Policy Models for Resource Management

Evelina Pencheva[1] Ivaylo Atanasov[2] and Dora Marinska[3]

Abstract – **In this paper an approach to modeling of policies for resource management is presented. Policy information models are structured according the quality of service mechanisms in Internet Protocol based multimedia networks. The usage of Open Service Access Policy Management interfaces is exemplified to illustrate the way policy information can be managed by 3rd party service providers. Formal description of policy rules is presented.**

Keywords – **IP Multimedia subsystem, quality of service, policy management, open access.**

I. Introduction

Internet Protocol Multimedia Subsystem (IMS) is standardized service control architecture that provides access-independence and IP connectivity. IMS is built on concepts that offer basic and advanced multimedia services to end-users using common Internet-based protocols. The underlying access and transport networks together with the IMS provide end-to-end Quality of Service (QoS). Via the IMS, the user equipment negotiates its capabilities and expresses its QoS requirements during a Session Initiation Protocol (SIP) session setup or session modification procedure. IP policy control means the capability to authorize and control the usage of multimedia traffic based on the signaling parameters at the IMS session [1]. It provides a way to allocate access and transport network resources, primarily network bandwidth, QoS, and security, according to defined business policies. This requires interaction between the IP connectivity access network and the IMS.

Policy is an ordered combination of policy rules that define how to administer, manage, and control access to resources. Policy defines the access to network resources, the traffic priorities, required bandwidth that has to be allocated to ensure guaranteed delivery and the eligible traffic for discard when the network becomes busy and congested.

Policy-based management systems are usually implemented for enterprise networks [2]. Network administrators apply application- and user-based centralized policy control to optimize resource allocation. Resources include devices that manage network bandwidth, security, IP addresses, storage, processors, and agents, as well as systems that manage services such as billing, accounting, and service mapping, and automated reliable policy deployment. The policy is operator specific and depends on network infrastructure and services provisioned [3].

The IMS standards just define a framework for policy control and do not specify in details the structure of QoS management policy. In this paper we suggest an approach to policy modeling in IMS environment. First we describe the IMS policy control architecture and then we model the structure of policy information for resource management using the QoS mechanisms. We exemplify the application of the Policy management service defined for Open Service Access (OSA) to illustrate the way in which policy information can be managed by 3rd party service providers.

II. IMS Policy Control Architecture

To deliver service performance that determines the degree of user satisfaction of the service, an architectural framework for QoS support is defined [4]. The QoS architectural framework is a set of generic network mechanisms for controlling the network service response to a service request, which can be specific to a network element, or for signalling between network elements, or for controlling and administering traffic across a network.

In IMS the Policy and Charging Enforcement Function (PCEF) encompasses service data flow detection, QoS handling, policy enforcement and flow based charging functionalities. This PCEF is located at the media gateway at the IMS User plane. The Policy and Charging Rule Function (PCRF) includes policy control decision and flow based charging control functionalities. It is responsible for finding routes in the network that meet QoS requirements and is located at the IMS Control plane. The PCRF provides network control regarding the service data flow detection, gating, quality of service and flow based charging (except credit management) towards the PCEF [5], [6].

Service requirements are signalled at the Control plane during session establishment and reflected on the underlying IP access and transport networks. Without interaction between User plane and Control plane the operator will not be able to provide the required QoS. The gateway containing PCEF is capable of policing packet flow into the IP network, and restricting the set of IP destinations that may be reached according to a packet classifier. This service-based policy "gate" function has an external control interface that allows the gate to be selectively "opened" or "closed" on the basis of IP destination address and port. When open, the gate allows packets to pass through (to the destination specified in the classifier) and when closed, no packets are allowed to pass through.

[1] Evelina Pencheva is with the Faculty of Telecommunications at Technical University of Sofia, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria, E-mail: enp@tu-sofia.bg.

[2] Ivaylo Atanasov is with the Faculty of Telecommunications at Technical University of Sofia, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria, E-mail: iia@tu-sofia.bg.

[3] Dora Marinska is with Global Communications Nets, 46 St. Kiril i Metodi, 1202 Sofia, Bulgaria E-mail: dmarinska@gcn.bg

In IMS, value-added services are delivered by Application Servers (AS). The OSA Service Capability Server (SCS) is a special type of AS which provides open interfaces to network functions (like call and session control, messaging, user interaction, location etc.) for 3rd party applications. The OSA Application Programming Interfaces (APIs) hide underlying network technology and protocol complexity from application developers. The OSA AS hosts third party applications that use network functions exposed through OSA APIs.

OSA Policy Management APIs have been defined to offer provisioning services [7]. Using the APIs it is possible to create, update or view policy information for any policy enabled service. The APIs facilitate interactions between clients and the policies of any policy enabled service. These include APIs to subscribe to policy events, to request evaluation of policies and to request the generation of policy events. Policy Management clients include both 3rd party applications and network service administration. It is expected that more and more OSA services will use policies to express operational criteria. It is also expected that network providers will host policy-enabled services that have been written by 3rd party application service providers. The network operator can populate the repository with the policy-related conditions and actions that it can support. The PCRF, PCEF and Policy repository form network policy engine as shown in Fig.1.

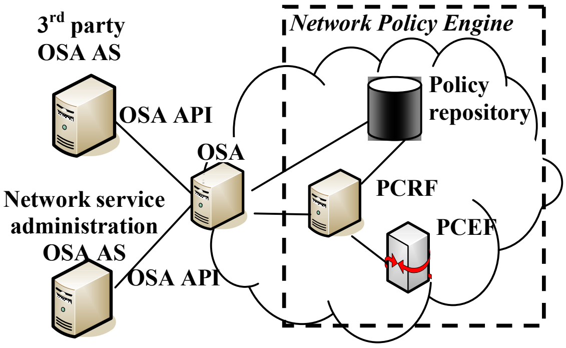

Fig.1 Deployment of OSA Policy Management APIs in IMS environment

III. Resource Management Policy Information Model

Policy domain allows aggregation of policy domains, policy groups, policy rules, or policy event definitions in a single container. Policy group aggregates policy rules or other policy groups. Policy rule is a combination of conditions and actions to be performed if the condition is evaluated as true. The repository is meant to hold unattached conditions and actions.

Considering control functions for IP policy control, we suggest the model the policy domain for Resource management composed of Charging Control Policy domain and Quality of service Provisioning Policy domains as shown in Fig.2. The Quality of Service Provisioning Policy domain includes QoS control domain, QoS data domain and QoS management domain. QoS Control Policy domain defines policy groups that deal with the pathways through which user traffic travels. These policy groups include admission control, QoS routing, and resource reservation. QoS Data Policy domain defines policy groups that deal with the user traffic directly. These policy groups include buffer management, congestion avoidance, packet marking, queuing and scheduling, traffic classification, traffic policing and traffic shaping. QoS Management Policy domain defines policy groups that deal with the operation, administration and management aspects of the network. These policy groups include SLA, traffic restoration, metering and recording.

The admission control policy rules control the traffic to be admitted into the network. Whether traffic is admitted depends on an a priori service level agreement. In addition, the decision can depend on if adequate network resources are available so that newly admitted traffic does not overload the network and degrade service to ongoing traffic. For a service provider, maximal traffic must be admitted while the same level of QoS is maintained for the existing traffic. The admission policy rules are typically parameter or measurement-based. The parameter-based approach derives the worst-case bounds for a set of metrics (e.g., packet loss, delay and jitter) from traffic parameters and is appropriate for providing QoS for real-time services. In contrast, the measurement-based approach uses measurements of existing traffic for making an admission decision. It does not warrant throughput or hard bounds on packet loss, delay or jitter and is appropriate for providing QoS for non real-time services. Admission control can also be used to meet requirements for service reliability/availability over a specified period for the desired transaction types as negotiated in the SLA. Admission control policies give preference to traffic streams (e.g., for emergency communications) deemed to be more critical by a service provider under conditions of congestion [8].

When a QoS resource is modified by the user equipment, such that the requested QoS falls outside of the limits which were authorized, then the PCEF needs to verify the authorization of this QoS resource modification. If the PCEF does not have sufficient information to authorize the QoS resource modification request, the PCEF sends an authorization request to the PCRF. The PCRF authorizes the modified QoS resources based on the current session information.

The resource reservation rules are used to set aside required network resources on demand for delivering desired network performance. Whether a reservation request is granted is closely tied to admission control. In IMS resource reservation is always initiated by the user equipment after successful authorization. The user equipment includes in the resource reservation request the authentication token granted. With request for QoS resource reservation, the PCEF in the gateway needs to assure that the requested resources match to the authorized resources. The PCEF forwards the token, together with the requested QoS parameters, to the PCRF. The PCRF checks if the corresponding requested QoS resources are within the limit of what was negotiated. The PCRF uses the token as the key to find the stored negotiated session description.

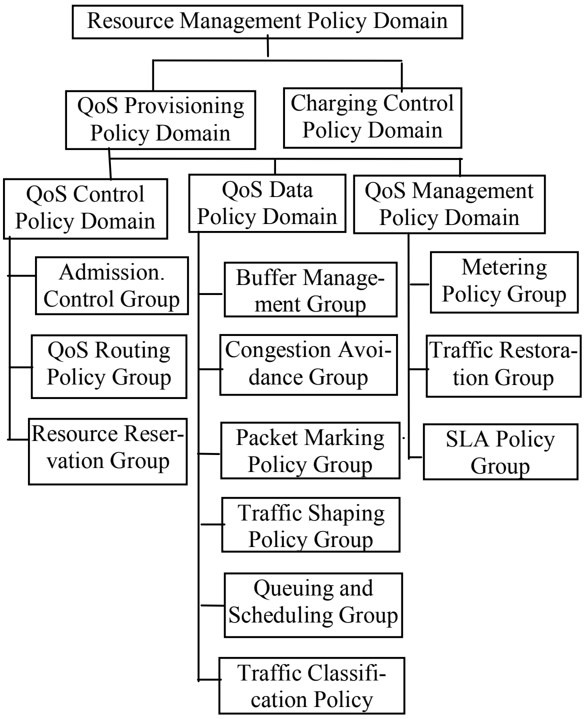
Resource Management Policy Domain
QoS Provisioning Policy Domain
Charging Control Policy Domain
QoS Control Policy Domain
QoS Data Policy Domain
QoS Management Policy Domain
Admission. Control Group
QoS Routing Policy Group
Resource Reservation Group
Buffer Management Group
Congestion Avoidance Group
Packet Marking Policy Group
Traffic Shaping Policy Group
Queuing and Scheduling Group
Traffic Classification Policy
Metering Policy Group
Traffic Restoration Group
SLA Policy Group

Fig.2 Resource management policy model

QoS routing policy rules concern the selection of a path satisfying the QoS requirements of a flow. Practical QoS routing schemes consider mainly cases for a single QoS metric (e.g., bandwidth or delay) or for dual QoS metrics (e.g., cost-delay, cost-bandwidth, and bandwidth-delay). The path selection process involves evaluation of policy rules having knowledge of the flow's QoS requirements and characteristics and information on the availability of network resources. To guarantee performance on a selected path, QoS routing needs to be used in conjunction with resource reservation to reserve necessary network resources along the path.

Queue or buffer management policy rules deal with which packets, awaiting transmission, to store or drop.

Congestion avoidance policy rules deal with means for keeping the load of the network under its capacity such that it can operate at an acceptable performance level, not experiencing congestion collapse.

Queuing and scheduling policy rule control which packets to select for transmission on an outgoing link. Incoming traffic is held in a queuing system, which is made of, typically, multiple queues and scheduler. Rules governing the queuing system determine the queuing and scheduling discipline it employs.

Packets can be marked according to the specific service classes that they will receive in the network on a per-packet basis. The policy rules for packet marking need to be provisioned or configured dynamically.

Traffic classification can be done at the flow or packet level. At the edge of the network, the policy rules determines the aggregate to which the packet belongs and the respective service level agreement.

Traffic policing rules deal with the determination of whether the traffic being presented is on a hop-by-hop basis compliant with pre-negotiated policies or contracts.

Traffic shaping rules deal with controlling the rate and volume of traffic entering the network.

A Service Level Agreement (SLA) typically represents the agreement between a customer and a provider of a service that specifies the level of availability, serviceability, performance, operation or other attributes of the service. Basic composition of the SLA content, regardless of the services provided includes the business part, service part, technology part and QoS report part [9]. The business part describes the general business information and business procedures related to the service. Policy rules may describe service violation processing and billing information. The SLA information stored in the service part related to negotiated service content and the agreed service level and SLA information in the technological part related to QoS parameters can be used in admission control rules as described above. The QoS report part includes the QoS report information provided to the service customer and the service provider in order to evaluate service level negotiated in the SLA. This information may be used to define policy events concerning QoS monitoring and reporting.

IV. OSA Policy Management Interfaces in Use

The OSA "Policy Management" interfaces allow policies to be provisioned and compliance of service usage with policies to be evaluated. Client (3rd party) applications can use the Policy Management API to express operational criteria in a form of policy. It is possible for an application to manage policy information, control access to it and to request evaluation of policies.

Fig.3 shows the formal definition of a rule for traffic marking based on Single rate Three Colour Marker (SRTCM) [10]. The SRTCM implements two Token Bucket mechanisms. The packet is first tested by the TB(CIR,CBS), where CIR denotes the committed information rate, while CBS denotes the committed burst size. If the packet conforms to the TB1(CIR, CBS) it is marked for low DP (green). Otherwise, it is forwarded to the TB2(CIR, EBS), where EBS denotes the contracted excess burst size. If the packet conforms to this TB, it is marked for medium DP (yellow) otherwise it is marled for high DP (red).

Fig. 4 shows the formal definition of a rule in Admission control policy group. The rule may be used in session authorization considering requested QoS parameters and the allowed QoS parameters as defined in the user profile.

```
if (TB1(CIR,CBS)-B(CIR,CBS)>=0)
  then setConformanceLevel(COLOR-MODE  FLAG,"green")
 else  if (TB2(CIR,EBS)-B(CIR,EBS)>=0)
   then setConformanceLevel(COLOR-MODE FLAG,"yellow")
  else setConformanceLevel(COLOR-MODE FLAG,"red") end
ConditionAttribute.AttributeName = “TokenBucketSize”.
ConditionAttribute.AttributeValue.SimpleValue.StringValue =
"MaximumSizeOfTokenBucket > CurrentPacketSize".
conditionList.Condition == <comparison between CIR, CBS parameters
of the bucket and the packet >.
conditionList.GroupNumber == 1; indicates how the conditions need to
be grouped in DNF or CNF in case more groups of rules exist.
conditionList.Negated == FALSE.
actionList.Action == <marking the packet with COLOR –MODE FLAG>
actionList.SequenceNumber == 1.
IF " Token bucket1(CIR, CBS) >= B(packet)" THEN "green mark ==
TRUE" , Else CBS -> EBS
IF " Token bucket2(CIR, EBS) >= B(packet)" THEN "yellow mark ==
TRUE", Else COLOR-MODE FLAG ==’red’
```

Fig.3 A rule for packet marking based on SRTCM

V. CONCLUSION

In this paper we investigate the IP policy control in IMS and present an approach to modeling of policy information. Policy information is structured according the quality of service mechanisms for controlling the network service response to a service request, which can be specific to a network element, or for signaling between network elements, or for controlling and administering traffic across a network.

The usage of Open Service Access Policy Management interfaces is exemplified. The interfaces can be used to perform administrative tasks on behalf of resource management, e.g. create, update or delete policy information and to invoke evaluation of policies of resource management service. Following the Policy Management specific data definitions we describe in a formal way resource management policy rules. The formal description of policy rules allows reuse of policy-related information in IMS policy engines.

ACKNOWLEDGEMENT

The research is partially supported by the Research project DO-02-135/2008 funded by Bulgarian Ministry of Education and Science.

REFERENCES

[1] Miikka Poikselka, Georg Mayer, Hisham Khartabil, Aki Niemi, The IMS Multimedia Concepts and Services, Wiley, 2008

[2] Michael Massimi, Ursula Wolz, Peer-to-Peer Policy Management System for Wearable Mobile Devices, www.dgp.toronto.edu/~mikem/pubs/MassimiWolz-ISWC03.pdf

[3] W. Lv, J. Kang, and W. Chen, TOOPM: A Telecom Operations-Oriented Policy Management System, Robotics and Applications and Telematics (RA 2007), Proceedings, pp.237-246

[4] ITU-T Y.1291, An architectural framework for support of Quality of Service in packet networks

[5] 3GPP TS 23.203 v8.4.0, Policy and charging control architecture

[6] ETSI TS 183 017 v1.1.1, Resource and Admission Control: DIAMETER protocol for session based policy set-up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF); Protocol specification

[7] 3GPP TS 29.198-13 v7.0.0, Open Service Access (OSA); Application Programming Interface (API); Part 13: Policy Management Service Capability Feature (SCF)

[8] ITU-T Y.2171, Next Generation Networks – Quality of Service and Performance, Admission control priority levels in Next Generation Networks

[9] ITU-T, M.3342, Guidelines for the definition of SLA representation templates

[10] J. Heinanen, R. Guerin, A Two Rate Three Color Marker, RFC 2697, 1999.

```
if (RVC)-(AVC)>=0)
      then setConformanceLevel(video resources,"allowed")
if (RAC)-(AAC)>=0)
      then setConformanceLevel(audio resources,"allowed")
if (RQoSclass)-(AQoSclass)>=0)
      then  setConformanceLevel(bidirectional
conversation,"allowed")
if (RVC)-(AVC)>=0) AND (RAC)-(AAC)>=0) AND
(RQoSclass)-(AQoSclass)>=0)
      then setConformanceLevel(IMS Session,"established")
      else  setConformanceLevel(IP flows,"unauthorized")
      setConformanceLevel(IMS Session,"failure") end
ConditionAttribute.AttributeName = "Session establishment".
ConditionAttribute.AttributeValue.SimpleValue.StringValue =
"MediaCharacteristicsOfNetwork > =UserProfileMediaCharasteristics".
ActionAttribute.AttributeName = "NegotiatedSDPParameters".
ActionAttribute.AttributeValue.SimpleValue.StringValue =
"AllowedVideo == TRUE".
ActionAttribute.AttributeValue.SimpleValue.StringValue =
"AllowedAudio == TRUE".
ActionAttribute.AttributeValue.SimpleValue.StringValue = "QoS class A
== TRUE".
conditionList.Condition == < establishing IMS session by comparing
allowed SDP parameters with the negotiated ones>
conditionList.Negated == FALSE.
actionList.Action == <authorization of IP flows of the chosen media
components by mapping from SDP parameters to authorized IP QoS
parameters >.
IF " requestedSDPparametersForVideo >= UserProfileAuthorized "
THEN "AllowedVideo == TRUE".
IF " requestedSDPparametersForAudio >= UserProfileAuthorized "
THEN "AllowedAudio == TRUE".
IF " requestedSDPparametersForQoSclass >= UserProfileAuthorized "
THEN "AllowedQoSclassA == TRUE".
IF "AllowedVideo == TRUE" & "AllowedAudio == TRUE" &
"AllowedQoSclassA == TRUE”
THEN “SessionEstablishmentWithRequestedParameters==TRUE”
Else
AuthorizationOfIPflows ==FALSE & SessionEstablishment ==FALSE.
```

Fig.4 A rule for admission control based on user profile data