2.12

MoAR: Mobile Access Router. Providing Security and Localised Mobility support for Mobile Networks

Carlos J. Bernardos, Ignacio Soto, **Universidad Carlos III de Madrid**
Santiago Zapata, Francisco J. Galera, **Universidad de Murcia**

ABSTRACT

Nowadays, users do not only expect to have Internet access from fixed locations (e.g., at home, work, or through hotspots deployed in airports, hotels or cafes), but also from mobile platforms, such as trains or buses. Host mobility support in IP networks was a first step towards achieving such a ubiquitous Internet environment. Nevertheless, supporting the movement of a complete network that changes its point of attachment to the fixed infrastructure, without requiring the intervention of the nodes attached to the network, also presents some advantages. Additionally, access to this kind of public Internet access networks must be secured and authenticated, in order to avoid unauthorised users to gain connectivity. A third issue that needs to be tackled is the performance of the mobility management solutions deployed in these scenarios, since handover latencies should be small enough to enable the deployment of real-time applications (e.g., VoIP). The use of Localised Mobility Management mechanisms aims at improving this performance, while reducing the overall system signalling overhead.

This paper proposes an architecture that integrates Network Mobility, Security and Localised Mobility management mechanisms, minimising the changes required on the network infrastructure and analysing relevant scenarios where this integration is required.

Index Terms

Network Mobility, Authentication, Security,
Localised Mobility Management, Mobile Router, Mobile IPv6, PANA.

2.12.1. 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 NEMO Basic Support protocol solves the very basic problem of network mobility support, but current use case scenarios pose additional challenges, mainly triggered by users' requirements and deployment issues. As an example, users demand seamless connectivity, no matter how they attach to the network or where they are located. This imposes additional challenges, such as the need of optimising the path followed by data packets (the so-called Route Optimisation problem [4]) or the minimisation of the delays/service disruptions due to handovers. Additionally, today's networks must be secure and access from unauthorised users must not be permitted, hence security and authentication should also be taken into account.

This paper presents an architecture that combines enhanced Network Mobility mechanisms - to provide transparent and route optimised mobility support for roaming networks - with localised mobility management solutions - to improve the handover performance and reduce signalling overhead -, and with a security framework, based on Protocol for Carrying Authentication for Network Access (PANA), to provide the designed architecture with security and authentication mechanisms.

The paper is structured as follows. Section 2.12.2 introduces some of the basic technologies and protocols that are integrated into the proposed architecture. Some relevant use case scenarios and the motivation to this work are described in Section 2.12.3, while the proposed solution is detailed in Section 2.12.4. Finally, Section 2.12.5 concludes the paper.

2.12.2. BACKGROUND

2.12.2.1. 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

(1) http://www.ietf.org/

an address from the visited network, called the Care-of Address (CoA), where the routing infrastructure can deliver packets without additional mechanisms.

The basic solution for network mobility support is quite similar to the solution proposed for host mobility (Mobile IPv6 [3]) 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.

The NEMO Basic Support protocol has several performance limitations, namely: it forces suboptimal routing (i.e. packets are always forwarded through the HA). It introduces non-negligible packet overhead and the HA becomes a bottleneck for the communication as well as a potential single point of failure. Because of these limitations, it is highly desirable to provide what has been called Route Optimisation (RO) support for NEMO [9], to enable direct packet exchange between a Correspondent Node (CN) and a MNN, avoiding traversing the Home Network. MIRON [2] is a proposal of a solution for Route Optimisation that does not require upgrades in CNs, MNNs, or HAs.

2.12.2.2. Localised Mobility management

The idea of Localised Mobility Management (LMM) 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.

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 [4]) 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.

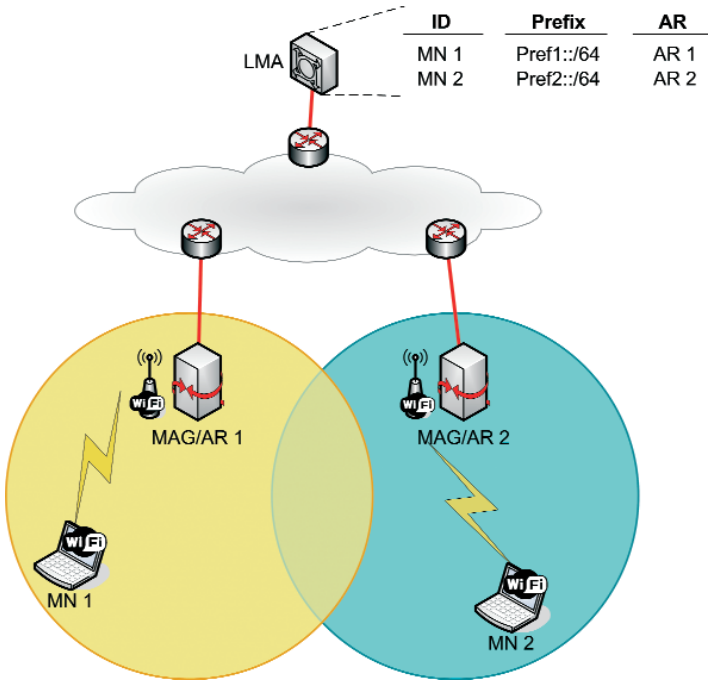
Unlike host-based mobility, such as Mobile IPv6, where mobile terminals signal a location change to the network to maintain routing states and to achieve reach ability, Network LMM (NetLMM) [5][8] approaches relocate relevant functionality for mobility management from the mobile terminal to the network. 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 Localised Mobility Domain (LMD), 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.

The LMM solution defined in the EU DAIDALOS II project is based on [5]. It basically defines a Localised Mobility Domain as a network domain where Localised Mobility Management support is provided. To do so, two new network entities are defined (see Figure 2.12.1):

- Mobile Access Gateway (MAG). This entity is also referred to as Access Router, so we will use both terms along the paper. It is a router that a mobile node is attached to as the first hop router in the LMM infrastructure. There are multiple MAGs/ARs in an LMD.

- Local Mobility Anchor (LMA). It is a router that maintains reachability to a Mobile Node's address while the Mobile Node moves around within the same LMD. It is responsible for assigning IPv6 addresses/prefixes to Mobile Nodes within the LMD, and maintaining forwarding information for the Mobile Nodes which includes a set of mappings to associate Mobile Nodes by their identifiers with their address information, associating the mobile nodes with their serving MAGs/ARs and the relationship between the LMA and the MAGs/ARs. There may be one or more LMAs in a same LMD.

Figure 2.12.1: Daidalos II LMM solution



2.12.2.3. Security and authentication in access networks

Access Networks require the provision of access to them in a secure way, but only for authorised users. This requirement implies the existence of a suitable authentication process which is able to supply 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.

A solution based on Protocol for Carrying Authentication for Network Access (PANA) [6] and IPsec has been designed within the framework of the EU DAIDALOS II project. In this case, PANA is in charge of the authentication process by carrying the Extensible Authentication Protocol (EAP) [7] 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 transfers 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.

This solution can be adapted to NEMO scenarios in the most possible transparent way, by splitting the global procedure in three phases:

- Authentication of MR. At this point, the MR authenticates itself in the network like a normal MN does, so it requires to deploy into the MR the modules in charge of authentication (mainly PANA Client).
- Establishment of Security Associations between the MR and the network. This is done to allow MNN's authentication and mobility management. For example, a PANA Agent should be located in the MR and should re-establish its SA with the corresponding AAA Server.
- MNN's authentication. The MNNs start authentication process with the PAA located in the MR like they did in authentication This is why it is required to deploy a PAA also in the MR.

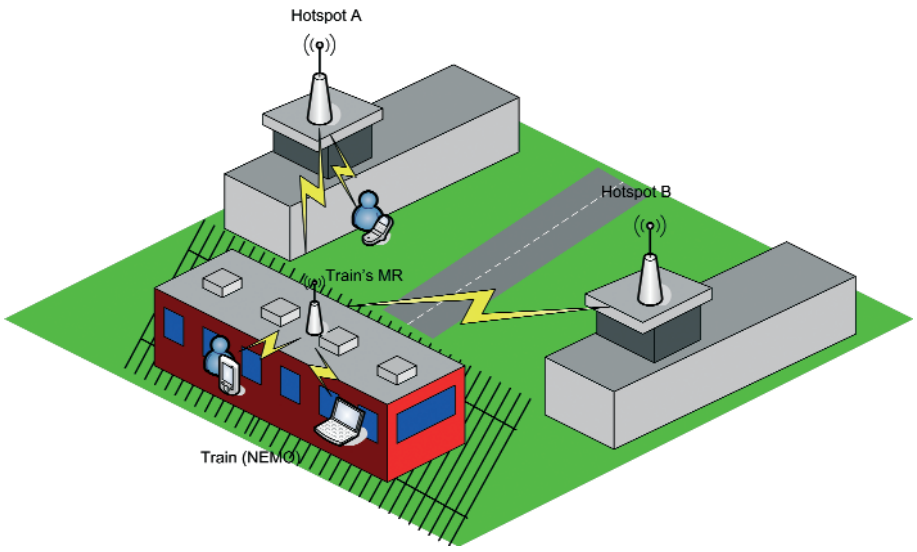
2.12.3. USE CASES SCENARIOS AND MOTIVATION

There are several potential scenarios where a secure combination of Host and Network mobility with Localised Mobility management solutions is required. Next, some of these scenarios are introduced.

2.12.3.1. Airport scenario

A possible scenario could be found when a user is connected via WLAN to a hotspot located in an airport's terminal, where it is already authenticated. At some moment, the user takes a train to commute to another terminal. A Mobile Network is deployed within the train, and therefore the user keeps its Internet connectivity, by performing a handover to the train's NEMO.

Figure 2.12.2: Airport scenario



While connected to the train, the MN does not deal with any mobility issue, since it is the MR deployed on the train the one managing the mobility of the whole train. As soon as the train arrives to the new terminal, the MN should perform another handover to the fixed infrastructure, in order to maintain its connectivity.

This scenario implies that the train's MR hand offs from hotspot in terminal A to hotspot in terminal B, and users using the train's NEMO hand off from the hotspot in terminal A to train's NEMO, and from train's NEMO to the hotspot in terminal B. Nevertheless, all the handovers are performed within the same administrative domain (airport), so Localised Mobility Management could enable the MN to keep its address, which can be exploited in order to provide seamless handovers.

New mechanisms need to be designed and integrated to enable Moving Networks belong to the same Localised Mobility domain that the fixed infrastructure.

2.12.3.2. Bus scenario

Another interesting scenario is the one in which a user is connected via WLAN to a hotspot in a bus station, while waiting a bus.

The bus provides connectivity - by having a NEMO deployed inside - while it is moving, and users keep their connectivity when they hand off from the bus to the fixed hotspots available at the stations. This connectivity is maintained while the bus is travelling and moving (potentially moving from an administrative domain to another), in a transparent way to the users.

In this case, a Localised Mobility Management solution can not be exploited when the bus moves from an administrative domain to another, but it can while the bus is connected into the same administrative domain.

2.12.3.3. Motivation

As pointed out in previous sections, the integration of Network Mobility and Localised Mobility solutions brings several interesting advantages, mainly the reduction in the required signalling (which in NEMO can be significant when a Route Optimisation solution is used) and the gain in the performance. However, this integration presents several challenges, depending on the type of nodes that are connected to the NEMO:

- Local Fixed Nodes (LFNs). Since mobility is hidden from the LFNs, a localised mobility management solution is transparent to them. An MR will configure an address belonging to the LMM domain (exactly as an MN would do) - this is the CoA for the MR - that can be registered in the HA by using the NEMO Basic Support protocol. The MR-HA tunnelled traffic will transparently traverse the LMA-AR tunnel in the LMM domain. The advantage of using an LMM solution is that when the MR moves from one AR to another inside the LMD, this does not require to send signalling to the HA. The infrastructure will use the same method to detect the movement of the MR as it uses for any MN, in fact it will not be able to notice the difference.
  The situation when the MR is using an RO solution as **MIRON** is the same. In MIRON, the CoA of the MR is not only registered in the HA of the MR, but also in the CNs that are communicating to LFNs of the NEMO. In this case the LMM provides an additional advantage in the intra-LMM handover, all the signalling to the HA and the CNs after a handover is avoided.
- **VMN** and nested NEMOs support with Route Optimisation: Supporting VMNs and nested NEMOs is somehow more difficult. VMNs require addresses topologically correct in the infrastructure that the NEMO is visiting to be able to perform Route Optimisation in an efficient way. The more challenging issue is how to manage an MN's handover between the fixed infrastructure and a NEMO (attached to the same LMD), in such a way that the MN does not require to change its IP address. This paper proposes a mechanism that solves this issue.

2.12.4. SOLUTION ARCHITECTURE

2.12.4.1. Overview

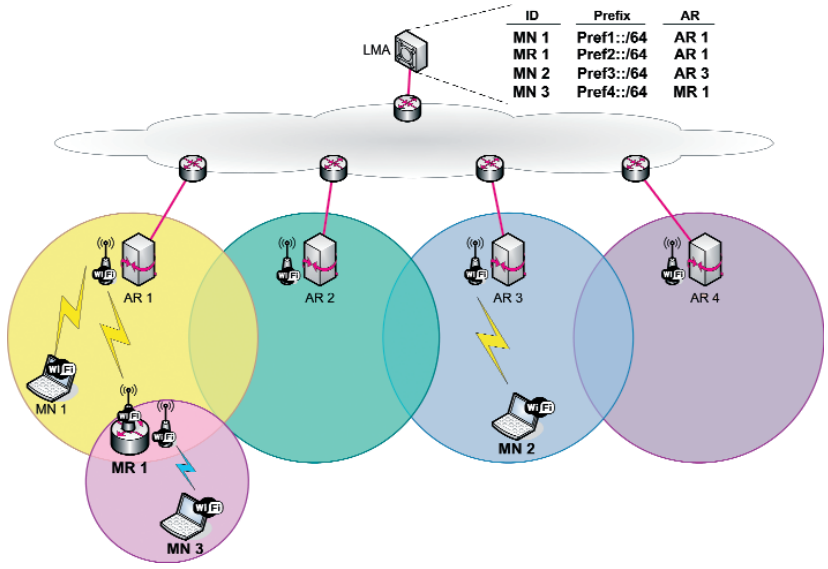
In order to extend an LMD with attached Mobile Networks, we propose an architecture in which the role of a Mobile Router is two-folded:

1. On one hand, the Mobile Router behaves as a Mobile Node (normal Mobile Router operation over its egress interface), so it obtains an IPv6 address/prefix from the LMA when it first enters the LMD and then keeps that address while roaming within the same LMD.
2. On the other hand, the Mobile Router behaves as a MAG/AR - that is why we call it Mobile Access Router (MoAR). It extends the LMD by providing IP addresses/prefixes to attached VMNs and forwarding/receiving packets to/from the LMA.

The basic operation of a MoAR is as follows. When an MR attaches to an Access Router belonging to an LMD, this Access Router informs its LMA about this event, providing it with the MR's identity. The LMA delegates an IP address/prefix to the MR and creates a binding, associating the MR's identity, the delegated address/prefix and the AR to which the MR is attached. This is the standard behaviour when a normal MN connects to an AR of an LMD. If the MR moves to another AR within the same LMD, the LMA updates the binding with the new AR's information.

If the MR is authorised (i.e. it has the required security relationship/trust with the LMA) to behave as a MoAR within the LMD, the MR also plays the role of a normal Access Router for VMNs that get attached to it. When a VMN attaches to an MR, the MR informs the LMA and gets an IPv6 address/prefix for the VMN. The LMA adds a new binding entry, associating the VMN's ID with the delegated address/prefix and the Access Router to which it is attached (i.e. the MR).

Figure 2.12.3: Solution overview

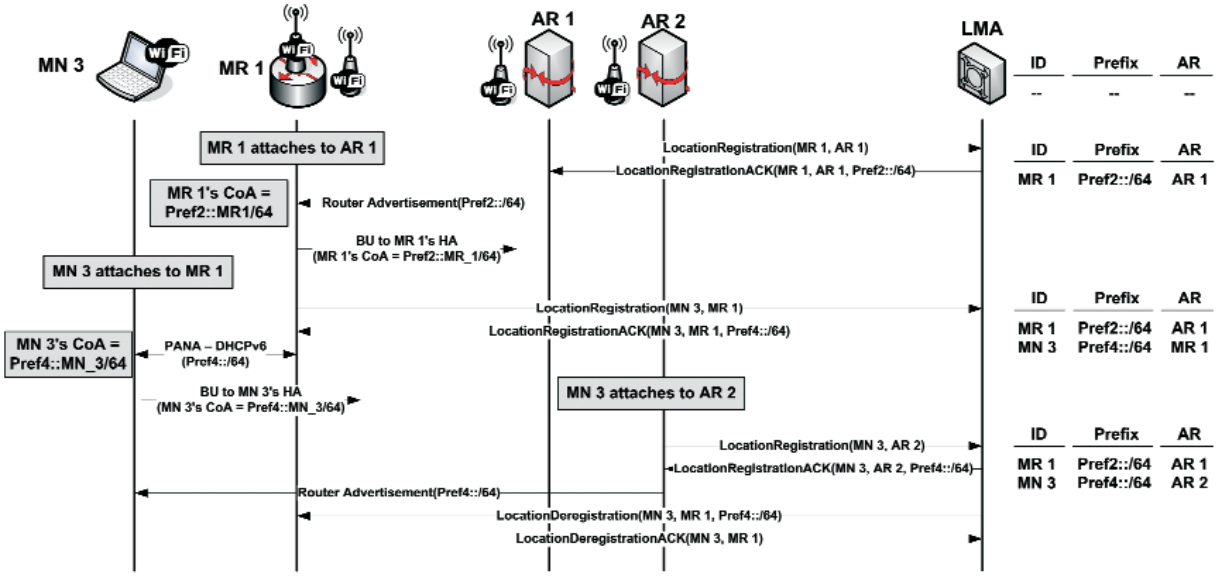


A change in the normal operation of the LMA is introduced to support MoARs. Basically, the LMA will need to recursively look into is binding table to find out how to deliver packets addressed to a VMN attached to connected MoARs. In a first look-up, the LMA obtains the MR to which the VMN is attached. After that, the LMA looks for the MR in its table and finds the associated Access Router. With this information, the LMA is able to encapsulate the received packet towards the Mobile Router, through the appropriate Access Router. The MR is then able to forward data packers from/to the VMN.

The MR also plays a double role in the security framework proposed:

1. Mobile Router must authenticate itself when it arrives to a visited network such a Mobile Node does. This authentication is required because the Mobile Router is an unknown entity in the visited network, and Access Routers need to trust the Mobile Router.
2. On the other hand, the Mobile Router plays the authentication agent role for attached Mobile Network Nodes.

Figure 2.12.4: Detailed operation signalling



Both MRs and MNNs authentication processes use PANA as the protocol in charge of carrying the EAP packets from PANA Client to PANA Agent. Then, the PANA Agent is forwarding the EAP packets for authentication purposes to AAA Server. The protocol used for exchanging these packets between PANA Agent and AAA server is the AAA protocol named DIAMETER [10]. For this interface, the PAA should act like a Diameter Client node asking for authentication/authorization to Diameter Server node.

It is important to notice that in order to allow MRs to behave as MoARs within the LMD, an association procedure between the MoAR and the LMA is required. Thus, MRs send a Association Request to the LMA for setting up the control and data plane between them, similarly as done between MAGs and LMA. The mechanism used by LMA to check if MAGs and MoARs are authorized to act as access routers is out of the scope of this paper.

2.12.4.2. Detailed Operation

This section describes in more detail the operation of our proposed architecture, using the network scenario that appears in Figure 2.12.3 and the Message Sequence Chart (MSC) depicted in Figure 2.12.4.

Let's assume that the network is bootstrapped, so there is no state in any network entity (that is, LMAs and Access Routers of the LMD). When a Mobile Router - MR 1 - attaches to AR 1, this event is detected by AR 1 and reported to its serving LMA, by means of a *LocationRegistration* message. Because there is no existing entry for MR 1 in the binding table of the LMA, a new entry is created, including the information of the IPv6 assigned prefix (Pref2::/64) and the AR to which the new arrived node (MR 1) is attached to (AR 1). The LMA then replies with a *LocationRegistrationACK* message, that includes the IPv6 prefix assigned to MR 1. With this information, AR 1 unicasts a Router Advertisement message to MR 1, so it can form a Care-of Address from the assigned prefix. At this stage, the MR is able to register/update its location with its Home Agent and start sending/receiving traffic. While the MR moves within the same domain, its CoA does not change.

When an MN - MN 3 - attaches to MR 1 (that is, MN 3 is a VMN), MR 1 sends a *LocationRegistration* message towards the LMA, which creates a new entry for MN 3 and informs MR 1 about the assigned prefix (Pref4::/64). MR 1 can then inform MN 3 about the IPv6 address it has to use (if we assume that MR 1 is using MIRON as Route Optimisation solution, it will use PANA-DHCPv6 signalling to make MN 3 obtain this address, as specified in [2]).

Figure 2.12.5: Packet encapsulation

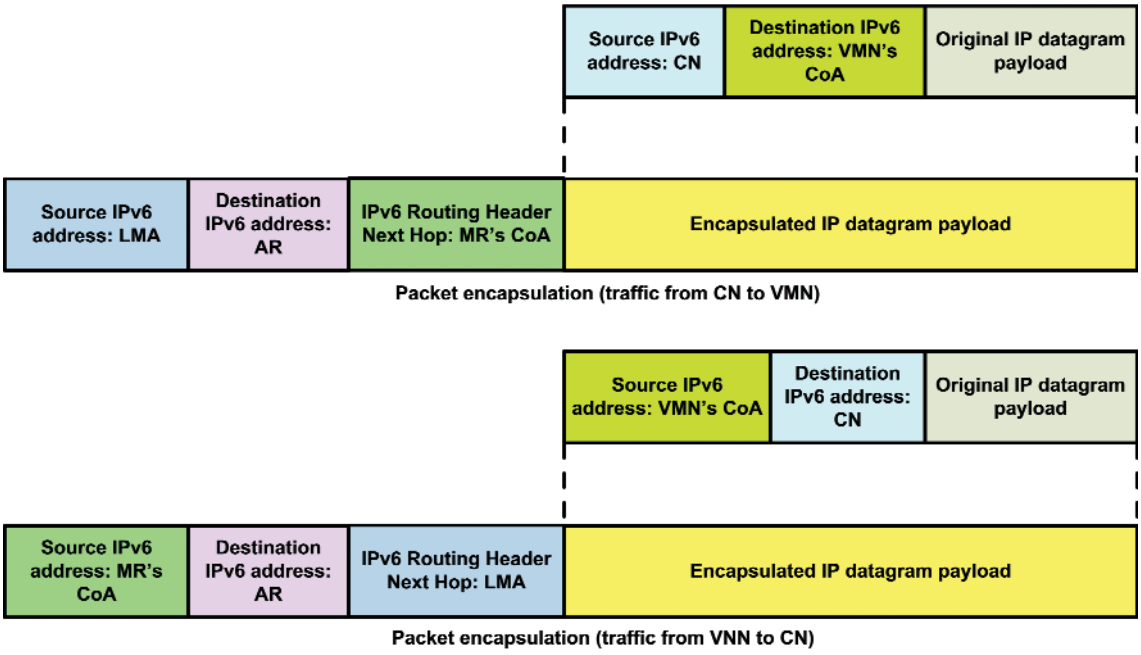


Figure 2.12.5 details the packet encapsulation performed by the LMA and MoAR while forwarding data traffic. Data packets from a CN are received by the LMA, which will look-up at its binding table which is the Access Router to which it has to forward packets received. This look-up is performed recursively until an infrastructure-Access Router (i.e. a non-MoAR) is found. Following our example, if the LMA receives a packet

from a CN addressed to MN 3, it will find that MN 3 is attached to MR 1. Since MR 1 is a MoAR, it will perform a second look-up at its table, searching for the Access Router to which MR 1 is attached to. Once that the LMA has found out that MN 3 is attached to MR 1, which is attached to AR 1, the LMA is able to forward data packets towards MR 1. To do that, LMA encapsulates each data packet in a new IPv6 packet towards MR 1, but using an IPv6 routing header[2], that ensures that the packet traverses AR 1 in the path towards MR 1 (the packet sent by the LMA has AR 1 as its destination address, and the Routing Header has only one hop, set to the MR 1's CoA). MR 1 decapsulates the packet, by removing the extra IPv6 header and delivers the packet to MN 3. In the reverse direction, MR 3 operates analogously, encapsulating data traffic sent by MN 3 towards the LMA.

If MN 3 performs an intra-LMD handover from MR 1 to AR 2, AR 2 informs the LMA, so it can update its binding table accordingly (now MN 3 is attached to AR 2, instead of to MR 1), which also informs MR 1 about the handover of MN 3.

The proposed architecture enables intra-LMD NEMO-to-infrastructure handovers. Roaming MNs keep their IPv6 addresses while moving within the same LMD, therefore reducing the mobility signalling outside the LMD, and improving the overall handover performance.

2.12.4.3. Security considerations

The whole authentication process is based on the introduction of PANA/AAA architecture into NEMO scenarios, which imply to satisfy several requirements:

- All MNNs should be provided with PANA Client (PaC) support (also LFNs).
- PANA Client (PaC) for authenticating the MR and PANA Agent (PAA) for authenticating MNNs must be located in the MR.
- Internal NEMO AAA architecture will consider the moving network as if the MR was physically located at MR's home domain, 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 Security Association (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.

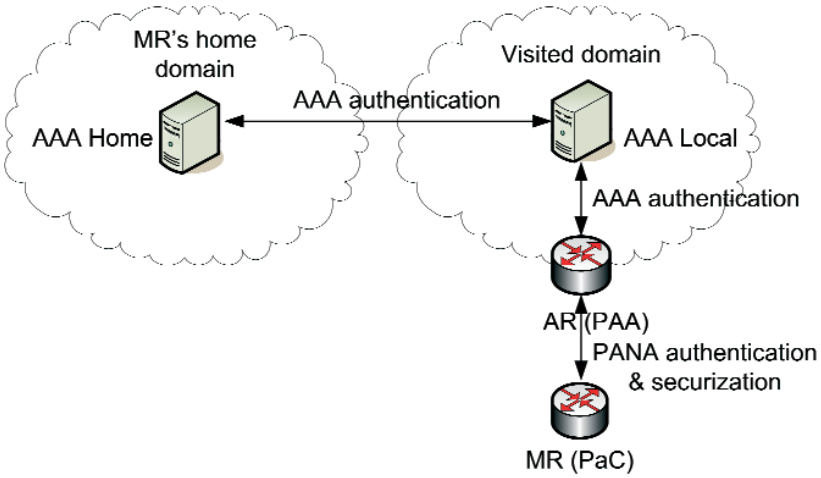
As already explained in the previous sections, the authentication process of a Mobile Network can be split in three phases:

1. Authentication of MR into the visited network

An MR arriving to a visited domain must authenticate itself within this domain before having access to the network, just like another MN arriving to this network. For this purpose, it uses PANA protocol to interact with the AR in the visited domain. Once the new AR is detected, the PaC in the MR starts the PANA/AAA authentication process. The PaC will interact with the PAA in the AR of visited domain. This interaction will be the normal authentication for a node arriving to the visited domain. AAA messages will be forwarded from AAA local server to AAA home server in MR's home domain (because this is the one having the authentication/authorization information for this MR). Figure 2.12.6 shows this process.

(2) A new type of Routing Header should be defined, with a new semantic that improves the security of the solution, by restricting in which situations it can be used.

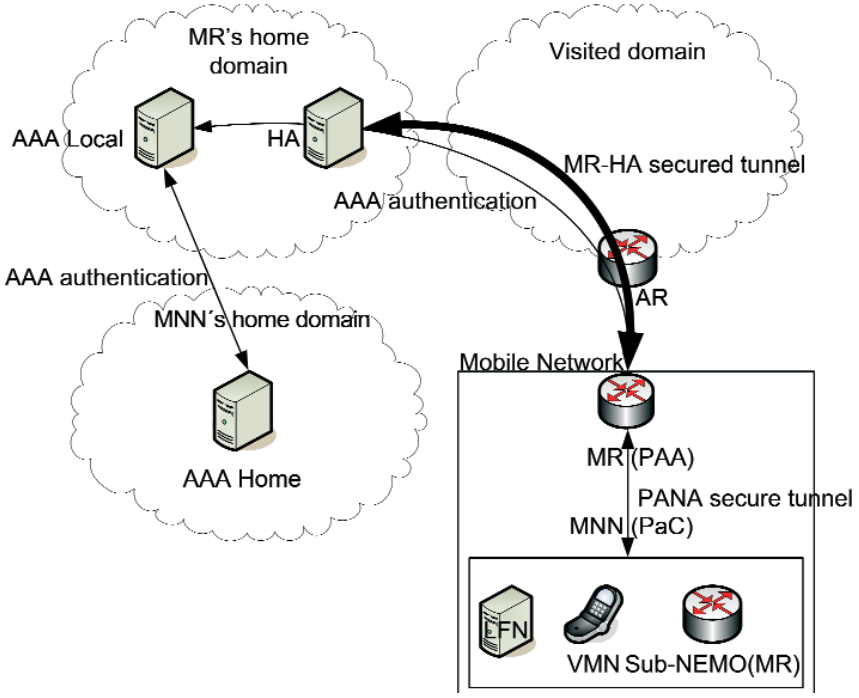
Figure 2.12.6: MR's authentication in the visited domain



2. Establishment of Security Associations

After receiving a successful notification of the MR authentication process, the AR and MR establish a secure tunnel for future communications. At this moment, the MR is able to get an IPv6 address and to establish the secured tunnel to its HA. Once the MR is authenticated and the Security Associations between MR and the network have been established, the bootstrapping process detailed in the previous section can be initiated.

Figure 2.12.7: MNN authentication into the NEMO



3. Authentication of the MNNs into the NEMO

Arriving MNNs must be authenticated into the NEMO. For this purpose, the PAA module is deployed into MR. This module is maintaining a secure connection with AAA server in MR's home network, so all the AAA messages will be forwarded through this server (this is the way also in which the AAA server can control the authorization information deployed into its MR by AAA servers of MNNs). This phase is depicted in Figure 2.12.7.

2.12.5. CONCLUSIONS

In this paper, we have proposed an architecture that provides localised mobility support for mobile networks in a secure way. We have identified and described several interesting real-life scenarios where this integration is needed and would improve users' connectivity.

The proposed architecture is based on a new network entity: the Mobile Access Router (MoAR), which is a NEMO (RFC 3963) Mobile Router extended to behave also as an LMM Access Router. Besides this, only the LMA is required to be extended to fully support our solution. Access Routers in the infrastructure of a Local Mobility Domain are not modified, therefore making easier the deployment of the solution.

The solution described in this paper integrates NEMO with one of the solutions for Localised Mobility Management that have been proposed at the IETF NetLMM WG. We are currently working on a solution that integrates NEMO and Proxy Mobile IPv6 (PMIPv6) [8], since this is the solution currently being adopted by the IETF. Another issue, not addressed in this work, in which we are currently working on, is the simulation of the proposed architecture and the evaluation of its performance under different network loads and scenarios.

2.12.6. ACKNOWLEDGMENTS

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 also partially sponsored by the Spanish Government under the POSEIDON Project (TSI2006-12507-C03-01).

2.12.7. REFERENCES

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

[2] 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, pp. 1702-1716.

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

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

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

[6] 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.

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

[8] S. Gundavelli et al., "Proxy Mobile IPv6", draft-ietf-netlmm-proxymip6-01.txt, IETF Internet-Draft (work-in-progress), June 2007.

[9] C.-W. Ng, P. Thubert, M. Watari, F. Zhao, "Network Mobility Route Optimization Problem Statement", draft-ietf-nemo-ro-problem-statement-03.txt, IETF Internet-Draft (work-in-progress) (September 2006).

[10] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, "Diameter Base Protocol", IETF, RFC 3588, September 2003.