MOON: a New Overlay Network Architecture for Mobility and QoS Support

MOON: a New Overlay Network Architecture for Mobility and QoS Support

Guido Albertengo, Claudio Pastrone and Giacomo Tolu
Electronics Department
Politecnico di Torino
Turin, Italy

***Abstract*—The continuously increasing diffusion of mobile devices such as laptops, PDAs and smartphones, all equipped with enhanced functionalities, has led to numerous studies about mobility and to the definition of new network architectures capable to support it.**
Problems related to mobility have been addressed mostly operating on the network or transport layers of the Internet protocol stack. As a result, most of these solutions generally require modifying the TCP and/or the IP protocol. Although this approach is well suited to handle mobility, it lacks in compatibility with the Internet Protocol Suite.
This consideration led us to study a fully TCP compatible and flexible approach we dubbed MOON, for MObile Overlay Network. This network architecture is currently under design at LIPAR, the Internet, Protocols and Network Architecture Lab of Politecnico di Torino.

Keywords-mobility; overlay network; authentication; wireless security; 802.11i

I. INTRODUCTION

The standard Internet architecture was not thought with mobility in mind. It just provides for a point to point communication between two fixed end points and routing is simply based on fixed IP addresses. However, in a mobility environment, the point of attachment to the network of the moving end point may change, requiring a variation of its IP address. In turns, the IP address change makes a moving end point unreachable when using TCP/UDP.

This is summarized in this simple observation [1]:

"The fundamental problem is that the Internet uses IP addresses to combine the notion of unique host identifier with location in the network topology".

Over the years, several proposals have been made to overcome these limitations [2],[3],[4],[5]. Some of them operate on the network layer while others focus on upper layers such as transport or application. Unfortunately, all these approaches present several shortcomings as described in [1].

In order to overcome these problems, we started studying a new network architecture, we named MObile Overlay Network or MOON, which supports mobility in a multi-domain environment, operates at the session layer and is fully compliant with the Internet Protocol Stack.

This paper is organized as follows. In Section II we precisely define what mobility is and we specify the goals of MOON. Section III describes the architectural model used. Section IV illustrates our solution while in Section V the security in MOON is analyzed. Section VI presents a proposal of integration of authentication and mobility services. Finally Section VII summarizes the paper.

II. MOBILITY

Mobility is a broad and sometimes confusing term. Hence, it is very important to give a precise definition of what mobility really is and to distinguish all its possible forms.

The first point is to distinguish mobility from portability. We refer to *portability* as the possibility for a user to access to information and network resources wherever he is. This implies that when a user moves to a new location, he is still able to obtain the same services he had in the previous location, but all the established connections are torn down during the movement from the old location to the new one.

Mobility overcomes the limitations of portability and allows the user to gain immediate access to the network after the movement has been completed. Mobility should also keep all the previously established connections active.

We can identify several types of mobility.

Host (or *terminal*) *Mobility*: it refers to the function of allowing a mobile node to change its point of attachment to the network, without interrupting IP packet delivery to, or from, that node. Accurate location and routing procedures are required in order to maintain the integrity of the communication [6].

Network Mobility: refers to the function of allowing an entire subnetwork to change its point of attachment to the network without interrupting IP packet delivery to, or from, that mobile subnetwork [6].

Personal Mobility: rather than on devices, this type of mobility focuses users and their movements. In the case of Personal Mobility, research has focused on two aspects, both of which operate at or above the network layer in the OSI reference model. The first addresses the issues associated with enabling a user to be contacted by another user, regardless of his location and the device he is using (*contactability*). The

This work was supported by the Network of Excellence "Euro-NGI".

second addresses the issues associated with personalizing a user's operating environment regardless of the terminal or network he is using (*personalization*) [7].

Session Mobility: Session Mobility tracks communication sessions as they move, either coincident with one of the above forms of mobility or not.

Obviously, mobility is more useful than portability but it raises many new problems. The first one is the *management of mobility*. When a user moves, the point of attachment to the network of its mobile device may change but, in any case, he should be reachable even in this new location. Unfortunately, it can happen that, due to the change in the attachment point, the mobile station gets a new IP address. However, if the IP address is changed, any established TCP connection is immediately shut down, since TCP addresses are composed of a port number, that has not been changed, and of the IP host address, that has been changed.

A network architecture aiming to support mobility must introduce some mechanisms to deal with this undesired behavior of TCP.

A second problem is represented by the *access control*. Wireless networks generally have a limited bandwidth with respect to wired networks and therefore limiting the access only to authorized users, and controlling the traffic they inject in the network, becomes an important aspect.

Moreover, security is a crucial issue to be considered in a wireless environment. Before verifying what are the resources a user can access to (i.e. performing the access control), the user must be authenticated. Performing an authentication, however, might require a long time. Even though the need of authentication mechanisms is not limited to wireless networks, it is more problematic for these environments than it is for wired ones. The reasons are multiple. First of all, the interruption of the connectivity due to the time required for authenticating a user could trigger the termination of TCP connections. If this happens, the network is no more able to support mobility. Moreover, in wireless networks, authentication is expected to be performed more frequently than in wired ones due to security concerns related to the broadcast nature of the wireless medium. Examples of this are 802.11 Wireless Local Area Networks (WLANs) where authentication is required whenever the mobile device associates to a new Access Point. In particular environments with specific security constraints and where encryption is used, authentication might be also periodically carried out in order to create new encryption keys.

Summarizing, authentication mechanisms and mobility management operations affect the total handoff latency. This is a strong limitation for real-time interactive (multimedia) applications, such as (video)telephony and (video)conference or whenever tight time constraints are required.

The last problems related to mobility are *accounting* and *billing*. In some environments, indeed, wireless access could not be free; therefore mechanisms to keep track of user movements are needed to be able to charge him.

Mobility embraces a wide range of technologies and mobile devices, but in the remainder of this paper we will essentially focus on 802.11 WLANs.

More precisely, the wireless environment we will consider is based on an 802.1X [8] compliant infrastructure for authentication and on MOON for mobility support. We recall that 802.1X is a port based authentication protocol requiring a user to authenticate to get access to the network.

The goal of MOON is to identify a network architecture with the following properties:

preservation of communications: all the previously established TCP connections must be preserved during handoffs, and in general a change in the point of attachment to the network must not affect any type of communication among peers.

higher layers independence from lower layers: current implementation of the Internet protocol stack introduces a dependence of higher layers (e.g. application layer) from lower layers (e.g. IP, TCP). Indeed, most of the Internet applications use lower layers identifiers (e.g. IP addresses and TCP ports) as unique network identifiers or titles, since they usually don't change during a communication session. This is an obstacle for mobility support. To eliminate this dependence, lower layer protocols should be fully transparent to applications. In this way, handoffs among network attachment points using both identical (e.g. from Wi-Fi to Wi-Fi) and different (e.g. from Wi-Fi to UMTS) technologies have no impact on mobility. This means that they can be treated in the same, or at the least in a very similar manner.

efficient routing: the performance of routing in MOON should be comparable with the one obtained in IP routing.

efficient handoff: handoff management should be optimized in order to reduce, or avoid if possible, packet loss. Moreover, other factors (e.g. the available bandwidth) than signal strength must be used to find out when and to which access point to perform a handoff.

simultaneous mobility: a mobile architecture should be able to handle simultaneous mobility of communicating peers.

flexibility: all types of mobility should be supported.

quality of service: the architecture should be able to support QoS provided that an underlying communication infrastructure able to provide QoS is available.

security: it comprises several aspects. First of all, only authorized users can access to network resources. Furthermore, in order to guarantee privacy on the air communication, encryption mechanisms must be used. Other operations such as accounting and billing require network security as well. Finally, all the procedures regulating the overlay network behavior should be protected by possible attacks.

The basic idea behind this new architecture is to put more intelligence inside the network, despite the Internet traditional approach where complex operations are performed by end points. By acting in this fashion, it is possible to provide mobility, along with other services, as a *network service*. This

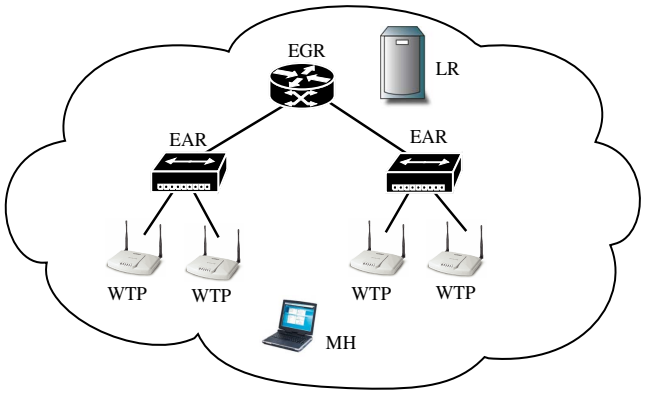

Figure 1 MOON Architecture Overview

also increases the security level of the network limiting the role of the Mobile Host (MH) in the service provision.

III. ARCHITECTURAL MODEL

Large scale deployment of Wireless Local Area Networks (WLANs), first inside enterprises and then in public areas, arose a lot of problems. They include management, monitoring and control of a large number of access devices or Access Points (APs). We can simply consider the problem of distributing and maintaining a consistent configuration of all the APs in a WLAN, or the dynamic update of wireless medium parameters in each AP to optimize the wireless medium usage, to understand the size and the complexity of this task. Securing the access to the network and preventing the installation of unauthorized APs are a further aspect to be considered. All of these issues could be treated in an easier way using a centralized approach. For the aforementioned reasons we choose as the architectural model for MOON the *Centralized WLAN Architecture* [11].

The main concept behind the Centralized WLAN architecture is the possibility to clearly distinguish between logical WLAN access network functions and individual physical devices, taking advantage of the flexibility of the 802.11 architecture.

Indeed, including 802.11 functions and services in a single device (i.e. the AP) is rather a vendor choice than a requirement of the standard. In a centralized WLAN architecture, instead, AP functionalities can be split between two components: the *Wireless Termination Point* (WTP) and the *Access Controller* (AC). Moreover, different types of centralized WLAN architectures are possible, according to the 802.11 MAC functions implemented in WTPs and ACs, respectively. Finally, WTPs and ACs can be interconnected in several fashions: for the sake of simplicity, and without loss of generality, in the rest of this paper we will only consider direct connections between a WTP and an AC.

From a security point of view, a centralized architecture significantly simplifies the management of the authentication. Moving the 802.1x authenticator functionality from a set of APs to a single AC allows grouping several WTPs (i.e. APs without authentication functionalities) in a single logical entity, so that all handoffs among them are simpler and faster. Moreover, unlike APs, ACs can be placed in a physically secure environment (a cabinet or a locked room) thus increasing the security level of the whole network.

It is important to observe that the point where MAC functionalities are implemented affects the way mobile client or *supplicant* and authenticator communicate. Indeed, if the WTP just implements the physical layer, it does not have a MAC address and the MAC advertised in beacons is the one of the AC (i.e. the authenticator). In this simple case, the supplicant can directly retrieve the authenticator MAC address from beacons, as it is currently done in Wi-Fi networks. This is not possible if the WTP has its own MAC address and a method to discover the authenticator MAC address must be found. An effective solution to this problem is to address the authenticator using the Port Access Entity (PAE) group address as specified in [8].

In the reminder of this paper, we will consider the most common scenario, where WTPs still maintain their MAC functionalities.

IV. THE MOON ARCHITECTURE

The hierarchical structure we propose for MOON is quite similar to the architecture of cellular networks and is shown in Figure 1. In MOON there are two routing entities:

Enhanced Gateway Router (EGR): it is the highest hierarchical entity in the overlay network. It is located at the border of an administrative domain and connects this administrative domain to the Internet.

Enhanced Access Router (EAR): it is an edge router with enhanced authentication and location functionalities. EARs are the entry points to the overlay network. They can be viewed as a sort of enhanced AC and, therefore, also have an active role (e.g. the authenticator) in authentication, according to the Centralized WLAN architecture paradigm. They are at the lower layer of the hierarchy.

EARs behave as the Mobile Switching Centers (MSC) of a GSM cellular network, whereas an EGR is similar to a Gateway MSC: to provide QoS and mobility for the communicating peers all IP packets are encapsulated and transferred thru virtual circuits in MOON.

To see how this happens let now examine what is inside a *Mobile Host* (MH): a *session layer handler* is used to manage inbound and outbound traffic and to control handoffs. All the packets sent from the host applications are encapsulated by the handler and delivered to the destination via the overlay network without breaking the end-to-end semantic of the connection. For native applications, new session layer sockets can be defined. However, support for legacy applications, although more problematic, can be provided as well. For this purpose, in order to masquerade IP address modifications due to the change of the point of attachment to the network caused by a mobility event, a *virtual interface* is defined. The IP address of this interface is fixed and does not change during any handoff. All the applications refer to this interface regardless of the real interface used to communicate. In this way, the applications become unaware of mobility. Finally, thanks to the session handler, it is possible to perform either horizontal handoffs (i.e. handoffs using the same real interface) or vertical handoffs (i.e.

handoffs using two different real interfaces, such as Wi-Fi and UMTS).

Hosts are the leaves of the MOON hierarchy (clients of the overlay network) and each MH is connected directly (in case of wired connections) or via a WTP (in case of wireless connections) to a single EAR.

In turns, EARs are logically grouped and interconnected with a meshed network. Each group refers to a single EGR. The switching nodes of the overlay network (i.e. EARs and EGRs) are coincident to the switching points of the underlying network in order to have a delivery path equal to the path defined by IP routing (efficient routing).

Moreover, being the overlay nodes coincident with the switching points of the "real" network no new points of failure are added.

To guarantee data delivery to the destination end point a new *session layer address space* is defined. A session address is structured in such a way that *end point location* and its globally *unique identifier* are separated, avoiding the well known problems of IP address used in a mobile environment. It is important to notice that a session between two end points is defined only by the identifier part of this address which does never change during handoffs. In such a way, simultaneous mobility can be treated as well as the case where there is only one end point in movement.

The session address for a given end point can be resolved using a DNS-like mechanism. The basic idea is to use a logical and unique name for end points. In particular, we adopted the following NAI [12] convention: *user@domain*. Subsequently, this logical name is resolved in a session address. Basing on the location information contained in this address, a hierarchic routing is performed inside the overlay network. Obviously, the location part of the session address changes whenever the end point moves.

The entity which is in charge of name resolution is called *location register (LR)*, which stores the logical name-session address mapping. Two operations are therefore needed to guarantee effective packet delivery after mobility: to update the session address (of the moving end point) contained in the location register and to redirect packets from the old EAR to the new one on the fly, using a proper signaling mechanism.

LR updating is needed in order to assure end point reachability for future sessions. Redirection, instead, is performed in order to keep all the connections alive during the handoff and reduce packet loss.

Indeed, the sending end point is not aware of the movement of the other peer until it does not receive packets from it notifying the new session address. It simply keeps sending to the old location. Using the redirection, these packets are not lost but forwarded to the new end point location. The redirection ends when the new session address is learned by the other end point involved in the communication. It is worth mentioning that the signaling protocol to be used could involve not only EARs but also EGRs if domain boundaries are crossed.

In conclusion, with respect to the most employed solution for mobility management, that is Mobile IPv4 [5], MOON presents several advantages: first of all, MOON operates at the session layer of the OSI reference model, thus avoiding all the problems related to the network layer, which are basically due to the double meaning of IP addresses (host identification and route identification).

The Mobile IP addresses this issue by forcing the MH to always use two IP addresses: a fixed home address and a care-of address changing at each new point of attachment. Thanks to the fixed address the MH may keep all its TCP connections alive even after a change in the point of attachment. For this to be achieved, a previous registration of the care-of address to the MH's home agent is necessary. In this way, all the packets directed to the MH are captured by the home agent and then forwarded to its current location. On the contrary, datagrams sent by the MH are, in most cases, directly delivered to their destination. This operation is known in literature as *triangle routing*. Moreover, it is worth mentioning that Mobile IPv4 could encounter some problems when ingress filtering is used inside the foreign network as security policy.

In MOON all the packets directed to a mobile host do not require to be addressed to its home network but are directly sent to the target instead. As a result the routing is more efficient.

Finally, the use of a session layer address allows to overcome the limitations of interconnecting hosts which belong to heterogeneous Internet address spaces (e.g. IPv4 and IPv6 public and private addresses).

Furthermore, the hierarchical structure of MOON makes it easier to manage and improves any pre-existent QoS mechanisms in the underlying network. MPLS solutions based on label switching are particularly suitable in this context.

V. SECURITY

So far we have presented the MOON principles. In this section we illustrate how the security problem is addressed in our proposed network architecture.

The most recent solution for security in wireless network is the IEEE standard 802.11i [13]. It basically relies on the 802.1x Port Based Authentication and uses the authentication messages exchanged between supplicant and authentication server (AS) via the authenticator to establish the keys required to secure on the air communications. All these keys are hierarchically related as follows:

- *MK*: the *Master Key* is at the top of the key hierarchy. It is a key shared between the AS (RADIUS server) and the supplicant (MH). It is also called the *AAA key*.
- *PMK*: the *Pairwise Master Key* is usually derived from the MK by both the supplicant and the AS. This key bonds the supplicant and the authenticator, and can also be directly obtained from a pre-shared key.
- *PTK*: the *Pairwise Transient Key* is directly derived from the PMK by the supplicant (MH) and the authenticator (AP). Actually, the PTK is a collection of three operational keys: the *Key Confirmation Key* (*KCK*), used to prove possession of the PMK, the *Key Encryption Key* (*KEK*), used to distribute the *Group*

Transient Key (GTK), and the *Temporal Key* (*TK*) used to secure the data traffic.

- *GTK*: the *Group Transient Key* is used to secure multicast or broadcast data traffic.

Full 802.11i authentication requires a lot of messages between supplicant, authenticator and AS. In order to mitigate this, 802.11i itself proposes a method (based on pre-authentication [13]) to speed up subsequent authentications on APs belonging to the same network of the first AP the MH authenticated to. However, pre-authentication can not cross subnet boundaries, limiting in this way the effectiveness of this method. Another solution presented by researchers of University of Maryland introduces the Pro-Active Key Distribution (PAKD) [15] to overcome this problem. The main idea is to pre-distribute the key material to those APs towards which the MH is likely to roam, regardless the subnet organization. The set of APs concerned in the pre-distribution is determined by means of *Neighbor Graphs*, a data structure containing, for each AP, an adjacency list (i.e. a list of all its neighbors). Nevertheless, PAKD does not take into account the possibility of a multi-domain environment.

To overcome this limitation, we choose, as authentication mechanism, the fast authentication procedures described in [14] (FAIWL). The reasons which lead us to make this decision are the following:

- it relies on 802.11i, the new IEEE standard for wireless security;
- it reduces the handoff latency caused by the authentication providing fast authentication mechanisms;
- it is thought for multi-domain environments;
- it fits the requirements of multimedia and interactive applications.

A short description of FAIWL will be provided in the following of this section.

A. FAIWL Overview

FAIWL aims to improve PAKD leveraging on a centralized WLAN architecture resulting in a more flexible, scalable and secure authentication mechanism.

The introduction of a centralized hierarchy modifies the structure of neighbor graphs, which now store a list of adjacent EARs (i.e. a group of WTPs), and the authentication process. In order to describe it, a MH and two domains are considered: the MH Home Network (HN) and a generic Foreign Network (FN). Moreover, a previously established *roaming agreement* between these two domains is assumed. At the beginning the MH is off and is in a location covered by FN.

When the MH is switched on, it must fully authenticate himself in order to gain access to the FN. This phase, which is basically the same as the 802.11i standard authentication, is crucial because during it the keys on which the fast authentication is based are created and distributed.

At the end of the authentication process, an *authentication context* for the specific MH is created. The authentication context of a MH is defined as the set of MK, PMK, user identity and MH MAC address. If, like in this case, the MH is not in its HN, this information is stored in the remote RADIUS server and then transmitted to the local AS. In this way, the FN is from now on able to treat the MH as a local host. Obviously, due to the importance of these data, the communication channel between the pair of RADIUS servers must be secure. Then the local RADIUS server is able to create the PMKs for the neighbors of the EAR currently hosting the MH, and to distribute them according to the PAKD procedure.

A full authentication is not always needed and is not the most suitable choice in some handoff scenarios. In order to understand what kind of authentication must be carried out, it is necessary to identify all the possible movements that a MH can do. This analysis leads to three different scenarios, which are:

- intra EAR movement,
- inter EAR intra domain movement,
- inter EAR inter domain movement.

In the following these three types of movement are briefly explained.

1) Intra EAR Movement

An intra EAR movement happens whenever a MH disassociates from a WTP and then associates to another WTP controlled by the same EAR. We refer to this kind of mobility as *nano-mobility* or *n-mobility*: it is expected to take place more frequently than other types of mobility which usually involve longer range movements.

Due to the likely high frequency of an n-mobility event, the authentication mechanism should be able to handle it as fast as possible. The solution proposed by FAIWL is the *Zero Authentication*. An example of the Zero Authentication conversation between a MH and an EAR is represented in Figure 3.

It consists of a challenge through which the MH demonstrates the possession of the right key material. In terms of elapsed time, we can observe that the Zero Authentication scheme only requires two local (i.e. between the EAR and the MH) round trip times against the long message flow of the full authentication.

2) Inter EAR Intra Domain Movement

An inter EAR intra domain movement happens whenever the MH handoffs between WTPs controlled by different EARs: we refer this case as *micro-mobility* or *μ-mobility*.

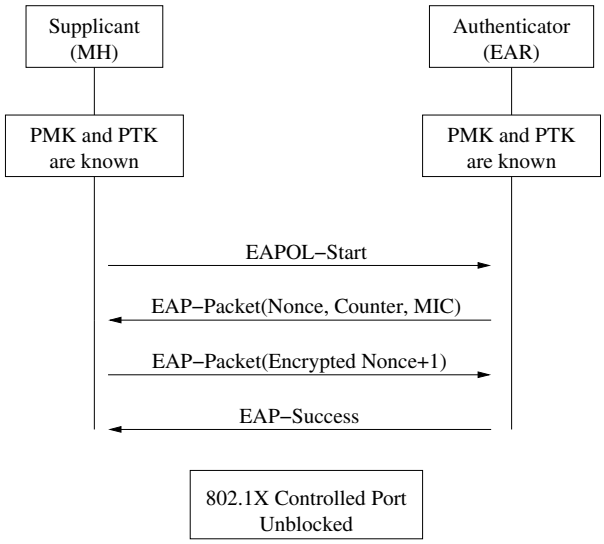

Figure 3 Zero Authentication message flow

Thanks to the pro-active key distribution, before the MH performs the handoff, the adjacent EARs already have a PMK to share with the MH.

When the EAR receives a request of authentication it checks the PMK for this MH. If it finds out that there is a correct PTK available, the Fast Authentication is started otherwise a full authentication is performed. Fast Authentication consists in the 802.11i four way handshake with two additional messages[1] (i.e. EAPOL-Start and EAP-Success) used to learn the authenticator (EAR) MAC address.

Finally, Fast Authentication does not require any interaction with the authentication (RADIUS) server, as it would be for a full authentication, and thus reduces the time required to perform the handoff. In the worst case (when the two additional messages are used), performing a Fast Authentication only takes three local round trip times and does not add any particular mechanism to the key management of 802.11i, making this mechanism easy to implement. The Fast Authentication message exchange is shown in Figure 2.

3) Inter EAR Inter Domain Movement

This scenario is the most complex, since the MH leaves a domain and enters a new one. This kind of mobility is referred to as *macro-mobility* or *M-mobility*.

In general, whenever the administrative domain is changed a full authentication is expected to be required. However, it is possible to distinguish three different cases, according to the different agreements among domains:

- no agreement,
- roaming agreement,
- trust relationship.

In the first case, the MH has no network access after the handoff, since no authentication can be performed.

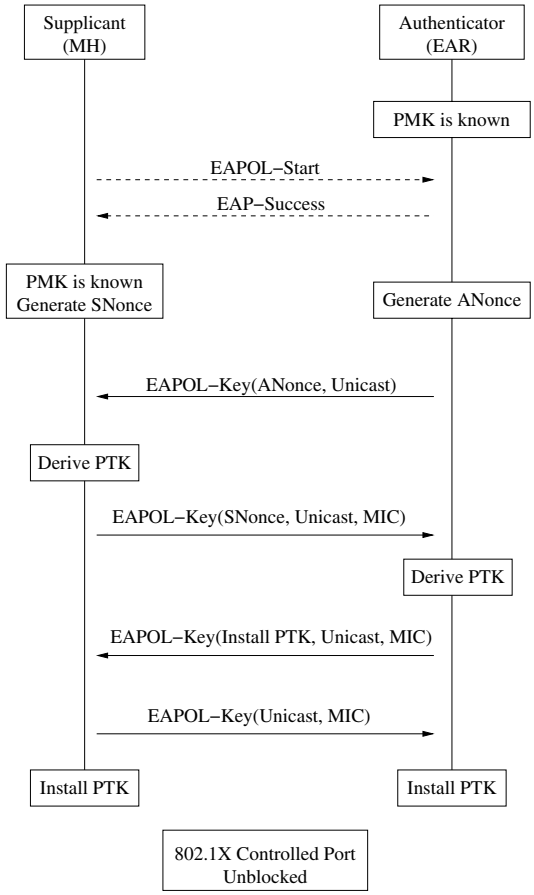

Figure 2 Fast Authentication message flow

If a roaming agreement exists, the MH can access the network after having fully authenticated himself to the new domain.

In the latter case, the MH can enter the new domain executing a Fast Authentication.

Before analyzing how Fast Authentication can be extended to a multi-domain environment, it is worth clarifying what is a trust relationship among domains. *Trust relationship* is defined as a particular roaming agreement where the authentication (RADIUS) servers of the parties involved can accept authentication context information without requiring the MH to fully authenticate himself to its home network: in a roaming agreement, the authentication context is transmitted to the local AS by the home network AS only after a successful full authentication; in a trust relationship the local AS directly receives the context from the AS of the domain from which the MH is coming. This server can either be the home AS (the MH was originally in its home network) or any other AS (the MH was already roaming in another network).

In order to manage the trust relationships among domains a new data structure called *list of trust* is introduced. This list, stored in the RADIUS server, contains all the trusted domains by the local domain.

[1] Actually, these two messages are not needed if MAC functionalities are not implemented in the WTPs.

If MH is in its home network and is preparing to roam towards an adjacent network, the context transfer is decided on the base of the HN list of trust, in case customized for the specific MH. More generally, a context transfer should be done only towards a subset of domains present in the list of trust, i.e. the ones enabled by the HN for this MH. Therefore, if MH is in a foreign network, having a local list of trust is not yet sufficient to decide whether the context of a MH is to be transmitted or not.

Let us consider the case where the MH is in a foreign network FN_1 and it is going to move to a WTP of a different foreign network FN_2. If there is not a trust relationship between the HN and the FN_2 the context of MH should not be transferred to this network even though a trust exists between FN_1 and FN_2. To solve this problem, an additional inter-RADIUS communication is proposed. When the MH enters the FN_1, this network advertises the HN for all its trusted neighbors. The HN in turns replies selecting the authorized domains for the related MH. For evident reasons such communication takes always place between the current network and the home network. Summarizing, the context of a MH belonging to a different network can be transferred to a third party only if both HN and FN_1 trust it.

Finally, it is important to point out that, using the proposed method, MHs belonging to the same network can have different sets of trusted domains. Furthermore, every change made in the list of trust is managed locally and need not be transmitted to other domains.

VI. INTEGRATING MOON AND FAIWL

In previous sections we have presented, separately, two mechanisms to manage mobility and security, respectively. The further step is to integrate these two elements in order to have a unique solution able to provide both mobility and authentication as network services. Moreover, this integration could avoid redundancy, decreasing the number of messages needed.

For this to be achieved, we propose to add to the authentication context further information useful for mobility such as the previous session address of the MH.

This information can be used, in case of roaming, by the new EAR in order to retrieve all data related to previous connections by the old EAR. In this way it is possible to redirect old sessions to the new EAR without requiring a direct MH interaction. Furthermore, authentication can be used as well to track MH in its movements. Indeed, whenever the MH moves to a new location it has to authenticate itself to gain access to the network. If the authentication successfully ends, the EAR can somehow advertise the location register of the MH of its new position. Again, the MH does not take active part in this operation.

Location updating and MH tracking are two examples of integration between mobility and authentication. More precisely, mobility can take advantage of the functionalities provided by the authentication service in order to perform secure and faster handoff.

The idea is to define a hierarchy among network services in order to allow a useful *integration* and *cooperation* among different functionalities belonging to specific network services. Integration is probably the most innovative point introduced by MOON. The advantages brought by this approach with respect to traditional solutions based on Mobile IPv4 are particularly clear when we consider the authentication of the network users which is mandatory for any wireless environment due to the nature of the physical medium. Several operations, such as the registration to a mobile agent, the location updating or the mobile host tracking are now implicitly handled by the network (and not by the mobile host) by simply elaborating the information obtained during the authentication phase. As a consequence the time required to re-connect to the network should be considerably shorter.

VII. CONCLUSIONS

In this paper we presented a new overlay network architecture called MOON which handles mobility and is fully compliant with the Internet Protocol Suite. We also described FAIWL, the security mechanism used in MOON. Finally, a proposal of integration of authentication and mobility services has been made in order to reduce time and messages required to perform a handoff.

This research activity is going on and we are currently analyzing and specifiyng the signaling protocols to be used in MOON, as well as the operations to be performed by its elements.

REFERENCES

[1] Shelley Zhuang, Kevin Lai, Ion Stoica, Randy Katz, Scott Shenker, “Host Mobility Using an Internet Indirection Infrastructure”, MobiSys '03, May 2003.

[2] Alex C. Snoeren and Hari Balakrishnan, “An end-to-end approach to host mobility”, in Proc. 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pages 155–166, Boston, Massachusetts, August 2000.

[3] Chu, Y., Rao, S. G., and Zhang, H., “A case for end system multicast.”, In Proc. of ACM SIGMETRICS’00 (Santa Clara, CA, June 2000), pp. 1–12.

[4] Jannotti, J., Gifford, D. K., Johnson, K. L., Kaashoek, M. F., and J. W. O’Toole, J., “Overcast: Reliable multicasting with an overlay network.”, in Proc. of the 4th USENIX Symposium on Operating Systems Design and Implementation (OSDI 2000) (San Diego, California, October 2000), pp. 197–212.

[5] C. Perkins, Ed., “IP Mobility Support for IPv4”, RFC 3344, August 2002.

[6] J. Manner and M. Kojo, “Mobility Related Terminology”, RFC 3753, June 2004.

[7] Binh Thai, Rachel Wan, Aruna Seneviratne, Thierry Rakotoarivelo. “Integrated Personal Mobility Architecture: A Complete Personal Mobility.” Mobile Networks and Applications, February 2003.

[8] IEEE, “IEEE Std 802.1X-2001 - Port-Based Network Access Control”, June 2001.

[9] C. Rigney and S. Willens and A. Rubens and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[10] IEEE, "IEEE 802.11-99 IEEE WLAN MAC and PHY Layer Specifications", August 1999.

[11] L. Yang and P. Zerfos and E. Sadot, “Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP)”, Internet-Draft, August 2004.

[12] B. Aboba and M. Beadles, “The Network Access Identifier”, RFC 2486, January 1999.

[13] IEEE, “IEEE Std 802.11i”, July 2004.

[14] G. Albertengo, C. Pastrone and G. Tolu, “Fast Authentication in Interconnected Wireless LANs”, submitted to IEEE International

Symposium on a World of Wireless, Mobile and Multimedia Networks - June 2005.

[15] Arunesh Mishra and Min ho Shin and Nick L. Petroni and Jr. and T. Charles Clancy and William A. Arbaugh, "Pro-active Key Distribution using Neighbor Graphs", IEEE Wireless Communications Magazine, February 2004.

[16] Alex C. Snoeren, Hari Balakrishnan, and M. Frans Kaashoek. “Reconsidering Internet Mobility”, in Proc. 8th Workshop on Hot Topics in Operating Systems (HotOS-VIII), May 2000.

[17] B. Landfeldt, Tomas Larsson, Yuri Ismailov, and Aruna Seneviratne, “SLM, a framework for session layer mobility management”, in Proc. IEEE International Conference on Computer Communications and Networks, pages 452–456, Natick, Massachusetts, October 1999.