Volume : 4 | Issue : 8 | Aug 2015 • ISSN No 2277 - 8179

Research Paper

Performance Problems and Security Limitations of Mobileipv6

Computer Science

KEYWORDS : Mobile IPv6, MIPv6 Security, Real-Time Communication, Fast Handover, Hierarchical Mobile IPv6, Multicast Mobility.

Sridevi Assistant Professor, Department of Computer Science,KarnatakUniversity,Dharwad.

Dr.Manjaiah.D.H Professor, Department of Computer Science, Mangalore University,Mangalore.

ABSTRACT

This research paper presents current mobility extensions of IPv6 as designed to create a real time compliant, secure mobile Internet. Starting from Mobile IPv6, the basic end-to-end mobility management protocol, it also discusses performance and security issues, as well as recent improvements to enhance mobility operations within the next generation Internet protocol.

1 Introduction

Mobile communication has established as a major driving force of industrial technology and service development, targeting at professional and consumer markets. Complementary, mobility in the Internet is one of the most challenging and demanded developments in computer networks today. All IP mobile real-time and group communication as needed for a global Voice or Videoconferencing service over IP (VoIP/VCoIP) – places an even stronger challenge on today's IP concepts and infrastructure. While the static architecture of the traditional Internet protocol only allows for tunnel-based mobility extensions, IPv6 unfolds its potentials by granting a route-optimal and transparent end-to-end mobility management on the network layer. Mobile IPv6 (MIPv6) [1], the base standard, self-consistently manages location transparency and handovers, i.e., changes of IP addresses, within the IP layer. It thus allows for the continuous operation of applications, while a user moves and the hosting device roams between networks. As stable MIPv6 implementations are around on today's major platforms, the question on actual user scenarios arises. At first, we may expect a use of MIPv6 for service-driven Home Address identification while away from home. 'User desktops' roaming between subnets may be likely to follow, as well as data services on 3GPP cellular phones. Some time and the deployment of currently developed improvements will be needed, until voice and video real-time traffic arrives at user's portables via mobile IP. However, it is the common believe that we all are heading at scenarios, where mobile VoIP is to become the real, predominant use case of IP. Synchronous real-time applications s. a. VoIP and VCoIP place new demands on the quality of IP mobility services: Packet loss, delay and delay variation / jitter in a constant bit rate scenario need careful simultaneous control. The MIPv6 base standard is not capable of operating handovers compliant to these constraints. End-to-end signalling performance may cause significant disruptions. At the same time security operations, which limit vulnerability to a common Internet standards, add additional overhead and delay to mobility operations. Thus further improvements to handover and security management are needed for a widely acceptable telephony service based on a next generation mobile Internet. As of today, the development, implementation and standardisation of enhanced MIPv6 protocols are well matured and may be widely available soon.

2 Mobile IPv6

Mobile IPv6 considers the scenario, where a Mobile Node (MN) moves between IP networks while continuously communicating with a Correspondent Node (CN). The IP interface of the MN keeps a permanent address derived from its home network, the Home Address (HoA), while it simultaneously configures changing addresses of visited networks, the Care-of Addresses (CoAs). The core objective of MIPv6 lies in transport layer transparency, i.e., the persistent presentation of HoA to the socket layer, while performing optimised routing using the topological correct CoA on the network layer. An additional component, the MIPv6 Home Agent (HA), preserves global addressability, while the mobile node is away from home. When at home, the MN uses its permanent HoA and communicates like a stationary IP device, with the addition of its (pre)configured Home Agent. When moving to a new IP network, i.e., after the discovery of a network change, the MN will use stateless or stateful auto configuration to add a new IP address valid in the visited network to its interface shown in figure 1. Having acquired a topological correct CoA, the MN immediately submits an (acknowledged) binding update to its HA. A binding denotes the association of a HoA with the correspondent CoA for a MN. At this stage, it regained the ability to send and receive packets using its permanent HoA, but only via a bi-directional tunnel with its HA. To achieve a direct, unencapsulated packet exchange, a route optimisation, the MN needs to inform its communication partners (CNs) about its new location. It does so by sending additional binding updates. HA and CNs keep these binding update information within their binding caches. Without further protocol operations, the MN is now enabled to exchange packets carrying its permanent HoA through a bi-directional tunnel directly spanned with the CN. Mobile communication bears a phenomenon known as "address duality": The technical address, which is used to identify and locate a stationary device, in the mobility case splits up into a permanent logical (HoA) and a transient topological (CoA) identifier. To avoid data encapsulation, MIPv6 transparently operates this address duality on the IP layer as a device moves from one network to the other. In contrast to traditional telecommunication schemes, it inherently performs address separation and re-combination, simultaneously invisible to routing and applications.

MIPv6 stack at the MN extracts the IP Home Address originating from the base header of the (static) IP stack and places it in a Home Address Destination Option as shown in figure 2. Using CoA as source address, the packet can be transparently routed to the CN. The MIPv6 stack at the latter extracts the mobility extension header, discovers the HoA, which is validated against the binding cache, re-places it into the base IPv6 header and thereby completely hides the differing route to the socket layer.

Conversely, in submitting datagrams to a MN, the MIPv6 stack at the CN identifies the HoACoA tuple in its local binding cache and issues a source route to HoA via CoA, i.e., it replaces the HoA destination address from the base header with the CoA, but adds the HoA in a (mobility-specific) type 2 routing header as displayed in figure 2. The packet is thus directly transferred to the MN (at CoA), which discovers the source route destined to its own interface Home Address, performs a virtual routing hop and passes the packet with its final destination address (HoA) onto the socket layer. In this way, hosts are enabled to maintain transport and higher layer connections when they change locations, but at the same time perform route optimisation in a topologically flawless fashion.

Volume : 4 | Issue : 8 | Aug 2015 • ISSN No 2277 - 8179

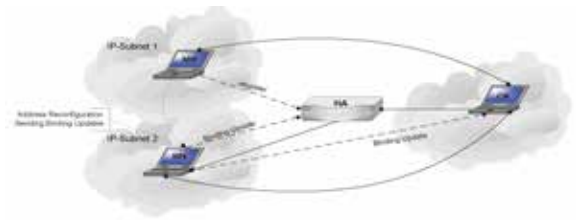

Figure 1:Handover operations of MIPv6: The MN signalling to its HA and CNs.

Some node wishing to contact the MN while away from home will be unaware of its current location. It will simply issue data to the HoA. Those packets are intercepted by the Home Agent and initially tunnelled to the MN. On reception of encapsulated packets, the MN will submit a binding update to the correspondent sender, which subsequently will perform MIPv6.

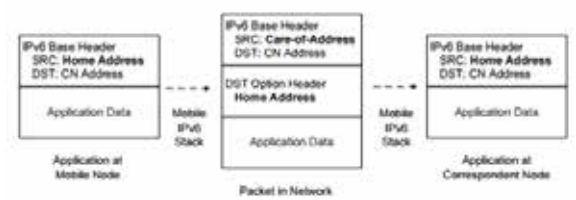

Figure 2: MIPv6 header extensions used at MN-to-CN communication

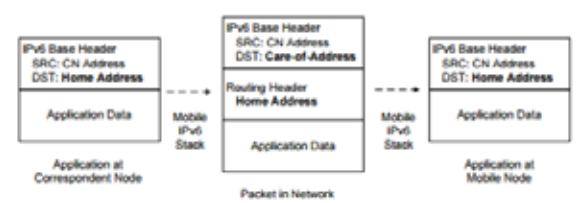

Figure 3: MIPv6 header extensions used at CN-to-MN communication

Route optimisation as described above. Mobility-unaware CNs may continue to use HA-based tunnelling. Thus, the Home Agent is the only infrastructural component required for a successful MIPv6 deployment. It may reside anywhere within the home network, i.e., as an additional router function or as a separate physical entity. The remaining protocol elements and operations may remain as transparent to the Internet infrastructure as the routing layer remains transparent to end nodes.

2.2 Basic Security

Mobile IPv6 protocol operations admit the characteristic of traffic redirects and consequently bear the risks of theft-of-service and distributed denial-of-service attacks. In its core, the protocol has to protect its binding updates and the validity of binding caches, respectively. These operations occur twofold, with the Home Agent as well as with the MIPv6 aware Correspondent Node. As communication roles of these partners are quite distinct, both parties need a dedicated, separate treatment.

The HA can be considered as a service entity, well-known to the MN and is commonly preconfigured at start-up. Without loss of generality, a pre-established security association can therefore be assumed. Initial standards closely associated with MIPv6 [5, 6] have foreseen such tight security coupling in the form of IPSec ESP authentication and integrity protection, assuring a trust relationship for binding updates with the Home Agent.

In contrast, any node throughout the Internet can attain the role of a CN without ever having contacted the MN before. No preshared configurations can thus be presupposed. Additionally, MIPv6 design intended to imply only light-weight and stateless security burdens onto common partners. Protocol designers had to invent a new security signalling as to protect binding updates with CNs, which operates under the name of Return Routability Procedure. The basic task of the Return Routability Procedure is to assure reachability of the MN at both of its addresses, i.e., directly via the CoA and indirectly via its HoA through the HA. The procedure thereby defends global man-in-the-middle attacks as applicable in case of a simple signalling from MN to CN. In detail the signalling proceeds as follows, cf. figure 4. Prior to a binding update the MN issues a home test init (HoTi) and a care-of test init (CoTi) message along with a random cookie on the paths via the HA and directly to the CN. Init signals are acknowledged by home test (HoT) and care-of test (CoT) messages, both carrying individual tokens. If these tokens, which are separately transmitted to the MN's dual addresses, arrive correctly, the MN is enabled to submit its binding update along with a joint token digest. It thereby proves network layer presence at both channels, directly at the CoA and authenticated via a tunnel through the HA.

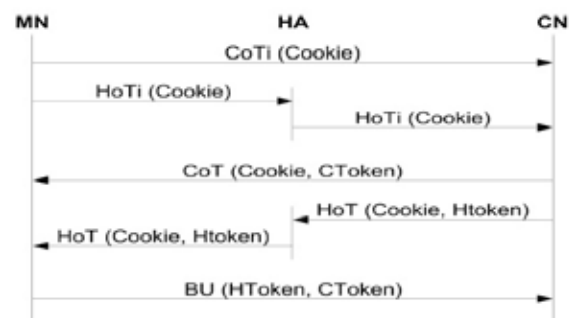

Figure 4: The Return Routability Procedure Issued with the CN.

OS		HA	CN	Implementation
BSD	X	X	X	SHISA/KAME: www.mobileip.jp, www.kame.net
HP-UX 11iv1/2		X	X	Tour 3.0: www.software.hp.com
HP Tru64		X	X	Mobile IPv6 4.0: www.hp.com
Linux	X	X	X	MIPL/USAGI: www.mobile-ipv6.org, www.linuxipv6.org
Windows XP			X	Included
Windows	X		X	Treck Mobile IPv6: www.treck.com

Table 1: Current MIPv6 Implementations

2.3 Implementations and Deployment

During its long standardisation process, various experimental protocol implementations arose for Mobile IPv6, the most current are summarized in table 1. Even though standardisation has completed, stacks for some operating systems are still of limited functionality or implementation project strategies remain unclear. Microsoft Research has developed a full RFC 3775 compliant MIPv6 stack, the Mobile IPv6 Technology Preview. It exists for different Windows versions, but is currently not available. The official Windows MIPv6 release, though, supports only CN functionality. Integrated in Windows XP and Windows Server 2003 it can be enabled via the netsh command. The IPv6 protocol for Windows Vista and Windows Server 2008 does not provide Mobile IPv6 at the moment. The company Treck offers a free embedded IPv4/6 stack as a Windows demo for testing purposes of their compiler, processor and OS independent commercial dual

stack. This demo comes with different applications, e.g., a FTP or HTTP server, and runs independently, i.e., in parallel with the Windows TCP/IP stack. Historically, Mobile IPv6 support for BSD variants has been developed within the KAME and Internet CAR projects. Now, they have been merged into a single extensive implementation called SHISA. Up until now, the new SHISA version is not ready for public release, but a fully functional MIPv6 stack can still be downloaded via the KAME website. Mobile IPv6 for Linux is available for kernel version 2.4 and known as the MIPL 1.1 stack. For kernel 2.6.16 there exists a joint development of the USAGI and MIPL project team, the so called MIPL2, with the intention of contributing extensions into the mainline Linux kernel. The version 2.0 is a complete re-write of the entire software, with most of the functionality residing in a user space daemon and only a thin support layer within the kernel. The MIPL distribution is split into two required packages for easier maintenance: the user space part, including tools to configure and analyse MIPv6, and the kernel part. To keep MIPL2 up-to-date with the latest Linux kernel developments, USAGI maintains and releases UMIP, a set of patches.

3. Performance Problems and Security Limitations

3.1 Handover Performance

In the event of a Mobile Node switching between access networks, a complex reconfiguration chain is initiated, which should remain unnoticeable to applications and their users. At first, the mobile device may completely disconnect from the link layer, demanding L2-specific reassociation times. There after it needs to perform a local IP reconfiguration and Binding Updates to its HA and CNs. Until completion of all these operations, the MN is likely to experience disruptions or disturbances of service, as are the result of packet loss, delay and jitter increases. In detail the handover process decomposes into the steps:

Link layer handoff which may be instantaneous or connection oriented, single- or multi homed, depending on the technologies in use. Times of disconnects range from 0 to several hundred milliseconds, the latter for poorly optimised 802.11 equipment.

Layer 3 movement detection can be achieved in a passive or active manner. A MN may learn about a new prefix by regular router advertisements, but – in the presence of link-layer triggers – may actively solicit a route-prefix advertisement subsequent to L2 handoff.

CoA configuration will follow without delay, after a valid prefix has been learned.

Duplicate address detection (DAD) leads the MN into a timeout, in case a unique address has been configured. To overcome this delay, asynchronous DAD processing has been suggested and widely implemented.

Binding update with HA requires binding acknowledgement from the HA and thus will take a round-trip time between MN and HA.

Binding update with CN initiates the Return Routability Procedure, which will involve a roundtrip signalling between MN and CN as well as between MN and HA.

While the first four steps are local, topologically independent operations, binding updates depend on the sum of roundtrip times between components. Assuming L2 triggers and asynchronous DAD in presence, MIPv6 stateless local handovers may become impressively fast. In a mobility-friendly environment, the solicited router discovery handshake may operate at a timescale of a few milliseconds, after the MIPv6 [1] timer variables MAX_RA_DELAY_TIME and MAX_RTR_SOLICITATION_DELAY at the router and the MN have been adjusted accordingly.

This may then reduce MIP local readdressing time well below 10 ms without adding base load to the network. For comparison note that the 802.11b clock tick allows for sending

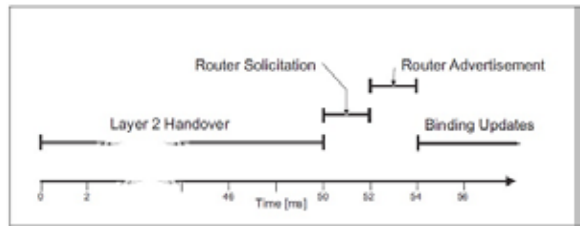

Figure 5: Optimized Local Handover Timing in Presence of L2 Triggers and Asynchronous DAD.

10 packets of the size of a Router Advertisement per ms. Figure 5 visualises the local handover steps and their temporal dimensions. However, binding update times are defined by the topological set-up beyond the control of MIPv6 and router stacks.

3.2 Security Limitations

Basic Mobile IPv6 security is robust and sufficiently simple. Based on security standards common to the static Internet, it ensures that a MN can use its Home Address for bindings and service access only if it either is at home or it is supported by a Home Agent located within its home network. Nevertheless it admits several drawbacks, which derive from the Return Routability Procedure. At first, binding updates remain vulnerable to man-in-the-middle attacks within the access network of the CN. Therein, and possibly at adjacent links, home and care-of test messages coincidently traverse. Furthermore, the procedure implies several roundtrip signals and thereby adds significant update delays. It withstands straightforward protocol optimisations for resolving the topological dependence in handover performance. Finally, unidirectional data distribution as used in IP multicast cannot utilize such handshake protocol for the exchange with many CN-listeners. An improved security scheme for the binding update operations with Correspondent Nodes is thus of vital importance. This intrinsically hard problem could take advantage of a recent concept of cryptographically generated addresses [7].

4. Firewall Issues

With the deployment of Mobile IPv6, network administrators have to adjust their currently established firewalls or ACLs to allow for the interplay of MIPv6. Socket parameters and the protocol type are used by firewalls to admit or decline network traffic. Stateful firewalls are able to adjust adaptively their rules to open channels, directed from the protected network to an outside node. Based on the end device function, i.e., MN, HA or CN, located in the secured domain, different requirements have to be fulfilled [8, 9]. We are focussing on the following issues:

The Problem of ESP Filtering One of the main problems with current firewall rules in conjunction with MIPv6 is the strict filtering of ESP packets, independently of Mobile IP. As the Binding Updates (BU) and Acknowledgements should be protected by IPsec ESP neither a communication to the Home Agent, nor to the Correspondent Node could be established. It is worth noting that a firewall cannot know the MN CoA in advance and may be unable to inspect ESP packets due to encryption. Consequently a minimum permit pattern should include the MNs visited subnet prefix and the ESP IP payload protocol number 50 [9]. Allowing for ESP packet traversal is also a prerequisite for route optimization with the CN, because the MN has to initiate an ESP protected Return Routability Test before sending the BU.

The Problem of Stateful Firewalls Even after the HA and CN have been successfully updated with the location of the MN, fire-

Volume : 4 | Issue : 8 | Aug 2015 • ISSN No 2277 - 8179

walls may prevent further communication. One simple example is a CN trying to initiate traffic to the MN behind a firewall. As signalling messages and data traffic appear decoupled to MIPv6 unaware firewalls, a binding update does not establish a state suitable for regular communication. Consequently only the MN could initiate traffic to the CN and enable a corresponding permit rule. The same happens if the CN resides behind a firewall and the MN wants to initiate a connection with the CN. Further on firewalls have to consider CoA changes. Every packet from the MN carries the CoA as source address, either in the outer tunnel header or in direct, route optimised flows to the CN. Any state established in a firewall persistently protecting MN or CN will invalidate, whenever the MN changes its subnet. For this reason it is equally important to track address changes or to reflect on the MN Home Address.

5. Improving MIPv6: Protocol Extensions and Future Issues

Hierarchical Mobility Management and Fast Handovers for MIPv6: Mobile IPv6 handover performance was shown to be strongly topology dependent. This weakness has been subject to further investigation within a performance optimisation working group with the result of optimising protocols. Two propositions to improve the roaming procedures ofMIPv6 are essentially around:

A concept for representing Home Agents in a distributed fashion by proxies has been developed within the Hierarchical Mobile IPv6 (HMIPv6) [10]. While away from home, the MN registers with a nearby Mobility Anchor Point (MAP) and passes all its traffic through it, see figure 6. The vision of HMIPv6 presents MAPs as part of the regular routing infrastructure. The MN in the micro-mobility concept of HMIPv6 is equipped with a Regional Care-of Address (RCoA) local to the MAP in addition to its link-local address (LCoA). When corresponding to hosts on other links, the RCoA is used as MN's source address, thereby hiding local movements within a MAP domain. HMIPv6 reduces the number of 'visible' handover instances, but - once a MAP domain-change occurs - binding update procedures need to be performed with the original HA and the CN. The alternate approach delegates handover negotiations to the access routers (PAR/NAR) and is introduced in the Fast Handover for MIPv6 scheme (FMIPv6) [11]. FMIPv6 attempts to anticipate layer 3 handovers, configure and verify a prospective new CoA prior to handover, and to redirect traffic to the new location, while the MN moves to its new point of attachment.

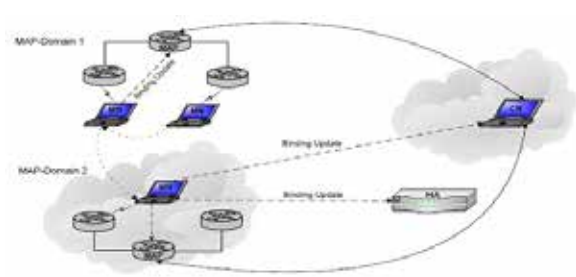

Figure 6 : Micro-Mobility Optimisation with HMIPv6.

As shown in figure 6, a MN issues its handover prediction in a fast binding update (FBU) to its PAR, which then negotiates the handover with NAR in a HI–HACK dialog. The protocol then specifies a tunnel between the Previous CoA (PCoA) and the New CoA to facilitate continuous communication of the MN using its PCoA. To enable predictions, FMIPv6 relies on layer 2 information and a layer 2 to 3 topology map. Consequently this approach requires layer 2 specific extensions. FMIPv6 aims at hiding the entire handover delay to communicating end nodes at the price of additional layer 2 intelligence, but falls back into a reactive handover, whenever predictive attempts fail. Binding updates with HA and CN are issued asynchronously subsequent to the handover. A functional risk arises from a conceptual uncertainty: As the exact moment of layer 2 handover generally cannot be foreseen, and even flickering may occur, a traffic anticipating redirect may mislead data and cause additional damage. Both approaches, HMIPv6 in the micro-mobility case and FMIPv6 for a L2-aware access infrastructure, resolve the topological dependence of handover performance and are suitable for real-time communication.

Enhanced Route Optimisation for Mobile IPv6

Route optimisation at the one hand forms the key performance characteristic of Mobile IPv6, on the other bears severe security risks and thus burdens the protocol with complex, tardy control operations. The central security problem a MN has to address for binding updates or service access lies in a proof of HoA ownership, which ideally should be inherent to a critical message itself. If a MN can provide a strong proof of identity within a single, self-consistent update packet, Mobile IPv6 could be considered seamless and secure.

Fortunately a discovery of applying public key cryptography arrived just with the development of MIPv6: Cryptographically generated identifiers can be employed as link-local addresses (CGAs) in IPv6 [7]. Using the public key as cryptographic source address, a sender can provide a signature within a packet and thereby entitles any receiver to authenticate and verify a single, self-consistent datagram against the sender IPv6 address. No additional cryptographic infrastructure like a PKI is needed. Applying this mechanism to the Home Address of the MN, a standard for enhanced route optimisation has been defined in [13].

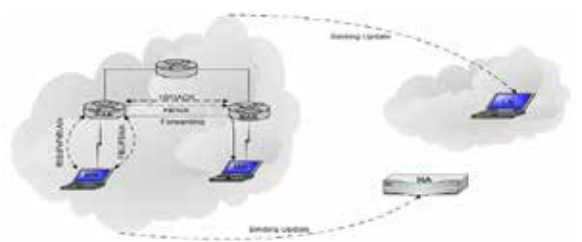

Figure 7: Optimised Handover Management at the Edges with FMIPv6.

A Mobile Node initially configures its local identifier on the home link by extracting the first 64 bits of the SHA-1 hash value taken from a CGA data structure, which is essentially generated from a public key. Combined with its home prefix, this ID forms the Home Address. To issue a sensitive message, e.g., a binding update, the MN includes a regular Home Address destination option along with its CGA parameters, which include the network prefix, and a CGA signature, which signs the CGA parameters and the remaining data with MN's private key. On reception of such packet, a CN can autonomously check for Home Address authentication and data integrity. This proof is cryptographically strong. The cryptographic Home Address in enhanced route optimisation does not play the role of source address within the packet base header, but is a parameter within an extension header. To prevent a possible misuse of artificially generated Home Addresses in remote attacks, any

CN needs to verify a HoA reachability at the initial binding. However, this test is required only once and may proceed prior to an actual handoff in an asynchronous way. Having done so, a MN is enabled to provide cryptographically strong proof of identity while sending a binding update message from anywhere in the world. As binding updates can be piggybacked on top of regular data, mobile communication after a handover can thus pursue as soon as the mobile has succeeded in local IP configuration.

Multicast Mobility Extensions

The Internet uniquely provides a globally distributed, scalable and serverless multicast support at the network layer. It thereby offers a valuable group communication service, which forms an integral building block of a wide variety of applications. This function is of enhanced relevance in a mobile environment, where bandwidth remains a shared limited resource and only lightweight applications comply with end system capacity constraints.

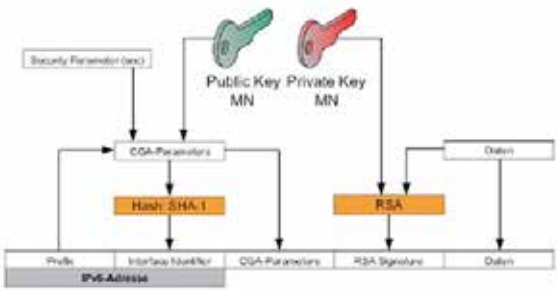

Figure: Figure 8: Optimized Secure Binding Update with Cryptographically Generated Addresses.

MIPv6 only roughly treats multicast mobility in a pure remote subscription approach or through bi-directional tunnelling via the Home Agent. Remote subscription relies on multicast adaptive routing, as a mobile listener re-joins groups in each visited network, and therefore suffers from slow handovers. Bi-directional tunnelling introduces inefficient overheads and delays due to triangular forwarding. Therefore none of the approaches can be considered solutions for a deployment on large scale. A mobile multicast service for a future Internet should admit 'close to optimal' routing at predictable and limited cost, robustness combined with a service quality compliant to real-time media distribution.

7. Conclusions

Mobile computing and communication have emerged to key technologies of the forthcoming decade, but the traditional IPv4 network layer is inadequately prepared to extend into the mobile regime. In this overview we tried to comprehend, how Mobile IPv6 can catch up with mobility requirements and rapidly further evolves to meet the demands of a seamless and secure all IP mobile worlds soon. At the same time we tried to illustrate that the enhanced architecture of IPv6 can elegantly host challenging new tasks such as a mobile computing milieu. At the present time, the major steps in technological development and standardisation for a next generation mobile Internet are close to completion. A sufficient variety of implementations and experimental experiences are around, as well. Thus the time for deployment has arrived now leaving us with the hope that the benefits and potentials of these new mobility protocols will persuade operators and domain administrators to get over traditional scepticism against new open end-to-end solutions.

REFERENCE

[1] D. B. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," IETF, RFC 3775,June 2004. | [2] H. Soliman, Mobile IPv6. Boston: Addison-Wesley, 2004. | [3] R. S. Koodli and C. E. Perkins, Mobile Internetworking with IPv6: Concepts, Principlesand Practices. Hoboken, NJ: Wiley and Sons, 2007. | [4] B. Stockebrand, IPv6 in Practice: aUnixer's Guide to the Next Generation Internet.Berlin: Springer-Verlag, 2007. | [5] Rostanski, M.; Mushynskyy, T. Security Issues of IPv6 Network Autoconfiguration. InProceedings of the 12th International Conference on Computer Information Systems andIndustrial Management Applications (CISIM 2013), Krakow, Poland, 25–27 September 2013;Springer: Heidelberg, Germany, 2013; pp. 218–228. | [6] V. Devarapalli and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec | Architecture," IETF, RFC 4877, April 2007. | [7] T. Aura, "Cryptographically Generated Addresses (CGA)," IETF, RFC 3972, March 2005. | [8] F. Le, S. Faccin, B. Patil, and H. Tschofenig, "Mobile IPv6 and Firewalls: Problem Statement,"IETF, RFC 4487, May 2006. | [9] S. Krishnan, N. Steinleitner, and Y. Qiu, "Firewall Recommendations for MIPv6," IETF,Internet Draft – work in progress 01, July 2007. | [10] H. Soliman, C. Castelluccia, K. Malki, and L. Bellier, "Hierarchical Mobile IPv6 mobility management (HMIPv6)," IETF, RFC 4140, August 2005. | [11] Syed, A.R.; Gillela, K.; Kumar, P.P.; Venugopal, C. Outline of IPv6 topology and best-practice security rules. Int. J. Adv. Res. Comput. Sci. Softw. Eng. 2013, 3, 1106–1111. | [12] T. C. Schmidt and M. Wählisch, "Predictive versus Reactive – Analysis of Handover Performance and Its Implications on IPv6 and Multicast Mobility," Telecommunication Systems, vol. 30, no. 1–3, pp. 123–142, November 2005. | [13] J. Arkko, C. Vogt, and W. Haddad, "Enhanced Route Optimization for Mobile IPv6," | IETF, RFC 4866, May 2007. | [14] D. Le and J. Chang, "Tunnelling-based route optimization for mobile IPv6," in Proceedings of the IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS '10), pp. 509–513, 2010 | [15] Botterman, M. IPv6 Deployment Survey; Technical Report; GNKS Consult: Rotterdam, The Netherlands, 2011.