Distributed call admission control in SIP based multimedia communication

Sajjad Ali Mushtaq, Osman Salem, Christophe Lohr, Annie Gravey

Distributed Call Admission Control in SIP Based Multimedia Communication

Sajjad Ali Musthaq, Osman Salem, Christophe Lohr, Annie Gravey
Telecom Bretagne Department of Computer Science Brest, France
Email: {sajjad.musthaq, osman.salem, christophe.lohr, annie.gravey}@telecom-bretagne.eu

***Abstract*—The Session Initiation Protocol (SIP) is a text based signaling protocol, which has been adopted in Next Generation Network (NGN) for controlling multimedia communications. The present paper addresses issues related to Call Admission Control (CAC) for a private network (A competitive cluster where proposed architecture blends various devices/components from several partners; Call Server (CS) from one partner and Session Border Controller (SBC) from another in the platform) accessing the rest of the world through various links. The standard SIP messages are used to share and distribute required information between different devices in the network. In this architecture, an efficient CAC function should take account of many factors, including user profile, call type and the state of the available access links. We propose to distribute the CAC function between the CS and SBC; the CS handles issues related to user profile and the SBC handles issues related to resource availability. The collaboration between CS and SBC is made possible by using the *"SIP Priority header"* to share and exchange information during Call Setup. This mechanism helps in isolating the service, control and transfer planes from each other.**

***Keywords*—Distributed Call Admission Control, SIP Priority Header, QoS (Quality of Service), Competitive Cluster**

I. Introduction

The emergence of multimedia services in IP network makes Quality of Service (QoS) management an unavoidable task. Call Admission Control (CAC) is one of the important mechanisms to provision the required QoS. The role of CAC is to determine whether or not a new call can be admitted. A large number of algorithms have been proposed in the literature. Classification, evaluation and performance analysis of some of the proposed algorithms have been done comprehensively in [1]. An interesting scalable CAC algorithm has been presented in [2]. A new dimension of dynamic pricing with CAC has been added in [3]. Distributed intelligent CAC for wideband multi-service CDMA system has been introduced in [4]. Networks require an effective resource management to provide required QoS, not only at connection setup as it has been implemented in most of existing CAC mechanisms, but also during the lifetime of the connection. CAC is regarded as an adequate tool to accomplish the required task in an efficient way.

Service provider has to take care of QoS requirements of the ongoing flows, before accepting a new request that may degrade the performance of ongoing flows. Several CAC schemes have been proposed focussing on call and packet level performances [5], [6]. Conventional CAC schemes take into account the inbound traffic load, outbound traffic load, QoS of the links, user profile, thresholds defined to limit the number of voice/video calls and Central Processing Unit (CPU) load. Network topology and resource status are essential for CAC mechanism. Dynamic/real-time awareness of the network topology and resources is key to ensure policy based dynamic CAC. Admission control in the present paper involves checking authorization based on policy rules computed while taking into account user profiles, Service Level Agreements (SLA), operator specific policy rules, business objectives and service info. Proposed CAC mechanism is distributed into profile and resource based phenomenon, according to the functionality and location of the service management devices. In our architecture, the policy based CAC mechanism has been splitted and performed at distinct locations (Call Server (CS) and Session Border Controller (SBC)) taking into account already admitted flows. Certain information elements need to be shared and exchanged between CS and SBC to achieve the goal of CAC distribution. There is no such algorithm/scheme and protocol at hands to be adopted for information exchange and sharing while distributing the CAC. Moreover, the utilization of a new protocol may complicate the problem, and requires more computation with rise in call/connection setup time. One of the motivations is to accomplish the CAC distribution mechanism within the session signaling flow and/or its initiation.

The remainder of this paper is organized as follows: In section II, we describe the proposed architecture along with its brief layered comparison with IMS. Section III explains the call admission control and its distribution along with use cases for incoming and outgoing calls. In section IV, we discuss the advantages of proposed architecture, CAC distribution advantages and disadvantages and finally some concluding remarks have been given.

II. Proposed Architecture

SIP [7] (The main signalling protocol in the proposed architecture) is widely used in IP based communication and is adopted in TISPAN and Next Generation Network (NGN)/IP Multimedia Subsystem (IMS). SIP is an ASCII based application layer protocol used to set up and tear down voice, video and data sessions. It is an Internet-centric protocol that establishes, maintains, modifies and terminates sessions. Despite the Network Address Translation (NAT) and firewall traversal issues, SIP has been admitted as the promising candidate for NGN and is being incorporated in the current

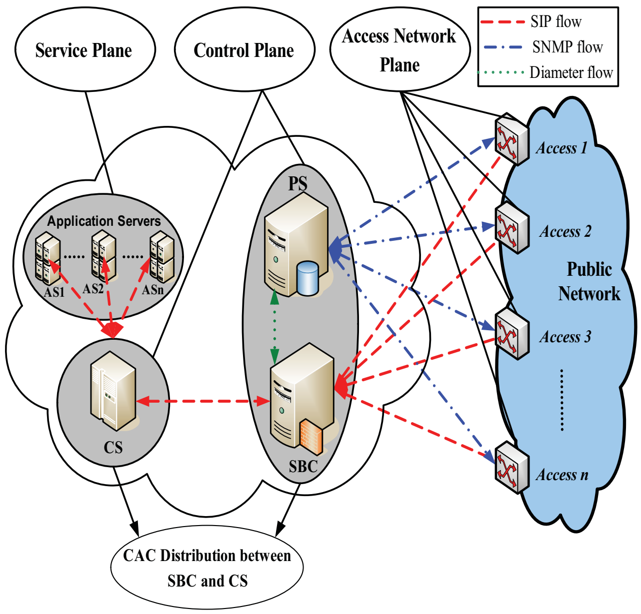

Fig. 1. Proposed Architecture.

and future multimedia services.

QoS-centered proposed architecture provides linkage between private network (Where companies offering versatile services are linked to the rest of the world via different accesses) and the public network (The Internet). Policy Based Network Management (PBNM) paradigm in the architecture envisaged an extended IETF framework [8]. This architecture (See figure 1) is proposed in the Companym@ges [9] project (A project that stems from Competitivity Cluster "Images and Network") which proposes a platform where companies are linked to the rest of the world via different network accesses offering data and multimedia services. The work presented in this paper relates to the sub-project for traffic management issues at the border of the company's network. Components of this platform are provided by partners: SIP Call Server (CS), Session Border Controller (SBC), and Policy Server (PS)) constituting the control plane in the proposed architecture (figure 1) are/will be developed by Alcatel-Lucent, Comverse and TELECOM Bretagne respectively. It is thus interesting to use the standardized SIP messages to distribute the CAC procedure. The proposed CAC mechanism has no impact on other priority header fields utilization/information.

Application Servers (AS); constituting the service plane and CS, SBC, PS; constituting the control plane are the main building blocks of the proposed architecture. CS is an important component of IP based PBX/Softswitch. It may also support proxy, registrar, redirect and location services. Most of the CS solutions are proprietary and support wide range of services. CS here provide registration, user profile management, service control and user profile CAC functionality.

SBC is another significant module of the proposed architecture. It is a session aware device. The primary functionality of the SBC is Network Address and Port Address Translations (NAT/PAT) and firewall traversal. The term SBC is not specific since its functionalities are not yet standardized or defined anywhere [10]. SBC provides a variety of functions to enable or enhance session based multimedia services (e.g. VoIP). The key functions of SBC are: Perimeter defence (access control, topology hiding, DOS prevention and detection), functionality not supported at the end points (protocol interwork, media repair) and network management (traffic monitoring, shaping and QoS). Some of these functions may also get integrated into other SIP elements like 3GPP P-CSCF, 3GPP I-CSCF etc. SBC can handle both signalling and media depending upon its functionality and deployment. In our case, we assume that SBC also embeds: a SIP/SDP (Session Description Protocol [11]) analyzer, a communicator function (used for policy and information exchange between PS and SBC), network QoS monitoring and policy enforcement module. It can also act as a Local Policy Decision Point (LPDP) to support provisioning mode policy enforcement. The modular inter-communication within the SBC and with other components of the platform is shown in figure 2.

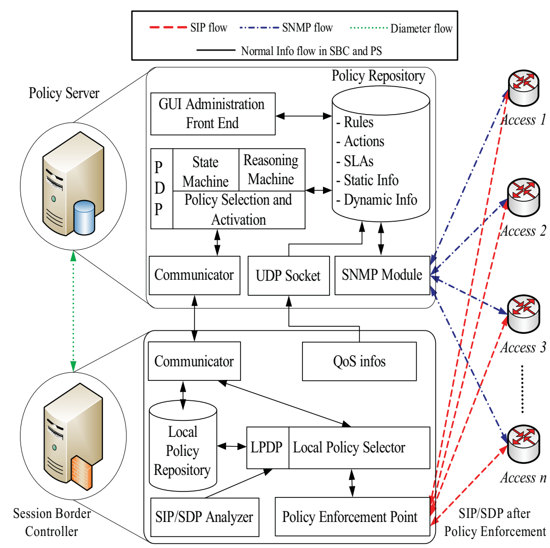

Fig. 2. PS and SBC modules and the modules inter-communication

PS is the core of our proposed architecture. An abstract modular diagram of PS is presented in figure 2. Policy based management system is emerging as the promising technology to address the challenging tasks in the converged NGN [12], [13]. IETF policy framework terminology and concepts has been adopted and extended to formulate an enhanced framework capable of taking into account high variability and dynamicity. policy framework keeping in view integrity and compatibility. Conventional policy based systems do not allow dynamic control, management and extensibility. Although some policy based systems have been proposed for managing telecommunication and enterprise network services [14], [15], but those systems were specifically designed for a certain set of services and environments with limited dynamicity. We have tried to provide a policy system which support converged network services with dynamicity emphasizing on access network optimization. PS is an intelligent and key player in our framework. It has to obey the Service Level Agreements (SLA) and reciprocal agreements. The business objectives of the enterprize must be fulfilled while the users and applications should get assured QoS. We have also addressed the access optimization by taking into account the information narrated along with routing rules and configurations entered by the administrator. In order to provide required QoS for multimedia services, the policy server provides a decision for every request by considering static information and dynamic information (e.g. time of day, context of the external links, Statistical analysis of QoS information or Call Details Records (CDRs), etc.).

The policy system supports multi-service and multi-vendor environment with high variability while isolating the service, control and access planes. The decoupling of three planes leads to distributed CAC functionality. The policy computation takes SLAs, business objectives, routing rules, services information, QoS of the accesses and profiles into account. The SNMP [16] flows presented in figure 1 are used by the policy server to gauge the QoS of the external links by performing statistical analysis on captured metrics(delay, packet loss etc). Further description of the PS and its behavior is outside the scope of the present document. The reader is refereed to [17] for detailed PS framework, functionality and behavior alongside the information required for dynamic policy control and management. In this paper, we have focussed on policy sensitive CAC issues, assuming that the PS provides decisions regarding call acceptance/rejection.

The profile and resource based CAC policies might be exemplified with some simple policies as follows

- If the user profile belongs to silver class and the requested communication type is video, then refuse the request immediately.
- Give priority to voice calls.
- Preempt the loaded link-A (marked with exceptional good QoS) for incoming call from some specific profile.
- Deny all video calls if occupied bandwidth is above predefined threshold.
- If the load is below a predefined threshold on an access then despite refusing the request, route sesion/call to consume the dedicated Best Effort bandwidth.
- While routing a session/call, look first for the best QoS link for a certain family of profiles then search/find the cheapest access.

A. IP Multimedia Subsystem (IMS) and the proposed architecture

An NGN is a packet based network able to provide telecommunication services and make use of multiple broadband, QoS enabled transport technologies. In NGN, service related functions are independent from underlying transport related technologies. IMS is a subsystem providing call processing and a variety of multimedia services over an IP based packet switching domain. IMS framework was originally designed for charging and mobility management in wireless environment. Later on it has evolved for wired networks along with new wireless standards(CDMA 2000). Telecoms & Intenet converged Services & Protocol for Advanced Network (TISPAN) is responsible for all aspects (Service, architectural, protocol, QoS, security, mobility within wireless and wireline aspects) of standardization for present and future converged networks including NGN. 3GPP IMS has been extended in the TISPAN NGN [18]. Despite fast-release pattern IMS/NGN is still evolving. Policy control function and Flow Based Charging (FBC) are combined to form Policy and Charging Control (PCC) function in IMS 7. Additionally merging of *Gq* and *Rx* as *Rx+* and integration of *Go* and *Gx* as *Gx+* are latest evolutions in the current IMS release 7 [19]. Due to aforementioned competitive nature of Companym@ges project, we need fine granularity at resource and profile level especially handling the private-public border traffic management issues along with external links optimization. IMS might not provide such fine tuned granularity at the private-public border. Adaptation effort may require lot of efforts and it might generate extra signalling traffic. Conventional SBC in IMS may offer packet classification and forwarding to a given link according to IntServ/DiffServ [20], [21] schemes. But we have introduced access prioritization and proposed an upper level(Session/Call level) classification framework. The focuss of present work is distributing the policy sensitive CAC mechanism irrespective of the components/devices from diverse vendors/partners. We therefore adopt high level layered approach for IMS and proposed architecture comparison as shown in figure 3.

Layer	IMS		Proposed Architecture		
	Interface/Servers	Protocol	Interface/Servers	Protocol	Functionality
Application	AS	SIP/Diameter	AS	SIP/Diameter	Policy based application, group, profile, presence and service management
Service	*PS*, SIP B2BUA, HSS	SIP/Diameter	SIP B2BUA, SIP UA	SIP/Diameter	
Session Control	P-CSCF, I-CSCF, S-CSCF	SIP/Diameter/ COPS	CS, SBC, Policy Server	SIP/Diameter	Policy based session control and management
Transport and Access	xDSL, WiFi, GSM	IPV4, PV6,SCTP, UDP, TCP	xDSL, WiFi, GSM	IPV4, PV6,SCTP, UDP, TCP	Policy based access and transport control and optimization

Legend

AS	Application Servers	HSS	Home Subscriber Server	P-CSCF	Proxy Call Session Control Function
PS	Presence Server	xDSL	A/S Digital Subscriber Line	I-CSCF	Interrogating Call Session control Function
WiFi	Wireless Fidelity	SIP B2BUA	SIP Back to Back User Agent	S-CSCF	Serving Call Session control Function
TCP	Transmission Control Protocol	SCTP	Stream Control Transport Protocol	COPS	Common Open Policy Service Protocol
UDP	User Datagram Protocol	IPV4/6	Intenet Protocol Version 4/6	GSM	Global System for Mobile Communication

Fig. 3. IMS and Proposed Architecture Layered Comparison

QoS oriented policy controlled framework emphasizing on SIP based multimedia communication is presented. The decoupling of service, control and access planes is one of the main features of the proposed architecture. This decoupling facilitates the distributed CAC mechanism despite interfaces/devices from diverse partners/vendors. A fundamental tenet is the policy control at each plane. Coordinated information sharing and retrieval among those planes ensures dynamic policy sensitive CAC distribution at different locations. This phenomenon stipulates reliable and efficient resource management and control.

III. Call Admission Control

A. Splitting the CAC procedure

Call Admission Control (CAC) is a mechanism used in networks to restrict access, in order to provide QoS for real

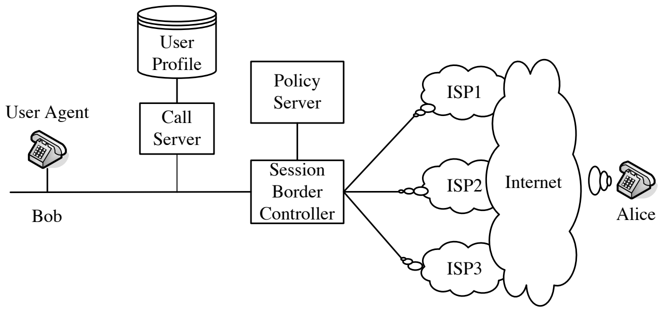

Fig. 4. Abstract Architecture.

time applications. CAC is used to limit the number of connections in the network and in some cases it works jointly with the bandwidth allocation and QoS routing [22]. It allocates available resources among the outgoing and the incoming connections, for maintaining the QoS performances of both types of connections at the required level. Network accepts or denies data flow on the basis of decision of CAC scheme. Decision (accept/deny) is based on predefined criterion which in turn depends on network environmental conditions in coordination with: rules, business objectives and administrative configurations of the platform. This decision has considerable influence on QoS parameters, which makes CAC an essential tool to guarantee various QoS parameters. Distributing the CAC mechanism on physical, data and network layer have been studied in [23]–[25]. Distributed connection admission control in wireless network has been addressed in [26].

PBNM and CAC are strongly correlated as they share the same framework and go hands in hands. In our architecture, we propose to distribute the policy sensitive CAC into user profile and resources availability. The SBC sitting at the edge, as an access point between private and public networks, can handle availability, cost and quality of the accesses, so resource based CAC should be performed at the network border. The CS on the other hand have the latest knowledge of registered users, services, profile related AAA (Authentication, Authorization and Accounting) information. Therefore, it seems quite obvious and suitable to perform profile based CAC at call server in the proposed architecture (shown in figure 1). Another dimension of splitting the CAC among SBC and CS is the distribution of intensive computational complexity.

In the architecture, we split the CAC into user and resource based admission control mechanism. In our framework, admission is performed at distinct locations (CS and SBC). CS in the global architecture of figure 1 embeds both the registrar and proxy functionality. SBC sitting at the border is behaving as a SIP proxy along with its functionalities described in section II. SBC is able to route the calls to different accesses according to the routing policies computed from the rules (Business Objectives, SLAs, Routing Rules etc) entered by the administrator of the platform through management console. Moreover, policy server also takes into account QoS parameters of access router interfaces (using SNMP), bandwidth, loss ratio, CDR (Call Details Records) details of previous call, etc while computing new set of policies.

B. Communication between CS and SBC

CAC in an enterprise is outside the scope of SIP at the moment except if an outbound proxy is used for outgoing calls, that proxy may control the firewall and thus restrict outgoing calls. The integration of QoS admission control with call signaling is presented in [27]. But it violates general Internet principles, which separate data transport from applications. Thus, the solution described in this Request for Comments (RFC) document is not applicable to the Internet at large.

In order to illustrate the basic problem, consider the following situation in which Bob's SIP User Agent (UA) is registered on the CS and it initiates a call to Alice by sending an INVITE to the proxy server at CS (figure 4). SIP proxy at CS can identify the profile (user type) of the call sent (received) to (from) a given UA, by querying the profile database. The SBC can identify the communication type (audio, video, etc.) by analyzing the SDP [11] payload of INVITE message. Therefore, the call server knows the profile type, while the SBC on the other hand, have the communication type information. In fact, the call server does not analyze the message payload and does not have any idea about the communication type while the SBC does not know the user type. Therefore, an information exchange and sharing is indispensable for policy base call routing at SBC.

One of the solution to this problem is that SBC accesses the profile database at CS and caches/mirrors the information within a duplicated database at SBC. This solution does not sounds efficient because the call server also accesses profile database frequently to filter incoming and outgoing calls. Hence the system has to access the profile base twice for each call, which is neither efficient nor elegant.

Our preference is the following: proxy server within the CS marks the INVITE with specific field that identifies the *user type*. '*Resource-Priority*' and '*Accept-Resource-Priority*' are defined according to the semantics in [28]. It is intended to describe a structure for fields inserted in the header of INVITE message. The fields are used to communicate a priority level for accessing the resources. The structure of the priority field used in our implementation is *name.number*. The name identifies the resource, and the number identifies the priority level. We could define a name (e.g. company) and different priority levels corresponding to the different user types (e.g. boss, administrator, trainee student, etc.). These header fields are used to transport the user priority which is taken into account when a policy decision must be taken. The '*Resource-Priority*' field will be used in INVITE messages while the '*Accept-Resource-Priority*' field will be used in 200 OK answers.

C. Handling incoming and outgoing calls

The user type is set up and stored into the users profile database at CS. The CS looks at the user profile database to accept or reject the call. If accepted, it add a proprietary SIP header to carry the user type info. The proprietary SIP header will be removed by the SBC once it got the user type.

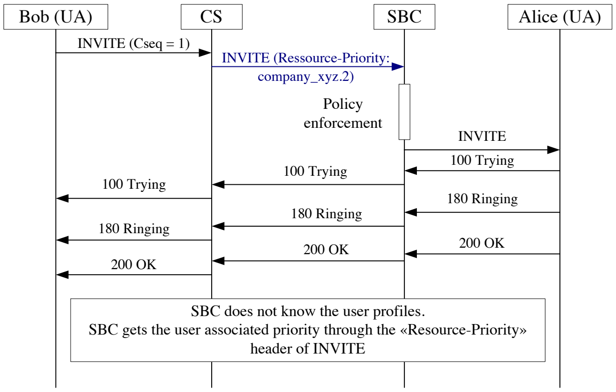

Fig. 5. Outgoing Call Flow.

A communication type is computed according to media & codec used by the user. Such information is described by the SDP message between user agents. The user type information is extracted from the *Resource-Priority* and *Accept-Resource-Priority* header fields, while the communication type is computed by the SIP/SDP analyzer at SBC (SDP offer/answer messages). This information is bundled into a pair and is compared with the switching table shown in table I (policy based QoS routing), computed from policy database.

Call Type	Access
(User Type-1,Communication Type-A)	1
(User Type-1,Communication Type-B)	3
(User Type-3,Communication Type-C)	2
(User Type-2,Communication Type-A)	1

TABLE I
SWITCHING TABLE FOR ROUTING

1) Outgoing Call: For outgoing calls (i.e. for INVITE sent from platform to outside), the '*Resource-Priority*' header must be added to the INVITE message as shown in table II. For an outgoing call, policy enforcement will be done on the INVITE response (200 OK). We should trigger on SDP offer/answer as shown in figure 5.

INVITE sip:bob@xyz.com SIP/2.0
Via: SIP/2.0/UDP 192.168.1.156:5060;branch=xxxx
Session-Expires: 86400
From: "Alice" <sip:alice@xyz.com:5060>;tag=xxxxx
To: <sip:bob@xyz.com:5060>;tag=xxxx
Call-Id: XXXXXxxxxx
CSeq: 1 INVITE
Resource-Priority: compagny_xyz.2
Contact: "Alice" <sip:Alice@xyz.com:5060>;tag=xxxx
Max-Forward: 70
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY, ...
User-Agent: useragent name
Content-Type: application/sdp
Content-Length: xxx

TABLE II
ADDITION OF *Resource-Priority* IN SIP INVITE FOR OUTGOING CALL.

2) Incoming Call: For incoming calls (INVITE from public to the private network), the *Accept-Resource-Priority* header must be added to the 200 OK message as shown in table III.

SIP/2.0 **200 OK**
Via: SIP/2.0/UDP 192.168.1.156:5060;branch=xxxx
Session-Expires: 86400
From: "Alice" <sip:Alice@xyz.com:5060>;tag=xxxx
To: <sip:bob@xyz.com:5060>;tag=xxxxx
Call-Id: XXXXXxxxx
CSeq: 1 INVITE
Accept-Resource-Priority: company_xyz.1
Contact: "Bob" <sip:bob@xyz.com:5060>;tag=xxxx
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY, ...
Content-Type: application/sdp
Content-Length: xxx

TABLE III
ADDITION OF *Accept-Resource-Priority* IN SIP INVITE FOR INCOMING CALL.

Policy enforcement in case of incoming call is applied in 200 OK response, as shown in figure 6.

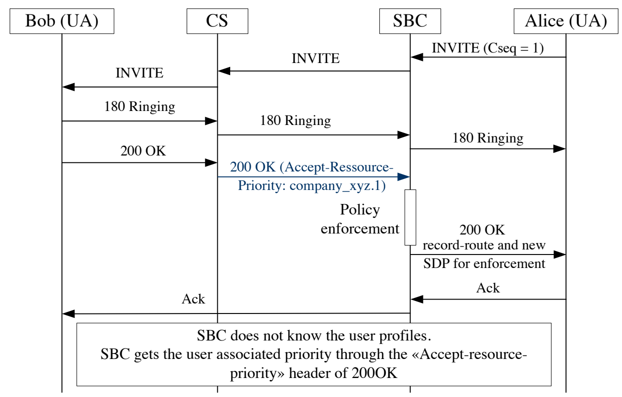

Fig. 6. Incoming Call Flow.

The proposed system's architectural, functional and specification design phase has been completed and at present it is in the initial development phase.

IV. CONCLUSION

We have proposed a novel QoS-centered architecture in multiservice packet network for PBNM addressing the SIP based communication while emphasizing on admission control and resource management. Twin drivers of the CAC distribution mechanism (CS and SBC) share and exchange information using standardized SIP messages. Due the competitivity nature of the proposed architecture we compared it with IMS on layered basis. Our proposed architecture combines the granularity of Integrated Services (IntServ) and the scalability of Differentiated Services (DiffServ) with additional functions (e.g. Distributed CAC, layer 5 call routing, addition of profile groups, etc.). Policy based management within the enterprise is being done on per call basis (IntServ), the packets on the other hand are handled on the accesses on per class basis (DiffServ). The service, control and network planes (figure 1) has been decoupled, except some control and transfer plane functions overlap. This decoupling leads to the distribution of complex CAC functionality between CS and PS. Addition of new services without hardware/software upgrade and interruption, automatic discovery of access network failure (topology change) and policy based control at service, user and network level are the key advantages. CAC has been distributed and handled inside the session initiation and/or signaling. Policy enforcement becomes flexible and scalable and its complexity is reduced. The SIP header fields added inside the enterprise during CAC operation are removed by the SBC (from 200 OK response) at the edge before forwarding the message to the public domain so that this information might not be exploited in the routers inside the public network.

The advantage of the proposed architecture is three fold. First, the service, control and network planes are kept isolated. Second, the change in topology likely due to an external link failure, recovery of a broken link, addition of a new link will be sensed and accommodated without interruption. Finally the policy based CAC has been distributed between the edge device (SBC) and the SIP CS. Computation intensive policy based CAC mechanism here is implemented in a distributed fashion splitting it into profile and resource based CAC. This is not a standardized methodology to achieve the goal but it is an efficient way of doing the job from our view point. Division of complex and resource (CPU, Memory etc) hungry functionality, reduction of policy enforcement complexity, isolation of service, control and network planes, affinity between the calls and external links, affinity between the calls and user profile are the key advantages of CAC distribution. Call processing twice at two distinct locations(CS and SBC) may be regarded as a disadvantage. The call setup time as a result may rise. Two additional fields (*Resource-Priority* and *Accept-Resource-Priority*) have been introduced in SIP header, for sharing and exchanging information for distributed CAC phenomenon.

ACKNOWLEDGMENTS

This work has been partially funded by the DGE (Direction Générale des Entreprises/Ministère des Finances et de l'Industrie) through the Companym@ges project. The authors would like to give many thanks to Antoine Gatineau from Comverse and to Yves Blanchard from Alcatel Lucent for their support and guidance.

REFERENCES

[1] E. Knightly and N. Shroff, "Admission control for statistical qos: theory and practice," *IEEE Network*, vol. 13, no. 2, pp. 20–29, 1999.

[2] Z. Ali, W. Sheikh, E. K. P. Chong, and A. Ghafoor, "A scalable call admission control algorithm," *Networking, IEEE/ACM Transactions*, vol. 16, no. 2, April 2008.

[3] M. Manaffar, H. Bakhshi, and M. Pilevari, "A new dynamic pricing scheme with call admission control to reduce network congestion," in *Peoceedings of 22nd International Conference on Advanced Information Networking and Applications (AINAW'08)*, 2008, pp. 347–352.

[4] D. Zhang and G. Zhu, "Distributed intelligent call admission control," *Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, 2005. MAPE 2005. IEEE International Symposium on*, vol. 2, pp. 1439–1443 Vol. 2, 8-12 Aug. 2005.

[5] H. Nan, S. Xing-hua, H. Zhi-qiang, N. Kai, W. Xiao-xiang, and W. Wei-ling, "Admission control algorithm for real-time services in packet-switched ofdm wireless networks - norm," *Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th*, pp. 1111–1115, 22-25 April 2007.

[6] X. Yang and G. Feng, "Optimizing admission control for multiservice wireless networks with bandwidth asymmetry between uplink and downlink," *Vehicular Technology, IEEE Transactions on*, vol. 56, no. 2, pp. 907–917, March 2007.

[7] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initiation Protocol," RFC 3261, Jun. 2002.

[8] A. Westerinen, J. Schnizlein, J. Strassner, M. Scherling, B. Quinn, S. Herzog, A. Huynh, M. Carlson, J. Perry, and S. Waldbusser, "Terminology for Policy-Based Management," RFC 3198, Nov. 2001.

[9] "https://www.companymages.eu."

[10] J. Hautakorpi, G. Camarillo, R. Penfield, A. Hawrylyshen, and M. Bhatia, "Requirements from SIP (Session Initiation Protocol) Session Border Control Deployments," IETF draft - work in progress (draft-ietf-sipping-sbc-funcs-05), Mar. 2008.

[11] M. Handley, V. Jacobson, and C. Perkins, "SDP: Session Description Protocol," RFC 4566, 2006.

[12] S. J. Shepard, "Policy-based networks: hype and hope," *IT Professional*, vol. 2, no. 1, pp. 12–16, Jan-Feb 2000.

[13] P. Flegkas, P. Trimintzios, G. Pavlou, I. Adrikopoulos, and C. F. Calvacanti, "On policy-based extensible hierarchical network management in QoS-enabled IP networks," in *Proceedings of the International Workshop on Policies for Distributed Systems and Networks (POLICY 01)*. London, UK: Springer-Verlag, 2001, pp. 230–246.

[14] L. Lymberopoulos, E. Lupu, and M. Sloman, "An adaptive policy based management framework for differentiated services networks," in *Proceedings of the Third International Workshop on Policies for Distributed Systems and Networks*, 2002, pp. 147–158.

[15] D. Verma, M. Beigi, and R. Jennings, "Policy Based SLA Management in Enterprise Networks," *Lecture Notes in Computer Science*, vol. 1995, pp. 137–152, 2001.

[16] D. Harrington, R. Presuhn, and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks," RFC 3411, Dec. 2002.

[17] S. A. Mushtaq, O. Salem, C. Lohr, and A. Gravey, "Policy-based QoS Management for Multimedia Communication," in *14th EUNICE Open European Conference on "Which networks for which services" (EUNICE, 08. IFIP)*, 8-10 Sept. 2008, pp. 78–85.

[18] N. Tispa, "ES 282 007 IP Multimedia Subsystem (IMS); Functional architecture NGN IMS Architecture," 2006.

[19] "3GPP TS 32.260 v7.3.0, IP Multimedia Subsystem (IMS) Charging R7," 2007.

[20] J. Wroclawski, "The Use of RSVP with IETF Integrated Services," RFC 2210, Sep. 1997.

[21] K. Nichols, S. Blake, F. Baker, and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," RFC 2474, Dec. 1998.

[22] T. Ezaki, H. Kawakami, and K. Asatani, "A new voip call admission control scheme with use of alternate routing for low call loss probability," *Communications, 2004 IEEE International Conference on*, vol. 4, pp. 2209–2213 Vol.4, 20-24 June 2004.

[23] H. Nan, W. Xiaoxiang, and W. Weiling, "Integrated Cross-Layer Design of Utility-Based Connection Admission Control in Packet-switched OFDM Wireless Networks," in *International Workshop on Cross Layer Design, (IWCLD '07).*, 2007, pp. 152–156.

[24] J. Chen and C.-W. Chang, "Traffic-Variation-Aware Connection Admission Control Mechanism for Polling Services in IEEE 802.16 Systems," in *International Conference on Wireless and Optical Communications Networks, (WOCN '07. IFIP)*, July 2007, pp. 1–5.

[25] D. Oulai, S.Chamberland, and S. Pierre, "End-to-End Packet Loss Constrained Routing and Admission Control for MPLS Networks," in *Canadian Conference on Electrical and Computer Engineering(CCECE 2007)*, April 2007, pp. 341–344.

[26] A. Safwat, "Distributed Connection Admission Control and Dynamic Channel Allocation in Ad hoc-Cellular Networks," in *International Conference on Digital Telecommunications (ICDT'06)*, 2006, pp. 52–52.

[27] E. W. Marshall, "Private Session Initiation Protocol (SIP) Extensions for Media Authorization," RFC 3313, 2003.

[28] H. Schulzrinne and J. Polk, "Communications Resource Priority for the Session Initiation Protocol (SIP)," RFC 4412, 2006.