A Viewpoint of the Network Management Paradigm for Future Internet Networks

Javier Rubio-Loyola[1], Joan Serrat[1], Antonio Astorga[1]
Andreas Fischer[2], Andreas Berl[2], Hermann de Meer[2], Giannis Koumoutsos[3]
[1]Universitat Politècnica de Catalunya, [2]University of Passau, [3]University of Patras
{jrloyola, serrat, aastorga}@tsc.upc.edu, {andreas.fischer, berl, demeer}@uni-passau.de, koumouts@ece.upatras.gr

***Abstract* – This paper presents a viewpoint of the management for the Future Internet. For this description we consider the architectural model developed by the EU IST Autonomic Internet – AUTOI – consortium for the management design of the Future Internet as a service- and self-aware network that guarantees built-in orchestrated reliability, robustness, mobility, context, access, security, service support and self-management of the communication resources and services. The paper positions the autonomic network management approach taken by the AUTOI solution in a Future Internet scenario and describes the main interactions involved of the different distributed management systems running within the network in the context of the aforementioned scenario. The paper also provides a selection of the technical difficulties encountered so far while developing such a management approach.**

I. INTRODUCTION

Future Internet is envisaged as a global network that handles the heterogeneity spanning across network technologies, device capabilities and user requirements. A network that has ubiquitous and pervasive characteristics, supports device and resource mobility and satisfies the diverse user demands. The management complexity of the current Internet should be reduced using autonomic management techniques that carry out time consuming tasks without or with minimum human intervention. For example, the different network entities can follow general rules specified by the administrators while the low-level management operations can be performed automatically, in consistency with these rules.

However, the network management paradigm for the Future Internet poses many key challenges:

- The management functionality should be imbedded in the service-aware networks.
- Exhibit self-management functionalities, in particular self - optimisation; - organisation; -configuration; -adaptation; - healing; - protection.
- Self-management functions controlled by the setting up and negotiation of common/agreed goals.
- Aware and Self-aware functions monitoring the network and operational context as well as internal operational network state in order to assess if the network current behaviour serve its service purposes.
- Adaptive and Self-adaptive functions triggering changes in network operations (state, configurations, functions) in function of changes in network context.
- Automatic self-functions as the means to enable self-control (i.e. self-FCAPS) of the internal network operations, functions and state, operating without manual external intervention. Only manual/external input is the setting-up of the goal(s).
- Dynamic programmability of management functions & services that allow adding new functions without disturbing the rest of the system, namely (Un) Plug and Play management functions & services.
- Simplicity in the management functions as to minimise life-cycle system operations' costs and energy footprint.

The above requirements represent big challenges for the research community. Several research efforts are being carried towards the assessment of the Future Internet but still, how the management of the Future Internet would look like and the practical implications that such a complex system may have for its realisation, represents a paradigm on its own. This paper presents a viewpoint of a management approach for Future Internet networks. For this we take into account the management principles of the ongoing EU IST Project Autonomic Internet AUTOI [1], which proposes a self-managing overlay of virtual resources that can span across heterogeneous networks.

This paper is structured as follows: After this Introduction, Section II provides some Future Internet related works, Section III details the background management approach in which this paper is centred. Section IV positions this solution proposal in a wide ranging scenario and Section V presents technical difficulties encounter thus far in this ongoing work. Section VI concludes our paper and gives some future work.

II. RELATED WORK ON FUTURE INTERNET INITIATIVES

Several research initiatives around the world are currently addressing challenges of today's Internet and Future Internet Networks. A few examples are:

The AKARI project [2] in Asia for example aims to implement a new generation network by 2015, through the development and design of a new network from a clean slate approach, without being impeded by existing constraints. The migration towards this Future Internet from the current one is also considered, once the new architecture design and principles are stable.

In America, FIND (Future Internet Design) [3] is a major initiative of the National Science Foundation that includes

research efforts working on the development of network architecture, security, advanced wireless and optical properties, economical principles, and in general, mechanisms to build a global network of 15 years from now, and its realisation without the concerns of the current Internet. The GENI (Global Environment for Network Innovations) [4] Program supports fundamental challenges of the current Internet like inadequate security, reliability, manage-ability and evolvability.

In Europe, a number of IST projects have targeted challenges of the Future Internet from different perspectives. Ambient Networks [5] for example is centred in the study of network control infrastructures for wireless and mobile networks, developing a control overlay that encompasses all control functions on a per-domain basis, in order to integrate and interoperate seamlessly any existing networks. The Autonomic Network Architectures project [6] targets the organizational problem and the position of networks beyond legacy Internet technology, designing and developing a new network architecture that enables flexible, dynamic, and fully autonomic formation of nodes and whole networks. Issues like adaptation and reconfiguration are pivotal to this approach which considers the dynamicity of management domains and economic models, all in all, building and testing an autonomic network architecture.

CASCADAS [7] develops an autonomic component-based framework to enable composition, execution and deployment of new services capable of flexing and coping with different environments by dynamic self-adaptation to different scenarios. CASCADAS aims at a vision of Future Internet as an ecology of simple lightweight components that are able to interact with each other and self-organize dynamically to serve in an adaptive and goal-oriented way. BIONETS [8] is inspired from emerging trends towards pervasive computing and communication environments, where the networks will enhance our five senses, our communication and tool manipulation capabilities. The architecture of this environment mimics biological organisms, ecosystems, and social systems, namely being able to work in the absences of central control and exploit local interactions.

HAGGLE [9] is a project that uses autonomicity principles to enable Communications in the presence of intermittent network connectivity exploiting the concepts of opportunistic communications. The project proposes a departure from the existing TCP/IP protocol suite, to eliminate the layering about the data link, and exploiting application-driven message forwarding, instead of delegating this responsibility to the network layer. EFIPSANS [10] aims at exposing the features in IPV6 that can be exploited or extended for the purposes of designing or building autonomic networks and services. EFIPSANS studies the emerging research areas that target desirable user behaviours, terminal behaviours, service mobility, e-mobility, context-aware communications, self-ware, how autonomic communication/computing/networking will be carried out, and out of these areas desirable autonomic(self-*) behaviours in diverse environments e.g. end systems, access networks, wireless versus fixed network environments will be captured and specified.

The EU IST Autonomic Internet AUTOI project suggests a transition from a service agnostic Internet to service- and self-aware Internet managing resources by applying Autonomic principles. In order to achieve the objective of service- and self-aware networking resources and to overcome the ossification of the current Internet, this initiative aims to develop a self-managing virtual resources overlay that can span across heterogeneous networks and that supports service mobility, security, quality of service and reliability. In this overlay network, multiple virtual networks could co-exist on top of a shared substrate with uniform control. One of the main research challenges for designing a new service-aware network is the inclusion of capabilities such as self-awareness, self-network knowledge and self-service knowledge. These capabilities are used to facilitate continuous tuning of the networks, adaptation to unpredictable conditions, prevention and recovery from failures and provision of a dependable environment. The next section elaborates on the AUTOI approach, which is pivotal in this paper.

III. AUTOI: BACKGROUND ARCHITECTURE & MOTIVATION

AUTOI advocates for an autonomic management architectural model consisting of a number of distributed management systems within the network, which are described with the help of five abstractions and distributed systems - the OSKMV planes (see Fig. 1) [11]: Orchestration Plane (OP), Service Enablers Plane (SP), Knowledge Plane (KP), Management Plane (MP) and Virtualisation Plane (VP). Together these distributed systems form a software-driven control network infrastructure that will run on top of all current networks and service infrastructures.

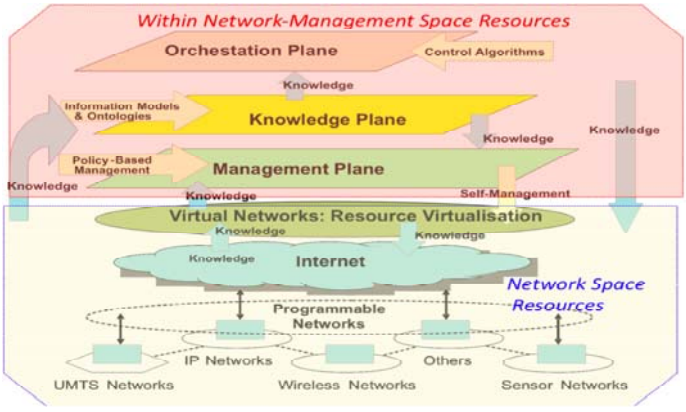

Figure 1. The Autonomic Internet (AutoI) Planes

A. *Orchestration Plane*

The Orchestration Plane is a conceptual definition for the instruments that govern and integrate the behaviours of the management systems distributed across the network, in response to changing context and in accordance with applicable business goals and policies insuring integrity of the

Future Internet management operations. The Orchestration Plane can be thought of as a control framework into which any number of components can be plugged into in order to achieve the required functionality. These components could have direct interworking with control algorithms, situated in the control plane of the Internet (i.e. to provide real time reaction), and interworking with other management functions (i.e. to provide near real time reaction). This plane supervises the optimisation and the distribution of knowledge within the Knowledge Plane to ensure that the required knowledge is available in the proper place at the proper time. The Orchestration Plane may use local knowledge to deserve a real time control as well as a more global knowledge to manage some long-term processes.

The Orchestration Plane would host one or more Autonomic Management Systems (AMSs) and it is made up of one or more Distributed Orchestration Components (DOCs), and a dynamic knowledge base consisting of a set of models and ontologies and appropriate mapping logic. Each AMS represents an administrative and/or organisational boundary that is responsible for managing a set of devices, subnetworks, or networks using a common set of policies and knowledge. The AMSs access a dynamically updateable knowledge base, which consists of a set of models and ontologies. A set of DOCs enable AMSs to communicate with each other for federation, governance and negotiation purposes.

B. Service Enablers Plane

The Service Enablers Plane (SP) consists of functions for the automatic (re)deployment of new management services, protocols as well as resource-facing (i.e. QoS functions) and end-user facing services. It includes the enablers to allow code to be executed on the network entities. The safe and controlled deployment of new code enables new services to be activated on demand. This approach has the following advantages: i. Automatic service (re)deployment allowing a significant number of new services to be offered on demand; ii. Special management functions and services can be easily enabled locally for testing purposes before they are automatically deployed network-wide; iii. Eases the deployment of network-wide protocol stacks and management services; iv. Enables secure and controlled execution environments; v. An automatic decision making infrastructure guides the deployment of new tested network services; vi. Optimised resource utilization of the new services and the system.

C. Knowledge Plane

The Knowledge Plane (KP) consists of models and ontologies, to provide increased analysis and inference capabilities; its purpose is to provide knowledge and expertise to enable the network to be self-monitoring, self-analyzing, self-diagnosing, and self- maintaining or –improving [12]. It brings together widely distributed data collection, wide availability of that data, and sophisticated and adaptive processing or KP functions, within a unifying structure that brings order, meets the policy, scaling and functional requirements of a global network, and, ideally, creates synergy and exploits commonality of design patterns between the many possible KP functions. The main KP components are an information and context service (ICS) plus models and ontologies, which enable the analysis and inferencing capabilities. Knowledge extracted from information/data models forms facts. Knowledge extracted from ontologies is used to augment the facts, so that they can be reasoned about. The ICS provides: i. information-life cycle management (storage, aggregation, transformations, updates, distribution) all information and context in the network and addresses the size and scope of the Internet; ii. responsiveness to requests made by the AMSs; iii. triggers for the purpose of contextualisation of AMSs (supported by the context model of the information model); iv. support for robustness enabling the KP to continue to function as best possible, even under incorrect or incomplete behaviour of the network itself; v. support of virtual networks and virtual system resources in their needs for privacy and other forms of local control, while enabling them to cooperate for mutual benefit in more effective network management.

D. Management Plane

The Management Plane consists of AMSs, which are designed to meet the following design objectives and functionality: i. Embedded (Inside) Network functions: The majority of management functionality should be embedded in the network and it is abstracted from the human activities. As such the AMSs will run on execution environments on top of virtual networks and systems, which run on top of all current network and service physical infrastructures.; ii. Aware and Self-aware functions: It monitors the network and operational context as well as internal operational network state in order to assess if the network current behaviour serve its service purposes.; iii. Adaptive and Self-adaptive functions: It triggers changes in network operations (state, configurations, functions) function as a result of the changes in network and service context.; iv. Automatic self-functions: It enables self-control (i.e. self-FCAPS, self-*) of its internal network operations, functions and state. It also bootstraps itself and it operates without manual external intervention. Only manual/external input is provided in the setting-up of the business goals; v. Extensibility functions: It adds new functions without disturbing the rest of the system ((Un)Plug_and_Play/ Dynamic programmability of management functions & services); vi. Simple cost functions: Minimise life-cycle network operations' costs and minimise energy footprint. The AMSs are designed to follow autonomic control loops [13][14].

E. Virtualisation Plane

One of the key requirements that differentiate AUTOI from other efforts is its emphasis on virtualisation [15]. Virtualisation platforms are used to provide virtual services and resources. Resource virtualisation abstracts physical resources into manageable units of functionality; for example

the concept of a virtual router, where a single physical router can support multiple independent routing processes by assigning different internal resources to each routing process. The Virtualisation Plane consists of software mechanisms to treat selected physical resources as a programmable pool of virtual resources that can be organised by the Orchestration and Management Planes into appropriate sets of virtual resources to form components (e.g., increased storage or memory), devices (e.g., a switch with more ports), or even networks. The organisation is done in order to realise a certain business goal or service requirement.

The Virtualisation Plane is used by the Orchestration plane to govern virtual resources, and to construct virtual services and networks that meet stated business goals having specified service requirements. The AMSs of the Management Plane manage through the Virtualisation Plane, the physical resources, and the construction of virtual resources from physical resources. In AUTOI the separation between the virtualisation plane and other planes relieves the other planes from dealing directly with physical resources. Only virtualised resources are manageable via the virtualisation interfaces and also monitoring information about the physical and virtual resources can be requested from the virtualisation interfaces. This separation enables a system-wide management of virtual resources by other planes, while the management of physical resources is done by the virtualisation plane.

IV. Management Viewpoint

A. *Application Future Internet Scenario*

This sub-Section describes an application service as a framework for the positioning of the management proposal outlined above. Let us consider an application service that provides large amounts of diverse-nature information, such as multimedia files or information to users with different profiles. Such information, which is stored on servers distributed in a given geographic area, should be provided to users with certain levels of service, specified in the relevant contracts. In this regard, let us consider two extremes, namely, a client at home whose time access to information and security of the same are not critical and a client of a corporation in which both are important requirements. Between these two extremes we can define an arbitrary number of cases.

In order to provide the information in the minimum period of time, we can say generally that it is preferable that the user could download it from the server that is closest to the user, and that this server in turn would get the information from the server that stores the information. This idea is based on the fact that the servers can provide a kind of P2P overlay network [16] with channels of communication with large capacity and therefore, the use of this overlay is usually more effective than downloading the information directly from the server that stores it.

The users are not associated to any permanent server; use different types and terminal manufacturers and their position change continuously. Indeed, these are mobile users, although the service can be provisioned to fixed users. The mobile users may pass through areas where there are various systems of access.

In order to cope with the different types of users, especially users with security requirements, the system will establish a virtual private network (VPN) probably with encryption between the server that has stored the information and the user terminal as long as it is appropriate and possible. Encrypting the information directly impacts on the performance and it will be necessary to arbitrate it properly. Even the corporate users may require at any given time the use of encrypted information, and not for other type of information. The encryption impacts the lifetime of the mobile device significantly. So, the encryption settings may be adaptive to the downloaded content (e.g., non-critical information may be transmitted unencrypted).

On the other hand, when we establish a VPN with encryption, any other encryption process in other sections of the path of the service that could not provide more security should be avoided, as of course they would limit even further the link performance. Please take note that if the appropriate measures are not considered and if the users access it via a protected WLAN with WPA and a connection via SSH is established, the users would pile three Systems of encryption, namely WPA, VPN and SSH.

Users access the network by means of various wireless access technologies. In particular, we assume an environment of mobile Internet offered by the family of IEEE standards. Specifically, it is assumed that there are points of access for local area network IEEE 802.11 (Wi-Fi), wide area network fixed and mobile (IEEE 802.16 and IEEE 802.16e respectively) and regional area network IEEE 802.22 (WRAN). Users can access through any of these technologies as long as their terminals can support them. Moreover, when the users enter the coverage area of another access point, there must be a change between access technologies (Handover) automatic and transparent to the user, depending on various factors including: specific service characteristics being offered; user's profile; signal intensity; time response of the switching process; position, speed and direction of movement of the users; traffic, load and applications supported by the various sub-networks; and cost and grade of service.

B. *Management Tasks to Support the Scenario*

The scenario described above needs a management system that ensures a transparent delivery of the service that the clients have contracted. This will require making, among others, the following management tasks: Deploy an appropriate management system that can support the provision of the services with the appropriate resources; Setting up VPNs on demand, depending on the context of the user and the network. This involves: Authentication and authorization of users; Establishment, maintenance and completion of VPNs with QoS and encrypted as appropriate; Support mechanisms for automatic vertical handover to ensure the best possible access to the network at any moment. The process of handover can be

driven by policies taking into account context variables; Support for the management communication overlays' setting up with uniform distribution of the traffic load injected to network resources. The creation of VPN should be done by taking into account the distribution of load on the network so that this is as homogeneous as possible; Reaction to the degradation of the quality of service, identifying the causes and taking corrective and preventive actions to solve it; Reaction to failures in the network infrastructures, identifying their causes and restoring the services concerned in a transparent manner.

C. *Overall Picture*

The overall picture of the virtualized infrastructure supporting the Future Internet scenario is shown in Fig. 2. The scenario basically consists in the provision of end-user multimedia services that need the collaboration of fixed-network aware elements and wireless access controllers in a wireless seamless Internet scenario. The five OSKMV planes solution defined by AUTOI provides support to set up and maintain a functional architecture like the one depicted in Fig 3.

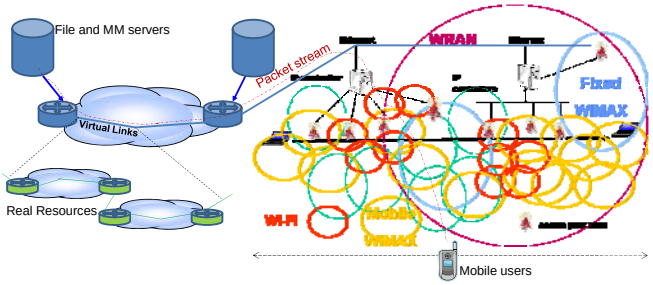

Figure 2. AUTOI Infrastructure supporting a Future Internet scenario

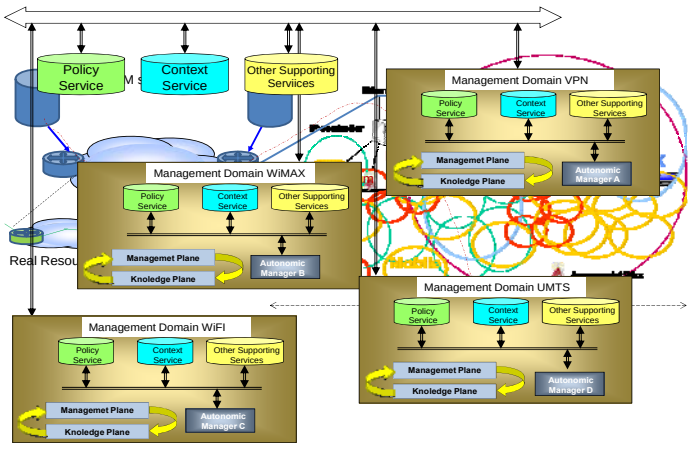

Figure 3. Practical viewpoint of the management system for the scenario

Each management domain (Management Plane) controls a number of virtual resources (Virtualisation Plane) and has its own knowledge base information (Knowledge Plane). Each management domain has its own goals and has its own policy service, information and context service (ICS) and other supporting services like programmable infrastructures (Service Enablers Plane) that enable that large scale autonomic services to be deployed. For simplicity, the exemplified picture in Figure 3 proposes an organizational domain per technology, namely one for the VPN setting-up, and one for each access technology; WiMAX, WiFi, UMTS, and so forth. Bootstrapping between management domains is made sure following on with the same structure pattern. This is, Orchestration (Orchestration Plane) between the different management domains and other Orchestration planes is enforced in this functional block through a policy service, a context service and other supporting services for programmability issues.

D. *Detailed Interactions between the OSKVM planes*

This section elaborates on the interactions that the five OSKVM planes make to do three main tasks: i) start up the network infrastructure and supporting services; ii) deploy an end-user service; and iii) service lifecycle support. The Figure 4 shows a rather generic, indicative and simplified example of the interactions for the first task. From now on, the interactions will be identified in *italics* within the text.

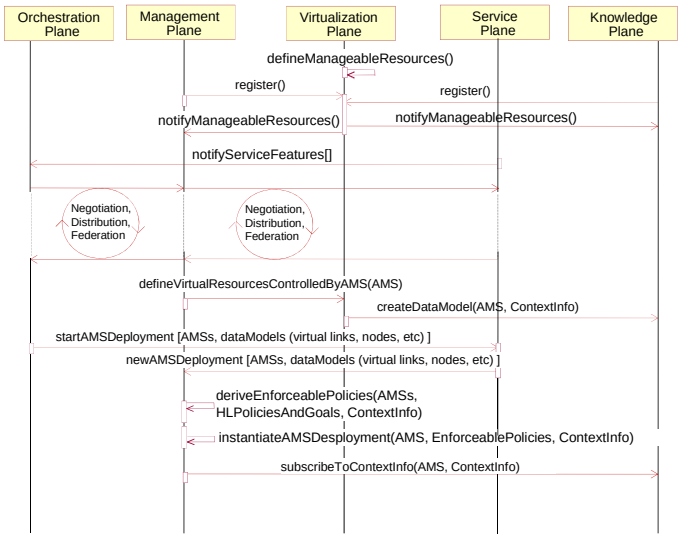

Figure 4. OSKVM planes interactions for network infrastructure start up

The Orchestration Plane triggers general guidelines for service provisioning and the Management Plane defines which Virtual Resources are needed for such a purpose. The Virtualisation Plane initially identifies what resources are subject to management activities *(defineManageableResources)* and associates Virtual Resources with AMSs. The *register* interaction allows the Virtualisation Plane to determine who is interested in virtual resource information, not only across planes but also within planes. Once this is successfully achieved, the Virtualisation Plane reports the manageable resources and their corresponding interfaces for their control to the Management Plane and to the Knowledge Plane *(notifyManageableResources)*.

The Service Enablers Plane must keep a catalogue of services that could be subscribed by the end-users, and that

will be invoked further. Other possibilities like on-demand service deployment are also valid. For this example the Service Enablers Plane notifies the requirements of the end-user service to the Orchestration Plane *(notifyServiceFeatures)*. This is a specialisation of a scene in which an ISP anticipates to the user needs, and that will eventually result in the setting up of deployable AMSs. The Service Enablers Plane controls the profiles of users and they are also part of this notification interaction. This interaction could also occur before the definition of manageable resources *defineManageableResources*.

The Orchestration Plane starts a round of interactions with the Management Plane, and supported by the Service Enablers Plane with the aim of determining the management services and resources that are needed to provision the end-user application services. In practical terms, the AMSs (Autonomic Management Systems) carry out a number of interactions in which the DOCs (Distributed Orchestration Components) mediate between them to achieve higher-level goals. These interactions are *Negotiation, Distribution and Federation* in Fig. 4. Potential results from this round of interactions are:

• The need to identify the nature of network services and resources that will support the service provision

• The need to group and identify the manageable resources and network services in each autonomous management domain

• In this seamless Internet use case the need to set up two deployable AMSs, one for the fixed part of the scenario (AMS fixed) and other for the wireless part (AMS wireless).

• A number of negotiated, federated and distributed high-level goals and policies to which the AMSs should align their management tasks.

• Context information that will be needed to configure the service and for its lifecycle support

The Management Plane reports to the Virtualisation Plane the resources that will be managed by the corresponding AMSs *(defineVirtualResourcesControlledByAMS)*. This information is used to create a concrete data model, specific for each AMS *(createDataModel)*. The data models at this stage should describe the characteristics of all virtual resource and virtual links / topologies and their associations so that the virtual resources can be deployed and minimising the impact on the deployable AMSs.

The Orchestration Plane starts the deployment of the AMSs *(startAMSDeployment)*, with the corresponding data model, with the help of the Service Enablers Plane. The Service Enablers Plane then coordinates and orders the deployment of the new AMSs to the Management Plane. The result is the formation of individual management systems that can manage the defined virtual resources with high-level goals *(newAMSDeployment)*.

The Management Plane uses the High-level goals and Policies drawn during the negotiation with the Orchestration Plane and the Service Enablers Plane to derive the policies that will be used in the autonomous control loops, namely the management tasks in the corresponding AMSs *(deriveEnforceablePolicies)*. This interaction also includes the deployment of enforceable policies to the corresponding Policy Enforcement Points. Possibly, during this process, more detailed context information is identified in each AMS.

The Management Plane now has all the information that is needed to enable the AMSs *(instantiateAMSDeployment)*. The AMSs are deployed including among other information, the enforceable policies and the concrete and specific context information to which each AMS should be aware of. Each AMS subscribes to specific context information represented with the interaction *subscribeToContextInfo* between the Management Plane and Knowledge Plane.

At this moment, the network infrastructure and the supporting services have been started up with the architectural composition shown in Figure 5 (by now ignore the VPN and the packet streams): an AMS is deployed to control the fixed network elements and another AMS to control the wireless access elements.

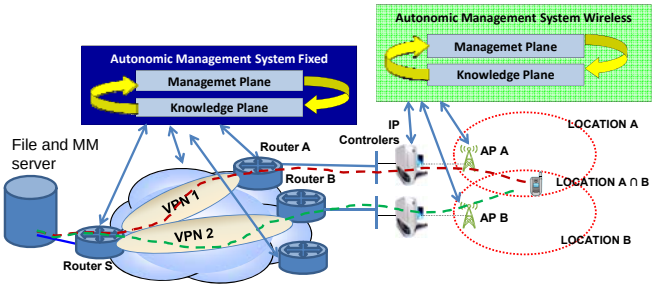

Figure 5. Architectural composition for the provision of end-user services

For simplicity in this diagram we consider two access points of two different access technologies. The end-user terminal supports both access technologies. The coverage area of each access point is depicted as an elliptic curve in Fig. 5. When the mobile terminal is located in the intersection of coverage areas A and B, the AMS Wireless must decide to which access point the user should be connected to. An example of interactions between the OSKVM planes to deploy an end-user service is described hereafter and represented in Figure 6.

Consider a user approaching the wireless environment in Location A, namely a location in which a unique wireless access controller is able to connect the end-user. In this situation the Service Enablers Plane detects the profile of the user *(detectUser)*. The interactions *Authorisation, Authentication, Accounting* in the Service Enablers Plane make sure that the end-user is effectively subscribed to the service it is trying to invoke and if so, it allows the end-user connection.

In the Knowledge Plane the context of the user is updated *(updateContextInfo)*, in this case, updating the location of a new user (Location A).

The Service Enablers Plane communicates the Management Plane that a new service is being invoked and that it needs to be provisioned with some guarantees *(newServiceInvocation)*. At this moment the Management Plane representation is divided in two parallel management plane tasks, namely the AMS Fixed and the AMS Wireless.

Being the end-used in the location point is a fact that is sensed by the AMS fixed *(contextSensing(user): LocationA)* as this information is part of the context information to which it is subscribed to previously. The AMS fixed autonomously executes the management tasks needed to fulfill the end-user requirements according to its profile. The result of these management tasks is the setting up of VPN1 between the video server and the virtual router (see Fig. 5) with which the wireless access controller A will hand in the content to the end user *(setUpVPN1)*. The setting up of the VPN1 will be achieved with the help of the virtualization interfaces.

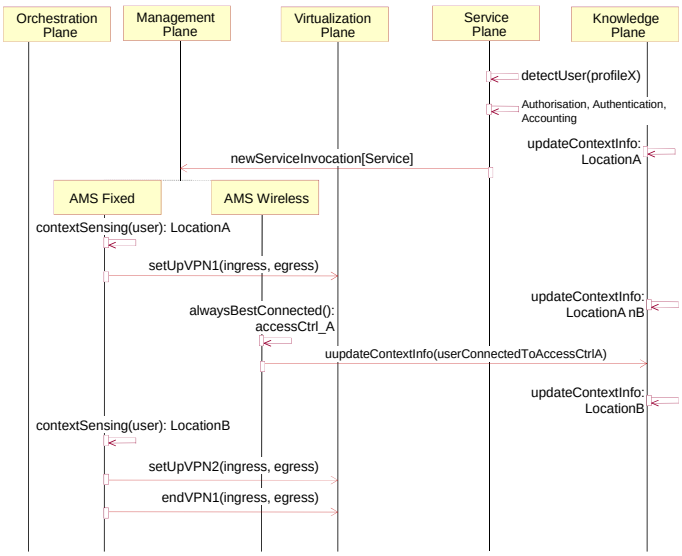

Figure 6. OSKVM planes interactions for the service provision

Now consider the case where the end-user moves towards a location in which both access controllers can connect the end-user. The interaction *updateContextInfo:LocationA∩ B* in the Knowledge Plane considers the case when the end-user moves from Location A to Location A∩ B. Under these circumstances the AMS wireless is in charge of deciding to which access controller the end-user will be connected *(alwaysBestConnected)*. For this, the AMS wireless evaluates a number of facts such as user load, profile, etc for such decisions. In this case, let us consider that the result of the Always Best Connected actions in the AMS wireless result in the end user kept connected to Access Controller A. The interaction *updateContextInfo(userConnectedToAccessCtrlA)* from the AMS wireless to the Knowledge Plane is to inform that the end-user is still connected to the access controller A. This is relatively important as a change in the context of this kind may have effects in the AMS fixed.

Finally, consider the case where the end-user moves to Location B *(updateContextInfo:LocationB)*. Hence the interaction *contextSensing(user):LocationB* in the AMS fixed Management Plane is important as it senses that the end-user has changed its location and that such a change is relevant for its management tasks. Namely the two interactions *setUpVPN2* and *endVPN1* between the AMS fixed and the Virtualisation Plane are the result of the management tasks in the AMS fixed as a result of the user being connected to the access controller B (see Fig. 5). Here VPN2 is created to enable the transmission of the packet stream from the content server to the access controller to which the user is connected to. Also the VPN1 is no longer needed and it is ended to release resources – *endVPN1*.

V. Relevant Technical Difficulties

The five OSKVM planes of the Autonomic Internet approach positioned in this paper is an ongoing work. In our efforts to capture a wide range of requirements for the management of the Future Internet we proposed this multiple plane solution and specified its functionality. A time consuming issue that is still under development is the interfacing between all these layers. Traditional approaches cannot provide an all-in-one solution as we are looking for an open and interoperable platform.

Two important functional components, AMSs and DOCs are defined in our solution. DOCS can be seen as components in charge of "managing the autonomic management systems" with dynamic on demand deployment and orchestration. The above definition is a novel contribution of the AUTOI approach. The meta-management function implemented through DOCs is justified in our architecture but its complexity demands a large amount of work to locate and resolve the conflicts in its functionality and responsibilities such as stability and convergence amongst other crucial issues.

The dynamic on demand deployment of complex components, as AMSs are, is also an open issue. The automation in this process handled by DOCs in cooperation with the knowledge layer is our goal. Human intervention must be minimized but dynamic deployment of AMSs that are not described as simple algorithmic control loops is a rather challenging goal. We have proposed some concrete examples but we have not yet specified the exact course that such a process would follow along with the implementation specifics.

Autonomic systems are mainly intelligent systems. Cognition, that involves sensing, reasoning, understanding and reacting, is applied to network management in order to adapt the system to the chaotic ecosystems of NGNs. Cognition, together with cooperation offered by the DOCs were selected as the main principles for creating autonomic network management systems. The injection of intelligence into machines making decisions was examined from multiple view points but a concrete and specific realization is a rather difficult task.

A step towards intelligence is the knowledge layer that we incorporated in our architecture. A clear definition for a simple distributed knowledge repository was given along with details about the interfaces to access it from other layers. The concept of knowledge retrieval, classification and management is vital in autonomic systems and in our architecture. Nevertheless we need to further explore issues like knowledge formalization, representation and exchange in our knowledge layer.

Appropriate formats must be selected to represent and exchange our models and ontologies. The equilibrium between computational resources and knowledge processing techniques must be met in the network management domain.

AUTOI was based on the definition of a common information model. During its development the need for multiple extensions to fully cover our needs was obvious. The compatibility with existing modelling approaches regarding the general view of the domain as well as the formalization and representation of the model was also examined. For example a simple Finite State Machine model was incorporated at the beginning for testing reasons with the perspective of integrating a full model from the existing ones if the need should arise. Compatibility when it comes to modeling is of major importance because it is almost impossible to foresee all needs of the future chaotic network management scenarios.

VI. Conclusions & Future Work

The Autonomic Internet approach [1] is an ongoing effort. In this paper we have described the principles of a management solution for Future Internet Networks according to our viewpoint, and in turn have positioned this solution in a simple wide ranging scenario. The distributed systems and their interactions to cope with such a case scene have been presented in an affordable manner.

In our research efforts, future work will be devoted to design and implement the instruments that will help validating our OSKVM planes solution; Distributed Orchestration Components, Autonomic Management Systems, Information and Context Services, Virtualisation interfaces, Service Enablers Plane instruments for programmability and the rest of the supporting services will be pivotal in the second year of our project.

Currently, several research initiatives are being carried out around the world, however, there is still very little consensus on how the Future Internet will be, the structure it will have, the services it will support, and the manageability paradigms that are still undiscovered. We hope that the ideas and the management viewpoint presented in this paper may be able to contribute solving the management paradigm for the Future Internet.

Acknowledgment

This work is partially supported by the European Union through the 7th Programme Autonomic Internet (AUTOI) project. We would like to acknowledge all the participants that have contributed with their ideas to this paper.

References

[1] Autonomic Internet (AutoI) Project http://ist-autoi.eu/autoi/
[2] AKARI "Architecture Design Project for New Generation Network" http://akari-project.nict.go.jp/eng/index2.htm
[3] FIND "Future Internet Design" http://www.nets-find.net/
[4] GENI "Global Environment for Network Innovations" http://www.geni.net
[5] EU-IST – Ambient Networks http://www.ambient-networks.org/
[6] EU IST FP6 ANA Project "Autonomic Network Architectures" http://www.ana-project.org/
[7] EU IST FET CASCADAS "Component-ware for Autonomic Situation-aware Communications, and Dynamically Adaptable Services" http://www.cascadas-project.org
[8] EU IST BIONETS "Biologically-inspired autonomic Networks and Services" http://www.bionets.eu/
[9] EU IST FP6 HAGGLE "An innovative Paradigm for Autonomic Opportunistic Communication" http://www.haggleproject.org
[10] EU IST FP6 EFIPSANS "Exposing the Features in IP version Six protocols that can be exploited or extended for the purposes of designing or building Autonomic Networks and Services" http://www.efipsans.org
[11] A. Galis, S. Denazis, A. Bassi, P. Giacomin, A. Berl, A. Fischer, D. H., J. Strassner, S. Davy, D. Macedo, G. Pujolle, J.R. Loyola, J. Serrat, L. Lefevre, and A. Cheniour. A management architerture and system for future internet networks. Future Internet Assembly Book (to be published by IOSPress), Future Internet Assembly FIA Conference Prague, 2009
[12] Cheng, L., Galis, A., Mathieu, B., Jean, K., Ocampo, R., Mamatas, L, Loyola, J.R, Serrat, J., Berl, A., de Meer, H., Davy, S., Movahedi, Z., Lefevre, L., - "Self-organising Management Overlays for Future Internet Services"- IEEE Manweek 2008 /MACE 2008; 22-26 Sept. 2008, Samos, Greece
[13] Kephart, J.O., Chess, D.M."The Vision of Autonomic Computing", IEEE Computer", January 2003
[14] B. Jennings et al. Towards Autonomic Management of Communications Networks. IEEE Communications Magazine, 45(10):pp. 112–121, 2007.
[15] Berl, A., Fischer, A., de Meer, H., Galis, A., Loyola, J.R.-" Management of Virtual Networks"- IEEE Manweek 2008/ EVGM 2008; 22-26 Sept. 08, Samos Greece
[16] E.K. Lue et al. "A Survey and Comparison of peer-to-peer overlay network schemes". IEEE Communications Survey and Tutorial, March 2004