A Communication Architecture Based on SCTP and SIP to Support Mobile Real-Time Multimedia Applications

[1]Daniel G. Costa, [2]Sergio Vianna Fialho

[1]Universidade Estadual de Feira de Santana – DTEC – Feira de Santana/BA
[2]Universidade Federal do Rio Grande do Norte – DCA – Natal/RN
[1]danielgcosta@ecomp.uefs.br [2]fialho@pop-rn.rnp.br

Abstract: New versions of SCTP protocol allow the implementation of handover procedures in the transport layer, as well as the supply of a partially reliable communication service. An end-to-end communication architecture is proposed herein, using SCTP with the session initiation protocol, SIP, besides additional protocols. This architecture is intended to handle real-time multimedia applications with mobility requirements. The Specification and Definition Language is used to specify the operation of a control module, which coordinates the operation of the system component protocols. This specification is intended to prevent ambiguities and inconsistencies in the definition of this module, assisting in the correct implementation of this architecture.

Keywords: real-time multimedia, internet mobility, end-to-end communication architecture.

(Received March 09, 2009 / Accepted July 04, 2009)

1. Introduction

Mobility in IP networks is demanding new tough solutions, due to the growing demand for improvement in communication applications and backbone structure. When time sensitive data makes part of this mobility demand, the resulting complexity encourages the specification of communication architectures adapted with these operation requirements. Mobile real-time multimedia applications are becoming common, due to the spreading of wireless network and new 3G/4G cellular technologies.

Stream Control Transmission Protocol (SCTP) [20] is an Internet transport protocol initially designed to allow telephone signaling over Internet backbones. In spite of that, SCTP can provide a series of services absent from traditional Internet transport protocols, as Transmission Control Protocol (TCP) [3]. One extension to this protocol takes advantage of native multihoming support on transport layer, not requiring any especial support from network devices, such as routers and switches, when the communication environment is formed by wireless and mobile networks. Another SCTP extension allows different data retransmission requirements within the same communication. Users of this communication service can specify what data must be retransmitted if some corruption or lack of information is detected, and what data must not.

Session Initiate Protocol (SIP) [16] is an Internet application layer protocol used to create, control and terminate real-time multimedia communications. Together with Session Description Protocol (SDP) [6] and Real Time Protocol (RTP) / Real Time Control Protocol (RTCP) [17], SIP presents itself as a complete and flexible public solution for real-time multimedia communication in Internet environments.

A communication architecture based on SIP signaling over SCTP can be proposed, aiming at mobile real-time multimedia applications on Internet backbones. Using only end-to-end protocols, this solution does not require any special support from backbone devices, as routers and switches. In this architecture, handover procedures are expected to be handled within transport layer by SCTP. The also necessary user localization service should be executed by SIP, with direct support from SIP Registrar servers. This end-to-end operation has a better performance than network layer based architectures [24] [15]. Typical communication environments for this architecture will be composed by hosts executing special software and application layer servers for specific functions. As no additional functionality must be added to routers, this architecture is potentially lighter and cheaper than other solutions based on network layer devices.

Previous works have already considered SIP over SCTP [8], handover procedures executed by SIP [23] and mobility on network layer supported by SCTP [11]. However, in [8] SCTP is used only to carry SIP messages, with no additional functionality expected from this protocol. In [23], mobility support is provided only by an application layer protocol, using no additional procedures than those already specified for SIP. The work presented in [11] regards just the use of SCTP in mobile communication scenarios supported by network layer protocols. On the other hand, the architecture presented herein put together SCTP and SIP to support mobile real-time multimedia applications, needing no special features from application proxies [23] or network layer devices [11]. Additionally, in this architecture, SCTP provides a transport communication service for SIP signaling and real-time data alike, in a different way of [8].

To avoid deadlocks and operations errors in the architecture, a control module is formally specified. This module coordinates the ordered operations of the different protocols that compose the architecture protocol stack. Doing so, one can attest that the architecture works properly as specified. Also, this formal specification can help in simulation and implementation of the architecture communication terminals. Internet protocols simulation tools used in academic scenarios do not support completely SCTP and its extensions. On the other hand, the recent SCTP extensions are not yet available in programming libraries. Formal specification can assist in future implementation of communication terminals of the architecture.

This paper is structured in the following way. Section 2 presents the concepts related with the main protocols that form the mobile real-time multimedia architecture. Section 3 describes the communication details of the solution presented by this paper. Section 4 brings the control module formal specification. At last, conclusions and references are presented.

2. Related protocols

SIP is an Internet protocol aimed at the control of real-time multimedia communications. One of the services provided by SIP and some other supporting protocol is user localization. Such service allows the IP address being currently used by a host to be known, even if that address recently changed due to user mobility through different networks. SIP Registrars servers keep track of user movements across networks: when a host acquires a new IP, it sends a SIP message to its home Registrar informing that new address. The current IP can be discovered by asking the proper record at that SIP server.

SCTP is a reliable transport protocol with typical transport layer services, but it introduces other features that are absent in the traditional TCP. One of them provides a selective retransmission procedure when corrupted data is received. In addition, multiple data streams create separate control of the data being transmitted, enhancing the protocol performance. The concept of a SCTP association, more complex than TCP connections, establishes multiple simplex streams with independent logical control of message oriented user data. Also, native multihoming support for SCTP association allows hosts to use more than one IP address to identify themselves in the communication links, since they have more than one connection point to the Internet. All these features put SCTP as a better solution for many communication environments traditionally associated with TCP.

Using SCTP flexibility due to its extensions, PR-SCTP (Partial Reliability - SCTP) [19] introduces a way to send data with distinct reliability requirements within the same association. User can dynamically specify what data must be retransmitted if some corruption occurs. With PR-SCTP, transport communication acquires other possibilities not present in TCP and User Datagram Protocol (UDP) [14], as, for example, an ordered but non-reliable transmission service.

ADDIP [22] is another SCTP extension which uses multihoming feature along with address reconfiguration procedures to supply handover support in transport layer. When a host gets a new IP address, resulting from user movement trough different networks, the current communication end point notices that new address upon the reception of especial messages described in ADDIP specification. Such address reconfiguration procedure does not result in any communication interruption or loss and does not need any additional support from Internet backbones. ADDIP extension, as other mobility solutions like Mobile IP [13], does not define user localization procedures. So, this extension can not be used alone to support mobile communication in the Internet.

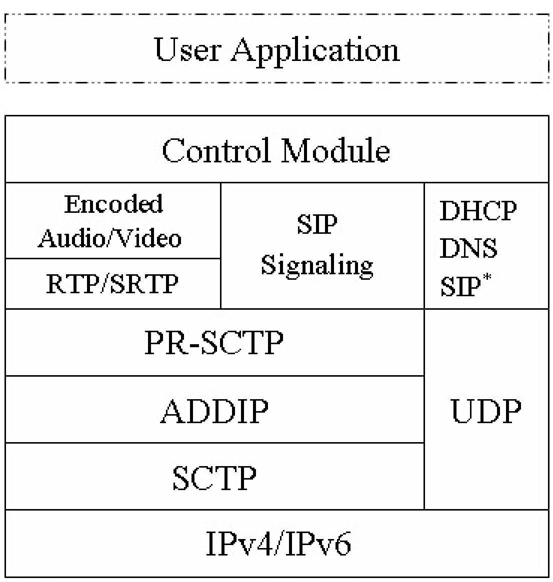
Using the best part of each of these protocols to support mobile real-time multimedia applications on

Internet, a communication architecture can be specified. The next section presents the functional specification of this architecture, followed by the formal specification of its control module.

3. Functional specification of the architecture

The communication architecture presented herein is intended to support mobile real-time multimedia applications, providing user localization and handover procedures. For such an end, services from SCTP, PR-SCTP, ADDIP and SIP are used, as well as some support protocols, as RTP and SDP. All of them are already defined for use in Internet backbones, so it is not expected any significant loss of performance or additional overhead when they work together. Moreover, the end-to-end nature of the architecture does not require any change on backbones, since all that is needed is the installation of software in each host that wish to communicate following this scheme.

Figure 1 presents the architecture protocol stack. The Control Module is a code specially designed to coordinate the ordered working of the protocols that compose the architecture. Such code also provides an interface between the service supplied by the architecture and the user application.



* SIP messages to Terminal ↔ Registrar communication

Figure 1: Protocol stack of proposed architecture.

In Figure 1, PR-SCTP, ADDIP and SCTP were presented separately in order to easy the perception of the individual functionality expected from these modules. In typical implementations of the architecture, however, all of these modules will be located in the Operating System as a Stream Control Transmission Protocol module with support of two extensions, since application layer protocols will require the transport service direct from SCTP.

For security reasons, multimedia data can be sent across the network using Secure RTP (SRTP) [2] support. This is not a requirement, but only an optional service with no direct impact on the architecture operation, though cryptographic algorithms can prejudice the overall latency and jitter of the communication procedures.

When a host changes the network to which it is attached, often due to a movement across different wireless networks, DHCP (Dynamic Host Configuration Protocol) [4] is used to indicate if such change requires a new IP address. This service can be provided by other protocols, with no harm to the architecture. It is also needed a special application layer protocol to support communication between architecture terminals and SIP Registrars. To locate the IP address of a Registrar server, DNS (Domain Name System) [9] can be used. In the same way as with DHCP, other similar service with the same functionality can be applied to the architecture.

As a last comment, SDP information, required for multimedia capability negotiation and the correct establishment of RTP streams, is carried within SIP signaling messages. In the architecture logical structure, the use of SDP is carried out by SIP.

Next subsections describe the architecture operation details associated with each functional part of this solution.

3.1. Terminal mobility

The architecture presented herein specifies the use of ADDIP dynamical reconfiguration procedures to support transport layer based terminal mobility. These reconfiguration procedures depend on three basic aspects. First, a host must discover if the network to which it was attached has changed. Second, if the new network is logically different from the previous one, the host has to acquire a new IP address from the backbone. At last, ADDIP handover procedures must be executed.

A mobile host (through a wireless link to the network), considering the power level of received signals broadcasted by access points [5], can identify a change in the network to which it is attached. This identification is managed by link layer procedures. If the logical network has not changed, there is no need to acquire a new IP address. So, in the same logical network, movements across different wireless cells do not require a new IP. However, if mobile hosts move to a different logical network, it has to get a new IP address, which indeed can be automatically received from some network service, as DHCP servers. To identify logical network changes, it is expected some support from an upper layer protocol, since link layer procedures do not handle IP addresses. As soon as the host realizes it is attached to a different logical network, it can start a procedure to get a new IP and subnet mask information. IP routing uses the subnet mask to decide if packets must be routed to a pre-defined path (default gateway) or if packets can be locally delivered. So, hosts in the Internet also need to know the address of the default gateway and DNS servers to send resolving queries. In order to maintain flexibility and high performance of the communications based on this architecture, DHCP is recommended to deliver IP address and other relevant information to mobile hosts.

If a mobile host is currently on communication with a remote host, when it receives a new IP address, it must immediately inform it. So, the host that has acquired the new IP address sends an ASCONF message to the communication endpoint, informing the new address. The correct reception of this message is confirmed by an ASCONF ACK message. This procedure uses the support from ADDIP extension, which provides transparent and seamless handover over IP networks. Such procedure has a better performance than other mobile architectures as MIPv6 (Mobile IP version 6) [7] and HIP (Host Identity Protocol) [10], as presented in previous works [24] [15].

Redirecting proxies specified for SIP are not used to support handover procedures in typical architecture communication scenarios. Terminal mobility is expected only from ADDIP extension support.

3.2. User localization

Communication among users in a mobile context may be of two kinds: a) the ones initiated from mobile hosts to non-mobile hosts, in wired or wireless networks, and b) the communications targeted to mobile hosts, no matter the origins. In the first case, there is no need of any user localization mechanism. All the mobile hosts must do is to use the handover support from ADDIP every time a new IP address is acquired. When the destination host is non-mobile, its address can be previously discovered using, for example, DNS. However, in the latter case, one should know the address being used in a specific moment by a host, tough such address can not be predicted or previously known.

ADDIP specification suggests the use of MIP (Mobile IP) home agents [13] to support user localization on mobile communication scenarios. This is a network layer solution based on redirection points that can add additional overhead and complexity to the overall communication. User localization service can also be obtained from application layer, as provided by Dynamic DNS [21]. Following a different approach, the architecture described herein uses SIP to control real-time multimedia communication and additionally support user localization. As SIP is already specified to form the core of the architecture, user localization executed by SIP prevents the using of additional protocols, as Dynamic DNS.

To manage user localization information, SIP uses Registrar servers to keep track of mobile hosts, while they move across different Internet networks. When mobile hosts register in home Registrars, these servers associate the currently used IP address with a globally unique SIP address (sip:user@domain). When a host acquires a new address from the network it moved into, this new information is registered in its home SIP Registrar.

To start a communication, a host has to know the SIP address of the destination point (for example, sip:daniel@uefs.br). The domain part of this SIP address represents the home Registrar of the destination end point. Using DNS, the IP address of that Registrar can be discovered. Then, the host should query the Registrar for the user part of the SIP address. This query returns the current IP address of the terminal being used by the user who has this SIP address. It does not matter where the terminal being used is actually placed, since the user is located by his/her SIP address.

The interaction with SIP Registrars depends on specific Resource Records of DNS domain tree. The association of the Registrar IP address with its domain name must be present in proper DNS server files, as for example “IN <IPv4 address> A <registrar domain name>” or “IN <IPv6 address> AAAA <registrar domain name>”.

All the communication between terminals and Registrars use special SIP messages already specified in [16].

3.3. Real-time multimedia communication

Using PR-SCTP, together with SCTP reliable transport service, real-time multimedia data and session control information can be transmitted at the same association. Multimedia data is to be sent as a non-reliable stream, since it is time sensitive, while control information flows constitute at a reliable stream. System resources associated with hosts and network overhead are potentially reduced by using one single SCTP association instead of many separate connections.

Time sensitive multimedia data in Internet are encapsulated by RTP packets [17]. Timestamp information present in RTP packet header is used in a communication endpoint for the decoding and reproduction of received media in communication endpoint. In the architecture, RTP is used for the same purpose, but not associated with UDP datagrams, as usual. Otherwise, RTP packets will be encapsulated by PR-SCTP.

As wireless links have a potential higher error rate than wired links, it is recommended the using of codecs with packet loss tolerance, as iLBC [1].

Optionally, encoded real-time multimedia can be sent in a cryptographic stream. When this option is chosen, SRTP must be used instead of RTP. Security management, comprising the keeping and distribution of cryptography keys, is out of the scope of the architecture. SCTP extensions for security can also be used.

4. Control Module specification

The architecture components consist of terminals and servers. Terminals are hosts that execute the control module software and the protocols forming the architecture protocol stack. Servers can be any of three types: SIP Registrar, DNS and DHCP. As the servers operate as specified by their standards, the new element to be considered is the terminal.

For the architecture specification, a control module is specially designed to coordinate the ordered operation of the involved Internet protocols. Also, this module provides an interface between the architecture operation procedures and the user application. The functionalities described in the previous section are indirect definitions of what the control module has to do.

In order to ensure the correct operation of the control module, the formal specification language SDL (Specification and Definition Language) and its extension SDL/GR (SDL Graphical Representation) [18] were used. Starting from the SDL specification, syntactic and semantic verification could be performed, attesting the specification is free of deadlocks and misunderstandings. The main parts of the final specification are presented in this paper, described in the next subsections.

4.1. Endpoint terminal

Every user who wants to communicate using the architecture service must access a terminal. Typically, the terminal will be deployed as software in a host or will make part of a special dedicated hardware following these standards. Terminals will comprise all protocols specified for the architecture, besides the control module. Additionally, it is expected hardware support for multimedia communication, in order to capture and reproduce audio and/or video.

The formal SDL specification was completed focused on the terminal. Figure 2 presents the SDL specification for the endpoint terminal.

The endpoint terminal is formed by many blocks: Control Module, SIP, RTP/SRTP, DHCP, DNS, UDP, PR-SCTP, ADDIP and SCTP. The communication between the blocks is identified by signals, as presented in Table 1. Most of these signals are messages from the constituent protocols.

Table 1. SDL signals of an Endpoint Terminal.

Signal	Channel	Description
ADDIP_Control	ADDIP ↔ SCTP	ADDIP control message (ASCONF or ASCONF ACK.)
Communication_Close	Control Module ↔ SIP	Request from the end point to close a current communication (SIP connection over a SCTP association).
Communication_Open	Control Module ↔ SIP	Request from the end point to open a new communication (SIP connection over a SCTP association).
DHCP_Message	DHCP ↔ UDP	DHCP message (to discover logical IP change and to provide new address), carried within UDP payload area. Message processed by DHCP servers.

DNS_Query	DNS ↔ UDP	DNS message carried on UDP payload area. Message treated by DNS servers.
IP_Changed	DHCP → Control Module DHCP → IP	Indication of change in IP logical network. DHCP module gives a new IP configuration to IP module.
IP_Packet	IP ↔ Network	IP packet transmitted through heterogeneous communication links.
Multimedia_Data	RTP/SRTP ↔ Control Module	Encoded audio or video (audio and video are transmitted in different RTP streams).
New_IP_For_Association	Control Module → ADDIP	A request to start handover procedures (sending of ASCONF and reception of ASCONF ACK).
PR-SCTP_Control	SCTP ↔ PR-SCTP	PR-SCTP control message (FWD-TSN).
PR-SCTP_Data	PR-SCTP ↔ SCTP	Conceptually, a SCTP_Data SDL signal. It is separated here for explanation purposes.
Remote_Home_Registrar_IP	DNS → Control Module	IP address returned after a DNS query for “registrar.domain”.
Remote_registrar.domain_query	Control Module → DNS	A DNS query for “registrar.domain”. As a result, the home registrar IP address of the destination end point will be returned.
Remote_Registrar _Query	Control Module → SIP	A query for the IP address associated with the user in his/her home registrar.
Remote_User_IP_Discovered	SIP → Control Module	The IP address of the destination host discovered by a query to his/her home registrar.
Renew_IP_Home_Registrar	Control Module → SIP	The new IP must be registered in home registrar.
RTP_Packet	RTP/SRTP ↔ PR-SCTP	RTP packet carried in SCTP DATA messages.
SCTP_Control	SCTP ↔ IP	SCTP control message (e.g. INIT, INIT ACK and SACK)
SIP_Message	PR-SCTP ↔ SIP	SIP message (e.g. INVITE, ACK, 200 OK, 180 RINGING and BYE) carried in SCTP DATA messages.
SIP_Registrar_Message	SIP ↔ UDP	A SIP message related with Registrar communication (management of an account in the home registrar).
Terminal_Status	Control Module ↔ User Application	General information about status of current and past communications.
UDP_Message	UDP ↔ IP	UDP message (typically, will carry DNS_query, DHCP_message and SIP_Registrar_Message)
User_Application_Control	Control Module ↔ User Application	Messages for User Application control of the terminal. Formed by service primitives.

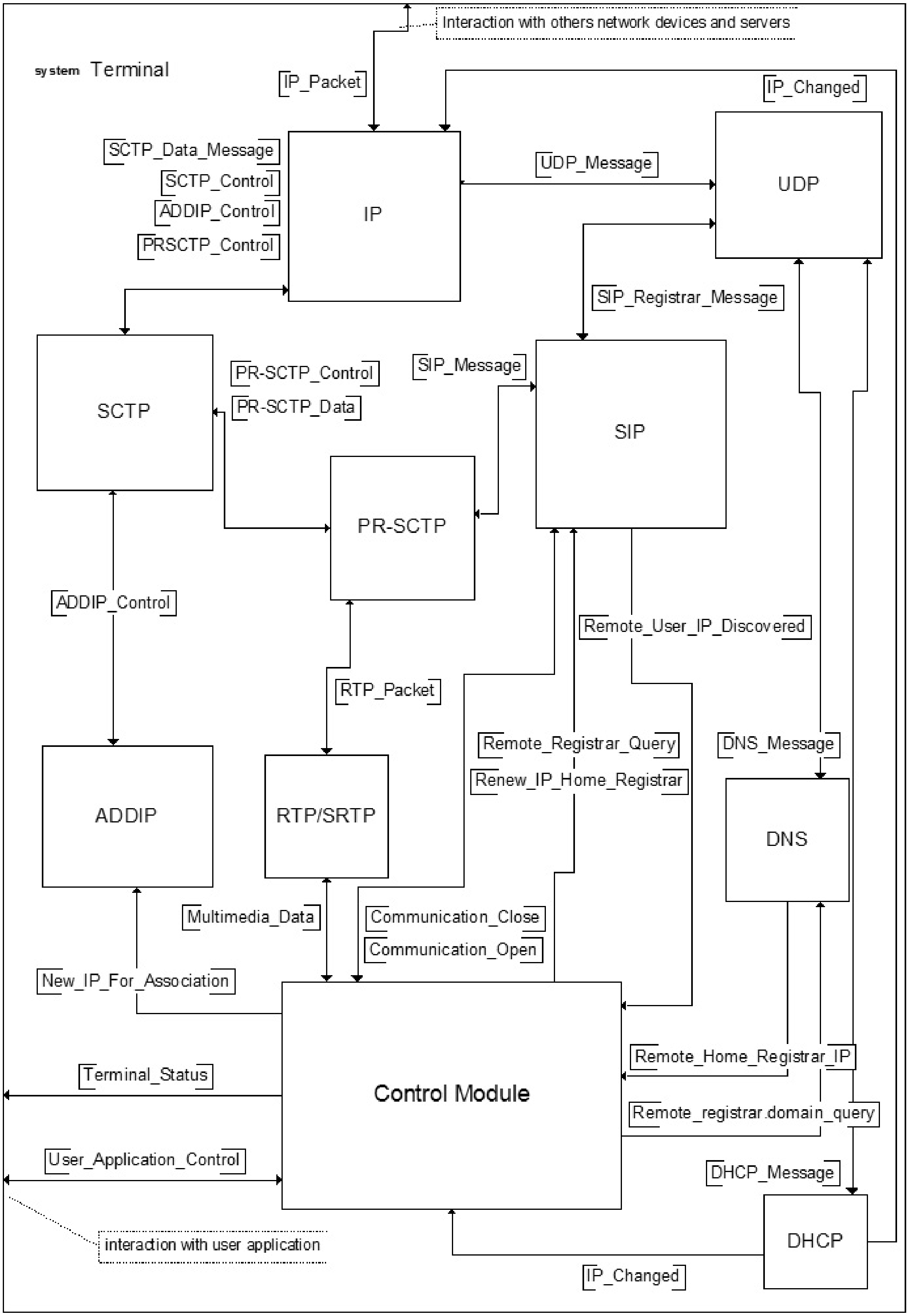


Figure 2: Terminal specification with its blocks.

4.2. Processes of Control Module

Control Module is specified as a SDL block with three processes: Call control, Mobility management and Real-time data communication. Each of these processes is related with the control of a specific part of the communication procedures specified for the architecture. Figure 3 presents the Control Module block with its three processes. Notice that the signals going in and out of the processes are described in Table 1. What is been done in the following is zooming in the Control Module structure. Next subsections focus on the operation details of each process.

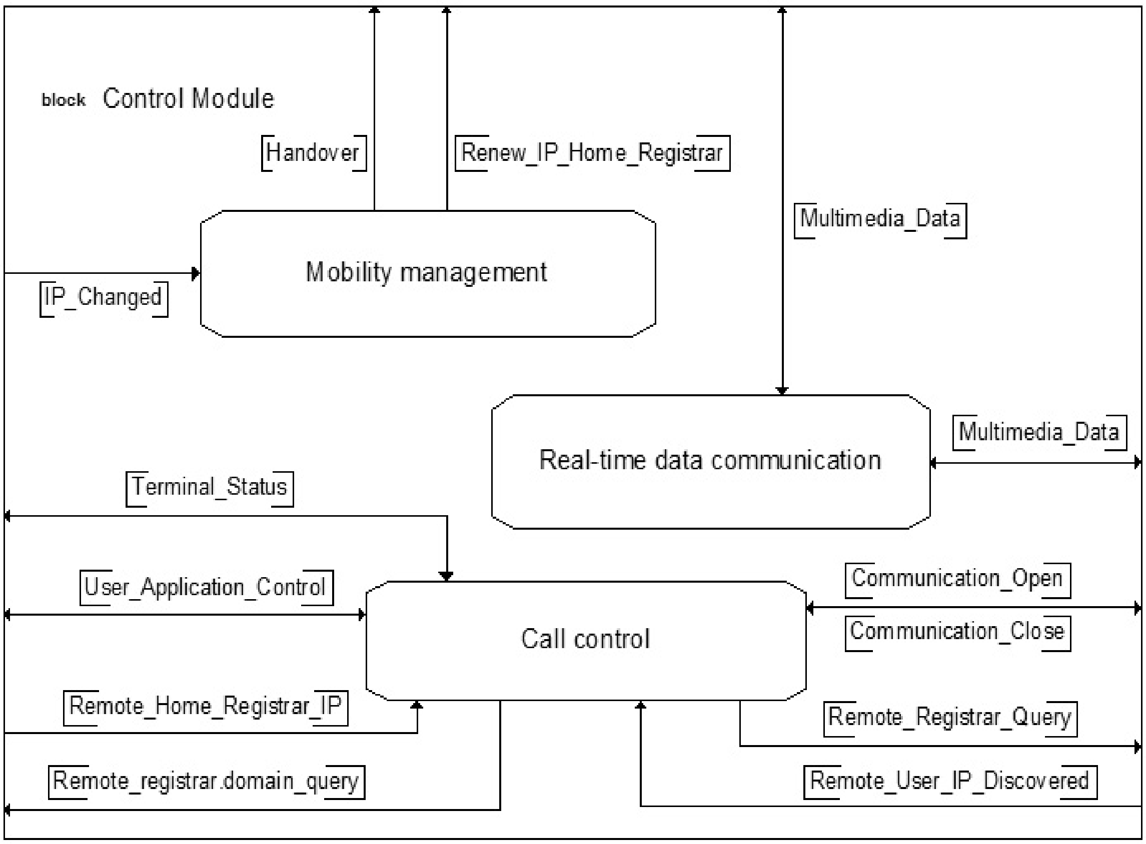


Figure 3: Processes of the Control Module block.

4.3. Service primitives

The architecture communication service is directly supplied by the Control Module. This module indicates service primitives that User Application must use to interact with the architecture protocols. These primitives are in the scope of the User_Application_Control signal, as previously presented. Table 2 points out these primitives.

It is important to say that the mobility management is completely transparent to the user. All a user application should worry about is to whom and what will be transmitted and received in a typical communication.

Table 2. Service primitives of the architecture.

Action	Service Primitive	Parameters
To open a connection	Communication_Open.request	Destination SIP address
	Communication_Open.indication	Source SIP address
	Communication_Open.response	The answer for a request to open a connection
	Communication_Open.confirm	Confirmation for a request to open a

		connection
To close a connection	Communication_Close.request	Destination SIP address
	Communication_Close.indication	Source SIP address
To send data	Data.request	Data (audio/video)
	Data.indication	Data (audio/video)
To verify host status	Status.request	Specific parameters
	Status.indication	Specific parameters

5. Conclusions

SIP is currently seen as the best public multimedia session control protocol for Internet, being used in almost all modern applications in this area. On the other hand, SCTP has many other advantages than only handover support, when compared with traditional Internet transport protocol. SCTP is still a recent protocol, but has the potential to become the standard transport protocol of TCP/IP (SCTP/IP) architecture. On the other side, SIP is currently the main solution for controlling multimedia sessions, especially for videoconference and VoIP applications. A communication architecture that employs both protocols has a potential advantage when compared with other solutions.

The last years have seen the increase of real-time multimedia applications in the Internet. As wireless networks are getting common, those applications tend to become mobile. Mobile VoIP, videoconferencing and web TV, for example, are applications that bring new possibilities to the Internet and its million of users. Supporting this specific but big and growing demand is a huge challenge that the architecture presented herein helps to solve.

SDL was used to specify the Control Module operation, and, additionally, the communication among the blocks that form the Endpoint Terminal. This specification, together with verification procedures adopted (syntactic and semantic check), attest the correctness of the architecture, since no operation error or deadlocks were found.

Although the actual efficiency of the architecture was not measured yet, due to implementation restrictions imposed by the still recent SCTP extensions, one can predict a better performance of this architecture over the traditional solutions adopted for Internet mobility, as MIP. Individual analysis of some specific communication scenarios provided by SCTP and SIP is a good evidence of this assumption. Moreover, its end-to-end nature and decentralized approach presents a huge advantage when compared to network layer based solutions.

This work is not completed finished. New specifications of the architecture will regard multipoint communication and optional charge procedures. Quality of Service, not present in this first specification, can be recommended for specific communication scenarios. These new functionalities must be considered by new versions of the architecture.

Recently, Peer-to-Peer Session Initiation Protocol Work Group [12] has begun to create a new standard that uses P2P paradigm as the basis for SIP operation. It intends to keep some very important information in a decentralized way, avoiding the use of specific servers, as SIP Registrars. Future specifications of the architecture will consider the use of P2PSIP as an alternative for user localization procedures based on SIP Registrars.

At last, the implementation of Endpoint Terminals is also envisaged in future works. New programming libraries, available for popular operating systems, will permit the development of communication terminals in SCTP enabled environments. Following the specification presented herein, these implementations will allow extensive testing of the architecture, finally attesting its already expected good performance.

References

[1] Andersen, S., Duric, A. and Astrom, H. RFC 3951. Internet Low Bit Rate Codec (iLBC). Available online: http://www.ietf.org/rfc/rfc3951.txt, 2004.

[2] Baugher, M., McGrew, D., Naslund, M., Carrara, E. and Norrman, K. RFC 3711. The Secure Real-Time Transport Protocol (SRTP). Available online: http://www.ietf.org/rfc/rfc3711.txt, 2004.

[3] DARPA. RFC 793. Transmission Control Protocol. Available online: http://www.ietf.org/rfc/rfc793.txt, 1981.

[4] Droms, R. RFC 2131. Dynamic Host Configuration Protocol. Available online: http://www.ietf.org/rfc/rfc2131.txt, 1997.

[5] Gast, M. S. 802.11 Wireless Networks: The Definitive Guide. 2nd ed. O´reilly. 632p, 2005.

[6] Handley, M. and Jacobson, V. RFC 2327: Session Description Protocol. Available online: http://www.ietf.org/rfc/rfc2327.txt, 1998.

[7] Johnson, D., Perkins, C. and Arkko, J. RFC 3775. Mobility Support in IPv6. Available online: http://www.ietf.org/rfc/rfc3775.txt, 2004.

[8] Marco, G., Vito, D., LONGO, M. and Loreto, S. SCTP as a transport for SIP: a case study, *Journal of Systemics, Cybernetics and Informatics*, Vol. 2, No. 3, 2006.

[9] Mockapetris, P. RFC 1034. Domain names - concepts and facilities. Available online: http://www.ietf.org/rfc/rfc1034.txt, 1987.

[10] Moskowitz, R. and Nikander, P. RFC 4423. Host Identity Protocol (HIP) Architecture. Available online: http://www.ietf.org/rfc/rfc4423.txt, 2006.

[11] Nooman, J., Perry, P. and Murphy, J. A study of SCTP services in a Mobile-IP network. *1st ACM Workshop on Wireless Multimedia Networking and Performance Modeling*. Montreal, Canada, 2005.

[12] P2PSIP. P2P SIP IETF Work Group. Available online: http://www.ietf.org/ html.charters/p2psip-charter.html, 2009.

[13] Perkins, C. RFC 3344. IP Mobility Support for IPv4. Available online: http://www.ietf.org/rfc/rfc3344.txt, 2002.

[14] Postel, J. RFC 768. User Datagram Protocol' Available online: http://www.ietf.org/rfc/ rfc768.txt, 1980.

[15] Ratola, M. Which Layer for Mobility? – Comparing Mobile IPv6, HIP and SCTP. *HUT T-110.551 Seminar on Internetworking*. Available online: www.tml.hut.fi/Studies/T-110.551/2004/papers/Ratola.pdf, 2004.

[16] Rosemberg, J. and Schulzrinne, R. RFC 3261. Session Initiation Protocol. Available online: http://www.ietf.org/rfc/rfc3261.txt, 2002.

[17] Schulzrinne, R. and Casner, S. RFC 3550. RTP: A Transport Protocol for Real-Time Applications. Available online: http://www.ietf.org/rfc/rfc3550.txt, 2003.

[18] SDL. SDL Forum Society. Available online: http://www.sdl-forum.org, 2009.

[19] Stewart, R. and Xie, Q. RFC 3758. Stream Control Transmission Protocol Partial Reliability Extension. Available online: http://www.ietf.org/rfc/rfc3758.txt, 2004.

[20] Stewart, R. and Xie, Q. RFC 4960. Stream Control Transmission Protocol. Available online: http://www.ietf.org/rfc/rfc4960.txt, 2007.

[21] Vixie, P., Thomson, S., Rekhter, Y. and Bound, J. RFC 2136. Dynamic Updates in the Domain Name System (DNS UPDATE). Available online: http://www.ietf.org/rfc/rfc2136.txt, 1997.

[22] Xie, Q. and Stewart, R. RFC 5061. Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration. Available online: http://www.ietf.org/rfc/rfc5061.txt, 2007.

[23] Wedlung, E. and Schulzrinne, H. Mobility Support Using SIP. *2nd IEEE International Conference on Wireless and Mobile Multimedia (WoWMoM 1999)*. Seatle, USA, 1999.

[24] Zeadally, S. and Siddiqui, F. An Empirical Analysis of Handoff Performance for SIP, Mobile IP, and SCTP Protocols, *Wireless Personal Communications Journal*, Vol. 43, Nª 2, 2007.