Diameter protocol stack development for IP Multimedia Subsystem(IMS)

Raseena Yousuf, Mini P.R.

Abstract—In this paper, we describe the Diameter protocol initially developed by the Internet Engineering Task Force (IETF) as an Authentication, Authorization, and Accounting (AAA) framework intended for applications such as network access and IP mobility. Diameter was further embraced by the Third Generation Partnership Project (3GPP) as the key protocol for AAA and mobility management in 3G networks. The paper discusses the use of Diameter in the scope of the IP Multimedia Subsystem (IMS) as specified by 3GPP, with emphasis on its use on the Cx interface between the Call Session Control Function (CSCF) and the Home Subscriber Server (HSS). The goal of this work was to implement basic Diameter functionality. The paper discusses the implementations of the Diameter Base Protocol that can be extended in order to provide AAA services to new access technologies.

Index Terms— AAA, CSCF, Diameter protocol, HSS, IP Multimedia Subsystem.

1 Introduction

EVOLUTION of the third generation network architecture is driven among other factors, by the requirement to provide a rather fast, flexible and cost-efficient way of introducing new services for operators, as well as third-party service and content providers. The IP Multimedia Subsystem (IMS)[1], as specified by the Third Generation Partnership Project (3GPP), represents the key element for supporting ubiquitous service access to multimedia Internet services, with adequate support for Quality of Service as well as advanced, service-differentiated charging. Initially specified by 3GPP/3GPP2, the IMS standards are now being adopted by other standards bodies including ETSI/TISPAN. For the purposes of Authentication, Authorization, and Accounting (AAA) and mobility management in 3G networks, 3GPP has adopted the Diameter protocol [2], developed by the Internet Engineering Task Force (IETF). This paper discusses the use of Diameter within the scope of the IMS.

The stovepipes in telecommunication can be avoided by adopting the horizontally internet model. The traditional model of one operator playing both the role of service provider and network operator is outdated. Due to this trend, new models need to be found that disengage the different roles. When multiple providers are part of the supply chain, interaction between these providers is necessary. Because every provider resides in its own domain, the services cross multiple domains. When enabling service interaction over multiple domains several issues arise.

Security of multi-domain service interaction is one of these issues. How does the interaction service know if a user is allowed to use the service? And how can the providers that reside in different domains trust each other? For example a user has a different telephony and television provider, and some service is in place to enable interaction between these two basic services. How can the user be billed for the different services? Or how does the television service know that the interaction service is allowed to intervene? For this reason authentication, authorization and accounting (AAA) is needed for multi-domain service interaction.

AAA can be provided by AAA protocols and an example of such protocol is Diameter [2]. Diameter is the newest AAA protocol developed in 2001 from the older AAA protocol RADIUS.

2 How Diameter Fits In IMS

The IMS is based on a horizontally layered architecture, consisting of three layers, namely, Service Layer, Control Layer, and Connectivity Layer. Service Layer comprises application and content servers to execute value-added services for the user. Control layer comprises network control servers for managing call or session set-up, modification and release. The most important of these is the Call Session Control Function (CSCF). Connectivity Layer comprises routers and switches, for both the backbone and the access network.3GPP standards body adopted DIAMETER as the primary signalling protocol for AAA and mobility management in IMS. A simplified IMS architecture is shown in Figure 1.

In this paper, we focus on the interface between the Home Subscriber Server (HSS) and the CSCF. The HSS serves as the main data storage for user related information, such as IMS user profiles (including location), security and registration information, access parameters, and application server profiles. The CSCF may serve three different purposes, as the Proxy CSCF (P-CSCF), the Interrogating CSCF (I-CSCF), and the Serving CSCF (S-CSCF). The S-CSCF uses the DIAMETER "Cx" interface both to request authorization information from the HSS in response to a SIP registration request and to retrieve subscriber information.

2.1 The Cx reference point

As per IMS technical specifications [3][4], the Cx reference point is located between the S-CSCF/I-CSCF and the HSS, as shown in Figure 2. The Subscription Location Function (SLF) is required in a network in which there is more than one HSS; it provides the mapping between a particular user address and its corresponding HSS. As already noted, the protocol used at the Cx reference point is Diameter. Here we focus on network having only one HSS.

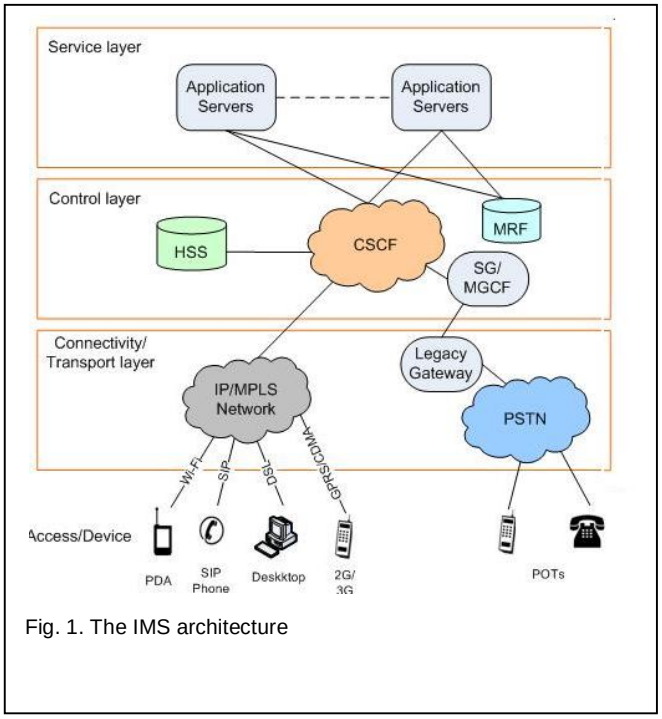

Fig. 1. The IMS architecture

Procedures in the Cx reference point may be grouped into three areas: Location management procedures, User-data handling procedures, Authentication procedures. Each group of procedures is briefly described next.

Location management procedures

In location management procedures, the User-Authorization-Request (UAR) command is sent to the HSS whenever the I-CSCF receives a SIP REGISTER request from the P-CSCF. The UAR command contains private and public user identity, visited network identifier, routing information, and type of authorization. In response to the UAR command, the HSS responds with the User-Authorization-Answer (UAA) command. The UAA command contains the name of the S-CSCF assigned to the user. After authorization, the I-CSCF finds an S-CSCF that will serve the user, and it forwards the SIP REGISTER request to the S-CSCF. Once the S-CSCF receives the SIP REGISTER request, it uses the Server-Assignment-Request (SAR) command to communicate with the HSS, and it informs the HSS which S-CSCF will be serving the user. The HSS responds with the Server-Assignment-Answer (SAA) command, which contains the user profile and charging information. Later, when the HSS wants to initiate de-registration it uses the Registration-Termination-Request (RTR) command, stating the reason for de-registration. The RTR command is acknowledged by a Registration-Termination-Answer (RTA) command. If an I-CSCF receives any SIP method other than REGISTER, a procedure for finding S-CSCF uses the Location-Info-Request (LIR) command containing public user identity and routing information. The HSS responds to LIR with Location-Info-Answer (LIA) command, containing the name of the S-CSCF.

User-data handling procedures

During the registration process, user and service-related data are downloaded from the HSS to the S-CSCF via the Cx reference point by using SAR and SAA commands. It is possible, however, for this data to be changed later, during the time while the S-CSCF is still serving the user. To update the data in the S-CSCF, the HSS sends a Push-Profile-Request (PPR) command with private user identity, routing information, and user data. The response to the PPR command is Push-Profile-Answer (PPA) command.

Authentication procedures

In the IMS, authentication relies on a pre-configured shared secret and a sequence number stored within the IP Multimedia Services Identity Module (ISIM) in the User Equipment (UE) as well as in the HSS in the network. To authenticate the user, the S-CSCF sends a Multimedia-Auth-Request (MAR) command to the HSS. MAR contains the private and the public user identities, S-CSCF name, routing information, number of authentication items, and authentication data. The HSS responds to the MAR command with the Multimedia-Auth-Answer (MAA).

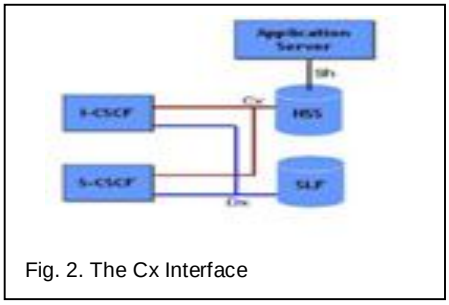

Fig. 2. The Cx Interface

2.2 Diameter Protocol

Diameter is an authentication, authorization and accounting (AAA) protocol developed by the Internet Engineering Task Force (IETF). It is based on an earlier IETF's AAA protocol called RADIUS (Remote Authentication Dial-In User Service), widely used for dial-up PPP (Point-to-Point Protocol) and terminal server access. Extending the functionality of RADIUS, Diameter is designed to provide AAA services for a range of access technologies, including wireless and Mobile IP. The Diameter specifications consist of the Diameter Base Protocol [2], Transport Profile, and applications such as Mobile IPv4, network access server, credit-control, and Extensible Authentication Protocol (EAP). The Diameter Base protocol is utilized for negotiating capabilities, delivering Diameter data units, handling errors, and providing for extensibility. On the other hand, the Diameter application defines application-specific functions and data units. Diameter is an application layer protocol. Transport protocols to carry Diameter messages include Transmission Control Protocol (TCP) and Stream Control Transmission Protocol (SCTP). For securing the connection, Internet Protocol Security (IPSec) and Transport Layer Security (TLS) are applied.

Diameter is a peer-to-peer protocol, meaning that any Diameter *node* may initiate a request. The three types of nodes are *clients*, *servers*, and *agents*. Clients are generally edge devices of a network which perform access control. A Diameter agent provides relay, proxy, redirect, and translation services, while Diameter server handles the AAA requests for a particular

domain, or realm. Message routing is based on the network access identifier of a particular user.

As to data structure, in each Diameter node there is a peer table, which contains a list of known peers and their corresponding properties. Each peer table entry is associated with an identity and can be either statically or dynamically assigned. It includes a relative priority setting, which specifies the role of the peer as primary, secondary, or alternative. The status of the peer relates to a specific configuration of the finite state machine of the peer connection, called the Diameter Peer State Machine. As a part of message-routing process, Diameter realm-routing table references the Diameter peer entries. All realm-based routing lookups are performed against a realm-routing table. The realm-routing table lists the supported realms, with each route entry containing certain routing information. Each route entry is either statically or dynamically discovered. Dynamic entries are associated with an expiry time and also route entry is associated with an application identifier, which enables route entries to have a different destination depending on the Diameter application. In a Diameter peer table the destination of a route entry corresponds to one or more peer entries.

A Diameter message consists of a Diameter header, followed by a certain number of Diameter attribute-value pairs (AVPs). The Diameter header is composed of fields denoting Command Flags, Command Code, and Application ID. The Command Code denotes the command associated with the message, while the Application ID identifies the application to which the message is applicable. AVPs define the method of encapsulating information relevant to the Diameter message.

3 Development of Diameter Base Protocol

3.1 Diameter Base Protocol

Diameter is a peer-to-peer protocol that involves delivering attribute-value pairs (AVPs). A Diameter message includes a header and one or more AVPs. The collection of AVPs in each message is determined by the type of Diameter application, and the Diameter protocol also allows for extension by adding new commands and AVPs. Diameter enables multiple peers to negotiate their capabilities with one another and defines rules for session handling and accounting functions.The base Diameter protocol may be used by itself for accounting applications but for use in authentication and authorization it is always extended for a particular application. Diameter nodes (Clients/Servers/agents) must support the base protocol, which includes accounting. In addition, they must fully support each Diameter application that is needed to implement the nodes service.

- *Raseena Yousuf is currently pursuing masters degree program in communication engineering in Federal Institute of Science and Technology,Mahathma Ghandhi University, India. E-mail: raseenayousuf123@yahool.com*
- *Mini P.R. is a professor in electronics and communication engineering in Federal Institute of Science and Technology, Mahathma Ghandhi University, India.*

The base Diameter protocol concerns itself with capabilities negotiation, how messages are sent and how peers may eventually be abandoned. The base protocol also defines certain rules that apply to all exchanges of messages between Diameter nodes. Communication between Diameter peers begins with one peer sending a message to another Diameter peer. The set of AVPs included in the message is determined by a particular Diameter application. One AVP that is included to reference a user's session is the Session-Id. The initial request for authentication and/or authorization of a user would include the Session-Id. The Session-Id is then used in all subsequent messages to identify the user's session. The communicating party may accept the request or reject it by returning an answer message with the Result-Code AVP set to indicate an error occurred. The specific behavior of the Diameter server or client receiving a request depends on the Diameter application employed. Session state (associated with a Session-Id) must be freed upon receipt of the Session Termination-Request, Session-Termination-Answer, expiration of authorized service time in the Session-Timeout AVP, and according to rules established in a particular Diameter application. The base Diameter protocol is run on port 3868 of both TCP [TCP] and SCTP [SCTP] transport protocols.

3.2 Connections vs. Sessions

A connection is a transport level connection between two peers, used to send and receive Diameter messages. A session is a logical concept at the application layer and is shared between an access device and a server, and is identified via the Session-Id AVP. In the example provided in Figure 3, peer connection A is established between the Client and its local Relay. Peer connection B is established between the Relay and the Server. User session X spans from the Client via the Relay to the Server. Each "user" of a service causes an authentication request to be sent, with a unique session identifier. Once accepted by the server, both the client and the server are aware of the session. It is important to note that there is no relationship between a connection and a session. Diameter messages for multiple sessions are all multiplexed through a single connection.

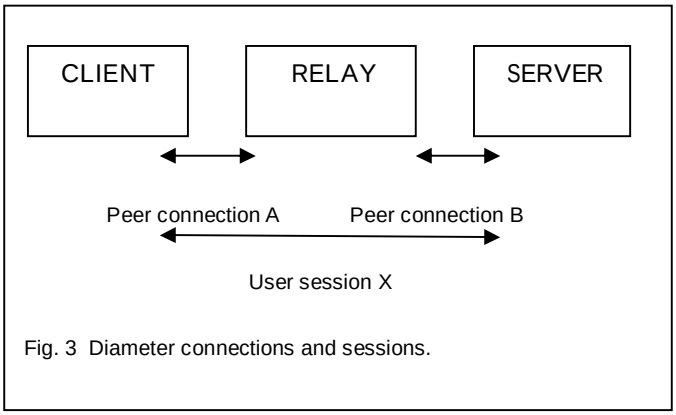

Fig. 3 Diameter connections and sessions.

3.3 Diameter Cx Interface

The Cx and Dx interfaces are the reference points for interac-

tions between Home Subscriber Server (HSS), Interrogating Call Session Control Function (I-CSCF) and Serving Call Session Control Function (S-CSCF).

A Serving-CSCF (S-CSCF) is the central node of the signaling plane. It is a SIP server but performs session control as well. It is always located in the home network. It uses Diameter Cx and Dx interfaces to the HSS to download and upload user profiles. It has no local storage of the user. All necessary information is loaded from the HSS. It handles SIP registrations, which allows it to bind the user location (e.g. the IP address of the terminal) and the SIP address. It sits on the path of all signaling messages, and can inspect every message. It determines which application server(s) the SIP message will be forwarded to, in order to provide their services. It provides routing services, typically using Electronic Numbering (ENUM) lookups. It enforces the policy of the network operator .There can be multiple S-CSCFs in the network for load distribution and high availability reasons. It's the HSS that assigns the S-CSCF to a user, when it's queried by the Interrogating-CSCF (I-CSCF).

I-CSCF is another SIP function located at the edge of an administrative domain. Its IP address is published in the Domain Name System (DNS) of the domain, so that remote servers can find it, and use it as a forwarding point (e.g. registering) for SIP packets to this domain. I-CSCF queries the HSS using the Diameter Cx interface to retrieve the user location (the Dx interface is used from I-CSCF to SLF to locate the needed HSS only) and then routes the SIP request to its assigned S-CSCF.

The Cx and Dx interfaces provide a number of message commands that can be used within the application. The command names are listed in Table 1.

TABLE 1
CX/DX INTERFACE COMMANDS

Command Name	***Abbreviation***	***Source***	***Destination***	***Code***
User-Authorization-Request	UAR	I-CSCF	HSS	300
User-Authorization-Answer	UAA	HSS	I-CSCF	300
Server-Assignment-Request	SAR	S-CSCF	HSS	301
Server-Assignment-Answer	SAA	HSS	S-CSCF	301
Location-Info-Request	LIR	I-CSCF	HSS	302
Location-Info-Answer	LIA	HSS	I-CSCF	302
Multimedia-Authentication-Request	MAR	S-CSCF	HSS	303
Multimedia-Authentication-Answer	MAA	HSS	S-CSCF	303
Registration-Termination-Request	RTR	HSS	S-CSCF	304
Registration-Termination-Answer	RTA	S-CSCF	HSS	304
Push-Profile-Request	PPR	HSS	S-CSCF	305
Push-Profile-Answer	PPA	S-CSCF	HSS	305

Both the Cx and Dx interfaces are designed to standardize communication between SIP IMS Proxies and HSS.

UAR/UAA performs the following operations: Authorize the registration of the Public User Identity, checking multimedia subsystem access permissions and roaming agreements. Perform the first security check, determining whether the Public User Identity in the message is associated with the Private User Identity sent in the message. Obtain either the S-CSCF where the Public User Identity is registered or unregistered (i.e. registered as a consequence of a terminating call or there is a S-CSCF keeping the user profile stored), or the list of capabilities that the S-CSCF has to support.

SAR/SAA performs the following operations: Assign an S-CSCF to a Public Identity, or clear the name of the S-CSCF assigned to one or more Public Identities. Download from HSS the relevant user information for the S-CSCF. Backup and retrieve the S-CSCF Restoration Information in the HSS.

LIR/LIA performs the following operations: Obtain the name of the S-CSCF assigned to a Public Identity .Obtain the name of the AS hosting a PSI for direct routing.

RTR/RTA performs the following operation: Notify the server that the public identity is to be unregistered, allow S-CSCF to clean state.

PPR/PPA perform the following operations: Update user profile. Update charging information. Update SIP Digest information.

4 IMPLEMENTATION AND RESULTS

4.1 Developing Diameter Protocol Stack

by the author. Diameter stack consists of 9 API's: Init, Un Init, Start Connection, Start Session, Terminate Connection, Terminate Session, Send message ,Forward message, Reject message.

Functionalities of API's: Init validates the application data, initializes & configures the Diameter Core. Un Init uninitializes the Diameter Core. Start Connection creates a new connection. Start Session starts a new session for a valid connection Id passed by the application. Terminate Connection terminates an existing connection, along with all its sessions and transactions Terminate Session terminates a particular session, along with all its transactions. Send Message sends a newly created message in the form of packet out of network

through socket. Forward Message forwards the received message from one peer to other peer. Reject Message rejects a message.

Description of Working of API's: First Init is invoked and all the data structures are initiated. After confirming that initialization is successful then the connections are established using Start Connection. Once connections are established sessions are established using Start Session and finally messages can be send from one peer to other peer using Send Message or message can be forwarded by Forward Message or the message can be rejected by using Reject Message. After all the functionalities have been completed the session has to be terminated using Terminate Session and next all the connections that have been created is to be terminated using Terminate Connection. Finally all the memory allocations are freed using Un Init.

4.2 Testing Protocol Stack

We first tested the initial Diameter implementation.

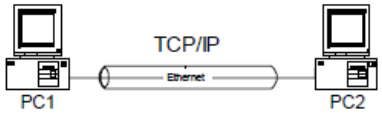

Fig. 4. Laboratory Setup

The laboratory setup shown in Figure 4.It consisted of two low-end PC-compatible computers, PC1 and PC2, attached to the local TCP/IP network via Ethernet interface. The PC1 served as the Diameter client and PC2 served as the Diameter server application.

We used wireshark network protocol analyzer to capture the Diameter messages exchanged between the client and server applications. Wireshark was installed on the both the client and the server. The purpose of the test was to establish the client and the server behaviour, and study the content of messages exchanged. We activated the packet capturing procedure within wireshark and then initialized the server and the client applications. Once both applications were properly started, we commenced the message exchange between them. Messages captured confirmed the correct operation on both the client and the server side.

4.3 Implementation.

A diameter structure contains several client/server examples, which are used to examine Diameter mechanisms. As a starting point in our development we used the example presenting an authorization application. In terms of specifications, we followed the specifications of the Diameter protocol [2][5] and Cx/Dx interface [3][4] provided by 3GPP.Our work included developing a diameter base protocol and adding the Cx/Dx interface specific Diameter messages – UAR, MAR, and SAR – and building the client and server applications. The client and the server code have rather similar structures, up to the point of Diameter session management.UAR, MAR, and SAR commands, which, according to the Cx specification, are sent from the client (CSCF) towards the server (HSS).

The distribution contains both the server and the client classes to enable a Cx node to operate in a peer-to-peer network. In our application, we implemented the functionality of the Cx interface as if the CSCF acted as a client and the HSS acted as a server. (This could have also been implemented the other way round to have both client/server, i.e. peer functionality on each side.) Figure 6 shows the exchange of messages in our implementation. It may be noted that each message transmission method (i.e. TxUAR) on the client side has its corresponding counterpart on the receiving, server side (i.e. RxUAR). The notation used here is Tx for transmission, and Rx for receiving. Messages are distinguished by their message code, embedded in the message header. The client composes a message with the specific code, and sends it to the server, which then recognizes the message code and initiates the appropriate receiving method.

Each message type carries some specific information, being coded as AVPs. Thus, it was necessary to implement the method for composing and resolving the message for all types of messages. This included definition of message parts, initialization of message fields. Finally, construction of message body.

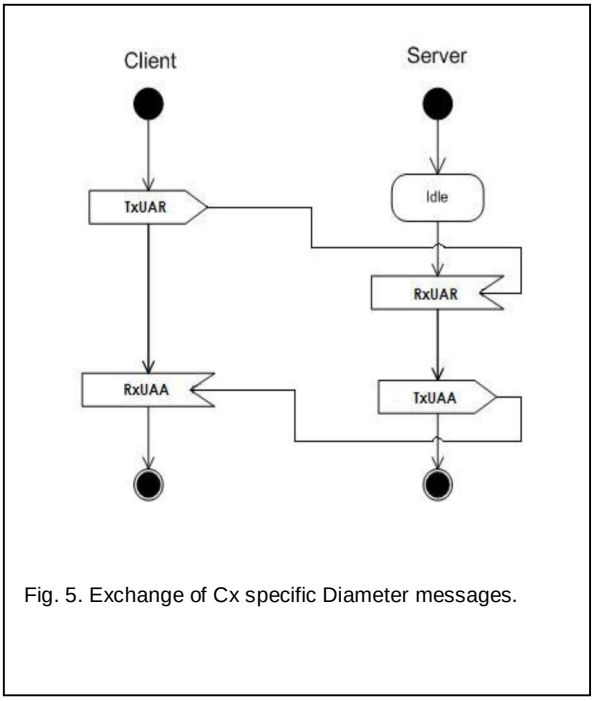

Fig. 5. Exchange of Cx specific Diameter messages.

5 Conclusion

With the emergence of new wireless access technologies and new applications envisioned in new generation networks, the need for AAA becomes more pressing. The AAA solution adopted by the 3GPP and 3GPP2 for use in the IMS is based on the Diameter protocol.

In this paper, we have studied the Diameter protocol and its application in the IMS Cx interface. We developed a Diameter protocol stack and we used it as a basis for implementing the AAA functionality that IMS needs, more specifically, the se-

lected Cx interface functions UAR, MAR, and SAR. The conformance of the implementation to the specification was verified by testing in a laboratory setup. Our further work includes implementation of the Diameter messages for the Cx interface.

REFERENCES

[1] G. Camarillo, M. A. García-Martín, *The 3G IP Multimedia Subsystem: Merging the Internet and the Cellular Worlds*, John Wiley and Sons, Ltd., England, UK, 2004.

[2] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, *Diameter Base Protocol*, IETF RFC 3588, September 2003.

[3] *IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signaling flows and message contents*, The 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; TS 29.228, 2005.

[4] *Cx and Dx interfaces based on the Diameter protocol; Protocol details,* The 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; TS 29.229, 2005.

[5] J. Loughney, Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5, IETF RFC 3589, September 2003.