A Prototype-based Evaluation of IP Technologies for Mobile VPNs

Antonio Liotta[1], Daniel H. Tyrode-Goilo[2], Adetola Oredope[1]

[1] University of Essex, Department of Electronic Systems Engineering
Wivenhoe Park, Colchester, CO4 3SQ, U.K.
{aliotta, aoredo}@essex.ac.uk
[2] University of Surrey, Centre for Communication Systems Research
Guildford GU2 7XH, U.K.
dtyrode4@yahoo.co.uk

Abstract. Virtual Private Networks have evolved considerably over the last few years, reaching their full maturity in fixed networks such as ATM, frame relay and the Internet. Wireless and cellular networks pose, however, more stringent requirements that have not yet been fully addressed. In order to assess the suitability of state-of-the-art technologies for the realization of mobile VPNs over the Internet, we have built a prototype based on Mobile IPv6 and IPsec. We report here the most significant findings on IP-based MVPNs over wireless LAN, GPRS and UMTS, highlighting capabilities and limitations. Our results indicate that we are just a step away from seeing commercially viable products, although there is still space for improvement as far as standardization and performance are concerned.

1 Introduction

A Virtual Private Network (VPN) is used to securely transport data with the adequate levels of authorization between endpoints, through non-secure, public infrastructures. VPNs have now gained importance with most businesses and companies, replacing most of the existing leased lines [1] whilst often reducing costs, increasing speed and providing simplified administration. VPNs are fully matured in fixed networks including ATM [2], Frame Relay [3] the Internet [4] an MPLS. Wireless and cellular networks pose, however, more stringent requirements that have not yet been fully addressed [5].

Given the importance gained by the Internet, some researchers have been looking at the integration of Mobile Internet Protocol version 4 (MIPv4) and Internet Protocol Security (IPsec) [6, 7]. However, limitations such as network address translation (NAT), setting up of tunnels and address updates still arise [6]. This motivated us to integrate the end-to-end tunneling capability of IPsec with Mobile Internet Protocol version 6 (MIPv6) which eliminates the NAT and foreign agent limitations of the IPSec/MIPv4 implementation. In addition MIPv6 overcome the IP address exhaustion problem suffered by IPv4.

Our aim is to assess the maturity of state-of-the-art IP technologies in relation to MVPNs. We have carried out an integration exercise resulting in an IP-based MVPN test-bed combining the key ingredients of MIPv6 and IPsec in a multi-access

environment including wireless LAN (WLAN), the General Packet Radio Service (GPRS) and the Universal Mobile Telecommunication System (UMTS). We have carried out a series of functional tests to verify the level of stability of our platform (validation). We later conducted a performance assessment involving horizontal and vertical handover in both transport and tunnel modes. These revealed several limitations that lead to problems such as the interference of source addresses with tunneling, the failure of bidirectional tunneling, and the flushing out of routing tables immediately after handover.

Upon a short description of the basic technologies used in our prototype (Section 2), we describe the test-bed in Section 3, followed by a sample of our experimental results based on four sets of tests. We find that, despite the performance limitations which have implications in terms of application-level communication, IP technologies are functionally mature for MVPNs. This indicates that we are getting closer to commercially viable MVPNs although there is still space for improvement as far as standardization and performance are concerned.

2 Background Technologies

2.1 Virtual Private Network (VPN)

VPNs are secured overlay networks built over public infrastructures in which access is controlled to permit peer connections only within a defined community of interest [8]. They can simply be described as building a secured Wide Area Network over a public infrastructure in which the Internet is usually considered. Security is the main issue in building any VPN and it can be achieved by encrypting data packets over the network. Existing VPNs for fixed networks, such as ATM and frame relay networks, enable security at the data link layer (L2). In IP networks, VPNs can be realized at the network layer (L3). Example security protocols include the Peer-to-Peer tunneling protocol (PPTP) [20], the Layer 2 Tunneling Protocol (L2TP) [21] (both operating at L2) and the Internet Protocol Security (IPsec) [22] (operating at L3).

Existing VPNs are not geared towards terminal mobility. We contribute to the understanding of the issues surrounding this topic by carrying out an integration exercise leading to an IP-based MVPN. As the basis of our experimental testbed we have chosen IPv6, motivated the fact that 3GPP [9] mandates its use in the IP Multimedia System (IMS) [9] (from Release 5 onwards). In addition, UMTS is based on IPv6. Due to the scope of our investigation we have chosen IPsec as a security support protocol. Therefore, our test-bed can be regarded as an elementary proof-of-concept prototype of state-of-the-art mobile networking systems for integrated services such as voice and data over IP-based packet switched networks [10].

2.2 Mobile Internet Protocol Version 6 (MIPv6)

True Mobility on the Internet requires for the mobile node to have a unique global address. This was actually achieved in the MIPv4 [6] that had, however, limitations in terms of performance, scalability and reliability. In MIPv4, every packet sent to a

Mobile Node (MN) is tunneled via the Home Agent (HA), a routing entity sitting in the MN's home network (the HA is the bottleneck and a single point of failure).

Security in MIPv4 has limitations too. First, outgoing packets may be dropped by ingress filters in visited or transit networks because of the use of the home address as the source address. Other problems arise when the Foreign Agent (FA) (which is a routing entity handling a MN in a visited network) is incapable of reading a MN request to register to its HA. This impedes the set up of the tunnel which, in turn, results in loss of connectivity.

To address the latter issue, in MIPv6 the MN registers also with the Corresponding Node (CN) [11]. By using additional headers such as the Type-2-Routing header and the *home or destination* address option header, MIPv6 allows route optimization, which avoids the triangle routes that lead to performance degradation in MIPv4.

Nevertheless, despite offering the essential mechanisms to incorporate mobility in IP, MIPv6 *per se* is not secure. For instance, since the binding updates among communicating nodes are not secured, it is relatively easy for intruders to gain illicit access to the network or impersonate other users. Therefore, MIPv6 only provides one of the fundamental requirements of MVPNs (terminal mobility) but needs to be complemented by some other security mechanism.

2.3 Internet Protocol Security (IPSec)

IPSec is an open standard protocol operating at the network layer which removes the burden of security from the network, placing it on the endpoints [22]. Encryption can protect the entire IP payload (*tunnel mode*) or just the upper-layer protocols of the IP payload (*transport mode*). IPsec, which is normally used between hosts and gateways, provides security services such as access control, data integrity protection, data origin authentication, anti-replay protection and confidentiality, offering protection to the protocols in the upper layers.

IPsec includes two types of protocols. The Encapsulation Security Payload (ESP) provides confidentiality, data integrity and data source authentication of IP packets by encapsulating the data to be protected (i.e. an upper-layer protocol or the entire IP datagram) between an ESP header and trailer. Only the data and part of the trailer are encrypted – the header is not. On the other hand, the Authentication Header (AH) supports data integrity and data source authentication but does not offer any form of confidentiality, which makes it a lot simpler than ESP and is less commercially desired.

3 Building an IP-based MVPN test-bed

We describe here the software architecture and integration strategy used to build the MVPN test-bed which is then assessed in the following section. The test-bed is built on Linux which seemed the most mature, open-source platform as far as MIPv6 and IPSec were concerned (although BSD-variants are more mature in IPv6). As a starting point we choose the USAGI (**U**niver**SA**l play**G**round for **I**Pv6) implementation of IPv6 because of the advantages it has over other implementations in its support for multiple paths to the same destination with equal or unequal metrics and its simplified

method for adding and removing default routes [19]. Also, USAGI has become the default IPv6 implementation in the Linux kernel.

We found, however, that the USAGI MIPv6 implementation available at that time was not suitable for our purpose, mainly because key mobility functionalities were not available on Linux 2.6x series (it was based on the 2.4 kernel written by HUT-Go [18]). Hence, we back-ported USAGI version 5 on our Linux 2.4 kernel for which we had full access to source code. We then used the MIPv6 Implementation for Linux (MIPL) which is a kernel patch for the 2.4.x series [18]. MIPL contains a specific module for the HA, MN and CN. The CN features are implicitly contained by the HA and the MN.

The USAGI implementation also supports IPSec which was chosen for our test bed because of its improved and developed kernel attributes supporting AH, ESP, SAD and SPD [19] which other implementations lacked.

4 Evaluation

4.1 Experimental Set-up and Tools

To fully experiment with mobility over a multi-access network all terminals (including MN, HA and FN) are connected via a WLAN 802.11b (5.5Mbps). We also included an impairment node whose role is to emulate GPRS and UMTS conditions that are typically experienced in real networks.

In the following sections we present a sample of the most representative experiments carried out so far, capturing four aspects: test-bed validation, horizontal handover (WLAN to WLAN), and vertical handover (WLAN to GPRS and WLAN to UMTS). The *tcpdump*[1] network sniffer was used to collect the data at the end-points (CN and MN) which was then stored in binary *pcap* files. Every test was repeated to ensure statistical significance.

The results reported herein focus on IPSec ESP. We have not included IPSec AH which has lost commercial interest due to its inability to protect the confidentiality of the IP packet payload. The IPSec configuration was manually *keyed*. We intended to test the robustness and effectiveness of the USAGI's stable release protocol stack.

4.2 TEST 1: Platform Validation (functional assessment and stability)

Aim

Validate the MVPN testbed, verifying the functionality, robustness and stability of the integrated core IPv6 and IPsec stacks.

Setup

A webserver running Apache was configured in order to perform downloads between end points and total of 22 different setup configurations were tested, assessing the following features:

[1] http://www.tcpdump.org/

- Route advertisement operation through the router advertisement deamon or radvd (both in static and dynamic mode – in static mode we manually allocated IPv6 addresses);
- IPv6/IPsec transport mode with stateful (static) address allocation;
- IPv6/IPsec transport mode with stateless address allocation (radvd);
- IPv6/IPsec tunnel mode with stateful (static) address allocation;
- IPv6/IPsec tunnel mode with stateless address allocation (radvd).

Results
The file transfer application succeeded in 100% of the 22 tested configurations. This was a result of a fine-tuning process during which we fixed various issues arising from the IPv6/IPsec integration process including also other software/hardware elements of the software environment. Unfortunately, due to space limitations we cannot report here any further details with this regard. We have, however, evidence that our platform is stable and performs all basic functions correctly.

4.3 TEST 2: Horizontal Handover over Wireless LAN

Aim
Validate and assess the functionality, stability and handover properties of our MVPN in a WLAN 802.11b environment.

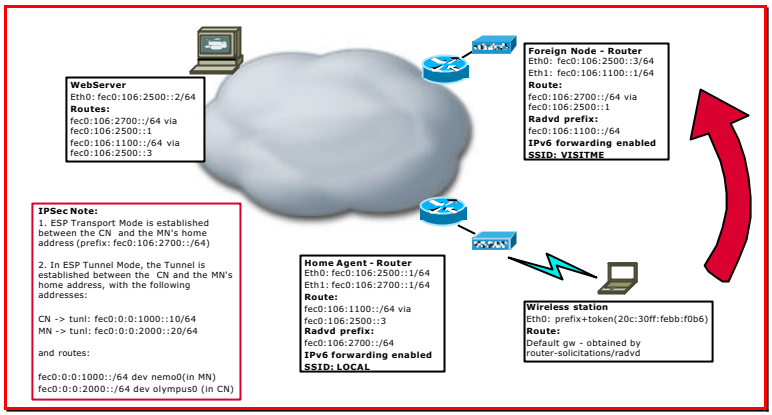

Fig. 1. Network setup for WLAN horizontal handover.

Setup
MIPv6 was enabled on both the Home Agent (HA) and the Corresponding Node (CN) with routes to the web server as shown in the network setup depicted in Fig 1. The test starts by initiating a file transfer between the MN – sitting in the home network – and the web server. During the transfer horizontal handover is forced. To emulate this process, the transition between Home and Foreign Networks was performed by setting different *Service Set Identifiers* (or SSID, a token used to identify an 802.11 WLAN network) and forcing the MN to change from one SSID to another. This

procedure is known as *Hard Handover* since the IP point of attachment is terminated before the MN is moved to a new point of attachment (*break-before-make*). Using *ethereal*[2] we could identify the key MIPv6 packet exchanges during handover, determining their precise position in the file-transfer timeline.
A total of 21 different setup configurations were tested, assessing the following features:

- Pure MIPv6 both with Route Optimization (RO) and Bidirectional Tunneling (BT);
- Integrated MIPv6/IPsec transport mode handover, both with RO and BT;
- Integrated MIPv6/IPsec tunnel mode handover, both with RO and BT.

Results

Due to space constraints we cannot present the individual results of all 21 tests. Representative data is illustrated in Figures 2-4. In the remainder we use common IPv6/IPsec terminology, referring to the abbreviations of Table 1.

key	***Abbr.***	***Meaning***
1	RA	Route Advert
2	BU (MN to HA)	Binding Update
3	BA (HA to MN)	Binding Ackn
4	CoTI (MN to CN)	Care of Test Init
5	CoT (CN to MN)	Care of Test
6	BU (MN to CN)	Binding Update
7	Next-TCP-Packet	
	RA	Route Advertisement
	RO	Route Optimization
	BT	Bidirectional Tunneling

Table 1. Abbreviations.

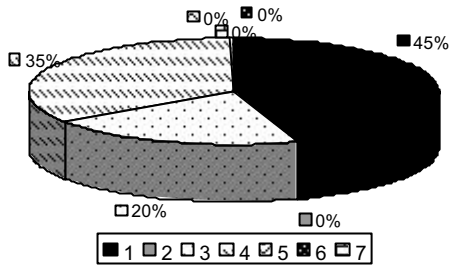

Fig. 2. Distribution of average time values for WLAN Pure MIPv6-RO.

The total horizontal handover times w.r.t. pure MIPv6 with RO were comprised between 4.25 and 8.84 seconds with an average of 6.96 sec. Their distribution among individual factors is depicted in Fig.2. In the case of BT we obtained slightly better results (min=1.78 sec; max=8.47 sec; avg=4.68sec) with a comparable distribution.

We can draw the conclusion that, the predominant factor in horizontal handover is the time taken by the MN to acquire information from the visited/foreign network (network prefix and default router). BT incurs less overhead than RO in terms of MIPv6 traffic needed to restart home running TCP conversations (no CoTI/CoT required). In fact, in RO mode the CoTI can become an issue of concern (if the application that is trying to reach the MN does not send packets during or shortly after handover, it may take considerable time for the MIPL implementation to send a CoTI).

Another determining factor is represented by the BA coming from the HA to the MN (21% and 20% in the case of BT and RO, respectively). This can considerably increase when network performance degrades.

Looking at MIPv6/IPsec transport mode, the aggregate times (considering 9 different configurations not reported here for brevity) are: min=1.70msec; max=9.58sec; avg=5.47sec. The aggregate distribution of average time values for the

[2] http://www.ethereal.com/

case of transport mode and tunnel mode are depicted in Fig.3 and Fig.4, respectively. These highlight some issues. In the case of transport mode, in RO mode CoTI takes a slightly higher percentage of the total handover time in comparison with pure MIPv6. This is due to the processing overheads introduced by IPsec. Because of this relative increase, the overall impact of waiting for a RA notification is reduced (8.5% on RO and 3.5% in BT) when compared with pure MIPv6. A similar impact of IPsec processing overheads is experienced also in BT mode. However, the overall performance in this case is 5.9% better than RO.

Overall, when compared to pure MIPv6, RO with IPsec performed 19.1% faster, whilst BT with IPsec increased its average handover time by 11.8%.

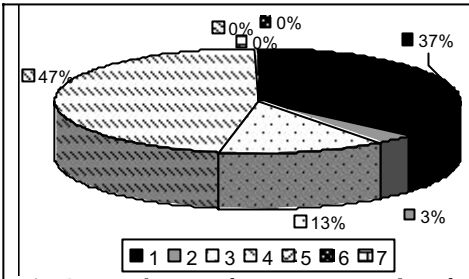

Fig. 3. Distribution of average time values for WLAN MIPv6/IPsec transport mode.

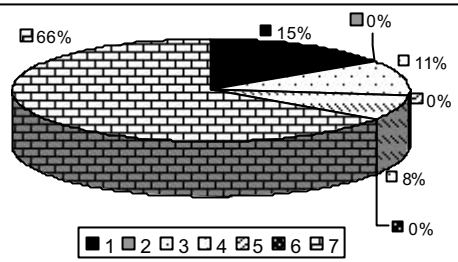

Fig. 4. Distribution of average time values for WLAN MIPv6/IPsec tunnel mode

In MIPv6/IPsec in tunnel mode (Fig.4), the *next-TCP-packet* value has considerably increased (from almost null to 66%). This can be explained by looking at how handover is implemented. During handover, routing tables are flushed so, in order to regain connectivity after handover, the private routing entries must be re-instated. This process can be largely improved but we haven't attempted this task at this stage since our priority was on assessing the extent to which existing protocol implementations would integrate into MVPNs.

4.4 TEST 3: Vertical Handover between WLAN and GPRS

Aim

Validate and assess the functionality, stability and handover properties of our MVPN in a multi-access network including WLAN 802.11b and GPRS. The sample of results presented herein is focused on the performance under vertical handover conditions.

Setup

The experimental setup is analogous to ones presented above but includes an additional impairment node which emulates network conditions typically experienced in a GPRS network. The conditions relating to the following results are: Upstream Bandwidth = 10kbps; Downstream Bandwidth = 40kbps; Round Trip Time = 700msec. The handover takes place between WLAN (Home network) and GPRS (Foreign Network), as depicted in Fig.5.

At the time of the tests it was quite difficult to find a network emulator satisfying all the requirements of our test-bed (mainly native IPv6 support over the relevant Linux

kernel). We finally had to implement the impairment node based on a modular router for Linux platform, the Click Router Project [16], patched against kernel revision 2.4.26. Bandwidth metrics were verified with the *iperf*[3], a tool supporting IPv6 and capable of determining TCP/UDP bandwidth between two endpoints. The experiments were performed over the same (21) set-up configuration of Test II.

Results

A representative sample of results is illustrated in Figures 6-8. The total vertical handover times w.r.t. pure MIPv6 with RO were comprised between 9.85 and 11.91 sec with an average of 11.08 sec. Their distribution among individual factors is depicted in Fig.6. In the case of BT we obtained slightly better results (min=5.9 sec; max=10.93 sec; avg=9.32sec) with a comparable distribution. In comparison to the corresponding figures obtained in the case of horizontal handover over WLAN (Sect. 4.3), the overall handover time is increased by 159.1% and 198.9% for RO and BT, respectively. Once again, BT performed better (15.9%) on the total handover time.

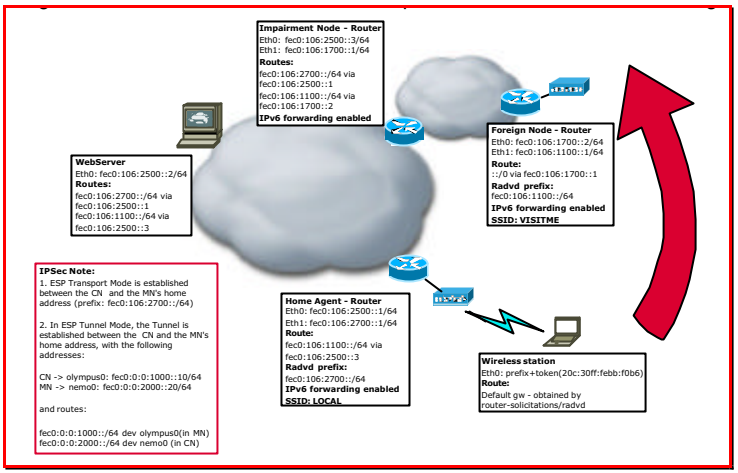

Fig. 5. Network Setup for WLAN/GPRS and WLAN/UMTS vertical handover.

This performance degradation was expected to some extent, because GPRS conditions have an increased round-trip-time (RTT) (700msec against the few msec of WLAN). Also its bandwidth is significantly reduced (e.g. from 5.5Mbps to 40kbps, on the download); so any communication arriving or leaving the MN will take significantly longer. The CoT and *next-TCP-packet*, increased in average from almost null values to 9% and 19% respectively. This reduces the percentage of impact that other parameters may have on handover, like RA, CoTI and BA which decreased by 20%, 5% and 3%, respectively.

Vertical handover in transport mode (Fig.7) resulted in RO with {min=4.65 sec; max=12.05 sec; avg=8.77 sec} and BT with {min=4.00 sec; max=9.91 sec; avg=7.56 sec}. In comparison to the corresponding figures obtained in the case of horizontal handover over WLAN (Sect. 4.3), the overall handover time is increased by 55.7%

[3] http://dast.nlanr.net/Projects/Iperf/

and 42.2% for RO and BT, respectively. The CoT and next-TCP-packet parameters have increased to about 12%. In BT mode, however, the impact of the different MIPv6 elements on the overall handover showed no significant changes (below 5% in all cases).

Vertical handover in tunnel mode (Fig.8) resulted in RO with {min=7.89 sec; max=19.36 sec; avg=14.91 sec}. In comparison to the corresponding figures obtained in the case of horizontal handover over WLAN (Sect. 4.3), the overall handover time is increased by 20.7%. The only difference is on the CoT which increased, on average form virtually 0% to 8.5%. This reduced the impact of the next-TCP-packet from 61.5 to 45%.

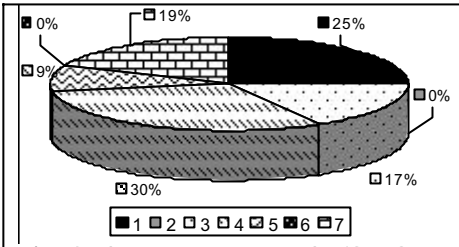

Fig. 6. Average times, WLAN/GPRS pure MIPv6.

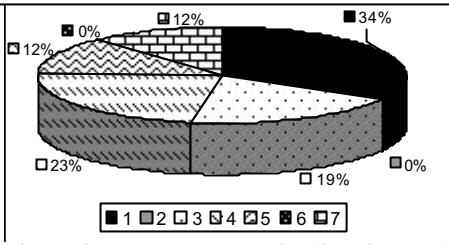

Fig. 7. Average times, WLAN/GPRS MIPv6 IPsec transport mode.

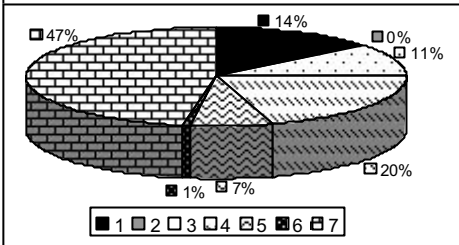

Fig. 8. Average times, WLAN/GPRS MIPv6 IPsec tunnel mode.

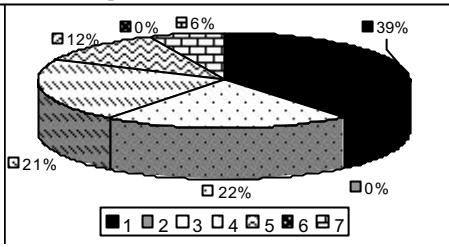

Fig. 9. Average times, WLAN/UMTS pure MIPv6.

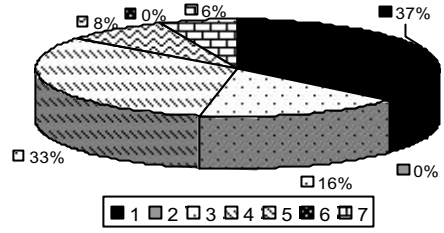

Fig. 10. Average times, WLAN/UMTS MIPv6 IPsec transport mode.

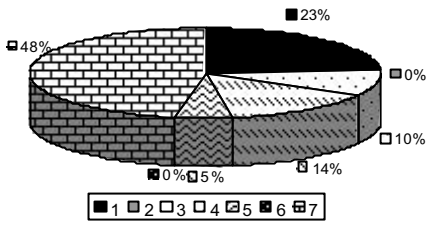

Fig. 11. Average times, WLAN/UMTS MIPv6 IPsec tunnel mode.

4.5 TEST 4: Vertical Handover between WLAN and UMTS

Aim

Validate and assess the functionality, stability and handover properties of our MVPN in a multi-access network including WLAN 802.11b and UMTS. The sample of

results presented herein is focused on the performance under vertical handover conditions.

Setup
The experimental setup is the same as the one involving GPRS (Sect.4.4) (Fig.5). The only difference was on the network conditions that were set to typical UMTS values. The conditions relating to the following results are: Upstream/Downstream Bandwidth = 128kbps; Round Trip Time = 500msec.

Results
A representative sample of results is illustrated in Figures 9-11. The total vertical handover times w.r.t. pure MIPv6 with RO were comprised between 2.93 and 11.39 sec with an average of 6.97 sec. Their distribution among individual factors is depicted in Fig.9. In the case of BT we obtained {min=4.15 sec; max=4.92 sec; avg=4.64sec}. The distribution of overheads is similar to those of GPRS (differences below 5%). The UMTS figures are comparable to the case of pure WLAN (Sect.4.3) (less than 1% difference) but significantly better than GPRS. Vertical handover in GPRS is on average 158.1% slower in RO and 200.5% slower in BT.

WLAN/UMTS Vertical handover in transport mode (Fig.10) resulted in RO with {min=5.07 sec; max=10.21 sec; avg=8.8 sec} and BT with {min=4.4 sec; max=10.18 sec; avg=7.7 sec}. The apparent slight performance degradation of UMTS was unexpected but can be entirely attributed to the WLAN. UMTS experiments were performed several months after their GPRS counterpart so it was difficult to obtain exactly the same conditions, given that we were using a WLAN shared by other users. Our study highlights, however, a strong similarity between the distribution of overheads of GPRS and WLAN. A closer look at the UMTS results indicates that MIPv6 elements traversing the network are the predominant factor. Besides RA, the average time to trigger CoTI is also critical (these two affect 60% of the handover time).

Finally, vertical handover in tunnel mode (Fig.11) resulted in RO with {min=7.49 sec; max=18.9 sec; avg=12.6 sec}. This places vertical UMTS handover between vertical GPRS handover and horizontal WLAN handover. This was expected, since the MIPv6 control packets incurred by the MN are beneficially affected by the better condition of UMTS. Our measurements help quantifying those differences. On average the proportion of next-TCP-packet is 49% (UMTS), 45% (GPRS) and 61.5% (WLAN). The overall handover time in UMTS in tunnel mode is on average 84.4% more efficient than GPRS.

5 Concluding Remarks and Recommendations

The integration exercise which has lead to the all-IP MVPN test-bed described herein, has helped assessing the level of maturity of IP technologies in relation to secure and mobile networking over multi-access networks. MIPv6 has only recently become an IETF RFC (July 2004); so relevant security-related studies are still on their early stages. IPv6 seems the obvious choice since 3GPP mandates its use for signaling interactions of IP and mobile communications. IPsec seems also the natural way to

support security not only because it is embedded in the IPv6 protocol stack but also, and most importantly, because of its ability to provide secure transport between end points without the need of pre-arrangements at network core. This is of special interest in mobile environments where the administrative overheads for traffic exchange between operators are always considerable.

In our testing environment, we reviewed IPv6, IPsec and MIPv6 first independently and, then, in combination as an MVPN solution. The work revealed some limitations. For instance IPsec tunnel mode failed to complete under MIPv6 BT and presented issues with MIPv6 RO too. However, all functional limitations can be overcome working on the source code.

The biggest shortcomings are, instead, performance related. These arise from the fact that MIPv6 expects handover between networks to trigger with layer-3 awareness of change. This has significant (negative) impact on time-sensitive applications, which suggests that there is scope for improvement by looking at ways to trigger handover prior to the interruption of layer-3 communication. Relevant efforts are already pursuing this direction but, at the time of writing, there are no publicly-available solutions. The handover figures presented in this article derive from an MIPL implementation. The fact that BT is faster than RO derives from the relative simplicity of the former. Nevertheless, BT was less reliable than RO.

We summarize below some recommendations for future development in the area:

- Further work is needed to ease the integration of IPSec tunnel mode with MIPv6. For example, by adjusting the routing table flushing procedure, vertical handover figures may significantly improve.
- The integration of virtual tunnel interfaces in mobile environments may significantly benefit from a re-design of the way MIPL overrides the source address of outgoing packets.
- Time-sensitive applications require fast-handover. It is imperative to provide alternatives to layer-3 based trigger mechanisms.
- Additional IPSec/MIPv6 network analysis tools are needed.
- IPsec moves part of the computation load away from the network into the terminal. It will be interesting to assess to which extent this can be sustained by thin mobile terminals.
- Our platform proved to be sufficiently stable to run applications over the MVPN. Next step is to perform tests on SIP (Session Initiation Protocol) over MVPN. SIP is an IETF protocol for handling multimedia sessions, now adopted by 3GPP in the context of the Intelligent Multimedia Subsystem (IMS). IMS allows mobile application over multi-access networks and is the standard of reference by network operators.

Acknowledgments

The equipment used to build the test-bed has been provided by Vodafone Group R&D, U.K who has also suggested the figures on typical GPRS/UMTS network conditions. Particular thanks go to N. Papadoglou, H. Zisimopoulos, and O. Gurleyen (all from Vodafone) who have provided feedback, suggestions, and insightful discussions during the whole project.

References

[1] Tanenbaum S.A. "**Computer Networks**", Prentice Hall, August 2002.

[2] Coppo, P. Dapos Ambrosio, M. Vercellone, V. CSELT, Torino; "**The A-VPN server: a solution for ATM virtual private networks**" Singapore ICCS '94. Conference Proceedings, 14-18 Nov 1994, Volume: 1, p. 298-304.

[3] Ferguson P., Huston G, "**What is a VPN**" The Internet Journal Volume 1(1), June 1998.

[4] Holmwood J., Reichert K, Feniak B., "**Providing Secure Access to Information Using the Internet**" USENIX Technical Program, August 2000.

[5] Schneyderman, A. and Casati, A "**Mobile VPN: Delivering Advanced Services in the Next Generation Wireless Systems**.", John Wiley & Sons, pp.1 – 352, December – 2002.

[6] Vesselin Tzvetkov, Erika Sanchez, "**Mobile Virtual Private Network**" <draft-tzvetkov-mvpn-01.txt> INTERNET-DRAFT Sheffield University 15 September 2000.

[7] Feder, P.M., Lee, N.Y., Martin-Leon, S., "**A Seamless Mobile VPN Data Solution for UMTS and WLAN Users**" Bell Laboratories - Mobility Solutions, Lucent Tech. Inc.

[8] Raouf Boutaba, "**On Managing Virtual Private Networks**" Computer Science Dept., University of Waterloo, IEEE Canadian Review - Winter 2002.

[9]Thrid Generation Partnership Project Release 5 www.**3gpp**.org/ftp/tsg_ran/TSG_RAN/TSGR_20/Docs/PDF/RP-030375.pdf

[10] 3RD Generation Partnership Project, **"Signaling flows for the IP multimedia call control based on SIP and SDP"**, 3GPP TS 24.228 v.5.6.0, pp. 7 – 816, September – 2003.

[11] Jhonson, D., Perkins, C., and Arkko, J. **"Mobility support in IPv6"** IETF RFC 3775, pp. 1 – 156, June – 2004.

[12] USAGI Project, **"Linux IPv6 Development Project"** p. 1, July – 2004. www.linux-ipv6.org (Accessed: 16 August 2004).

[13] KAME Project, **"KAME Project Home Page"**, pp. 1 – 2, August – 2004. www.kame.net (Accessed: 16 August 2004).

[14] Arkko, J., and others, "**Using IPSec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents**" IETF -ietf-mobileip-mipv6-ha-ipsec-06.txt, pp. 1-48, June 2003.

[15] Tuominen, A. and Petander, H. **"MIPL Mobile IPv6 for Linux in HUT Campus Network MediaPoli",** pp.1-6, July 2001. http://lwn.net/2001/features/OLS/pdf/pdf/mipl.pdf (Accessed: 16 August 2004).

[16] PDOS UCLA, **"The Click Modular Router Project"**, pp.1-4, July 2004. http://www.pdos.lcs.mit.edu/click/ (Accessed: 16 August 2004).

[17] Yoshifuji, H., Miyazawa, K., Nakamura, M., and Sekiya, Y. **"Compound Data Oriented Processing in USAGI IPv6 Stack"**, IEICE TRANS. ELECTRON., VOL.E87-C, NO.3 pp. 1- 6, March 2004.

[18] Mobile IP Linux (MIPL), **"Mobile IPv6 for Linux"**, May 2004. www.mobile-ipv6.org (Accessed: 16 August 2004).

[19] Kanda, M., and others, **"USAGI IPv6 IPsec Development for Linux"**, pp.1-5, January 2004. http://hiroshi1.hongo.wide.ad.jp/hiroshi/papers/SAINT2004_kanda-ipsec.pdf (Accessed: 16 August 2004).

[20] Hamzeh, K., G. Singh Pall, W. Verthein, J. Taarud, and W. A. Little. "**Point-to-Point Tunneling Protocol—PPTP.**" draft-ietf-pppext-pptp-02.txt, July 1997. See also: http://www.microsoft.com/backoffice/communications/morepptp.htm

[21] Valencia, A., K. Hamzeh, A. Rubens, T. Kolar, M. Littlewood, W. M. Townsley, J. Taarud, G. S. Pall, B. Palter, and W. Verthein. "**Layer Two Tunneling Protocol 'L2TP**.'" draft-ietf-pppext-l2tp-10.txt, March 1998.

[22] Kent, S. and Atkinson, R. "**Security Architecture for the Internet Protocol**" IETF RFC 2401, pp. 3 – 66, November – 1998.