

AAA for Spontaneous Roaming Agreements In Heterogeneous Wireless Networks

Zhi (Judy) Fu¹, Minh Shin², John C. Strassner¹, Nitin Jain¹, Vishnu Ram¹, and William A. Arbaugh²

¹Motorola Inc., 1301 E Algonquin Rd., Schaumburg, IL 60196
{judy.fu, john.strassner, nitin, vishnu}@motorola.com

²Department of Computer Science, University of Maryland, College Park, MD, 20742
{mhshin, waa}@cs.umd.edu

Abstract. A current challenge in heterogeneous wireless networks is to enable them to work together in a spontaneous fashion, without having pre-established roaming agreements. Currently, formal roaming agreements are manually set up, which is a costly and time-consuming process. It is highly desirable for network cooperation to be established on the fly. However, establishing spontaneous roaming agreement is a very challenging research issue. This paper presents a novel AAA (Authentication, Authorization and Accounting) architecture to support policy-based negotiation for establishing spontaneous roaming agreements. The new architecture integrates policy-based negotiation into the normal user association and authentication process for spontaneous and dynamic roaming agreements and interworking. This integration minimizes changes to existing AAA architecture for enabling the new paradigm of automated provider interworking and cooperation.

1 Introduction

Providers are using heterogeneous wired and wireless systems to offer consumers increased network connectivity. Since it is unlikely that one wireless provider can provide ubiquitous coverage, high bandwidth access, and all possible services, the best way for consumers to get the most coverage for their desired services is for heterogeneous providers to cooperate and provide a single “composite” service in a seamless manner. However, the heterogeneous technologies and different administrative policies create significant challenges when various wireless networks are converged.

Currently, different wireless providers work together through formal roaming agreements that are statically defined. Setting up a roaming agreement today between two providers is a manual process. Typically, business people from the two operators meet and agree on the commercial terms and sign the necessary paperwork defining the agreement, and then technicians from each operator exchange technical information and configure elements within their own network. Even with industry standards, the roaming agreement setup is a costly and time-consuming process. It is therefore appropriate for long-term partnerships with large sessions but not suitable for spontaneous collaborations with short sessions. On the other hand, there will be numerous

providers with different service offerings, technologies, size and locations. It is not feasible to set up formal roaming agreements with every possible provider. However, since a consumer's access and services are limited by established roaming agreements, if a roaming agreement does not exist, users will either be disconnected or need to buy access at a prohibitively high cost.

It is thus highly desirable to enable spontaneous inter-working without pre-established roaming agreements between heterogeneous wireless providers. Not only would consumers get more services and coverage with only one subscription, providers would be able to generate more revenue with flexible partnerships and lower cost in providing more services to their customers. This is also beneficial for start-up providers to quickly offer their differentiated values versus established providers.

To address this need, brokered roaming agreement models have been deployed [1,2]. With the brokered model, operators establish roaming agreements with a broker and the broker then acts as a proxy to handle all roaming related signaling and traffic on behalf of the operators. With this model, operators benefit from not having to establish individual roaming agreements with other operators. However, there are also serious drawbacks to this model. First, the signaling, AAA and roaming traffic will have to go through the broker, incurring unnecessarily long latency. Second, operators have limited control and flexibility over establishing roaming terms with another operator. Third, operators have to pay brokers for any traffic going through the broker, and thus the profit margin becomes lower.

To overcome the limitations of the brokered roaming model, the Ambient networks project [3] proposed mechanisms for automatically establishing bilateral roaming agreements directly between operators. They proposed automatic negotiation between two servers to replace manual negotiation. The negotiations are conducted offline with triggers such as a new member of an industry association or deployment of a new access networks. With this automation, bilateral roaming agreements can be established efficiently at a lower cost. However, the agreements are still pre-established but not spontaneous roaming agreements that can be established on the fly. The main limitation of this approach is that random roaming activities at different locations cannot always be predicted; thus, pre-determined roaming agreements cannot cover all possible networks that users may roam to.

Therefore, the ideal case is to enable spontaneous roaming agreements to fulfill the vision of seamless and ubiquitous roaming for users. This also gives operators the highest flexibility and efficiency with the lowest attendant cost. However, there are significant challenges in enabling spontaneous roaming agreements of heterogeneous networks. First, there are significant challenges in establishing roaming agreements that fulfill all of the terms of current paper roaming agreements in an automatic yet efficient manner in (near) real time. Second, access to local resources still need to respect each organization's access, billing, administration, and other policies.

We propose to address these issues by adding a new module in existing AAA (Authentication, Authorization and Accounting) architectures to handle policy based negotiation for spontaneous roaming agreement establishment. Our paper makes the following contributions.

- We propose a novel AAA architecture with a Partnership Management Module to enable policy based negotiation for defining spontaneous and dynamic roaming agreements.

- We propose methods and models for basic trust establishment between providers for spontaneous inter-working.
- We design a new user entry and authentication process (i.e., a modified EAP_AAA process) at a unknown foreign network for spontaneous interworking with the home network with minimized changes to existing AAA processes.
- We specify policies and policy based negotiation processes for negotiating specific QoS, security, pricing, and other per-session parameters.
- We design a new Diameter application, called PMA (Partnership Management Application), for supporting spontaneous roaming agreements.
- We propose mechanisms to optimize the performance of establishing spontaneous roaming agreements.

The remainder of the paper is structured as follows. Section 2 describes the overall framework of our proposed AAA architecture. Section 3 presents the detailed Diameter PMA application design. Section 4 defines the policies for inter-working with unknown networks and presents a detailed policy based negotiation process. Section 5 discusses related work, and finally in section 6, we conclude the paper and outline our future work.

2 Architectural Design of AAA for Spontaneous Roaming Agreement

2.1 AAA for Spontaneous Roaming Agreement Architecture

Nowadays heterogeneous wireless networks are converging to provide IP services. The standard AAA architecture for cellular networks interworking with WLAN/WiMax is EAP with backend RADIUS or DIAMETER AAA server. To enable spontaneous roaming agreements, the new AAA architecture is illustrated in the following figure.

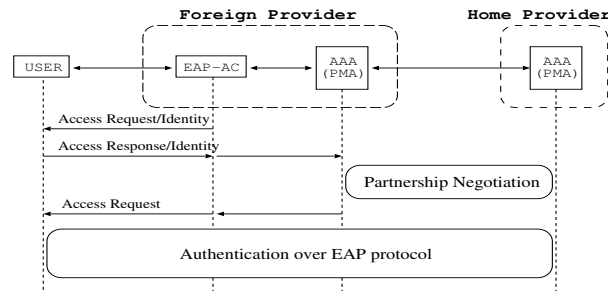


Fig. 1. New AAA Architecture with Partnership Negotiation

In this figure, the user is a subscriber of the home provider and the foreign provider is unknown to the home provider. EAP-ACⁱ (Extensible Authentication Protocol [4] Access Controller) is used to process EAP messages. In the above AAA framework, there is a new module called the Partnership Management Application (PMA) that enables two providers to conduct policy-based negotiation. As illustrated above, the EAP-AC passes the identity response to AAA of the foreign provider. When it is determined that the user belongs to an unknown home network, the local AAA starts the PMA module for policy based negotiation. When dealing with unknown providers, the partnership negotiation must first succeed before the normal authentication process for inter-working can start.

1.2 Trust Establishment Between Providers

Without prior agreements, establishing trust among providers is the driving factor for inter-working. Without trust, there is no guarantee that services will be honored and paid for. In addition, the performance can be a huge issue for starting negotiation from scratch. In today's world, the problem with negotiating everything on paper roaming agreements (even through on-line version, such as through secure web services) is that this process takes too long to be usable for users that want immediate, on-demand services, and in any case two providers have to have a basic trust to start with for negotiation. We propose the following possible trust models for two providers to establish a basic level of trust as a starting point for further focused and speedy negotiation.

- **Consortium model:** Providers join a consortium in which they all agree upon a basic set of agreements on common offerings, such as liability, customer care, basic security, minimum and maximum charging, and basic QoS. Members of the consortium are issued certificates, so that providers carrying a consortium-issued certificate are trusted by other consortium members that their subscribers will pay for the service as in the basic agreement.
- **Third Party Certification Model:** An independent trusted third party evaluates different providers, giving them a certificate with a relative score. A provider can check another provider's score on the fly through the third party to determine the trustworthiness of an unknown provider.
- **Transitive Trust Model:** Participating providers build a set of established trusts between them; using transitive trust, providers can derive additional trust relationships as needed.

In all three models, some sort of certificate verification will suffice to establish a basic trust between different providers.

The above models present alternative trust models that providers can match their own specific AAA and security requirements to, enabling them to establish a basic

ⁱ EAP-AC is either the native layer-2 EAP entity like Access Point (AP) or a special entity for processing EAP over IP PANA authentication traffic. See section 2.6 use case for further explanation.

level of trust as a starting point. Among the three models, the first model is considered the most practical, and thus we will focus on the first model in this paper.

In the consortium model, different providers have joined one consortium, say consortium X. Consortium X has a Master roaming agreement that includes a dispute settlement procedure, limitation of liability, billing procedure and responsibilities, customer care responsibilities, fraud tools and processes, agreement suspension and termination, minimum maximum charge of airtime or wholesale rate, and other required features. Members of X agreed on the above basic requirements and X issues a certificate to its members. This enables all members of X to identify each other, and hence establish trust.

If a member of X encounters an unknown provider, the two providers need to establish a basic level of trust (such as that provided by X to its members) to ensure that the new partner will fulfill its responsibilities and liabilities. The member of X can either request the unknown provider to join consortium X (which will then enable trust to be provided through certificate verification) or the member of X can use policy to decide if trust negotiation should be initiated or not. If trust is not established, then no inter-working will be possible; otherwise, if trust is established, on-line negotiation can be performed to define specific per-session requirements (such as QoS, security, and pricing) to finalize their partnership agreement.

The consortium model can also be extended to a multiple consortium case with cross-certification. For example, a group of GSM providers is one consortium, and a group of WiMax providers is another consortium. If two different consortiums have issued cross-certifications, then members of two consortiums will be able to verify each other and establish a basic trust between them. This model has the advantage that providers can keep their existing membership without having to join new consortiums.

2.3 Inter-Provider Policy-Based Negotiation for Spontaneous Roaming Agreement

2.3.1 Policies

Before conducting the negotiation, each provider prepares and specifies two different sets of policies – one for working with known providers, and another for working with unknown providers. The policies for working with unknown providers include at least the following functions:

- Foreign Provider's policy in providing service to non-subscribers
 - Home Provider trust policy: the certification and qualification of the non-subscriber's Home Provider that the Foreign Provider can trust
 - Non-subscriber's identification, authentication, and authorization policies
 - Other policies governing per-session features for the non-subscriber, such as QoS, security, and billing settings

- Home Provider's policy for subscribers accessing unknown Foreign Providers
 - Foreign Provider trust and qualification policies
 - Subscriber's identification, authentication, and authorization policies
 - Other policies governing per-session features for the non-subscriber, such as QoS, security, and billing

2.3.2 Inter-Provider Negotiation Overview

To enable spontaneous inter-working, the Foreign Provider and the Home Provider negotiate to achieve the following:

- **Establish Secure Channel:** Two providers will first establish a secure channel to protect their negotiation. For example, they use IPSec tunnel with consortium-issued certificates for mutual authentication.
- **Establish Business Trust:** Two providers exchange qualification related info to establish business trust. With the mutual trust, the Foreign Provider ensures that the service will get paid and the Home Provider ensures that the Foreign Provider is a legitimate and trusted partner...
- **Agree on Session Profile:** the two providers negotiate and agree on per-session features, such as what type of QoS is provided for which services.
- **Agree on Session Security:** the two providers negotiate and agree on methods for identification, authentication, and authorization, as well as for mechanisms for protecting user traffic.
- **Agree on Billing:** the two providers negotiate and agree on pricing and other billing related features.

To achieve the above goals, two providers will first exchange consortium identities and find a common consortium. Then, the two providers will use the consortium certificate to authenticate each other and establish an IPSec [5,6] tunnel to protect their further negotiation traffic. Once the basic level of trust and the secure tunnel for negotiation are established, they will focus on specific features, such as QoS, security and pricing in the negotiation. The negotiation can be done using a simple request/response protocol in the new PMA application. More detailed negotiation process will be presented in section 4.

2.4 Performance Optimization for Spontaneous Roaming Agreement Negotiation

The following performance optimization techniques are adopted.

- Once the basic trust and security tunnel for negotiation are established, the negotiation on QoS, security and other functions can be done in parallel.
- Subscribers of a Home Provider can be categorized into groups (e.g., Gold vs. Silver vs. Bronze classes), and one negotiation result can be reused many times in other sessions for the same user class.
- Similarly, a past negotiation result can be either suggested to the user or group or automatically reused, if desired

- Latency at handoff between providers can be critical. However, negotiation can be done at the pre-authentication phase while still connecting to the current network for seamless handoff.

3 DIAMETER AAA Framework for Spontaneous Roaming Agreement Establishment

In this section we describe the enhancements to existing AAA frameworks for establishing spontaneous and dynamic roaming agreements. To facilitate the formation of dynamic roaming agreements, existing AAA frameworks need to be upgraded with the new PMA module (Partnership Management Application). This requires appropriate interfaces to be added to the PMA application, so that it can be integrated with the existing AAA and L2 authentication protocols (e.g., EAP). A summary of the new additions to existing AAA frameworks is listed below.

- New PMA module in AAA servers
- Related impacts to the AAA messaging
- Changes to EAP messaging
- Changes to User device

One of our design goals is to minimize the changes to existing AAA infrastructure, although some changes are inevitable. In the following subsections, we will discuss these changes individually.

3.1 PMA (Partnership Management Application)

To facilitate the formation of spontaneous roaming agreements, existing AAA frameworks will have to be enhanced with the PMA module. The PMA is an AAA application that performs the negotiation portion of the roaming agreement. This application provides a framework for the negotiation and also specifies the roaming agreement parameters to be negotiated between the two operators. The PMA module can be implemented either as a DIAMETER[15] application or as middleware interfacing with the AAA server. Since the PMA is a policy defining entity for the access network, it is a good design option to integrate it with the AAA framework by building the PMA module as a Diameter application for Diameter server. For an AAA server using the RADIUS protocol, the middleware is the only option. While we focus on DIAMETER application design in this paper, the design of the middleware for RADIUS will be similar.

We define four main messages: CRR (Credential Request), CRA (Credential Answer), NIR (Negotiation Information Request) and NIA (Negotiation Information Answer). The new AVPs we define for PMA application include type of negotiation, trusted CA IDs, proposed price, data rate, security algorithm etc. More attributes can be easily added to support negotiation of other features. One of the advantages that our new framework has is to support providers to negotiate only issues that they care about the most and skip other issues that have been specified in the Master roaming

agreement, which enables both dynamics and fast performance in roaming agreement establishment. We omit detail here for respect of page limit.

3.2 Changes to Standard AAA Server

The new AAA server will be different from the traditional AAA server, exhibiting the following new behaviors:

- The AAA server has a new PMA application or module, and communicates with a policy system to learn the appropriate policies to use for a given situation.
- The foreign AAA server will start the PMA upon a request from a non-subscriber.
- Upon completion of the PMA negotiation process, the foreign AAA will send the negotiation result (e.g. authentication method) to EAP-AC, which then relays the result to the MS (Mobile Station/Device).
- If the negotiation is a success, normal AAA process to the home AAA will start. Otherwise, a “negotiation failure” error message will be communicated to the user and the user is disconnected.

3.3 Other Changes

- **Changes to EAP Messages:** Similarly, the EAP message needs to be extended to communicate the negotiation result back to the MS. The negotiation result may contain 1) identification, authentication and authorization methods, 2) other per-session features, such as QoS and billing. The Diameter EAP messages can be found in RFC4072.
- **Changes to User Device:** The entire negotiation process is almost transparent for the users. However, the user device is required to be equipped with EAP client capability if it has not already done so. Other than that, the only change to the user device is the added capability to process the EAP negotiation result message and to start the authentication process after a successful negotiation.

4 Policy Engine for Spontaneous Roaming Agreements

Foreign and Home Providers use policies to govern the negotiation on what Providers they will establish roaming agreements with as well as the per-session features that each Provider will support. In this section, we explore various policies required for Providers to allow spontaneous access.

The Foreign Provider needs a policy that defines the requirements for a non-subscriber’s access and its restrictions (called a *non-subscriber policy*). In contrast, the Home Provider needs a policy that defines the requirements for a subscriber’s access to outside services (called a *foreign-access policy*). In this section, we discuss each type of policy and present some examples.

We use [14] as a source for the following formal definitions. **Policy** is a set of rules that are used to manage and control the changing and/or maintaining of the state of

one or more managed objects. A **Policy Rule** is an intelligent container. It contains data that define how the Policy Rule is used in a managed environment as well as a specification of behavior that dictates how the managed entities that it applies to will interact. The contained data is of four types: (1) data and metadata that define the semantics and behavior of the policy rule and the behavior that it imposes on the rest of the system, (2) a set of events that can be used to trigger the evaluation of the condition clause of a policy rule, (3) an aggregated set of policy conditions, and (4) an aggregated set of policy actions. For flexibility, the DEN-ng model defines three clauses (a Policy Event clause, a Policy Condition clause, and a Policy Action clause) that aggregate individual and groups of **Policy Events**, **Policy Conditions**, and **Policy Actions**. Each of these three clauses are treated as atomic objects that are in turn aggregated by a Policy Rule. A Policy Event defines the necessary occurrence or combination of occurrences that are used to trigger the evaluation of the Policy Condition clause. A Policy Condition defines the necessary state and/or prerequisites that define whether the actions aggregated by that same Policy Rule should be performed. This is signified when the Policy Condition clause associated with a Policy Rule evaluates to TRUE. (Note that in the DEN-ng policy language, an alternative set of Policy Actions can be defined that are executed when the Policy Condition clause evaluates to FALSE.) A Policy Action defines the necessary actions that should be performed if the Policy Condition clause evaluates to TRUE.

Most importantly, the effect of the Policy Action clause is to apply a set of actions to a set of managed objects, and have the effect of either **maintaining an existing state**, or **transitioning to a new state**, of that set of managed objects.

We have designed our policy system as a set of reusable components and built a prototype policy implementation. We have to omit details here due to page limit.

5 Related Work

We have talked about major related work in the introduction section. For respect of page limit, we briefly discuss related work here. First, brokered roaming agreement model [1, 2] is being deployed to reduce burdens of bilateral agreements. Comparing with them, our proposed system offers a more efficient, low cost, and dynamic solution to roaming. To overcome the limitations of the brokered roaming model, Ambient networks project [3] proposed mechanisms for automatically establishing bilateral roaming agreements directly between operators. However, this type of pre-determined roaming agreements are relatively fixed and can't be dynamically adapted in different conditions. Current inter-working related AAA work assumes the use of pre-established roaming agreements. [7, 8, 9]. Research on spontaneous access is, to date, mostly devoted to access control models [12, 13] without authentication architecture.

6 Conclusion

We presented a novel AAA architecture for heterogeneous providers to work together spontaneously and securely without pre-established formal roaming agreement. Spon-

taneous and dynamic roaming agreements are established through policy based negotiation. Building upon basic agreements established at a consortium(s), policy based negotiation for spontaneous roaming agreement is conducted upon user request and is seamlessly integrated into user association and authentication process. The online negotiation focuses on the issues that providers care about the most and can be done quickly with performance optimization techniques. Furthermore, we designed a new Diameter application to handle the negotiation for spontaneous roaming agreement, and we also designed policy language and policy based negotiation process. Work is currently in progress to prototype the system, and refine the proposed model.

References

1. Weroam service: <http://www.weroam.com>
2. Comfone service: http://www.comfone.com/_main_pages/services/broker/key2roam.htm
3. Ambient Networks Security Architecture document at: http://www.ambientnetworks.org/phase1web/publications/D7_2_Ambient_Network_Security_Architecture_PU.pdf
4. B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowitz, "Extensible Authentication Protocol (EAP)", RFC 3748, (2004)
5. IPsec information may be found here: <http://www.ietf.org/html.charters/OLD/ipsec-charter.html>
6. IETF, "Internet Key Exchange (IKEv2) Protocol, RFC4306
7. H. Kim, W. Ben-Ameur, and H. Afifi, "Toward Efficient Mobile Authentication in Wireless Inter-domain", in Proceedings of IEEE ASWN (Applications and Services in Wireless Networks), Berne, Switzerland, (2003)
8. Ulrike Meyer, Jared Cordasco, and Susanne Wetzel, "An Approach to Enhance Inter-Provider Roaming Through Secret Sharing and its Application to WLANs", WMASH 2003, Cologne, Germany, (2005)
9. Salkintzis, Ke. et al., "WLAN-GPRS Integration for Next-Generation Mobile Data Networks", IEEE Wireless Communications, (2002)
10. [3GPP TS 23.234](#) v2.4.0, "3GPP system to Wireless Local Area Network (WLAN) Interworking; System Description (Release 6)", (2004)
11. [3GPP TS 33.234](#) v1.0.0, "Wireless Local Area Network (WLAN) Interworking Security (Release 6)", (2003)
12. Ramiro Liscano and Kaining Wang, "A SIP-based Architecture model for Contextual Coalition Access Control for Ubiquitous Computing", Mobiquitous 2005, (2005)
13. Eve Cohen, Roshan K. Thomas, William Winsborough, and Deborah Shands, "Models for Coalition-based Access Control (CBAC)", SACMAT 2002, (2002)
14. J. Strassner, "Policy Based Network Management", Morgan Kaufman Publishers, (2003)
15. P. Calhoun et al, RFC 3588 - Diameter Base Protocol, <http://www.faqs.org/rfcs/rfc3588.html>