Integrating P2P with Next Generation Networks

Athanasios Christakidis[2], Jens Fiedler[1], Nikolaos Efthymiopoulos[2], Konstantinos Koutsopoulos[4], Evangelos Markakis[5], Stephen Garvey[3],Spyros Denazis[2], Spyridwn Tombros[2], Shane Dempsey[3], Evangelos Pallis[5], Odysseas Koufopavlou[2]

[1]Fraunhofer Fokus, Berlin, Germany
[2]Electrical and Computer Engineering,University of Patras, Greece
[3]Waterford Institute of Technology, Waterford, Ireland
[4]Blue Chip Technologies S.A., Athens, Greece
[5]Centre for Technological Research of Crete

Contents

1

Integrating P2P with Next Generation Networks

This chapter 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 are then used to support multimedia applications and content distribution services. To this end, P2P is enhanced with advanced authentication, DRM mechanisms while NGN benefits from the enhanced scalability, reliability and efficient distribution of service and content 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.

1.1 Introduction

The widespread adoption of the Internet technology in daily life as a major communication medium has led to the emergence of a plethora of e-applications some of which have already become more popular than the conventional telephony. Assisted by the wider roll-out of broadband communications technologies, Internet and its use has elevated digital communications to higher levels and made audiovisual communications, such as content distribution, digital TV, video on demand affordable for everyone and mainstream among the Internet applications of today. Among them computer based applications like the TVtube, Skype and Music City, offer rich-content to users, in real time with acceptable quality, making use of sophisticated peer-to-peer (P2P) technology algorithms for content tracking, downloading, synthesis and playback. 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 creating new challenges in network and service management, configuration, deployment, protocols etc. **P2P is primarily an**

end-users' technology that fosters self-deployment and self-organization while it achieves optimized resource utilization for the deployed applications and services. In other words P2P technology has succeeded where QoS mechanisms have failed being deployed and operating at large scales.

On the other hand, latest trends in telecommunication networks have led to the emergence of the first version of converged IP communication platforms known as Next Generation Networks (NGN). AN initial instance of NGN is the IP Multimedia Sub-system (IMS). IMS networks constitute fully-fledged IP networks offering, in contrast to Internet communications, quality-controllable fixed, mobile and wireless links. With IMS, users is said to be able of making ubiquitous use of operator services using 3G UMTS, WiFi and PC-based terminals. **IMS is a control plane technology that primarily addresses issues of heterogeneity of access technologies, addressing schemes, AAA, security and mobility management from an operator's perspective**.

In so far, these two seemingly competing technologies, NGN and P2P have been deployed independent of each other thus failing to mutually exploit their strengths towards creating a new and more powerful paradigm.

When comparing IMS and P2P [2], we compare two inherently different worlds. IMS as a technology for controlling media flows, administering subscribers and controlling access to services, both operator-services and third-party. IMS is a highly centralized architecture, which business goals such as manageability, security and charging. P2P technologies on the other side have been designed to be scalable, adaptable, and failure resilient, mainly for the distribution of media (files, streams). Figure 1.1 illustrates the complementary features of both technologies, which are discussed in the following.

As already mentioned, scalability is one of the biggest features of P2P networks, while scaling up an IMS core network can only be done by means of laborious configuration operations that increase the management overhead. P2P networks usually have no single point of failure as they are self-healing, while e.g. the HSS is a single point of failure for an IMS network. In a P2P network, users are often the only content providers, while this concept is not supported in the IMS, which clearly distinguishes between consumers and service providers. 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, as e.g. an I-CSCF may be flooded and put out of service for all users. Access to a P2P network can be considered easy, as there is no access control in open P2P networks. Nevertheless, password- controlled P2P

	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 1.1 IMS vs. P2P comparative overview

solutions exist, but none of them are standardized. Access to an IMS and its services is quite complex, as cryptographic mechanisms need to be deployed for even the simplest access. Additionally, each user must be provisioned and its profile, which is stored in the HSS, must be maintained.

But in the direct comparison, IMS does not only have disadvantages against P2P technologies. The complexity of access results in a much better security situation among IMS users due to the AAA management in the IMS core network for all users. Due to the fact that IMS is located in an operator network, it can also access network topology information in a standardized way from a Network Attachment Sub-System (NASS)[1]. This information must be estimated or measured in a pure P2P overlay and therefore the incorporation of information from a NASS will result in a better and more efficient overlay if presented to an overlay construction algorithm. IMS is a standardized architecture with standardized network protocols and functions, which makes development for an open market possible, while P2P overlays are usually dictated by the associated piece of software. For the same reason as for topology awareness, IMS components can influence the data paths between users and service nodes in terms of bandwidth (resource reservation), which is completely unthinkable for any pure user driven P2P network, as user nodes cannot influence routers in any of the involved networks. P2P

[1] ETSI, TISPAN Release 1 Architecture, Dec 2005

systems usually need to provide remarkable efforts, up to dictating the architecture of the overlay, in order to make clients communicate with each other which are behind a NAT. In the IMS, the P-CSCF has the task to deal with NATed[2] users (proxy, holds pinhole open, all communication goes through the P-CSCF). Last but not least, the probably biggest advantage of IMS is the easy way to deploy new services, which is very expensive in a P2P system, as a P2P system is usually designed directly on the use case (e.g. file sharing).

This chapter describes the VITAL++ architecture [4] which is the result of **combining and experimenting with the best features of the two worlds, namely, IMS-like control plane functionality and P2P technology**. This has given rise into a combined communication paradigm that brings benefit to both users and operators and makes multimedia applications readily and securely available.

1.2 Use Cases as motivation

The combination of P2P with NGN/IMS technologies opens numerous possibilities, a few of which will be described in this section. These are based on use cases implemented in the Vital++ IST project[3]

The first use case is Remote Services Access (Geo-Blocking).Due to licensing policies AV Content on the internet is often geo-blocked, i.e. only available in certain areas. This, however, excludes users who have paid their broadcast licence fees but happen to be temporarily outside the geographic area where they live and pay their fees.

With IMS technology, viewers can be enabled to consume content they have a right to access wherever they are. A suitable area of application would be the streaming AV (IPTV) offers by national public broadcasters, which could then be made available for all rightful viewers anywhere throughout Europe. As these public broadcasters by law and regulation often cannot pay for distribution outside their business area, the use of P2P technology may be very useful to reduce costs for content distribution.

The second use case is Content Distribution in Rural Areas. In some remote rural areas, served by satellite connections or radio access, the use of P2P technologies can improve the way operators serve multimedia on-demand content. In a rural area where a number of users are connected to

[2] IETF, RFC 2663 - IP Network Address Translation (NAT) Terminology and Considerations, Aug 1999, web: http://tools.ietf.org/html/rfc2663

[3] ICT-Vital++ Project website, web: http://www.ict-vitalpp.upatras.gr

a broadband network using a number of satellite accesses the same content may be forwarded at different times at several satellite accesses using a high amount of bandwidth. This scenario can be improved if subscribers are connected to a local area network (wired, WiFi, etc.) and share one satellite access.

The network operator can improve the use of the expensive and scarce bandwidth satellite access using a P2P approach. This approach can be a user P2P, where a user serves contents to other users or even an operator P2P, where every on-demand content requested by a user to the network is stored at a local element belonging to the operator. In both cases, when a second remote user asks for the same content, it is distributed from the local broadband network, instead of using the satellite access time and again.

Another use case is Science Video Blog. The architecture and functionality of VITAL++ enables the creation of a video pool for science communication. Individual institutions could connect with others - whether inside a closed group like Fraunhofer Gesellschaft or between free, individual organizations sharing interest in a certain topic - and share information on the latest developments and findings.

Such an application would not require much of an elaborate GUI design but rather should be based on decent metadata handling to ensure that interested community users will find what they are interesting in.

The fourth use case is Personalized Radio and Video Service. As a demonstrator for the usage potential of combining P2P and IMS technology, the VITAL++ consortium developed a demonstrator application which empowers a personalized radio experience way beyond broadcast radio programmes. This service, SoftMix, will be described further down below.

1.3 VITAL++ architecture: An Overview

The VITAL++ architecture has been derived from several major design criteria, which are:

1. Minimal modification of standardized functions.
2. Easy to deploy into existing IMS networks.
3. A high-degree of extensibility.
4. Security for media and user data.
5. Optimal overlays with intelligent path management.

From these design aspects, it has been decided to position IMS sided functionalities of the VITAL++ architecture in an application server; while the

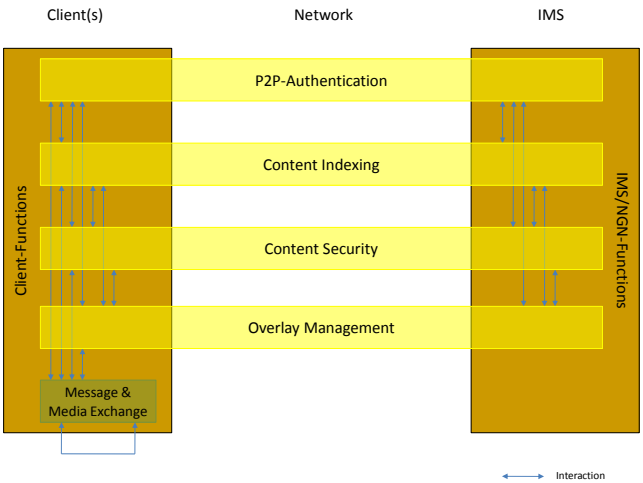

Figure 1.2 VITAL++ abstract view of the overall architecture

client sided functionalities are located directly in the client so that no additional nodes become necessary. Figure 1.2 illustrates an overview over the architecture and its functional blocks, which are explained in the remaining sections of this work.

In order to address the VITAL++ challenges, a number of Sub-Architectures (SA's) that interact with each other have been defined, each one responsible to address specific design criteria. These are the P2P Authentication sub-architecture (P2PA), the Content Index sub-architecture (CI), the Content Diffusion Overlay sub-architecture (CDO) and the Content Security sub-architecture (CS). Each sub-architecture spans across the client, the network and the IMS with its components. Sub-architectures may interact with each other in an arbitrary way, especially in the client, while on the NGN side there need to be well defined interfaces. Thus the media exchange is not entitled as sub-architecture, but it interacts with these and itself in the same as well as in remote clients.

Peer-to-peer Authentication (P2PA) SA is responsible for enabling clients (peers) to authenticate messages, which they receive in order to ensure that clients know who has really created the message. This is a basic requirement in order to enable secure P2P messaging. Based on this, additional features can be introduced, like a secure DHT or authentic media streaming, etc.

The content index (CI) SA has three major objectives. Firstly it allows the publishing of a content item from users and content providers, enables queries for items that our system maintains and distributes, acts as a tracker and provides the initial insertion of a peer to the overlay that distributes the items that it requests.

Content Diffusion Overlay (CDO) SA is a graph that participating peers dynamically form and maintain by selecting each one of them 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 in 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 their content using a Digital Rights Management technology. Vital++'s DRM system took its requirements from network operators and a content provider participating in the Vital++ IST project. In this context it answers real-world business issues required for commercial exploitation of the Vital++ platform such as charging and billing. More specifically, the requirements range from Identity-based conditional access to streaming content (providing a better alternative to Geo-Blocking), encryption of file-based and streamed content where appropriate, flexible rights expression, integration with micro-charging accounting, respect for privacy and consumer rights and an innovative explicit support for fair-use assertions such as backup/critique/education.

1.3.1 P2P-Authentication Sub-Architecture

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 the VITAL++ scope, 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

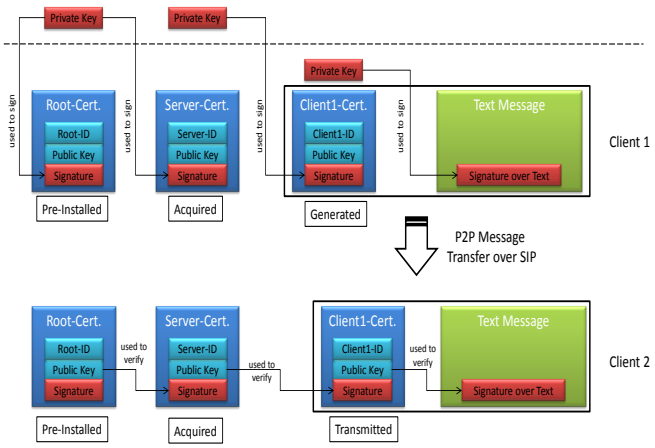

Figure 1.3 Relation between Certificates and Messages

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 in the following paragraphs.

The relation between the certificates and their use in order to enable authentic message exchange is depicted in Figure 1.3. In every transaction there is either a certificate or signature being transported between the entities. Both are encoded as XML documents and attached as a MIME multipart message to the corresponding SIP message.

Initial certificate provision: The P2P Authentication module in the VITAL++ AS will process the registration hint from the S-CSCF and supply the newly registered user with its server certificate, signed by the common Root-CA, as illustrated in figure 1.3.

Client certificate authorization:The client hereby generates its personal private-public key-pair and creates an unsigned certificate with its identity and public key. This is then being 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 being sent back to the client, which stores it as its own personal certificate. After performing this transaction, the

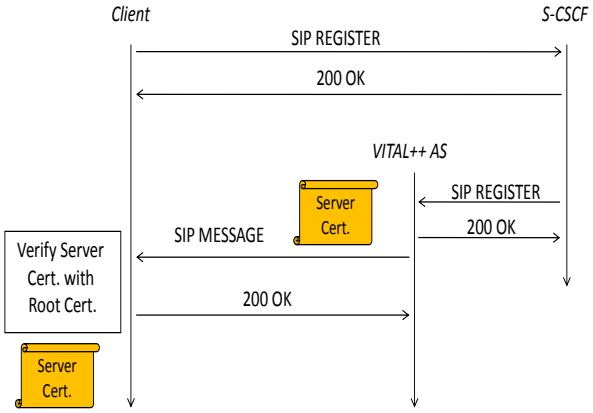

Figure 1.4 Initial server certificate acquisition.

client owns a valid certificate verifiable by every instance, which also knows the server certificate.

The client hereby generates its personal private-public key-pair and creates an unsigned certificate with its identity and public key. This is then being 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 being sent back to the client, which stores it as its own personal certificate. After performing this transaction, the client owns a valid certificate verifiable by every instance, which also knows the server certificate.

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 its own 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.

1.3.2 Content Security SA

The Content Security Sub-Architecture (CS-SA) is implemented as a SIP Instant Messaging based service. The CPS is integrated within the IMS network as shown in Figure 1.5.

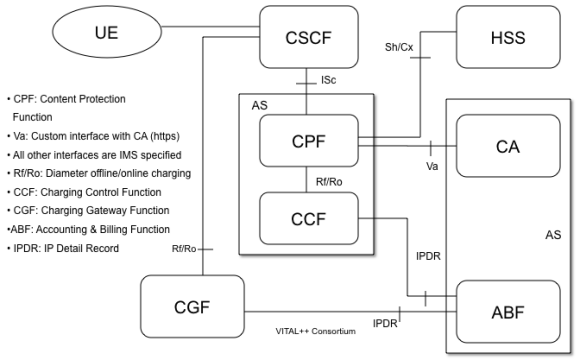

Figure 1.5 CPS integration within the IMS.

The User Equipment (UE) here represents a Vital++ node. The node accesses the functions of the Content Protection Function, the logic of the Content Security Sub-Architecture) using the IMS ISc interface. The ISc is a SIP protocol connection that is used when the S-CSCF loads a trigger point corresponding to the message that has been presented to it. In our case the message is matched based on a known ”service indentifier” e.g. content-protection@vital-domain and the Vital++ SIP header that is added to all Vital++ messages.

Licensing Content: 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. By re-using an existing mechanism we rely on the standard IMS authentication and message security mechanisms.

The Content Protection Function (CPF) is deployed within a standard IMS application server corresponding to the Java Community Process’s JSR 289[4] specification. The CPF may additionally use the HSS to verify a subscriber’s credentials using the Sh interface (profile information).

The content licensing process is orchestrated using a ”Licensing Conductor”, implemented to the design specified by the Open Media Commons[5] group. In realizing this implementation, the Java Business Process Manage-

[4] JSR SIP Servlet v1.1, http://jcp.org/en/jsr/detail?id=289

[5] Open Media Commons, http://www.openmediacommons.org

ment (JBPM) open source workflow management engine was chosen to describe the licensing process. AS denotes an Application Server hosting the specified node in the CP-SA.

Identity Management: Similar to the P2P-SA, the CPF uses Public Key Infrastructure (PKI) to mutually authenticate content provider and content consumer. The CPF 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.

Business Rules: The Drools Expert[6] rules engine is used to process business logic encoded in text-based rules. The content provider registers licensing rules with the Content Security Sub-Architecture. 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). For example: the following is true if the subscriber has a prepay account and their account balance is sufficient to afford the content item.

$$\text{Subscriber(Account\_type == ”prepay”) \&\&}$$
$$\text{Subscriber(account\_balance)} \geqslant \text{Content(cost\_estimate)}$$

Figure 1.6 shows how request handling, rules processing and accounting are integrated within a single workflow following the Service-Oriented principle of ”loose coupling” [7].

Integration with Accounting:The Accounting subsystem consists of elements including:

- A Charging Gateway Function (CGF) - An IMS charging gateway for storing usage data. The CFG exposes a diameter interface to switching and application server nodes.
- ” An Accounting and Billing Function (ABF) - A flexible and highly scalable accounting system based on spreadsheet worksheets. The ABF

[6] Drools Expert - Jboss Community, http://www.jboss.org/drools/drools-expert.html
[7] Kaye D. ”Loosely Coupled - The missing pieces of the web”, RDS Press, 2003

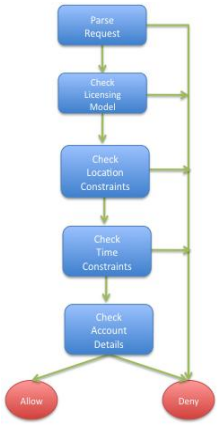

Figure 1.6 Licensing Workflow.

has a web service interface. It receives usage data in the IP Detail Record (IPDR) XML format and responds with an XML rating document. The rating document may be transformed into a customer bill for service and network usage.

- A Charging Control Function (CCF) - A rules-based charging decision function that evaluates whether a service can be provided to a particular user based on their charging profile and that of the service. E.g. The service may require ”post-pay” and the user account may be ”pre-pay” only. The CCF is implemented using JBPM workflows.

The ABF within the Accounting system associates a charging worksheet with a service or content provider and the service or content being provided. The worksheet describes additional logic for special tariffs to incentivise good behavior on the overlay e.g. relaying content. We have adopted the extensible XML-based IPDR (Internet Protocol Detail Record) Network Data Management-Usage (NDM-U)[8] scheme for charging data.

[8] ipdr.org. Network Data Management Usage (NDM-U) for IP-based Services, version 3.1.1 edition, October 2002.

1.3.3 Content diffusion P2P overlay (CDO) SA

The objective that we fulfill through the architecture of the CDO 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 graph to dynamic peer arrivals and departures and continuously reorganize it according to them. Special attention has been given to the adaptation of 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 CDO that deploy a P2P overlay graph structure that ensures the maximum of the utilization of upload bandwidth contributed by highly heterogeneous participating peers while a newly-designed p2p block scheduler exploits the properties of the P2P overlay in order to uniformly distribute the sum of the upload bandwidth resources to every participating peer.

The P2P overlay graph structure (Figure 1.7- 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 class 1 peers create in order to provide peers of class 2 with additional upload bandwidth resources. The number of these connections is proportional to the surplus of upload bandwidth of class 1 peers. This surplus is also assigned uniformly in peers of class 2.

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. It also ensures high levels of bandwidth utilization. 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 called 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 1.7 (right) the length of the arrows expresses the value of the energy function. The one initiator in the left figure has surplus bandwidth twice as much as the other. We observe that the execution of DOMA minimizes the sum of energy functions while

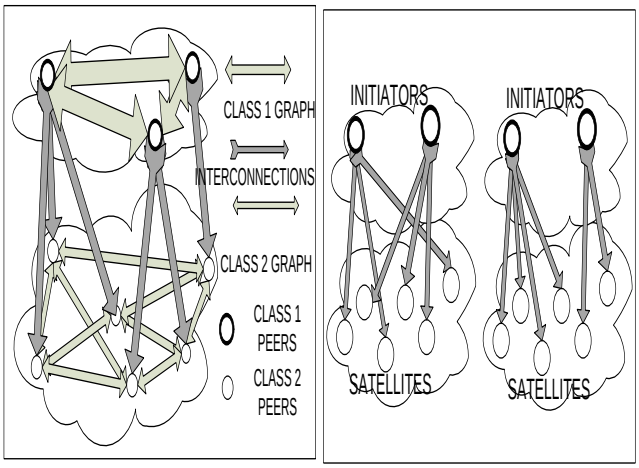

Figure 1.7 Left- The graph structure of the CDO, Right - Execution of DOMA.

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 CDO while it always converges to the desired graph structure and to a minimized sum of energies[1].

1.3.4 Content Index SA

In IMS networks, context indexing is used for distinguishing calls with respect to requested content type. Quite often in commercial P2P services content indexing is used not only for accelerating the content searching process, but as a tool for content publication, together with content description information.

In the scope of the VITAL++ network, content indexing is defined as a Sub-Architecture (CI-SA) implemented as part of the SIP Instant Messaging standard[9] and offering the following services:

- **Content Publication**: The content publication service can be used by IMS users interested in offering content. The service works by declar-

[9] Campbell B. [et al.], RFC 3428 - Session Initiation Protocol (SIP) Extension for Instant Messaging, IETF, Dec 2002.

ing 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**: Content searching is the basic service offered , 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**: Contrary to the regular session setup process of IMS, whereby connection parameters are negotiated during bearer set-up, the Vital++ client has to join P2P overlays well before this process takes place, 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 Overlay Management SA (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.

1.3.5 VITAL++ client architecture: An Overview

The terms "Client" and "Peer" are used equivalently in this document as they refer to the same thing. The VITAL++ client is a hybrid client. This means it is an IMS client and a P2P client at the same time. The IMS functionalities are used to mainly interact with an IMS core or system for exchanging control information, while the P2P part is used to exchange content with other peers.

The components of the client are directly derived from the necessity to interact with other clients and the IMS core in order to fulfill the envisaged features. Figure 1.8 illustrates the functional blocks inside the client. These are the content manager, which is responsible for publishing and discovering content as well as triggering DRM operations via the client DRM module if a license needs to be obtained. The authentication module obtains and manages certificates of VITAL++ entities (clients, application servers, root-

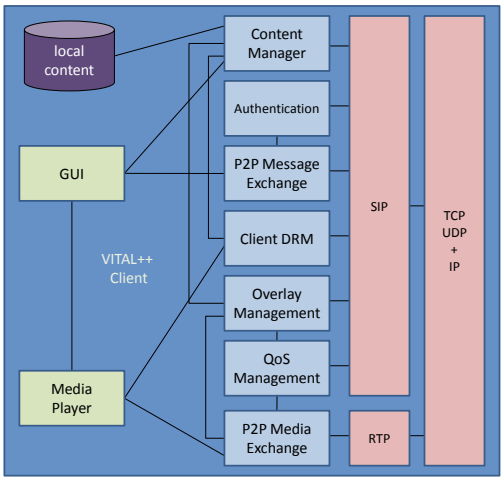

Figure 1.8 Client functional blocks.

certificate). It interacts mainly with the P2P message exchange in order to sign and verify messages. The latter has the purpose to exchange P2P messages with other peers for generic purposes (i.e. playlist exchange, etc.). The overlay management module obtains overlay changes from the application server and re-organizes its neighborhood accordingly, also to respect to QoS requirements, issued by the QoS management module, which can also realize QoS enforcement via NGN mechanisms. Also standard IMS client functionality is realized (not depicted) for initial IMS registration and IMS session management.

The platform side of the architecture consists of four application server entities, which can be co-located in the same box (as depicted), or distributed over several machines. The communication with the client occurs mainly through the IMS core and its call/session control functions (P/I/S-CSCF). Each of the functional blocks in the application server refers to a related sub-architecture.

Figure 1.9 depicts the platform components and their relation with other IMS objects. The functional blocks are the

- P2P-Authentication module, which stores client certificates for use by other modules, serves the client with initial credentials and signs the client's certificates on request.

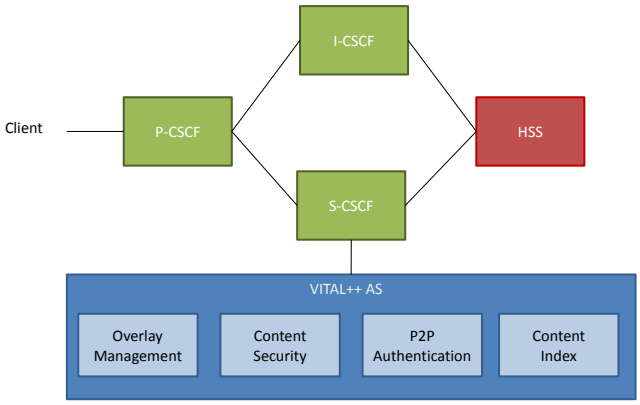

Figure 1.9 Platform components.

- Content Index module, which stores content descriptions and metadata and provides search functions to the clients.
- Overlay Management module, which constructs and maintains optimized overlays according to the client's connectivity.
- Content Security module, which provides and maintains DRM licenses for published content.

P2P communication concept integration in the frame of the server/client network architecture of IMS is realized by mapping P2P mechanisms for content management on the components of the core IMS network. Under this concept, overlay communication is enabled using IMS signaling for decentralized operations implementation for peers removal and addition.

Once the desired content has been found, realization of media streaming is done using a RTP protocol version that deviates from the traditional client/server communication model concerning its capacity for tiny content retrieval from many different sources. This enhanced RTP version is tolerant to frequent handovers for content between peers.

Session initiation and negotiation, which in IMS is handled by SIP Invite dialogs, has been replaced by P2P mechanisms, while media streaming is handled by the transport layer of the IMS. In this context, the VITAL++ client has been implemented following the architecture depicted in Figure 1.10.

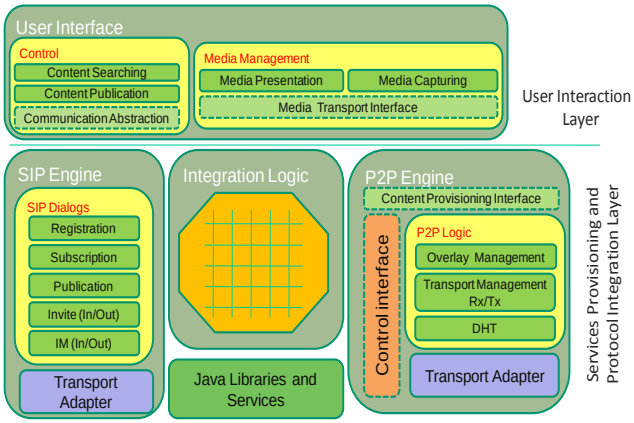

Figure 1.10 VITAL++ Client architecture.

The user interaction layer is the part of the client that interacts with the user. It provides all media playback and capturing capabilities as well as means for aiding the discovery and publication of content. This layer operates in a transport and communication agnostic manner. It produces and consumes both control information and media content. Control data are generated and processed by GUI elements that allow the use navigate in the acquired information. The control information that is produced identifies either criteria for content searching/publishing or content selection for acquisition through the underlying layers procedures. Media management contains all the required mechanisms for media representation or capturing by use of the available media libraries. Control on the media components is restricted to configuration regarding media playback or capturing leaving transport layer dependencies to be handled by the underlying layers according to UA configuration.

The services provisioning and protocol integration layer contains one SIP engine and one P2P engine. The SIP engine is built as a library that allows for the establishment of a number of SIP dialogs. The dialog objects can be configured to provide the content that is exchanged in their lifetime so that it can be processed in other application modules for the provision of a specific service.

The P2P engine provides a configuration interface through which all the control information can be applied for the proper initialization and mainte-

nance of the engine. Additionally the P2P engine provides a content exchange interface through which media content can be transmitted to the network or retrieved and forwarded to the media handling modules.

1.4 VITAL++ P2P functionality for live streaming

We have used VITAL++ architecture (client and network sides) to deliver live streaming as it has strong requirements in terms of bandwidth that it needs, introduces high amounts of traffic in the underlying network and strict time constraints in the distribution of content as peers consume it in real time.

The multimedia stream generated by individual users and/ or content providers is divided into blocks and distributed by the deployed overlay. 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 until its delivery to every participating peer. An efficientP2P-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 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 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 1.11 depict the performance of our system. In the left graph we demonstrate the cumulative density function of average network latency with their neighbors (energy) that peers have in a randomly formed overlay and one built by our CDO, described in other publications as ”Liquid Stream”. We observe a reduction of energy by approximately 90%. In the right graph we depict the cumulative density function with the percentage of the successful block transmissions that each peer that participates in our

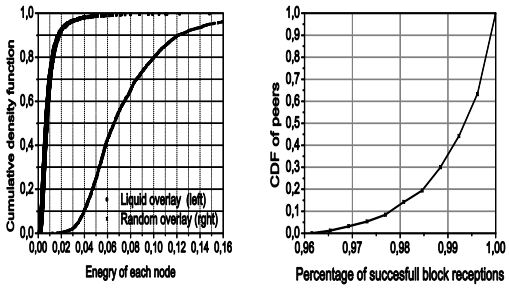

Figure 1.11 Left:CDF of the average network latency, Right: CDF of the successful block receptions.

system has. We mention here that the video steaming 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).

1.5 Use Case (SoftMix)

The SoftMix service, developed by content provider Rundfunk Berlin Brandenburg (RBB) over the course of VITAL++, serves as main demonstrator for the full functionality of the VITAL++ individual components and overall architecture.

Independent of the technological setting, its basic aim is to enable users to experience a truly personalized radio, which serves exactly the kind of content that they like. This service is meant to be a prototype of a radio of tomorrow, combining the traditional experience of the radio with the possibilities of the Internet: while traditional radio runs in the background and does not require any kind of interaction with the ”output device/user interface” (i.e. the radio), the Internet offers a variety of opportunities to interact with

the content through the service, including browsing, skipping, downloading, etc. SoftMix aims to enable the user to listen to the radio and personalize this experience according to his/her preferences. In this case ”user” is the most suitable term as the service enables active use and influence, way beyond passive listening. As long as the user is happy with the programme, however, s/he will not have to interact at all. The radio will just keep playing without further intervention.

The SoftMix service is intended for use on different IP-networked devices, stationary or mobile. Depending on their peer-to-peer capabilities, bandwidth, screen displays and other potentially limiting factors some such devices may not offer all of the service features. However, it is clearly intended that all of them offer the basic capabilities of receiving multimedia content according to their preferences and to further influence their profiles.

The SoftMix service will be offered via a dedicated RBB website where interested users can download the client and choose a start profile. Users will have to register for the service, saving some basic information as a first step towards their personal radio style. As RBB’s six radio channels are already targeting certain interest groups they will be a good starting point. Therefore, the first step towards a user profile is to choose the one RBB radio channel profile that most suits their interest and taste. From the moment that they selected one they can start receiving their radio programme and will receive more general recommendations soon according to their first reactions (like/dislike) to the programmes they received. The respective procedures will be described and explained in the following chapters.

The player will display the current media file on a screen, plus the basic information (channel, series, title/short description) - most other information will be available for searching and profiling but not visible in the player view. This player offers a reduced palette of buttons for maximum usability:

* **PLAY/PAUSE**.
* **BOOKMARK: (this file)**, so you can listen to it later.
* **SUBSCRIBE: (to this series)**; it will be added to your profile and any new episode added to your playlist with every new update.
* **RECOMMEND:** will show a bar with icons of friends that are online and can be selected to receive a recommendation. This file will then appear in their playlists.
* **LIKE:** this file and/or its related series will be uprated in your profile.
* **DISLIKE:** this file/series will be downrated in your profile.
* **SKIP:** Skipping a content item will also influence the profile.

There will not be any active search facility. Content search will happen in the background, being triggered by the user's profile in combination with an editorial frame which ensures that the order of files is not arbitrary but keeps listening to SoftMix a high quality radio experience.

To organize content search only according to user preferences would generate a random radio programme which would most certainly not have the quality of traditional radio programmes. In order to avoid arbitrary playlists the concept of Programme Frames was introduced. Over long periods radio experts have developed concepts to organize radio programmes so that they entertain and inform people in different ways at different times of the day; the famous morning radio shows are a prominent example for this.

SoftMix now also offers such Programme Frames in order to organize the radio programme in the way that generic frames define what type of content should follow the current item. This would avoid that three recipe podcasts or weather forecasts would be played in a row.

The Recommendation Engine which matches the user profile with the available content will now do this according to the currently relevant frame and thus filter the search request and at the same time organize the order of the playlist.

Using *Broadcast Mode*, users can "publish" simple media files or complete playlists as their own little radio show. Other users can tune in to their show and listen to this prepared playlist rather than to their own playlist as recommended by the SoftMix application based on their profile.

For devices with slow connectivity or small disk space the VITAL++ architecture employs a transcoding service converts media files between different content formats, e.g. codecs and bandwidth, depending on the requirements of the end user device.

IMS features are used, among others, for registering users, especially to enable decent influence and control on users who want to publish their own files or put together their own radio shows from own and public files by creating and publishing a playlist in "broadcast mode".

1.6 VITAL++ Test bed Deployment

In order to test/evaluate the proposed VITAL++ paradigm a number of heterogeneous telecommunication platforms were interconnected into a common experimental playground, as depicted in Figure 1.12. This unified testbed environment includes the IMS-enabled telecommunication infrastructures from FOKUS (Fraunhofer Institut), Telekomm Austria (TA), Telefonica I+D (TID),

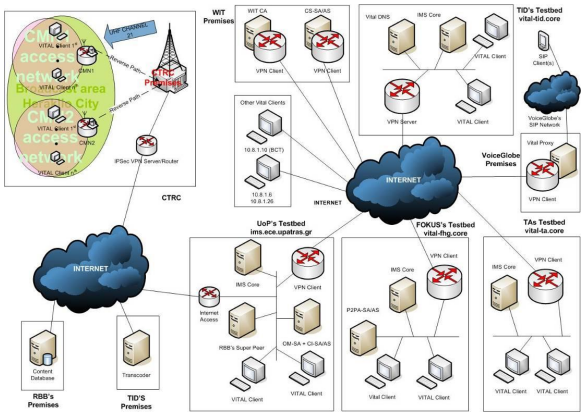

Figure 1.12 VITAL++ testbed.

University of Patras (UoP), and Voiceglobe, as well as an interactive DVB-T platform (at CTRC premises) acting as a Media Provider (Broadcaster) and Data injector in the services that we offer. More specifically, here we describe a scenario where, live streaming TV content (IPTV) is fed from an active-user located within the DVB-T broadcasting footprint (potential Broadcaster) onto the p2p engine, via a VPN connection. The received IPTV stream is processed by the P2P engine and distributed over the entire VITAL++ infrastructure via a number of specially configured VPN tunnels, established with OpenVPN software[10], enabling both IMS and P2P connectivity. This was achieved by means of VPN tunnels (see Figure 1.13).

Towards these, a VPN server was installed in Telefonica I+D's premises and VPN clients in the remaining testbeds, in order to establish a VPN tunnel between Telefonica I+D and each partner's testbed. A DNS server was also installed to resolve the domain names of each IMS core, therefore enabling the placement of calls between users registered at different IMS cores. Once basic IP and IMS connectivity was achieved, it was the turn of adapting the cores to VITAL++ needs, deploying the elements and entities required by the architecture.

First, the PCs hosting the IMS clients would also host the VITAL++ clients, both Monster's and BlueChip Technology's. It was decided that VI-

[10] http://openvpn.net/

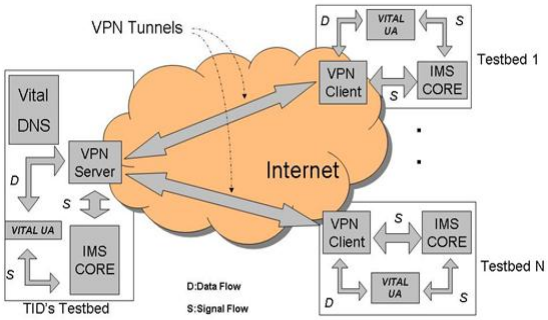

Figure 1.13 VITAL++ testbed connectivity.

TAL++'s users were going to be created only at Franunhofer's IMS Core, which would be considered as the home network for those users. While testing from another testbed, those users would act as roaming users accessing to their home network from a visited network, via the local P-CSCF. The Sub Architectures defined in the project would be distributed among the testbed, not centralized, and would be located at the following testbeds. Content Indexing (CI-SA) and Overlay Management (OM-SA) at University of Patras's. P2P Authentication (P2PA-SA) at Fraunhofer's and Content Security (CS-SA) at Waterford Institute of Technology (WIT). In this case, two VPN tunnels were required, one for the CS itself and other for the Certificate Authority, CA, the CS relies on). Those SA are considered as IMS Application Servers (SA), and are registered as such in Fraunhofer IMS core, in order to route IMS traffic among them and the clients.

However, besides adapting the testbeds, VITAL++ requires a number of external elements to carry out its functionalities properly. They are listed briefly here:

- In the case of Voiceglobe, a commercial provider of SIP telephony, a direct connection to the testbeds' network can not be established since its subscribers are assigned real IP addresses. In order to circumvent this obstacle, a VITAL++ Proxy has been implemented, that would appear to VITAL++ system as an standard VITAL++ Client and will en-

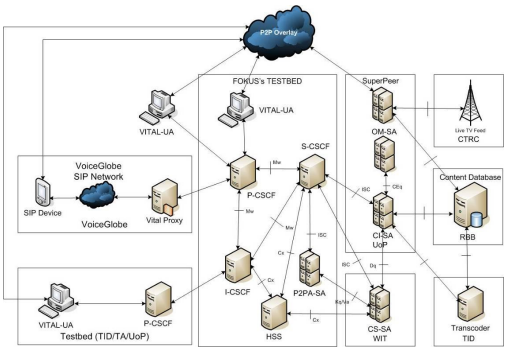

Figure 1.14 VITAL++ Configuration.

able Voiceglobe clients to download the contents made available by VITAL++.

- A database containing the data and metadata of the contents distributed by VITAL++ is located at Rundfunk Berlin Brandenburg's (RBB) premises. This database will not be connected directly to the network comprising the VPN tunnels or visible by the VITAL++ Clients, but indirectly accessed via University of Patras's testbed.
- In order to provide the content format that best fits the terminal capabilities (i.e. bandwidth, spatial resolution) a transcoding utility has been made available at Telefonica I+D's premises, which will automatically convert any uploaded contents into a set of predefined formats, served by respective overlays, enabling VITAL++ clients to join the most appropriate for their needs.
- In the case of the IPTV injection scenario, the Centre for Technological Research of Crete (CTRC) has inject a live streaming TV content onto the UoP test-bed from an active-user (potential Broadcaster) located within the regenerative DVB-T platform at CTRC premises, via a VPN connection. This stream is processed by the P2P engine and distributed over the entire VITAL++ infrastructure.

1.6.1 Test bed configuration

From a logical standpoint, the relationships and interfaces among the different entities involved in VITAL++ are depicted in figure 1.14. VITAL++

client registration will be carried out using the Fraunhofer's IMS core within Fokus's tesbed or via VPN connections from the partners in the case of roaming users from other testbeds ("visited networks" in IMS terminology). In the case of VoiceGlobe subscribers, the use of VITAL++ Proxy is mandatory. Once registered the VITAL++ Clients will be able to interact with the VITAL++ SA by sending and receiving IMS messages, in order to carry out the following tasks:

* To upload a content into Rundfunk Berlin Brandenburg's systems and create as many overlays as required for transcoding purposes plus a superpeer to serve them, in case the original uploader leaves the overlay.
* To search for contents, according to user's preferences stored in a personal profile, in order to retrieve a list of recommendations.
* To play that list of recommendations, joining the overlays serving each object. Notice that the play will be sequential and the user will be given the option of skipping tracks (though not of direct selection).
* To compose a playlist with contents already available in the system or stored in its HD and publish it.
* To join the playlists of the users in broadcast mode, who will identified as such in the user interface.
* To join the overlays offering Live TV and audio broadcast.

1.6.2 The IPTV injection scenario

In order to provide to the VITAL++ test-bed a live video event stemming from a real operational DVB-T platform in the Heraklion city [3] the following modules were configured:

* To upload a content into Rundfunk Berlin Brandenburg's systems and create as many overlays as required for transcoding purposes plus a superpeer to serve them, in case the original uploader leaves the overlay.
* An interactive DVB-T platform in regenerative configuration, where the common DVB-T downlink stream is transmitted in channel 40 of the UHF band (i.e. 622-630MHz), utilizing 8K operation mode with 16QAM modulation scheme, 7/8 code rate, 1/32 guard interval and the multi-protocol encapsulation mechanism (MPE) for the distribution of the IP datagrams. These transmission parameters provide a total available downlink capacity of about 20.5Mb/s, according to the DVB-T standard, part of which (12.5Mb/s) was allocated among three digital TV programs

(MPEG-2 live and non-live TV broadcasts), while the rest bandwidth was dedicated to IP services (i.e. 8Mb/s).

* A Cell Main Node (namely CMN1 in figure 1.15) located in an urban area of Heraclion City, providing triple play services to the end-users. The communication between this CMN and the DVB-T platform is via a one-way point-to-point link IEEE 802.11g (uplink), while downlink data are received by the CMN over the DVB-T broadcasting stream. The communication between the end-users and this CMN (access network) is over IEEE 802.11g full-duplex links.
* One rural-based CMN (namely CMN2) located 10 kilometers away from the DVB-T platform. This CMN serves a number of end-users exploiting ADSL technology (downlink 8048/uplink 1024) in the access network, while communicating with the regenerative DVB-T over common PSTN/ISDN lines in the uplink, and over the broadcasting stream in the downlink.
* A number of end-users located inside the access network of the cell main nodes. The Users located inside the Broadcast area are potentially users of the whole VITAL++ test-bed via the UoP test-bed.
* A VPN client that has two network interfaces, a) one real IP interface (fxp0:192.92.9.xx), and b) one interconnected with the DVB-T network (rl0= 10.0.67.xx). It has to be noted that the VPN client is an openBSD router that routes all traffic stemming from the DVB-T Network to the UoP testbed via a IPSec tunnel (enc0=192.168.184.xx).

In order to inject the stream inside the UOP testbed the following method was followed:

1. An end user using a digital TV tuner in order to capture the transmitted live video stream and forward it to the CMN.
2. A CMN capable of Transcoding the stream stemming from the end user and forwarding it to the central broadcasting point in RTP format.
3. A central broadcasting point where the transcoded stream was encapsulated and broadcasted in the UHF channel enabling the end users to be capable of viewing the RTP based transcoded DVB-STREAM.
4. A CORE module located in the central broadcasting point forwarding the transcoded video stream to the IPSec tunnel connecting CTRC with UoP.
5. At the UoP site the transcoded live video stream is received by the VITAL++ p2p client enabling all the VITAL++ end users interconnected with the UoP test-bed to access the live video service stemming from the

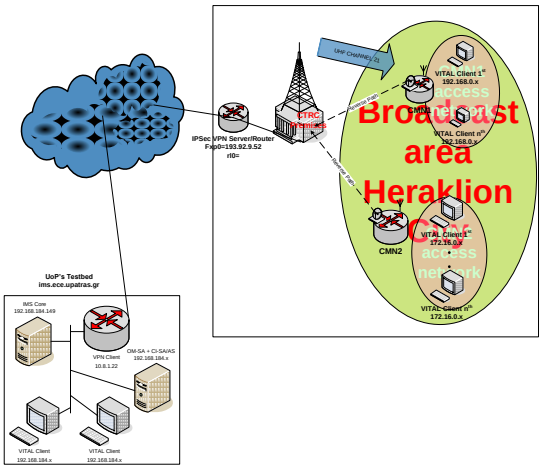

Figure 1.15 The IPTV injection scenario architecture.

end user located in the broadcasting area of the DVB-T infrastructure in Heraklion City.

1.6.3 VITAL++ test-bed deployment over an interactive DVB-T infrastructure

By deploying the VITAL++ Paradigm to an interactive DVB-T infrastructure, we enhance the scalability as well as the performance of the entire network, by exploiting P2P technology. On the other hand, the deployment of the IP Multimedia subsystems (IMS) tries to address issues of heterogeneity in the access technologies, AAA, security, and mobility management.

In order to enable the end users of the DVB-T interactive to become end users of the VITAL++ test-bed the following modules will be configured: A DVB-T platform, where the common DVB-T stream is transmitted in channel 40 of the UHF band (i.e. 622-630MHz), utilizing 8K operation mode with 16QAM modulation scheme, 7/8 code rate, 1/32 guard interval and the multi-protocol encapsulation mechanism (MPE) for the distribution of the IP datagram's.

The DVB/IP core network (see figure 1.16) utilizes the I-CSCF, S-CSCF and HSS (based on Fokus OpenSource IMS Core software). The core network will be able to receive the users/nodes IP traffic and IMS signaling information over the uplinks (via the appropriate Proxy Call Session Control

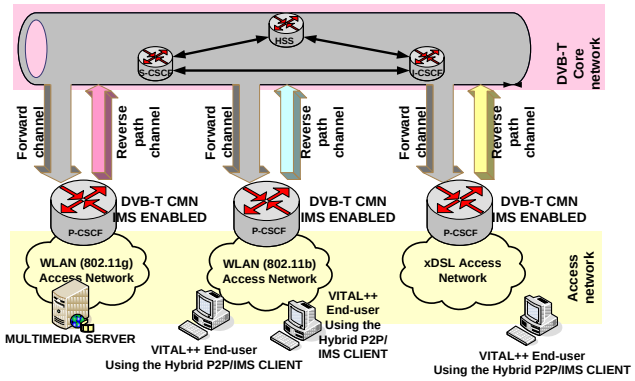

Figure 1.16 Proposed configuration of VITAL++ paradigm in an Interactive DVB-T infrastructure.

Function (P-CSCF)). The visited domains that are allowed to roam will be also defined in the IMS Core.

The CMN will gather all IP traffic stemming from its users, while the Proxy Call Session Control Function (P-CSCF) operating as the first contact point of the IMS domain, will create the necessary signaling for the provision of secure data transmission, authorization of the media and compression support of the SIP signaling, where required. The end user will utilize the VITAL++ HYBRID IMS/P2P Client.

A VPN client that has two network interfaces, One real IP interface and one interconnected with the DVB-T network. It has to be noted that the VPN client will routes all traffic stemming from the DVB-T Network to the VITAL++ test-bed via a IPSec tunnel.

1.7 Conclusions

In this work we analyzed how IMS, with it's centralized management and features for AAA and charging can exploit a P2P networking paradigm to offer content distribution services that are scalable, adaptable, secure, reliable while simultaneously offer new functionalities to the users. Through the development of the Vital++ platform we learned that P2P authentication is a promising solution for scalable and secure content distribution services.

Content security and accounting may be successfully combined with P2P overlays in order to meet business requirements. A centralized content indexing reveals P2P capabilities and doesn't hurt system scalability. Finally the optimization and the dynamic adaptation of the content distribution overlay is a critical factor for the successful operation of P2P content distribution services.

1.8 Acknowledgements

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

Bibliography

[1] N. Efthymiopoulos A. Christakidis S. Denazis and O. Koufopavlou. Liquidstream - network dependant dynamic p2p live streaming. *Springer Peer-to- Peer Networking and Applications (Accepted to be published)*, 2010.

[2] J. Fiedler T. Magedanz and J. Mueller. Extending an IMS client with peer-to-peer content delivery. In *Proceedings of the Second International Conference on MOBILe Wireless MiddleWARE, Operating Systems, Applications - ICST MOBILWARE*, 1978.

[3] E. Markakis E. Pallis and H. Skianis. Exploiting peer-to-peer technology for network and resource management in interactive broadcasting environments. In *Proceedings of IEEE Globecom*, 2010.

[4] VITAL++. http://www.ict-vitalpp.upatras.gr/.