3GPP TSG SA WG3 Security — S3#23 S3-020337
9 - 12 July 2002
Helsinki, Finland

BROADBAND RADIO ACCESS NETWORKS

The Multimedia Mobile Access Communication Systems Promotion Council MMAC

Chairman of ETSI Project Broadband Radio Access Networks
Jamshid Khun-Jush, Dr.-Ing.
Ericsson Eurolab Deutschland GmbH
Ericsson Research, Corporate Unit
Neumeyerstr. 50
D-90411 Nürnberg
Germany
Tel: +49 911 2551260 / Fax +49 911 2551961
Email: jamshid.khun-jush@eed.ericsson.se

Chairman of High Speed Wireless Access Committee of MMAC-PC
Masahiro Umehira, Dr.
Wireless Systems Innovation Laboratory
NTT Network Innovation Laboratories
Yokosuka
Japan
Tel: +81-468-59-3547 FAX: +81-468-55-1497
Email: umehira@wslab.ntt.co.jp

To: Michael Walker Chairman 3GPP SA3
~~Cc:~~

Date: 09~~3~~ May 2002

Dear Michael,

ETSI Project (EP) BRAN and the MMAC HSWA committee would like to take this opportunity to present you with some more information about our ongoing work on *WLAN – 3G and other Public Access networks interworking (standard on interworking).* It is the intention of this liaison letter to inform you of the work we are currently working on with respect to security and authentication and encourage discussion on those areas within which we believe we can co-operate together.

Introduction

Since we have communicated with you previously, our two groups have progressed further along the path of creating a harmonised standard on interworking.

It is the intention of our groups to achieve the re-use of authentication procedures, accounting, mobility, QoS and other such fundamental functionalities between the two WLAN systems. Furthermore, it is our understanding that this will additionally assist 3GPP SA, by helping them in their ongoing work on 3G-WLAN interworking by the provision of a common interface.

Definition of “W” Interfaces

To aid discussion within the rest of this document, it is necessary to define the following interfaces~~-~~:

- “W.1” is the air interface defined by ETSI BRAN TSs (TS 101 475, TS 101 761, TS 101 763, TS 101 493, TS 101 762).
- “W.2” is the interface that represents the innermost interface within the scope of this standardisation activity. This interface is mainly devoted to allow the interworking with public network, carrying the appropriate signalling information in the most suitable manner for WLAN systems and public networks. The W.2 interface should be defined in order to reduce as much as possible on existing requirements for both WLAN system and 3GPP systems. The defining of this interface requires co-operation between the system to the right and to the left of the W.2 in addition to co-operation with the standardisation body maintaining the protocols to be used.
- “W.3” is the interface that represents the external interface between the interworking functions and the external public networks (both fixed and 3G) and is out of scope of this standardisation activity.

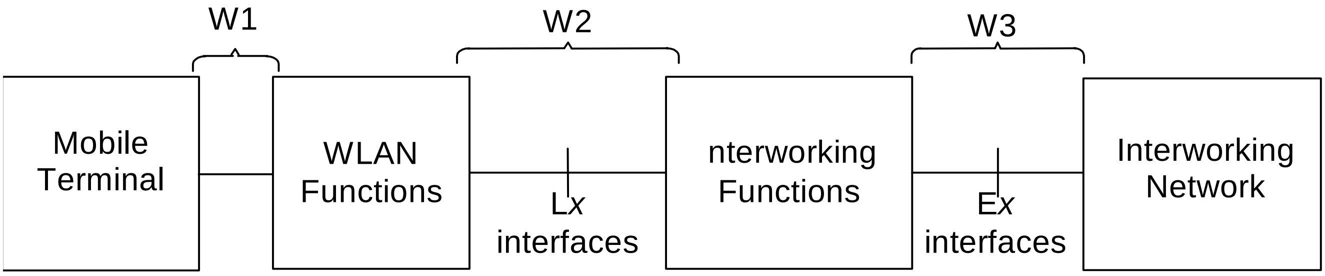

Figure 1: Outline of reference architecture.

Areas of co-operation

After careful consideration we have identified several principle areas for co-operation:

- Agreement of scope between our organisations along a common interface W.2. An example of the usage of W.2 is the Ls interface would be used for the exchange of authentication messages between the WLAN network and interworked networks Local authentication function. The co-operation among ETSI BRAN and 3GPP SA3 should deal with agreement on functionalities, which should be supported, on suitable protocol stack, etc
- Unified positioning towards other relevant bodies e.g. IETF.
- Ensuring that the requirements (such as those for authentication and security) of both our organisations are compatible.

Scope and Purpose of ETSI BRAN and MMAC HSWA standardisation

The scope of the present draft technical standard (DTS) is to provide the first release of the work towards the provisioning of a HIPERLAN/2 and HiSWANa interworking standard that is generically applicable to different 3G networks and other types of public access networks.

This first release (R1) is concerned with the establishment of functionality to provide a secure authentication scheme through the network to be interworked. Also R1 is concerned with the establishment of some basic functionality to allow for the provision of accounting and charging support. It further establishes an architectural baseline for the interworking concept and currently we do not have a specific deadline for this release.

The next stage (R2) is to provide the support for functionality such as service integration, mobility and QoS interworking support.

Reference Architecture

The goal of the reference architecture is to focus on the functionality required in the Access Point Control (APC) Part and to specify the interface between the APC functions and the control functions within the interworking network.

The following section provides an overview of the proposed reference architecture. It identifies the functions required within the network and the interfaces between them for R1.

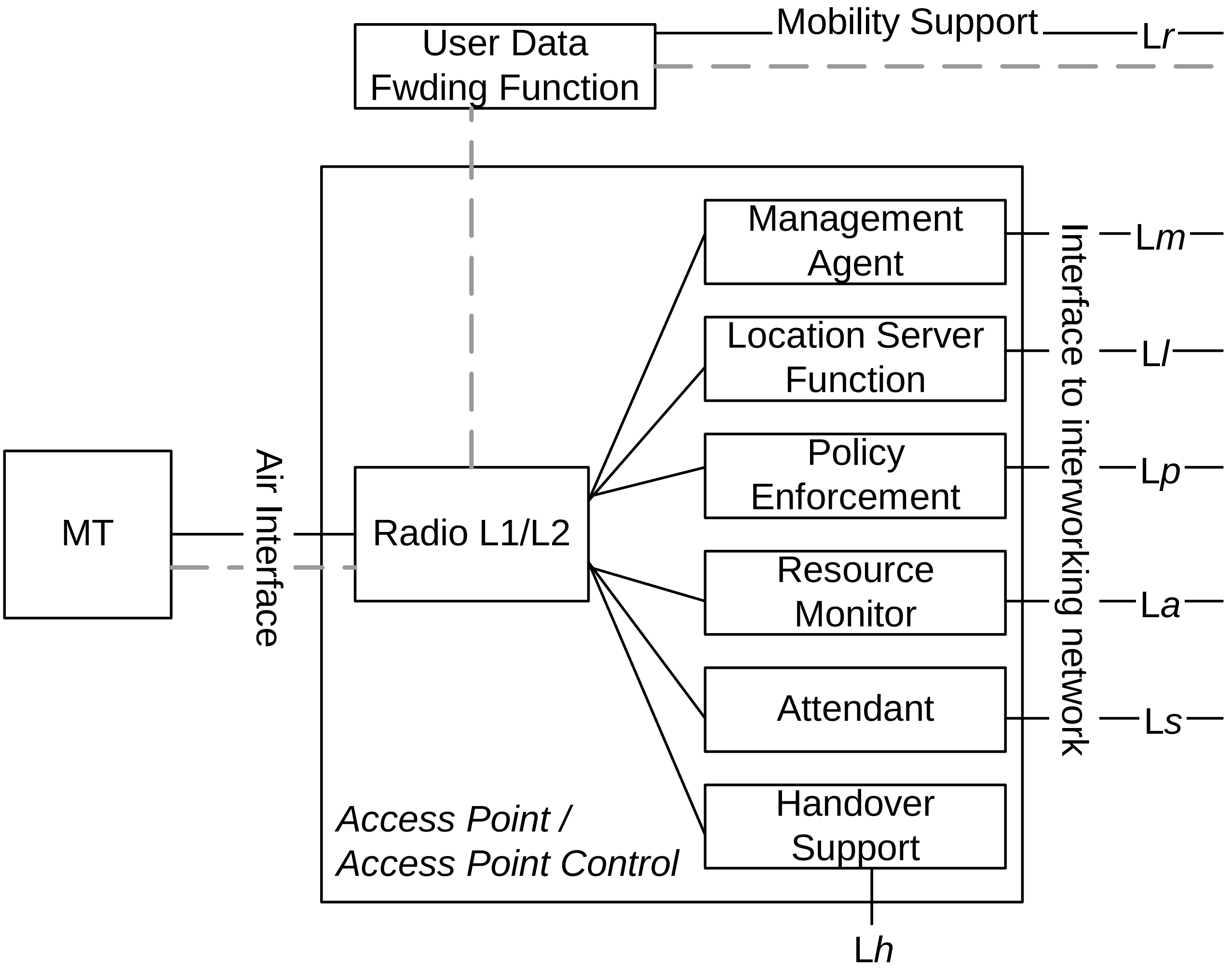

Figure 2: Reference Architecture.

The AP may be a single network node or it may be distributed function of many network nodes, and the reference architecture does not define any particular AP/APC implementation.

The reference architecture is shown in Figure 2. The terminology used in naming the different functions tries to follow IETF conventions where possible but does mandate the use of any particular transport infrastructure within the interworking network.

The interfaces are labeled as follows:

~~□~~L interfaces pass across the W.2 interface. These are the interfaces that are proposed for standardisation within the current scope of the reference architecture, excluding the L*r* interface due to its dependence on the transport infrastructure of the interworking network. The L interfaces are required to run over a transport infrastructure that may vary depending on the scenario.

- E interfaces pass across the W.3 interface. These interfaces are not proposed for standardisation within our organisations these would be the responsibility of the interworking network.

Within these categories of interfaces, the letters following the first letter indicate the type of function(s) the interface is used by.

The convention is as follows:

- *a* interfaces are used by accounting functions
- *p* interfaces are used by user policy control functions
- *n* interfaces are used by network policy control functions
- *s* interfaces are used by authentication mechanisms
- *h* interfaces may be used by handover functions between heterogeneous networks

Although many of the interfaces identified within the reference architecture will not be specified, it is useful to identify these interfaces in order to determine what information needs to be exchanged across the standardised interfaces.

It is necessary to have a common architecture for all WLAN systems and we feel that the above model presented in Figure 2 is a good working assumption.

Requirements

We would like to inform you that we have defined a set of system level requirements (ETSI TR 101 957 Ver. 1.1.1), specific to interworking and we invite you to review these, hopefully with the intention that they may also be applicable to future 3GPP SA3 needs. We would appreciate your feedback on these as to their applicability to 3GPP SA3.
We are currently in the process of mapping these requirements to the W.2 interface.

Authentication

Authentication provides a way to identify a user that wishes to access the HIPERLAN/2 or HiSWANa network and to authenticate the network with the user. The mechanism for authentication is typically undertaken through the exchange of logical keys or certificates between the MT and the AP. The AP may then forward this exchange towards the interworking network for the purposes of centralised user administration. Authentication is supported by the Local Authenticator and the Attendant in the AP, and by the Authenticator in the MT.

Please note that all references to HIPERLAN/2 are equally applicable to the HiSWANa system, within this section.

It is our opinion that the mechanisms for remote authentication concerning the inter-working between the WLAN and interworking network, is an area that would need to be common amongst WLAN systems in order to achieve the aim of a single common view towards the 3GPP system and hence this is an area upon which we must within the WLAN community cooperate in the interests of this attainment of this goal. The view taken by 3GPP SA2 on these matters would be most appreciated.
To aid understanding of our current work we now describe some of our current working assumptions.

Authentication within HIPERLAN/2 can in principle proceed on two different “layers”. At the lower layer, there is authentication performed by the RLC entity of HIPERLAN/2. Or at the higher layer, applications or services using a particular Convergence Layer may perform their own (Convergence Layer specific) authentication. We refer to the lower layer authentication as “network authentication”, and the higher layer authentication as “service authentication”.

Previous consideration has concluded that these two forms of authentication are separate and cannot reasonably be combined into a single authentication procedure. Further, “service authentication” can be understood as operating over the HIPERLAN/2 user plane, whereas “network authentication” operates over the HIPERLAN/2 control plane.

Under this view, “network authentication” may be regarded as granting access to the physical HIPERLAN/2 network, and “service authentication” as giving authority to use a particular (Convergence Layer specific) service provided over the network.

Network Authentication

The network authentication scheme is based on EAP (the Extensible Authentication Protocol)[1]. This scheme has been dubbed "EAPOH" - EAP over HIPERLAN/HiSWANa - by analogy with IEEE 802.1X EAPOL (EAP over LANs) ~~)~~— extending it in order to allow both username/password and SIM card based (i.e. (U)SIM) authentication.

We believe this allows for a common system whilst allowing for the carrying of a number of different forms of authentication depending upon the type of network being interworked with and the form of authentication messages it employs. For example this scheme directly supports IETF flavour authentication, and by use of the proposed EAP AKA (Authentication and Key Agreement) mechanism would also directly support the UMTS authentication.

We would be delighted to share more information with you on the network authentication scheme that is our current working assumption.

[1] As described by ~~Blunk and Vollbrecht;~~ Blunk L & ~~,~~ Vollbrecht J, 1998, “PPP Extensible Authentication Protocol”, RFC 2284

Service Authentication

HIPERLAN/2 Convergence Layers

Within the HIPERLAN/2 protocol stack, provision is made for one or more Convergence Layers to provide interfaces to the higher level applications. For example, Convergence Layers are proposed to support IP, Ethernet (IEEE 802.3) and FireWire (IEEE 1394) applications.

Applications using the different Convergence Layers typically have different requirements and capabilities with respect to AAA. Additionally, the AAA information is carried in the Convergence Layer native format. Thus, for example, a (mobile) IP application will exchange AAA information carried in IP packets with a router on the visited network; an Ethernet application will exchange AAA information (encapsulated) in Ethernet packets, perhaps using 802.1X EAPOL.

An important consideration is whether a Convergence Layer will “look inside” the packets it is to transfer to see whether the information contained is “ordinary” user data, or whether the information is “special” – for example, AAA data. If the Convergence Layer does not “look inside” packets, all packets must pass through the user plane of the HIPERLAN/2 protocol stack. On the other hand, if the Convergence Layer does “look inside” packets, the “special” packets could be routed via the control plane of the HIPERLAN/2 protocol stack (leaving the “ordinary” packets to be passed through the user plane).

Impact on RLC

If Convergence Layer specific “special” packets are filtered off and routed via the control plane, there is the additional consideration of how they can be handled. Here we focus only on packets carrying AAA information.

If the MT should already be associated with an AP, there is (currently) no defined mechanism for handling the information. In particular, there is no mechanism to require authentication during the set-up of DLC user connections.

If the MT should not yet be associated with an AP, perhaps the information could be used during the authentication phase of the association procedure. However, that procedure would then need to specify a mechanism for transferring arbitrary (e.g. Convergence Layer specific) AAA information.

Concluding Comments.

We would like to again express our potential areas of co-operation and encourage comments on these:

- Agreement of scope between our organisations along a common interface W.2. An example of the usage of W.2 is the Ls interface would be used for the exchange of authentication messages between the WLAN network and interworked networks Local authentication function.
- Unified positioning towards other relevant bodies e.g. IETF.
- Ensuring that the requirements (such as those for authentication and security) of both our organisations are compatible.

We look forward to your response.

Kind regards

Jamshid Khun-Jush & Masahiro Umehira