

# A Kerberos-based EAP Method for re-authentication with integrated support for fast handover and IP mobility in Wireless LANs

Herbert Almus, Eduard Bröse, Klaus Rebenburg  
IT-Service-Center (tubIT)  
Technische Universität Berlin  
Berlin, Germany

**Abstract** — Increasing demands for open broadband access anytime and anywhere is a challenge for telecoms and Internet service providers. In addition to technologies like UMTS and WiMAX-based networks, IEEE 802.11-based WLAN technologies can contribute significantly to Open Access Networks if commonly-used services can be supported. This paper describes a solution for fast handover as well as for re-authentication including mobility support. This allows interactive services to be used when switching between WLAN access points, even if connected to different IP sub-networks.

**Keywords:** *WLAN, 802.11x, authentication, fast-handover, Open Access Networks*

## I. INTRODUCTION

Open Access Network (OAN) is nowadays a well-known buzzword. Wikipedia delivers the following short description: “In telecommunications, Open Access Network (OAN) refers to horizontally layered network architecture and business model that separates physical access to the network from service provisioning. The same OAN will be used by a number of different providers that share the investments and maintenance cost. The term was coined by Roberto Battiti 2003 in his article “Global growth of open access networks: from warchalking and connection sharing to sustainable business.”<sup>1</sup>

The term OAN doesn't say anything about the underlying technology. Instead it focuses on the idea to separate network architecture from service provisioning and implicitly suggests openness. This is why the term OAN is often used for community-provided networks especially if they are free of charge. But there are also other access networks in line with the OAN definition, which are more or less commercialized. Boingo [1], The Cloud [2], and FON [3] are well-known examples. All the actors mentioned above are using WLAN as the main technology. Public access is realized by enhancing functionality, often based on additional or enhanced equipment to be installed. Common to all these offers is that the customer has to authenticate himself to the network, obviously a prerequisite for a business model today. Some of these initiatives (e.g. LinSpot, FON) are reselling capacity, which is available based on a contract of a private user with his ISP, which may

– depending on the contract of the private user – be illegal in some cases. There are other legal aspects also to be considered. The new Data Retention Directive [4] approved by the European Parliament demands records of traffic and identification of users that connect. This is expected to be a requirement not easy to meet by some of the current offers.

The WLAN access networks mentioned before have different weaknesses compared to GSM/UMTS networks, especially regarding Quality of Services (QoS) and fast handover to support mobility. Another drawback is the exclusion of access network providers (ANPs) as well as Internet service providers (ISPs) and hence lacking the potential integration with second and third generation of mobile phone networks (2G/3G) and WiMAX.

## II. THE OBAN PROJECT

Within a project called OBAN [5] (Open Broadband Access Network), funded by the European Commission under the Information Society Technologies (IST) priority of the Sixth Framework Programme (FP6), an innovative approach has been introduced in order to establish a broadband mobile network in line with present Beyond Third Generation (B3G) visions. The architecture [6] developed in OBAN is based upon an Open Access Network (OAN) approach, but it is especially designed to be offered by telecommunication operators. The solution is characterized by the following:

- Private wireless LANs and broadband access lines are made generally available for public use, thus the stationary users (home user, HU) may use their wireless LAN as they did before
- Casually passing users (visiting users, VU) may access and maintain communication via the WLAN access points (AP) of the HUs.
- Visiting users and home users will share the access lines according to a general service agreement between users and the network operator.

The OSP installs an overlay network allowing the visitors to roam between private access points (APs) without service interruption even if the AP switched to, is operated in a network connected to a different ISP.

<sup>1</sup> See [http://en.wikipedia.org/wiki/Open\\_Access\\_Network](http://en.wikipedia.org/wiki/Open_Access_Network)

Compared to conventional cellular mobile networks consisting of a limited number of optimally located out-door base stations and antenna masts, such a network will consist of a much higher number of micro-base stations randomly located. Essential functionalities like mobility, security, QoS etc. must be implemented in the network in such a way that security and privacy requirements for owners and visitors are safeguarded, owners' and visitors' QoS requirements are met, and they fulfill requirements of any realistic business model being beneficial for the involved parties - visiting users, home users, network operator, and service providers.

Besides the aspects mentioned above, one of the objectives of the OBAN project has been to support mobility for a moving object of up to 15 km per hour. The pilot implementation within the OBAN project succeeded to support roaming between different APs including the handover of the IP sub-network, but the duration of the service interruption on network layer was around 800 to 900 milliseconds (ms). Therefore, many IP services could be used while moving, but for voice conversations, ITU-T considers delays of more than 150 ms to be unsatisfactory [7].

### III. EAP-FAMOS

Within the framework of our research activities at the Interdepartmental Research Center FSP-PV at TUB, a new EAP<sup>2</sup> method FAMOS (FAST MOBILE Secure) has been developed, implemented and tested, which allows secure and true session mobility. Only for the initial authentication, EAP-FAMOS requires the use of an (other) EAP method, which has to support keying by delivering a piece of information used as keying material (e.g. EAP-SIM). EAP-FAMOS uses the keying material, delivered during initial authentication, for its Kerberos-based solution for fast re-authentications.

Mobility is based on Mobile IPv4 (MIP) and a sophisticated handover supported by a so-called Residential Gateway (RGW) together with a Mobility Broker (MB), located in the ISP's backend network. The RGWs are enhanced DSL routers associated to a specific MB. MBs are responsible for a regional area; multiple MBs may be used because of scalability and performance issues. A MB has two major roles, to support fast handover by provisioning of location-related information and to support the fast Kerberos-based re-authentication by acting as Key Distribution Center (KDC). In our pilot implementation, the mobile terminal (client) is a notebook running under Linux, using Mobile IP and acting as EAP-FAMOS supplicant.

Current WLAN technologies do not support a "make-before-break" concept as used in GSM/UMTS-based mobile networks. Instead, IEEE 802.11 WLAN technology allows only one single connection at a time. In a conventional WLAN environment a client will typically connect to a new access point when the connection to the current AP is lost.

<sup>2</sup> EAP, Extensible Authentication Protocol, a universal authentication framework, frequently used in wireless networks

Starting to scan for available access points at that time, to choose one and to connect is a matter of delay of several seconds.

The introduction of a Mobility Broker (MB) allows distribution of information of nearby candidate access points for the next handover as well as selected information in order to speed up the MIP registration process. In combination with the inclusion of the MB in the re-authentication process, which avoids the otherwise required full authentication via the AAA<sup>3</sup> server of the ISP, reliable handover times for connectivity on the Network Layer (Layer 3) below 100 ms have been achieved.

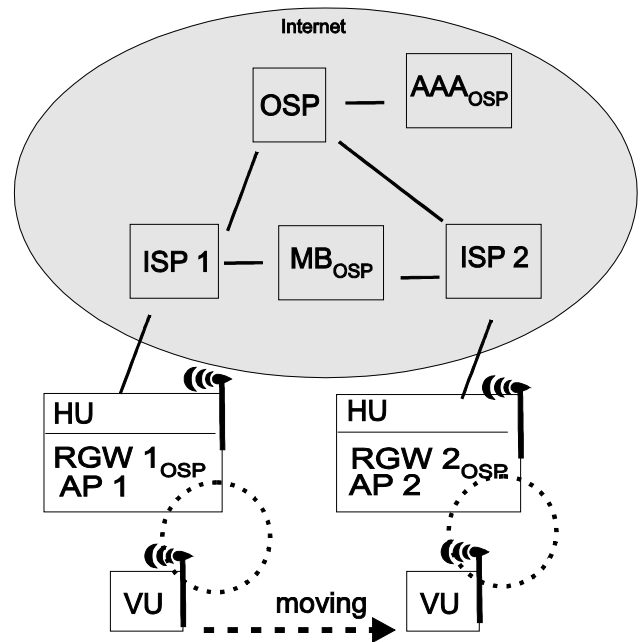


Figure 1. Example of an OBAN network and its major components

Figure 1 shows a simple OBAN network configuration and gives an overview about initial authentication and fast re-authentication developed. In our simplified scenario, home users (HU) are authenticated against their service provider. Visiting users (VU), which join the OBAN service, authenticate against the OBAN service provider (OSP). In order to demonstrate that the mobility broker (MB) may be placed anywhere in the network, preferable nearby the Residential Gateways (RGWs) the MB provides service for. ISP 1 and ISP 2 are competitors providing the Internet access for residents, typically via DSL technology.

There are many other possibilities to setup OBAN networks and how access and service provisioning may be provided. Especially the close integration of the ISP as envisioned within the OBAN project should be considered to allow better integration with other networks, especially 2G/3G architectures. Regarding secure authentication the model has to be extended in such scenarios, e.g. additional trust relations between the providers have to be set up.

<sup>3</sup> AAA; Authentication, Authorization, Accounting – a network service for access control, policy enforcement and billing

Nevertheless the developed method itself can be used also in such scenarios without major changes.

#### A. Scanning for OBAN access points and Layer 2 setup

When connecting to the OBAN network for the first time, the client has no knowledge which access points from those detected on the wireless scan are OBAN-enabled. It will attempt to establish a connection with each of them using EAP-FAMOS authentication method until it succeeds<sup>4</sup>. The number of access points to try can be reduced by verifying the encryption mode used by the access point (advertised in the scan data) or possibly by defining a common SSID used by all OBAN-enabled APs. For the further (fast) handovers, the client will use the MB to check in advance that an AP supports OBAN.

After the Client associates with an access point using EAP authentication method, a limited and unencrypted Layer 2 connectivity is established, which only serves the purpose of authentication. Only EAPoL<sup>5</sup> packets from the Client will be allowed to pass through and passed to a RADIUS server integrated into Residential Gateway. Once the authentication is successful, both Client and Access Point will be in possession of the identical keying material which is then used to establish encryption keys for the wireless link.

#### B. Layer 3 connectivity setup in Mobile IP

An ordinary use of MIP for Layer 3 connectivity includes the following steps:

- The client listens on a specific multicast address for the advertisement message of the Foreign Agent (FA), typically sent out every second.
- Upon receiving the advertisement message, the Mobile Node (MN) obtains the information necessary to setup client-side routing, and to send out the MIP registration message, such as IP and MAC addresses of the lower interface (facing the access point) of the RGW, and the Care-of-Address (used in the MIP registration to specify to what address should the Home Agent (HA) send the packets destined for the client).
- MN sends registration request to his HA, providing its Home Address, the Care-of-Address and the necessary MIP authentication information.
- After receiving and checking the request, the HA modifies routing for the client's packets and thus restores the Layer 3 connectivity.

Because setup of the Layer 3 connectivity has to be done not only when establishing the first connection, but also anytime when switching to another AP - which is part of a different IP subnet - it is obvious that the procedure above is by far too slow in order to support mobility as envisioned here.

<sup>4</sup> Faked OBAN APs are detected because of not supporting the EAP-FAMOS authentication method

<sup>5</sup> EAPoL, acronym for EAP over LAN

#### C. Integration of Mobile IP registration into EAP-FAMOS

In order to speed up the Mobile IP registration process, we included the according protocol exchange into the EAP-FAMOS fast re-authentication. The RADIUS server configuration contains information about FA, including aforementioned addresses. This allows sending the MIP advertisement information (in an adopted format) as part of the EAP exchange. Instead of waiting for the advertisement from the FA which may take up to 1 second, the Client now sends the MIP registration immediately after successful authentication.

A further optimization could be considered (not yet implemented): The authenticated client may even prepare a MIP registration packet in advance and forward it to the RGW, which in turn sends this packet to the HA. This would allow the MIP registration to be done in parallel to the key exchange phase which immediately follows the authentication. In case of WPA, this phase requires around 25 ms to finish. Using this time for sending the registration packet to the HA instead of waiting for the Client to obtain full Layer 2 connectivity is a direct time saving for the handover process.

While implementing and testing the architecture on a Linux platform, we encountered two artificial limitations in the Linux kernel that effectively made fast handovers impossible, but would be barely noticeable by conventional use of wireless and/or Mobile IP. In one case, the link state was allowed to change once per second only, presumably in order to fend off faulty network drivers. During the handover, the Layer 2 wireless connection would not permit sending until 1 second after the association, disrupting the authentication process. In another case, routing table update was artificially delayed by 2 seconds, in order to allow any outstanding packets to be flushed before routing reconfiguration. This has prevented HA from redirecting the traffic towards client to the correct FA, even though registration itself was performed quickly.

#### D. EAP-FAMOS initial authentication

The authentication process is initialized by the access point after successful association by sending a EAP-Request/Identity message. Client answers with EAP-Response/Identity containing the user name and the authentication realm. The RADIUS server performing authentication would usually select the authentication method and locate the user's credentials, but since EAP-FAMOS uses tickets for authentication, a generic user name is used. These packets as well as eventual EAP-Success are common messages for all EAP methods.

After Response/Identity, the RGW continues with EAP-FAMOS-specific authentication by sending EAP-Request/FAMOS/Challenge to the Supplicant. RGW always expects the client to possess a ticket for the fast re-authentication and expects it to respond to the challenge with a Ticket.

In the initial phase, client does not possess a ticket, and sends a NoTicket message in order to signal the RGW that

initial authentication against provider is needed. In the following steps, the client communicates with the provider in order to initialize the authentication system and to obtain the first ticket.

EAP-SIM is used for this initial task; its packets are tunneled within EAP-FAMOS/Encapsulated messages, encapsulation and decapsulation occurs on client and on MB, while RGW transparently forwards the messages. A provider will only receive packets of the encapsulated method. This authentication architecture therefore only requires OBAN-related modifications on the Client, RGW and MB components, full user authentication can be performed against existing authentication facilities, e.g. SS7<sup>6</sup> network of a mobile phone provider for EAP-SIM authentication.

Once the encapsulated authentication process is successful, keying material is generated on both provider and client components. Unlike conventional EAP authentication, where the keying material is sent to the access point and used to generate encryption keys, here it is intercepted on the Mobility Broker component. The keying material is used as Kerberos User Key in order to generate TGT and one initial Ticket, which are then transferred to the user as a final result to its NoTicket message.

After this procedure, both Client and RGW will arrive at the state where they have sufficient information in order to perform the initial authentication using Kerberos Tickets, i.e. the final stage of the initial authentication is identical to the fast re-authentication process.

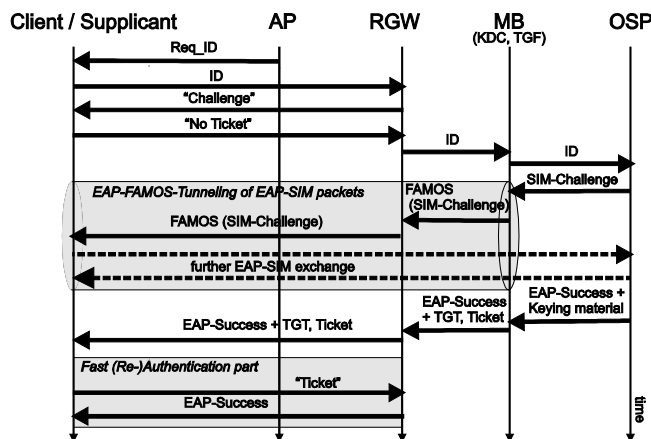


Figure 2. EAP-FAMOS Authentication

Regarding the further Kerberos-like authentication procedure, the MB acts as Key Distribution Center (KDC) and provides a ticket generating function (TGF). Usually the client would contact the Kerberos authentication service to get a TGT and in turn ask for a ticket. Because of the trusted relation already established between MB and the supplicant (i.e. keying material generated by EAP-SIM) this step is omitted. The MB therefore immediately generates the TGT

<sup>6</sup> SS7, Signaling System #7, a set of telephony signaling protocols

(based on the keying material) as well as a first ticket. The MAC address of the AP (besides TGT required for the ticket generation) is already known by the MB (extracted from previous RADIUS packets during initial EAP-SIM authentication). Therefore, the MB completes its role in the initial authentication process by sending out an EAP-Success message with TGT and Ticket attached as additional attributes. For the RGW, it's a signal to continue the authentication process (i.e. it no longer acts as a proxy); the EAP-Success message from the MB is transformed into EAP-FAMOS/TGT packet that delivers the tickets to the Client. This message basically serves as a conclusion to the Client's EAP-FAMOS/NoTicket packet that triggered the initial authentication process.

#### E. EAP-FAMOS fast re-authentication

The fast re-authentication principle of EAP-FAMOS can be considered a variation of pre-authentication methods – the Client makes preparations for the fast handover while still having full connectivity to the network. However, in our case the target access point does not have to be informed of the upcoming handover. This gives the Client the perfect flexibility for its handover decision - the target access point can be selected literally microseconds before handover.

While using the IP connectivity established the client will scan for additional APs. This can be done in specific time intervals or based on other parameters (e.g. SNR value of the current connection). Scanning delivers the MAC addresses of actually reachable APs. In order to check which of the APs are supporting OBAN the list of MAC addresses together with the TGT are sent to the MB. The TGF on the MB checks correctness of the TGT and afterwards it checks each of the MAC addresses against its database of served APs/RGWs. For all MAC addresses, which represent APs supporting OBAN, a ticket will be generated and the resulting list sent to the client. If the client decides to switch to one of those OBAN APs, the ticket is used for authentication. Because of the trusted relation established between MB and RGW, the RGW can verify the clients' identity on its own and complete the authentication locally, without communicating with other entities.

Our architecture provides a replay protection mechanism similar to that used in Kerberos. Whenever a ticket is presented for authentication, the Client must also provide an authenticator. The authenticator contains authentic information, for example fresh timestamp, counters or a nonce provided by the authenticating party encrypted with the respective ticket's inner key. The authenticator is therefore a proof that the entity is indeed in possession of a key and is able to read the ticket and therefore prohibits that someone else may replay a captured ticket for authentication.

#### IV. MEASURED PERFORMANCE RESULTS

To figure out the performance achievable with the EAP-FAMOS design a pilot implementation was used for testing and measurements. The pilot implementation consists of the following hardware components:

- BookSize PC NE252-9670 VIA 1Ghz, used for all servers and equipped with multiple 1 Gigabit Ethernet interfaces
- Cisco 1200 series access points with 802.11b/g and a capabilities
- Notebook with Pentium M 1.4 GHz processor as client

Implementation is based on following software components and modules:

- Linux kernels used for client, RGW and MB
- FreeRADIUS
- Dynamics Mobile IP, open-source implementation of MN, FA, HA, tested against HW-based implementations (Cisco)
- MadWifi driver for Atheros chipset based wireless cards, supporting arbitrary scan channel selection
- wpa\_supplicant

First measurements delivered following execution times for different phases:

TABLE I. EXAMPLE OF MEASURED RESULTS FOR INITIAL AUTHENTICATION

Event triggered	Duration (ms)	Sum (ms)
IEEE 802.11 Authentication + Association	0.0	
EAP Request Identity + Response	3.3	3.3
EAP Success	440.6	443.9
EAPOL Key (unicast + group)	10.9	454.8
ICMP Router Solicitation	7.0	461.8
MIP Registration Request (to HA)	0.2	462.0
MIP Registration Reply (from HA)	50.4	512.4
First UDP Ping (new AP)	1.8	514.2

TABLE II. EXAMPLE OF MEASURED RESULTS FOR FAST-HANDOVER AND RE-AUTHENTICATION

Event triggered	Duration (ms)	Sum (ms)
Last UDP ping (old AP)	0.0	
IEEE 802.11 Authentication + Association	14.8	14.8
EAP Request Identity + Response	3.3	18.1
EAP Success	13.7	31.8
EAPOL Key (unicast + group)	9.1	40.9
ICMP Router Solicitation	12.8	53.7
MIP Registration Request (to HA)	0.3	54.0
MIP Registration Reply (from HA)	15.3	69.3
First UDP Ping (new AP)	1.4	70.7

As expected, the initial Registration (EAP as well as Mobile IP) consume more time compared to the duration used during fast-handover due to multiple round-trips to the

provider entity and access to the SIM card. Nevertheless, initial registration is still quite fast compared to non-optimized drivers and operating system kernels.

Regarding the measurements we executed the above values seem to be characteristic; deviation is in the range below  $\pm 20$  ms. Regarding performance achieved it has to be considered that the work hasn't been finalized yet. The implementation will be improved by some additional optimizations, but further improvement is expected to be in the range of 10 to 20 ms only.

Our measurements showed that service interruption, documented by the time gap between last UDP packet received from the old AP and the first one received from the new AP, was below 100 ms. Therefore it is expected that services like Voice over IP can be used without noticeable interruptions while changing APs.

Judging the performance achieved it has to be considered that the duration values also depend on the performance of the systems used. During testing the CPU of the notebook used was running with 1.4 GHz. In order to save power, CPU frequency of the notebook can be reduced to 600 MHz, but a short test has shown that the handover performance was generally worse when power-saving mode is active or the CPU was running on lower frequency.

## V. CONCLUSIONS AND OUTLOOK

The performance values measured clearly show that WLAN technology can be used in mobile scenarios where moving wireless communication objects are limited to speeds below 15 kmh. Even applications requiring very low delay and allowing only very short service interruptions can be supported. But until today, the performance required cannot be achieved with software components available from the shelf. Especially implementations of WLAN drivers and their integration into the operating systems seem to have been worked out without WLAN mobility in mind.

Based on the achieved results the rollout of WLAN-based Open Access Networks, offering most of the services available today, seems to be reasonable. Such a rollout may include various network operators, supporting not only service continuation between WLANs but also between WLAN and 2G/3G and WiMAX networks. In order to setup such a network additional research has to be done, especially in order to cover extended requirements regarding security, billing and service provisioning. The deliverables and reports of the OBAN project mentioned are available on the public OBAN web server [5], and they can be considered as a solid basis for further evaluation.

## REFERENCES

- [1] Wireless Services at Boingo, 02 April 2008, [online] – URL: <http://www.boingo.com>
- [2] The Cloud: Wireless Broadband Network, 02 April 2008, [online] – URL: <http://www.thecloud.net/About-us/>
- [3] FON: Wi-Fi-everywhere!, 02 April 2008, [online] – URL: <http://www.fon.com/>

- [4] European Parliament – The legislative Observatory. Electronic communications: personal data protection rules and availability of traffic data for anti-terrorism purposes (amend. direct. 2002/58/EC) (The Data Retention Directive). Procedure File COD/2005/0182. 02 April 2008, [online], URL: <http://www.europarl.eu.int/oeil/file.jsp?id=5275032>
- [5] OBAN. 02 April 2008, [online] – URL: <http://www.ist-oban.org>
- [6] Frans Panken, Haakon Bryhni, Paal E. Engelstaad, Leif Hansson, Gerard Hoekstra, Martin G. Jaatun, Tor H. Johannessen, “Architecture for Sharing Residential Access with Roaming WLAN Users”, *Teletronikk* Volume 102 No. 3.4-2006 ISSN 0085-7130, pp. 48-59.
- [7] ITU. General Characteristics of International Telephone Connections and International Telephone circuits. International Telecommunication Union, 1998. (ITU-TG.114)