

# Emergency Services Control Model for Next Generation Networks

Fabricio Carvalho de Gouveia (Corresponding author), Yacine Rebahi, Joaquim Ruiz  
Planella

Fraunhofer Institute FOKUS

Kaiserin-Augusta-Alle 31, D-10589, Berlin, Germany

{ Fabricio.Gouveia | Yacine.Rebahi | Joaquim.Ruiz.Planella }@fokus.fraunhofer.de

Thomas Magedanz

Technische Universität Berlin

Franklinstr. 28-29, D-10587, Berlin, Germany

E-mail: tm@cs.tu-berlin.de

## Abstract

Functioning and effective telecommunications are fundamental during and after disasters, be they natural or man-made, and it is specially in these particular situations that communications might congest at a very high rate. Therefore, emergency sessions need to be prioritized over non-emergency sessions to ensure the best coordination. For the more, it becomes clear that the control of Quality of Service in the on-going non-emergency sessions or even the acceptance of new non-emergency sessions is a key feature for the success of emergency services in critical situations. For all these reasons we propose a novel portable model for telecommunications operators for the support of emergency services, which through specific thresholds and dynamic policies will enhance the performance of Next Generation Networks under exceptional circumstances. The model complements the work done in emergency situations from other related work and conveys with the requirements defined by the ITU-T.

**Keywords:** Emergency Services, Call Admission Control, Quality of Service

## 1. Introduction

Emergency services are among the most fundamental and critical services to be offered by telecommunications networks. As countless new applications arise in heterogeneous network environments, there is an urge of adaption in Next Generation Networks to serve all kind of emergency situations with the appropriated Quality of Service. In earlier times, call signaling on a circuit-switched network proved sufficient to provide suitable Quality of Service (QoS). However, since Next Generation Networks are based on packet-switched technology there is a need to consider the technical issues and potential solutions that could prove themselves useful in the improvement and realization of emergency telecommunications capabilities in these networks.

The Internet Engineering Task Force (IETF) and the International Telecommunication Union (ITU) – among other international organizations – have focused their efforts in the development of standards and recommendations for emergency telecommunications in Next Generation Networks. Nevertheless, there exists a need for a better delimitation and definition of what aspects can be effective in the different possible solutions.

This paper describes the design of a portable model for emergency in Next Generation Networks, which follows the general lines established by the IETF and the ITU-T recommendations, for enabling operators to offer efficient communications under emergency situations.

The remainder of this paper is as follows: section 2 describes the related work, section 3 the methodology followed by the design and scenario description in section 4. Section 5 presents the call admission algorithm and finally, section 6 concludes the work and recommendations are made for further study.

## 2. Related Work

In [1] the authors discuss the Quality of Service policy to prepare for emergency situations and then classify the traffic based on the character of SIP and media data. In their work the authors concentrate on VoIP traffic (a real-time application) for emergency services. In order to establish a new class of service –specific for emergency sessions– among the ones already offered, they remark the need to clearly differentiate this new class. There are several methods to achieve this goal: relative priority marking, service marking, label switching, integrated Services/RSVP, etc. The authors declare DiffServ [2] to be fundamental for the classification of Internet traffic in order to prepare for emergency conditions (or highly congested conditions). Then they propose a call admission procedure based on the flow information and a SIP message log. Service differentiation is desired to accommodate heterogeneous application requirements and user expectations, and to permit differentiated pricing of services.

In [3] the author reviews the Emergency Telecommunications Services (ETS) requirements, dividing them into two different groups: Deployment-related issues and impact on current and future protocols. The paper also stresses that there are four key areas of general requirements for ETS for Internet systems, that is:

- Signaling. If emergency telecommunications is indicated via signaling, it must support the use of labels, e.g., a label may indicate an emergency call.
- Labels. May exist at different layers. Labels may be carried by signaling, and/or as a part of the header of a data packet.
- Policy. Local policy identifies the mechanisms to implement the effects of labels, i.e., labels do not have global significance.
- Network functionality. For ETS, this should be offered as a better than best effort service through a higher probability of reduced packet loss, and/or minimal jitter, and/or minimum end-to-end delay.

Dr. Chandra also remarks in his paper the usefulness of DiffServ mechanisms for the priority treatment.

In [4] the Third Generation Partnership Project (3GPP) establishes the service description for emergency services in the IP Multimedia Core Network Subsystem (IMS), including the elements necessary to support IP Multimedia emergency services.

In [5] the authors propose an extension of the 3GPP IMS emergency service architecture in order to lead to more efficient emergency operations. Specifically, they add context management entities: Sensor Gateways (SGW) – which interwork between information sources and the 3G core network – and a Context Information Base (CIB) – responsible for the management and dissemination of the contextual information provided by the first entities. They also propose enhancements for the Location Registration Function, Emergency-Call section Control Function and the Public Safety Answering Point (PSAP). As this work in progress from 3GPP is already taking care to specify how location can be obtained during an emergency call, we do not address this issue in the present work. There is still a lack of information about the way of defining possible situations within Emergency Services and that leads to the general term Emergency Services, not distinguishing among the different situations, although in [6] the authors criticize this fact and propose two new classes to improve the initial model, as well as define different QoS profiles in terms of QoS guarantees based on the needs of emergency communication services. In [6] the authors also propose an extended model for the IMS emergency service architecture, adding two new elements: the Session Prioritization Function (SPF) – which would make resource allocation/reallocation decisions – and the aforementioned CIB.

In [7] the authors present the use of DiffServ in mobile emergency telemedicine, emphasizing that the DiffServ model fits as an appropriate architecture for QoS provisioning in wireless medical networks. Telemedicine systems demand a highly reliable QoS. Therefore, the authors make a classification of the E-Health QoS requirements that can be contrasted with the characteristics of the different Behavior Aggregates presented in the DiffServ Request for Comments (RFCs).

Considering the three categories of emergency telecommunications presented in [8], i.e. citizen to authority, authority to authority and authority to citizen; we take into account for the development of the model the category citizen to authority, which is used by the general public to report problems or difficulties to learn the state of relatives and properties through

specific numbers provided by the government agencies in case of disaster; or to summon help from the authorities.

There is an ongoing initiative called Emergency Services Workshop Series that is aimed at coordinating global standards and technologies for emergency calling and emergency notification. Their discussions were focused on emergency service identification, mapping location to Public Safety Answering Point (PSAP), architectural aspects of location information delivery, and location determination and conveyance in SIP [9], [10]. This leaves an open point in the traffic load balancing, where we focus our work.

Finally the IP-based Emergency Application and serviCes for nExt generation networks (PEACE) project [11] is defining mechanisms for fast and lightweight establishment of trust relations between ad-hoc members of an emergency team and ensuring the security of their communication. Also other aspects like emergency calls identification, caller location retrieval and routing are being addressed.

The work we are presenting in this paper envisages complementing the work being developed in the PEACE project by developing a model that can adapt the network's traffic load in case of different levels of emergency sessions. Furthermore, the method chosen is based on DiffServ, which is a widely accepted prioritization mechanism shared also by the other related work cited before. This work is a complimentary to standardization efforts (like 3GPP, ITU-T) and the other work cited before. To the best of our knowledge we didn't find any solution on traffic distribution for emergency services at the time of writing.

### 3. Methodology

In order to define the thresholds that will trigger different actions in the network, the following methodology is considered: In the first place we define a new class to identify emergency sessions and differentiate them from all the other classes (Gold, silver, Bronze), which are the default non-emergency sessions. DiffServ-based technology is used to provide different treatment to diverse types of traffic [5].

The detection of emergency sessions is done through a specific header in the SIP signaling [4], [12]. The header field can have the values "non-urgent", "normal", "urgent", and "emergency". The model takes into account the amount of emergency sessions, so boundaries will need to be established in order to detect the breaking points (or the thresholds, as they are called in this paper) where control actions need to be taken, such as non-emergency sessions' quality be downgraded, new non-emergency sessions be restricted or even dropped depending on parameters like available Bandwidth.

The concept of thresholds is used in the model to balance the network traffic depending on the current load of the network. The thresholds take into consideration the current number of emergency and all the other ongoing sessions. Two terms used in this work need to be defined:

- Occupancy: refers to the percentage of subscribers that currently have a session established over the total number of subscribers: "number of sessions"/"number of

subscribers”;

- Emergency sessions: In this paper we address the citizen to authority scenario. All sessions identified as “Emergency” by the specific parameter in the SIP header [4], [12] are counted as an emergency session. On a given time, the normal scenario (where no big emergency event has occurred) the emergency sessions correspond to up to 5% of the total ongoing sessions.

The definition of the thresholds is done by increasing both variables (occupancy and number of emergency sessions) progressively and separately and/or at the same time, to study the bandwidth required by subscribers and balance the traffic among all classes in order to get the best distribution at each different emergency load. The main objective of our model is to give priority and best QoS for the emergency sessions and, at the same time, provide the best service possible to subscribers by accepting the maximum number of non-emergency sessions. Therefore our evaluations define when there is the need to implement new policies to the Call Admission Control (CAC) based on this objective. These are the defined thresholds, which change the current policies being applied in the new incoming resource requests.

Then policies are defined and a different set of them is triggered depending on the threshold achieved. The designed policies affect differently Bronze, Silver and Gold users, since they have different privileges in how packets from these different classes are treated by the network. The main objective on the definition of these policies is to be able to make the existing architecture be capable to accept as many sessions as possible within the limited resources under critical situations, and always ensuring the best Quality of Service possible for emergency sessions. These different policy strategies aim to improve the overall system performance under heavy emergency sessions’ requests. In very congested situations, it is assumed that non-emergency sessions may experience blocking thorough connection admission control procedures, in order to allow for emergency sessions to complete.

The next section exemplifies with a scenario and shows in more detail the definition of these thresholds.

#### **4. Design and Scenario**

The QoS Class Identifiers (QCIs) defined for the classes proposed and their correspondent DiffServ Code Points (DSCP) [2] are:

- QCI 1: Expedited Forwarding (EF)
- QCI 2: Assured Forwarding (AF41)
- QCI 3: Assured Forwarding (AF42)
- QCI 4: Best Effort (BE)

QCI 1 is set to emergency and Gold sessions during normal circumstances (with total emergency sessions under 5% of total sessions); QCI 2 is reserved for Gold sessions when the network is congested; QCI 3 is set for Silver sessions and QCI 4 for Bronze.

We define a theoretical scenario in order to study how the network should behave in case

of emergency and afterwards define a basic model that can be adjusted to specific operators' needs, which makes the model applicable in different sizes of enterprises with different customer distributions and available bandwidth.

In the studied scenario we have a big operator with 25 GB of available bandwidth in the ingress router and two million subscribers (distributed among Gold: 300,000; Silver: 700,000; and Bronze: 1,000,000 accounts), where all users who establish a session use the most bandwidth-expensive service that their subscription allows them to use (i.e. we have considered the worst possible case along the whole scenario). The top services assigned by contract to the users are: high-quality video for Gold (640 Kbps), low-quality video for Silver (320 Kbps) and audio only for Bronze (32 Kbps). Although in most cases emergency calls use audio, we have assumed that in the near future there will exist the possibility that most people contact the authorities through video, as images contain more specific information to help in emergencies and current telecommunication architectures are enhancing data rate transfer for mobile users. Therefore, emergency sessions are able to use any kind of media and, in the scenario, we have considered the use of high-quality video.

In the considered scenario we study the evolution of the network's resources before, during and after a critical event (specifically a terrorist attack in the central stations of Berlin, similarly to the events on March 2004 in Madrid) and seek to endure the traffic load under the objectives described in section 2.

We depart from different initial occupancies characterized by the average traffic rate per category. This distribution is operator specific and we setup in this scenario the distribution of the ongoing sessions into: 5% emergency sessions, 20% Gold sessions, 35% Silver sessions and 40% Bronze sessions. We have assumed that under standard circumstances (when no terrorist attack has taken place) the maximum percentage of emergency sessions over the total number of ongoing sessions is up to 5% and we depart in all the initial statistics from such percentage in order to perform the analysis. Then we see what happens when there is an increase in the current occupancy (more subscribers establish new sessions) maintaining the distribution of the sessions and check what is the total bandwidth required.

Afterwards we assume that the terrorist attack has occurred and, therefore, we progressively increase the percentage of emergency sessions over the whole number of ongoing sessions. The effect of this increase in the emergency sessions is studied with different occupancies, e.g. considering that the total number of sessions is constant, but the increase of emergency sessions affects the distribution of the rest of categories; as well as what the increase of emergency sessions implies an increase in the total number of sessions. By these means we observe when the system reaches the maximum capacity in terms of bandwidth, study the consequences of applying different strategies to improve the system's performance and set the thresholds with these new policies.

By increasing the number of sessions until these require the total bandwidth capacity of the operator (25GB), we have defined the first threshold at 11.2% of the total bandwidth for the emergency sessions (see Table 1). If no action is taken, the network cannot accept new sessions. Therefore the first change of policies is done at this point (Figure 1), where the

network becomes able to support more sessions.

Table 1: Total bandwidth being reached by 5% emergency sessions

Category, QCI	Percentage of sessions	Number of sessions	Bandwidth per session (Kb)	Total bandwidth per category (GB)	% Total BW
ES, 1	5%	35.000	640	3	11,20%
Gold, 1	20%	140.000	640	11	44,80%
Silver, 3	35%	245.000	320	10	39,20%
Bronze, 4	40%	280.000	32	1	4,48%
<b>TOTAL</b>	100%	700.000		<b>25</b>	99,68%

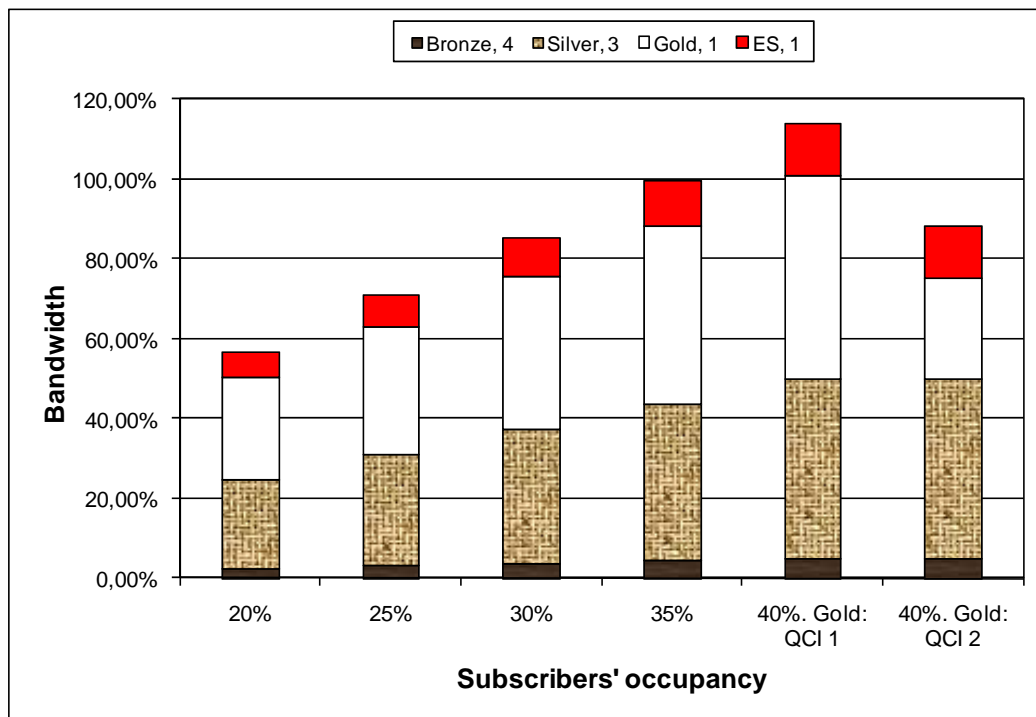


Figure 1. Linear increase of occupancy by the standard distribution

For the second threshold we have proceeded similarly, but considering that the emergency event influences the rate of emergency sessions by increasing them. Therefore, with different occupancies and different distributions of the sessions among the categories, the maximum capacity is reached at different points, optimizing the compromise between all the possible statistics; we define the second threshold at 25.6% of the total bandwidth. For the last two thresholds we have proceeded the same way, but as the maximum capacity of the operator was quickly reached (video sessions consume a lot of bandwidth), the objective to apply QoS changes to permit a higher number of sessions per category is maintained. Therefore the defined thresholds are: Th1 = 11.2% (of the total BW), Th2 = 25.6%, Th3 = 40% and Th4 = 60%. The first thresholds are more critical as they tend to be the most triggered. The policies triggered by each threshold are:

- Th1: redistribution of reserved bandwidth

- Th2: redistribution of reserved bandwidth and downgrade to QCI 2 for Gold sessions
- Th3: redistribution of reserved bandwidth
- Th4: redistribution of maximum bandwidth, downgrade to QCI 4 for Silver sessions and rejection of Bronze sessions

To illustrate the behavior of these distributions the bandwidths assigned and subscribers supported (considering that they use the most bandwidth-expensive resource available according to their category) are presented and compared within each margin in figures 2 and 3. In Figure 2 we can observe the evolution of the bandwidths assigned and, in the Figure 3, the subscribers supported.

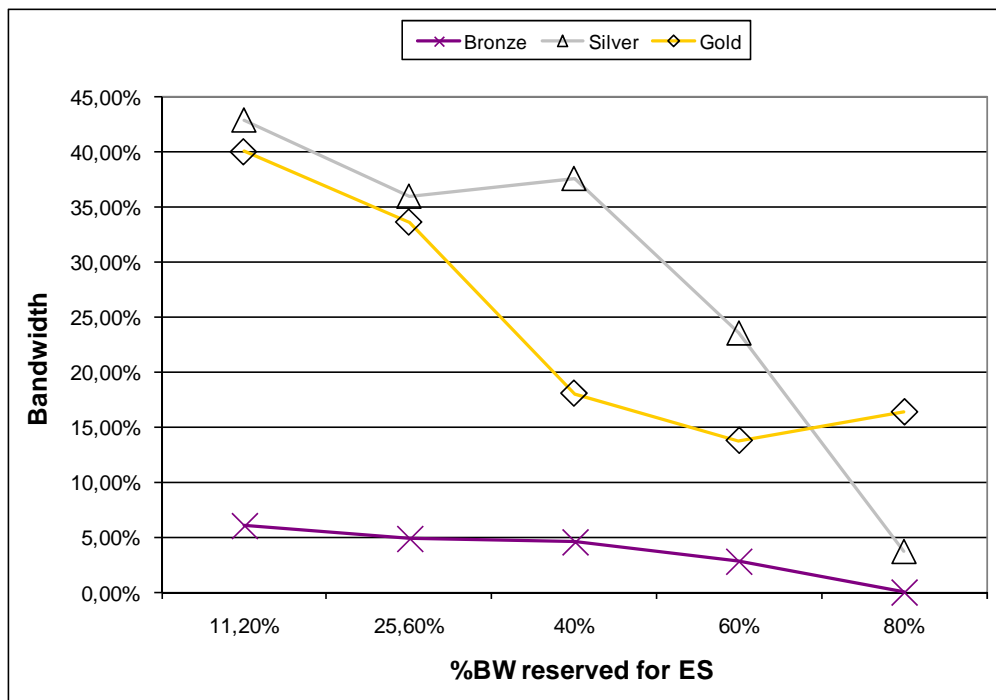


Figure 2. Assigned Bandwidth.

Figure 2 shows how the bandwidth is smoothly reduced for Bronze subscribers along the established margins; of course, this is due to the low bandwidth per session needed (compared to the other categories).

Gold and silver’s reserved bandwidths present a particular behavior at two specific points: The first one, at 40% bandwidth reserved for ES, is due to the change in Gold sessions’ QCI; which allows the network to re-assign bandwidth to Silver subscribers. The second one, at 80% bandwidth reserved for ES, is due to the change in Silver sessions’ QCI, permitting to increase the bandwidth assigned for Gold sessions (as the chart clearly reflects) and dramatically reducing the necessary bandwidth to maintain the expected Silver sessions.

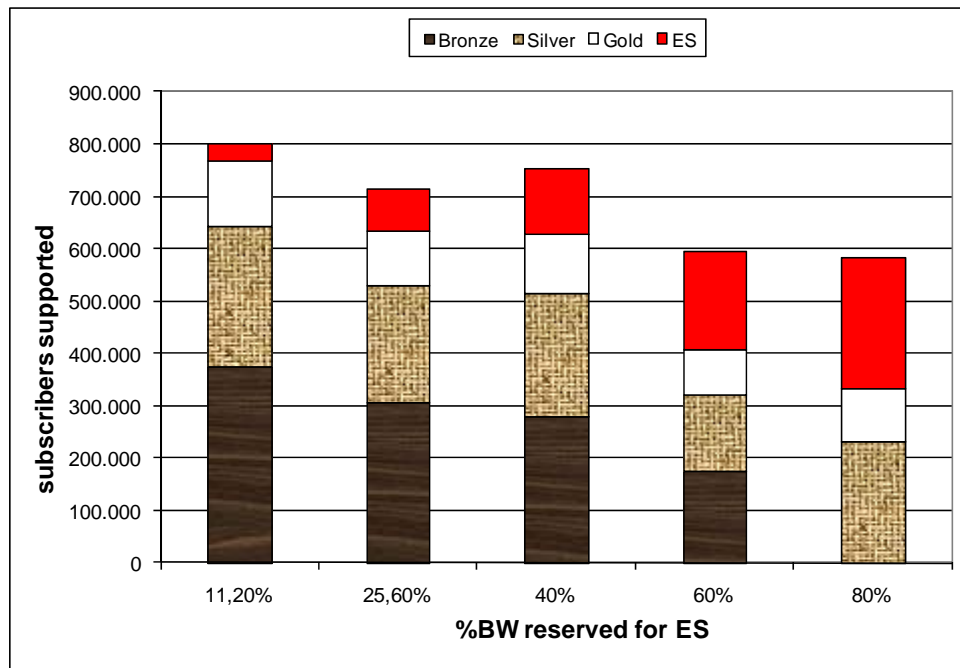


Figure 3: Subscribers supported

Figure 3 shows the subscribers supported for each category within each margin. The first noticeable characteristic is that at 40% the subscribers supported increase instead of decreasing. This is due to the QoS downgrade for Gold sessions at this point.

Regarding the various categories, we can observe that emergency sessions increase consistently, in contrast with Bronze sessions, which have the opposite behavior. The number of Gold sessions allowed remains relatively stable and only decreases significantly when 60% of the bandwidth is reserved for ES (Bronze sessions are not yet automatically dropped and Silver subscribers' QoS has not been downgraded). Similarly to Gold sessions, Silver ones suffer a considerable decrease at 60% bandwidth reserved for ES, but increase in approximately the same proportion at 80%, in expense of the change of QCI from 3 to 4 (DSCP from AF42 to BE).

## 5. Call Admission Algorithm

Admission control can ensure high-quality communication by ensuring the availability of bandwidth to carry a load. Inelastic real-time flows such as Voice over Internet Protocol (VoIP) or video conferencing services can benefit from use of an admission control mechanism, as generally the telephony service is configured with over-subscription, meaning that some users may not be able to make a call during peak periods. We define a call admission algorithm to cope with the aforementioned problem. Therefore, in order to limit the bandwidth to the bandwidth reserved per category according to the basic model, the sessions must be accepted or rejected through this Call Admission Algorithm (CAA).

In the first place, when a new session arrives, the IMS architecture checks what category of subscription the user has through the Subscription Profile Repository (SPR). Then the

algorithm checks at which emergency stage of the scenario the Network currently is. Presumably, most of the time, the system should be under 11.2% of bandwidth dedicated to ES and, if more emergency events (or a big scale one like the one in the scenario) take place, this rate shall increase over the aforementioned threshold.

In the second place, the algorithm checks the bandwidth permitted at each point. Through the Policy and Charging Enforcement Function (PCEF) we can know the number of on-going sessions per category of subscriber, as well as the current bandwidth used: along the scenario we have worked with number of sessions (assuming the worst case, i.e. that each session consumes the maximum bandwidth permitted). Considering  $\varphi$  the number of sessions permitted and  $\gamma_i$  the maximum bandwidth per category in Kbps per session (where sub-index  $i = [E, G, S, B]$  indicates the category), we can establish the upper limit as shown in equation (1) below:

$$UL_{ESR, i} [MB] = (\varphi \cdot \gamma_i) / 8,000 \quad (1)$$

The  $\varphi$ 's (number of sessions) shown in Table 1 are the result of the scenario analysis. We establish the upper limits in MB (last column in Table 1) because in this manner we can easily change the reserved bandwidth within each margin by modifying the PCC rules when escalating the model (allowing operators to adapt the model to their necessities), as well as allow a greater number of sessions than the maximum defined in the " $\varphi$ " column in Table 1, because subscribers will not use the most bandwidth-expensive service each time they establish a session.

Table 2: Upper Limits for the Call Acceptance Algorithm

ES Rate	i = Category	QCI	$\varphi$ (sessions)	$\gamma_i$ (Kbps/session)	$UL_{ESR, i}$
<b>ESR ≤ 11.2%</b>	ES	1	35,000	640	<b>2,800</b>
	Gold	1	125,000	640	<b>10,000</b>
	Silver	3	267,500	320	<b>10,700</b>
	Bronze	4	375,000	32	<b>1,500</b>
<b>11.2% &lt; ESR ≤ 25.6%</b>	ES	1	80,000	640	<b>6,400</b>
	Gold	1	105,000	640	<b>8,400</b>
	Silver	3	224,375	320	<b>8,975</b>
	Bronze	4	306,250	32	<b>1,225</b>
<b>25.6% &lt; ESR ≤ 40%</b>	ES	1	125,000	640	<b>10,000</b>
	Gold	2	112,500	320	<b>4,500</b>
	Silver	3	234,375	320	<b>9,375</b>
	Bronze	4	281,250	32	<b>1,125</b>
<b>40% &lt; ESR ≤ 60%</b>	ES	1	187,500	640	<b>15,000</b>
	Gold	2	85,625	320	<b>3,425</b>
	Silver	3	146,875	320	<b>5,875</b>
	Bronze	4	175,000	32	<b>700</b>
<b>60% &lt; ESR ≤ 80%</b>	ES	1	250,000	640	<b>20,000</b>
	Gold	2	101,875	320	<b>4,075</b>
	Silver	4	231,250	32	<b>925</b>
	Bronze	-	0	-	-

In Table 2 we present all the data required for the calculation of the Upper Limits within each ES rate’s margin. The thresholds that trigger the next bandwidth reservation stages are the upper limits in the “ES rate” column, i.e. 11.2%, 25.6%, 40% and 60%.

The algorithm’s structure is shown in Figure 4. The algorithm shows that the system will only accept a new session if its load is placed within the acceptable parameters (reserved bandwidths) defined for each margin. When a session is accepted it is assigned the appropriate QCI.

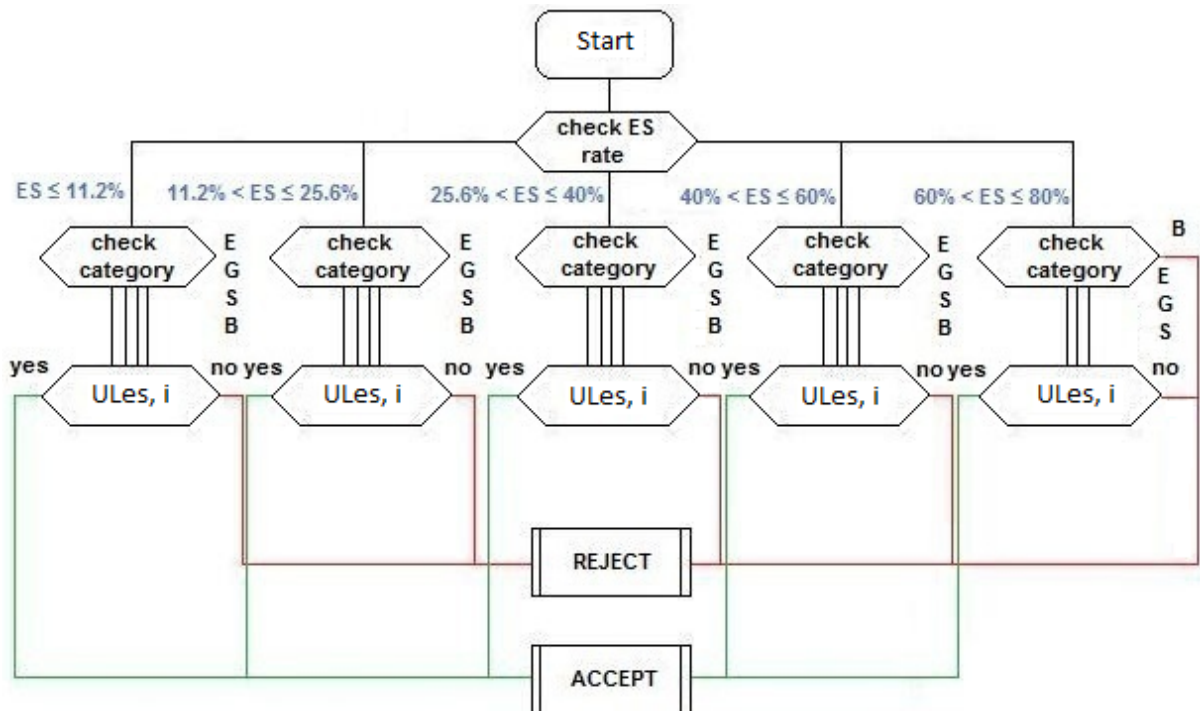


Figure 4: Call Admission Algorithm

The CAA is implemented through structured Policy and Charging Control (PCC) rules (policies in XML format) stored in the Policy and Charging Rules Function (PCRF) and enforced by the PCEF. The conditions supported by the PCRF are summarized in the Table 3 (for more information on the implemented PCRF and PCC rules please refer to [13]). The actions supported by the PCRF are summarized in Table 4.

Table 3: PCC rules’ conditions

Condition Tag	Description
<service-identifier>	The application function identifier
<service-class>	The Subscriber Media Profile Identifier
<max-bandwidth>	Maximum bandwidth requested for a particular media
<codec>	Codec identifier for audio and video media sessions
<media-type>	Type of media of the request
<emergency-sessions-rate>	The ESR_X, where X = [1, 2, 3, 4 or 5]
<current-bandwidth>	Which indicates the current bandwidth or number of on-going sessions of E, G, S or B

Table 4: PCC rules' actions

Action Tag	Description
<subscribe>	Contains the network level events for which the PCRF requests reports from the gateway
<set>	May include the QCI (<qci>) or the maximum bandwidth (<max-bandwidth>) authorized for the session
<abort>	Abort the session
<reject>	Reject the session

We include an example of PCC rule (Figure 5) where an incoming Gold session – that will be accepted as the <current-bandwidth> does not exceed the Upper Limit for Gold sessions in ESR3 (which according to Table 1 is 25.6%<ESR<40%), which is 4,500 – and will be assigned the appropriate QCI (2 in this case).

```

<rule id="ESR3-Gold">
  <conditions>
    <service-class>
      gold
    </service-class>
    <media-type>
      video
    </media-type>
    <codec>
      LQ-video
    </codec>
    <emergency-sessions-rate>
      ESR3
    </emergency-sessions-rate>
    <current-bandwidth>
      3250
    </current-bandwidth>
  </conditions>
  <actions>
    <set>
      <qci>
        2
      </qci>
      <max-bandwidth>
        320
      <max-bandwidth>
    </set>
  </actions>
</rule>

```

Figure 5: Accept Gold session rule

## 5. Conclusions and Future Work.

In this paper, we have proposed a complementary emergency solution for NGNs. Complementary because it takes into account certain aspects that the IMS architecture and other related work does not, such as provisioning of preferential treatment not only to emergency communications, but also for non-emergency communications; bandwidth reservation with the best distribution possible and sets of policies that are triggered based on different thresholds indicating emergency calls.

A discussion about how to apply this model to other operators with different parameters (e.g. available bandwidth) and different number of users and distributions through classes need to be included. This portability of the model is achieved by applying certain coefficients to the basic model. For instance the variables defined for escalating the model are:

- $\alpha$ : non-dimensional variable proportional to [BW / S]: [bandwidth/subscribers]; with  $\alpha=1$  for BW = 25 GB, S = 2•106 subscribers (referenced to the basic model)
- $\tau_i$  with  $i = [1, 2, 3, 4]$ . The different thresholds defined, with the following values:
  - $\tau_1 = 11.2\%$
  - $\tau_2 = 25.6\%$
  - $\tau_3 = 40.0\%$
  - $\tau_4 = 60.0\%$
- $\beta = \langle \text{restrictions} \rangle = [\beta_G, \beta_S, \beta_B, \beta_{S2}]$ ; where:
  - $\beta_G$  = Gold sessions change QoS from  $q_{ci} 1$  to  $q_{ci} 2$
  - $\beta_S$  = Silver sessions change QoS from  $q_{ci} 3$  to  $q_{ci} 4$
  - $\beta_B$  = Bronze sessions are aborted and rejected
  - $\beta_{S2}$  = Silver sessions are aborted and rejected
- $\gamma = \langle \text{bandwidth redistribution parameter} \rangle = [\gamma_G, \gamma_S, \gamma_B]$ :  $\gamma$  is proportional to [ bandwidth / session ]. Therefore:
  - $\gamma_G$  is proportional to [ bandwidth / gold session ]
  - $\gamma_S$  is proportional to [ bandwidth / silver session ]
  - $\gamma_B$  is proportional to [ bandwidth / bronze session ]

These algorithms need to be further enhanced and optimized based on the above coefficients for making the model easily portable to other different scenarios.

## Acknowledgement

The research is financed partially by the European Commission in the context of the IP-based Emergency Application and serviCes for nExt generation networks (PEACE) project. <http://www.ict-peace.eu/>.

## References

- [1] Noro, M.; Kikuchi, T.; Baba, K.; Sunahara, H.; Shimojo, S.: “QoS Support for VoIP Traffic to Prepare Emergency”, in the IEEE Applications and the Internet Workshops, SAINTW’04 IEEE, Nara, Japan, 26-30 January, 2004.
- [2] Blake, S.; Black, D.; Carlson, M.; Davies, E.; Wang, Z.; Weiss, W.: “An Architecture for

Differentiated Services”. RFC 2475, December 1998.

[3] Chandra, S.: “Priority services for supporting emergency telecommunications in Internet Protocol-based networks”, *The Telecommunications Review*, Page(s): 45-53, 2006.

[4] 3GPP TS 23.167. “Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS) emergency sessions”. December 2008.

[5] May El Barachi, A.K.; Glitho, R.; Ferhat Khendek, R.D. “An Architecture for the Provision of Context Aware Emergency Services in the IP Multimedia Subsystem”, in the 67th IEEE Vehicular Technology Conference VTC Spring 2008, 11-14 May, Singapore, 2008.

[6] May El Barachi, A.K.; Glitho, R.; Ferhat Khendek, R.D. “Enhancing the QoS and Resource Management Aspects of the 3GPP IMS Emergency Service Architecture”, in the 5th IEEE Consumer Communications and Networking Conference, (CCNC 2008), Page(s):112 – 116, 2008.

[7] Vergados, D.J.; Vergados, D.D.; Maglogiannis, I.: “Applying Wireless Diffserv for QoS Provisioning in Mobile Emergency Telemedicine”, in the IEEE Global Telecommunications Conference (GLOBECOM '06), San Francisco, CA, 2006.

[8] ITU-T Recommendation Y.2205. “Next Generation Networks – Emergency telecommunications – Technical considerations”. September 2008.

[9] Edge, S.: “3GPP support for IP based Emergency Calls”, presented in the Standards Development Organization (SDO) Emergency Services Coordination Workshop (ESW06), Columbia University, New York, October 5-6, 2006. Available at <http://www.emergency-services-coordination.info/2006/slides/>

[10] Polk, J.; Rosen, B.: “SIP Location Conveyance”, presented in the Standards Development Organization (SDO) Emergency Services Coordination Workshop (ESW06), Columbia University, New York, October 5-6, 2006. Available at <http://www.emergency-services-coordination.info/2006/slides/>

[11] PEACE website (IP- bases Emergency Applications and serviCes for nExt generaton networks), available at: <http://www.ict-peace.eu>

[12] Shulzrinne, H.; Polk, J.: “Communications Resource Priority for the Session Initiation Protocol (SIP)”. RFC 4412, February 2006.

[13] A. Diez Albaladejo, A.; Carvalho de Gouveia, F.; Corici, M.I., Magedanz, T.: “The PCC Rule in the 3GPP IMS Policy and Charging Control Architecture”, IEEE Global Telecommunications Conference, New Orleans, USA, 30th November - 4 December 2008.