Accessing the Internet through Moving Networks

Carlos J. Bernardos, Ignacio Soto, Santiago Zapata, Dirk v. Hugo, and Susana Sargento

***Abstract*—The success of cellular communications networks shows the interest of users in mobility. Host mobility support in IP networks is a first step in the adaptation of these networks to the needs of users in this field. But, there exists also the need of supporting the movement of a complete network that changes its point of attachment to the fixed infrastructure. This paper describes the architecture designed in the EU DAIDALOS II project to provide Internet access through moving networks. The designed moving networks architecture support the following main features: Route Optimisation, Multicast traffic delivery, security and authentication integration, end-to-end QoS and interaction with Localised Mobility Management solutions.**

***Index Terms*— Network Mobility, Route Optimisation, Multicast, Authentication, Security, QoS, Mobile Router, Mobile IPv6, PANA, IEEE 802.11e, Mobile communication.**

I. Introduction

USERS demand Internet access not only from fixed locations (e.g., at home, at work, in hotels, cafeterias, universities, etc.) but also in public transportation systems (e.g., planes, trains and buses). In order to satisfy such demands, the technical community worked on the design of the required protocols to provide Network Mobility support. The Internet Engineering Task Force[1] (IETF) has standardised the Network Mobility (NEMO) Basic Support protocol [1], which enables mobile networks to change their point of attachment while maintaining the sessions that the nodes of these networks may have established.

The DAIDALOS II project[2] is working on the design and development of a network mobility architecture that builds on top of the basic solution defined by the IETF, but fulfilling a more ambitious set of requirements, including: global Route Optimisation support – mitigating the effects of the sub-optimal routing introduced by the NEMO Basic Support protocol; multicast support – enabling optimised multicast traffic delivery from/to moving networks; authentication and security support – based on the IETF PANA framework; end-to-end QoS support – based on Diffserv and IEEE 802.11e; and Localised Mobility Management integration – based on IETF NetLMM solutions.

The paper describes the DAIDALOS II NEMO architecture, highlighting its main features and describing the solutions involved to provide a secure and seamless access to the Internet through moving networks.

The paper is structured as follows. Section II introduces some of the basic technologies and protocols that are integrated into the DAIDALOS II NEMO architecture. The DAIDALOS II NEMO architecture is detailed in Section III. Finally, Section IV concludes the paper.

II. Background and motivation

A. Network Mobility

To address the requirement of transparent Internet access from mobile platforms, the IETF standardised the NEMO Basic Support protocol [1], which defines a Mobile Network (or Network that Moves, NEMO) as a network whose attachment point to the Internet varies with time. The router within the NEMO that connects to the Internet is called the Mobile Router (MR). It is assumed that the NEMO has a Home Network where it resides when it is not moving. Since the NEMO is part of the Home Network, the Mobile Network has configured addresses belonging to one or more address blocks assigned to the Home Network: the Mobile Network Prefixes (MNPs). These addresses remain assigned to the NEMO when it is away from home. Of course, these addresses only have topological meaning when the NEMO is at home. When the NEMO is away from home, packets addressed to the Mobile Network Nodes (MNNs) will still be routed to the Home Network. Additionally, when the NEMO is away from home, i.e. it is in a visited network, the MR acquires an address from the visited network, called the Care-of Address (CoA), where the routing infrastructure can deliver packets without

Manuscript received January 28, 2007. The work described in this paper is based on results of the IST FP6 Integrated Project DAIDALOS II. DAIDALOS II receives research funding from the European Community's Sixth Framework Programme. Apart from this, the European Commission has no responsibility for the content of this paper. The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Carlos J. Bernardos and Ignacio Soto are with the Department of Telematics Engineering of Universidad Carlos III de Madrid, Avda. Universidad, 30, 28911 Leganés, Madrid (e-mail: {cjbc, isoto}@it.uc3m.es).

Santiago Zapata is with Faculty of Computer Science, University of Murcia, 30100 Murcia, Spain (e-mail: canela@dif.um.es).

D. v. Hugo is with Deutsche Telekom/T-Systems, 64295 Darmstadt, Germany (e-mail: dirk.hugo@ t-systems.com).

Susana Sargento is with Instituto de Telecomunicações, Universidade de Aveiro, Campus Universitário de Santiago, 3810 Aveiro, Portugal (e-mail: ssargento@det.ua.pt).

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

[2] http://www.ist-daidalos.org/

additional mechanisms.

The basic solution for network mobility support is quite similar to the solution proposed for host mobility (Mobile IPv6 [2]) and essentially creates a bi-directional tunnel between a special node located in the Home Network of the NEMO (the Home Agent, HA), and the CoA of the MR.

B. *Localised Mobility*

The idea of Localised Mobility Management is not new. Early in the development of mobility solutions in IP networks, it was recognised that Mobile IP alone was not sufficient and improvements were needed to provide adequate performance when a Mobile Node (MN) roamed across access networks far from its home network. Some of the proposals to deal with this issue were based on the idea of managing the local mobility differently from the global mobility.

The initial proposals had as main objectives to reduce signalling outside the local domain, and improve efficiency by managing the local mobility closer to the MN (reducing the time needed for the mobility signalling and improving handover latency). These early proposals (such as Hierarchical Mobile IPv6 – HMIPv6 [3]) were host based, i.e. hosts were active elements in the mobility process, taking care of the signalling needed to manage the local mobility, and being aware of the local and global solutions, thus acting accordingly.

Unlike host-based mobility, such as Mobile IPv6, where mobile terminals signal a location change to the network to maintain routing states and to achieve reachability, the NetLMM [4] approach relocates relevant functionality for mobility management from the mobile terminal to the network. In the localised mobility domain, the network learns through standard terminal operation, such as router and neighbour discovery or by means of link-layer support, about a terminal's movement and coordinates routing state update without any mobility specific support from the terminal. While moving inside the local domain, the MN keeps its IP address, and the network is in charge of updating its location in an efficient manner. Such an approach allows hierarchical mobility management on one hand, where mobile terminals signal location update to a global mobility anchor only when they change the localised mobility domain, and mobility within a localised domain for terminals without any support for mobility management at all on the other hand. NetLMM complements host-based global mobility management by means of introducing local edge domains.

C. *Security and authentication in access networks*

One of the main requirements of the access networks is to provide the access to the network services to the allowed users in a secure way.

For this purpose, a suitable authentication process should be deployed in the access network. Furthermore, this process should supply to other mechanisms with cryptographic material for providing the security into this network. This is especially important in mobile scenarios in which the user is visiting a foreign network, and there is not a direct way to provide access to the network without a previous authentication process.

In the DAIDALOS I project, a solution based on Protocol for Carrying Authentication for Network Access (PANA) [5] and IPsec was designed. In this solution, PANA is in charge of authentication process by transporting the Extensible Authentication Protocol (EAP) [6] packets from PANA Client (PaC, in the MN) to PANA Agent (PAA, in the Access Router - AR) which is acting as an EAP Authenticator. On the other hand, the transport of authentication packets into the core network requires the deployment of an Authentication, Authorisation and Accounting (AAA) infrastructure. Once the MN is authenticated, the PAA is deploying keying material derived by the EAP method to the Access Point (AP) to which the MN is attached. In that way, the AP is sharing a Security Association (SA) with the MN.

Following this architecture, a similar solution for NEMO architecture has been designed. This is described in Section III.D.

D. *QoS*

In recent years, much interest has been devoted to the design of wireless local area networks (WLAN's) with Quality of Service (QoS) support. The Enhancements Task Group (TGe) was formed under the IEEE 802.11 project to recommend an international WLAN standard with QoS support. This group has recently approved a new standard for QoS support. This standard is called 802.11e and has been built as an extension of the basic WLAN 802.11 standard. The IEEE 802.11e standard [7] defines two different access mechanisms: the Enhanced Distributed Channel Access (EDCA) and the HCF (Hybrid Coordination Function) Controlled Channel Access (HCCA).

Furthermore, NEMO, because of its multi-hop and dynamic nature, poses additional challenges to the inherent difficulty of providing QoS over wireless links. Indeed, QoS provisioning in a NEMO involves extra mechanisms in addition to providing QoS to the various wireless links of the mobile network. Statistical analyses are required in order to guarantee the desired performance resulting from traversing several wireless links each of which provides only statistical guarantees. In addition, novel signalling mechanisms need to be devised for performing QoS signalling over such a dynamic environment.

Another important aspect is the QoS support beyond the NEMO, towards the other end-point of the communication, the so-called end-to-end QoS support. To support integrated end-to-end QoS, QoS signalling needs to be in place between the source and destination. Our aim is to support QoS in communications between users in different networks, transparently irrespective of their locations, considering NEMO networks as one of the possible locations.

III. DAIDALOS II NEMO ARCHITECTURE

A. *General Architecture*

In DAIDALOS II, the Network Mobility capabilities are supported by the Mobile Router and Home Agent. These two network entities host the modules that provide the architecture with the desired functionalities (namely, basic Network Mobility support, Route Optimisation, multicast, security and authentication, and end-to-end QoS). To achieve all of these functionalities, the NEMO architecture also relies on network capabilities enabled by the general DAIDALOS II architecture. As an example, DAIDALOS II networks provide support for Localised Mobility Management (LMM), by following one of the solutions discussed within the IETF NetLMM WG [4], authorisation and security, by using the PANA framework [5], and end-to-end QoS, by following a Diffserv approach [8] in the wired access and core network, with per-flow admission control and IntServ [9] in the wireless access network. Additionally, the control plane for layer-3 handover management is based on the IEEE 802.21 framework as specified in [10].

From a mobility point of view, it is worth to mention that the LMM approach followed in DAIDALOS II, defines Local Mobility Domains (LMDs) – formed by different access networks –, wherein nodes can move within without changing their IP addresses. As previously referred, this provides several advantages, such as a reduction of the signalling load due to handovers, and an improvement on the handover delay.

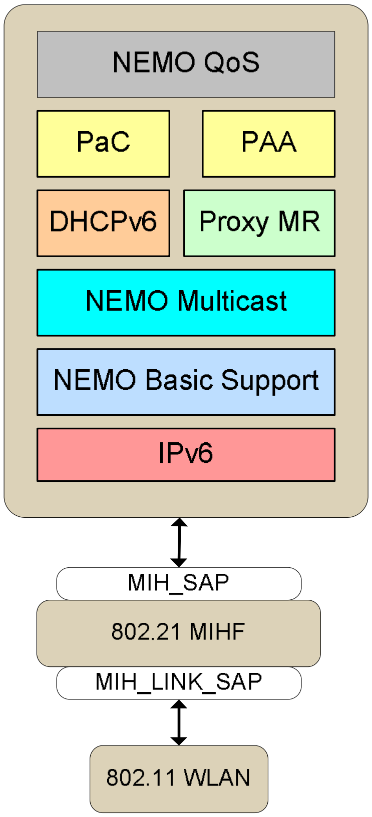

Figure 1 Mobile Router's architecture

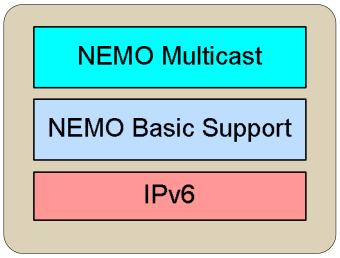

Figure 2 Home Agent's architecture

The architecture of the DAIDALOS II Mobile Router and the Home Agent are shown in Figure 1 and Figure 2, respectively. In order to bring all the functionalities provided by the DAIDALOS II NEMO architecture, most of the required modules are located on the Mobile Router. Next sections describe how the components of the NEMO architecture provide all the aforementioned capabilities.

B. *Route Optimisation*

The Route Optimisation (RO) solution is built on top of the solution developed in DAIDALOS I, called Mobile IPv6 Route Optimisation for NEMO (MIRON) [11], [12] (this first solution provided Route Optimisation for nodes without mobility support, called Local Fixed Nodes, LFNs). We add to this solution the support for Route Optimisation by mobile-capable nodes (called Visiting Mobile Nodes, VMNs). We keep the name MIRON for the NEMO RO general solution even if it is an enhanced version of the MIRON solution developed in DAIDALOS I.

The Route Optimisation approach that MIRON defines for VMNs is based on taking advantage of the mobility support that these nodes already have, providing the means to the VMN to perform the RO.

In order to allow the VMN to manage its own mobility and enable it to perform RO with the Correspondent Nodes (in a way that avoids the MR-HA bi-directional tunnel), we propose the following [13]:

- Provide a topologically meaningful IPv6 address to the VMN. These addresses are those that belong to the network that the root-MR is visiting.
- Enable this address to be routable inside the NEMO, as it only has topological meaning in the visited network. The MR has to perform proxy neighbour discovery for this address in the egress interface that is attached to the network to which the address belongs. Besides, the MR has to insert a host route for this address to be able to route packets destined to it.
- Perform source address routing in the MR in order to send directly (that is, avoiding the bidirectional MR-HA tunnel that still exists and is used for non-optimised traffic) packets sent by the VMN.
- Update the address of the VMN when the NEMO moves to a different Localised Mobility Domain (LMD).

The Route Optimisation mechanism for VMNs that we propose uses a particular functionality that is included in the PANA protocol, namely, the capability of telling a node that it must change its IPv6 address and how to get a new one. This imposes the requirement that the PaC software must be available in VMNs for providing them with RO, and PaC and PAA software must be available in MRs.

C. Multicast

IP Multicast proves to be a resource efficient measure for several promising new mobile applications often requiring definite QoS and low delay characteristics. The regular change of the point of attachment to the infrastructure due to mobility, however, is a challenge to performance issues: either routing paths may increase unduly high or a frequent update of branches or - in case of a moving source of multicast traffic - even of the complete multicast tree will occur.

Several approaches to solve the mobile multicast problem have been proposed (e.g. see [14]). The high complexity of an efficient solution makes the implementation within the MR inside a moving network interesting providing an entity for centralised intelligent multicast control on behalf of a plurality of terminal nodes. An extension to a former solution developed within DAIDALOS I [16] is proposed within DAIDALOS II. A method for dynamic path selection implemented within the MR uses information on network movement and multicast router distance, as well as session and traffic flow characteristics of the different multicast groups, to come to the most efficient decision in terms of delay and overhead.

The dynamic agent located within the MR has to run a database with a set of prior access routers and multicast forwarding paths as entries. The routing paths for previous routers are compared with that of the defined default solution (we chose for start-up routing via the HA known as Bi-directional Tunnelling, BT) and a possible new mode using the visited AR as proxy multicast agent (Remote Subscription, RS). Based on the outcome, the control entity decides on the optimised multicast routing path for the actual situation. Including potential future paths assuming expected movement of the NEMO in this routine is subject for forthcoming research.

Algorithms to differentiate between global and localised mobility, and to provide seamless multicast sessions in case of handover of VMNs to and from mobile networks, are also under investigation to achieve optimised routing paths for group management messages and traffic forwarding.

An integration of the NEMO Multicast approach with broadcast technologies might prove highly efficient in terms of scarce radio resource utilization. This applies for both, bi-directional systems as UMTS/MBMS (Multimedia Broadcast/Multicast Service), and unidirectional DVB (Digital Video Broadcasting) requiring a hybrid solution with separate return path. Common protocol used for all these cases is MLDv2 (Multicast Listener Discovery) [16], thus facilitating the update for a multi-mode MR, which will be further investigated in the framework of the project.

D. Security

The security applied in NEMO is based in two main concepts: authentication and securing the communication. As already was explained in Section II.C, the security in the communication is the result of authentication process, so it is only possible after this process.

At the same time, the authentication of the MNNs of a Mobile Network must be split in two phases.

1) Authentication of MR into the visited network

This authentication is required because the MR is an unknown entity in the visited network, and the Access Routers (AR) need to trust the MR.

The MR plays the role of MN, so it must run a PANA Client, and it must own a special identity which is recognized in its home domain. In that way, the MR is going to authenticate itself to the PANA Agent located in the AR. Once the MR is authenticated, a SA is shared with the AR, and the traffic to the AP can be secured.

2) Authentication of the MNNs into the NEMO

The authentication of the MNNs requires also the existence of PANA Agent in the MR, because the PANA Clients located in the MNNs should contact to it for authentication process. The internal NEMO authentication architecture will consider the moving network as if the MR was physically located at home. So NEMO management should be in charge of sending the AAA messages to the corresponding home domain.

The PANA Agent located in MR should maintain a SA with AAA server in MR's home domain. This is required to enable the Diameter peers (PAA in MR, and AAA server in home domain) be connected in a secure way. However, this is not an extra requirement, because the MR will be a PAA when the MR is attached at home, and so, it should maintain this SA. Nevertheless, the security protocol protecting this communication should be appropriate for supporting the MR's movement.

E. QoS

Nodes communicating through a NEMO must have the same QoS support as other nodes in the DAIDALOS II architecture. QoS must be provided end-to-end, and we can identify three different steps for the QoS support:

- Inside the NEMO.
- In the access to the infrastructure.
- In the rest of the path until the other end-point of the communication.

Last step is common to the DAIDALOS II architecture. The first step is specific for NEMOs, but solutions to provide QoS in a local network (e.g. wireless) can be applied. The second step is conditioned by the fact that we want to keep the NEMO support transparent to the infrastructure; therefore, no new requirements will be imposed on the functionality of the infrastructure to be able to support NEMOs. Therefore, the infrastructure will deal with NEMOs in the same way that it deals with terminals.

For providing QoS inside the NEMO, the MR will do local admission control functions. It receives a QoS request through, for example, a Next Steps In Signalling (NSIS) message, and checks the available resources in the specific AP (L2 resources); this request is only forwarded to the infrastructure if there are available resources in the NEMO network and it can be accepted locally. The solution uses the same signalling as the global DAIDALOS II QoS signalling architecture for hosts. The MR receives QoS requests for connected terminals and if these requests can be accepted locally, then it calculates the QoS parameters and forwards these requests towards the other end-point of the communication. These requests will then be processed in the origin and destination access networks, and resources will be reserved for the flows. In this way, the MR works as a proxy for the QoS signalling. To provide this functionality, a main NEMO QoS module has been defined.

IV. Conclusion

This paper describes a modular architecture which provides seamless Network Mobility support, therefore enabling a transparent and ubiquitous Internet access from mobile platforms, such as trains, buses, planes, boats or cars. The provision of Internet access through moving networks presents several advantages – provided by the NEMO Basic Support protocol defined by the IETF – such as not requiring any specific software on the nodes that connect to the moving network in order to gain connectivity to the Internet. An additional feature is that it is possible to provide wide area mobile connectivity (e.g., Internet connectivity) to devices that can only access to personal area networks (e.g., Bluetooth).

The proposed architecture provides the following features: basic network mobility support, as defined by the IETF in the RFC 3963; Route Optimisation support mitigating the effects of the sub-optimal routing introduced by the NEMO Basic Support protocol; multicast support extending the basic NEMO standard to enable the delivery of multicast traffic from and to a moving network; security and authentication support integrating the PANA framework in the NEMO architecture; end-to-end QoS support providing QoS guarantees to the applications running on nodes attached to a moving network; and integration with Localised Mobility Management solutions, to benefit from reduced signalling and better handover latency performance.

References

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

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

[3] H. Soliman, C. Catelluccia, K. E. Malki, and L. Bellier, “Hierarchical Mobile IPv6 Mobility Management (HMIPv6),” IETF, RFC 4140, August 2005.

[4] H. Levkowetz, Ed., “The NetLMM Protocol”, draft-giaretta-netlmm-dt-protocol-02.txt, IETF Internet-Draft (work-in-progress), October 2006.

[5] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig and A. Yegin, “Protocol for Carrying Authentication for Network Access (PANA)”, draft-ietf-pana-pana-13.txt, IETF Internet-Draft (work-in-progress), December 2006.

[6] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson and H. Levkowetz, “Extensible Authentication Protocol (EAP)”, RFC 3748, June 2004.

[7] IEEE 802.11, “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY). Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements”, IEEE Standard, 2005. Amendment to IEEE 802.11 Standard.

[8] S. Blake et al, “An Architecture for Differentiated Services”, RFC 2475, December 1998.

[9] Braden et al., “Integrated Services in the Internet Architecture: an Overview”, RFC 1633, June 1994.

[10] IEEE P802.21/D01.09 Draft IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services.

[11] Carlos J. Bernardos, Marcelo Bagnulo, and María Calderón, “MIRON: MIPv6 Route Optimization for NEMO”, in Proceedings of the 4th Workshop on Applications and Services in Wireless Networks (ASWN). August 2004.

[12] Carlos J. Bernardos, Antonio De La Oliva, María Calderón, Dirk von Hugo, and Holger Kahle, “NEMO: Network Mobility. Bringing ubiquity to the Internet access”, demonstration at IEEE INFOCOM 2006, April 2006.

[13] María Calderón, Carlos J. Bernardos, Marcelo Bagnulo, Ignacio Soto, and Antonio de la Oliva, “Design and Experimental Evaluation of a Route Optimization Solution for NEMO”, IEEE Journal on Selected Areas in Communications (J-SAC), issue on Mobile Routers and Network Mobility, Volume 24, Number 9, September 2006.

[14] Th. C. Schmidt and M. Waehlisch, “Multicast Mobility in MIPv6: Problem Statement”, IRTF Internet-Draft (work-in-progress), October 2006.

[15] D. v. Hugo, H. Kahle, C. J. Bernardos, M. Calderón, “Efficient Multicast support within moving IP sub-networks”, 15th IST Mobile Summit, Mykonos, Greece, June 2006.

[16] R. Vida et al., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.