities for multimedia content delivery. Based on the directionality and the number of participants in the communication, IPv6 addresses are grouped into unicast, multicast and anycast address groups. Due to its one-to-many directionality, multicast addressing is an efficient way of transporting multimedia content, which will be described in greater detail later in the chapter.

The distribution and assignment of unicast IPv6 addresses is another key feature for mobile environments. When a node connects to an IPv6 network it receives Router Advertisement (RA) messages from the router present on the network (Narten, Nordmark, Simpson, & Soliman, 2007). These RA messages contain the prefix used on the network and the validity of the addresses among other information. After processing the message the node generates a unique 64-bit identifier from its physical interface identifier. In case of 48-bit MAC addresses the uniqueness is guaranteed by a simple mapping from 48-bit to the 64-bit EUI address format. The generated address together with the network identifier received from the router is the unique global IPv6 address for the given host. This address configuration method is called stateless address autoconfiguration (Thomson, Narten, & Jinmei, 2007), and only available in networks with 64-bit or less prefix size.

When the stateless method is not applicable on a given network due to prefix size or other reasons, different IPv6 address provisioning mechanisms may be used. Stateful address autoconfiguration such as DHCPv6 (Droms, 2003), is a technique where address provisioning and accounting is managed by a dedicated node on the network.

The faster address configuration shows its advantage in mobile environments, allowing fast handovers between access networks, while granting media carrying transport and application protocols to continue to work seamlessly, anytime and anywhere.

The simplified header format offers several options to increase the performance of IPv6 when carrying multimedia content.

The Traffic Class field, which marks the priority of packet delivery, is used to ensure QoS (Quality of Service). As media content takes up significant slice of the overall Internet traffic, the networking protocol needs to be prepared to ensure the quality of service and experience remains positive for the user. IPv6 has a number of ways to improve support for QoS (Rajahalme, Conta, Carpenter, & Deering, 2004), (Ping & Desheng, 2010), (Zhenhua, Qiong, Xiaohong, & Yan, 2010). The Flow Label field allows labeling of packets belonging to the same data stream, such as TCP stream. Payload Length marks the size of the payload carried in the IPv6 packet, while Hop Limit defines the max number of hops a packet is allowed to travel. Fragmentation related fields are missing from the IPv6 header as IPv6 does not fragment the payload. Instead, communication parties perform Path MTU Discovery (McCann, Deering, & Mogul, 1996) to determine the maximum payload size between the source and the destination.

The protocol uses the Next Header field to mark the type of the next protocol in the packet, allowing the presence of multiple IPv6 extensions while making it possible to prioritize transport protocols more easily.

Communication in the open, packet-based Internet must consider also security aspects. It is much easier to capture voice information transmitted by a VoIP solution through the Internet than by PSTN operating on basics of circuit switching. The same applies to all multimedia traffic using IP-based architecture as transport medium. The level of threat is even more serious if the medium is shared, as in case of wireless and mobile environments. That is why another significant advantage of the new IP protocol is the standardized and deeply integrated IPsec security framework, implementing flexible end-to-end media security in the network layer (Kent & Seo, 2005).

IPsec has two different communication modes: tunnel and transport mode. On one hand the transport mode is used to secure the IPv6 payload between communication endpoints. The IPv6 header is left intact and data is encrypted through the ESP (Encapsulating Security Payload) protocol which provides confidentiality and authenticity of the payload. This mechanism is perfectly suitable to secure confidential multimedia content over IPv6. When encryption can be omitted, but authentication is still required, AH (Authentication Header) can be used. The AH header is inserted between the IPv6 header and the payload. As both ESP and AH modify the original structure of the IPv6 packet, the value of the Next Header field is modified to reflect the changes in the payload so that it can be reassembled at the receiving end. On the other hand tunnel mode is used to protect traffic between a router and another communication node which could be either a host or a router. Unlike transport mode, in tunnel mode the entire IPv6 packet is encapsulated by ESP/AH and a new IPv6 header with different endpoint addresses is created. The tunneling mechanism along with the security features presented above is a powerful tool to create Virtual Private Networks (VPN) or secure packet delivery on unsecure links such as WLAN backbones.

Due to the rapid and widespread introduction of world-wide multi-play services, mobile IPTV started to grow significantly, fastly creating mobile video and TV services as an essential part of consumers' lives. Current data network infrastructure both on the wired and the wireless segments mainly uses unicast (one-to-one) communication for content delivery, but it is not effective for providing such bandwidth-hungry multimedia services. Contrarily, the multicast data communication paradigm (one-to-many media transmission) provides resource efficient solution for wired IPTV provision and also could help to handle the estimated amount of future mobile video and mobile IPTV traffic. However, the small address space of IPv4 makes hard to grant the necessary support and acceptance for universal multicast communication. Widely deployed multicast services can only be built on the enhanced features of IPv6 multicasting: the large address space and the use of scoped multicast addresses with sophisticated control mechanisms can serve as essential basis for resource-saving

multimedia applications with efficient traffic engineering capabilities (Pike, Russell, Krumm-Heller, & Sivaraman, 2007). This promising toolset of IPv6 multicasting has also been seriously considered for organic integration into 3G networks and beyond, as the Multimedia Broadcast Multicast Service (MBMS) concept was created by 3GPP to establish a framework for the point-to-multipoint downlink bearer service for IP multimedia in current and future mobile Internet architectures (3GPP TS 23.246, 2011).

The multicast traffic in IPv6 is managed by employing the Multicast Listener Discovery protocol (MLD) that aims to define which nodes are supposed to receive the multicast data in a network (Deering, Fenner, & Haberman, Multicast Listener Discovery (MLD) for IPv6, 1999). MLD controls the flow of traffic in a network using multicast queriers (network devices sending query messages to find out which nodes are members of a given multicast group) and hosts (receivers sending report messages to inform the querier of their multicast membership information). Querier and host devices both use MLD reports to join and leave different multicast groups and also to begin the reception of group media traffic.

Multicast routing protocols manage the information exchange between routers in order to construct and maintain multimedia distribution trees and also to forward multicast packets from the source to destination nodes. Because multicast addresses identify transmission sessions rather than specific physical destinations, multicast routing is more complex than in the unicast case. Protocol Independent Multicast - Sparse Mode (PIM-SM) is a good example for multicast routing. PIM-SM is an IPv6-compatible solution that can either use the underlying unicast routing information base or a separate multicast-capable routing information base to build unidirectional shared trees rooted at a special entity called the Rendezvous Point (RP) per group, and optionally creating shortest-path trees per source (Fenner, Handley, Holbrook, & Kouvelas, 2006).

There are several solutions to provide multicast services to mobile hosts such as results of (Sang-jo & Seak-jae, 2006) and (Zheng, 2006). However, the most elaborated and standardized solution is the Multimedia Broadcast Multicast Service (MBMS) which was created to overcome the shortcomings of the Cell Broadcast Service (CBS) of cellular networks and to introduce more sophisticated multicasting and broadcasting in the packet switched domain (3GPP TS 23.246, 2011). The core concept of MBMS is to save radio resources by sharing them between users belonging to the same multicast group. The main 3G (and beyond) packet switched elements and the radio access nodes and controllers should be all MBMS enabled to offer MBMS services while user terminals also should support MBMS, and also a new functional entity called the BM-SC (Broadcast/Multicast Service Center) should be available. BM-SC serves as an ingress point for multicast content providers, and manages and sets up the MBMS transport services operator's network. The IPv6-aware standard family of MBMS extends the 3G/4G mobile network to enable any multimedia traffic that uses multicast or broadcast addressing scheme to reach mobile subscribers in a resource efficient and well scalable way.

IPV6 MOBILITY MANAGEMENT FOR ON-THE-MOVE MEDIA APPLICATIONS

All the above mentioned features are more or less achievable in the presence of IPv4 as well. Basically, IPv6 is a conceptual copy of the IPv4 protocol, with almost all the functionalities existing in IPv4. The real difference lies in the extended address space, the integrity of the standard and the advanced mobility support. When designing IPv6, the authors were aware of the existing functionalities of IPv4: they tried to integrate all functionalities (including mobility management capabilities) of IPv4 extensions into the basic IPv6 standards. Thus, the IPv6 standards are more complete, and thus IPv6-based mobility management took the leading role in mobility-oriented research and development. Its importance is even more specific in future wireless systems: as access networks are becoming more heterogeneous, the issue of vertical handovers, where a mobile node has to change its point of connection to the Internet among different access media types, must be solved. Also offloading techniques are becoming increasingly popular in the cellular world (3GPP TR 23.829, Sept. 2010), allowing mobile operators to perform various policy enforcements without affecting user experience and creating even more complicated mobility scenarios to be handled. Therefore the role of the mobile IPv6 technologies is crucial: without efficient management of different mobility events in evolved mobile scenarios and use cases it will not be possible to provide multimedia services to mobile users in future Internet architectures with reasonable QoS and QoE (Quality of Experience).

MOBILE IPV6 (MIPV6)

The Mobile IPv6 protocol (Perkins, Johnson, & Arkko, 2011) together with its extensions provide solution for all the above problems allowing hosts to have a topology independent unique IPv6 address that is independent from its point of attachment to the Internet. Using a temporary address – called Care-of Address (CoA) – taken from the visited network the Mobile Node (MN) establishes a bidirectional tunnel to a known central entity, known as the Home Agent (HA), allowing uninterrupted IPv6 communication in diverse mobility scenarios.

Fig. 1 shows the general architecture and main protocol operation of Mobile IPv6 networks, where each MN has a globally unique static Home Address (HoA) independent from its actual point of attachment to the Internet. When a MN is visiting a foreign network, it registers a binding at the Home Agent. With the binding containing the actual CoA taken from the remote access network and the HoA of the MN, the Home Agent always knows the location of the Mobile Node. The binding is registered and updated in the Binding Update (BU) control message sent by the MN, and acknowledged by the HA with the Binding Acknowledgement (BA) message. As long as the binding is kept up-to-date, the bidirectional IPv6-in-IPv6 tunnel is kept alive between the MN and the HA. The tunnel, similarly to a VPN, uses the actual CoA as source address and the address of the HA as destination. The inner IPv6 header, containing the payload is addressed by the Home Address the address of the Correspondent Node (CN). The job of the Home Agent is to encapsulate and decapsulate the packets belonging to the Mobile Node by impersonating presence of the Mobile Node on the Home Network.

Because of the above operation, a usually sub-optimal route containing the HA inside the MN-CN path will be used for communication. This so called triangular routing phenomenon introduces additional delays and unwanted overhead, but it can be eliminated by directly registering the MN at the CN with a Binding Update/Acknowledgement message pair. Of course this needs the CN to have MIPv6 capabilities, and also to employ some additional security mechanisms: in order to provide the CN with some reasonable assurance that the MN is in fact addressable at its stated CoA as well as at its HoA, the return routability procedure (HoTI-CoTI-HoT-CoT) must be executed before the BU/BA sequence (see Fig. 1).

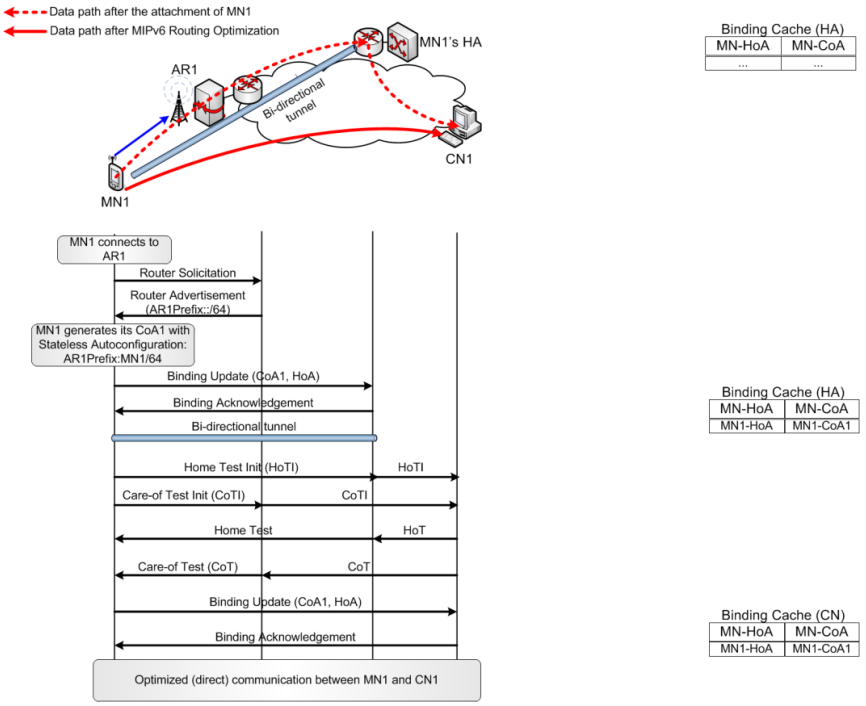

Figure 1. Basics and architecture of Mobile IPv6

While Mobile IPv6 with its security extensions is a viable solution to provide always-on connectivity for nodes on the move, as large part of the Internet still uses IPv4, content delivery would not be

efficient without an IPv4-IPv6 transition mechanism. Dual-Stack Mobile IPv6 (DSMIPv6) (Soliman H., 2009) is one of the techniques which extend the functionality of MIPv6 to the presence of IPv4 access networks, however due to its complexity it is not widely used.

NETWORK MOBILITY BASIC SUPPORT (NEMO BS)

In order to support persistent connection of moving networks (e.g., trains with wireless hosts of passengers inside the carriages) to the Internet, the NEMO Basic Support protocol (Devarapalli, Wakikawa, Petrescu, & Thubert, 2005) – as an extension of MIPv6 – was designed and approved as an RFC by the IETF. The main goal of this scheme is to preserve ongoing internal and external communication sessions of nodes attached to a moving network during the network's movement: using this protocol the mobile node becomes a mobile router, providing transparent, legacy network access to its Mobile Network Nodes, while performing mobility actions as a mobile node. Network Mobility is commonly used in Intelligent Transport Systems (ITS), where multiple mobile nodes move at the same time.

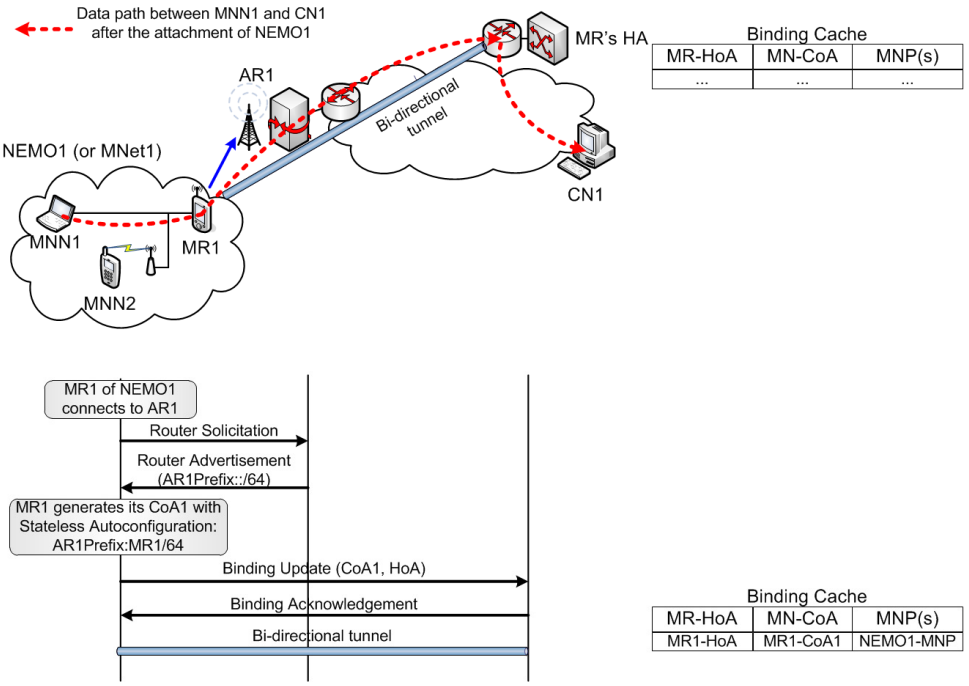

Figure 2. Overview of NEMO BS

In NEMO BS terminology a moving network (MNet) is defined as an entity handling several inside nodes and/or subnetworks as a whole whose Internet point of attachment changes in time. A moving network consists of one or more Mobile Routers (MR) and several Mobile Network Nodes (MNN). MR is the node that manages the tasks of internal routing within the moving network and connects the whole MNet to the external infrastructure. MNNs can either be fixed or mobile. The architecture of NEMO BS (see Fig. 2) makes possible that only the MR must be involved in the handover operations on behalf of the whole moving structure. Data traffic between MNNs and Correspondent Nodes (CNs) is managed by establishing bidirectional tunnels between the HA and the MR of the moving network to which the MNNs belong. The solution used by NEMO BS is similar to Mobile IPv6 but without routing optimization: when a MR leaves its home link, it configures a Care of Address (CoA) in the visited network and registers this CoA with its HA using the binding procedure. However, the Binding Update (BU) message in NEMO BS is quite different from that in MIPv6. While a BU message in MIPv6 contains the Care-of and the Home Address (HoA) of a mobile node, till a BU of an MR contains additional information: the IP subnet prefix or prefixes of the moving network. These so called Mobile Network Prefixes (MNPs) in the Binding Updates instruct the Home Agent to create a binding cache entry linking the MNPs to the MR's Care-of Address.

After a successful registration, the HA intercepts and forwards packets destined not only to the MR, but also to any MNNs that have acquired an address from one of the Mobile Network prefixes of the MR. When the moving network changes its actual network point of attachment, only the MR configures new CoA and sends Binding Update (containing the MNPs) to the HA. Observing that the MNNs don't need to configure and bind new CoA as long as they are inside the moving network, signaling overhead can be reduced but it has its cost. A CN usually sends packets to a mobile node using the MN's HoA. Since the Home Addresses of the MNNs inside a moving network are associated with the MNPs registered in the HAs, the HA of the network's MR intercepts all the packets addressed to MNNs and forwards them towards the MR's CoA. The MR decapsulates the packets destined to MNNs and forwards them on its appropriate ingress interfaces. Packets originated from inside the moving network will follow the same routes but in the reverse direction. It is obvious that the big number of encapsulations cause header overhead, and the fact that all the HAs should be involved in the communication path results using traffic routes far from the optimal ones. In order to deal with these problems route optimization schemes like (Kafle, Kamioka, & Yamada, 2006) (Calderón, Bernardos, Bagnulo, Soto, & Oliva, 2006) are investigated within the research community.

Based on the above procedures and extensions of MIPv6, a practical and complete IPv6-based network mobility support can be achieved without the need of changing the addresses of MNNs. NEMO routing optimization techniques further improve the solution, such enabling the roaming of whole networks and providing transparent provision of Internet access in public transportation systems for passengers, in the widest scale of ITS scenarios (e.g., road safety on the move entertainment) or even in personal area networks (PAN) where various electronic devices carried by people (like tablets, digital cameras, e-health sensors, etc.) would connect to the Internet through a smartphone playing the role of the mobile router.

MULTIPLE CARE-OF ADDRESSES REGISTRATION AND FLOW BINDINGS

While the aforementioned protocols only allow the connection to one access network at a time, redundancy, handover delays and offloading techniques cannot be adopted in any of the mobility scenarios. To address this shortfall, a new extension called Multiple Care-of Addresses Registration (MCoA) (Wakikawa, 2009) was introduced to the Mobile IPv6 protocol family. By utilizing that mobile nodes or routers can connect to multiple access networks simultaneously, it is now possible to enhance handover latency, network redundancy and perform policy based routing.

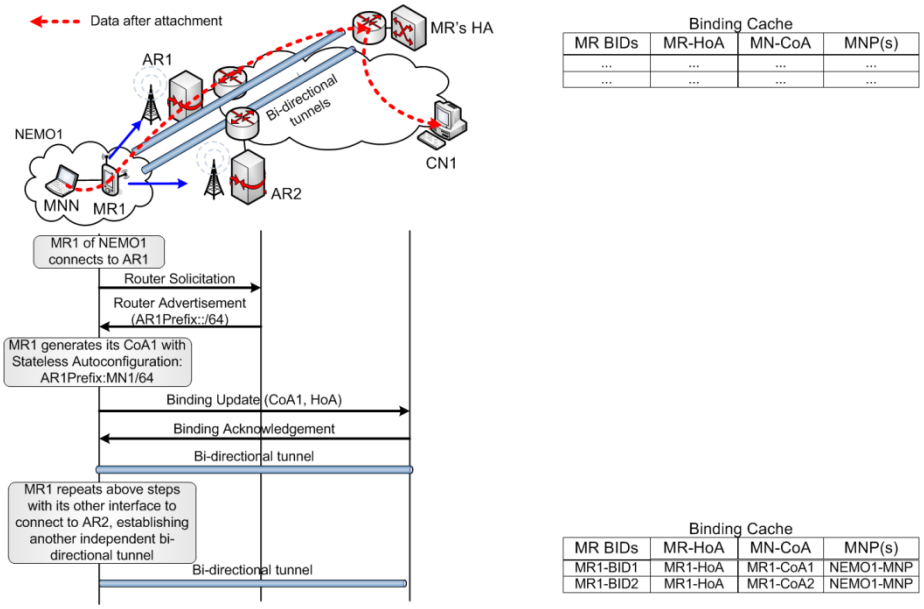

Figure 3. NEMO multihoming with MCoA

Fig. 3 depicts a scenario, where the Mobile Router has two external interfaces, where each interface is connected to an access network with a CoA, and through each CoA a Mobile IPv6 tunnel is created to the Home Agent. While with NEMO BS, identifying a binding was enough using the CoA and the

HoA, it is no longer the case with NEMO MCoA as each mobility tunnel endpoint uses the same Home Address on the MR. Using network layer information, the MR can no longer perform an exact routing decision to select an individual tunnel. To solve this issue another identifier, known as Binding Identifier (BID) was introduced to identify the network interface over which the tunnel is established. As the BID is sent to the HA in the BU signaling message, the HA can differentiate between tunnels originating from the same MR. To identify and route packets toward the desired tunnel, policy routing must be used, which allows fine grained diversification among data packets and streams based on network layer and upper layer information. To avoid asymmetric routing where packets belonging to the same packet flow are routed on different tunnels, a flow binding mechanism has to be implemented. Using flow binding control messages, the MR registers flow descriptor and BID pairs at the Home Agent, so the HA would properly know which tunnel to use when it forwards packets of the data flow back to the mobile node (Tsirtsis, Soliman, Montavont, Giaretta, & Kuladinithi, 2011).
Using the above introduced multihoming solution, routing of individual media streams can be easily solved, enhancing the experience for not only moving, but stationary mobile nodes as the presence of multiple egress interfaces makes content delivery more reliable and robust.

PROXY MOBILE IPV6 (PMIPV6)

Although Mobile IPv6 works logically and theoretically allows roaming to devices in wireless networks, in real mobile environments the performance of this protocol is not always satisfactory since the handover procedure can cause significant delay. As MIPv6 is a host-based solution it requires implementation of the protocol mechanisms in the kernel of the mobile (or even fixed) devices and this raises some serious problems, therefore the deployment of MIPv6 in new devices could be very slow. The implementation of MIPv6 in end user device kernels also provides an additional interface for security vulnerability.
To avoid these problems IETF created a working group called Network-based Localized Mobility Management (NetLMM) to define network-based mobility protocols instead of host-based ones. A network-based protocol can manage MN handovers inside the mobile network core without involving or requiring anything from the MN itself. The main idea is to let the MN keep its IPv6 address during movements across multiple access routers and make this roaming transparent to the IP layer and above.

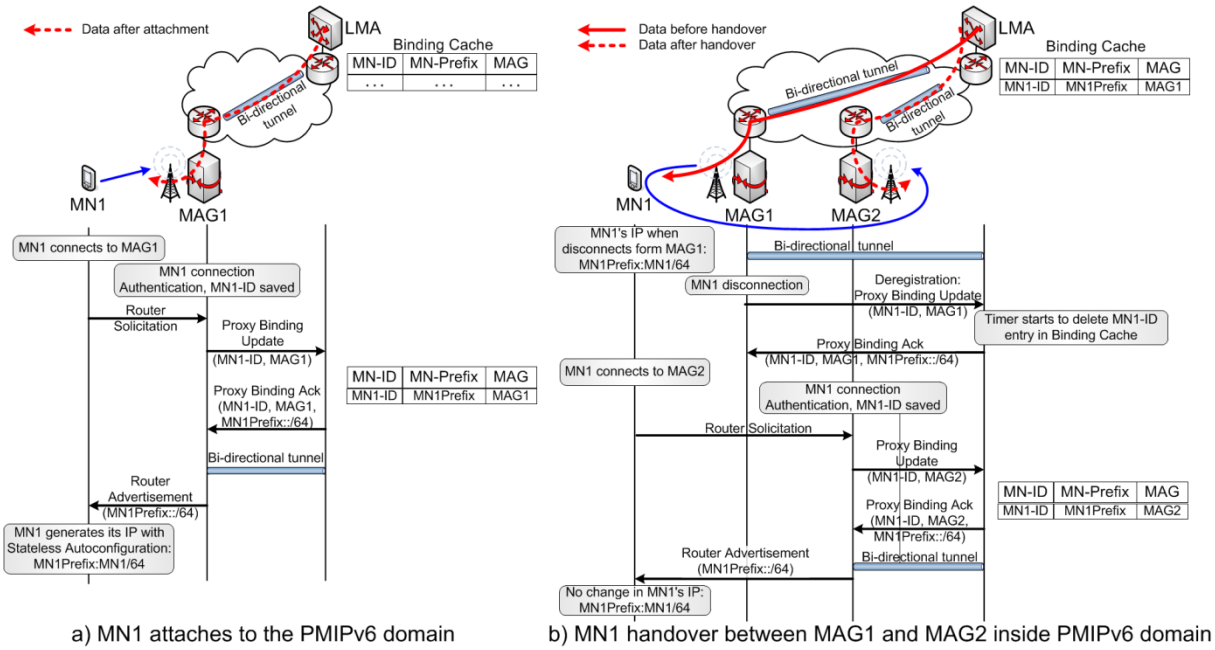

Figure 4. PMIPv6 architecture and operation

The proposed solution is Proxy Mobile IPv6 (PMIPv6) (Gundavelli, Leung, Devarapalli, Chowdhury, & Patil, 2008) and this name came from using proxy-like nodes to manage handovers on behalf of the

mobile entities. The main advantage of PMIPv6 is that it needs no additional modifications on the MN (kernel and user space software), therefore it is transparent to the user devices. It is an access technology independent solution, so it can be used with WLAN, WiMAX, 3G UMTS, LTE, LTE-A or any other technology in the future. Provides fast handovers according to its localized nature, which means PMIPv6 has a well-defined domain area (Local Mobility Domain, LMD) where exchanging signaling messages is quite fast. PMIPv6 grants the same IP address to the MN during movement so it also provides session continuity within a single access technology domain, which means user space applications do not have to build up new sessions after a handover because the IP address and the transport protocol ports remain the same.
There are two new nodes defined in PMIPv6: the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG). LMA acts as a Home Agent (HA) in MIPv6, it maintains a set of routes to every MN in the LMD and all the traffic from and to the MNs go through on this node. The LMA stores the Home Network Prefix (HNP) for every MN in its Binding Cache (BC) which is soft-state table and needs to be updated periodically. A MAG is the first hop router (access router) of the MNs attached to it and this node performs the mobility signaling on behalf of these MNs towards the LMA. The signaling messages are Proxy Binding Update and Proxy Binding Acknowledgement, which are the modifications of the original BU and BA messages from MIPv6.
According MIPv6, in PMIPv6 we can also find a bi-directional tunnels, but not between the MN and the LMA (HA) but between the MAG and the LMA. For the same reason there is a Proxy Care-of Address (Proxy CoA) for every MAG and this is the end point address of the tunnel towards the LMA. The architecture and main scenarios of PMIPv6 are depicted in Fig. 4 which also emphasizes that the whole LMD seems to be a virtual link from the viewpoint of the MN, as roaming between the LMD's MAGs the MNs IPv6 address (and the opened sessions) remains the same. The first part of Fig. 4 (a) represents the signaling flow when a MN arrives in the LMD and attaches itself to the closest MAG. The second part (b) shows the signaling flow during a handover inside the PMIPv6 domain.
This operator centric solution is a promising mobility management candidate for future mobile systems: 3GPP adopted the scheme for beyond 3G architectures.

HIERARCHICAL MOBILE IPV6 (HMIPV6)

HMIPv6 (Soliman, Castelluccia, Elmalki, & Bellier, 2008) is an extension to MIPv6 with the straight purpose to decrease handover delay and make MN movements in the same domain transparent for the Correspondent Nodes (CN) and the HA by using micro-mobility. The main properties of this protocol are that some elemental MIPv6 signaling messages were modified (extended) to be able to be used in HMIPv6 architecture as well and this solution is independent from the underlying access layer technologies.
HMIPv6 introduces a new network node called Mobility Anchor Point (MAP) which has the functionality of a HA, so it can store bindings between two IPv6 addresses. Two different types of addresses are used by the HMIPv6 protocol: the Regional Care-of Address (RCoA) and the On-link Care-of Address (LCoA). The second one, LCoA, has the same functionality as the CoA in MIPv6 and the name LCoA is only to distinguish it from RCoA. The RCoA is an address from the subnet of the MAP.
After a HMIPv6-aware MN arrives to a domain, it generates an address for itself from the Router Advertisement of its default router and this will be the LCoA. The RA also contains information about MAPs in the domain. If it has one or more MAPs, the MN can decide whether to use HMIPv6 or just simply MIPv6 (with LCoA). When HMIPv6 is chosen the MN asks an RCoA from the MAP and then sends a local BU message with the address pair of LCoA and RCoA. The MAP processes the BU and stores the address pair in its Binding Cache and from this point it acts like a HA for the RCoA address: intercept packages sent to this address and sends it to the actual position of the MN. Then a Binding Acknowledgement is sent back to the MN and this initiates a build-up of a tunnel between the MAP and the MN. After this the MN sends a BU to its real HA with the RCoA in the CoA field.

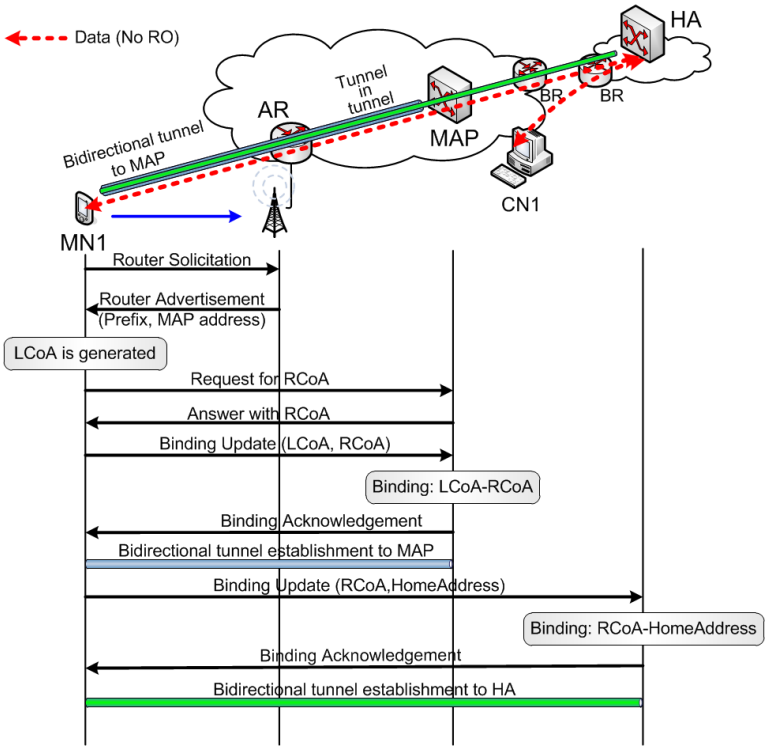

Figure 5. HMIPv6 architecture and connection establishment

This means that within the domain managed by the chosen MAP the handovers are handled locally, with no need to send signaling messages to the maybe far away HA, and the movement of the MN is transparent for communication partners outside of the domain. Fig. 5 shows the message flowchart of the scenario when a MN arrives in a HMIPv6 domain and establishes connection to its HA. Moving from one AR to another in the same MAP domain the MN has to send a BU message only to the MAP containing the MN's new LCoA and its RCoA.

MOBILE IPV6 FAST HANDOVERS (FMIPV6)

FMIPv6 (Koodli, 2009) is also an extension to MIPv6 and independent from access layer protocols. The aim of FMIPv6 (Fig. 6.) is to fasten up handovers and decrease the amount of lost packets when the MN is moving from one AR to another.

The first idea is to know the local environment in order to predict the next AR the MN will connect to during its movement and make it possible to get a new IPv6 address prior to connecting to the New AR (NAR). The second idea of this scheme is to use the Previous AR (PAR) to forward the packets addressed to the MN towards the NAR and by this way reduce the number of lost packets during the handover.

FMIPv6 defines a new message called Router Solicitation for Proxy Advertisement (RtSolPr) which is sent by the MN to its AR (PAR) to get information about adjacent ARs. The PAR answers with a Proxy Router Advertisement (PrRtAdv) message. The MN chooses the appropriate NAR from the list and generates a New CoA (NCoA) according to the prefix used by in the subnet of the NAR. Based on the timing of the Fast BU (FBU) message there two scenarios for the fast handover: the predictive and the reactive one.

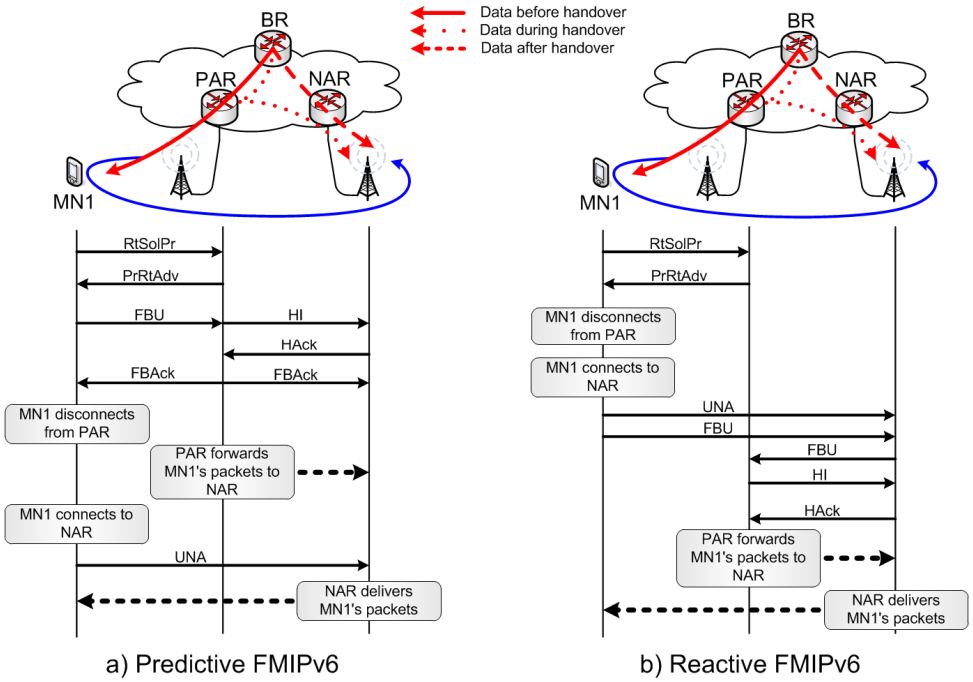

Figure 6. FMIPv6 architecture and handover modes

The predictive method requires from the MN to send the FBU message from its previous network to the PAR (the actual one) and wait for the Fast BAck (FBAck) there. The PAR sends a Handover Initiate (HI) message to the NAR which acknowledges the handover by a Handover Ack (HAck) message. The PAR generates and sends the FBAck message to the MN when it receives the HAck from the NAR. In parallel it starts forwarding the MN's packets to the new network. When the MN arrives to the new network, it sends an Unsolicited Neighbor Advertisement (UNA) to its NAR and from then a MN can immediately receive its packets from the CNs.

The reactive method does not require sending the FBU from the previous network, right after receiving the PrRtAdv the MN can attach itself to the NAR by sending an UNA message to it. Then the FBU is sent from the new network to the PAR which initializes the handover with the method mentioned above except that the FBAck message is also forwarded to the new network of the MN. In both cases during the handover, packets are forwarded from PAR to the MN through NAR. For performance reasons HMIPv6 and FMIPv6 are often used together (Lee & Ahn, 2006), (Pérez-Costa, Schmitz, Hartenstein, & Liebsch, 2002), (Pérez-Costa, Torrent-Moreno, & Hartenstein, A Performance Comparison of Mobile IPv6, Hierarchical Mobile IPv6, Fast Handovers for Mobile IPv6 and their Combination, 2003) .

GNSS AIDED PREDICTIVE HANDOVER MANAGEMENT FOR MULTIHOMED NEMO CONFIGURATIONS

The colorful palette of mobility solutions for IPv6 proves that transparent mobility in the network layer is a powerful tool for sensitive application protocols. However, lower layer protocols are usually not considered when performance of such solutions is evaluated. The authors developed a method which combines the benefits of MCoA with a new prediction-based cross-layer management entity which allows mobility solutions to operate using only the best available access networks (Kovács, Bokor, & Jeney, 2011).

Predictive handover management is based on the following simple idea: as the node/network moves along a path, it records all access network related data in a database together with the geographical location information. The next time the node/network moves along the same path, based on the geographical information and speed vector, the stored information can be used to predict and prepare handovers before the actual availability of the networks based on calculated weighted performance parameters.

When multiple interfaces are used, the above introduced MCoA and Flow Bindings solutions can be of use. The handover preparation consists of the following components.
Flow Bindings are applied to direct the whole traffic of the MR through one active egress interface. Although the benefits of redundancy are lost, we gain the possibility to use inactive interfaces for handover preparation: selecting appropriate access network, performing lower layer connections and acquiring new IPv6 addresses. The scheme requires several interfaces for operation. Some of the interfaces are used for normal communication (they will be referred as "active"), the others are used for handover preparation (they are termed as "inactive"). The activation of a new interface must be accurately synchronized with the deactivation of the old one. The activation/deactivation procedure means simultaneous reallocation of NEMO tunnels. It can be implemented by properly scheduled flow binding policy control messages on the HA and the MR.

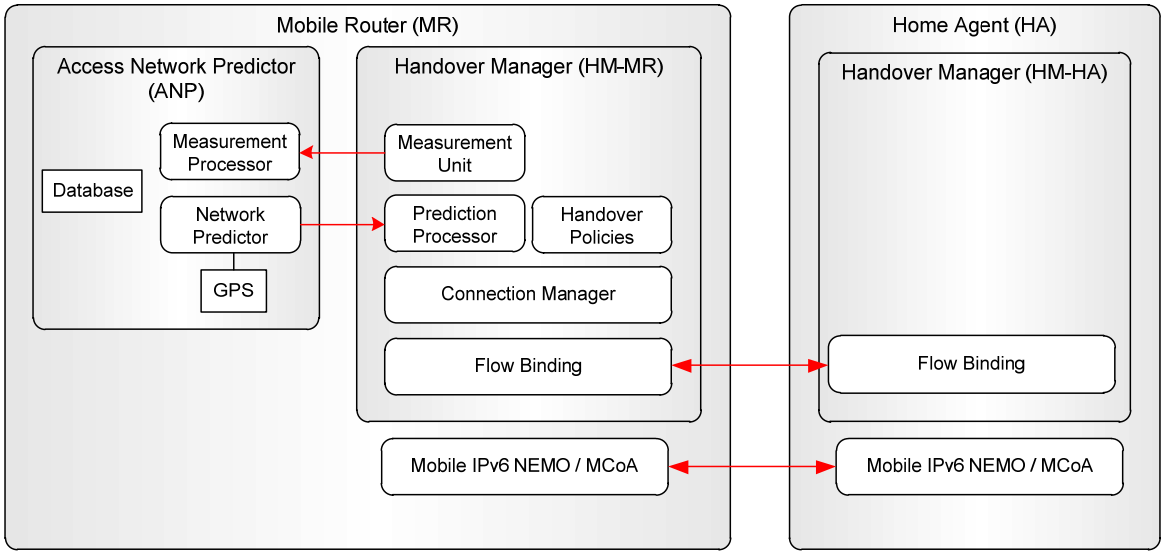

Figure 7. Prediction system architecture for GNSS aided predictive mobility management for IPv6

The proposed architecture of the proposed prediction system, as depicted on Fig. 7, has three main components: Access Network Predictor (ANP), Handover Manager Mobile Router (HM-MR) and Handover Manager Home Agent (HM-HA). The ANP is responsible for maintaining a database containing information of access networks, and sending periodic prediction messages to the HM-MR module based on the current velocity vector and the contents of the database associated with the predicted geographical location. The database is kept up-to-date by the Measurement Unit residing in the Handover Manager, which passively monitors the available access networks via one of its passive interfaces, periodically sending network availability and performance indicators such as SNR and IPv6 prefix to the Access Network Predictor. Based on the predictions received from the ANP, the Connection Manager may decide that the currently active access network will no longer be the best available network in the predicted timeframe. When the HM decides to perform a handover, in order to use the benefits of MCoA, the following steps are executed. Using one of the inactive interfaces the HM connects to the new access network and establishes a new Mobile IPv6 binding. At this stage, the current and new access networks are both connected and Mobility Tunnels are established between the MR and the HA. Handing over to the new access network is entirely based on flow-binding, which in this case means that all flows are moved from one interface to another. To avoid asymmetric routing, the MA and HA has to modify their bindings simultaneously. The schedule is communicated by the Flow Binding modules as an extension of the Flow Binding protocol. When the changes of flow bindings are executed, the new interface is marked as active, while the rest of the communication interfaces are set to inactive mode. Different Handover Policies may have different effects on handover strategies. In our case, the implemented solution supports 3G and WLAN access networks, and WLAN is always preferred over 3G due to its advantageous bandwidth and latency properties.

When multiple WLAN networks are available, the network with the best Signal-to-noise ratio (SNR) is selected.

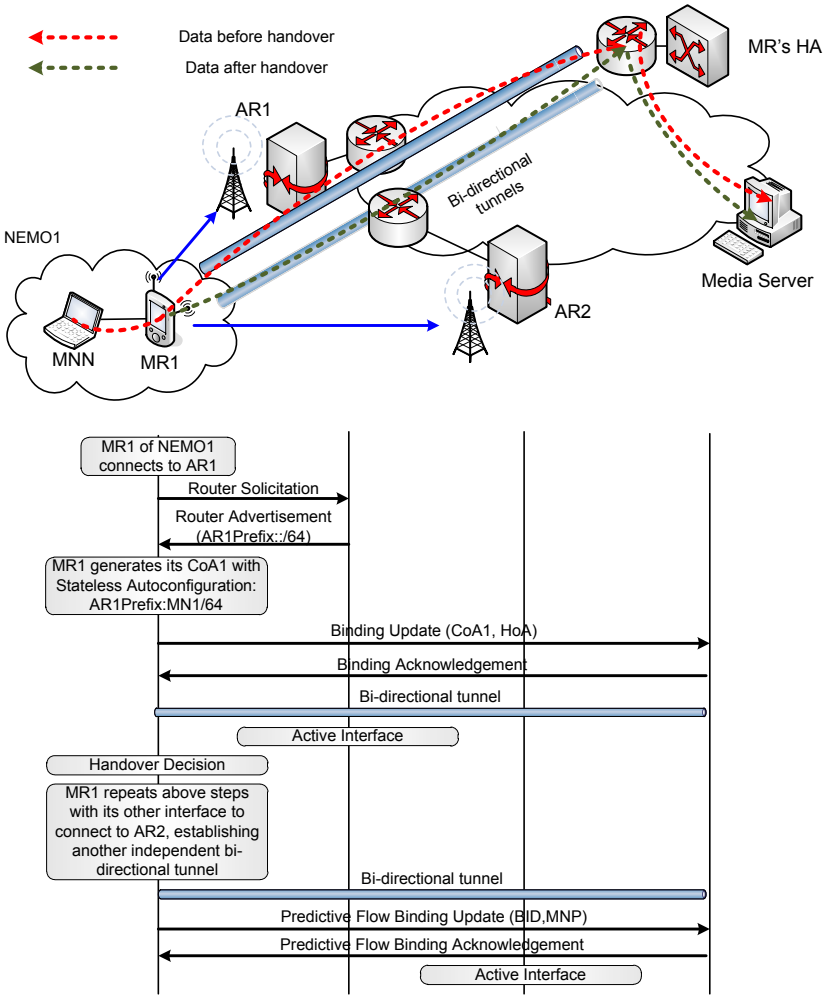

Figure 8. Predictive MCoA handover

A performance evaluation of the above introduced handover system is already published in (Kovács, Bokor, & Jeney, 2011), however, no application layer protocols were evaluated in the test setup. The results introduced in this chapter build on the same principles, extending the test environment with a media server as Correspondent Node, illustrated in Fig. 8. To simplify the testing methodology, the database used by the ANP is predefined and actual movement is simulated by a prerecorded path using the *gpsfake* utility. The quality of WLAN access networks is adjusted by the *txpower* property of the radios. The resulting handover points serve as heterogeneous set of use-cases to compare mobility solutions. The *tshark* utility was responsible for packet capture and analysis, while VLC was applied as media server. A sample 512 kbit/s CBR video stream was streamed over HTTP from the media server and playback experience was subjectively observed via buffering time periods and buffer underrun events, as the stream was played with VLC client on the Mobile Node.

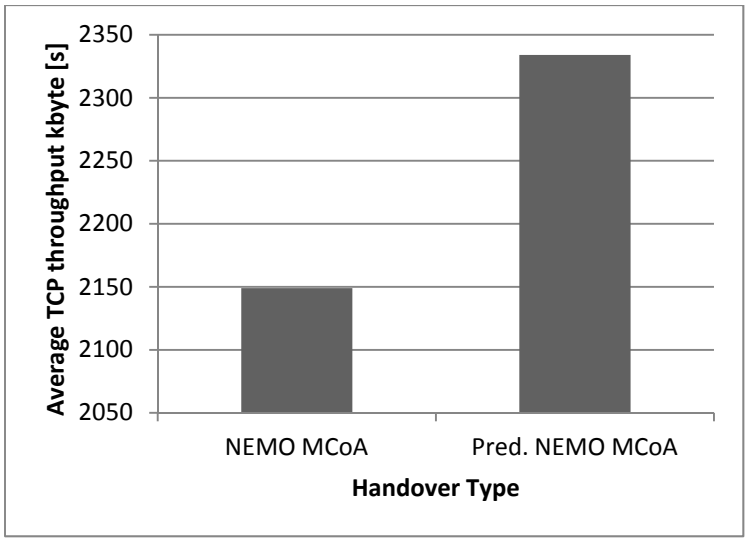

Figure 9. Average TCP throughput

Using MCoA handovers, the transport protocol performed within acceptable limits. This proved our assumptions, that when an inactive interface is used for connecting to the new network during a handover, the time duration of the actual handover is almost instantaneous. Fig. 9. explains, that although the mobile node spent time on the 3G medium as well, the average throughput had not degraded significantly. Allowing the node to use networks with poor performance properties, such as overloaded WLAN networks could be the bottleneck of this solution, as with low buffer sizes, the continuity of media playback could not be guaranteed. Comparing this solution to Predictive NEMO MCoA, the selection of the best available access network is not possible when multiple choices are available. Using prediction, low quality networks were avoided, boosting the average throughput of the transport protocol. While the difference in average throughput may not be significant when the overall path is evaluated, small disruptions in media streaming may occur due to sudden drops of available network bandwidth. Predicting the available access networks will allow the mobile node to choose the best available network and thereby maximize the user experience.

FUTURE RESEARCH DIRECTIONS

The currently standardized mobility management solutions introduced above rely on hierarchical and centralized architectures which employ anchor nodes for mobility signaling and user traffic forwarding. In 3G UMTS and beyond, centralized and hierarchical mobility anchors are implemented by the entities in the architecture that handle traffic forwarding tasks using the apparatus of GPRS Tunneling Protocol (GTP). The similar centralization is noticeable when Mobile IPv6 is applied: the Home Agent administers mobile terminals' location information, and tunnels user traffic towards the mobile's current locations and vice versa. Up to this day, almost all the standardized enhancements and extensions of MIPv6 preserve the centralized and anchoring nature of the original scheme. This results in unscalable data and control plane with non-optimal routes, overhead and high end-to-end packet delay even in case of motionless users, centralized context maintenance and single point of failures. Anchor-based traffic forwarding and mobility management solutions also cause deployment issues for caching contents near the user. To solve all these problems and questions novel, distributed and dynamic mobility management (DMM) approaches must be envisaged, applicable to intra- and inter-technology mobility cases as well. The IETF DMM Working Group (formally known as the Mobility EXTensions for IPv6 WG) controls the work within this area.

The basic idea of this hot research topic is that anchor nodes and mobility management functions of wireless and mobile systems could be distributed to multiple locations in different network segments, hence mobile nodes located in any of these locations could be served by a close entity.

A first alternative for achieving DMM is core-level distribution. In this case mobility anchors are topologically distributed and cover specific geographical area but still remain in the core network. A good example is the Global HA to HA protocol (Thubert, Wakikawa, & Devarapalli, 2006), which

extends MIP and NEMO in order to remove their link layer dependencies on the Home Link and distribute the Home Agents in Layer 3, at the scale of the Internet.

A second alternative for DMM solutions is when mobility functions and anchors are distributed in the access part of the network. For example in case of pico- and femto cellular access schemes (FemtoForum, 2010) it could be very effective to introduce Layer 3 capability in access nodes to handle IP mobility management and to provide higher level intervention and even cross-layer optimization mechanisms. A good proposal here is the concept of UMTS Base Station Router (BSR) (Bauer, Bosch, Khrais, Samuel, & Schefczik, 2007) which realizes an access-level mobility management distribution technique where a special network element called BSR is used to build flat cellular systems. BSR merges the all the crucial architecture building blocks and functions into a single element: while a common 3G network is built from a plethora of network nodes and is maintained in a hierarchical and centralized fashion, the BSR integrates all radio access and core functionalities. Furthermore, the BSR can be considered a special wireless edge router that bridges between mobile/wireless and IP communication. In order to achieve this, mobility support in the BSR is handled at three layers: RF channel mobility, Layer 2 anchor mobility, and Layer 3 IP(v6) mobility.

A third type of possible distribution of mobility management functions is the so-called host-level or peer-to-peer DMM where once the correspondent node is found, communicating peers can directly exchange IP packets. In order to find the correspondent node, a special information server is required in the network, which can also be centralized or distributed. A good example for host-level schemes in the IP layer is MIPv6 which is able to bypass the user plane anchor (i.e., Home Agent) due to its route optimization mechanism, therefore providing a host-to-host communication method (Arkko, Vogt, & Haddad, 2007).

The three above DMM approaches can be applied together in an integrated manner for more flexibility and enhanced performance. PMIPv6 extension proposals like (Bernardos, Oliva, Giust, Melia, & Costa, 2012) are going on this path.

Another emerging area of IPv6 mobile multimedia delivery researches is the flow mobility. There are cases in multihoming Mobile IPv6 environments when flow mobility (or flow binding) is initiated by a central entity, such as the always available Home Agent. Operations like network-controlled flow binding revoking, moving, or provisioning are equally possible with this mechanism; making it possible to revoke an existing flow binding in case of an error, or move a flow from one interface to another on the MN side, or simply provide default flow settings for newly connected Mobile Nodes. The approach is not mutually exclusive with the MN initiated flow binding described in RFC 6089 (Tsirtsis, Soliman, Montavont, Giaretta, & Kuladinithi, 2011), it merely extends the mobility features it provides, meaning that flow bindings are not always initiated by the HA. There are drafts like (Yokota, Kim, Sarikaya, & Xia, 2011) in which authors introduce a new Mobility Header and signaling messages based on the flow binding protocol implemented in RFC 6089. Also PMIPv6 protocol extensions exist for this purpose (Bernardos C., 2012). Possible application use cases of HA Initiated Flow Bindings may be default flow binding provisioning, traffic offloading and flow binding revocation. Default flow binding provisioning is used for example in an environment where a central entity wants to force Service Level Agreements (SLA) to a customer, e.g., forcing multimedia traffic through WLAN while allowing 3G access for HTTP traffic. The traffic offloading technique makes it possible to move certain data flows from one interface to another, e.g., in case of increasing traffic load in 3G segment move video streams to the WLAN segment. Policies can be much complex based on the fact that the core network entities know about their actual traffic conditions. Flow binding revocation is useful when due to an administrative decision; a certain flow binding is no longer valid for the MN.

The last group of research directions to be introduced here is about media handover optimization by applying cross-layer techniques. Several different mobility management schemes exist in the literature but their optimization for heterogeneous access architectures just have been started. 802.21 Media Independent Handovers (MIH) (IEEE, 2009), and Access Network Discovery and Selection Function (ANDSF) (3GPP TS 23.402, June, 2011) are emerging methods for proactive handover control in heterogeneous architectures, but their ways of application in mobile environments and synthesis with different mobility execution mechanisms or with higher layer functions has not yet defined precisely. Integration of 802.21 MIH, and ANDSF and similar standards with existing mobility management schemes (e.g., Dual-Stack Mobile IP, Proxy Mobile IPv6) in order to reduce or even totally eliminate

deteriorations during mobility events are still hot topics. Also evaluation of mobility management schemes strongly relying on multiple existing host interfaces (i.e., multihoming) and integrate them with handover preparation/prediction mechanisms and cross-layer information provision in order optimize access to heterogeneous access architectures, benefit from overlapping coverages and also to build up a strong interworking between applications and handover procedures (e.g., to prepare a real-time mobile media flow for a handover event by proactively setting media codec parameters at the sender side) is an important research activity nowadays.

CONCLUSION

In this chapter we tried to give a comprehensive overview of the complex relation system between IPv6 and the multimedia driven future mobile Internet, to highlight how the IPv6 standard family emerges with its suitability and applicability for mobile multimedia applications and services, and to introduce how IPv6 can serve as the main cornerstone for mobile architectures. The chapter introduced a new method to improve the feasibility of Mobile IPv6 for multimedia content delivery. The discussion of the above areas together with the review of the most current research efforts hopefully guides the readers from the basics of IPv6 towards the most complex features of the protocol and power to build a novel Internet architecture for future multimedia-centric mobile communications.

ACKNOWLEDGEMENT

The research leading to these results has received funding from the European Union's Seventh Framework Programme ([FP7/2007-2013]) under grant agreement n° 288502 (CONCERTO), and partly by the FP7 project ITSSv6. The authors would like to thank all participants and contributors who were involved in the work.

REFERENCES

3GPP TR 23.829. (Sept. 2010). *Local IP Access and Selected IP Traffic Offload, Release 10, V1.3.0.* 3GPP Technical Report.

3GPP TS 23.246. (2011. June). Multimedia Broadcast/Multicast Service (MBMS) Architecture and functional description. *3GPP Technical Specification*. Release 10, V10.1.0.

3GPP TS 23.402. (June, 2011). *Architecture enhancements for non-3GPP accesses, Release 10, V10.4.0.* 3GPP Technical Specification.

Arkko, J., Vogt, C., & Haddad, W. (2007. May). Enhanced Route Optimization for Mobile IPv6. *IETF RFC 4866*.

Bauer, M., Bosch, P., Khrais, N., Samuel, L. G., & Schefczik, P. (2007). The UMTS base station router. *Bell Labs Tech. Journal, I.: Wireless Network Technology, 11*(4), 93–111.

Bernardos, C. (2012. March). Proxy Mobile IPv6 Extensions to Support Flow Mobility. *IETF I-D*. draft-ietf-netext-pmipv6-flowmob-03.

Bernardos, C., Oliva, A. d., Giust, F., Melia, T., & Costa, R. (2012. March). A PMIPv6-based solution for Distributed Mobility Management. *IETF I-D*. draft-bernardos-dmm-pmip-01.

Bokor, L., Faigl, Z., & Imre, S. (2011). Flat Architectures: Towards Scalable Future Internet Mobility. *LECTURE NOTES IN COMPUTER SCIENCE, 6656*, 35-50.

Calderón, M., Bernardos, C. J., Bagnulo, M., Soto, I., & Oliva, A. d. (2006. September). Design and Experimental Evaluation of a Route Optimization Solution for NEMO. *IEEE JSAC, 24*(9).

Cisco VNI. (Feb. 2011). *Global Mobile Data Traffic Forecast Update, 2010-2015.* Cisco.

Deering, S., & Hinden, R. (1998. December). Internet Protocol, Version 6 (IPv6) Specification. *IETF RFC 2460*.

Deering, S., Fenner, W., & Haberman, B. (1999. October). Multicast Listener Discovery (MLD) for IPv6. *IETF RFC 2710*.

Devarapalli, V., Wakikawa, R., Petrescu, A., & Thubert, P. (2005. January). Network Mobility (NEMO) Basic Support Protocol. *IETF RFC 3963*.

Dohler, M., Watteyne, T., & Alonso-Zárate, J. (Dec. 2010). Machine-to-Machine: An Emerging Communication Paradigm. *GlobeCom'10.*

Droms, R. (. (2003. July). Dynamic Host Configuration Protocol for IPv6 (DHCPv6). *IETF RFC 3315*.

FemtoForum. (2010. June). Femtocells – Natural Solution for Offload – a Femto Forum brief.

Fenner, B., Handley, M., Holbrook, H., & Kouvelas, I. (2006. August). Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised). *IETF RFC 4601*.

Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., & Patil, B. (2008. August). Proxy Mobile IPv6. *IETF RFC 5213*.

Hinden, R., & Deering, S. (2006. February). IP Version 6 Addressing Architecture. *IETF RFC 4291*.

IEEE. (2009. January). IEEE Standard for Local and metropolitan area networks- Part 21: Media Independent Handover. *IEEE Std 802.21-2008*.

Kafle, V. P., Kamioka, E., & Yamada, S. (2006. January). MoRaRo: Mobile Router-Assisted Route Optimization for Network Mobility (NEMO) Support. *IEICE Trans. Inf. & Syst, E89-D*(1).

Kent, S., & Seo, K. (2005. December). Security Architecture for the Internet Protocol. *IETF RFC 4301*.

Koodli, R. (. (2009. July). Mobile IPv6 Fast Handovers. *IETF RFC 5568*.

Kovács, J., Bokor, L., & Jeney, G. (2011). Performance Evaluation of GNSS Aided Predictive Multihomed NEMO Configurations. *ITST-2011: 2011 11th International Conference on ITS Telecommunications*, (old.: 293-298). St. Petersburg, Russia.

Lee, J., & Ahn, S. (2006. June). I-FHMIPv6: A Novel FMIPv6 and HMIPv6 Integration Mechanism. *IETF I-D*. draft-jaehwoon-mipshop-ifhmipv6-01.txt.

McCann, J., Deering, S., & Mogul, J. (1996. August). Path MTU Discovery for IP version 6. *IETF RFC 1981*.

Narten, T., Nordmark, E., Simpson, W., & Soliman, H. (2007. September). Neighbor Discovery for IP version 6 (IPv6). *IETF RFC 4861*.

NetLMM, I. (dátum nélk.). *Network-based Localized Mobility Management (NetLMM) WG homepage*. Letöltés dátuma: 2012. March 27, forrás: http://datatracker.ietf.org/wg/netlmm/charter/

Pérez-Costa, X., Schmitz, R., Hartenstein, H., & Liebsch, M. (2002). A MIPv6, FMIPv6 and HMIPv6 Handover Latency Study: Analytical Approach. *IST Mobile & Wireless Telecommunications Summit (IST Summit)*. Thessaloniki, Greece.

Pérez-Costa, X., Torrent-Moreno, M., & Hartenstein, H. (2003). A Performance Comparison of Mobile IPv6, Hierarchical Mobile IPv6, Fast Handovers for Mobile IPv6 and their Combination. *ACM SIGMOBILE Mobile Computing and Communications Review (MC2R), 7*(4).

Perkins, C., Johnson, D., & Arkko, J. (2011. July). Mobility Support in IPv6. *IETF RFC 6275*.

Pike, T., Russell, C., Krumm-Heller, A., & Sivaraman, V. (2007). IPv6 and multicast filtering for high-performance multimedia application. *Australasian Telecommunication Networks and Applications Conference (ATNAC'07)*, (old.: 146-150).

Ping, G., & Desheng, F. (2010). The Discussions on Implementing QoS for IPv6. *International Conference on Multimedia Technology (ICMT)*, (old.: 1-4).

Rajahalme, J., Conta, A., Carpenter, B., & Deering, S. (2004. March). IPv6 Flow Label Specification. *IETF RFC 3697*.

Sang-jo, Y., & Seak-jae, S. (2006). Fast Handover Mechanism for Seamless Multicasting Services in Mobile IPv6 Wireless Networks. *Wireless Personal Communications, 42*(4), 509-526.

Soliman, H. (. (2009. June). Mobile IPv6 Support for Dual Stack Hosts and Routers. *IETF RFC 5555*.

Soliman, H., Castelluccia, C., Elmalki, K. E., & Bellier, L. (2008). Hierarchical Mobile IPv6 Mobility Management (HMIPv6). *IETF RFC 5380*.

Thomson, S., Narten, T., & Jinmei, T. (2007. September). IPv6 Stateless Address Autoconfiguration. *IETF RFC 4862*.

Thubert, P., Wakikawa, R., & Devarapalli, V. (2006. September). Global HA to HA protocol. *IETF I-D*. draft-thubert-nemo-global-haha-02.

Tsirtsis, G., Soliman, H., Montavont, N., Giaretta, G., & Kuladinithi, K. (2011. January). Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support. *IETF RFC 6089*.

UMTS Forum. (June, 2010). *Recognising the Promise of Mobile Broadband.* White Paper.

Wakikawa, R. e. (2009. October). Multiple Care-of Addresses Registration. *IETF RFC 5648*.

Yokota, H., Kim, D., Sarikaya, B., & Xia, F. (2011. December). Home Agent Initiated Flow Binding for Mobile IPv6. *IETF I-D*. draft-yokota-mext-ha-init-flow-binding-01.

Zheng, W. (2006). An Efficient Dynamic Multicast Protocol for Mobile IPv6 Networks. *31st IEEE Conference on Local Computer Networks*, (old.: 913 - 920).

Zhenhua, W., Qiong, S., Xiaohong, H., & Yan, M. (2010). IPv6 end-to-end QoS provision for heterogeneous networks using flow label. *3rd IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT)*, (old.: 130-137).

ADDITIONAL READING SECTION

Joseph Davies, J. (2003). *Understanding IPv6*. Microsoft Press.

Jo Groebel, Eli M. Noam, Valerie Feldmann, (2006). *Mobile Media – Content and Services for Wireless Communications*. Lawrence Erlbaum Associates, Inc., Publishers

Qing Li, Tatuya Jinmei, Keiichi Shima, (2007)**.** *IPv6 Advanced Protocols Implementation.* Morgan Kaufmann Publishers.

Gour Karmakar, Laurence S. Dooley, (2008). *Mobile Multimedia Communications: Concepts, Applications, and Challenges.* IGI Global.

Qing Li, Tatuya Jinmei, Keiichi Shima, (2009). *Mobile IPv6: Protocols and Implementation*. Elsevier Inc.

KEY TERMS & DEFINITIONS

IPv6: Internet Protocol version 6 (IPv6) is the next-generation Internet Protocol version designed to overcome the imperfections of IPv4. The main motivation for the redesign of IPv4 was the presumptive IPv4 address exhaustion. IPv6 was firstly introduced in December 1998 in RFC 2460. IPv6 is a conceptual copy of the IPv4 protocol with several modifications and extensions to the basic standard.

Multimedia: Multimedia is a noun or adjective, introducing a medium which describes the usage of different types of content forms usually in the same time. A content form (media) can be: written text, still images, animation, audio, video, and interactivity. Some examples for multimedia: social networking (who-is-who websites); online journals and news sites; a Blue-ray disc with video, audio, subtitles, and interactive menu points; or online gaming with other people.

Mobile multimedia: Mobile multimedia denotes different types of media content that are either accessed or created by employing portable devices like Smartphones with sound and video playback capabilities, microphone and camera for mobile content creation, and wireless Internet access for on-the-move content reception and transmission.

Mobility management in the networking layer: A mobility solution where the networking layer is responsible for handling various mobility scenarios, such as handover between different access network types, connecting to multiple access networks simultaneously, allowing the mobile node global reachability regardless of its current attachment to the Internet or the type of access medium in use.

Micromobility: If wireless networking domains are aggregated and a special protocol is responsible for the local mobility management of this group of domains in order to offer fast and seamless handover control over a limited geographical area, than we speak about micromobility, the aggregated group of domains is called micromobility domain, and the special control protocol is called micromobility protocol.

Network Mobility: A special mobility scenario, which arises when a router – connecting a network to the Internet dynamically – changes its point of attachment to the fixed infrastructure, thereby causing the accessibility of the entire network to be changed in relation to the fixed Internet topology.

Flow mobility: If a mobile user runs several applications (e.g. file downloading, voice communication, video streaming, e-mail) on a device with multiple interfaces and simultaneously available access networks, and the actual connection (i.e., out- and inbound interface) of each flow is handled independently according to QoS requirements and environmental parameters, than we are talking about per-application mobility.

Multicasting: Delivery of information to a group of destinations simultaneously using the most efficient strategy to deliver the messages over each link of the network only once, creating copies only when the links to the destinations split.

Network controlled media delivery: A special routing system, which utilizes the multihoming feature of Mobile IPv6 and the overall status of the network, allowing network operators to force network preferences to the host based on predefined routing policies and actual network status parameters.