Towards Always Best Connected Multi-Access: the MULTINET Approach

Qi Wang[1], Robert Atkinson[2], John Dunlop[3]

Mobile Communications Group, Department of Electronic and Electrical Engineering
University of Strathclyde, Glasgow G1 1XW, UK

[1]qwang@eee.strath.ac.uk
[2]r.atkinson@eee.strath.ac.uk
[3]j.dunlop@eee.strath.ac.uk

***Abstract*— The next-generation wireless networks are envisioned to provide an Always-Best-Connected (ABC) paradigm for mobile users who can access to multiple networks simultaneously. Thus, the design and evaluation of practical ABC multi-access systems are gaining increasing importance. The EU MULTINET architecture aims at advanced policy-based multi-access support for nomadic users roaming with a personal area network. In this paper, we present the design, implementation, validation and evaluation of the MULTINET approach towards realising the ABC concept.**

I. INTRODUCTION

Concurrent access to multiple wireless networks has become a reality for end users whose terminals are equipped with multi-radio interfaces. Such users expect to be Always Best Connected (ABC) to enjoy their multimedia applications with their subscribed Quality of Service (QoS) [1]. The EU IST Framework 6 project MULTINET concentrates on policy-based multi-access support architecture that is aware of QoS enabled by intelligent network selection algorithms. The primary user scenario is targeted to nomadic workers who roam to a visited site for high-tech machinery maintenance. Such a worker is travelling with a Personal Area Network (PAN) composed of a set of communication devices that are managed by a Personal Gateway (PG).

Providing mobility to a PAN is supported by the IETF Network Mobility (NEMO) protocol [2]. NEMO is an extension to Mobile IPv6 (MIPv6) [3], which is the de facto standard IPv6 mobility management protocol for single mobile nodes. In MIPv6, a mobile node is known by its long-term Home Address (HoA) obtained from its home network; when visiting foreign networks it obtains and registers a Care-of Address (CoA), bound to the HoA, with its Home Agent (HA) and optionally with its correspondent nodes (CNs) if the Route Optimization is enabled. NEMO extends MIPv6 to handle the mobility of an entire moving network such as a PAN through mobile routers. To enable multi-access, multiple CoAs are allowed to be bound with a single HoA [4]. Policy-based flow distribution mechanisms [5][6] are also being investigated in the IETF although further design, implementation and evaluation are still needed. The MULTINET architecture further extends and integrates these building blocks, together with intelligent network selection and other supporting techniques, for advanced QoS-aware policy-based multi-access support.

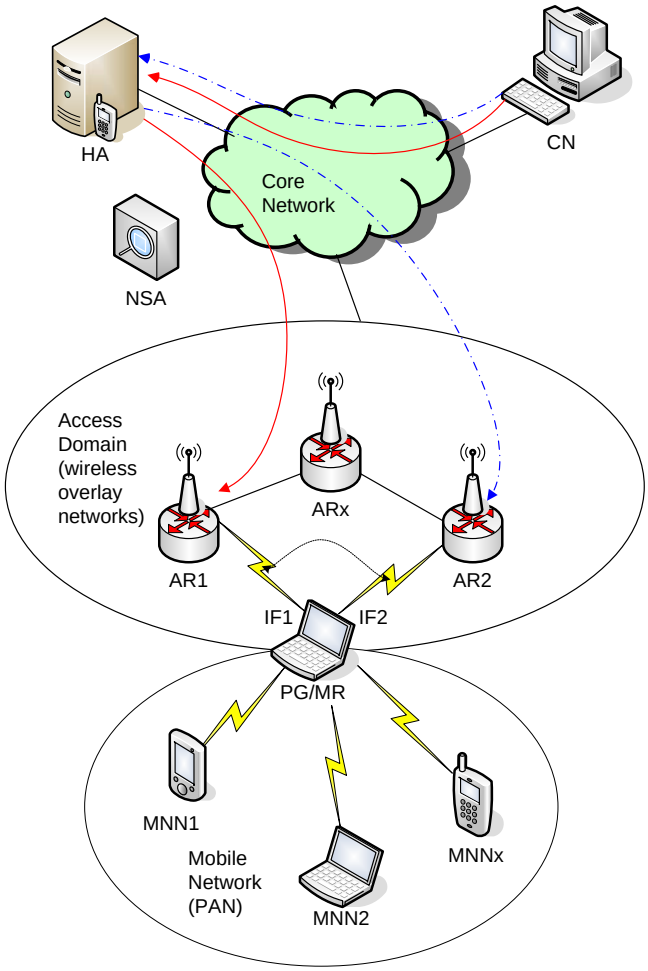
The remainder of the paper is structured as follows. We introduce the MULTINET architecture in Section II. We then present the proposed design of the policy-based multi-access support in Section III. In Section IV, the implementation, validation and evaluation of the proposal are described. Finally, we conclude the paper in Section V.

II. THE MULTINET ARCHITECTURE OVERVIEW

The MULTINET architecture, as illustrated in Fig. 1, is based upon the NEMO paradigm. The foreign access domain comprises homogeneous or heterogeneous wireless overlay networks whose coverage areas are overlapped to provide simultaneous multiple wireless connections. The intelligent network selection algorithms (NSA) subsystem continuously monitors and analyses the conditions of the multiple networks so that it can determine in real time the policies for optimal distribution of diverse application flows over these networks. A decision is made according to a set of predefined algorithms that take into account the user's preferences, applications' requirements, operator's regulations as well as the network conditions. Detailed design of the NSA subsystem is beyond the scope of this paper as we focus on the subsequent operations once the policies are generated.

The mobile network is a PAN moving as a whole with the mobile user visiting the foreign access domain. The multi-access and mobility functionality of the PAN is managed at the PG, which is a NEMO-enabled Mobile Router (MR) enhanced with additional supporting functions for intelligent network selection. The PG also serves as a gateway to the fixed infrastructure for all the Mobile Network Nodes (MNNs) in the PAN. The PG (and thus the PAN as a whole) has multiple network interfaces (e.g., IF1, IF2), each of which has a globally routable IPv6 CoA associated with the corresponding access network.

The MNNs communicate with their CNs located in the fixed infrastructure partition for a number of tasks such as file downloading and real-time video streaming. To comply with the standardised NEMO basic support protocol [2], the



- HA: Home Agent
- CN: Correspondent Node
- NSA: intelligent Network Selection Algorithm server
- AR: Access Router
- PG/MR: Personal Gateway/Mobile Router
- MNN: Mobile Network Node
- IF: Interface
- PAN: Personal Area Network

Fig. 1 Multi-access support in MULTINET

bi-directional tunnelling mode is assumed and thus all communications are through the PG's HA, deployed in the home domain. Accordingly, the HA and the PG are responsible to enforce the policies generated by the NSA dynamically so that both the downlink and the uplink application flows can be distributed over the multiple access networks as expected.

III. Policy-Enabled Multi-Access Support

A. NEMO-Enabled Basic Multi-Access

In the standard NEMO, only one CoA of a MR can be registered at the HA at a given time. A new CoA always overrides the existing one. The MCoA draft [4] allows multiple CoAs to be bound with the same HoA of a MR by introducing a binding unique identification (BID) to distinguish different (HoA, CoA) bindings. Each (HoA, CoA) binding is assigned a different BID. Typically, each BID corresponds to an interface of the MR, and thus a certain BID can be used to represent a specific interface at both the HA and the MR.

With the multiple CoAs enabled, the MR is able to utilise the corresponding interfaces simultaneously. After a successful registration of each CoA through a pair of Binding Update and Binding Acknowledgement messages, multiple bi-directional tunnels are established between the HA and the MR/PG. CoAs can be obtained through either IPv6 stateless host auto-configuration or DHCPv6. The whole procedure is illustrated in Fig. 2.

B. Policy-Based Advanced Multi-Access

To facilitate QoS-aware multi-access, policies are issued by the NSA based on real-time QoS measurements and intelligent network selection algorithms so that the multiple interfaces can be exploited in an optimal way. In principle, an output policy from the NSA defines a binding of a specific interface (for a given PG), i.e., a BID and a specific application flow. Clearly, a BID can be bound with more than one application flow and many applications can share one network interface.

Furthermore, an application flow can be identified by different parameters present in the application data's IPv6 or higher layer headers [5] such as the Flow Label, the Class of Service, and/or the Security Parameter Index. More commonly, a flow may be specified by a flexible combination of a pentuple consisting of five objectives: source IP address, destination IP address, source port number, destination port number, and the transport protocol. It is noted that many popular Internet applications can be simply identified by their "well-known" port numbers, e.g., 80/8080 for HTTP and 20 for FTP.

In more generic scenarios, the port number (the source

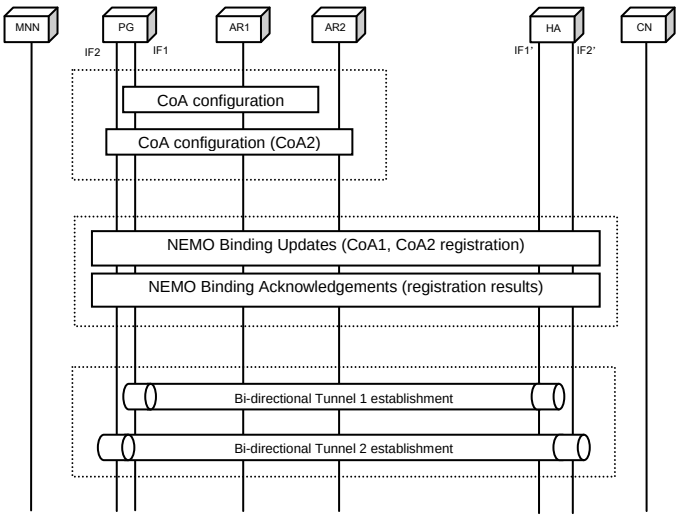


Fig. 2 Basic multi-access

and/or the destination port number) needs to be combined with one or more of the five objectives in a pentuple to identify a fine-grained application flow. An example of a policy encoded in XML is shown in Fig. 3. In this policy, the transport protocol is UDP and the destination port is 1234 (the source port is unspecified). This identifies a UDP-based video streaming application whose destination port is 1234. The source and destination addresses indicate the transmission direction as well as the source and the destination. Consequently, the combination of these four objectives specifies a unique downlink video streaming flow from the server to the client (an MNN). The home address refers to the PG that manages the MNN and the BID identifies an interface of the PG. Thus, the policy binds the specified flow to the specified interface. Finally, a specific action should be associated with a policy for a policy enforcement entity to proceed. Essential actions include adding (as in the example) and deleting policies though additional actions can be defined.

Once produced at the NSA, a policy needs to be packed into a message referred to as a *trigger* since this message is designed to provoke a policy-based flow (re)distribution (also referred to as a flow handoff/handover) over a selected set of active interfaces. If more than one policy is generated at the same time, these policies may share the same trigger message for signalling efficiency.

There are two major approaches to achieving the signalling of triggers and their acknowledgements between the policy transmission and reception entities. One approach is to extend the existing MIPv6/NEMO mobility messages so that the policy information can be piggybacked and signalled in both uplink and downlink directions. The other approach is to introduce new dedicated bi-directional messages, preferably standard based for implementation convenience and high interoperability. We have investigated the first approach in previous work [7]; we further explore the second approach in this paper.

The Simple Object Access Protocol (SOAP) has been chosen as the bearer of the policy-related signalling for its high extensibility and readability. As a Recommendation of the World Wide Web Consortium (W3C), SOAP is a standard protocol for delivering structured information such as a complex policy based on XML in a decentralised, distributed environment. Typically, HTTP is coupled with SOAP for bi-directional request-response messaging over a TCP connection. For secure signalling, the policy signalling can be encoded in HTTPS. Compared with [6], we propose that downlink policies should be issued by the dedicated QoS-aware subsystem NSA other than the HA. The NSA subsystem can be deployed in a more flexible and distributed way to facilitate real-time QoS measurements.

Commonly, policies need to be generated for both downlink and uplink traffic flows. Symmetric policies are used in the MULTINET architecture so that bi-directional flows belonging to the same session or of the same type are distributed over the same access network. Depending on which entity generates and sends the symmetric uplink policy to the PG, two schemes were designed. Scheme I uses the HA whilst Scheme II uses the NSA. In both schemes, downlink policies are generated by the NSA other than the HA. Scheme I and Scheme II are two alternate signalling procedures, and thus they are not used at the same time. There are pros and cons in each scheme. Scheme I avoids the interfacing between the NSA and the PG, and can avoid generating invalid symmetric policies due to interface unavailability as it allows the HA to double check this. Scheme II alleviates the extra burden in the HA for generating the symmetric policies and prompts the policy signalling to the PG. The choice is the network service provider's. Fig. 4 demonstrates the signalling sequences of the two schemes.

```
<?xml version="1.0" encoding="UTF-8" ?>
<flowDistributionPolicy>
 <policy>
   <action>add</action>
   <homeAddr>2001:192:168:106::100</homeAddr>
    <protocol>UDP</protocol>
    <srcAddr>2001:192:168:106:10</srcAddr>
    <dstAddr>2001:192:168:3::100</dstAddr>
    <srcPort></srcPort>
    <dstPort>1234</dstPort>
    <BID>200</BID>
  </policy>
 </flowDistributionPolicy>
```

Fig. 3 Policy for a UDP flow

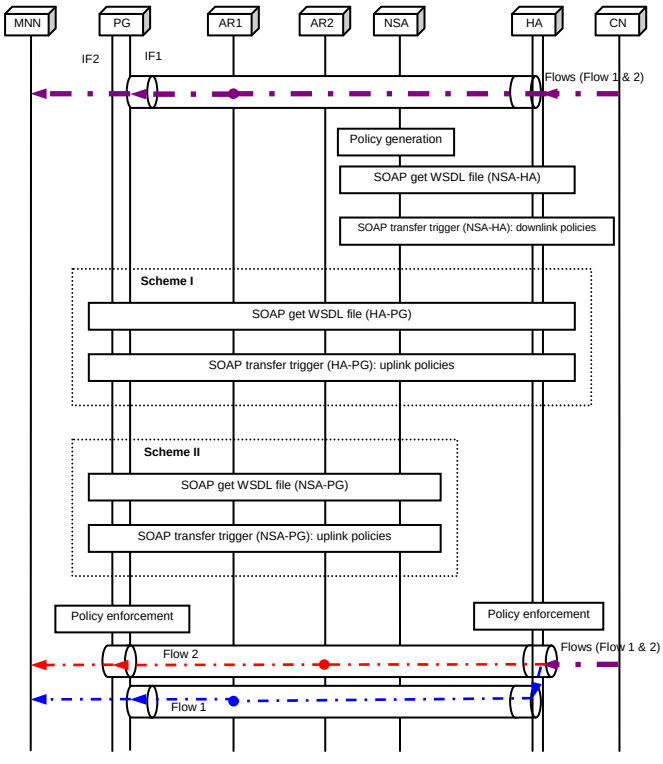


Fig. 4 Policy-based multi-access

IV. Implementation and Evaluation

A. Implementation

To verify and evaluate the proposed policy-based multi-access architecture, we have implemented the proposed designs on a local IPv6-enabled wireless networking testbed, as shown in Fig. 5. A set of customised Linux PCs and routers was configured to act as the NSA, the CN, the HA and the PG equipped with two Wi-Fi interfaces IF1 and IF2. The MNN is a Windows XP PC in the mobile network whose multi-access and mobility proxy is the PG. The NSA was simplified as a network trigger/policy generator in the following experiments although the full version of NSA that is QoS aware through QoS monitoring and intelligent network selection algorithms is being realised in the MULTINET project. The CN is a video streaming server and a FTP server for the MNN. VLC [8] and ProFTPD [9] applications were used for video streaming and FTP, representing typical real-time and non-real-time applications, respectively. A couple of 802.11b/g ARs provide the PG with two wireless connections (and thus two separate routes between the HA and the PG) whose data rates were set to be 11 Mbps.

The SOAP-based policy signalling schemes were implemented with PHP5 [10], which has built-in C-based SOAP support. Apache2 was installed as the HTTP/HTTPS server. The handoff execution functionality was built upon the NEMO implementation NEPL with integrated MCoA support [11]. Policy processing is handled through ip6tables. Once a trigger is received and parsed, the enclosed policies are installed and enforced with the ip6tables at the HA and the PG. The subsequent packets meeting a policy are marked with the corresponding BID, e.g., 100 or 200. A routing table per BID is generated, e.g., routing tables 100 and 200. These tables are looked up for forwarding the marked packets to the corresponding interfaces.

IPv6 stateless host auto-configuration was achieved through the radvd module [12]. Consequently, the PG automatically configures a CoA for each of its interfaces and registers the CoA with the HA via the MCoA support so that two bi-directional tunnels are established.

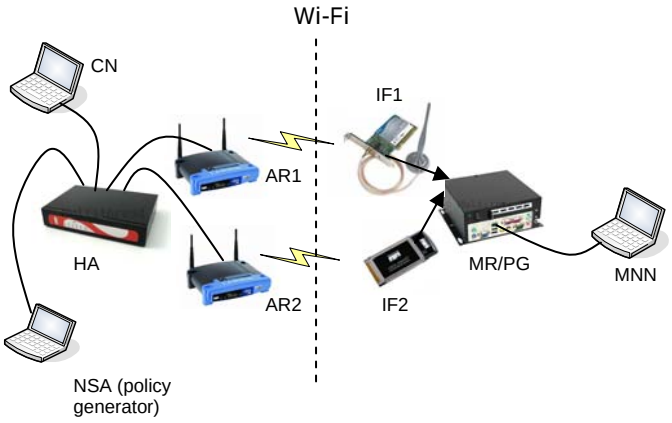


Fig. 5 Testbed layout

B. Validation

We have performed numerous experiments to verify the proposed policy-based multi-access support. In the following, we present a case study of flow redistributions (handoffs) of two different applications: FTP file downloading and UDP-based video streaming. As illustrated in Fig. 6, the X Axis represents the time sequence of the experiment whilst the Y Axis shows the traffic volume of the application flows.

At time T0, a RTP/UDP-based video streaming has been established and is being transmitted from the CN towards the MNN via the PG. By default, all traffic travels through the IF2 interface of the PG and the corresponding interface of the HA.

At time T1, the NSA issues Trigger 1, which contains one policy to be enforced at the HA. The policy indicates that the ongoing video streaming should be handed off from IF2 to IF1. The symmetric policy for the PG is optional as the streaming is a one-way traffic (no uplink traffic for acknowledgement or reverse streaming). After the policy is enforced at the HA, the streaming flow is handed over from IF2 to IF1. This flow redistribution decision could be made according to the output of the intelligent network selection algorithm for different reasons such as load sharing, fault tolerance or

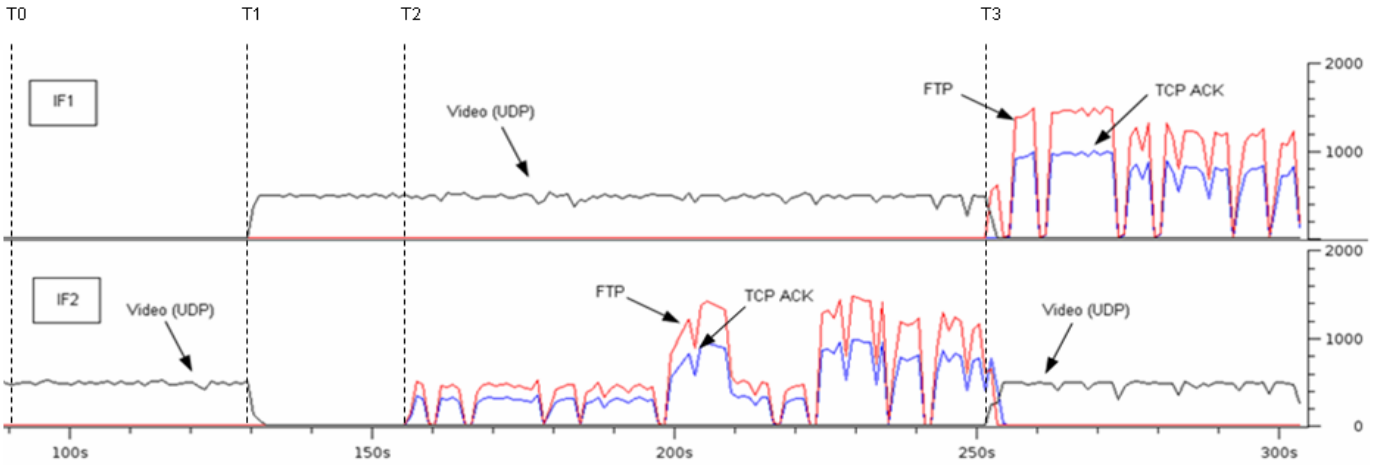


Fig. 6 Policy-based flow redistribution

user/application preferences. For instance, the NSA had detected that the route via IF1 was underutilised or the route via IF2 was overloaded (or temporarily going down). It could also result form an establishment request of a new application session (e.g., the subsequent FTP downloading), which has the priority to use the IF2 route and demands other applications to use alternative routes if possible.

At time T2, a FTP file transfer was initiated by the MNN to download a large file from the CN. Again, by default the FTP flow (from the CN to the MNN) and the corresponding TCP ACK flow (from the MNN to the CN) were transmitted through IF2.

At time T3, the NSA issues Trigger 2, comprising two new policies. One policy is to switch the FTP flow (downlink traffic) from IF2 to IF1. A symmetric policy was also generated at the HA for the PG to redirect the corresponding TCP ACKs (uplink traffic) together with the FTP flow. Meanwhile, the other policy demands that the video streaming be handed off from IF1 to IF2. The symmetric policy to the latter one is optional.

C. Evaluation

Such experiments were repeated with random flow handoffs of the applications between the interfaces. When the flow handoffs occurred in these experiments, no noticeable disruptions were perceived by a number of observers viewing the video streaming at the MNN. Therefore, it seems that the subjective QoS of real-time applications is maintained during and after the flow handoffs.

Further experiments were carried out to investigate the performance of the FTP/TCP applications under flow handoff conditions. Fig. 7 demonstrates a typical result showing the sequence numbers of the received TCP segments at the MNN as the time of a FTP downloading elapsed. As shown in Fig. 7, the TCP segments received at the MNN are in good order all the time, despite the fact that a couple of flow handoffs were experienced at the time instances around 11 s and 34 s, respectively. It is noted that the time instances on the X Axis are not evenly distributed since the FTP downloading is not of constant bit rate as can be found from Fig. 6. Such in-sequence delivery was also found in additional flow handoff experiments for a TCP flow of constant bit rate. As illustrated in Fig. 8 (with the X Axis plotted to scale), though three handoffs occurred during the session, packets were well received.

To quantitatively assess the signalling performance of the flow handoff signalling over HTTP or HTTPS, additional experiments were conducted and results were obtained in terms of flow handoff signalling loads and delays, as shown in Fig. 9 and Fig. 10, respectively. The flow handoff signalling loads are incurred from the policy-based flow handoff messages over HTTP or HTTPS, the corresponding TCP acknowledgements, and other TCP messages for connection setup and teardown. The flow handoff signalling delay is defined as the elapsed time between a Trigger message is generated by the NSA and the final acknowledgements are received at the NSA from both the HA and the PG (on completing the distribution and enforcement of both the trigger at the HA and the symmetric trigger at the PG).

Firstly, in either case (HTTP or HTTPS) it is intuitive that both the handoff signalling loads and delays increase with the number of policies coded in the Trigger message. Moreover, we found that a Trigger message starts to be segmented due to being oversized when it encloses more than two full pentuple policies. The segmentation and reassembly operations incur additional loads and delays due to the added messaging and processing. This factor also contributes to the growth of signalling loads and delays.

When the two cases are compared with each other, generally the SOAP over HTTPS signalling loads and delays are significantly larger than those of the SOAP over HTTP. This is the price paid for security as more operations are incurred. The signalling loads range from 5 to 8 Kbytes over HTTP and from 10 to 13 Kbytes over HTTPS. In next-generation wideband wireless networks, such signalling loads seem acceptable. With regard to signalling delays, they range from 0.17 to 0.30 s over HTTP and from 1.72 to 1.91 s over HTTPS. It is observed that the fact that the signalling delays over HTTPS are fairly high does not seem to affect the smoothness of policy-based flow handoffs seriously. The reason is that the original interface is still being used before the handoff to the target interface is completed.

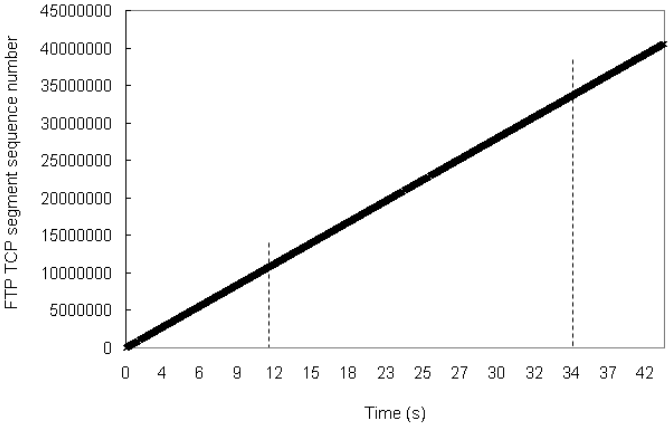


Fig. 7 FTP flow handoff performance

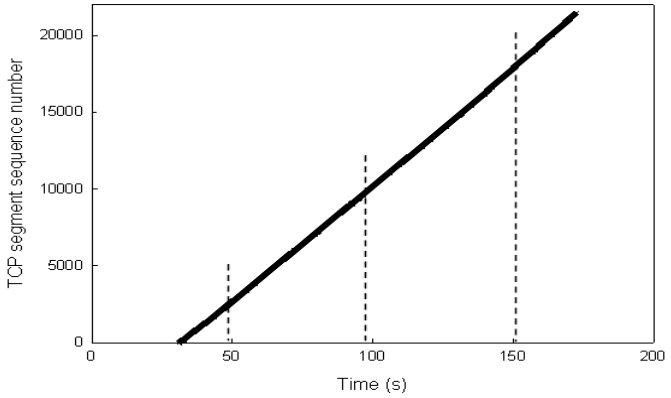


Fig. 8 Constant-bit-rate TCP flow handoff performance

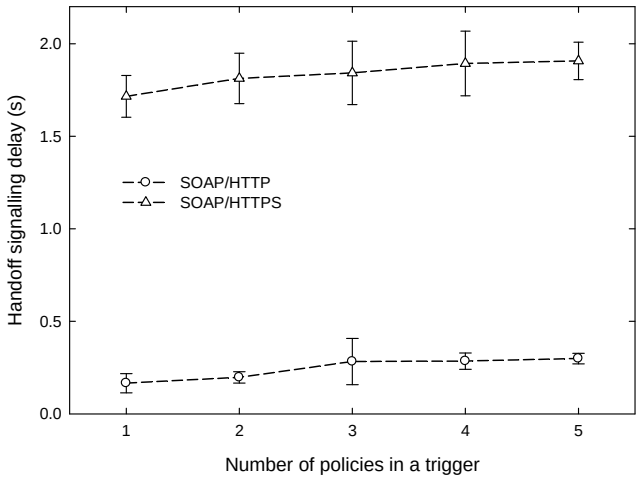


Fig. 9 Handoff signalling delay

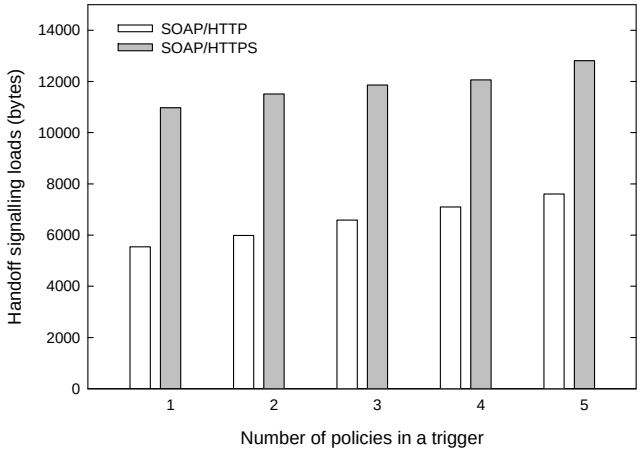


Fig. 10 Handoff signalling loads

V. Concluding Remarks

In this paper, we have addressed the design, implementation, validation and evaluation of policy-based multi-access support in the MULTINET architecture.

The MULTINET architecture is established upon the NEMO paradigm and it exploits the multiple care-of addresses extension to enable basic multi-access for a nomadic user who has a personal area network. To facilitate Always Best Connected services, policy-based multi-access support is necessitated. Compared with existing IETF drafts, in MULTINET policies are dynamically generated by a dedicated QoS-aware NSA subsystem based on intelligent network selection algorithms that take into considerations real-time QoS measurements and user/application profiles. In addition to introduce advanced intelligence into network selections, such a design can facilitate a more flexible and distributed deployment of the NSA subsystem. A policy defines the distribution of a selected application flow over a specific network interface and thus the corresponding access network. With a set of dynamic policies enforced at the HA and the PG for downlink and uplink traffic respectively, flows of diverse applications can be distributed in an optimised way over the multiple access networks. Policy signalling is a crucial enabler to the dynamic policy-based multi-access support. Two SOAP-coded schemes have been designed depending on which entity (the NSA or the HA) is responsible to generate and transfer the symmetric policies to the PG. The choice is thus implementation specific.

The proposed architecture has been implemented, verified and assessed on a working IPv6 WiFi multi-access testbed. The experimental results show that the achieved policy-based multi-access support is applicable to both typical real-time and non-real-time applications such as video streaming and FTP downloading. Furthermore, it is expected that the proposed dynamic flow handoffs would help to sustain the subjective or objective QoS for real-time and non-real-time applications, respectively, by keeping selecting access networks intelligently. Therefore, the MULTINET architecture appears a promising approach to the highly desired Always Best Connected paradigm to realise customised adaptive QoS for mobile roaming users in a multi-access environment.

Acknowledgment

This work has been funded by the EU IST FP6 Project MULTINET: Enabler for Next Generation Service Delivery (No. IST-2005-027437).

We would like to thank all the MULTINET project partners for their contributions during the development of various ideas presented in this paper.

References

[1] G. Fodor, A. Eriksson, and A. Tuoriniemi,, “Providing Quality of Service in Always Best Connected Networks,” *IEEE Communications Magazine*, Vol. 41, No. 7, pp. 154-163, Jul. 2003.

[2] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, “Network mobility (NEMO) Basic Support Protocol,” IETF RFC 3963, Jan. 2005.

[3] D. B. Johnson, C. Perkins, and J. Arkko, “Mobility Support in IPv6,” IETF RFC 3775, Jun. 2004.

[4] R. Wakikawa, T. Ernst, and K. Nagami, “Multiple Care-of Addresses Registration,” IETF Internet Draft, <draft-ietf-monami6-multiplecoa-03.txt>, work in progress, Jul. 2007.

[5] H. Soliman, N. Montavont, N. Fikouras, and K. Kuladinithi,, “Flow Bindings in Mobile IPv6 and NEMO Basic Support,” IETF Internet Draft, <draft-soliman-monami6-flow-binding-04.txt>, work in progress, Feb. 2007.

[6] K. Mitsuya, K. Tasaka, and R. Wakikawa, “A Policy Data Set for Flow Distribution,” IETF Internet Draft, <draft-mitsuya-monami6-flow-distribution-04.txt>, work in progress, Aug. 2007.

[7] Q. Wang, R. Atkinson, C. Cromar, and J. Dunlop, “Hybrid User- and Network-Initiated Flow Handoff Support for Multihomed Mobile Hosts”, in *Proc. IEEE VTC2007-Spring*, Dublin, Ireland, Apr. 2007, pp. 748-752.

[8] (2007) VLC media player. [Online]. Available: http://www.videolan.org/vlc/

[9] (2007) ProFTPD FTP server. [Online]. Available: http://www.proftpd.org/.

[10] (2007) Hypertext Preprocessor (PHP) SOAP functions. [Online]. Available: http://uk2.php.net/soap

[11] (2007) NEMO Implementation for Linux (NEPL). [Online]. Available: http://www.nautilus6.org/nemo/

[12] (2007) Linux IPv6 Router Advertisement Daemon (radvd). [Online]. Available: http://www.litech.org/radvd/