Towards a Secure and Seamless Host Mobility for the real world

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

***Abstract*—Mobile IPv6 has been developed for quite a few years now, but it has yet to bring its constant connectivity and global reachability benefits to mobile devices in real world scenarios, mainly due to lack of trouble-free and secure network access and data transmission for devices as they roam. In this paper we propose a Unified Architecture that combines the strengths of Mobile IPv6 and AAA services and closes the gap between the Mobile Node and the Access Network's requirements. Our approach provides a comprehensive solution in a setting where users require seamless roaming, secure network access and secure data transmission in a dynamic fashion as they commute, whereas Access Networks require powerful AAA services without compromising their security policies. The qualitative and quantitative evaluation of our Unified Architecture through thorough laboratory tests, demonstrate the efficiency of our approach and highlight its potential and suitability for real world deployment in the current Internet architecture.**

***Index Terms*—Mobile IPv6, AAA, Security, Host Mobility**

I. Introduction

The number of mobile devices, varying from PDAs to smartphones, tablet-PCs, notebooks or laptops, that people use every-day to obtain Internet connectivity as they commute, has been largely increased to tens of millions during the last two decades. It is without doubt that this number will continue to increase in the near future and more and more people would like to get advantage of Internet connectivity on-the-go, and be able to do all their every-day online tasks on-demand, no matter where they are, from their mobile devices.

From a networking perspective, when a mobile device (also referred onwards as Mobile Node - MN) connects to a wireless Access Network (AN), it obtains an IP address that is topologically correct and allows the device to transmit and receive packets to the global Internet. A mobile device at the hands of a commuter who, for example, goes to his office in the morning, will high likely have to connect to quite a few different wireless ANs and also try to roam from one to another as quickly and seamlessly as possible to facilitate the user's connectivity requirements. However, following the principles of the IP protocol, when a MN associates to a new AN, it has to change its current IP address, thus causing its connections and in turn its applications' sessions to break, causing nothing but frustration to its user. Mobile IP, being Mobile IPv4 [1] or Mobile IPv6 [2], has been developed for a few years now to facilitate this MN's roaming, also dubbed as host mobility, and provide efficient roaming, seamless connectivity and global reachability for the MN, no matter where its point of attachment is or how frequently it roams. Mobile IP guarantees that a roaming MN is constantly reachable at its address on its Home Network (HN), by mapping it with any new IP address the device acquires when connecting to a new AN, thus providing great benefits to roaming users.

However, Mobile IP is not seeing large scale real world deployment and thus does not benefit commuters because, in our opinion, secure network access for MNs and secure transmission of their data via the AN are not ensured. Mobile IP was designed with the goal to provide constant connectivity for a roaming user, and assumes that the user has an easy way to quickly connect to any available Access Points (APs) even from different ANs. To make things more difficult, nowadays it is not enough for a roaming MN to just connect to an available third party wireless AP and obtain untrusted connectivity; secure network access to the AP is a necessity. In addition, a MN requires secure transmission of its data, both locally, in the vicinity of the wireless AP that is connected to, and globally, as data leave the wireless network and travel to the Internet. Although more and more ANs are nowadays configured to provide secure access and transmission of data, the problem still exists and lies in the fact that MNs cannot establish a trustworthy association with the AN quickly and in a dynamic fashion, and allow them to perform their security configuration automatically and unobtrusively to the user. Authentication, Authorization and Accounting (AAA) procedures can provide solutions to the aforementioned problems where users require seamless roaming, secure network access and data security in a dynamic fashion, and ANs require granting and maintaining secure and authorized network access to and for the MNs, whilst keeping accounting records.

This paper describes a Unified Architecture (UA) that combines the strengths of Mobile IPv6 and AAA services to satisfy the requirements of both the MNs and the ANs. The rest of the paper is organized as follows. Section II discusses the motivation behind our research and Section III gives some background information on its cornerstones. Section IV provides the design of our UA and Section V evaluates qualitatively and quantitatively our approach. Finally, Section VI concludes this body of work and highlights its benefits.

II. 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 stockbroker who commutes from his house to his office every day, by doing a short walk through the town centre, then taking the train for a twenty minute ride to a station where the company's van is going to pick him up with other fellow employers and take them to the office. During this morning ride the stockbroker uses his Internet enabled PDA to learn the news that affect the stock market worldwide and get prepared for the business day. Therefore, during this ride he constantly listens to the news from an online streaming radio service, he skims the headlines of a few news portals, he checks the rates of important shares in foreign stock markets and he replies to some clients' emails, all, over the Internet.

It is apparent that as the stockbroker commutes from his house to the office he requires constant, uninterrupted and reliable Internet connectivity from the different ANs he encounters during this morning ride. It is also evident that he needs secure network access quickly and trouble-free, without him having to configure different type of credentials to comply with the variety of authentication mechanisms the different available ANs he encounters on his way to his office require. Ideally, the stockbroker's device would like to dynamically establish some sort of trust with the ANs it connects to, so that he would avoid being connected to freely available, but deceitful ANs, that would try to sniff his authentications credentials and hack into the transmitted packets. At the same time, the stockbroker's device would like to be granted secure network access in an authenticated way, without revealing its identity directly to the AN, for privacy purposes. Finally, he also requires secure data transmission and reception over the wireless medium, no matter what AN he uses to acquire connectivity from or how frequently he roams.

On the other end, AN providers need some incentive for setting up and administering wireless networks in towns or transportation means that would allow commuters to acquire connectivity from. Financial benefits is always an important incentive for providers, however it should not compromise the need for strong security policies. ANs require a way to authorize clients and account their network usage according to their own AAA policies. Providing secure and authorized access and transmission of data on their networks is very important for ANs, not only because clients will favor these networks compared to insecure ones and will agree to pay for using them, but also in order to prevent unauthorized users to perform illegal activities over theirs networks. Therefore, ANs require well configured and refined AAA procedures for all the MNs that require access. At the same time, is is unrealistic to expect that all different ANs would have the appropriate means to authenticate all roaming users requesting network access. Therefore, efficient and reliable cooperation of providers is also required for a robust service, which can be established based on Service Level Agreements (SLA) between the cooperating parties.

However, the reality today goes against the aforementioned requirements of both the MN and AN. Although the number of publicly available APs from ANs nowadays is increasing, not only are they not open and free for use by commuters, but they require in advance configuration with different types of credentials according to each AN's AAA and security policies. The lack of a standardized authentication method in conjunction with the plethora of types of authentication credentials, varying from a username and password pair, to a one-time key or use of certificates being issued by different certificate authorities, makes the problem even worse. In this setting of troublesome authentication, where an individual has to spend a considerable amount of time configuring its device instead of being benefited from Internet connectivity, Mobile IP cannot even begin to operate and provide seamless and constant connectivity when the user roams, since the user cannot get trouble-free network access in the first place. The requirement of secure data transmission after the user is connected to an AN is an additional ordeal, as the user has to set up certain security configuration on his device (e.g. preshared keys) according to the policies of each AN, which again, makes him spending time on configuration instead of his actual task. The reality from the AN's point of view, is that instead of having a cooperative and secure architecture among different ANs that satisfies the users' connectivity requirements whilst offering secure AAA procedures and financial benefits to the AN, we observe a competing setting which is, eventually, more expensive and less efficient for the ANs. ANs end up in trying to set up and administer as many APs as possible, in an effort to lure as many users as possible, and neglect the fact that they will never achieve full connectivity in all places, neither will have a database with all the possible roaming users requesting network access. A more cooperative model where both the AN and the HN that a user originates from get financial benefits without compromising their security and AAA procedures, and at the same time, the user has the opportunity to experience constant, trouble-free and secure connectivity as he commutes, is required, and will bring benefits to all parties involved.

III. Background

This section introduces the cornerstones of this research work; Mobile IPv6, IPsec, the Radius AAA protocol, TLS based authentication methods and wireless security protocols.

A. Mobile IPv6

Mobile IPv6 is designed to facilitate host mobility and allows a MN that moves from one network to another to maintain seamless connectivity and be constantly reachable via a permanent IPv6 address, even though it changes its point of attachment and has to change IP addresses as it roams. Mobile IPv6 provides seamless host mobility and maintenance of transport and application layer connections to a roaming MN, by transparently maintaining a binding between two differently scoped IP addresses, namely a Home of Address (HoA) and a Care of Address (CoA). The HoA is a permanent IP address that has been assigned to the MN at its own Home Network (HN), and the CoA is the IP address that the MN obtains when visiting a Foreign Network (FN) (term interchangeably used with AN), which is any other network

than its own. The binding between the HoA and the CoA is maintained by a mobility agent at the MN's HN, dubbed as Home Agent (HA), which is responsible to keep track of the MN's mobility using a registration procedure. Every time the MN roams to a new AN and acquires a new CoA, it sends a Binding Update (BU) to its HA containing that address. The HA after validating the contents of the BU, it stores its data in a binding table and sends a Binding Acknowledgment (BA) to the MN to denote a successful binding. A successful binding, automatically establishes a bi-directional tunnel between the HA and the MN, over which all the future traffic will occur (as illustrated in Fig. 1). Onwards, every packet sent from a Correspondent Node to the HoA of the MN will be intercepted from the HA and redirected using tunneling to the CoA of the MN dictated by an entry in the HA's binding table. If the MN roams to another AN, then the only task it should perform in order to maintain its connectivity, would be to deregister its previous CoA and repeat its registration procedure with the CoA it obtained from the AN it just connected to.

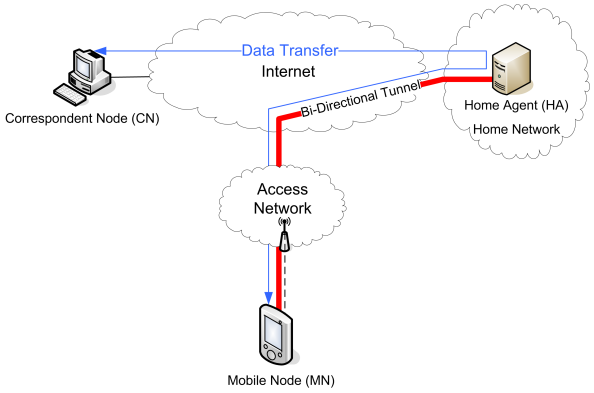

Fig. 1. Data Transfer in Mobile IPv6

B. IPsec

IPsec [3] is a protocol suite for establishing secure IP communications between peers (hosts or gateways) over an insecure network. IPsec uses a combination of different protocols to provide mutual authentication, data confidentiality, data integrity, non-repudiation and anti-replay protection in a per packet basis without any regard to the communication path between parties. IPsec mainly uses three different 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 and parameters of the secure communication channel that IPsec will operate upon. AH and ESP cryptographic protocols are used in two different modes, transport mode, where protection is provided from the Transport layer and higher, and tunnel mode, where protection is provided for the whole packet. The exact protocol and mode used is determined from the requirements of the application scenario. Both [3] and [4] discuss the use of IPsec in Mobile IP scenarios and mandate its use to avoid attacks such as man-in-the middle, hijacking, passive wiretapping or impersonation attacks. ESP in transport mode is mandated to protect control traffic between the MN and the HA in both directions, whereas ESP in tunnel mode could optionally be used to protect all the application traffic the MN generates and is being sent via the AN the MN is connected to. This is the IPsec configuration which we will follow in our UA.

C. RADIUS AAA Protocol

The RADIUS AAA protocol [5], which we will be using in our UA, is the most well known and widely deployed AAA protocol worldwide. Its functionality is build on the generic AAA framework defined in [6] and mainly involves three entities; the user's device (supplicant), the Network Access Server (NAS) and the AAA server (Fig. 2).

The process for performing a AAA service for a wireless device using RADIUS is as follows (see Fig. 2). 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, to 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 consists of a AAA client implementation that is responsible to collect all the information the supplicant sends in e.g. EAP frames, convert it to Attribute Value Pairs and encapsulate them in AAA packets. In turn, these packets will be encrypted with a strong key the NAS shares with the AAA server and finally send these packets to the server. When the AAA server receives these packets, it authenticates the supplicant using the chosen authentication method, and optionally, with the aid of other resources, such as local databases or a PKI. If authentication is successful then 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, and sometimes comply with specific configuration requirements of the supplicant (e.g. provide an IP address from a certain address pool), it replies using AAA packets to the NAS, which is then responsible to relay the AAA's 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 in regular intervals.

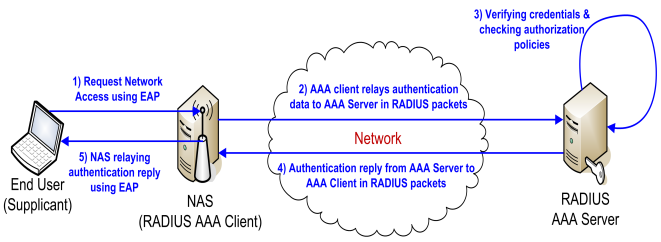

Fig. 2. Authenticating and Authorizing a MN using RADIUS

D. 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 end client (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 maintains the client's privacy by preventing it to reveal its identity and credentials to an intermediate AP or AN, and ensures that these are transmitted to the AAA server only over the tunnel they have established. Of particular importance for our research are EAP-TLS [7] and EAP-TTLS [8]. During Phase 2, when 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 an additional authentication mechanism such as CHAP. One important advantage that EAP-TLS and EAP-TTLS offer to roaming users, is the ability to skip completely 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 is enabled at the AAA server, when an end client is authenticated fully with the AAA server once, the latter keeps a unique entry in its cache for that client. Therefore, when the node roams to another AP requesting the same authentication procedure to occur, after completion of Phase 1 the AAA server realizes that it knows the user based on its cached entry from the previous authentication of the client and thus skips Phase 2. SR brings significant advantages for roaming users as the need for transmitting extra packets back and forth for a full authentication might be costly both in terms of time and money. SR speeds up the authentication process even though the user might have been roaming to a new AP, with which it has not performed an association before.

E. Wireless Security

The need for securing wireless networks is much higher when ANs deploy APs publicly to offer connectivity for commuters. The WiFi Alliance in the process of defining the 802.11i standard 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 different 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, much more complex authentication schemes can be supported since 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 an 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 of the wireless client with the AP, 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 ups the authentication procedure of the roaming client without compromising the security of the network.

IV. Design & Configuration

In order to be able to bridge the gap between Mobile IP and AAA services, we created a unified design that combines the respective architectures and satisfies the requirements of all parties involved. Fig. 3 presents our devised Unified Architecture (UA) where we overlay the AAA model in its extended form for roaming users [6], over Mobile IPv6's architecture and integrate them in a unified way. According to our design, the HN of a MN now consists of the HA that is responsible to provide the Mobility service for the MN while it is away, and the AAA Home Server (AAAHS) that is responsible to provide the AAA service when the MN roams to foreign ANs. Conceptually, the HN represents either a small home network at the house of the owner of the MN, or his organization's network or his ISP that provides these services for the MN while commuting. The AN on the other hand, represents any network that the MN could encounter during its commuting that can provide Internet connectivity usually over an AP that projects a wireless hotspot in the vicinity 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 for the AN and are able to exchange packets with the AAAFS. Conceptually the AN could be a small cafe at a town's centre offering WiFi connectivity to its customers, or a bigger University campus' WiFi network or even a publicly available WiFi municipally network, being offered by static hotspots scattered in a town or moving ones installed in public transportation offering connectivity to commuters.

It is important to emphasize that our UA does neither augment nor alter the design of the AN itself, making our

devised UA 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, which evidently has more appropriate information for authenticating the MN. This provides important benefits to all parties involved, as the AN does not require to know the MN in advance, neither has to have any preconfigured information about it. In addition, if a TLS based authentication method is being used the MN 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 MN (as described in Subsection III-D). If the authentication procedure 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 that they use to secure the AAA packets they exchange, thus, the MN can trust the AN's AP. ANs have financial incentives to get SLAs with HNs because these would allow them to serve MNs that are away from their HNs and in turn bill them appropriately for the provided service. On the other end, HNs are interested in getting SLAs with as many ANs as possible because the latter will serve their users when they are away from "home", inducing financial benefits to both network providers and bigger connectivity coverage and support 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 them 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 will forward packets to the next AAA server in the chain until data reach 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.

Let us now consider the phases a MN has to go through from the time it starts roaming to a new AN until it obtains full Internet connectivity. According to our design, in order for the MN 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 Mobile IPv6 and its security related configuration, as required by the local AP and the use of IPsec for MNs. These occur sequentially in the following three distinct phases :

• **Phase 1 - Layer 2 Association** : The MN 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 AN will perform the AAA procedure with the MN using RADIUS protocol according to the procedure described in Subsection III-C. Since the MN 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. As discussed previously, the AAA client implementation of the AP, converts the data from EAP frames to AVP attributes which are encapsulated in IP AAA packets and are sent to its AAAFS. According to the requirements of a TLS based EAP authentication methods, which we choose for our UA, the initial packets that are sent from the MN should reach its AAAHS server over a TLS tunnel. In order to accomplish this, in these initial packets the MN presents its "identity" to the AP by complying to the standardized Network Access Identifier (NAI) (defined in [9]). Therefore, the network access request from the MN should contain the domain name of the HN it originates from, in the form of "anonymous@homenetwork.com" and thus enables the local AAAFS 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 MN and carries out the full authentication process by exchanging a lot of 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 strictly related to the actual policies the AN and HN have in place for roaming users. 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 III-E, and the AAAFS starts the accounting procedure for the MN and updates the AAAHS with billing records sent in a batch format at a regular interval.

• **Phase 3 - Layer 3 Mobility & IPsec configuration:** If the MN successfully finishes Phase 2 and is granted access, it obtains a topologically correct IPv6 address by contacting a DHCPv6 server or configures it by listening to Router Advertisements. When the MN has an IPv6 address, its first task is to perform its mobility binding with its HA and at the same time to enable its IPsec configuration so that each packet it transmits is secured by IPsec according to the configuration defined in [4]. As described in Subsection III-B, at this moment, the MN configures its security associations and applies its IPsec policies to ensure that its control traffic to and from its HA will be secured by ESP in transport mode and all its subsequent traffic will be secure by ESP in tunnel mode. Therefore, to successfully finish Phase 3 the MN sends its secured BU to the HA and waits for the matching BA that denotes a successful binding and a fully operational MN.

V. Evaluation

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

A. Qualitative

Our UA brings significant benefits to both the roaming MN and the AN that serves it. Section II discussed the motivation

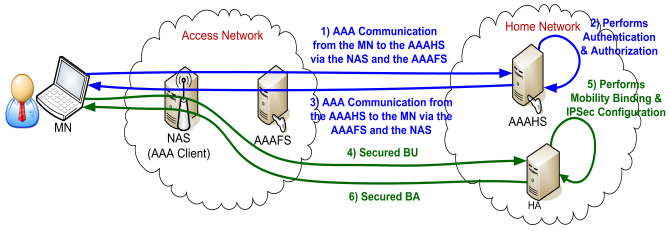

Fig. 3. The devised Unified Architecture

behind our research. Here we revisit the presented motivation and detail it in requirements that are satisfied with our solution. Our UA satisfies the following requirements of the MN :

1) Secure, unobtrusive and trouble-free network access :
   a) The user does not need to configure different types of credentials according to the requirements of each AN the MN is visiting, since the actual AAA procedure is performed with its AAAHS and this configuration is known to the MN in advance.
   b) The MN does not reveal its identity to each AN it is visiting, thus keeping its privacy while roaming.
   c) The MN establishes trust dynamically with the AP it is connecting to, by relaying this task to its HN when the AAA procedure is being carried out. If its AAAHS does not trust the AAAFS when the latter forwards packets to the former, the AAA process fails and thus the MN does trust the AN's AP.
2) Secure transmission of data locally, in the vicinity of the AP using WPA/WPA2, and globally, as data leave the AN and travel to the Internet using IPsec.
3) Constant, uninterrupted and reliable connectivity is provided with the use of Mobile IPv6, 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 MN without requiring to have information about it in advance. The AN relays the authentication procedure to the MN's network that has more appropriate information to authentication the MN.
2) Authorization of the MN according to its policies.
3) Accounting of the MN for its network use in order to bill the HN of the served MN appropriately.

B. Quantitative

Having discussed the theoretical benefits that our architecture introduces by bringing together Mobile IPv6 and AAA, we wanted to evaluate the real potential of our approach on our experimental testbed by carrying out a series of Tests in order to evaluate the applicability and efficiency of our approach. 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.

1) Hardware and Software Testbed Setup: To evaluate the capabilities and performance of our architecture we configured the testbed illustrated in Fig. 4. The testbed configuration consists of three Access Networks (AN1, AN2 and AN3), a laptop acting as a MN and the HN the MN originates from. All PCs of 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 being connected over Ethernet, one of them acting as an AP by projecting a 802.11g wireless hotspot, using a D-Link DWL-AG530 wireless network card running the ath5k driver, and the other acting as the AN's AAAFS. The desktop PC operating as AP runs the hostapd deamon version 0.7.3 that is configured in WPA1-Enterprise mode for AN1 and WPA2-Enterprise mode for AN2 and AN3 to allow us experiment with different wireless AP configurations. The HN has also two Linux desktops that are connected over Ethernet using a Cisco router, one of them acting as a HA by running the Mobile IPv6 stack from [10] in HA configuration and the other acting as the AAAHS. All the AAA Servers of our testbed, run the FreeRadius AAA Server version 2.1.10 and each of the AAAFSs have a shared secret with the AAAHS in order to communicate with it securely. All the equipment of our testbed is IPv6 enabled. AN1 and AN2 are connected with the HN over Ethernet using the native IPv6 support of our laboratory, whereas we decided to connect AN3 with the HN over the Internet using an IPv6 Tunneling service from HE Tunnel Broker [11]. This IPv6 tunneling approach introduces approximately 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 present real-time traffic characteristics in the communication, such as congestion and delay. The MN used for our tests runs the Mobile IPv6 stack from [10] being configured in MN mode, with the appropriate IPsec configuration that matches the one at its HA. In addition the MN runs WPA_supplicant version 0.7.3 to allow the node to connect to the APs and perform all the AAA related tasks and local WiFi security configuration according to the chosen authentication method. Finally, we created a Certificate Authority and issued certificates with 2048 bit keys for all the FreeRadius Servers and the MN to be used during the authorization phase of the tests.

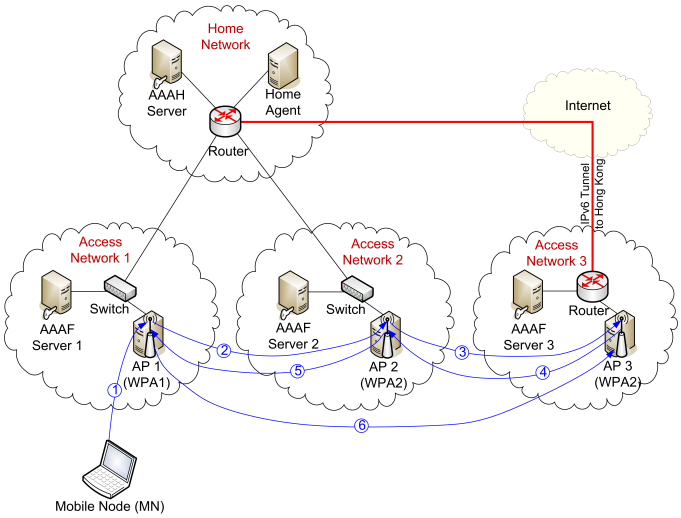

Fig. 4. Experimental Testbed

2) 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 a MN roams from one AN to another. To perform a thorough evaluation of our UA we decided to perform four different Tests, each of which consisting six Stages representing six roaming movements from one AP to another. Each Stage consists the three Phases the MN has to perform before it becomes fully operational as described in Section IV. The focus of our Tests is to see how fast these Phases are performed, i.e. how quickly the MN becomes fully operational using different authentication methods and configuration over our UA. Therefore, we repeat each Test 50 times and detail the average timing it takes for each of these Phases to complete on each Stage of each Test, and present them individually in Tables II, III, IV and V in the following Subsection.

The Tests we performed on our testbed are as follows; Test 1 uses EAP-TLS without SR, Test 2 uses EAP-TLS with SR, Test 3 uses EAP-TTLS without SR and finally, Test 4 uses EAP-TTLS with SR. For all our Tests Layer 2 handovers (Phase 1) and Layer 3 MIPv6 and IPsec tasks (Phase 3) remain the same, whereas Phase 2 is different on each Test according to the chosen authentication method. Each Test includes six roaming movements from one AP to another which are presented in Fig. 4 in blue arrows, associating the MN with AP1, AP2, AP3, AP2, AP1 and finally AP3, representing the six Stages respectively. We decided to perform the aforementioned roaming movements because they demonstrate realistic scenarios, where an individual might connect repeatedly to an AP or swap from one AP to another repeatedly. Reconnecting to the same AP, or connecting to a new one that will eventually communicate with the same AAAHS at the MN's HN, demonstrates how useful features such as PMKSA caching of WPA2 and SR of EAP-TLS and EAP-TTLS are.

3) Results: Table II shows the recorded results from Test 1 where the MN used EAP-TLS and performed all Stages by roaming from one AN to another as presented in Fig. 4. During Stage 1 of this Test, the MN connected to AP1 and performed its Layer 2 association (Phase 1) in approximately 3.9 seconds. Then, all the EAP-TLS exchange of packets (Phase 2) was carried out in approximately 0.587 seconds, which is remarkably low, since this phase requires 23 packets to be exchanged in total. As Table I presents, 7 out of the 23 packets are transmitted locally between the MN and the AP, and 16 are transmitted "globally", following a 3 hop route from the MN to the AN's AP, then to the AAAFS and finally, to the MN's AAAHS. After successfully carrying out Phase 2, Phase 3 was performed in approximately 1.63 seconds for Stage 1 of Test 1, where the MN performed its binding successfully and securely, and configured its IPsec policies to secure any future application traffic. The MN became fully operation when all Phases of Stage 1 finished, i.e. in approximately 6.121 seconds in total. In Stage 2 of Test 1, the MN roamed to the WPA2 AP2, and experienced similar results although transmitting 2 less local packets. Stage 3 consists of the MN being connected to AP3, where all the Phase 2 packets are routed to the AAAHS of the MN's HA over the IPv6 tunnel to Hong Kong. The tunnel overhead increased Phase 2 timing to an average of 5.198 seconds, almost 10 times more compared to the time it took for Phase 2 to complete in previous Stages. This is an expected delay as 16 packets have to travel using the IPv6 tunnel that adds 315ms per packet transmission. Approximately a 600 millisecond increase is also observed during Phase 3 of this Stage, as now the BU and BA of the binding the MN performs, also travel over the tunnel. The results from Stage 4, where MN roams to AP2 where it has been connected before in Stage 2, illustrate the benefits of PMKSA caching of WPA2, as the MN does not perform a full EAP-TLS authentication, but just a 4-way handshake. With PMKSA caching Phase 2 of Stage 4 completes in just 0.035 seconds, almost 20 times less when compared to the observed 0.615 seconds timing of Stage 2 when the MN connected to AP2 for the first time, leading to a considerably lower total timing for this Stage. Stage 5 is where the MN 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 0.018 seconds despite the tunnel setup to Hong Kong, since only the local 4-way handshake is required. Due to PMKSA caching, 17 packets less are being exchanged in Stage 6 compared to Stage 3, which leads to a total 5.978 seconds for this Stage, considerably lower than the overall 9.684 seconds required in Stage 3. Regarding Phase 1 timings (Layer 2 Handovers) of this Test, we observe that they vary from 1.756 seconds to 3.904 seconds, which is reasonable if we take into account the interference and variation of signal strength levels of the different APs in our testbed. Regarding Phase 3 timings of this Test, results were very consistent varying from 1.630 seconds to 1.874 seconds with the addition of approximately 630 ms in Stages 3 and 6 where the tunnel was used.

Test 2, repeats Test 1 but with the Session Resumption feature enabled at the AAAH Server at the MN's HN. As Table III presents, Stage 1 of this Test presents similar results with Stage 1 of Test 1 as nothing has in fact changed for this Stage. However, during Phase 2 of Stage 2 the AAAHS realized that the MN had performed a successful authentication with it some minutes ago (during Stage 1) and thus skips the second part of the EAP-TLS procedure. As Table I presents, only 8 packets compared to 16 are exchanged in Phase 2, which completes in only 0.064 seconds, almost 10 times less compared to the same Stage of Test 1 when SR was disabled. Further demonstration of the benefit of using SR is illustrated in Stage 3, where again only 8 packets are transmitted over the tunnel and thus the time it takes for this Phase to complete gets halved to 2.5 seconds compared to Test 1. Stages 4 and 6 of this Test present the same results as Test 1, due to PMKSA caching. During Stage 5, SR affirms its advantages again, with a significant reduction of Phase 2 timing down to 0.093 seconds compared to 0.474 seconds of Stage 5 of Test 1, since PMKSA caching

is not applicable as AP1 is in WPA configuration. Phase 1 and Phase 3 timings of Test 2 remain at similar values compared to Test 1. 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 MN instead of a certificate. As Table IV shows Phase 2 timings in this Test, were slightly decreased in Stages 1, 2 and 5 where the full authentication was performed with the AAAHS, although the number of "global" packets now required for EAP-TTLS are more, i.e. 20, compared to 16 in EAP-TLS (see Table I). This decrease is attributed to the less time it takes for the AAAHS to process the inner packets of EAP-TTLS compared to those of EAP-TLS packets that contain the client's certificate. During Stage 3 of Test 3, we observe 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 (0.015 seconds and 0.009 seconds respectively) thanks to PMKSA caching which prohibits the need for any "global" packets exchange. Generally, it can be stated that the overall timings of this Test remain at the same level of Test 1 with slight differences due to the difference of the authentication method being used.

Finally, Test 4 repeats Test 3 with SR being enabled at the AAAHS of the MN's HN. All the overall timings of this Test (Table V) 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 (0.048 seconds, 0.029 seconds and 0.095 seconds respectively), because SR reduces the number of "global" packets that needed to be exchanged from 20 down to 8 (see Table I). Phase 2 of Stages 4 and 6 of this Test, required only 4 local packets to be exchanged, compared to 27 in total for a full EAP-TTLS authentication, because again PMKSA caching was enabled and ensured that only the 4-way handshake was performed.

# of Packets	TEST 1	TEST 2	TEST 3	TEST 4
Stage 1	7/16	7/18	7/20	7/20
Stage 2	5/16	5/8	5/20	5/8
Stage 3	5/16	5/8	5/20	5/8
Stage 4	4/0	4/0	4/0	4/0
Stage 5	7/16	7/8	7/20	7/8
Stage 6	4/0	4/0	4/0	4/0

TABLE I
LOCAL/GLOBAL NUMBER OF PACKETS FOR PHASE 2

Stages / Phases	ST.1	ST.2	ST.3	ST.4	ST.5	ST.6
Phase 1 (sec.)	3.904	3.728	2.168	1.756	3.636	3.520
Phase 2 (sec.)	0.587	0.615	5.198	0.035	0.474	0.018
Phase 3 (sec.)	1.630	1.874	2.318	1.828	1.832	2.440
Total (sec.) :	6.121	6.217	9.684	3.619	5.942	5.978

TABLE II
EAP-TLS RESULTS WITHOUT SESSION RESUMPTION

Stages / Phases	ST.1	ST.2	ST.3	ST.4	ST.5	ST.6
Phase 1 (sec.)	3.818	3.696	2.204	1.878	3.572	3.485
Phase 2 (sec.)	0.469	0.064	2.500	0.028	0.093	0.011
Phase 3 (sec.)	1.906	1.672	2.264	1.734	1.806	2.256
Total (sec.) :	6.193	5.432	6.968	3.640	5.471	5.752

TABLE III
EAP-TLS RESULTS WITH SESSION RESUMPTION

Stages / Phases	ST.1	ST.2	ST.3	ST.4	ST.5	ST.6
Phase 1 (sec.)	3.731	3.334	1.795	2.210	3.652	3.614
Phase 2 (sec.)	0.379	0.369	6.347	0.015	0.365	0.009
Phase 3 (sec.)	1.912	1.786	2.484	1.849	1.752	2.462
Total (sec.) :	6.022	5.489	10.627	4.074	5.769	6.085

TABLE IV
EAP-TTLS RESULTS WITHOUT SESSION RESUMPTION

Stages / Phases	ST.1	ST.2	ST.3	ST.4	ST.5	ST.6
Phase 1 (sec.)	3.773	3.561	1.818	1.811	3.572	3.553
Phase 2 (sec.)	0.481	0.048	2.503	0.029	0.095	0.009
Phase 3 (sec.)	1.554	1.536	2.326	1.848	1.754	2.440
Total (sec.) :	5.808	5.146	6.647	3.688	5.421	6.003

TABLE V
EAP-TTLS RESULTS WITH SESSION RESUMPTION

VI. CONCLUSION

In this paper we presented a UA that combines the strengths of Mobile IPv6 and AAA services and satisfies the requirements of both MNs and ANs that provide connectivity for roaming users. 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 AAA services in a secure and profitable fashion, without compromising their security policies. Our qualitative evaluation discussed the merits of our approach and how it satisfies the requirements of all the communicating parties. The results from our thorough quantitative evaluation with two different authentication methods (EAP-TLS and EAP-TTLS), demonstrated the performance and applicability of our approach for a real world deployment.

REFERENCES

[1] C. Perkins, "IP Mobility Support," IETF RFC 2002, Oct. 1996.
[2] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support for IPv6," IETF RFC 3775, Jun. 2004.
[3] S. Kent and K. Seo, "Security Architecture for the Internet Protocol," IETF RFC 4301, Dec. 2005.
[4] J. Arkko, V. Devarapalli, and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents," IETF RFC 3776, Jun. 2004.
[5] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)," IETF RFC 2865, Jun. 2000.
[6] C. de Laat, G. Gross, L. Gommans, J. Vollbrecht, and D. Spence, "Generic AAA architecture," IETF RFC 2903, Aug. 2000.
[7] D. Simon, B. Aboba, and R. Hurst, "The EAP-TLS Authentication Protocol," IETF RFC 5216, Mar. 2008.
[8] P. Funk and S. Blake-Wilson, "Extensible Authentication Protocol Tunneled Transport Layer Security (EAP-TTLSv0)," IETF RFC 5281, Aug. 2008.
[9] B. Aboba, M. Beadles, J. Arkko, and P. Eronen, "The Network Access Identifier," IETF RFC 4282, Dec. 2005.
[10] Umip Mobile IPv6 Stack, http://umip.org/.
[11] Hurricane Eectric IPv6 Tunnel Broker, http://www.tunnelbroker.net/.