New standards on mobile communications

Gonzalo Solas[1], Paul Bustamante[1,2], Juan Meléndez[1,2], Pablo Cabezas[1]

Dpto. Electrónica y Comunicaciones
[1]CEIT y [2]TECNUN (Universidad de Navarra).
Manuel Lardizábal 15, 20018 – San Sebastián
Teléfono: 943 219 877 Fax: 943 311 442
E-mail: {gsolas, pbustamante, jmelendez, pcabezas}@ceit.es

Abstract. The new generation of mobile communications, characterized by the ubiquity of the services and the heterogeneity of the technologies, has new needs: it shows the deficiencies of the present standards in several aspects and arise others that cover the new requirements. In this work, on the one hand, the deficiencies in security aspects of the current standards, and on the other hand, two new works that are being carried out at the moment are going to be shown. One of them is the UMA (Unlicensed Mobile Access) standard, which has begun to be implemented, and another one, the IEEE 802.21 or Media Independent Handover (MIH), which is still under development. Although a general analysis is going to be carried out, covering all the aspects, the emphasis is going to be focused in security aspects (authentication and authorization, access control, users' identity and content of the data protection, etc.).

1. Introducción

The horizontal handover is the process by which a communication session is transferred between two different networks that use same technologies. Vertical handover however, tries to make the same but between networks that use different technologies. This it is going to be the future of the mobile communications, due to the great number of wireless networks that are going to coexist in a next future, and the diverse nature of them. There will be cellular networks of several types (GSM, GPRS, UMTS) as well as 802 family wireless networks, i.e. Wi-Fi or WiMAX.

This article arises from a previous study and later analysis that has been made within the framework of the SUMO project (**S**ervice **U**biquity in **MO**bile and Wireless Realm) [1], a European project that is being carried out within the ITEA program. Among the participants telephony operators (Telenor, Norway; Euskaltel, Spain), telcos (Alcatel, France), universities (University of Paris, France) and research centers (UNIK, Norway; INT, France) can be found. The main characteristic of this project is that, while the standardizing efforts are being made towards the data link and network layers, SUMO puts a special emphasis in the services that are going to be offered with the new technology and the platform for the delivery of these services.

2. Deficiencies of the current standards in security aspects

For the analysis of the security of the current technologies, those which take part in any type of mobile communication have been selected. More concretely the cellular technologies (GSM/GPRS and UMTS), Wi-Fi and WiMAX have been selected. As most representative Near Field Communication (NFC) technology, Bluetooth has benn chosen. Although the number of new technologies in the world of the mobile communications has increased greatly in recent times, only the most interesting have been selected, those which are going to end up being the most relevant ones in a near future.

The security of the communications includes several aspects, among which, the most outstanding are:

- **Autentication:** with this mechanism can be determined if a user is really who claims to be.
- **Authorization:** with this mechanism, the acces to certain system resources can be limited, depending on the privileges of the user.
- **Access control:** thanks to the access control it can be determined whether a user has or not enough privileges to accede to a certain physical resource, i.e. a zone of radio coverage or an equipment of the network.
- **Encryption:** it referes to any technique which allows to codify the information so that it is unintelligible for anyone who hasn't got the decryption key.
- **Key management:** in a big and complex system an elevated number of keys have to be handled and the management of these turns out crucial to avoid security flaws.

In this analysis the deficiencies that the current standards present are wanted to be emphasized, facing the future generation of mobile communications. This will be characterized mainly by the unified access to the mobile services, what is to say, the capacity to use any radio network, no matter its nature, to access any service through a unique personal mobile terminal (since in a next future the number of available wireless networks is going to be very high, and their nature very diverse). The most important requirement to arrive at this point is the system being capable of making vertical handovers, the switch between different access technologies, seamlessly for the user, without loss of quality of service and guaranteeing the continuity of the sessions.

Whenever a new technology is devised, new security requirements arise, which are going to be analyzed in this point:

- **Access control:** the current mechanisms must be reviewed since they do not offer a non subscription based access control, something fundamental for the new generation.
- **Dynamic agreements:** in every handover process there are two entities involved, and with the proliferation of wireless networks it can be very probable those two organizations not having any previous agreement. Thus, the establishment of a mechanism which guarantees the security of dynamically generated agreements becomes very necessary,
- **Unified addressing/Universal identifiers:** one of the objectives is to have access to any type of network through an only device. Therefore, this device is

going to have to identify itself in any type of network and have a valid identifier no matter the technology.

- **New key management and exchange mechanisms:** nowadays each access technology works separately and has its own key management mechanisms. But when working with several technologies which use different algorithms and keys, new mechanisms for the management of all the keys are necessary.
- **User/device authentication:** there are technologies that only carry out a device authentication, whereas others also authenticate the user. The new authentication mechanisms must be independent of the underlying technology and to provide a unified algorithm.
- **The new mechanisms must be resistant to already known threats:** as mentioned already, a new mechanism, i.e. the vertical handover, presents new security threats, but it is essential the new technology to be resistant to already known threats, in addition to the new ones that arise.

3. Unlicensed Mobile Access (UMA)

UMA (nowadays known as Generic Access Network o GAN) allows the access to GSM and GPRS mobile services through unlicensed wireless technologies, i.e. Bluetooth or 802.11. It allows the users to switch in a seamless way between private WLAN networks, GSM networks, traditional LAN networks and PSTN networks using an only mobile telephone equipped with multiple interfaces. The final goal is the convergence of the fixed telephony, mobile telephony and telephony through the Internet.

3.1. General characteristics

The Basic characteristics of this new Standard are the following [2]:

- Seamless delivery of mobile voice and data services over unlicensed wireless networks.
- Provides the same mobile identity on Cellular RAN and unlicensed wireless networks.
- Seamless transitions (roaming and handover) between Cellular RAN and unlicensed wireless networks.
- Independent of underlying unlicensed spectrum technology (e.g. WiFi, Bluetooth).
- Transparent to existing, standard CPE devices (e.g. access points, routers and modems).
- Utilizes standard “always on" broadband IP access networks (e.g. DSL, Cable, FTTH…).
- Security equivalent to current GSM mobile networks.
- No impact to operations of Cellular RAN (e.g. spectrum engineering, cell planning,…).

The architecture, as it is defined in the ETSI TS 143 318 V6.3.0 standard (or also 3GPP TS 43.318 version 6.3.0 Release 6) [3], appears in the following figure:

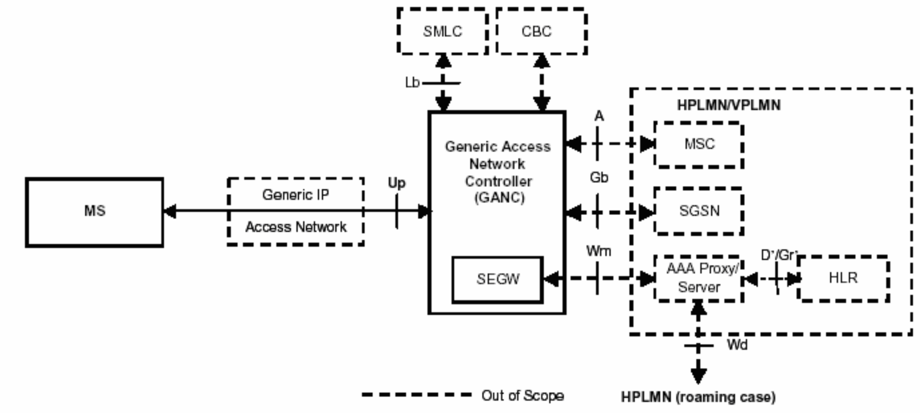

Fig. 1. UMA architecture.

The key of the UMA operation is that the broadband wireless Internet connections can be used to accede to mobile telephony services. After configuring the parameters of the WLAN connection, the mobile device equipped with UMA technology can be connected to Internet through a WLAN network and, using IP, be connected to which is called the UMA Network Controller (UNC) or Generic Access Network Controller (GANC). This one will be the one in charge of redirecting the call towards the public network.

3.2. Aspectos de seguridad

The security mechanisms supported by UMA appear in the following figure (Source: ETSI TS 143 318 [3]):

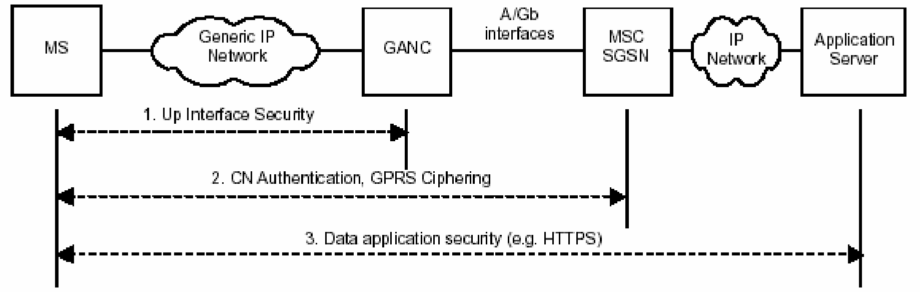

Fig. 2. UMA security mechanisms.

The first group of mechanisms protects the communications between the mobile terminal and controller GANC (signalling, voice and data). They support mechanisms such as the authentication (it is carried out using EAP-SIM or EAP-AKA and GSM or UMTS credentials), the encryption and the integrity of the information. As a result of the initial authentication process in this interface, a IPSec tunnel is stablished, through which all the information of the control and user plane is sent.

The second group of mechanisms carries out the user authentication towards the u the core network, and it is made between the mobile station (MS) and the SGSN. In this case, the GPRS coding is used to carry out this operation.

The third group defines mechanisms that can be used in the packet switching domain in order to provide end-to-end communications. An example of this mechanism can be the execution of HTML over a SSL session for a safe Web access.

Refering to the encryption, the algorithm to be used is determined during the establishment of the SA (Secure Association) between the mobile terminal and GANC. The first one is the one that indicates which are the available algorithms and which of them is the mandatory one, although the decision of which algorithm to use is taken by the GANC.[1]

3.3. Actual applications and implementations

The first implementation that has appeared in the market has been a Nokia mobile telephone, more concretely the 6136 model [4]. According to the manufacturer, UMA technology offers a good cover and quality of service in the calls through wireless networks. In addition, it allows smooth transitions between networks GSM and WLAN, which constitutes a step towards the future generation of mobile telephony.

4. IEEE 802.21 - Media Independent Handover (MIH)

The cellular and 802.11 networks use handover mechanisms for the session or call transfer within a same network, and Mobile IP (MIP) does the same but with different networks of the same type. Nevertheless, no 802 standard supports handover processes between different types from networks.

The primary target of this standard, as mentioned in a preliminary version of the specification [5], is "to provide a link layer intelligence and other related information to the upper layers, with the purpose of optimizing the handover between different networks", like for example third generation telephony networks and WLAN networks.

4.1. General characteristics

How the different factors that may affect handovers are addressed within the IEEE 802.21 proposal:

[1] There is also the possibility of not using any type of algorithm.

- **Service continuity:** a handover process between two different access technologies implies two requirements: the user can or not be conscious of this change, but in no case it must require a reestablishment of the service. Besides, a change in the quality of service can occur, depending on the capacity of the networks origin and destiny of the handover process.
- **Application class:** various applications have different tolerance characteristic for delay and data loss. Application aware handover decisions can be enabled by making a provision for such characteristics.
- **Quality of service:** it is a very important characteristic and 802.21 standard specifies the means by which the information about the QoS of each supported access network can be obtained.
- **Network discovery:** it is an important factor to offer several possibilities at the moment of the network selection. The 802.21 standard defines which is the most important information of the available networks and the form in which this can be obtained and offered to the upper layers.
- **Network selection:** the network selection, according to MIH standard, can be based on several different criteria, i.e. the QoS, the cost, user preferences, determined selection policies, etc.

4.2. Architecture

The standard defines a set of handover-enabling functions within the mobility-management protocol stacks of the network elements and the creation therein of a new entity called the MIH Function. The location of this new entity in the general network architecture can be seen in the following figure:

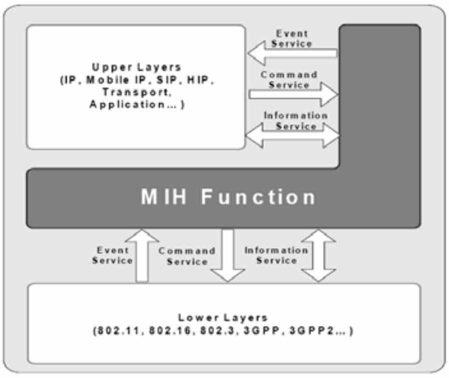

Fig. 3. Location of the MIH Function entity.

This new entity offers three new types of services which enhance the handover between heterogeneous access networks:

- **Media Independent Event services:** which provides a set of events and triggers from local as well as remote interfaces.

- **Media independent Command services:** p provides set of commands that enables MIH users to issue commands to control link behavior relevant to handovers.
- **Media Independent Information services:** provides information model and an information repository to make more effective handover decisions. The moble terminal accesses information from this repository using it's current network point of attachments.

4.3. Security aspects

Events, commands and information messages carried between a MT (Mobile Terminal) and a network PoA (Point of Attachment) cannot be secured until the MT is securely associated with the network PoA. This association can be achieved either via lower or higher layers security mechanisms. Once such a secure association has been established between the MT and the network PoA, any messages exchanged between two MIH Function entities should retain integrity and be replay protected over a secure transport. Otherwise the exchanged MIH messages are prone to integrity, replay and man-in-the-middle attacks.

The 802.21 standard may specify the means for security information to be made available to the upper layers to setup secure connections.

5. Conclusions

There are two main differences between the two exposed technologies. On the one hand, the development level, as UMA has a complete and finalized specification, whereas MIH is still in phase of development.

On the other hand, MIH is more generalist, since its aim is to create an interface between the link or network layers and the upper layers, the application ones. UMA's objective is not to create a platform to support any kind of wireless technologies, but to allow the access to the mobile telephony services through unlicensed spectrum radio technologies.

References

[1] SUMO Project homepage: http://www-inf.int-evry.fr/~belaid/cgi-bin/twiki/view/Sumo/WebHome

[2] UMA homepage: http://www.umatechnology.org/

[3] ETSI TS 143 318 V6.3.0; "Digital cellular telecommunications system (Phase 2+); Generic access to the A/Gb interface; Stage 2"

[4] http://www.nokia.es/telefonos/nokia6136/index.jsp

[5] http://www.ieee802.org/21/doctree/2005-05_meeting_docs/21-05-0271-00-0000-One_Proposal_Draft_Text.doc