VITAL++ A New Communication Paradigm: Embedding P2P Technology in Next Generation Networks

Athanasios Christakidis*, Nikolaos Efthymiopoulos*, Jens Fiedler®, Shane Dempsey#, Konstantinos Koutsopoulos©, Spyros Denazis*, Spyridwn Tombros*, Stephen Garvey# ,Odysseas Koufopavlou*

®Fraunhofer Fokus, Berlin, Germany
*Electrical and Computer Engineering,University of Patras, Greece
#Waterford Institute of Technology, Waterford, Ireland
©Blue Chip Technologies S.A., Athens, Greece

Abstract – This paper describes the major components and their interactions of a novel architecture called VITAL++ that combines the best features of the two seemingly disparate worlds, Peer-to-Peer (P2P) and NGN in particular IMS, which is then used to support multimedia applications and content distribution services. To this end, P2P is enhanced with advanced authentication and DRM mechanisms while NGN have become more scalable, reliable and less centralized by exploiting P2P self-organization properties. We describe novel P2P algorithms for optimizing network resources in order to efficiently distribute content among various users without resorting to laborious management operations required in NGN.

1. Introduction

The continuing evolution of the Internet has elevated digital communications to higher levels and made audiovisual communications, such as content distribution, digital TV, and video-on-demand mainstream among the Internet applications of today. These emerging types of applications, rich in user-created content, enabled by P2P technology, with high demands for network resources are rapidly changing the landscape of network operations and requirements. Replacing the traditional client-server operations with light-weight and highly distributed architectures for content delivery creates new challenges in network and service management, configuration, deployment, protocols etc.

Cisco predict that by 2014 more than 90% of the traffic traversing the internet will be video content, whether delivered using P2P networks or streamed from servers [1]. Deep-packet inspection vendor, Ipoque, have released a study [2] showing P2P traffic dominates as a percentage of the total Internet traffic. Much of this P2P traffic consists of BitTorrent file-sharing and the Skype telecoms platform which are viewed as a nuisance by many network operators as they consume significant bandwidth, see unlicensed content distributed throughout the network and, in the case of Skype, subtract from Network Operator's voice revenues.

Recent advances in P2P streaming [6][9] indicate the potential for optimum exploitation of the available user resources, e.g. up to 95% utilization of the total available upload bandwidth in the network. This combined with the ease of introducing and integrating dynamically resources in P2P overlays, wherever they are

needed, without resorting to laborious and costly management operations, makes P2P a promising technology that can be integrated with existing telecommunication practices and efficiently distribute all content. Initiatives like ALTO [3] in the IETF recognize that consumer demand drives the distribution of content to the edge and access networks where P2P may play an important role. Accordingly, Content Distribution Network (CDN) architectures may be created to support more efficient distribution of content by unburdening the network core.

The International Telecommunications Union (ITU) study group on IPTV described CDN and P2P solutions for content distribution, which are compatible with the IPTV architectures proposed by ETSI and ITU standardization groups [4]. Their solution is primarily based on the extensive use of Content Distribution Servers. As CDN servers cannot be "installed infinitely" and the number of clients that can be served at any time depends on the power and number of CDN servers, a P2P system is required that increases scalability and allows for situations where "each end node can be both a media producer as well as a media consumer".

The arguments above provide a strong motivation towards investigating and experimenting with ways of integrating P2P with telecommunication network architectures, standards and practices for multimedia distribution services. This leads to a "managed P2P" architecture that incorporates features required by network operators and service providers such as authentication, accounting, digital rights management and configurable QoS for content delivery applications such as IPTV.

Next Generation Networks (NGN) represents the latest architectural evolution in core and access networks aiming at creating converged IP communication platforms with IP Multimedia subsystem (IMS) rapidly becoming one instance of a NGN control plane technology. IMS primarily addresses issues of heterogeneity of access technologies, addressing schemes, AAA, QoS, security and mobility management from an operator's perspective. To this end, it becomes the ideal candidate for embedding desirable P2P functionality.

However, these two seemingly competing technologies have thus-far been deployed independent of each other, therefore failing to mutually exploit their strengths towards creating a new and more powerful paradigm. When comparing IMS and P2P we compare two inherently different worlds (*Figure 1*). IMS as a technology for controlling media flows, administer subscribers and control access to services in a highly centralized system. In contrast, P2P is a highly distributed system that has been designed to be scalable, adaptable, and failure resilient, mainly for the distribution of media (files, streams).

	P2P	IMS
Scalability	Very good	Difficult
Single Points of Failure	No	Yes
Users as Content Providers	Yes	No
DDoS vulnerable	No	Yes
Access	Easy	Difficult
Security / AAA	Bad	Good
Topology aware	Difficult	Yes
Standardized	No	Yes
Quality of Service	No	Yes
NAT Client Problem	Difficult	No
Service Deployment	Difficult	Easy

Figure 1 IMS vs. P2P comparative overview

This paper describes the VITAL++ architecture [5], which is **a communication paradigm that fulfils the requirements of both users and operators and proposes a new architecture for content distribution systems.**
More specifically, in Section 2 we identify the requirements to be taken into account and the VITAL++ architecture that meets these requirements. We note here that the innovation of our work relies on the methodology of how P2P can be embedded into an NGN architecture like IMS and vice versa, rather than the specifics of IMS. To this end, any future NGN architecture can be integrated with P2P in a similar manner. In Section 3 we show how innovative P2P algorithms developed as part of VITAL++ are capable of optimally utilizing the available user resources thus offering live streaming without additional management overhead. Section 4 presents our conclusions.

2. VITAL++ requirements and architecture

With VITAL++, we propose a Network Operator and Service Provider "managed P2P" architecture, compatible with the ITU-specified P2P IPTV architecture. Our architecture is modular and can also deliver other applications including file-based content distribution and video on demand.
We annotate the major functionalities that our system has to deliver in five categories that also form our sub-architectures (SA).
The first is the P2P authentication (P2PA) SA that is responsible for enabling clients (peers) to authenticate messages in order to ensure that those received messages come only from authorized peers.
The Content Index (CI) SA has three major functionalities. It allows the publishing of objects from users and/or content providers, enables queries for objects that our system maintains and distributes, tracks which peers have what objects, and provides the initial insertion of a peer to the overlay that distributes the object that it requests.

The next major functionality of our system is the Overlay Management (OM) SA. This SA is responsible for the management of the Content Diffusion Overlay (CDO). The CDO is a graph that participating peers cooperatively form and maintain by selecting dynamically a small subset of peers that act as its neighbors. The purpose of the CDO is the distribution of the content, which users exchange with their neighbors real time in the form of data (content) blocks. This graph determines the network paths that the system uses in order to distribute the content according to the user requests. The system creates and maintains one CDO for each media object that it distributes.

The Content Security (CS) sub-architecture has been designed to enable content providers to control the distribution of the content using Digital Rights Management technology. VITAL++'s DRM was designed to satisfy real content provider requirements and so it is related to real-world business requirements. More specifically, the requirements range from Conditional Access to streaming Content, Encryption of file-based and streamed content where appropriate, flexible rights expression, integration with Accounting, respect for privacy and consumer rights, assertion of "fair-use" for purposes such as backup/education etc, and identity-based conditional access (providing a better alternative to Geo-IP blocking).

The QoS SA manages the network resources in order to dynamically guarantee their availability for the distribution of every object. In pure peer-to-peer content distribution systems, the upper bit rate that can be delivered successfully to all the participating peers is bounded by the average of their upload bandwidth. As a result, a pure peer-to-peer architecture can't guarantee delivery with a specific bit-rate, as the average value of the peers upload bandwidth varies, due to dynamic behavior of the peers and the dynamic conditions of the underlying network. Our proposed solution is scalable, calculating accurately and dynamically the minimum amount of bandwidth resources that servers have to contribute towards this goal.

Finally an application specific P2P Block-Exchange Scheduling Algorithm (P2P-BESA) is a distributed scheduling algorithm that ensures the complete distribution of each object to every user on time. These SAs have been designed in such a way as to meet the following requirements that are necessary towards the fulfillment of the users, the service providers and the network provider's needs.

- The first one is **scalability** in terms of participating users. The functionalities that introduce high overhead to the system are: the bandwidth provision for the distribution of every object, the management and the dynamic adaptation of the CDO according to varying traffic conditions and peer behavior, the authentication between peers and finally the block scheduling process. We implemented these functionalities using distributed architectures in order to ensure scalability in our system.
- We ensure the **high performance** of the system by the use of a specific graph structure of the CDO that exploits all the available resources, an intelligent P2P-BESA that guarantees the diffusion of every object to every peer on time and the QoS SA that controls the resources that are required towards the distribution of each object. Finally P2PA ensures the entrance in the system of authorized peers

- The **minimization of the network traffic** that our system introduces to the underlying network is realized by a CDO where each peer has neighbors close to it in the underlying network.
- The **fault tolerance** of the system is guaranteed by the continuous adaptation of the CDO to peers arrivals and departures and in link failures in the underlying network. Additionally the flexibility that P2P-BESA introduces in the data flows between peers guarantees the on-time delivery of every data block before its playback deadline.
- Under normal circumstances, a P2P network is not vulnerable to **DDoS attacks**, because an attacked node will behave as a single failure, which is subject to self-healing in the rest of the network. IMS is more vulnerable and so P2P instills resilience in the system to DDoS attacks.
- The CI-SA enables the ability of participating **users to act as content providers** while simultaneously ensure the manageability of the objects from a Network Operator and a Service Provider perspective.
- User **Authentication** is a basic requirement in order to enable secure P2P messaging and so avoid unauthorized access in the system.
- **Anonymity** is also preserved as the key distribution is done only when a peer enters the system from an application server and the only information that each peer reveals to other peers is that it is an authorized peer in the system.
- **Accounting** functionality maintains an audit trail of licenses granted for content and the network bandwidth and overlay statistics associated with delivering that content..
- Content protection provides digital rights management whereby content providers can specify licensing rules and costs for individual users based on details such as their subscriber id, location, network provider, and service "package" (e.g. gold, silver, bronze).
- P2P is primarily an end-users' technology that fosters self-deployment and self-organization while it achieves optimized resource utilisation for the deployed applications and services. With the development of our **QoS** SA we succeeded where QoS mechanisms have failed to be deployed and operate at large scales.
- Finally VITAL++ through the use of IMS provides a **well-defined, modular and standards-based** way to deploy applications, reusing supporting services such as security and accounting. This enhances P2P systems where services are usually designed to meet one specific use case (e.g. file sharing).

From these design considerations, it has been decided to position IMS sided functionalities of the VITAL++ architecture in various application servers; while the client sided functionalities are located directly in the client so that no additional components are necessary. Figure 2 illustrates an overview of the architecture and its functional blocks, which are explained in the remaining sections of this work. For the sake of complexity we consider the QoS SA part of the Content Indexing and we also consider CDO and P2P- BESA part of Overlay management.

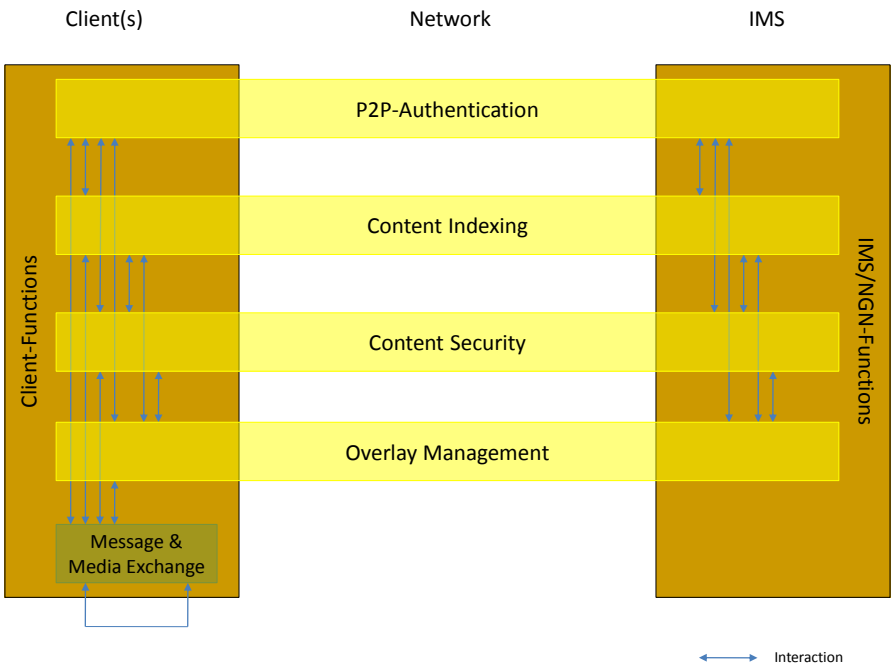

Figure 2: VITAL++ abstract view of the overall architecture

2.1.P2PA-SA

The purpose of the P2P-Authentication Sub-Architecture (P2PA-SA) is to enable clients (peers) to verify the authenticity of messages which have been sent by other clients directly to them, without passing through any operator controlled entity. This envisages the security of services, which are based on pure P2P message exchange, like sharing of contacts or media, etc.

The P2P-Authentication sub-architecture works with certificates, which describe an entity and its properties. In VITAL++, three types of certificates are distinguished. The root certificate that is self-signed and pre-installed in every client and P2P-authentication server module. The server certificate that is signed by the Root-CA, is pre-installed in every P2P-Authentication server module, describes the identity of the server domain and its public key and is acquired by each client during registration. The third is the client certificate that is signed by a P2P authentication server on request and describes the identity of the client and its public key.

Finally, each client is equipped with these three certificates, which allow it to perform all authenticity transactions and checks as explained below.

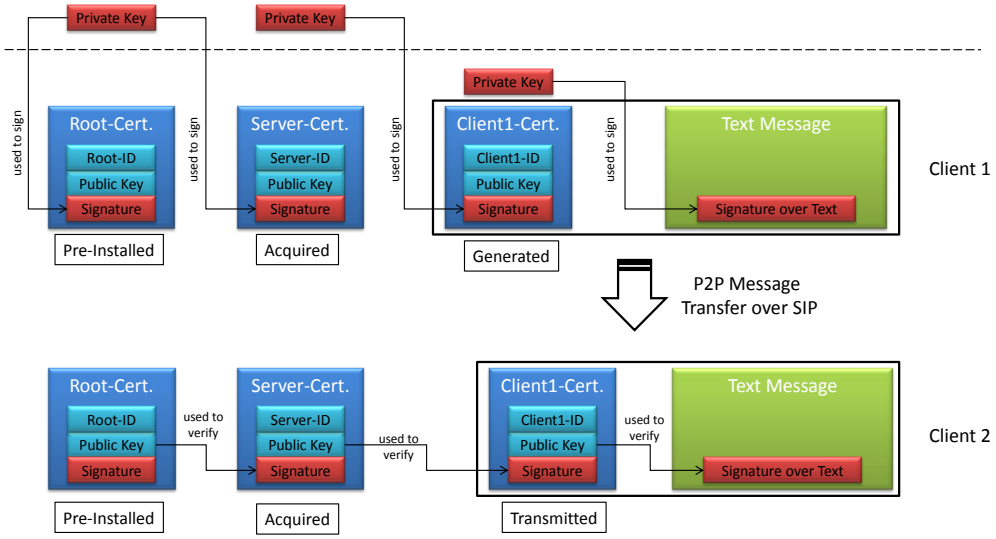

Figure 3: Relation between Certificates and Messages

The relation between the certificates and their use in order to enable authentic message exchange is depicted in Figure 3. In every transaction there is either a certificate or signature being transported between the entities.

For the **initial certificate provision** the P2P-Authentication module in VITAL++-application server (AS) will process the registration request and supply the newly registered user with its server certificate, signed by the common Root-CA,

For the **client certificate authorization** it generates its personal private-public key-pair and creates an unsigned certificate with its identity and public key. This is then sent to the VITAL++-AS, which checks the identity and other fields of the certificate before he signs it with his private server key. The signed certificate is then sent back to the client, which stores it as its own personal certificate. Then, the client owns a valid certificate verifiable by every instance, which also knows the server certificate. As this process is vulnerable against a man-in-the-middle attack, it is advised to encrypt this transaction. For that purpose, we suggest a Diffie-Hellman key agreement transaction before the main transaction in order to establish a common secret knowledge, which is then used to generate a symmetric key for message encryption.

For the **client-to-client message authentication** the sender creates a text message, which he signs with his private key, which corresponds to its own client certificate. He then sends the text message along with his client certificate and the message signature to the receiver. This one can then first check the authenticity of the client certificate using its server certificate, followed by checking the message signature with the public key from the client certificate and inform the user accordingly.

2.2. Content Security CS-SA

The CS-SA provides the VITAL++ platform with Digital Rights Management (DRM) functionality. It provides block and stream encryption features so content can be distributed throughout overlays in encrypted form. A licensing feature enables users to obtain a decryption key in order to play the multimedia content. Content providers can create rules describing when, to whom, where and how their content can be licensed and how much it will cost to do so.

The IMS subscriber identity of the licensing user is used to identify the user meaning that over-simplistic access restrictions such as geo-blocking of IP's need not be applied. This addresses a requirement of national and regional broadcasters within several EU countries to provide free services to citizens of those countries, even if they are travelling abroad.

The process of **licensing** a piece of **content** follows a Request/Response model and uses the SIP Instant Messaging conversation mechanism defined by the 3GPP. The content licensing process is orchestrated using a "Licensing Conductor", implemented to the design specified by the Open Media Commons [10] group. The licensing process is described graphically as a web-service workflow which orchestrates the flow of information between services s used by the licensing process; authentication, content transcoding and accounting.

Licensing rules are encoded in text-based policy statements *(e.g. if <condition> then <rule>)*, according to the specifications of the Drools rules engine [11]. The content provider registers licensing rules with the CS-SA. These rules can be parameterized and hence associated with individual users, user groups, content types, network context (e.g. user location) and billing scenarios (e.g. pre-pay, post-pay). The content provider, acting as a licensee, may programmatically allow content to be distributed under a "fair-use" license for education, criticism or parody. The licensor must explicitly assert their intentions to make fair use in their licensing request.

For the **Identity Management** functionality The CS-SA uses PKI to mutually authenticate content provider and content consumer. The CS-SA acts as a trusted intermediary meaning that the content consumer and provider do not have to interact directly in the licensing process. This is necessary as the content is super-distributed among peers in the overlay. Mutual authentication means that the content consumer can be confident the licensed content is being licensed from the correct provider and hasn't been tampered with. The content provider similarly benefits from IMS Authentication and PKI being used to identify the consumer. A Certificate Authority (CA) is used to associate public-private key pairs with IMS identities.

The **Accounting** subsystem facilitates micro charging for content items. Charging Detail Records for individual content items are produced during the licensing process by the CS-SA. The Accounting subsystem aggregates these with CDR's produced by IMS network elements involved in the transport of the licensed content to the subscriber. The IMS charging data is obtained from an IMS Charging Gateway Function (CGF) using the Diameter protocol in line with the relevant ETSI & 3GPP specifications.

A **Billing and Rating Function** (BRF) generates a user bill showing the charge for the item, the associated network utilization charges and an incentives-based discount

arising from good overlay behavior using statistics provided by the Overlay Manager. Arbitrarily complex charging schemes may be created using spreadsheets which are then loaded into the system. An earlier version of this technology is described in [12] and further developed in [13].

2.3. Overlay Management SA

The objective that we fulfill through the OM-SA is the creation and the maintenance of a scalable system, in terms of participating peers, through the distribution of this its management and organization process to them. Additionally we focus on adapting the system to dynamic peer arrivals and departures and continuously reorganize it according to them. Special attention has been given to the adaptation of Content Diffusion Overlay (CDO) to the dynamic network conditions and exploitation of network locality in the selection of neighbors from each peer. Finally innovative algorithms have been designed and run in the CDO that deploy a graph structure that ensures the maximization of the utilization of upload bandwidth contributed by highly heterogeneous participating peers.

The CDO graph structure (Figure 4- left) consists of two interacting sub graphs. In the first graph we insert only peers (class 1 peers) that their upload bandwidth exceeds the bit rate of the service rate that our system has to sustain while in the second we insert the rest (class 2 peers). These two graphs are constructed in such a way that all nodes have an equal number of connections. The interconnection between two graphs is done with connections that the class 1 peers create in order to provide peers of class 2 with additional upload bandwidth resources. The number of these connections is analogous to the upload bandwidth of class 1 peers. These connections are assigned uniformly in peers of class 2

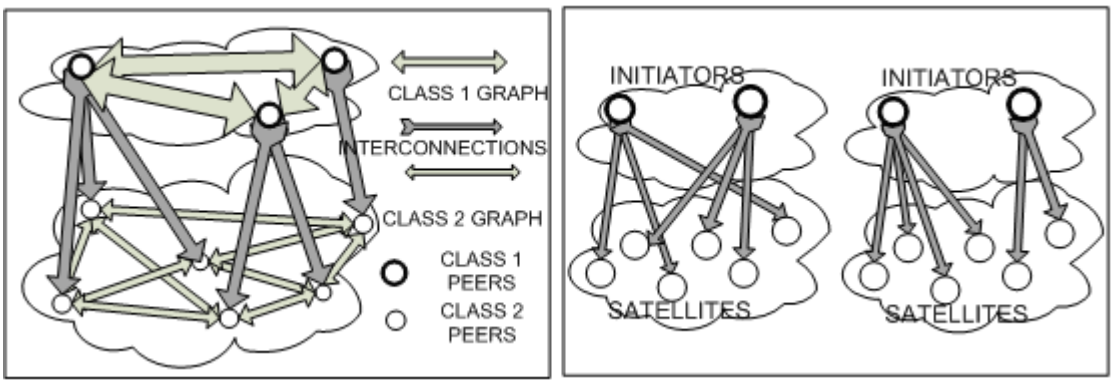

Figure 4. Left- The graph structure of the CDO, Right – Execution of DOMA

In both graphs, all the peers periodically execute a distributed optimization and maintenance algorithm (DOMA) that reorganizes the “neighborhoods” of CDO in order to keep the structure of the graph optimal for content delivery even during peer arrivals and departures. The algorithm makes use of an “energy function” that captures the impact of specific parameters e.g. network latency, between any two nodes in the overlay. DOMA is executed between two neighbors that we note as

initiators and their direct neighbors that we call satellites. Its purpose is to minimize the overall sum of the energy functions between initiators and satellites under the constraints on the number of neighbors that the aforementioned graph structure implies. In Figure 4 (right) the length of the arrows expresses the value of the energy function. The one initiator in the left figure has more bandwidth than the other. We observe that the execution of DOMA minimizes the sum of energy functions while it reassigns the number of neighbors according to their upload bandwidth resources.
Every change in the underlying network, in the resources of a peer, peer arrivals and departures or execution of DOMA in neighboring nodes triggers new changes in the CDO while it always converges to the desired graph structure and to a minimized sum of energies [6].

2.4.Content Index SA

In our proposed system content indexing is used not only for accelerating the content searching process, but also as a tool for content publication, together with content description information. CI-SA is implemented using a SIP Instant Messaging mechanism and offers the following services:

- **Content Publication** that can be used by IMS users interested in offering content. The service works by declaring content availability to the network that may be fed to the users through the CI-SA. Context searching and download is possible from third-parties by executing network search on the basis of content description information publicized along with the content.
- **Content Searching** whereby users looking for particular content are browsing other users' publicized content on the basis of certain criteria. These criteria are submitted to the CI-SA and the result is fed to the requesting users as a list of descriptions of available content items. The list also contains matching criteria, which are used as filters against relevance of the result for presentation to the user.
- **Overlay Bootstrapping/Maintenance.** Whenever a VITAL++ user enters the system they contact the CI-SA, in order to be able to acquire content indexing information. For this purpose, once the user has selected a specific content item to be retrieved and reproduced locally, this has to be communicated to the CI-SA. In this case the CI-SA interacts with the OM-SA in order to either create a new overlay or to update an existing one. In any case the outcome of the OM-SA, which is a list of peers per overlay member, is sent either to a newly added member of an overlay or to an existing member for which the list of its peers has been updated.
-

2.5.QoS SA

The QoS-SA is responsible for dynamically provisioning the correct amount of bandwidth resources for the uninterrupted distribution of each object. It is comprised

of two components: the monitoring component and the resource allocation component.

The **monitoring component** is responsible for monitoring the resources of each CDO and for calculating the additional bandwidth needed for the uninterruptable object delivery. A server samples periodically a small subset of the participating peers from CDO and calculates the mean of their incoming flows in bytes and the mean of the time in which they were transmitting content during that period. The attributes of P2P-BESA are useful for a very good approximation of the average value of upload bandwidth that sets of peers in a CDO have. Using these values, the monitoring component is able to calculate the average upload bandwidth of the peers and thus the minimum additional bandwidth, if needed.

The **resource allocation component** uses a set of bandwidth provisioning servers, which can control the upload bandwidth. These have been designed to comply with ETSI's Resource and Admission Control System (RACS) functionality, first defined in the 2006 release of their NGN specifications [8]. Having as input the output of the monitoring component, the QOS-SA provisions the excess bandwidth that is required in such a way that each server is connected with peers, which belong to the same ISP (if possible) in order to minimize the inter-ISP traffic.

3. VITAL++ functionality for live streaming

When using the VITAL++ platform in a live-streaming scenario, each multimedia stream generated by individual users and/or content providers is divided into blocks and distributed by overlay CDO. A P2P Block Exchange Scheduling Algorithm (P2P-BESA) – also part of the VITAL++ client -ensures the distribution of each block to every user that requests the specific multimedia stream with low latency. This latency is known as setup time and it is defined as the time interval between the generation of each block from the stream producer and its delivery to every participating peer. An efficient P2P-BESA has to maximize the delivery rate of the multimedia stream with respect to the participating peers uploading capabilities while ensuring the reliable delivery of the stream in the presence of dynamic conditions such as batch peer arrivals and departures, dynamic network latencies and path bit-rates.

Neighbors in the CDO periodically exchange the set of blocks that they have. Each receiver exploits this information and proactively requests blocks from its neighbors in the CDO in order to: a) avoid the duplicate block transmissions from two peers, b) eliminate starvation of blocks and c) guarantee the diffusion of newly produced blocks and/or rare blocks in a neighborhood. In contrast, each sender every time that it is ready to transmit a new block examines the set of blocks that its neighbors have and using as criteria the most deprived neighbors (miss the largest number of blocks) and neighbors with high capabilities of upload bandwidth selects one of them and transmits to it a block.

Graphs in Figure 5 depict the performance of our system. In the left graph we demonstrate the CDF of average network latency with their neighbors ("energy" required for transmission) that peers have in a randomly formed overlay and one built

by our CDO, noted as Liquid stream. We observe a reduction of energy by approximately 90%.

In the right graph we depict the CDF with the percentage of the successful block transmissions that each peer that participates in our system has. We mention here that the video streaming rate is 95% of the average upload bandwidth of the participating peers and the latency between the generation of a video block and its distribution in every peer in the system is 4 seconds. Through these graphs we observe the optimal and stable delivery of a video (right graph) while simultaneously our system minimizes the traffic that it introduces in the underlying network (left graph).

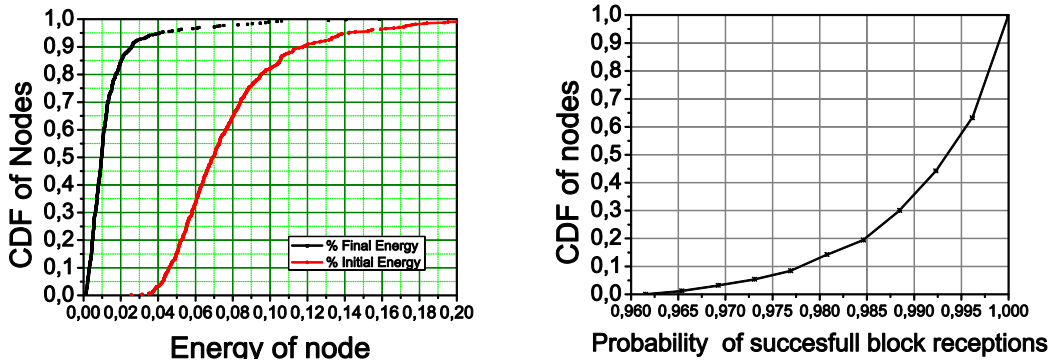

Figure 5. Left:CDF of the average netowrk latency, Right: CDF of the succesful block receptions

4. Conclusions

In this work we have described an overview of a novel architecture that combines the benefits and features of NGN technology like IMS and P2P in order to deliver content in a secure and efficient way. To the best of our knowledge this is the first attempt to provide a holistic operational solution. Introducing P2P allows for scalable, adaptable and resource optimal content distribution. When combined with NGN operations and procedures, it produces a system that is secure and reliable, properties that are currently lacking in common P2P systems. NGN in turn benefits from reduced resource management and signaling overhead when P2P-optimisation is incorporated within the data transport function. We are currently completing implementation of the architecture and the VITAL++ client and we are about to start large-scale experimentation with real users.

Acknowledgements

This work is funded from the European project VITAL++ with Contract Number: INFSO-ICT-224287.

5. References

[1] CNET, Streaming Video to outpace P2P Growth (referencing Cisco Visual Networking Index Forecast 2009-2014), http://news.cnet.com/8301-30686_3-20006530-266.html

[2] Ipoque, Internet Study 2008/2009, http://www.ipoque.com/resources/internet-studies/internet-study-2008_2009

[3] IETF, Application Layer Traffic Optimisation (ALTO) Working Group, http://datatracker.ietf.org/wg/alto/charter/
[4] ITU-T, IPTV Focus Group Proceedings, 2008
[5] http://www.ict-vitalpp.eu/
[6] N. Efthymiopoulos, A. Christakidis, S. Denazis, O. Koufopavlou, LiquidStream – Network dependent dynamic P2P live streaming, Springer, Peer-to-Peer networking and applications, vol. 1, no. 1, Jan. 2011
[7] J. Fiedler, T. Magedanz, J. Mueller, "Extending an IMS Client with Peer-to-peer Content Delivery", Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2009, Volume 7, pp. 197-207
[8] ETSI, ES 282 003 Ver. 1.1.1, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN);Resource and Admission Control Sub-system (RACS);Functional Architecture, June 2006D.
[9] Wu, Y. Liu, K.W. Ross, Queuing Network Models for Multi-Channel Live Streaming Systems, IEEE INFOCOM, Apr 2009, pp. 73 – 81
[10] Sun Labs, Open Media Commons, web: http://www.openmediacommons.org
[11] JBoss Community, Drools Business Logic Integration Platform, web: http://jboss.org/drools
[12] Brazil J.de Leastar, E. Ryan, C. Foghlu, M.O, "Workbook approach to algorithm design and service accounting in a component orientated environment". IEEE Workshop on IP Operations and Management. Dec. 2002, pp. 44-48
[13] B. Jennings, P. Malone, "Flexible Charging for Multi-provider Composed Services using a Federated, Two-phase Rating Process", IEEE/IFIP Network Operations & Management Symposium, NOMS 2006, New York, pp. 13-23

Author CVs

Athanasios Christakidis (schristakidis@ece.upatras.gr) received his degree of Electrical Engineer in 2004 and his PhD in the field of distributed network systems in 2010 from the University of Patras, Greece. He has participated in various IST projects and has been a co-author in a number of papers since 2004 in the areas of P2P systems. His current work involves further research in distributed video streaming, content distribution networks and distributed storage systems as well as the development of distributed algorithms towards the realization of an actual P2P client.

Nikolaos Efthymiopoulos (nefthymiop@ece.upatras.gr) was born in 1980. In 2010 he received his Phd from University of Patras, Greece. Sicne 2007 he was a Lecturer in Telecommunications Systems and Networks Department and now he works as an Assistant Professor in Informatics &MM Department in Greece. His main research interests are network optimization, distributed video streaming, distributed searching and achieving QoS in content distribution networks. He has around 15 publications in these areas. He has participated in various IST projects since 2004.

Jens Fiedler (jens.fiedler@fokus.fraunhofer.de) finished his diploma in computer science in October 2004 at the Technische Universität Berlin (TUB). Since May 2005 he works as a researcher at the Fraunhofer institute for open communications systems - FOKUS in the competence center for next generation network infrastructures - NGNI. His expertise includes knowledge in several programming languages, e.g. C/C++, Java.His core competences are VoIP Infrastructures, High Availability, Reliability and Scalability in VoIP Infrastructures, Peer-to-peer technologies, P2P integration and general network protocols. He worked in projects like 6NET, SNOCER, VITAL++ (FP7). He is currently involved in several industrial Evolved Packet Core related projects.

Shane Dempsey (sdempsey@tssg.org) is Next Generation Network (NGN) Architect within TSSG. He graduated with 1st class honours in Industrial Computing from WIT in 1999 and went on to obtain an MSc in Telecoms in 2001. His research interests include AAA for composed services, SOA tools for telecoms and financial software. He has published papers in these areas, contributed to research commercialisation initiatives and served as a technical committee member of several conferences.

Konstantinos Koutsopoulos (k.koutsopoulos@bluechip.gr) received the degree of Electrical Engineer and his PhD in the field of Personal and Mobile Telecommunications from the National Technical University of Athens. He has participated in various IST projects since 1998. He has experience in mobile communications, security, networking and software development. His research interests include networking, embedded systems, security and software techniques. He has been working for BCT since March 2006.

Spyros Denazis (sdena@ upatras.gr) received his B.Sc. in Mathematics, University of Ioannina, Greece, in 1987, and in 1993 his Ph.D. in Computer Science, University of Bradford, UK. He worked the European industry for 8 years and he is now an assistant professor at the Department of Electrical and Computer Engineering, University of Patras, Greece. His current research includes P2P, and Future Internet. He works in PII, VITAL++, AutoI EU projects. He has co-authored more than 40 papers.

Spyridon Tombros (s.tompros@creativese.eu) Electrical, Electronics Engineer received his PhD in broadband communications from the National Technical University of Athens and his Master on the same faculty from university of Patras. His research interests are in the field of protocols and physical communication systems design for mobile, wireless and home networks. He has many years of working experience on network testfloors and test tools manufacturing and over 30 scientific publications and book contributions in the same area.

Stephen Garvey (sgarvey@tssg.org) has a B.Sc. (Hons) in Software Development, a H. Dip in Business Systems Analysis and is currently completing a M.Sc. in Distributed Computing. Stephen has over a decade worth of experience in the ICT sector having worked for several multinational technology in a variety of roles such as information architect, software engineer, technical lead etc. As well as running his own software development and consultancy business he was also chief architect and engineering manager for Nubiq Ltd. He is now involved in NGN research within the TSSG.

Odysseas Koufopavlou (odysseas@ece.upatras.gr) University of Patras, Greece.From 1990 to 1994 he was at the IBM Thomas J. Watson Research Center. He is currently Professor with the Department of Electrical and Computer Engineering, University of Patras. His research interests include computer networks, high performance communication subsystems architecture and implementation, VLSI. Dr. Koufopavlou has published more than 200 technical papers and received patents and inventions in these areas. He has participated as coordinator or partner in many Greek and European R&D programmes.