

# Towards Autonomic Service Control In Next Generation Networks

Andreas Klenk<sup>\*</sup>, Michael Kleis<sup>#</sup>, Benoit Radier<sup>◦</sup>, Sanaa Elmoumouhi<sup>◦</sup>, Georg Carle<sup>\*</sup>, and Mikael Salaun<sup>◦</sup>

<sup>\*</sup> University of Tübingen,  
Sand 13  
72076 Tübingen, Germany  
*{klenk,carle}@uni-tuebingen.de*

<sup>#</sup> Fraunhofer FOKUS  
Kaiserin-Augusta-Alle 31  
10589 Berlin, Germany  
*michael.kleis@fokus.fraunhofer.de*

<sup>◦</sup> France Télécom R&D  
Avenue Pierre Marzin 2  
22307 Lannion, France  
*{benoit.radier, sanaa.elmoumouhi, mikael.salaun}@orange-ft.com*

## Abstract

Current standardization efforts aim towards a unifying platform for fixed and mobile telecommunication services. The IP multimedia subsystem is advocated as the candidate for building next generation networks (NGNs). However the direction taken in standardization is towards a rather static architecture with centralized features. The downside is an expected increase in service management complexity and the need for highly specialized infrastructures. This paper presents an approach for improving service quality, scalability and reliability while facilitating service management towards self-managing next generation networks. To approach this we utilize and combine functionality available in the network using a Peer-to-Peer based service composition mechanism. The construction of composed services is based on a service chain principle and incorporates information about available services, QoS and applicable SLAs.

## 1. Introduction

Fixed mobile convergence is a hot topic in telecommunications industry. An important building block for next generation converged networks is the IP Multimedia Subsystem(IMS) defined by 3GPP<sup>1</sup> and

taken into account by TISPAN<sup>2</sup>. The IMS allows for different types of access technologies while allowing mobile usage as well as an easy service integration. The main approach in IMS standardization is to define functional components and interfaces. The technical realization of this architectural model is inherently centralized and usually demands for a careful administration and deployment. Even in the case that IMS components are very reliable, the failure of an IMS component can lead to service interruption. This fact combined with the increasing complexity of service provisioning can result in a high management and configuration overhead for future IMS based services and thus high costs. In addition it can be expected that the resources of IMS components have to be allocated for peak usage, and will most of the time be underutilized. Thus CAPEX and OPEX for new services can be high and as a consequence the IMS architecture may be in fact not as flexible as expected.

In contrast, the prospects of autonomic networking research are to allow the network to take care of itself and to resolve problems automatically. In fact, the success of peer-to-peer (P2P) technology for Voice-over-IP (e.g. Skype) has already proven the value of distributed self-organizing architectures for telephony. Thus the question arises: *Does a P2P and overlay technology based service platform lead to a more flexible and easier maintainable service provisioning in NGNs?*

---

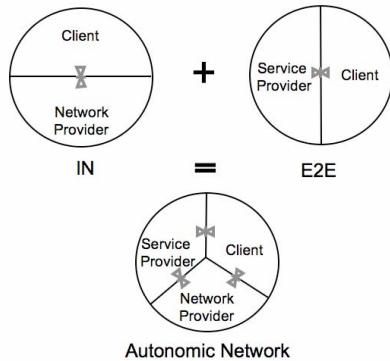
<sup>1</sup> 3GPP: Third Generation Partnership Project

---

<sup>2</sup> TISPAN: Telecoms & Internet converged Services & Protocols for Advanced Networks

In this paper we describe the approach followed by the research project *Situated Autonomous Service Control* (SASCO) to explore and develop a secure, overlay based platform for an autonomous service provisioning in NGNs. To address the above-named question we start with the premises from the viewpoint of a multimedia service provider. The core requirements of a solution covering multimedia processing as well as QoS aware transport and routing are low costs, low management and configuration complexity as well as scalability. Based on these requirements the core research challenge is the exploration of a self-\* [10][12] system for service provisioning in future networks. In this paper self-\* denotes self-configuring, self-organizing, self-managing and self-repairing. We will concentrate on an overall picture containing the required core concepts, and for a more detailed discussion of technical aspects we refer to [13][14]. As one result, the aspired approach would change the way how subscriber, network operator and service provider interact in a beneficial way for all parties. In the past two traditional business relationships with regard to service provisioning dominated:

1. A direct business relation between clients and service providers in networks based on the end-to-end principle [11] as e.g. the Internet. The network provider is offering essentially the same interface to the transport service to client and service provider.
2. A business relation between the client and an operator or the network provider as in networks based on the intelligent network principle. In such networks, new services have to be introduced either by the network provider itself or by a third party provider using a special interface (e.g. Parlay X defined by ETSI) offered by the network provider for this purpose.



**Figure 1 Entity Model**

We propose to combine the strengths of both principles with the aim to define an architecture that can be the basis for future and autonomic networks. The resulting entity model is depicted in Figure 1. As a consequence the approach will allow:

- The service provider to concentrate on service/content provisioning and to abstract from transport or end user terminal related issues.
- The network provider to offer value added transport services as: media adaptation to client terminals and access technology, broadcast/multicast services, caching, as well as seamless services and connectivity for clients.

One of the main anticipated research challenges to realize this vision in the area of service composition is to resolve concrete service chains with a scalable distributed algorithm and obey quality of service constraints imposed by the corresponding data transport and the services itself. In addition there is a need for explicit knowledge about the service chain to help the signalling between the partaking processing nodes. We discuss the benefits of this service chain knowledge within a dynamic access control scenario using the IMS Session Border Controller.

The paper is organized as follows: In Section 2 we present related work on autonomic overlay technology and security research. Section 3 outlines the features of the overlay whereas Section 4 motivates why knowledge about the service chain is important for access control. Section 5 concludes this paper with an outlook on the next steps.

## 2. Related Work

Using Overlay Networks as the platform for Service Provisioning and/or Composition has been the topic of several research proposals. However, the proposed schemes are either targeting at small scale scenarios for Audio/Video realtime data, covering only management aspects, or focus on caching and replication techniques for static content. In contrast to related approach as [5][6] our architecture is not necessarily based upon a central entity having global knowledge during the task of service overlay setup or for the discovery of valid processing chains. The key focus of our approach is to study how the Distributed Hash Table(DHT) principle can be extended to realize a distributed control plane for the setup of Service Overlays.

### 3. Situated Overlays as an Enabler for Autonomic Service Control

To establish overlay creation, maintenance and routing we start at the question: "How can the network provider take an active role in the provisioning of services in future network environments?" In fact by integrating the Network Provider into the process of service provisioning, QoS related problems can be addressed cooperatively by interaction between the Service Provider, the Network Provider and the Client. The reason for this is simply that in such a case all entities involved in transport of data related to a service are also aware of the service itself. As a side effect, a Network Provider can be part of the service value chain e.g. providing value added transport to third party service providers as well as its clients. As an expected positive impact such an approach will allow

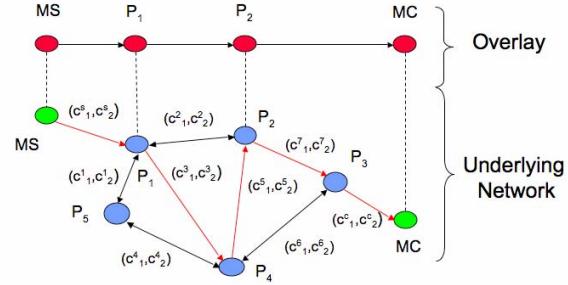
1. The Service Provider to concentrate on Service/Content and to abstract from transport or end user terminal related issues.
2. The Network Provider to offer value added transport services as: Media Adaptation to client terminal as well as access technology, Broad/Multicast services, Caching.
3. The Client to access services that are optimised for his/her end user terminal as well as access network technology.

We discovered the following three classes of Overlays as central. **Type One:** QoS aware Transport service for inter-domain environments. **Type Two:** Media/Data adaptation service. **Type Three:** Registry service.

In the following we will focus on Media/Data adaptation services since they demand QoS aware transport and thus we implicitly cover also overlays of type one. An overlay of type three will be used to maintain the information about available media adaptation functions. In the remainder of this chapter we assume that a Situated Overlay consists out of an ordered sequence of processing modules interconnecting a service source and sink. In Figure 2 we provide an illustration of a service chain with two processing steps. The figure also shows the corresponding path in an underlying network with two constraint values per link. Figure 3 illustrates the two main steps required for the setup of a Service Overlay.

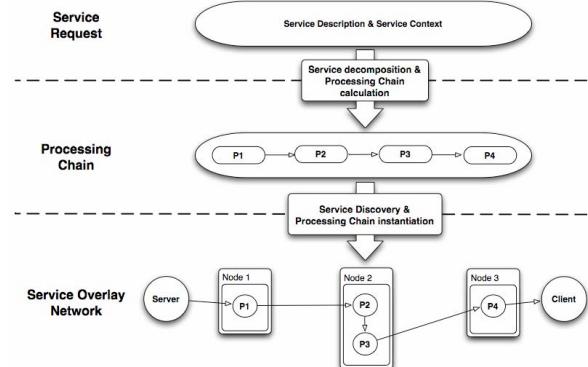
The first requirement is a methodology to decompose a given service request into a set of distributable sub services. In general there are two main ways to address this: *Online decomposition*: the decomposition of the service at time of request or *Offline decomposition*: the

decomposition during registration of a new service in advance of the first request.



**Figure 2 Service Chain**

We propose here to focus on *offline service decomposition* using a Service Level Agreement (SLA) principle. The SLA has to be established between a service provider and a third party provider (e.g. Network Provider) in advance of the first service request. The main reason for the SLA based approach is low complexity compared to the requirement of using e.g. service description languages to formulate respectively parse service requests.



**Figure 3 Service Overlay Approach**

A second advantage of the SLA approach is the fact that both parties can proactively optimise their server or network infrastructure in advance of the first service request based on the knowledge of registered services and the expected number of clients.

After receiving a request for a decomposed service it is required to locate nodes inside and/or at the edge of the network, hosting the processing modules required for the instantiation of the requested service. To accomplish this *Service Discovery* task we maintain the information about available processing modules using a DHT[8][9]. Based on the result of this service location step it is now required to interconnect the

service source and sink through a sequence of processing modules (PM) using an Overlay Network principle in a way that the QoS constraints of the service are not violated and the costs of service provisioning are minimised. This step is considered as the core problem to be addressed and corresponds to a Constraint Based Routing Problem (CBRP)[6]. To address this problem, we work towards a distributed search principle combined with a hop-by-hop QoS constraint verification and propagation technique instead of extending classical routing algorithms as Dijkstra or Bellman-Ford to be applicable for Overlay creation, adaptation and routing[6]. Using a DHT as the distributed control plane for a search & verify based approach has the following promising properties:

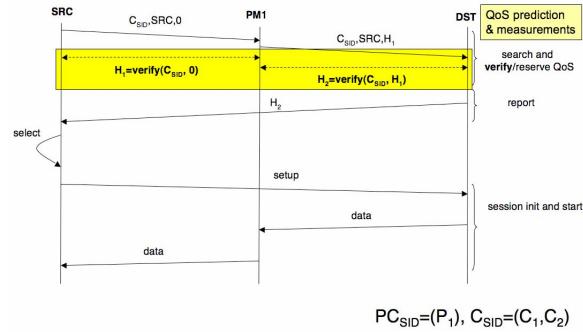
- *The resulting system can be realised in a fully distributed fashion and inherits the self-\* properties of DHTs. Further it can be realised with comparable low management state per node e.g.  $O(\log N)$ , where  $N$  is the number of DHT nodes.*
- *DHTs represent a well studied, resilient and fully decentralised domain for search based problems.*

In addition, in case every node hosting processing functionality is also actively integrated into the search process, it is possible to build up the service overlay layer while performing the search. However, standard DHTs are providing only a function to map keys to transport addresses where data related to the given key can be fetched. In contrast, for the proposed approach it is also required to incorporate control, verify and measurement functionality into a search process for chains of keys. We therefore have to extend a DHT towards a new DHT+++ [13] principle supporting:

1. The management of information about available Service Modules: *Registration functions using a service specific indexing scheme for embedding a system Service Graph into a DHT address space.*
2. Enhanced Search Function: *A scheme to search for processing chains (i.e. support for recursive queries).*
3. Verification of QoS constraints: *A function for the on demand verification of QoS constraints between any arbitrary pair of nodes hosting PMs.*

To address the before mentioned CBRP problem we apply a Search & Verify principle to distribute and parallelise the search for a processing service chain between the nodes forming the DHT+++ layer. This Search & Verify approach is illustrated using a simple example in Figure 4. Depicted is a case where it is required to process a media flow before it can be

consumed by the client. The two QoS constraints  $C_1$  and  $C_2$  of the service are assumed to correspond to an additive metric. For this example the search and verify approach would work in the following way: After the media source received the request for the service with  $PC_{SID}=(P_1)$  it initiates a search for a processing module able to accomplish  $P_1$ . For each match a verify procedure is started measuring the values  $H_1=(h^1_1, h^1_2)$  between the source and the PM, to verify the QoS parameters associated with the service. The corresponding QoS parameters have been specified via  $C_{SID}$  during the before mentioned SLA phase. If  $h^1_1 \leq C_1$  and  $h^1_2 \leq C_2$ , the corresponding PM is starting a new measurement task between itself and the destination with result  $h^2_1, h^2_2$ .



**Figure 4 Search and Verify Approach**

In case  $h^1_1 + h^2_1 \leq C_1$  and  $h^1_2 + h^2_2 \leq C_2$  the destination is contacted and informed about the possible service chain found. In case not, all resources bound by the process are freed. In this simplified example, the client now reports all the possible service chains back to the source which selects the most adequate one based on QoS and cost values and is initiating the data transfer.

In case of more complex services, the set of all possible processing chain candidates is in general defining a Directed Acyclic Graph (DAG) connecting the source and destination. For more information about the proposed P2P based service specific self configuration strategy, the DHT+++ principle as well as an analysis of the underlying problem space we refer to [13].

## 4. Access Control in the Service Chain

We chose an access control scenario to discuss the need for service chain knowledge at the individual services. Access control is a critical point for a provider with regards to P2P based overlay technology is the fact that security and access control is often not an integral part of overlay networks [4]. P2P research

primarily perceived firewalls as an obstacle for the mutual connections between the participating overlay hosts [2][3] some overlays even disguise their traffic and tunnel through firewalls [1]. However, firewalls are successful security components that serve as single points of control to effectively guard services in the protected domain from unauthorized access. Firewalls loose their protective features if they cannot distinguish between legitimate and unauthorized overlay traffic, they will end up with a decision to either allow or to block all inbound overlay traffic.

Our approach is to extend the situated overlay by service chain aware access control functionality. NGN infrastructures possess already a number of suitable access control functions, such as the IMS/TISPAN Border Gateway Function (BGF) [15]. The BGF can be integrated in the Session Border Controller (SBC). As there is no standard, what functionalities a SBC consists of, the deployment scenarios vary. SBCs can be used for IP-PBX (e-SBC), for access (A-SBC), core (C-SBC) and interworking (I-SBC) security. We want to utilize SBC functions that allow us to block unauthorized traffic.

In the envisioned Situated Overlay, a service requester might be obliged to authorized at services that can appear anywhere in the service chain. Assume a SBC that is the only means to allow access to a service that is part of the service chain. The authentication and authorization usually involves the cooperation with the service requester. However, the service requester is no next neighbour to the SBC of the service, which makes signalling dependent on knowledge about the service chain. On the one hand the requester must be aware, that she must authenticate herself against the SBC. On the other hand the SBC must know the addresses of the services to allow the communication within the service chain. The integration of the overlay access control with the service chain instantiation solves these problems. The Situated Overlay discovers during the service composition, that authorization is required at SBCs along the service chain. The service requester will be prompted to authorize her request at the SBC. Each SBC will be supplied with the next-hop and prior-hop address in the service chain and can allow according traffic. Hence, the knowledge about the dependencies of the services within the service chain is required to configure access control to allow the Situated Overlay to operate.

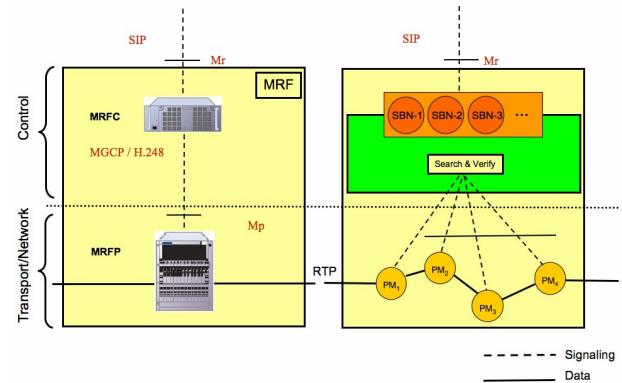
## 5. P2P Principles for an Autonomic Service Control in the IMS

To be able to use P2P principles in the IMS context it is first required to address the question: What are IMS

functions that can be realised using P2P principles? As one candidate we identified the Media Resource Function (MRF) which is responsible for resource consuming tasks e.g. playing, transcoding and mixing of media streams. As an example from TISPAN, the Resource and Admission Control Subsystem (RACS) realizes access and would profit from the proposed Situated Overlay approach by a better insight into service relationships for authorization decisions.

Another important issue is: What entities should run the corresponding P2P software? To address this, we categorise potential candidates into three main categories:

1. **Dedicated infrastructure nodes** are part of the network infrastructure and are particularly trustworthy and reliable.
2. **Home gateways and set top boxes** are fixed clients under partial control of the network provider that are already deployed in the order of several million devices in Europe.
3. **Mobile clients** have unsteady availability and would typically appear as service-originator or consumer in the situated overlay.



**Figure 5 P2P Media Resource Function**

Based on this categorisation we propose to used a hybrid P2P IMS approach using a combination of infrastructure nodes and fixed clients for a P2P based IMS since these nodes can be assumed to have the necessary stability and connectivity to be integrated into a service provisioning process.

To illustrate this, Figure 5 shows how a distributed IMS MRF can be realised using the situated overlay and the IMS Mr interface to link the situated overlay to the rest of the IMS. The right side of the figure also illustrates our concept of Service Bootstrap Nodes (SBNs). SBNs are responsible to initiate a service composition process.

## 6. Conclusions

We are at the brink of the realization of next generation networks with IMS at the core. To be able to manage the expected increasing configuration complexity caused by the plethora of future services we are convinced that self-management capabilities are crucial for the success of IMS/TISPAN based technology. To reach this we propose to exploit the autonomic functionalities of peer-to-peer based overlay technology to form an Autonomic Service Control for next generation networks. We identified suitable entities that could form the P2P overlay network and IMS functions that benefit from a realization as overlay service. We introduced a decentralized service composition mechanism that obeys quality of service parameters. We argued with an access control scenario how service chain knowledge facilitates the required signaling for authorization of service usage. Future work is to realize the Autonomic Service Control and evaluate its role for IMS/TISPAN architectures.

## 7. Acknowledgements

This research is performed in the context of the Situated Autonomic Service Control (SASCO) project, which is gratefully funded by the France Télécom R&D.

## 8. References

- [1] Androulidakis-Theotokis, S. & Spinellis, D., 'A survey of peer-to-peer content distribution technologies', *ACM Comput. Surv.* 36(4), 335—371 (2004).
- [2] Baset, S.A. & Schulzrinne, H., 'An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol', *Arxiv preprint cs.NI/0412017* (2004).
- [3] Ennis, D.; Anchan, D. & Pegah, M., 'The front line battle against P2P, in 'SIGUCCS '04: Proceedings of the 32nd annual ACM SIGUCCS conference on User services', ACM Press, New York, NY, USA, pp. 101—106 (2004).
- [4] Wallach, D.S., 'A Survey of Peer-to-Peer Security Issues., in 'ISSS', pp. 42-57 (2002).
- [5] D. Xu and K. Nahrstedt, "Finding service paths in a media service proxy network," Proceedings of the ACM/SPIE Conference on Multimedia Computing and Networking, (2002).
- [6] K. N. Jingwen Jin, "Source-based qos service routing in distributed service networks", Proceedings of IEEE International Conference on Communications 2004 (ICC2004), 2004.
- [7] X. Gu, K. Nahrstedt, and B. Yu.'SpiderNet: An Integrated Peer-to-Peer Service Composition Framework',Proceedings of the thirteenth IEEE International Symposium on High-Performance Distributed Computing (HDPC-13) 2004
- [8] P. Maymounkov and D. Mazieres, "Kademlia: A peer-to-peer information system based on the xor metric," in Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS '02), March 2002
- [9] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker, "A scalable content-addressable network," in Proceedings of the 2001 ACM SIGCOMM Conference, August 2001.
- [10] Ganek, A. G. Corbi, T. A.: The dawning of the autonomic computing era. *IBM Systems Journal.* 42(1), 5—18 (2003)
- [11] J. H. Saltzer, D. P. Reed, Anind Dey, Understanding and D. D.Clark. End-to-end arguments in system design. *ACM Transactions on Computer Systems*, pages 277-288, 1984.using Context, Personal and Ubiquitous Computing, 2001
- [12] O. Babaoglu, M. Jelasity, A. Montresor, C. Fetzer, S. Leonardi, A. van Moorsel, and M. van Steen, Eds., *Self-Star Properties in Complex Information Systems*, ser. Lecture Notes in Computer Science, Hot Topics. Springer-Verlag, 2005, vol. 3460.
- [13] Michael Kleis, Kai Büttner, Sanaa Elmoumouhi, Georg Carle, Mikael Salaun, "CSP, Cooperative Service Provisioning using Peer-to-Peer Principles" Proceedings of 2<sup>nd</sup> IEEE/IFIP International Workshop on Self-Organizing Systems (IWSoS), 2007
- [14] Andreas Klenk, Frank Petri, Benoit Radier, Mikael Salaun, Georg Carle "Automated Trust Negotiation in Autonomic Environments" Proceedings of 2<sup>nd</sup> IEEE/IFIP International Workshop on Self-Organizing Systems (IWSoS), 2007
- [15] "Telecommunications and Internet converged Services and Protocols for Advanced Networking" TISPAN; NGN Functional Architecture Release, ETSI ES 282 001 V1.1.1, 2005