Integrated Mobility and Third-Party AAA Management for 4GWW[1]

IVAN GANCHEV, FINTAN McEVOY, MAIRTIN O'DROMA
Department of Electronic and Computer Engineering
University of Limerick
IRELAND

Abstract: - In the near future it is expected that IPv6 will lie at the backbone of all networks. Networks will consist of more mobile devices than wired terminals. Mobile users will demand to be always best connected and served (ABC&S). Such a dynamic system will require seamless mobility and flexible authentication, authorization and accounting (AAA) scheme. Various emerging protocols may play a part in this fourth generation wireless world (4GWW), e.g. Mobile IPv6 (MIPv6), hierarchical MIPv6 (HMIPv6), fast MIPv6 (FMIPv6) and the Diameter protocol. Used alone each of these protocols have their own strengths and weaknesses, however, a hybrid of all these protocols may emphasize their various strengths and eliminate their individual weaknesses. This paper proposes a new third-party AAA architectural framework, employing a hybrid signaling protocol and integrating mobility and AAA functions for 4GWW orientated to a more consumer based business model (CBM).

Key-Words: - ANWIRE, Always Best Connected and Served (ABC&S), Third-Party AAA (3P-AAA), 4G wireless world (4GWW), Mobile IP (MIP), Hierarchical Mobile IP (HMIP), Diameter.

1 Introduction

Wireless network business models used today place the User Home Access Network Provider (UHANP) at the center as both the effective manager of all the user's wireless communication activities and the supplier of part of these wireless communication services. These models are described as Subscriber-based Business Models (SBM) [1, 2]. They do not benefit the user who desires to be always best connected and served (ABC&S), always getting the best value for money and having access to unlimited services. The need to have administrative and management support in place, provide services and network access before being able to start seeking 'home user accounts' also constrains new UHANPs from entering the market. ANWIRE[2] (Academic Network for Wireless Internet Research in Europe) suggests the need for a new business model [1, 2]. This business model divides the tasks of providing network access, services, management and administration amongst multiple parties. It is a more Consumer-based Business Model (CBM).

At the heart of this new CBM model is the new third-party Authentication, Authorization and Accounting (3P-AAA) management system (Figure 1). The Mobile User has an agreement with the 3P-AAA service provider (SP), much like s/he would have with a credit card company. All billing information for the mobile user is filtered through the 3P-AAA provider. As can be seen in the model, all service providers (xSP, VASP) and access network providers (ANP) have a pre-arranged business agreement (B.A.) that 3P-AAA will handle all billing.

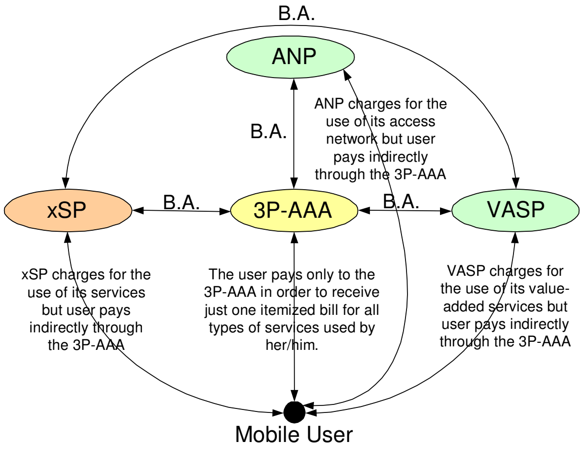
B.A.
ANP
B.A.
ANP charges for the use of its access network but user pays indirectly through the 3P-AAA
xSP
B.A.
3P-AAA
B.A.
VASP
xSP charges for the use of its services but user pays indirectly through the 3P-AAA
The user pays only to the 3P-AAA in order to receive just one itemized bill for all types of services used by her/him.
VASP charges for the use of its value-added services but user pays indirectly through the 3P-AAA
Mobile User

Fig.1 CBM with a 3P-AAA SP at the center

In existing mobile wireless networks, the security profile of users is handled within an AAA

[1] This publication has emanated from research conducted with the financial support of Science Foundation Ireland under the Basic Research Grant Ref. No. 04/BR/E0082.

[2] www.anwire.org

framework. The AAA server is located in the access network, and an AAA signaling protocol is used between the AAA server, the current access router and the mobile host.

In future 4G networks, the main issue will be to reuse this existing AAA framework in the heterogeneous communication environment by introducing a 3P-AAA management system as illustrated in the ANWIRE business model. This will allow easy and automatic AAA of users in a heterogeneous environment comprising different access network providers exploiting different access network technologies.

It is notable that the task of gaining access to networks and the task of user mobility are closely related. It would be beneficial to combine the tasks of mobility and AAA into one signaling protocol to support this new third-party AAA system.

2 Mobility and AAA Protocols

2.1. Mobile IPv6 & Hierarchical Mobile IPv6

Mobile IPv6 allows mobile devices to move between networks while maintaining reachability and on-going connections between mobile host (MH) and correspondent nodes (CNs) [3]. This is achieved by sending Binding Update (BU) packages to the Home Agent (HA) and CNs upon movement from one domain to another. There is a significant delay from time of MH movement into a new domain to MH completed registration with the home domain. For this reason it is desirable to perform BUs only when absolutely necessary.

When using MIPv6, if a MH changes its attachment point, even if remaining in the same domain, the process of BUs still has to take place. Consequently the IETF has introduced Hierarchical Mobile IPv6 (HMIPv6) as an extension to the MIPv6 protocol [4]. HMIPv6 uses the idea of a local mobility anchor point (MAP) within foreign domains to reduce signaling requirements. The MAP acts essentially as a local domain HA and can be located at any level in a hierarchical network of routers including the Access Router (AR). Figure 2 gives a simple example of HMIPv6 enabled network architecture.

In this architecture MAP ensures seamless handoff when MH is moving from AR1 to AR2. When a HMIPv6 enabled MH moves into a domain such as the one given in figure 2, it is immediately informed of the global address of the MAP via router advertisements (RAs). From then on each time the MH changes its access point, the RA, using the MAP option, will inform the MH whether it still resides within the same MAP domain or not. If the MH is not within the same MAP domain, BUs must again be performed with HA and CN.

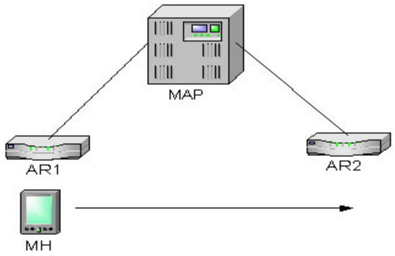

Fig.2 Simple HMIPv6 setup

Upon arrival in this new domain the MH must configure two addresses: (i) on the MAPs subnet a regional care of address (RCoA) corresponding to the CoA in MIPv6 and formed in a stateless manner based on the IP prefix in the MAP option; (ii) an on-link care of address (LCoA) indicating the actual location of the MH. If the MH moves from AR1 to AR2 its LCoA will change while its RCoA will not. A BU is sent to the MAP to inform of the MH's LCoA and HA. Now when packets are sent to the MH they will be first interpreted at the MAP and then forwarded to the MH's LCoA. This has the extra advantage of giving the MH location privacy relative to a CN. A CN is only aware of RCoA.

The architecture in Figure 2 could be easily extended to include a hierarchy of MAPs. This may be necessary in the case of a much bigger domain. To efficiently use bandwidth a MH can choose to register with more than one MAP simultaneously and use each MAP address for a specific group of CNs. For example if the CN exists on the same network as the MH it would be more efficient to use the first hop MAP for communication between them.

2.2 Fast Mobile IPv6

When a MH moves into a network it demands immediate ability to send and receive packets. This is inhibited by the time it takes for movement detection and new CoA (NCoA) configuration to take place. FMIPv6 attempts to eliminate some of this time delay by enabling the MH to perform a few operations ensuring low latency handoff before leaving its current network [12].

A MH discovers new AR using link layer functionality. It sends a Router Solicitation for Proxy advertisement (RtSolPr) to its previous access router (PAR). Information from the new access point is returned via proxy router advertisement (PrRtAdv). The MH uses this to formulate a prospective NCoA. At this stage the MH sends a fast binding update (FBU) to the PAR. The PAR and new AR (NAR) exchange handover initiate (HI) and handover acknowledge messages in order to verify acceptability of NCoA and set up a tunnel between PAR and NAR. The PAR then sends a fast binding update acknowledge (FBack) to the MN alerting it that it can now switch to NAR. All packets arriving at the PAR will be tunneled to NAR from that point on. Within the new network the MH can send BU to CN alert of new location.

In the case the MH moves before FBU is sent or before FBack is received. It is also possible for MH to send FBU through NAR to PAR. This process is similar to the previous one.

2.3 RADIUS and Diameter

RADIUS [5, 6] is an AAA protocol initially defined by IETF to help with managing dispersed serial lines and modem pools. By using RADIUS an organization can store information (including authentication and configuration information) in a central database. This information can be delivered to the user in a number of different ways, for example by using the Point-to-Point Protocol (PPP) or TELNET.

RADIUS uses the client-server model. The RADIUS client is known as a Network Access Server (NAS). The NAS is responsible for forwarding user requests to the RADIUS server and interpreting responses from the server sent to the user. The RADIUS server holds a database of all users, their authentication information and configuration information. The server interprets and authenticates NAS requests and forwards to the relevant user configuration information. A server may also act as a proxy to another RADIUS server. The NAS and the RADIUS server use a shared secret value, which is never sent over the network. All user passwords are sent encrypted between NAS and RADIUS server to avoid snooping.

RADIUS is the main AAA protocol in use today. However, as routers and NASs have increased in complexity and problems such as seamless mobility have become an issue, the RADIUS protocol has become increasingly unsuitable for use in today's networks. RADIUS is also limited in command and added value parameter (AVP) space, which makes it difficult to introduce new services. RADIUS also operates over UDP, which has no timing and re-sending mechanisms. In addition RADIUS does not support encryption of all AVPs and only supports hop-by-hop security. Due to these problems some vendors have come up with their own adjusted versions of RADIUS. This has resulted in incompatibility between protocol implementations.

In recent years the IETF has been developing a new AAA protocol, called 'Diameter' [13]. Diameter is completely backwards compatible with RADIUS, retains the basic RADIUS format but attempts to fix all its various deficiencies. The basic idea of Diameter was to create a base protocol that could be extended in order to allow new access methods. Hence Diameter consists of a Base Protocol and different extensions / applications like the Extensible Authentication Protocol (EAP), NAS and MIPv4 applications [7-9]. All basic functionality common to all applications and services is implemented in the Base Protocol while all application specific functionality exists within the different applications. The Base Protocol assumes a peer-to-peer communications model as opposed to a client-server model. Diameter uses TCP and SCTP for reliable transport. The Base Protocol design, among other features, incorporates a large AVP space, support for vendor AVPs and commands, reliability provided by underlying SCTP, a well-defined failover scheme, support for unsolicited messages to clients, integrity and confidentiality at the AVP level and end-to-end security.

3 3P-AAA Architectural Framework

In this section we propose a new third-party AAA architectural framework (Figure 3), employing a hybrid signaling protocol based on MIP, HMIP, FMIP and Diameter, and integrating mobility and AAA functions for 4GWW orientated to a more consumer based business model.

Every mobile user owns a smart card inserted into the MH currently used. This smart card contains a user access profile including details such as: the users' network access identifier (NAI), access network preferences, and authentication and authorization details. These are essential pieces of information for a MH to enter and use any access network. Access technology is arbitrary, e.g. WLAN, 2G/2.5G/3G etc. but the core structure remains the same. All traffic is IPv6 based.

Any movement of the MH within the local domain is supported by HMIP. The MAP structure makes it possible to avoid the heavy signaling associated with MIPv6. The Local MAP also functions as an AAA client to the local AAA server. Inter-Domain movement is supported by MIPv6 and FMIPv6. The MH is enabled with a hybrid MIPv6, HMIPv6, FMIPv6.

In the past AAA and mobility operations

have been carried out as separate operations. In reality these activities are interdependent. If a MH moves into a new network it must be authenticated and authorized for that network. It has been observed that round trip times (RTTs) can be reduced if the two operations are knitted together [10]. In our architectural framework, mobility information is piggybacked on AAA packets. More specifically, MIP type packets are encapsulated in Diameter messages.

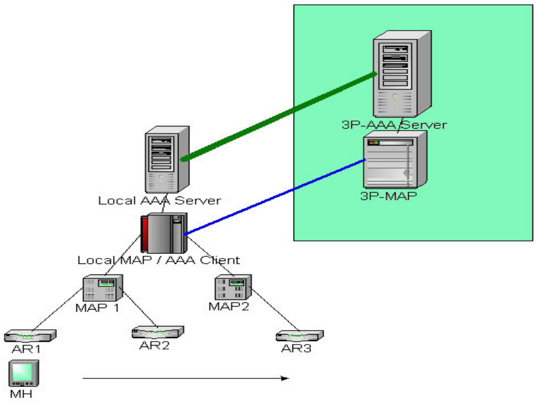

Fig.3 3P-AAA Architectural Framework

In the CBM a third party handles AAA operations. This model is extended to incorporate a 3P-AAA server coupled with a 3P-MAP. Together they handle MH security, keep track of MH billing information and current MH network location. The MAP also functions as a router and an AAA client. All data exchange is done through MAPs just as it would be using normal network routers. For each connection passing through a MAP, the MAP has the capability of requesting a Diameter accounting session with the local server. This way all billing information can be kept for data sessions.

4 3P-AAA Hierarchy

Figure 3 above depicts the 3P-AAA architectural framework as having one single 3P-AAA central server. This is suitable for small-scale adoption of the scheme but for large-scale introduction, a hierarchy of such 3P-AAA servers would likely exist. In figure 4, such a hierarchy is illustrated, showing separate 3P-AAA servers in use on Local, Regional, and National level. A typical situation where this level of hierarchy might be applicable is where locally WLAN is used while on a regional and national level an all-IP UMTS is used. It is clear that the user can reside in two types of user access network (UAN). For instance in figure 4, the user has access to UAN1, UAN2, UAN3 and UAN4 on a local level, and to UAN(i) and UAN(ii) on a regional and national level[3].

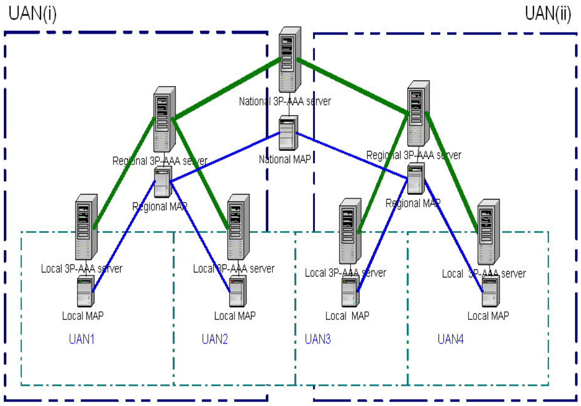

Fig.4 3P-AAA hierarchy

A user can be authenticated on any UAN within whose range s/he is currently of. This means any one user can be authenticated and authorized to use many access networks at once. A typical situation is where the user has a dual access mode terminal and can access both local and regional networks in range. Depending on the required scope of the user, the user may require to login as a local, regional or national user. To access local services a user need only be authenticated on the local 3P-AAA server. To access any local services within a region, the user must be authenticated on the regional 3P-AAA server. To access any services nationally the user must be authenticated nationally. According to what level of access the user requires, extra charges may be incurred. Generally the user will have preset preferences as to behavior of the terminal in demanding access. These settings can be stored in the terminal's smart card.

All billing information for a user is centralized. In this case billing information is stored by the National 3P-AAA server. Accounting information is collected by the individual regional and local servers and forwarded to the national server. The 3P-AAA servers are physically linked as shown in figure 4 (ideally by a high-bandwidth optical backbone). This means that any requests on national level are proxied through local and regional servers. All answers are similarly treated in the opposite direction.

The basic task of each MAP is to route all incoming and outgoing data packets and to store

[3] The use of four local UANs and two regional/national UANs is purely for illustration purposes. Numbers may be increased greatly in an actual national network.

binding update information for MHs when requested. Also MAPs incorporate an AAA client, which is responsible for requesting accounting sessions. Any MAP can demand an accounting session for incoming or outgoing packets for any user.

As mentioned in the previous section each user has a smart card. This stores the users' NAI. RFC2486 gives a definition of NAI and outlines its use for roaming between networks [11]. Each user will have a unique identity. An example might be "0981234567". If this user happened to be in café foobar, in Limerick city, in Ireland, the user's NAI would be 0981234567@foobar.Limerick.Ireland. When the user accesses the network, the user's location needs to be stored for incoming call connection (ICC) routing purposes. The authenticating server decides where on the network the user's NAI should be stored. Usually this will consist of local storage as well as instructing other MAPs to do so as well. Within the 3P-AAA architecture the NAI system is envisaged as working very much like the DNS system. When one user wishes to make a call to another (say to user "0981234567"), the receiving user must first be located. For this a NAI query (similar to a DNS query) is first made. NAI's requests and answers are iteratively routed through the 3P-AAA server hierarchy until an 3P-AAA server finds an NAI match on its corresponding MAP. This MAP (also acting as an AAA client) responds with location information of user "0981234567". The incoming call (this may be any type of voice/data communication) is then directed to this location. The communication is handled by IPv6 packets and addresses (hidden from the user in the background). Each NAI is stored with a corresponding IPv6 address.

4.1 Using Diameter as a 3P-AAA Signaling Protocol

Diameter is the most suitable signaling protocol for the proposed 3P-AAA architectural framework [14]. Much of the basic functionality required to support the 3P-AAA scheme is found in the Diameter Base specification. In the case where a usage scenario is not able to fit into an existing Diameter application a new Diameter application needs to be defined. The 3P-AAA system outlined above requires the definition of a new Diameter application, which would be supported by full Diameter Base protocol functionality. In particular the support for mobility over this new 3P-AAA architectural framework demands new Diameter messages specified in Table 1.

Table1. New Proposed Diameter Messages

Message	Use
3P-AAA-MH-Request	This message is sent by the MH when entering a new network. It is essentially an access request with a Binding Update (BU) request piggybacked.
3P-AAA-MH-Answer	This message is sent in reply to a *3P-AAA-MH-Request*. It indicates whether access request and Binding Update where successful. If successful it may also carry configuration info.
MAP-Binding-Request	This message is sent by an AAA server to the local MAP to request a BU for a MH.
MAP-Binding-Answer	This message is sent in reply to a "MAP-Binding-Request". It must indicate whether binding was successful or not.
NAI-Request	This message is used by a MH attempting to connect to another MH. It indicates the user identifier of the host being called.
NAI-Answer	This message is sent in reply to an *NAI-Request*. It indicates the current IPv6 address of the user being called.

To support these messages many new Diameter AVPs need to be defined. For instance new AVPs will be needed to carry the BU information for *3P-AAA-MH-Request* and *3P-AAA-MH-Answer*, and also possibly to support some FMIPv6 functions.

5 Usage Scenario

The 3P-AAA server to use is selected according to the users current needs matched with the user's smart card user profile. Say for example a hierarchical system such as illustrated in Figure 4 is to be set up in Ireland. Ireland can be broken down into four regions: Munster, Leinster, Connaught, and Ulster. Each region can be broken down into localities. Munster consists of Clare, Limerick, Waterford, Tipperary, Cork, and Kerry. Within each of the individual localities and regions an AAA server and MAP is placed to service users. Additionally a national AAA server and MAP exist. Each user has a unique identifier. In our example user's identifier is "userA". UserA resides in the Limerick locality. UserA has current NAI of "userA@Limerick.Munster.Ireland". It is assumed that userA has an account with the Ireland 3P-AAA provider. The following example illustrates how userA registers to have access to networks on a national level (Figure 5).

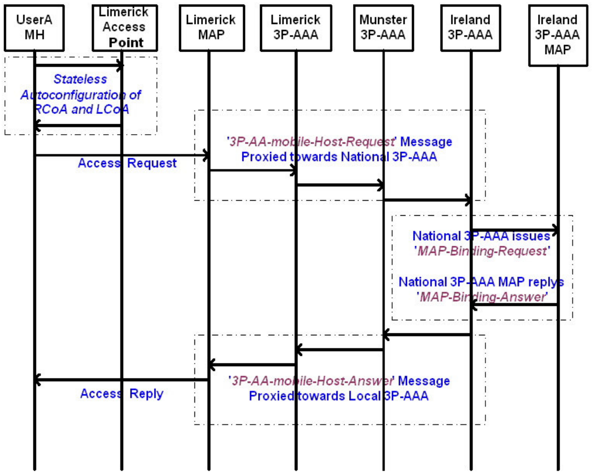
UserA MH
Limerick Access Point
Limerick MAP
Limerick 3P-AAA
Munster 3P-AAA
Ireland 3P-AAA
Ireland 3P-AAA MAP
Stateless Autoconfiguration of RCoA and LCoA
Access Request
'3P-AA-mobile-Host-Request' Message Proxied towards National 3P-AAA
National 3P-AAA issues 'MAP-Binding-Request'
National 3P-AAA MAP replys 'MAP-Binding-Answer'
'3P-AA-mobile-Host-Answer' Message Proxied towards Local 3P-AAA
Access Reply

Fig.5 3P-AAA register example

6 Conclusion

This paper has presented an idea on how the functions of mobility and AAA may be handled in future 4G networks. It has put forward a theoretical view on how an enabling protocol would operate. It seems appropriate to use the Diameter AAA protocol as an encapsulating protocol for mobility messages since mobility is dependent on a user gaining access to a network. This paper has built on the foundation of MIPv6, HMIPv6, FMIPv6, and Diameter protocols and suggested a hybrid protocol that draws on the most beneficial elements of all four protocols. Most of the adjustments suggested are given in the form of a new Diameter application.

Further study is needed in order to determine the particulars of the new Diameter messages suggested in section 4. Also additional thought is needed on the subject of how third-party accounting will be carried out. Although the Diameter Base Protocol supplies basic accounting functions, additional functions will likely be necessary.

A development would also be needed to create a suitable smart card system. This paper mentions user profiles but does not go into many specifics on the topic. The development of an NAI query system akin to the DNS system is an issue that is closely related to this smart card system.

Although the idea presented in this paper is in its infancy, it is our hope that future 4G networks will enable to adopt this type of 3P-AAA architectural framework under a consumer based business model (CBM). With such a system in place, an environment may be created where the potential benefits to be reaped in the wireless service provision market and in turn for the consumer are limitless.

References:

[1] Alonistioti N., N. Passas, A. Kaloxylos, H. Chaouchi, M. Siebert, M. O'Droma, I. Ganchev, C. B. Faouzi. *Business Model and Generic Architecture for Integrated Systems and Services: The ANWIRE Approach (white paper).* In Proc. CD of the WWRF 8bis meeting, 8 pages, Beijing, China. (Feb. 2004).

[2] O'Droma M. and I. Ganchev. *Techno-Business Models for 4G*, In Proc. of the International Forum on 4th Generation Mobile Communications, Pp. 3.5.1-30, King's College London, London. (May 2004).

[3] Johnson, D., C. Perkins, and J. Arkko, *Mobility Support in IPv6.* RFC3775, (June 2004).

[4] Soliman, H., et al., *Hierarchical Mobile IPv6 mobility management (HMIPv6).* "draft-ietf-mipshop-hmipv6-04.txt", (December 2004).

[5] Rigney, C., et al., *Remote Authentication Dial In User Service (RADIUS).* RFC2865, (April 1997).

[6] Rigney, C., *RADIUS Accounting.* RFC2866, (April 1997).

[7] Calhoun, P.R., et al., *Diameter Mobile IPv4 Application.* "draft-ietf-aaa-diameter-mobileip-20.txt", (August 2004).

[8] Calhoun, P.R., et al., *Diameter Network Access Server Application.* "draft-ietf-aaa-diameter-nasreq-17.txt", (July 2004).

[9] P. Eronen, E., T. Hiller, and G. Zorn, *Diameter Extensible Authentication Protocol (EAP) Application.* "draft-ietf-aaa-eap-10.txt", (November 2004).

[10] Engelstad, P., T. Haslestad, and F. Paint. *Authenticated access for IPv6 supported mobility*. in *Computers and Communication, 2003. (ISCC 2003). Proceedings. Eighth IEEE International Symposium on*. 2003.

[11] Aboba, B.a.M.B., *The Network Access Identifier.* RFC 2486, (January 1999).

[12] Rajeev Koodli, *Fast Handovers for Mobile IPv6* "draft-ietf-mipshop-fast-mipv6-03.txt", (Oct. 2004).

[13] Calhoun, P.R., et al., *Diameter Base Protocol.* RFC3588, (September 2003).

[14] Siebert M., C. F. Bader, H. Chaouchi, W. Xing, M. Dikaiakos, N. Passas, M. O'Droma, I. Ganchev et al. *System and Service Integration: Functional Entities and Reference Model.* ANWIRE, Academic Network for Wireless Internet Research in Europe, Deliverable D1.5.2. EU-FP5-IST-2001-38835. Pp. 1-101, (August 2004).