A Collaborative AAA Architecture to Enable Secure Real-World Network Mobility

Panagiotis Georgopoulos, Ben McCarthy, and Christopher Edwards

School of Computing and Communications,
Lancaster University, Lancaster, LA1 4WA, UK,
Email : [panos, b.mccarthy, ce]@comp.lancs.ac.uk

Abstract. Mobile Networks are emerging in the real world in various scenarios, from networks in public transportation to personal networks in consumer electronics. The NEMO BS protocol provides constant network connectivity and reachability for the nodes of these Mobile Networks in a seamless manner despite their roaming. However, NEMO BS has yet to show its advantages in real world deployment because it lacks trouble-free and secure network access for the whole network, and secure data transmission for the nodes it provides connectivity for. On the other hand, Access Networks provide connectivity for Mobile Networks, but currently lack a robust AAA service which would enable network mobility support in a fast, trouble-free, but also secure and authenticated manner. Our paper describes a collaborative Unified Architecture that satisfies the requirements of both Mobile Networks and Access Networks, and our evaluation proves its efficiency and applicability for real world deployment in today's Internet infrastructure.

Keywords: Network Mobility, NEMO BS, AAA, RADIUS, Security

1 Introduction

Mobile IP (both Version 4 [11] and Version 6 [8]) is designed to support the mobility of individual mobile nodes, such as laptops, netbooks or smartphones that are roaming from one network to another, maintaining session continuity for their applications. However, there is a strong requirement nowadays to support the mobility of an entire group of devices (termed a Mobile Network (MN)) that usually moves as a whole, whereas its individual devices (termed as Mobile Network Nodes (MNNs)) remain relatively immobile in relation to one another. For example, networks in public transportation, such as in trains, buses, coaches and airplanes that offer connectivity to passengers' devices as they move can be considered as MNs, whilst the end-devices are MNNs. Another example of a MN is a PAN in a consumer electronics scenario, where connectivity for all the different devices a user may carry as he moves, is maintained by a lightweight personal mobile router. For example, a mountain rescuer may have such a PAN that could consist of a wireless IP camera, a PDA with a live mapping application, IP sensor devices on his body to monitor his health condition and a VoIP application for communication with fellow rescuers during a rescue mission.

The NEMO BS protocol [4] is responsible for offering constant connectivity and seamless session continuity to the MNNs of a MN without them having to be aware of their mobility, even though the MN might change it point of attachment from one Access Network (AN) to another. However, for real-world deployment, in order for the MR to run NEMO BS and support the mobility of the network, it has to be able to obtain secure and authenticated access from an AN in a fast and trouble-free manner. In addition, in such wireless mobile scenarios secure transmission of data is paramount, both in the range of the wireless hotspot the MR offers, but also as packets travel beyond the MN to the Internet via the AN. Furthermore, the AN has to have an efficient and scalable AAA infrastructure in order to authenticate, authorize and account the MN's connectivity.

Building on our previous work [6], this paper describes a Unified Architecture (UA) that combines the strengths of Network Mobility and AAA services to satisfy in a secure manner the requirements of both MNs and ANs. The rest of the paper is organized as follows. Section 2 discusses the motivation behind our research and Section 3 gives some background information on its cornerstones. Section 4 provides the design of our UA and Section 5 evaluates our approach qualitatively and quantitatively. Finally, Section 6 concludes this body of work and highlights its benefits.

2 Motivation

In order to describe the motivation behind this work, let us discuss a real-life example that reveals the current problems and explains the reasoning and motivation behind our research. Let us consider a scenario where a bus company decides to offer Internet connectivity to passengers that board its buses every day. In this scenario, as the bus does its every-day route through town, its MR is responsible to obtain Internet connectivity from various publically available AN's Access Points (APs) being sporadically located around town, and share it to the passengers' devices by projecting a wireless hotspot in the bus.

During this real-life scenario, the MN of the bus requires :

1. Seamless mobility and uninterrupted connectivity for all its MNNs, despite the fact that the MR has to change its IP address whilst roaming from one AN to another, thus causing the MNNs' applications sessions to break.
2. Quick, effortless and secure network access to each AN it connects to. The MR should avoid requiring to be configured with the different type of authentication credentials and protocols each AN it encounters require.
3. Dynamic trust establishment with the AP it roams to, to avoid being connected to available but deceitful APs that would try to sniff its authentication credentials and hack into the MNNs' transmitted packets.
4. Avoid revealing its identity to each AN it roams to for privacy purposes.
5. Secure data transmission both locally, in the vicinity of the hotspot it provides to its MNNS, but also globally, as its MNNs' data are transmitted from the MN to the Internet via the AN.

At the same time, AN providers have their own requirements to satisfy in order to provide connectivity for MNs. To be specific, ANs require :

1. Financial benefit for setting up and administering wireless networks possible scattered around a large area, for the MNs to connect to.
2. A robust and well configured service to Authenticate, Authorize and Account the MNs' connectivity in a practical and scalable manner. It is unrealistic to expect that each AN should know in advance each MR requesting network access on behalf of a MN.
3. Avoid compromising their security policies and disallow unauthorized access to their networks.

3 Background

This section introduces the cornerstones of this research work; NEMO BS, IPsec, Radius, TLS based authentication methods and wireless security protocols.

3.1 NEMO BS Protocol

The NEMO BS protocol [4] grants session continuity to the nodes of a MN that is roaming across different ANs, changing its point of attachment to the Internet. NEMO BS takes advantage of the large IPv6 address pool that guarantees global reachability of every MNN and also, manages to keep the mobility of the network transparent to its MNNs, by removing completely the need for the MNNs to run any extra protocols themselves to support their mobility.

According to NEMO BS, when a MR moves away from its Home Network (HN) and finds an AN to connect to, it sends a Binding Update (BU) to its Home Agent (HA) containing its new topologically correct IPv6 Care-of-Address (CoA), optionally along with one or more Mobile Network Prefixes (MNPs). These MNPs represent the networks that the MR serves and advertises to its MNNs in Router Advertisements, so that each MNN can configure an IPv6 address itself and be globally reachable. When the HA receives a valid BU from a MR, it updates its binding cache for that MR and its MNPs, and then acknowledges it with a Binding Acknowledgment (BA). From this moment a bi-directional tunnel between the HA and the MR is instantiated and the HA intercepts packets destined for all the MNPs that the MR has registered, and forwards them to the MR's CoA to ensure reception of packets by the MNNs.

3.2 IPsec

IPsec [9] is a protocol suite for establishing secure IP communications between peers (hosts or gateways) over an insecure network. IPsec uses a combination of protocols to provide mutual authentication, data confidentiality, data integrity, non-repudiation and anti-replay protection on a per packet basis without any regard to the communication path between parties. IPsec mainly uses three cryptographic protocols; IKE, AH and ESP. IKE is used to exchange cryptographic keys among peers, establish the Security Associations (SA) among them for inbound and outbound traffic per peer and negotiate all the cryptographic algorithms of the secure communication channel that IPsec will operate upon. AH and ESP are used in two different modes based on the requirements of

the application scenario; transport mode, where protection is provided from the Transport layer and higher, and tunnel mode, where protection is provided for the whole packet. Use of IPsec is mandatory in mobility scenarios ([2],[4]) to avoid attacks such as man-in-the middle, passive wiretapping or impersonation. Our UA complies with the aforementioned references and uses ESP in transport mode to protect control traffic between the MR and the HA in both directions, and ESP in tunnel mode to protect all the application traffic the MNNs generate.

3.3 RADIUS AAA Protocol

The RADIUS AAA protocol [12] is the most well known and widely deployed AAA protocol worldwide. Its functionality is built on the generic AAA framework defined in [10] and mainly involves three entities; the supplicant (end-device), the Network Access Server (NAS) and the AAA server

The process of performing a AAA service for a wireless device using RADIUS is as follows. When a device requests network access it uses a Layer 2 protocol (such as PPP or EAP) to communicate with the NAS and, among other information, send to it its authentication credentials. The chosen authentication method (e.g. EAP-TLS, PEAP etc.) will define the number of packets that should be exchanged for the authentication of the client, in addition to the type and format of the authentication credentials (e.g. a hashed password, a certificate etc.). Since the NAS has no appropriate means to authenticate the supplicant itself, it will initially collect all the information the supplicant sends, then use its AAA client implementation to encapsulate it in appropriate AAA packets, and then encrypt those with a strong key it shares with the AAA server before finally sending them to the server. When the AAA server receives these packets, it authenticates the supplicant usually with the aid of other resources, such as local databases or a PKI. If authentication is successful, the RADIUS server tries to authorize the user by checking its authorization policies which are, usually, ISP specific. When the AAA server reaches a decision whether the user should be granted or denied access to the network, it replies using AAA packets to the NAS, which is then responsible for relaying the reply to the supplicant over Layer 2 frames. When this phase is completed, the user is granted (or denied) access with a defined authorization level and the AAA server starts collecting accounting information for the supplicant's network usage from the NAS using specific accounting messages, that update the AAA server at regular intervals.

3.4 TLS based Authentication methods

There are more than 40 EAP based authentication methods that can be used in conjunction with a AAA protocol, which will encapsulate the data found in EAP frames into appropriate AAA messages and transfer them from the NAS to the AAA server. However, EAP authentication methods that are based on a Transport Layer Security Tunnel, such as EAP-TLS, EAP-TTLS, PEAP or EAP-FAST and others, appeal more to our research not only because they are more secure, but also because they bring significant advantages to roaming users. During Phase 1 of such an authentication method, the AAA server is authenticated to the supplicant, and then a secure TLS tunnel is created between them,

which is then used from the client to submit its own authentication credentials. This process allows the supplicant to maintain its privacy as it does not disclose its authentication credentials to an intermediate AP or AN, but ensures that these are only transmitted to the AAA server over the tunnel they have established. Of particular importance for our research are EAP-TLS [13] and EAP-TTLS [5]. During Phase 2, where the AAA server authenticates the client, EAP-TLS uses a client's certificate, whereas EAP-TTLS uses a password in a hashed format, usually dictated by another authentication mechanism such as CHAP. One important advantage that EAP-TLS and EAP-TTLS offer to roaming users, is the ability to skip Phase 2 of the authentication process if the user has been authenticated with the AAA server before. This feature is called Session Resumption (SR) and when enabled, allows the AAA server to keep a unique cache entry for a client that gets successfully authenticated once. Therefore, when the client roams to another AP requesting the same authentication procedure to occur, after completion of Phase 1, the AAA server realizes that it has a cached entry for it from its previous authentication, and thus skips Phase 2, even in scenarios where the client has not been connected to that AP before.

3.5 Wireless Security

The need for securing wireless communication is much higher for publicly available APs. The WiFi Alliance has designed WPA and WPA2 protocols to secure wireless networks by offering packet encryption, message integrity, protection against replay attacks and authorized network access with the use of cryptographic algorithms. WPA and WPA2 protocols support two authentication modes; Personal mode and Enterprise mode. When Personal mode is used, wireless clients can connect to an AP using a preshared key (PSK), whereas when Enterprise mode is used authentication is performed with the aid of a AAA backend server. One of the big advantages of the Enterprise mode of WPA2, is that after successful authentication, the wireless client and the AAA server are the only owners of a Master Key, which they then use to derive a Pairwise Master Key (PMK). The PMK is then sent from the AAA server to the AP in a secure AAA message, and is being used as a symmetric key, bound to the session of the AP and the client. With the knowledge of the PMK, a subsequent 4-way handshake is performed between the AP and the wireless node, that derives, binds and verifies additional operational keys that are used in the future communication of the node with the AP. This significant feature of WPA2 in Enterprise mode means that session keys are being securely derived and negotiated in a way that security is enhanced and preconfiguration is avoided. One additional advantage that the aforementioned key derivation procedure brings to mobile users, is that when a roaming node connects to a WPA2 AP, it firstly checks if it has a collection of keys, called PMK Security Association (PMKSA), that can be used with this AP. If this information has been cached from a previous association, then there is no need for a full authentication procedure with a AAA server, but only the 4-way handshake has to be performed locally between the AP and wireless client. PMKSA caching significantly speeds up the authentication procedure of the roaming client without compromising the security of the network.

4 Design

We devised a Unified Architecture (UA) with the goal of bridging the gap between Network Mobility and AAA services in a secure manner and satisfying the requirements of all the parties involved. Fig 1 illustrates our design where we overlay the AAA model in its extended form for roaming scenarios [10] over NEMO BS's architecture and integrate these services in a unified way. According to our design, the MN's HN now consists of a HA and a AAA Home Server (AAAHS) that are responsible for providing the Mobility and AAA services for the MN respectively, whilst it is away from its HN. Conceptually, in our bus scenario the HN could be represented by servers located at the IT department of the company or provided by an ISP offering these services. The AN depicted in Fig. 1 represents any network that can provide Internet connectivity via wireless hotspots in the area the MN roams. The AN (also known as Foreign Network) consists of its own AAA Foreign Server (AAAFS) and many APs that act as NASs and are able to exchange packets with its AAAFS. Conceptually the AN could be a wireless ISP's town network or a municipal network, offering publicly available WiFi connectivity to MNs.

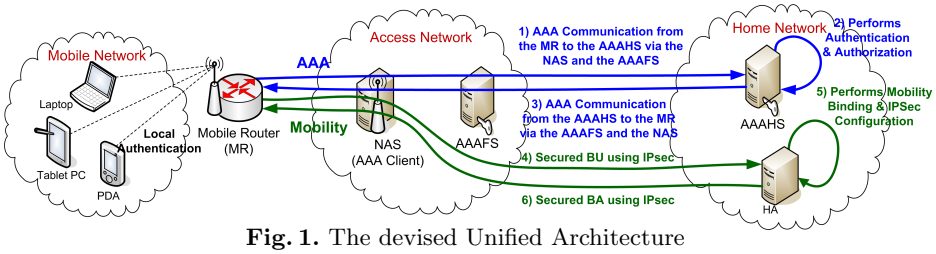

Fig. 1. The devised Unified Architecture

It is important to emphasize that our UA does neither augment nor alter the design of the AN itself, making it ready to be used in the current Internet infrastructure. What our UA requires though, is that the AN has a Service Level Agreement (SLA) with the HN of a MN, through which, the AAAFS has the ability to relay the authentication process to the MN's AAAHS. The AAAHS has evidently more appropriate information to authenticat the MR, and permit it to offer connectivity to its MNNs. This collaborative design provides important benefits to all parties involved, as the AN does not require to know the MR in advance, neither has to have any preconfigured information about it or its MNNs. In addition, if a TLS based authentication method is being used the MR avoids revealing its identity and credentials to the AN itself, as its authentication data are forwarded securely to its HN over a tunnel, after the initial authentication of the AAAHS to the MR (as described in Subsection 3.4). If the authentication procedure of the MR is successful, this means that the AAAFS has a secure partnership with the AAAHS dictated by the SLA and confirmed from the knowledge of the shared secret they use to secure the AAA packets they exchange, thus, the MR can trust the AN's AP. ANs have financial incentives to get SLAs with HNs because these would allow them to serve MNs and in turn bill their HNs appropriately for the provided service. HNs

are also interested in getting SLAs with as many ANs as possible, because the latter will serve their MNs when they are away from "home", inducing financial benefits to both network providers and bigger connectivity coverage for the end users. Our UA does not oblige the establishment of SLAs between all small-scale networks, on the contrary, it can easily facilitate a hierarchical model where only big ISPs have SLAs between each other and through them accommodate the smaller networks they provide connectivity for. This model is simply fitted into our UA by introducing a chain of intermediate AAA servers of the involved ISPs in the path between the AAAFS of the AN and the AAAHS of the HN. According to this model, each AAAFS will play the role of the proxy AAA server and forward packets to the next AAA server in the chain until data reaches an ISP that has a partnership with the MN's HN and is able to finally route these packets to the MN's AAAHS, leading to a model that scales for the real world.

Following the principle of NEMO BS, where the MR is responsible to provide the mobility service for all its MNNs without them having to run any mobility protocols themselves, our UA dictates that the MR should carry out the AAA service on behalf of the whole network as well in a similar fashion. Therefore, when the MR connects to an AN it is responsible to authenticate itself and the entire network to its AAAHS, and include the MNP of the network it is serving in its BU. This important process ensures that only MNNs of a certain IPv6 address pool are authenticated and authorized for Internet connectivity. However, since the MR is carrying the authentication procedure on behalf of the whole network, it should also perform local authentication of the MNNs connected to it, using for example WPA2/PSK or WPA2/EAP-TLS. In our bus scenario this can easily be facilitated if, for example, regular commuters subscribe to the Internet-on-the-bus service and obtain a username and password to authenticate to the bus' MR, or if non-regular commuters could get a WPA2/PSK scratch card when they purchase their ticket. The two distinct authentication procedures that our UA defines (MNNs authenticated to the MR and the MR authenticated to its AAAHS) provide important advantages in roaming scenarios. Although the MR might be changing its point of attachment from one AN to another roaming, the MNNs will experience only a slight connectivity disruption whilst the roaming take place, but none of them would have to reauthenticate after this roaming. In addition, the MNNs could join or leave the MN whenever they want, without having to "inform" a distant server about it, reducing significantly the number of packets that have to travel from the MN to the Internet (and vice versa) saving bandwidth and minimizing processing delays.

Let us now consider the phases a MR has to go through to provide Mobility, Security and AAA for all its locally authenticated MNNs, from the time it starts roaming to a new AN until it obtains full Internet connectivity. According to our design, in order for the MR to become fully operational it has to perform its Layer 2 handover, its AAA communication as required by RADIUS and the chosen TLS based authentication method, its mobility tasks as required by NEMO BS and its security related configuration, as required by the local AP it connects to and the use of IPsec for the traffic generated by or destined to its MNNs. These occur sequentially in the following three distinct phases :

• **Phase 1 - Layer 2 Association** : The MR performs the Layer 2 association with the AP of the AN it roams to.

• **Phase 2 - Layer 2 & 3 AAA Communication and WiFi Security Configuration** : During this phase the MR will request network access to the AN and will perform the AAA authentication with its HN using the RADIUS protocol (described in Subsection 3.3). Since the MR does not have an IP address yet, its communication with the AP occurs using EAP frames that carry all the required information using Layer 2 (MAC) addresses. The AAA client implementation of the AP, encapsulates the data from the EAP frames to IP AAA packets and sends them to its AAAFS. However, since we are using a TLS based EAP authentication method in our UA, the initial packets that are sent from the MN should eventually reach its AAAHS server in order to establish a TLS tunnel. In order to accomplish this, in these initial packets the MR presents its "identity" to the AP, essentially revealing only its domain name in the form of "anonymous@homenetwork.com" by complying to the standardized Network Access Identifier (NAI) (defined in [1]), and thus enabling the local AAAFS to identify where it should forward all the AAA packets to. When the AAAFS relays the initial authentication data to the MN's AAAHS, the latter forms a tunnel with the MR and carries out the full authentication process by exchanging packets back and forth according to the chosen authentication method. When the authentication process finishes, the AAAHS replies to the AAAFS of the AN, and then the later according to the authentication reply either grants network access to the MN or denies it. Authorization usually occurs after authentication and is related to the actual policies the AN and HN have in place for roaming networks. When authentication and authorization finish, and if the MN has been granted access, the MN derives secure session keys for its communication with the AP as described in Subsection 3.5, and the AAAFS starts the accounting procedure for the MN and updates the AAAHS with billing records.

• **Phase 3 - Layer 3 Mobility & IPsec configuration:** If the MR succesfully finishes Phase 2 and is granted access, it obtains a topologically correct IPv6 address either by contacting a DHCPv6 server or using IPv6 autoconfiguration. When the MR has an IPv6 address, its first task is to perform its mobility binding with its HA and at the same time to configure its security associations and apply its IPsec policies. According to [4] and [2], at this moment, the MR ensures that its control traffic to and from its HA will be secured by ESP in transport mode and all the subsequent traffic to and from its MNNs will be secured by ESP in tunnel mode. Therefore, to successfully finish Phase 3 the MR sends its secured BU with its MNPs to the HA and waits for the matching BA that denotes a successful binding and a fully operational MN.

5 Evaluation

This section describes a qualitative and quantitative evaluation of our UA.

5.1 Qualitative

Our UA brings significant benefits to both the roaming MN and the AN that serves it. Section 2 discussed the motivation behind our research. Here we revisit

the presented motivation and detail it in requirements that are satisfied with our approach. Our UA satisfies the following requirements of the MN :

1. Secure, unobtrusive and trouble-free network access :
   a) The MR does not need to be configured with different types of credentials each visiting AN requires, since the actual AAA procedure is performed with the MN's AAAHS and this configuration is known to the MR in advance.
   b) The MR does not reveal its identity to each AN it is visiting, thus keeping its privacy whilst roaming.
   c) The MR is able to establish trust dynamically with the AN it roams to, by relaying this task to its HN during its authentication. If its AAAHS does not trust the AAAFS when the latter forwards packets to the former, the AAA process fails and thus the MR should not trust the AN's AP.
2. Secure transmission of data locally, in the range of the AP using WPA/WPA2, and globally, as data leave the AN and travel to the Internet using IPsec.
3. Constant and reliable connectivity is provided with the use of NEMO BS, which in conjunction with the trouble-free network access that is provided using the AAA service, leads to seamless and quick roaming for the MN.

Our UA satisfies the following requirements of the AN:

1. Authentication of the MR without requiring to have information about it in advance. The AN relays the authentication procedure to the MN's HN that has more appropriate information to authenticate the MR.
2. Authorization of the MR according to its local policies.
3. Accounting of the MR for its MNNs' network use in order to bill its HN for the provided service appropriately.
4. All the previous transactions are performed without compromising the security policies of the AN and by bringing financial benefits to it.

5.2 Quantitative

In order to evaluate the true applicability and efficiency of our approach, we carried out a series of performance Tests on our experimental testbed. In this Section we describe the hardware and software setup of our testbed, the tests that we carried out and finally, we analyze and discuss the results observed.

Hardware and Software Testbed Setup : To evaluate the capabilities and performance of our UA we configured the testbed illustrated in Fig. 2. Our testbed consists of three Access Networks (AN1, AN2 and AN3), a MN, and the HN the MN originates from. All PCs on our testbed have a P4 2.8GHz CPU, 2GB RAM and a 80 GB hard drive and run Ubuntu 10.04 LTS. Each AN consists of two PCs, one of them acting as an AP by projecting a 802.11g wireless hotspot using the nl80211 driver and the hostapd deamon (version 0.7.3), and the other acting as the AN's AAAFS. The AP in AN1 is being configured in WPA1-Enterprise mode, whereas the APs in AN2 and AN3 are being configured in WPA2-Enterprise mode, allowing us to experiment with different wireless AP configurations. The HN consists also two PCs, one of them acting as a HA by running the NEMO BS protocol stack from [7] in HA configuration, and the other

acting as a AAAHS. All the AAA Servers on our testbed run the FreeRadius AAA Server (version 2.1.10) and have a certificate which we issued by creating a Certificate Authority. Furthermore, each AAAFS has a shared secret with the AAAHS in order to communicate with it securely. All the equipment on our testbed is IPv6 enabled. AN1 and AN2 are connected with the HN over Ethernet using native IPv6 addresses, whereas AN3 is connected to the HN over the Internet using an IPv6 Tunneling service from HE Tunnel Broker [3]. This IPv6 tunneling approach introduces approximately a 315 ms delay (630ms roundtrip) and routes all the packets from AN3 to HN and vice versa via the Internet, using global IPv6 addresses. This technique ensures that our tests are being carried out not only on a local basis, but also over a long distance route over the Internet that presents real-time traffic characteristics in the communication. The MR used in our tests runs the NEMO BS stack from [7] being configured in MR mode, with the appropriate MNPs and IPsec configuration that matches the one at its HA. Finally, the MR runs WPA_supplicant (version 0.7.3) to allow it to connect to the ANs' APs, and also runs the hostapd deamon to create a wireless hotspot for three MNNs (two laptops and an HTC Touch 2 PDA) and use its internal RADIUS functionality to authenticate the MNNs.

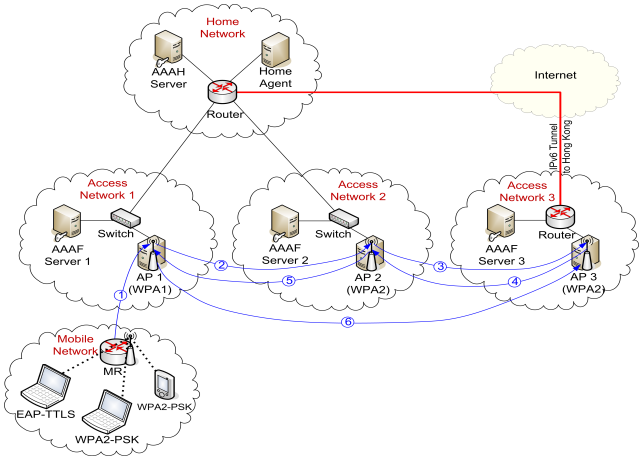

Fig. 2. Experimental Testbed

Testing Sets : The aforementioned testbed setup allows testing to take place via APs that have different configuration and over different routes, mimicking how communication would take place in an actual deployment scenario where MNNs are connected to a MR, and the MR roams from one AN to another. Following the design of our UA, we perform two separate Testing Regimes, one to test the performance of local authentication of the MNNs to the MR, and another one to evaluate the roaming of the MR from one AN to another. We repeat each Test of each Testing Regime 50 times, with the focus on how quickly the MNNs or the MR become fully operational using different authentication methods and configuration over our UA.

In our first Testing Regime we use three different MNNs (two laptops and a PDA) and record how long it takes them to connect to the MR's AP (Layer

2 association), to authenticate to it, and finally, to obtain an IPv6 address and become fully operational (Table 1). The PDA and one laptop are using WPA2-PSK for authentication, whereas the other laptop is using EAP-TTLS. Our second Testing Regime, includes four different Tests where the MR authenticates to the ANs using EAP-TLS without SR (Test 1, Table 3), EAP-TLS with SR (Test 2, Table 4), EAP-TTLS without SR (Test 3, Table 5) and EAP-TTLS with SR (Test 4, Table 4) respectively. Each Test includes six roaming movements (Stages) of the MR from one AP to another which are presented in Fig. 2 in blue arrows, associating the MR with AP1, AP2, AP3, AP2, AP1 and finally AP3. We decided to perform the aforementioned roaming movements because they demonstrate realistic scenarios, where a MR might connect repeatedly to the same AP, or swap from one AP to another repeatedly.

Results : Table 1 details the results from our first Testing Regime where our three MNNs connected to the MR'S AP, authenticated to it using WPA2-PSK or WPA2-EAP-TTLS and obtained an IPv6 address from the MNP the MR advertised. Although the results from this Testing Regime seem very reasonable, we could note the significant difference on the average time it takes for the PDA to do its WPA2-PSK authentication (3.690 sec.) compared to the laptop's average time (0.05 seconds), which is attributed to the big difference on the resources the two devices have. All three MNNs remained connected constantly to the MR and were transmitting packets while we were performing the roaming Tests of the second Testing Regime that follow.

	WPA2-PSK PDA	**WPA2-PSK LAPTOP**	**WPA2-EAP-TTLS LAPTOP**
Layer 2 Assoc. (sec.)	2.585	2.300	3.670
Layer 3 Auth. (sec.)	3.690	0.050	0.320
Layer 3 IP (sec.)	3.167	2.390	1.905
Total (sec.) :	9.442	4.740	5.895

Table 1. Authenticating MNNs to the MR

# of Packets	**TEST 1**	**TEST 2**	**TEST 3**	**TEST 4**
Stage 1	7/14	7/16	7/16	7/16
Stage 2	5/14	5/6	5/16	5/6
Stage 3	5/14	5/6	5/16	5/6
Stage 4	4/0	4/0	4/0	4/0
Stage 5	7/14	7/6	7/16	7/6
Stage 6	4/0	4/0	4/0	4/0

Table 2. Local/Global number of Packets for Phase 2

For our second Testing Regime we performed four different Tests where we roamed the MR of the MN, and essentially the whole MN from one AP to another in Six Stages using four different authentication methods and configuration. Before focusing on the results of the different authentication methods (noted as Phase 2 on each Table), we could note that Phase 1 results (Layer 2 Association) were similar in all Tests, varying from 0.883 seconds to 1.499 seconds. Similarly, Phase 3 results in all Tests, where the MR configures an IPv6 CoA, performs its

Stages / Phases	ST.1	ST.2	ST.3	ST.4	ST.5	ST.6
Phase 1 (sec.)	1.208	1.045	1.084	0.959	0.969	1.016
Phase 2 (sec.)	0.780	0.208	4.549	0.014	0.690	0.009
Phase 3 (sec.)	1.630	1.585	2.310	1.833	2.123	2.433
Total (sec.) :	3.618	2.838	7.943	2.806	3.782	3.458

Table 3. EAP-TLS Results without Session Resumption

Stages / Phases	ST.1	ST.2	ST.3	ST.4	ST.5	ST.6
Phase 1 (sec.)	1.110	0.985	0.883	1.068	0.887	1.081
Phase 2 (sec.)	0.345	0.090	1.906	0.038	0.126	0.045
Phase 3 (sec.)	1.770	1.372	1.754	1.686	2.487	2.290
Total (sec.) :	3.225	2.447	4.543	2.792	3.500	3.416

Table 4. EAP-TLS Results with Session Resumption

binding registration with its HA and applies its IPsec policies for all the traffic the MNNs might send, did not present notable differences, varying from 1.372 seconds to 2.574 seconds.

Focusing on the results of the different authentication methods and the route they take place via, we concentrate on Phase 2 of each Test of the second Testing Regime. During Test 1 of our second Testing Regime, the MR used EAP-TLS without SR and roamed from one AN to another as presented in Fig. 2. As Table 3 illustrates, in Stage 1 the MR connected to AP1 and carried out its EAP-TLS authentication in approximately 0.780 seconds, which is remarkably low, since this phase requires 21 packets to be exchanged in total. As Table 2 presents, 7 out of the 21 packets are transmitted locally between the MR and the AP, and 14 are transmitted "globally", following a 3 hop route from the MR to the AN's AP, then to the AAAFS and finally, to the MR's AAAHS. In Stage 2 of Test 1, the MR roamed to the WPA2 AP2, and did its EAP-TLS authentication faster and transmitted two less local packets. Stage 3 consists of the MR being connected to AP3, where all the Phase 2 packets are routed to the AAAHS over the IPv6 tunnel to Hong Kong. The tunnel overhead increased Phase 2 timing to an average of 4.549 seconds, almost 10 times more compared to the previous Stages. This is an expected delay as 14 packets have now to travel over the IPv6 tunnel which adds significant delay6. The results from Stage 4, where MR roams to AP2 where it has been connected before in Stage 2, illustrate the benefits of PMKSA caching of WPA2, as the MR does not perform a full EAP-TLS authentication, but just a 4-way handshake. With PMKSA caching Phase

Stages / Phases	ST.1	ST.2	ST.3	ST.4	ST.5	ST.6
Phase 1 (sec.)	1.299	1.207	0.932	0.961	1.491	1.090
Phase 2 (sec.)	0.335	0.242	5.124	0.010	0.335	0.015
Phase 3 (sec.)	1.876	2.269	2.574	2.320	1.763	2.340
Total (sec.) :	3.510	3.718	8.630	3.291	3.589	3.445

Table 5. EAP-TTLS Results without Session Resumption

Stages / Phases	ST.1	ST.2	ST.3	ST.4	ST.5	ST.6
Phase 1 (sec.)	1.603	2.086	0.977	0.981	0.845	1.090
Phase 2 (sec.)	0.291	0.055	1.888	0.022	0.080	0.032
Phase 3 (sec.)	1.554	1.544	2.660	2.222	2.620	2.220
Total (sec.) :	3.448	3.685	5.525	3.225	3.545	3.342

Table 6. EAP-TTLS Results with Session Resumption

2 of Stage 4 completes in just 0.014 seconds, almost 15 times less compared to Phase 2 of Stage 2, when the MR connected to AP2 for the first time. Stage 5 is where the MR connects to AP1, where, although it has been connected to before, as it is a WPA1 AP, it does not support PMKSA caching and thus records similar timings with Stage 1. Stage 6 further affirms the advantages of PMKSA caching, as Phase 2 completes only in 0.009 seconds despite the tunnel setup to Hong Kong, since only the local 4-way handshake is required. Due to PMKSA caching, 15 packets less are now being exchanged in Stage 6 compared to Stage 3, which also leads to a reduction of approximately 4.5 seconds of the total time it takes for Stage 6 to complete.

Test 2 of the second Testing Regime, repeats Test 1 but with the SR feature enabled at the AAAH Server. During Phase 2 of Stage 2 of this Test, the AAAHS realized that the MR had performed a successful authentication with it some seconds ago (during Stage 1) and thus skips the second part of the EAP-TLS procedure. As Table 2 presents, only 6 packets compared to 14 are now exchanged in Phase 2, which completes in only 0.090 seconds (Table 4), more than twice as fast compared to Test 1 when SR was disabled. Further demonstration of the benefit of SR is illustrated in Stage 3, where again only 6 packets are transmitted over the tunnel, reducing the time of this Phase to just 1.906 seconds compared to 4.549 seconds of Test 1. Stages 4 and 6 present similar results with Test 1, as PMKSA caching takes effect. During Stage 5, SR affirms its advantages again, with a significant reduction of Phase 2 timing down to 0.126 seconds compared to 0.690 seconds of Stage 5 of Test 1, since PMKSA caching is not applicable as AP1 is in WPA configuration. Overall, it has to be noted that the SR feature, where applicable (Stages 2, 3 and 5) has demonstrated significant advantages and reduction in Phase 2 timings compared to Test 1 and further improved the overall timings of the Stages where PMKSA caching was not applicable.

To further evaluate our UA we repeated Tests 1 and 2 using a different authentication method, namely EAP-TTLS, that uses a username/password pair to authenticate the MR instead of a certificate. As Table 5 shows Phase 2 timings in this Test, are in similar levels with Test 1 although the number of "global" packets now required for EAP-TTLS are now 16, compared to 14 in EAP-TLS (Table 2). During Stage 3 we observed an expected increase of the timing of Phase 2, as now more packets have to travel over the IPv6 Tunnel and thus the additional delay is reflected in the results. However, once again, Phase 2 timings of Stage 4 and Stage 6 are remarkably low, thanks to PMKSA caching which prohibits the need for any "global" packets exchange.

Finally, Test 4 repeats Test 3 with SR being enabled at the AAAHS. All the overall timings of this Test (Table 6) are decreased compared to those of

Test 3, as both Session Resumption and PMKSA caching are triggered where applicable. In particular, Phase 2 timings for Stages 2, 3 and 5 are remarkably low (0.055 seconds, 1.888 seconds and 0.080 seconds respectively), because SR reduces the number of "global" packets that needed to be exchanged from 16 down to 6 (Table 2). Phase 2 of Stages 4 and 6 of this Test, required only 4 local packets to be exchanged, compared to 21 in total for a full EAP-TTLS authentication with a WPA2 AP, because again PMKSA caching was enabled and ensured that only the 4-way handshake was performed.

6 Conclusion

In this paper we presented a UA that combines the strengths of NEMO BS and AAA services in a secure way and satisfies the requirements of both MNs and ANs. Our UA enables roaming MNs to experience constant Internet connectivity with trouble-free but secure network access, and secure transmission of their data despite their frequent roaming. Using our UA, ANs are able to provide efficient and secure AAA services in a profitable fashion. Our qualitative evaluation discussed the merits of our approach and how it satisfies the requirements of all the parties involved. The results from our thorough quantitative evaluation with different authentication methods and configuration, demonstrated the performance and applicability of our approach for a real world deployment.

References

1. Aboba, B., Beadles, M., Arkko, J., Eronen, P.: The Network Access Identifier. IETF RFC 4282 (Dec 2005)
2. Arkko, J., Devarapalli, V., Dupont, F.: Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents. IETF RFC 3776 (Jun 2004)
3. Hurricane Eectric IPv6 Tunnel Broker: http://www.tunnelbroker.net/
4. Devarapalli, V., Wakikawa, R., Petrescu, A., Thubert, P.: NEMO Basic Support Protocol. IETF RFC 3963 (Jan 2005)
5. Funk, P., Blake-Wilson, S.: Extensible Authentication Protocol Tunneled Transport Layer Security (EAP-TTLSv0). IETF RFC 5281 (Aug 2008)
6. Georgopoulos, P., McCarthy, B., Edwards, C.: Towards a Secure and Seamless Host Mobility for the real world. In: 8th International Conference on Wireless On-demand Network Systems and Services (WONS2011), Italy (To appear)
7. Umip Mobile IPv6 Stack: http://umip.org/
8. Johnson, D., Perkins, C., Arkko, J.: Mobility Support for IPv6. IETF RFC 3775 (Jun 2004)
9. Kent, S., Seo, K.: Security Architecture for the Internet Protocol. IETF RFC 4301 (Dec 2005)
10. de Laat, C., Gross, G., Gommans, L., Vollbrecht, J., Spence, D.: Generic AAA architecture. IETF RFC 2903 (Aug 2000)
11. Perkins, C.: IP Mobility Support. IETF RFC 2002 (Oct 1996)
12. Rigney, C., Willens, S., Rubens, A., Simpson, W.: Remote Authentication Dial In User Service (RADIUS). IETF RFC 2865 (Jun 2000)
13. Simon, D., Aboba, B., Hurst, R.: The EAP-TLS Authentication Protocol. IETF RFC 5216 (Mar 2008)