Towards Service Continuity in Emerging Heterogeneous Mobile Networks

Sandro Grech
Networking Laboratory,
Helsinki University of Technology
P.O. Box 3000, FIN-02015 HUT
sandro.grech@hut.fi

Abstract

There are indications that the next generation mobile communication systems will shift away from the traditional vertically integrated approach in system design and instead allow access to a set of services through a variety of heterogeneous access technologies. To some extent this transition is already taking place with the introduction of WLAN (IEEE 802.11) local access networks adjacent to traditional wide-area cellular access networks. This trend will continue as a new wave of emerging access technologies such as WiMAX (IEEE 802.16) are introduced. As each access technology is introduced to serve a niche in the cost/performance/coverage matrix, aggregation of access technologies enhances the value of the offered services by creating a utility of the aggregated access systems that is greater than the sum of the utilities of the individual silo access systems.

With the emergence of multimode mobile devices, the next step in the integration of heterogeneous mobile networks, i.e. inter-access service continuity, gains relevance. This paper reviews emerging heterogeneous access networks and their integration, and studies service continuity, including the relevance of Mobile IPv4 and Mobile IPv6 and other mobility solutions at, above, and below IP layer, in this context. The selected architecture is evaluated in a laboratory environment. The results are used to build up an analysis of the solution and draw up some conclusions.

1 Introduction

Up until release 5, the 3GPP specifications were limited to access technologies within 3GPP control. 3GPP first deviated from this trend with the introduction of the 3GPP-WLAN interworking work item in release 6. Together with High Speed Uplink Packet Access (HSUPA), IP Multimedia Subsystem (IMS) Phase 2 (which amongst other things, introduces access independence), Multimedia Broadcast Multicast Service (MBMS), and enablers for Push to Talk over Cellular (PoC), interworking with WLAN represents one of the main new features introduced in 3GPP release 6. By the time that work on 3GPP release 6 was starting, WLAN was gaining significant importance as a wireless access technology and 3GPP could not ignore its significance as a local-area complement to wide-area cellular packet access. 3GPP thus introduced WLAN access into the 3GPP architecture[1]. The 3GPP specifications do not set 3GPP specific requirements for the WLAN access systems, but instead rely on the existing functionality available in a typical WLAN access network based on IEEE 802.11 standards.

3GPP TR 22.934 [1] introduces six interworking scenarios, representing various levels of integration between WLAN and 3GPP networks. These scenarios are outlined next.

Scenario 1 – *Common Billing and Customer Care:* The subscriber receives one bill from the mobile operator for the usage of both 3GPP and WLAN services. This does not pose any new requirements on 3GPP specifications.

Scenario 2 – *3GPP system based Access Control and Charging*: Authentication, authorization and accounting for WLAN access are provided by the 3GPP system using (U)SIM credentials. After successful authentication, the subscriber is authorized to receive direct Internet access from the WLAN hot-spot.

Scenario 3 – *Access to 3GPP system PS based services*: This interworking scenario enables the subscriber to access 3GPP PS services e.g. IMS based services, instant messaging, presence based services, MBMS, and operator hosted corporate access, through WLAN.

Scenario 4 – *Service Continuity*: This scenario allows the services supported in scenario 3 to survive a change of access between WLAN and UTRAN/GERAN. The change of access may be noticeable to the end-user, but there will be no need for services to be re-established. Due to the different access network capabilities, there may be a change in service quality after the transition across access technologies.

Scenario 5 – *Seamless services*: This scenario provides seamless service continuity between the access technologies for the services supported in Scenario 3. This is achieved by minimizing aspects such as data loss

[1] The resulting stage 1 description can be found in 3GPP TR 22.934 [7], stage 2 description in 3GPP TS 23.234 [1] and stage 3 description in 3GPP TS 24.234 [2] and 3GPP TS 29.234 [3]

and break time during the switch between access technologies.

Scenario 6 – *Access to 3GPP CS Services*: This scenario allows access to services provided by the entities of the 3GPP Circuit Switched Core Network to be accessible over WLAN.

3GPP release 6 specifications cover the operation of scenarios 2 and 3. An overview of the resulting architecture is given in [27]. In a nutshell, scenario 2 uses EAP-SIM [19] or EAP-AKA [24] to allow a WLAN access network to use AAA infrastructure that interfaces with 3GPP Home Subscriber Servers (HSS) to authenticate and authorize a SIM- or USIM- enabled device to use access network's resources. Scenario 3 introduces a Packet Data Gateway (PDG) adjacent to the Gateway GPRS Support Node (GGSN) to allow secure access to private services in the operator's home network. The PDG is essentially an IPsec gateway that is used to establish a secure tunnel through the WLAN access network between the mobile device and the service domain. The IPsec tunnel is established, managed and thorn down using IKEv2 [14] with EAP-SIM [19] or EAP-AKA [24] methods. While scenario 2 is limited to public WLAN deployments, scenario 3 is generic enough so that it can be applied through any WLAN and non-WLAN access network. Work on further interworking scenarios will be taken up in 3GPP release 7.

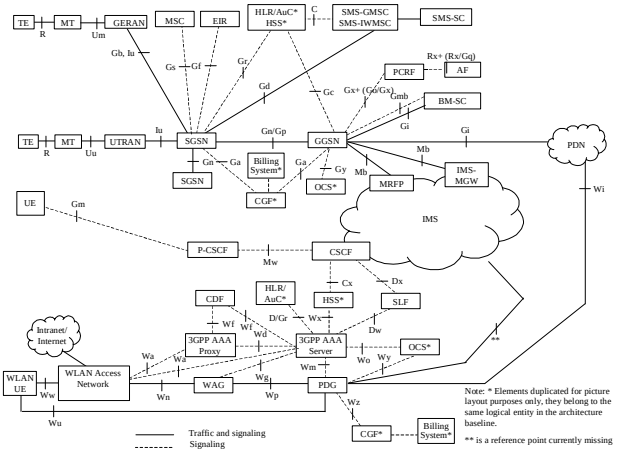

Figure 1: 3GPP Release 6 logical architecture [2]

In this paper we start by studying the motivation for service continuity across heterogeneous mobile networks. We focus the paper to 3GPP-WLAN interworking in particular. We present alternative approaches addressing mobility across cellular and WLAN. We then proceed to introduce the role of Mobile IPv4, Mobile IPv6 and other mobility solutions at or above IP and we propose an architecture based on the selected building blocks. In order to evaluate the functionality, issues and performance of the selected architecture we build a laboratory testbed, and we present an analysis based on the results observed from the testbed.

2 Motivation and problem space

Besides the 3GPP-WLAN interworking work item in 3GPP[2], which was initially mostly focused on the integration of 3GPP access systems with public WLAN networks, there have been other recent interest in other industry fora in utilizing non-cellular networks to access a common set of communication services. The European Telecommunications Standards Institute (ETSI) and the Alliance for Telecommunications Industry Solutions (ATIS) are in the progress of specifying the access to communication services based on the IMS[3] specified in the 3rd Generation partnership Project (3GPP), through residential networks. The work in ETSI and ATIS, known as Next Generation Networks (NGN) focuses primarily on fixed residential access based on ADSL or cable. However, as the penetration of residential WLAN access continues to increase, a more interesting variant of the technology will be access of IMS services through residential WLAN. Even further, it should be possible to avid disruption of the multimedia services (including VoIP) when a multimode mobile device switches across cellular and WLAN accesses. This is exactly the topic that is investigated in this paper. Providing communication services via the IMS platform is however not the only possible approach. Some operators have seen an opportunity gap for providing a solution, known as Unlicensed Mobile Access (UMA), based on the more traditional circuit-switched mobile communication systems, at least until the other solutions are mature enough and provide enough added benefit to justify the transition.

2.1 The Unlicensed Mobile Access

Mobile communication systems based on cellular technologies have gained widespread popularity during the past decade, and in most developed countries their availability has become ubiquitous. However, in some countries, such as the United States, it has turned out to be difficult to support adequate indoor coverage using cellular systems [38].

In response to this shortcoming, several industry players have formed a consortium to specify access to GSM and GPRS services over unlicensed radio technologies, such as Bluetooth and IEEE 802.11 Wireless LANs. The specifications resulting from the Unlicensed Mobile Access (UMA) consortium have been recently published [39]–[41], and deployment of the first commercial systems based on these specifications is expected shortly. The standardization work is continued by the 3rd Generation Partnership

[2] There is a similar work ongoing also in 3GPP2 for integration of CDMA-2000 and IEEE 802.11 networks

[3] Note that the IMS is in turn based on the Session Initiation Protocol (SIP) specified in the Internet Engineering Task Force (IETF)

Project (3GPP), under the "Generic access to the A/Gb interface" work item [6]–[8].

Figure 2 illustrates the basic principle behind the UMA solution. The existing cellular network remains unmodified, and a new network element, the UMA Network Controller (UNC), is introduced. The UNC acts as a gateway between the mobile operator core network and Internet or a broadband IP access network such as ADSL or cable. The phone connects to the IP network using a standard WLAN or Bluetooth access point.

UMA does not introduce any changes to the existing cellular network. The new network element, UMA Network Controller (UNC) acts as a gateway between the IP side (typically consisting of a customer-owned WLAN access point and an ADSL/cable based broadband access network) and the cellular core network. The UNC is connected to the core network using the same A/Gb interface as GSM base station controllers (BSCs). The protocols stacks resemble traditional voice-over-IP solutions, except that GSM signaling protocols are used instead of SIP or H.323. The main advantages of using the existing GSM protocols and services are easier deployment (for existing GSM operators) and the ability to perform mobility between GSM and UMA during a call. UMA also supports access to GPRS packet switched services. The protocol stacks are similar as for circuit switched case, replacing the lower layers from GPRS radio with IP.

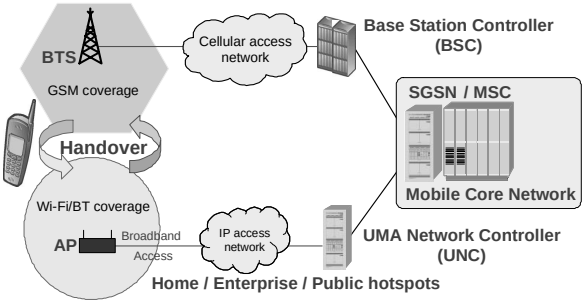

Figure 2: Unlicensed Mobile Access Architecture

3 Solution space and proposed architecture

UMA represents a tight interworking of unlicensed and cellular protocols. UMA achieves mobility across unlicensed and cellular access, since in the UMA architecture WLAN is abstracted as a carrier for cellular protocols and mobility across BSC and UNC is treated like a traditional inter-BSC handover by the cellular mobility management protocols. When considering loose interworking between WLAN and cellular, as is the case in 3GPP-WLAN interworking and NGN, mobility across cellular and WLAN turns out to be a problem of IP address portability across access networks. The problem associated with the dual role of an IP address acting as both an identifier and a locator can be solved in various ways:

- utilizing a transport protocol that does not use IP address as an identifier (e.g. TLS [37] or DTLS [17]), or allows recovery from a change in underlying IP address (e.g. SCTP [31])
- solving the problem where it occurs, i.e. at the IP layer by introducing a virtual link with an associated static or semi-static IP address that hides IP address changes associated with the physical links from the layers above IP. This is the approach taken by Mobile IPv4 [15] and Mobile IPv6 [16], [25].
- introducing an intermediate layer between network and transport layers that isolates transport protocols from the changes happening at the IP layer by introducing a static cryptographic host identifier. The Host Identity Payload (HIP [30]) protocol provides such a solution through which the IP address retains only one of its functions, i.e. that of a locator.

TLS and DTLS are security protocols operating at the transport layer, but neither of them are yet widely adopted end-to-end. Thus, a solution based uniquely on the assumption that (D)TLS will be used would require the introduction of (D)TLS proxies or gateways with the primary interest of enabling mobility – which is not a good approach. In addition, (D)TLS protection would need to be applied over all access technologies including those that are considered already secure, for example through robust layer 2 encryption, as is the case in current cellular systems.

HIP provides an interesting approach for host mobility. Its main advantage is that security and mobility have been tightly integrated, and whereas Mobile IP can be seen as a fix to the current host mobility problem, HIP introduces a more elegant long-term solution by fixing the problem at the root cause. However, HIP assumes that both communicating endpoints support the protocol layer between network and transport layer. Also, the socket API needs to be adapted to the use of the new host identities, and consequently all applications that use the socket API need to be patched. Consequently, at least in the shorter term, the applicability of HIP is limited to closed deployment environments, such as a mobile sensor network, where requirements can be set on both communication endpoints. As HIP matures and gains wider deployment we will probably start to see devices that support both HIP and traditional TCP/IP stacks, such that two communicating parties can first try to negotiate the operation of HIP, and subsequently use Mobile IP, if the operation fails. However, there will be a long time-span until HIP will be implemented in a sufficient number of devices such that it can be

considered a stand-alone solution in a wide deployment scenario such as the Internet.

This leads us to the conclusion that we need to look at a mobility solution at layer 3. Building on top of 3GPP-WLAN scenario 3 interworking represents the full stretch of the problem space. In addition to basic inter-access service continuity, building on top of scenario 3 requires operation across and within security domains where IPsec needs to be dynamically enabled, disabled or maintained, according the to the requirements set by the source and target domain. This problem has been studied in IETF in [18] and a solution is proposed in [36]. The latter essentially proposes two layers of Mobile IP, one above, and one below IPsec. We argue that this approach is unnecessary complex and bears too much overhead, at least for the deployment scenario considered in this paper. Instead we propose to use Mobile IP only when crossing access boundaries, whereas IP address changes that may occur while the mobile device is using IPsec can be handled using the IKE mobility extensions that are being specified in the IETF MobIKE working group [23]. Such changes in IP address would occur for example if the mobile device is roaming across a large WLAN domain that spans multiple IP subnets.

3.1 IP version considerations

Ultimately, the IMS was specified as an IPv6 platform, since it was originally limited to the cellular domain. However, the introduction of residential access, which cannot be guaranteed to always support IPv6, leads to the requirement that IPv4 also needs to be supported. In addition there may be also other services, besides IMS that would be accessible through multiple access technologies. Consequently, an inter-access mobility solution is needed for IPv4-only and dual-stack devices across IPv4 and IPv6 access networks and for IPv4 and IPv6 services. Wile the IKEv2 mobility extensions exhibit the property of being IP version agnostic, i.e. both IPv4 and IPv6 address updates can be carried out, including transitions across IP versions, Mobile IP operation is limited within an IP version. Consequently, the selected solution must include both Mobile IPv4 and Mobile IPv6. This topic is discussed further in section 3.4.

3.2 Procedures

This section covers the mobility procedures in more detail with the aid of signaling flow diagrams. The high-level overall view is illustrated in Figure 3. The mobile device first gains IP connectivity in one of the access technologies (step 1.1), i.e. through a PDP context activation in (E)GPRS/WCDMA or DHCP, or some other mechanism in WLAN. This step may already include an authentication sequence. Following this, the mobile device may need to establish an IPsec tunnel towards the PDG (step 1.2), if the nature of the communication is sensitive and the path towards the service domain cannot be trusted. This is typically the case when accessing 3GPP services through WLAN[4]. At some point in time, the mobile device needs to change IP address, for example due to a change in access technology (step 2). Before being able to perform Mobile IP operations, the mobile device needs to be provisioned with the necessary parameters (step 3), if these are not yet available or are about to expire. The detailed procedures are presented in sections 3.2.1 - 3.2.3 Finally the mobile device can engage in mobility procedures using standard Mobile IP (step 4) or IKEv2 mobility procedures (step 5), depending on the security domain. IKEv2 mobility procedures are discussed in more detail in section 3.2.4.

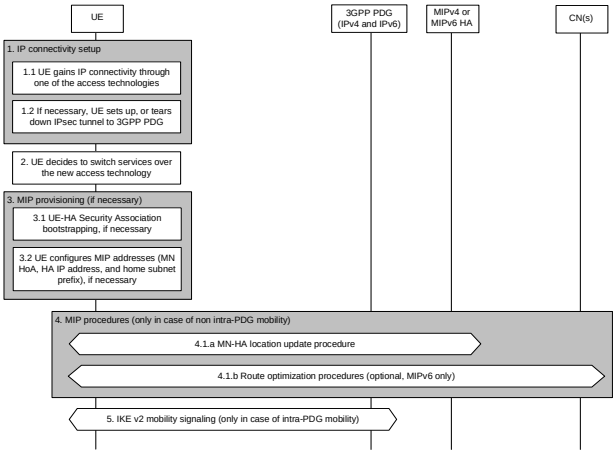

Figure 3: Master signaling flow diagram

3.2.1 Security association bootstrapping

Both Mobile IPv4 and Mobile IPv6 require a mobility security association between the Mobile Node and the Home Agent. This security association is based on a shared key, or in the case of Mobile IPv6, also a subscriber certificate is possible. Bootstrapping these security associations needs to be automated in order to facilitate deployment and usability. 3GPP has specified a general authentication and key distribution solution called Generic Authentication Architecture (GAA), in release 6 [9]. Using GAA, a shared symmetric key, identified with a bootstrapping transaction identifier (B-TID), can be provisioned to USIM-enabled device using USIM authentication. The bootstrapping operation is carried out between the mobile device and a Bootstrapping Function (BSF) using HTTP Digest AKA [13]. A Network Application Function (NAF) verifies the credentials supplied by the client by communicating with the BSF using the DIAMETER protocol. This framework fits very well the purpose required for

[4] Note that the WLAN link can be rendered secure through Wi-Fi Protected Access (WPA) or IEEE 802.1i [33], however the path between the WLAN access network and the service domain may not always be trusted.

bootstrapping the mobility security associations in the context studied in this paper, assuming that all the relevant mobile device are USIM-enabled. The resulting signaling flow is illustrated in Figure 4.

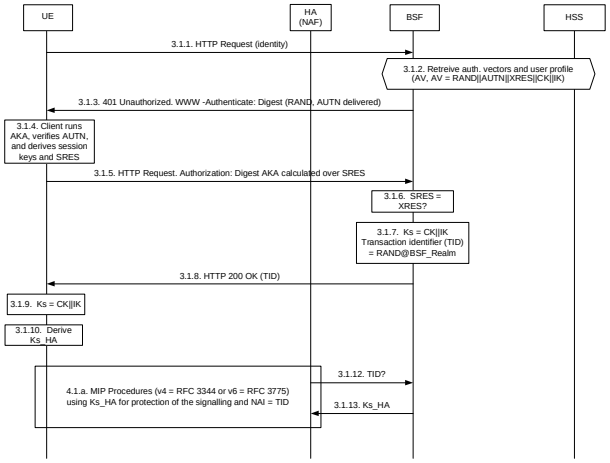

Figure 4: Security association bootstrapping

3.2.2 Mobile IPv4 address autoconfiguration

IP address configuration is typically automated using dynamic mechanisms such as DHCP. Besides the on-link care-of address which can be autoconfigured using one of the traditional mechanisms, a mobile IPv4 device, however, needs to configure also a Home IP address. The autoconfiguration must work also if the mobile device is off-link. In addition, the mobile device needs to discover the IP address of the Home Agent. We propose that well-known identifiers are specified for Mobile IP service, such that DNS can be used to map the HA identity into the corresponding IP address. A new DNS SRV record [12] for Mobile IP may be most appropriate for this purpose. For the Home IP address autoconfiguration we re-use the null-home-address procedure, originally adopted by 3GPP2 in [11]. Figure 5 illustrates the co-located mode of operation. This mode of operation is particularly relevant since when the mobile device transits into a WLAN access network without using an IPsec tunnel we can be almost sure that there is no Mobile IPv4 Foreign Agent deployed.

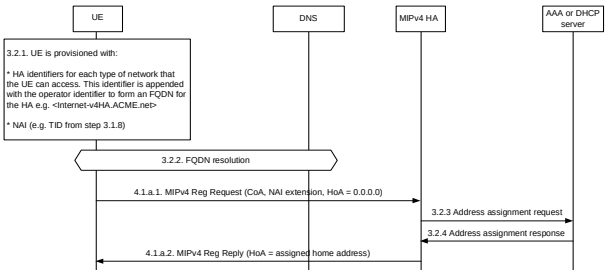

Figure 5: Mobile IPv4 address autoconfiguration

3.2.3 Mobile IPv6 address autoconfiguration

The requirements for Mobile IPv6 autoconfiguration are essentially identical to those discussed in section 3.2.2 for Mobile IPv4. In Mobile IPv6, the Home IP address autoconfiguration is best handled using IKEv2 configuration payloads as proposed in [42], and illustrated in step 3.2.4 in Figure 6.

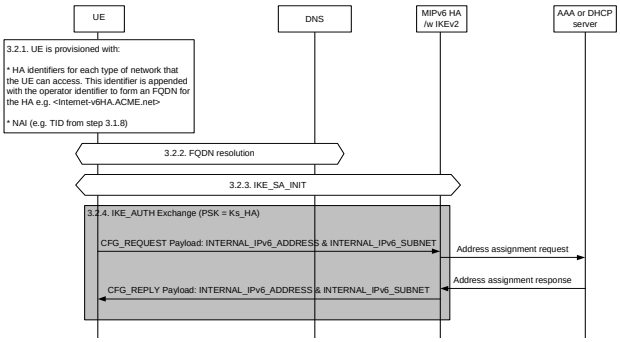

Figure 6: Mobile IPv6 address autoconfiguration

3.2.4 IKEv2 mobility procedures

The IKEv2 mobility procedures avoid the need to support a Mobile IP layer below IPsec. The protocols for this are being developed by the MobIKE WG in IETF [23]. The basic procedure relevant for the purpose of this paper is fairly straightforward and is illustrated with the aid of Figure 7 with reference to [28].

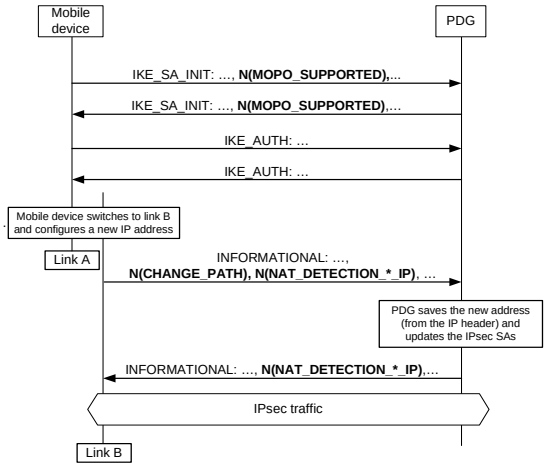

Figure 7: IKEv2 mobility operation

3.3 Performance optimizations

So far we have discussed only the co-located mode of operation for Mobile IPv4. This is due to the fact that we cannot always be guaranteed that a Foreign Agent is available in a WLAN access network – indeed it will most likely not. In order to reduce tunneling overhead inherent with the co-located mode of Mobile IPv4

operation, however, a Mobile IPv4 Foreign Agent can be co-located with the GGSN and PDG for (E)GPRS/WCDMA and WLAN scenario 3 access respectively. This kind of optimization is however not possible in Mobile IPv6. We thus argue that tunneling overhead is best handled using IP header compression techniques at overhead sensitive links such as cellular air interfaces. In principle, it is also possible to assign one of the access links to represent the Mobile IP home link (applies for both Mobile IPv4 and Mobile IPv6), such that no tunneling overhead is incurred over that particular link. We argue, however, that this should be left as a deployment option, and not as a design criterion.

3.4 Operation across IPv4 and IPv6 access networks

We have already addressed the motivation behind the need of supporting both Mobile IPv4 and Mobile IPv6 in section 3.1. This is unfortunate, but cannot be easily avoided. The dual nature of IP versions however raises an important issue, i.e. the how to support mobility across access networks with different IP versions. For this we need to assume a dual-stacked mobile device, and we will assume that Mobile IPv6 will be selected by default. The question then boils down to how does the mobile device behave when it encounters an IPv4 access network. The straightforward approach is to treat this as a classic IPv4-IPv6 transition problem and utilize one of the mechanisms developed in that space. This is a possible approach, however there is also a second approach that assumes that the Mobile IPv6 Home Agent is dual-stacked and can bind IPv4 care-of addresses to IPv6 home addresses and decapsulate IPv6-over-IPv4 tunnels. This approach is proposed in [32] and [20].

4 Evaluation

After presenting the proposed architecture for (E)GPRS/WCDMA-WLAN service continuity, we now proceed to evaluate the availability, complexity, stability, QoS impact and performance of the solution. We perform this evaluation by setting up the testbed as illustrated in **Figure 8**.

We limit the testbed to the most basic operation, i.e. we do not yet support access using 3GPP-WLAN scenario 3 interworking (and consequently we do not evaluate IKEv2 mobility extensions). Also, the mobile device is manually configured with the Mobile IP home address, Home Agent IP address, and mobility security association parameters. The testbed supports IPv4 and IPv6 operation in isolation (i.e. the mechanisms in section 3.4 are not evaluated).

For Mobile IPv4 we use a laptop with WLAN/(E)GPRS/WCDMA PCMCIA cards running a Mobile IPv4 client[5] on a WIN2k platform. The Mobile IPv6 counterpart is a Symbian OS plugin running on top of the Nokia 9500 (E)GPRS/WLAN terminal. The Home Agent for both Mobile IPv4 and Mobile IPv6 are the implementations from Helsinki University of Technology [21], [22].

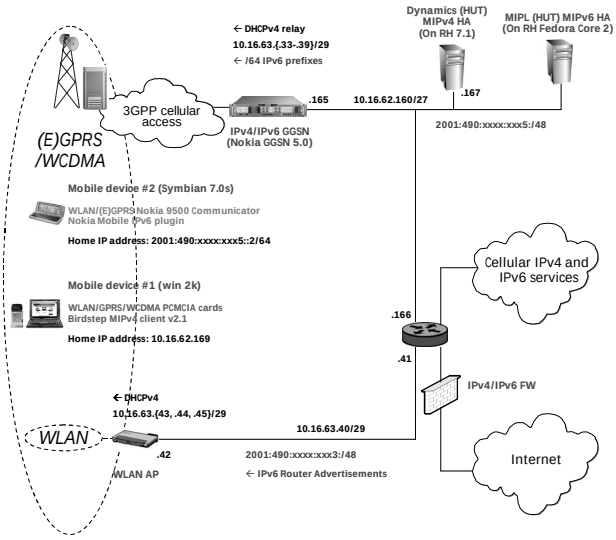

Figure 8: 3GPP-WLAN mobility testbed

4.1 Results

We are particularly interested in the service continuity performance characteristic of the selected solution. In order to represent the results graphically we used a custom made tool that generates a continuous stream of packets and monitors the reception at the receiving end[6]. The results are illustrated for GPRS/WLAN and WCDMA/WLAN mobility in **Figure 9** and **Figure 10**, respectively.

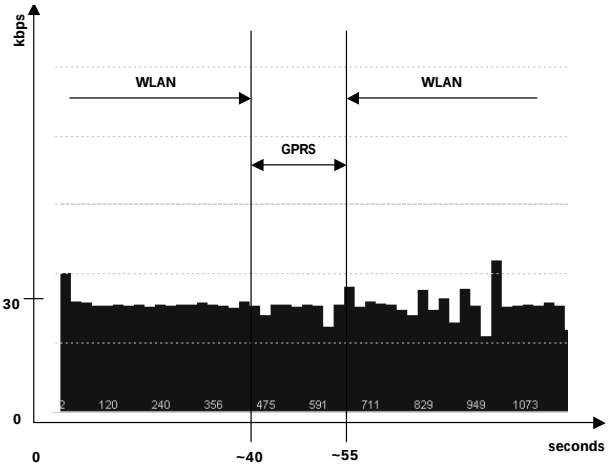

Figure 9: GPRS/WLAN Service continuity performance

[5] The Mobile IPv4 client is an evaluation version of the Intelligent Mobile IP client from Birdstep Inc.

[6] It was not possible to make use of traditional packet capture tool such as Ethereal, since these did not recognize the (E)GPRS/WCDMA driver.

These results were generated using physical mobility of the mobile device, and represent the typical performance observed after repeating the test several times by moving in different directions and around different obstacles. The plots illustrate results for 30kbps streams, characteristic of VoIP applications.

The results indicate that smooth transitions (i.e. no packet loss and no latency) across (E)GPRS and WLAN are achievable with one important condition. In these measurements we have maintained an active PDP context on the cellular side even while the mobile device is using WLAN. This PDP context does not consumer cellular resources, but facilitates a faster transition back to cellular access, when needed. From the cellular perspective the mobile device is inactive while it is using WLAN. The Traffic Block Flow establishment procedure is the only signaling that is required before the mobile device can start sending and receiving user-plane data over the (E)GPRS link. The latency incurred by this procedure is small enough not to cause any noticeable degradation to the performance of the transition.

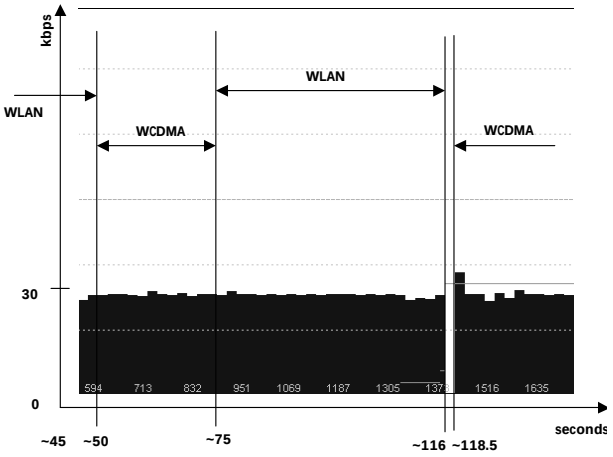

Figure 10: WCDMA/WLAN Service continuity performance

Similar results are obtained for transitions across WCDMA and WLAN. These are illustrated in Figure 10. In this case the transitions from WCMA to WLAN are also smooth, but transitions from WLAN to WCDMA incur a small outage period of about 2.5 seconds. This result is studied in more detail in section 5.

5 Analysis and Discussion

From the Evaluation carried documented in section 4, we conclude that the necessary technology for vertical handoffs utilizing Mobile IPv4 and Mobile IPv6 is available in the open source community and increasingly in commercial products. No significant complexities or challenges were encountered in deploying the testbed.

The first multi-radio commercial products that can effectively make use of vertical handoffs have just recently reached commercial adoption. Widespread deployment of the solutions requires further system level specification from standards bodies such as 3GPP(2).

Next we analyze some of the performance considerations in more detail.

5.1 Transition outage

One of the issues identified in section 4.1 is the transition outage during transitions from WLAN towards WCDMA. This can be explained with the help of Figure 11, which illustrates the WCDMA UE Modes and RCC states in Connected Mode [10]. CEL_DCH is the state in which a continuous stream of packets can be sent and received in the steady state. The limited resources associated with the CEL_DCH state are released after a configurable inactivity timer elapses.

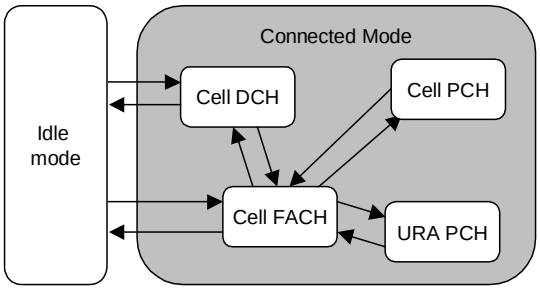

Figure 11: WCDMA UE Modes and RCC states in Connected Mode

Figure 12 illustrates the observed inactivity timers are state transition delay in the live network. While the mobile device is using WLAN, the inactivity timer in WCDMA will start running, consequently the RRC state machine will cause the mobile device to release any dedicated resources. In turn, this will cause some delay in recovering these dedicated cellular resources when WLAN coverage is lost.

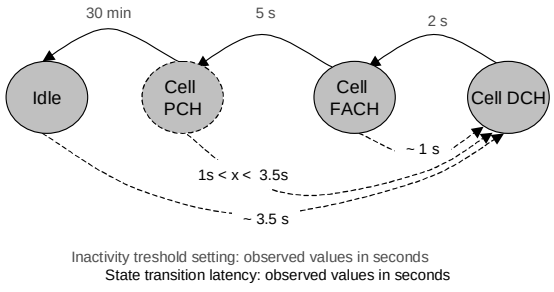

Figure 12: WCDMA RRC transition state diagram

5.2 TCP considerations

The impact of vertical handoffs on TCP performance have been studied for e.g. in [26]. For the first time we were now able to verify these results on a live network.

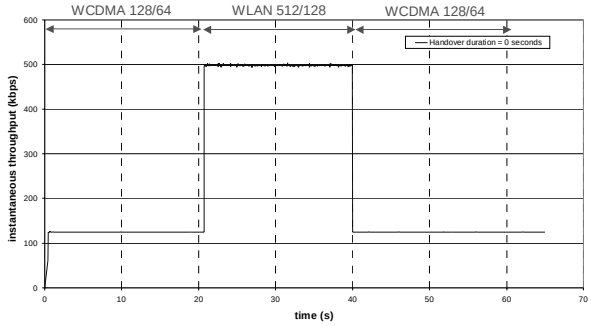

Figure 13: TCP performance during WCDMA/WLAN mobility with no outage during system transition

The results depicted in Figure 13 representing a smooth handoff across WCDMA and WLAN indicate that any artifacts related to a the sharp change in link bandwidth-delay product does not lead to any practically significant deterioration in TCP performance.

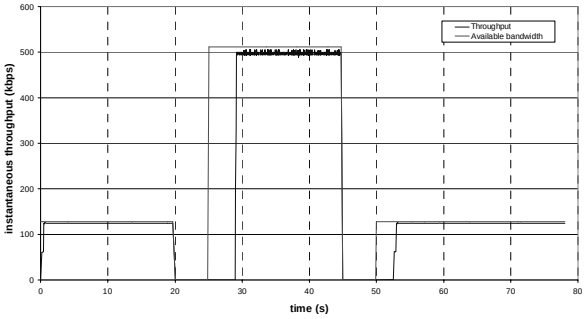

Figure 14: TCP performance during WCDMA/WLAN mobility with 5s outage during system transition

Figure 14 illustrates the same results, but for 5 seconds outage during the inter-system transition. In this case we can observe that TCP takes some time to recover from the transition. This is attributed to the TCP sender backoff algorithm. As highlighted in **Figure 15**, after link B goes up again after 5 s outage, it will take some time till the TCP sender starts re-transmitting from the last unacknowledged segment.

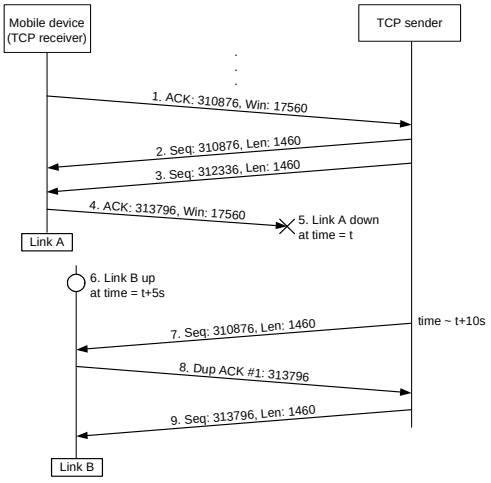

Figure 15: TCP packet trace

6 Conclusions

The first commercial multi-radio capable mobile devices have just recently been launched into the market. In order to maximize the utility of such devices there is a need to ensure that mobile device is always connected through the best suited access technology given a set of parameters such as availability of access technologies in a specific location, and the services being consumed. In order to avoid disrupting services during transitions across access technologies an inter-access device mobility solution is required.

While there are various ways on how to fulfill this requirement, Mobile IP is seen to be most suited for the deployment scenario considered in this paper. As layers above IP that are resilient to IP address changes gain deployment the role of Mobile IP will start to diminish. In the meantime solutions for inter-access mobility below IP have also been specified, for example in UMA. These solutions are based on tight-interworking between access technologies, and arguably represent short term solutions since they are based on legacy voice-centric circuit-switched communication infrastructure. Solutions based on IMS will enable a new wave of multimedia communication services, however some functionality such as inter-access service continuity is still missing. Providing a solution for this has been subject of this paper.

We argue that this gap is best filled with Mobile IP. We propose, evaluate and analyze an architecture based on this recommendation. We observe that despite the fact that a lot of effort has been invested to optimize the Mobile IP handoff performance in IETF, much of this effort has been focused on Layer 3 and consequently access-agnostic. We note that access layer characteristics have significant effect on the performance on inter access service continuity.

References

[1] 3rd Generation Partnership Project (3GPP), "Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) Interworking", TR 22.934 v6.2.0, September 2003.

[2] 3rd Generation Partnership Project (3GPP), “3GPP system architecture evolution: Report on technical options and conclusions”, work in progress, TR 23.882, April 2005.

[3] 3rd Generation Partnership Project (3GPP), “3GPP System to Wireless Local Area Network (WLAN) Interworking: System Description”, 3GPP TS 23.234 v6.3.0, December 2004.

[4] 3rd Generation Partnership Project (3GPP), “3GPP system to Wireless Local Area Network (WLAN) Interworking; User Equipment (UE) to network protocols; Stage 3”, 3GPP TS 24.234 v6.2.0, March 2005.

[5] 3rd Generation Partnership Project (3GPP), “3GPP system to Wireless Local Area Network (WLAN) Interworking; Stage 3”, 3GPP TS 29.234 v6.2.0, April 2005.

[6] 3rd Generation Partnership Project (3GPP), “Feasibility Study on Generic Access to A/Gb Interface”, TR 43.901, Aug. 2004.

[7] 3rd Generation Partnership Project (3GPP), “Generic Access to the A/Gb interface; Mobile Generic Access Interface Layer 3 Specification”, work in progress, TS 44.318, Jan. 2005.

[8] 3rd Generation Partnership Project (3GPP), “Generic Access to the A/Gb interface; Stage 2,” work in progress, TS 43.318, Jan. 2005.
[9] 3rd Generation Partnership Project (3GPP), “Generic Authentication Architecture; Generic Bootrsapping Architecture”, 3GPP TS 33.230.
[10] 3rd Generation Partnership Project (3GPP), “Radio Resource Control (RRC) protocol specification”, TS 25.331.
[11] 3rd Generation Partnership Project 2 (3GPP2), “cdma2000 Wireless IP Network Standard: Simple IP and Mobile IP Access Services”, X.S0011-002-C v1.0, Nov. 2003.
[12] A. Gulbrandsen, P. Vixie, and L. Esibov, “A DNS RR for specifying the location of services (DNS SRV)”, IETF RFC 2782, Feb. 2000
[13] A. Niemi, J. Arkko, V. Torvinen, ” Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)”, IETF RFC 3310, Sept. 2002.
[14] C. Kaufman, "Internet Key Exchange (IKEv2) Protocol", work in progress, IETF draft-ietf-ipsec-ikev2-17, Oct. 2004.
[15] C. Perkins (ed.), "IP Mobility Support for IPv4", IETF RFC 3344, August 2002.
[16] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", IETF RFC 3775, June 2004.
[17] E. Rescorla, M. Modadugu, “Datagram Transport Layer Security”, work in progress, IETF draft-rescorla-dtls-04, April 2004.
[18] F. Adrangi et al., “Problem Statement and Solution Guidelines for Mobile IPv4 Traversal Across IPsec-based VPN Gateways”, work in progress, IETF draft-ietf-mobileip-vpn-problem-statement-guide-03, Oct. 2004
[19] H. Haverinen and J. Salowey, “Extensible Authentication Protocol method for GSM Subscriber Identity Modules (EAP-SIM)”, work in progress, IETF draft-haverinen-pppext-eap-sim-16, Dec. 2004.
[20] H. Soliman, “Dual Stack Mobile IP”, work in progress, IETF draft-soliman-v4v6-mipv4-01, Oct. 2004.
[21] Helsinki University of Technology: Dynamics Mobile IPv4 implementation from Helsinki University of Technology. Available at: http://dynamics.sourceforge.net/ (Refereed April 2005).
[22] Helsinki University of Technology: MIPL –Mobile IPv6 for Linux. Available at: http://www.mobile-ipv6.org/ (Referred April 2005)
[23] IETF IKEv2 Mobility and Multihoming (MOBIKE) Working Group, available at: <http://www.ietf.org/html.charters/mobike-charter.html>, Referred May 2005.
[24] J. Arkko and H. Haverinen, “EAP AKA Authentication”, work in progress, IETF draft-arkko-pppext-eap-aka-13, Dec. 2004.
[25] J. Arkko, V. Devarapalli, F. Dupont, “Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents”, IETF RFC 3776, June 2004.
[26] J. Poncela, S. Grech, P. Serna, "An Analysis of TCP Behaviour during Wireless to Cellular Handovers". In proceedings of the 2nd International Conference on Communications, Internet, and Information Technology, (CIIT) 2003, Scottsdale, USA. November 17-19, 2003.
[27] K. Ahmavaara, H. Haverinen, and R. Pichna, “Interworking architecture between 3GPP and WLAN systems,” IEEE Communications Magazine, vol. 41, no. 11, pp. 74–81, Nov. 2003.
[28] P. Eronen, “Mobility Protocol Options for IKEv2 (MOPO-IKE)”, work in progress, IETF draft-eronen-mobike-mopo-02, Feb. 2005.
[29] R. Mononen, S. Grech, "Location Privacy in Mobile IPv6". In proceedings of the 3rd International Workshop on Wireless Information Systems (WIS-2004), Porto, Portugal. April 14-17, 2004
[30] R. Moskowitz, P. Nikander, P. Jokela, T. Henderson, “Host Identity Protocol”, work in progress, IETF draft-ietf-hip-base-02, Feb. 2005.
[31] R. Stewart et al., “Stream Control Transmission Protocol”, IETF RFC 2960, October 2000.
[32] R. Wakikawa, V. Devarapalli, C. E. Williams, ”IPv4 care-of address registration”, work in progress, IETF draft-wakikawa-nemo-v4tunnel-01, Aug, 2004.
[33] S. Grech, J. Nikkanen, "A Security Analysis of Wi-Fi Protected Access". In proceedings of the 9th Nordic Workshop on Secure IT-systems (Nordsec), Otaniemi, Finland. November 4-5, 2004
[34] S. Grech, J. Poncela, P. Serna, "An Analysis of Mobile IPv6 Signaling Load in Next Generation Mobile Networks". In proceedings of the 6th IFIP IEEE International Conference on Mobile and Wireless Communication Networks (MWCN), Paris, France. October 25-27 2004
[35] S. Grech, P. Eronen, “Implications of Unlicensed Mobile Access (UMA) for GSM security”, submitted to the first IEEE/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks.
[36] S. Vaarala and E. Klovning, “Mobile IPv4 Traversal Across IPsec-based VPN Gateways”, work in progress, IETF draft-ietf-mip4-vpn-problem-solution-01
[37] T. Dierks, C. Allen, “The TLS protocol version 1.0”, IETF RFC 2246, Jan. 1999.
[38] T. Rappaport, A. Annamalai, R. Buehrer, and W. Tranter, “Wireless communications: past events and a future perspective,” IEEE Communications Magazine, vol. 40, no. 5, pp. 148–161, May 2002.
[39] UMA Consortium, “Unlicensed Mobile Access (UMA) Architecture (Stage 2),” R1.0.0, Technical specification, available from http://www.umatechnology.org/specifications/index.htm, Sept. 2004.
[40] UMA Consortium, “Unlicensed Mobile Access (UMA) User Perspective (Stage 1),” R1.0.0, Technical specification, available from http://www.umatechnology.org/specifications/index.htm, Sept. 2004.
[41] UMA Consortium, “Unlicensed Mobile Access (UMA) User Protocols (Stage 3),” R1.0.0, Technical specification, available from http://www.umatechnology.org/specifications/index.htm, Sept. 2004.
[42] V. Devarapalli, “Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture”, work in progress, IETF draft-ietf-mip6-ikev2-ipsec-01, Feb. 2005.