Objective ICT-2007.1.1

The Network of the Future

Project 216041

"4WARD – Architecture and Design for the Future Internet"

D-4.1
Definition of scenarios and use cases

Date of preparation: **09-04-02**
Start date of Project: **08-01-01**
Project Coordinator: **Henrik Abramowicz**
Ericsson AB

Revision: **2.0**
Duration: **09-12-31**

Document Properties:

Document Number:	FP7-ICT-2007-1-216041-4WARD / D-4.1
Document Title:	**Definition of scenarios and use cases**
Document responsible:	Fraunhofer
Author(s)/editor(s):	Editors: Rudolf Roth, Fabian Wolff, Tanja Zseby (Fraunhofer); Susanne Engberg, Catalin Meirosu, Johan Nielsen (EAB), Mads Dam, Alberto Gonzalez, Rolf Stadler (KTH) Dominique Dudkowski, Chiara Mingardi, Giorgio Nunzi (NEC) Frank-Uwe Andersen (NSND) Victor Marques, Vitor Mirones, Susana Sargento (PTIN) Kurt Eder, Attila Katona (Siemens ROM) Tudor Mihai Blaga, Andrei BogdanRus, Virgil Dobrota (TUCN) Avi Miron (Technion) Stefan Schnitter (DT) Miguel Ponce de Leon, Chris Foley, Sasitharan Balasubramaniam (TSSG)
Target Dissemination Level:	PU
Status of the Document:	Final
Version	2.0

This document has been produced in the context of the 4WARD Project. The research leading to these results has received funding from the European Community's Seventh Framework Programme ([FP7/2007-2013] [FP7/2007-2011]) under grant agreement n° 216041

Abstract:

Limitations of traditional network management make new approaches necessary to successfully cope with management challenges of the future Internet. 4WARD In-Network Management addresses deficiencies of traditional network management by placing management functionality inside the network close to the nodes.
As starting point for the research in In-Network Management scenarios and use cases have been selected, which are described in this document.
The four scenarios comprise self-Management in wireless multi-hop networks, network management in large operator networks, home networks and large-scale adaptation in response to dramatic events.

Keywords:

Future Internet, In-Network Management, scenarios and use cases, scalable and robust management systems, self-managing capabilities, self-organisation, situation awareness

Table of Contents

Executive summary

The 7th Framework Program project 4WARD addresses Architecture and Design for the Future Internet. It is developing a set of radical architectural approaches following a clean slate approach.

The current document is the first deliverable coming out of the In-Network Management work package. It describes a core set of scenarios and use case that will guide the further work performed in the work package.

The goal of In-Network Management is to overcome limitations of traditional network management: it is developing engineering principles for automated configuration management, but also real-time monitoring functions that trigger adaptation of configuration. In-Network Management will support future large-scale networks that self-configure, dynamically adapt to external events and allow for low-cost operation. Its key idea is that management stations outside the network delegate management tasks to a self-organizing management plane inside the network.

In order to kick-off the work on In-Network Management a problem-driven approach has been adopted. As starting point for the research concrete scenarios and use cases have been selected that allow for a fundamental analysis of management problems encountered in the future Internet.

The four scenarios that have been selected highlight the wide range of challenges. They address self-management in wireless multi-hop networks, network management for a large operator network, management needs of home network environments, and management strategies availability under extreme conditions like catastrophes and natural disasters. For each scenario major use cases have been identified that analyse in more detail and on a concrete level the specific problems of that particular environment.

Based on the scenarios, evaluation criteria are derived that provide guidance for the follow-up activities in the work package and also offer the opportunity of a common ground for the cooperation between the other project work packages to help in the integration into a coherent overall framework of the various tracks of research performed by 4WARD.

Chapter 1 Introduction

1.1 Motivation of document

The work dedicated towards network management in 4WARD is triggered by limitations becoming apparent in current network management. Today's centralised network management will no longer be applicable to the large-scale, possibly ad hoc networks foreseen in the future; therefore new approaches for management architectures are needed.

4WARD In-Network Management addresses these challenges by introducing a thin, pervasive layer which performs core management functionalities already inside the network, but which can be complemented by additional management functionality outside the network where necessary.

The approach adopted by the work package is problem-driven. Concrete scenarios and use cases have been selected to serve as starting point for the research; they allow for a fundamental analysis of management tasks that need to be addressed in the future Internet.

This document presents the initial results of that problem analysis. Its goal is to come up with a small set of scenarios and use cases that are representative for the full range of challenges encountered in this area. They are chosen to demonstrate where traditional management approaches fall short and new approaches are needed. For each scenario, use cases are defined that describe required functionality from network management functions and requirements concerning aspects such as functionality, scalability, efficiency, timeliness etc.

The scenarios create awareness for the complexities that need to be addressed in the project, and they will allow for a test and validation of the generality of the proposed In-Network Management approach at later project stages.

1.2 General presentation of the 4WARD project

4WARD aims to increase the competitiveness of the European networking industry and to improve the quality of life for European citizens by creating a family of dependable and interoperable networks providing direct and ubiquitous access to information. These future wireless and wire-line networks will exploit all available resources and be readily adaptable to current and future needs, at acceptable cost. 4WARD´s goal is to make the development of networks and networked applications faster and easier, leading to more advanced and more affordable communication services.

1.3 Presentation of related Work Packages

1.3.1 WP1: Business Innovation, Regulation and Dissemination (BIRD)

WP1 follows the idea that research on technology should be accompanied by research on the context of its intended usage. The BIRD WP covers non-technical topics and focuses especially on society, business and governance issues. It ensures that their requirements are properly addressed with the technical solutions developed within the other work packages. The non-technical issues considered in WP1 are structured into three main themes:

- **“Usage and Service”** investigates how users will benefit from the new technologies developed in 4WARD. Usage scenarios and service concepts are evaluated.
- **“Socio Economics”** investigates the impact on the society as well as on global business approaches on new and existing players. Business models are analysed and new market opportunities are investigated.
- **“Policy and Governance”** includes the principle of “network neutrality”. The impact of existing regulation and hypothetical regulation for the future internet is investigated.

The relation with WP4 can be summarised as follows:

- The scenarios defined in this document can form a valuable input for those non-technical topics since they highlight selected areas, where change is needed and anticipated in future technical solutions from the perspective of network management. Those changes will surely effect society, business and governance issues.
- WP4 will evaluate its network management framework regularly with respect to the hypothetical regulation considered in WP1 and validate if the designed functionality matches the usage patterns and service requirements that are foreseen by WP1. This effort has to be implemented as a continuous process.

1.3.2 WP2: New Architecture Principles and Concepts (NewAPC)

WP2 NewAPC is exploring the development of a design process for combining existing, or specifying and generating new networks with customised architectures. To enable very different architectures to co-exist and inter-operate in a cost-efficient manner, NewAPC is creating a framework that will allow these many networks to bloom as a family of interoperable networks coexisting and complementing each other. Different networks will be able to address individual requirements such as mobility, QoS, security, resilience, wireless transport and energy-awareness.

In relation to WP4, it is necessary that the key topics being undertaken by In-Network Management are threaded in a coherent way into the overall architectural concept(s), as proposed in WP2. Examples of these topics are:

- Thin pervasive self-organizing network management plane.
- Registration and access mechanisms for embedded self-descriptive management functions.
- Scheme, strategies, and protocols for collaborative monitoring, self-optimizing, and self-healing.

An additional point of contact with WP4 is the identification and definition of technical requirements steering the development of the architectural framework along a set of architectural themes and to develop an approach for analysing dependencies & tradeoffs and functional integrity of such In-Network Management choices.

1.3.3 WP3: Network Virtualisation (Vnet)

WP3 will investigate the approach of using virtualisation to enable flexible and innovative networking architectures. Virtualisation allows an evolution of communication technology while largely reusing deployed infrastructure. It further provides a general framework for network sharing: providing different networking services of different network service providers on a common physical infrastructure.

The relationship with In-Network Management (INM) exists at two levels. On a first level, WP3 requires a set of management functionalities to support virtual networks on top of the underlying physical infrastructure. Such management functionalities can include monitoring of network-wide status information, identification of faulty nodes or service discovery and they are needed to bootstrap a virtual network and to maintain the physical resources supporting it. On a second level, virtual networks act as independent networks and therefore require management functionalities for maintenance purposes. These management functionalities must operate over the virtual resources instantiated by WP3 and include monitoring of QoS or self-healing.

1.3.4 WP5: Forwarding and Multiplexing for Generic Paths (Formux)

WP5 is focused on development of a model and underlying mechanisms for generic path abstraction that would provide unified means for applications to address transport capabilities of the network. Generic path is expected to provide enhanced performance and resilience of the transport service by exploitation of recent advances in transport techniques like e.g.

multipath routing, network and cooperative coding, and swarm communication. The research in WP5 is split into four main streams:

- **"Generic paths by cooperation and coding mechanisms"** investigates techniques that can effectively support a single generic path. In particular, network coding and cooperative coding, and also code mobility are considered.
- **"Realising a generic path by routing"** investigates techniques for efficiently supporting a single generic path. Design of scalable routing protocols with mobility support that adapt to the varying structure of wireless and mobile networks as well as the state of the underlying heterogeneous physical environment is of particular interest.
- **"Interaction of multiple generic paths"** aims at design and evaluation of principles, mechanisms, protocols, and algorithms to manage shared physical resources between multiple generic paths.
- **"Mobility support by generic path"** investigates support of mobility by generic paths in a multi-homing environment. In particular, the aim is on the use of link parameterisation and context awareness for a mobility management scheme that knows about wireless technology behaviour.

In terms of its internal operation, generic path (GP) can be expected to be a dynamic entity able to adapt to changing conditions (e.g. state of underlying resources or location of mobile end-points). Depending on type of GP, such adoption can be achieved by either using internal mechanisms of GP (possibly specific) or relying on the features already available at the network level. Thus, both WP4 and WP5 can impact each other in at least two canonical ways.

In the case of self-sufficient GP, WP5 could define requirements for WP4 concerning the information about the network to be provided by INM to GP (e.g. network topology, link characteristics). It is interesting that in this case, internal management of GP (although separate as a *GP management plane instance* from the INM management plane instance that is operating at the network level) can at least partially be based (inherited from) the model defined by INM. The latter would thus enhance the applicability of INM framework as such. In the second case, when GP relies on INM features (e.g. failure protection capabilities), WP5 can define requirements regarding the functionalities of INM so that GP can achieve its overall goals. It is to be expected that achieving a good balance between both approaches will be a significant architectural challenge.

1.3.5 WP6: Network of Information (NetInf)

The overall objective for WP6 is to investigate a new information architecture, called NetInf, where information retrieval and storage act on the objects themselves rather than on the nodes. The main components of NetInf are a modelling framework that facilitates objects to be discovered and used on the basis of their names, and a reference model specifying the syntax and semantics of object operations. In addition, specific networking services and mechanisms are used within the architecture. The architecture is based on two boundaries, a lower API towards infrastructure such as ForMux (WP5) and an upper level API to for example applications.
WP6 and WP4 are related in that WP4 intends to use the NetInf results as part of the INM framework and the NetInf architecture will make use of self-management guidelines of INM.

1.4 Objective of document

Out of a pool of potential scenarios, four scenarios have been selected that highlight management challenges in the future Internet. They comprise issues of

- self-management in wireless multi-hop networks,

- management requirements in the networks of a large operator,
- the management needs of home networks environments, and
- preservation of network availability under extreme conditions such as catastrophes and natural disasters.

Within each scenario a major use case is identified which allow to analyse in more detail and on a concrete level the specific problems that arise in this particular environment.

The environment of wireless multi-hop networks is characterised by mobility and high dynamicity building strongly on peer-to-peer principles, such that traditional centralised management approaches are no longer feasible. The second scenario looks at the evolution of today's core network infrastructures. Operators will highly benefit from improvements in management technology leading to a reduction in operational costs and increasing efficiency. Home networks represent a major market for the future Internet. This environment relies on plug and play solutions that do not require maintenance operations from the user. Particular challenges will arise through inter-connection to multi-providers of services, which will require cooperation of the various involved players. The pervasiveness of networking and the dependency on network availability for critical infrastructures is highlighted in the last scenario *networking under extreme conditions* which may arise in case of catastrophes or natural disasters; these conditions will put a challenging stress test on the management solutions proposed by the work package.

Based on the scenarios, evaluation criteria are derived that provide guidance for the follow-up activities. The scenarios represent a useful tool in the further work within the work package and offer the opportunity to create a common ground for the cooperation between the other project work packages supporting the integration of various tracks of research performed with 4WARD.

1.5 Structure of document

The document is organised as follows:

Chapter 2 starts with the motivation for In-Network Management, which is triggered by up-coming challenges in the future Internet and obvious limitations of traditional network management approaches to appropriately respond to them. This situation is contrasted in Chapter 3 with the vision of the 4WARD In-Network Management approach, which places management functionality inside the network close to the nodes, and it sketches basic concepts for a distributed self-organising and self-adaptive management plane. Based from this analysis, key issues regarding In-Network Management are discussed in Chapter 4 .This is complemented by an in-depth discussion of current State of Art with respect to In-Network Management in Chapter 5 . The chapter lists relevant projects and initiatives and identifies enabling technologies, paradigms and models that are expected to become promising candidates for application within In-Network Management.

Chapter 6 represents the core part of the current document. It identifies a set of scenarios that provide a reference framework for the research activities around In-Network Management.

The selected scenarios comprise:

- self-management in wireless multi-hop networks (Sec 6.2)
- networks of a large operator (Sec. 6.3)
- home networks (Sec. **Error! Reference source not found.**)
- networks under extreme conditions (Sec. 6.4)

For each scenario we first describe the general networking environment that applies and identify key challenges that arise in this specific context. A more detailed use case is then

selected. The current state of the art is discussed and the limitations of traditional management approaches in this field are pointed out. This is contrasted with the benefits that we expect from an In-Network Management approach; and requirements that need to be addressed by the In-Network Management solution are identified. At the end we indicate relationships and potential areas for collaboration with other work packages in the project.

The subsequent Chapter 7 discusses evaluation criteria derived from the scenario work and steps how to apply them to the results developed in the work package. The conclusion Chapter 8 summarises the major achievements so far and sketches next steps to be undertaken by the work package.

Chapter 2 Motivation for a new Network Management Paradigm

In traditional Internet management, the management functionality resides outside the network, in management stations and servers. These entities interact via management protocols such as SNMP or CLI with the network elements to execute FCAPS management functions (Fault, Configuration, Accounting, Performance, Security management). In commercial networks, these interactions often occur out-of-band, through special communication networks.

Such a management approach has proven successful for relatively small networks (up to hundreds of nodes) and static configurations. For emerging large-scale, dynamic network environments however, the approach turned out to be inadequate and alternative approaches must be developed.

The time and cost of deploying, configuring and operating networks, already significant today, is expected to grow even further due to the exponential growth in numbers of network elements in the Internet, mobile networks, etc. Furthermore, the increasing sophistication and dynamic nature of many new networks and services adds to the complexity of the management task. The solution is to increase the level of automation and manageability by

1. automating as large a part of the configuration process as possible, and
2. providing accurate, real-time, and easily configurable estimates of global or aggregated network state for human feedback and control.

The ultimate goals are to support future large-scale networks that will self-configure, dynamically adapt to external events, allow for low-cost operation and minimise the need for human intervention.

Current practices in configuration management are generally performed through low-level interfaces on a per-device basis. However, it is hard if not infeasible to generate, validate and tune configuration parameters per-device in large-scale networks. On the other hand, many of the existing top-down configuration approaches lack scalability and testability in operational networks. Similarly, existing end-to-end monitoring applications usually depend on low-level network activity information, such as traffic counters, MIB variables, device logs, and alarms. A major challenge then is how to efficiently aggregate and analyse these data to construct high-level views of network operations in real-time.

From the point of view of a network administrator, manual interaction is generally required for management tasks, involving analysis of the monitored data and giving low-level commands to the managed devices. Such manual interventions are error-prone and expensive, and should be eliminated as far as possible. Furthermore, the lack of self-optimizing management functions leads network operators to overprovision network resources, which results in a high level of capital expense. Lastly, the Future Internet will be richer in terms of services offered, technologies employed, business models and many other drivers that are beyond of what current management solutions can sustain. Consider the multitude of networked devices that will be present in homes and will need to cooperate in order to provide reliable operation and enable converged multimedia services; at the same time, other devices, such as networked sensors and controllers, will become ubiquitous and will require management support.

Limitation of current management solutions will be exemplified and illustrated in Chapter 6 with a list of scenarios and use cases. There, we will also show the potential benefits of In-Network Management in those scenarios.

Chapter 3 4WARD Vision and Key Idea of In-Network Management

In order to overcome the limitations of current management technologies discussed in the previous chapter, we envision a new paradigm for network management, which we call *In-Network Management*. Its key idea is that management stations outside the network delegate management tasks to a self-organizing management plane inside the network.

The goal of In-Network Management is to achieve scalable, robust management systems with low complexity for large-scale, dynamic network environments. The guiding principles to achieve this goal are decentralisation and self-organisation.

The realisation of the In-Network Management paradigm includes developing a network management plane that self-configures and dynamically adapts to changes in networking conditions. The plane provides communication and coordination primitives for a range of distributed management functions.

The In-Network Management paradigm can be interpreted as pushing management intelligence into the network, and, as a consequence, making the network more intelligent. The network, which now includes the management plane as a part, can execute end-to-end management functions on its own and perform, for instance, reconfigurations in an autonomous fashion. It reports results of management actions to an external management system, and it triggers alarms if intervention from outside is needed.

Figure 1 shows the main difference between In-Network Management (right side) and traditional approaches (left side) regarding the components and their interactions.

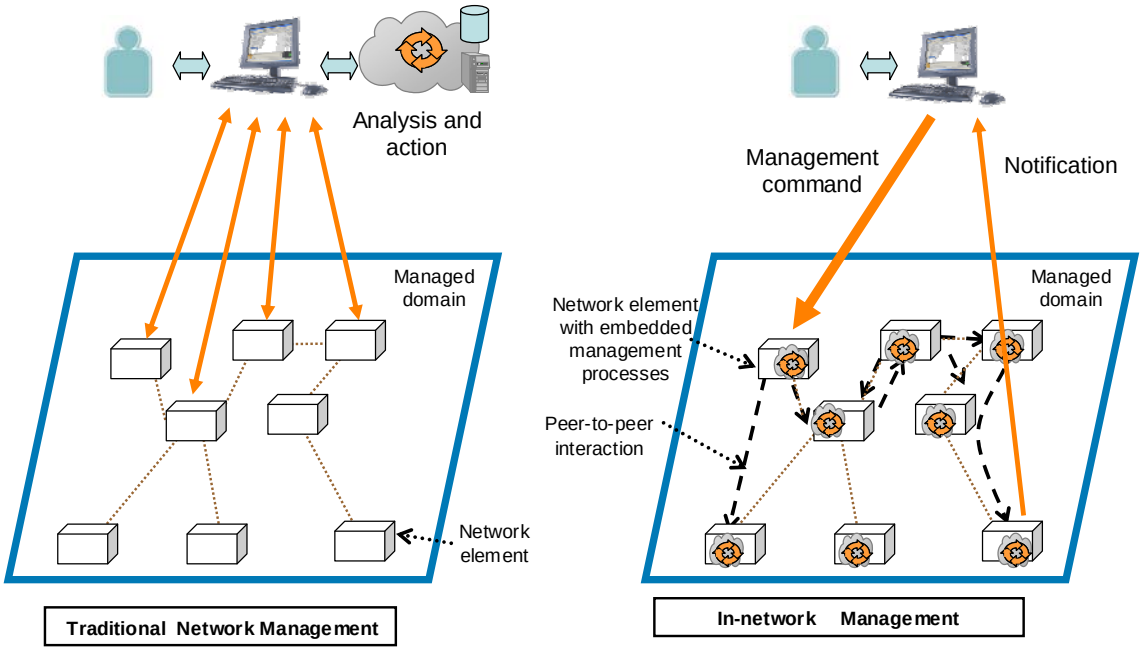

Figure 1 Comparing traditional network Management (left) with In-Network Management (right).

In traditional management approaches, the external management system interacts with each managed device individually. First, it polls the devices for learning their states. Then, it analyses the states and determines the actions to execute, taking into account business policies. Finally, it executes these actions in a per-device fashion, e.g., through remote CLI commands. This control loop is generally initiated and supervised by a human administrator.

In contrast, with In-Network Management, external management entities do not interact with each managed device individually. Instead, they interact with access points of the management plane (Figure 2), which provides network-wide management functionality. To provide this functionality, the management plane executes a set of distributed, self-stabilising protocols for monitoring and control.

Figure 2 shows a possible realisation of the management plane. It includes management processes that are associated with network devices and communicate with neighbouring processes through an overlay. Every process serves as an access point for In-Network Management operations.

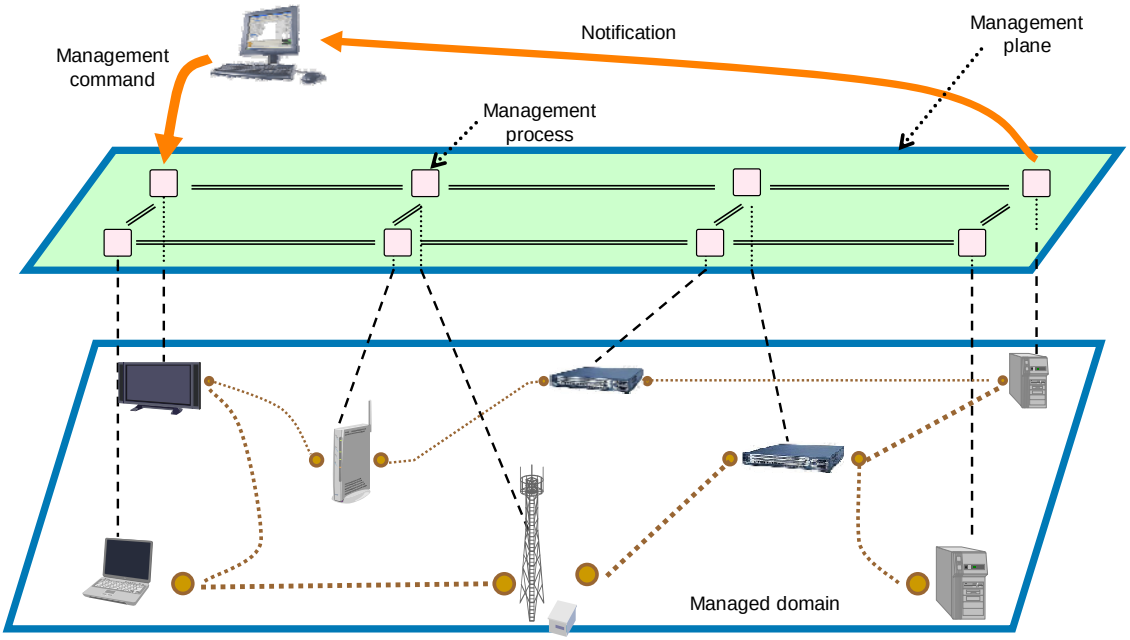

Figure 2 Management plane for In-Network Management.

In-Network Management calls for a device to have embedded "default-on" management capabilities, consisting of several autonomous components which interact with each other in the same device and with components in neighbouring devices. The architecture of In-Network management first of all models how management capabilities are embedded inside the services of a node. On this basis, it is then possible to compose them, in such a way that the embedded functions are coordinated with each other. Out of smaller autonomous components, more complex management functions can be constructed in the management plane. Additionally, Figure 2 shows that communication between network elements is based on peer-to-peer paradigms: In-Network management relies on different propagation schemes to enforce management processes in the network.

In-Network Management relates to autonomic management in two ways. First, the management plane inside the network is self-organizing and exhibits autonomic behaviour. Second, the functions that the management plane offers are either autonomic themselves, for instance distributed fault diagnosis and self-healing, or they are building blocks for autonomic management functions. For example, many autonomic functions require the availability of real-time network-wide state information.

In the 4WARD project, we will develop and evaluate the above described idea for In-Network Management. Specifically, we will develop a framework that identifies the components and their interactions. We will provide descriptions of how functions in the management plane can

be discovered and accessed, how they interact with each other, how inter-domain management can be realised, etc. Using this framework, we will develop a range of distributed algorithms for situation awareness and anomaly detection. Based on this functionality, we will further develop a set of algorithms for auto- and re-configuration and self-healing. Selected functions of the management plane will be evaluated in a prototype implementation.

We believe that In-Network Management will be particularly beneficial in large-scale, dynamic network environments. In-Network Management capabilities will allow for a level of real-time awareness of the network behaviour that is not feasible with current management technology. Further, we envision that the management plane will typically reconfigure within a sub-second, in response to node addition or failure, and resume correct operation thereafter. Such a capability will significantly reduce the reaction time in comparison to today's centralised management systems, specifically in large networks.

Chapter 4 Key Issues for In-Network Management

We have identified the following set of general key requirements that a holistic INM architecture should take into account. Of course, due to time constraints within the project it might be not possible to address all of them, thus the main part of the work will rather deeply focus on a set of key requirements than trying to plainly touch all of them. While this compilation is not exhaustive, it may be used as a background for assessing existing work related to INM in Chapter 5 and the scenario descriptions in Chapter 6 as well as a guideline in the design of the INM framework and algorithms that follow in subsequent deliverables of Work Package 4.

Scalability: INM must support scalability in terms of network size (i.e. the number of network components to be managed) and in terms of the number of management tasks, which also grows with the network size.

Heterogeneity: INM must support heterogeneity on different dimensions, such as heterogeneous devices (different manufacturers and vendors, proprietary network components and functionality), heterogeneous network structures (MANETs, WSNs, WMNs, wireless access networks, hybrid network structures, etc.), and heterogeneous environments (homes, cars, offices, open country).

Interoperability: INM relies on interoperability between different devices to support management operations. The coexistence of different interfaces and information models should be avoided, because it poses a serious limitation to the degree of automation in the network.

Real-Time-Support: INM should support management operations within limited time constraints, i.e. real time. The limits of these time constraints may be specific to every application and refer in general to the absence of mistakes in that application due to delays in the management operations.

Robustness: INM must be robust with respect to failures in components and subsystems, with respect to potential attacks (security), and with respect to incomplete or inaccurate information that is available (data collection).

Small Footprint: INM must have a small footprint with respect to storage space, bandwidth consumption, energy consumption, and other resources, in order to impact the network to the least extend possible and avoid side-effects.

Level of Localisation: The localisation of management tasks / control loops to a small subset of components is a prerequisite for scalability and a small footprint. In other words, the more localised a management application can be executed, the larger the number of management tasks that can be executed at the same level of resource utilisation.

Level of Integration: Management tasks need to be tightly integrated within network components and subsystems (compare to external, partially embedded (e.g. only monitoring), and fully embedded (inseparable management capabilities in network components)).

Comprehensiveness of Management Information Model: The Information model of INM must be comprehensive in the sense that it must provide sufficient expressiveness (to capture various types of management tasks), extensibility with respect to future requirements (e.g. energy management), and flexibility (e.g. only partial implementations for lightweight management tasks).

Functional Comprehensiveness: INM must provide functional richness to support a variety of essential management tasks (e.g. fault detection and remedy), it must be possible to specify tasks on different levels of abstraction (→ degree of specification of a task, see [MartinFlatinEtAl1999a]), and allow tasks to be translated to concrete implementations in different environments (e.g. WSNs, WMNs).

Interactivity: INM must provide the possibility for humans to intervene on different levels of abstraction – this requires abstract and clear interfaces to the outside to bridge between human understanding and implementations at the lowest level. An extreme approach to this requirement would be to have flexible views to management operations, where the interface can be adapted with respect to the information presented.

Comprehensibility: INM must be comprehensible in the sense that it is possible to understand parts of the INM system, for example, in situations of failures that cannot be resolved by INM itself and that still require human assistance.

Adaptability: The overall INM must be able to embrace current and proprietary technologies, allow them to be maintained in existing systems, and allow migration/evolution to new approaches (that are more INM-like) with respect to new system components, network technologies, functionality, etc.

Security: INM must address security along different dimensions, e.g., as to what extend autonomy can be granted to management algorithms, in order to avoid parts of the overall system to be compromised or harmed in their operation.

Learning: INM must provide mechanisms to learn new knowledge about the network. For example, patterns of performance values about faulty conditions can be identified and registered to prevent other faults in the future.

Extensibility: INM must assure that capabilities of nodes can be extended with new functionalities. New functionalities could be added locally in a node or discovered dynamically in the management plane.

Chapter 5 State-of-the-Art

This section reviews the state-of-the-art related to our vision of In-Network Management (INM). While we focus on general approaches that are relevant for the overall INM architecture pursued within Work Package 4.2, more specific work will be presented within the scenario descriptions in Chapter 6 and complement this general presentation.

The authors of [MartinFlatinEtAl1999a] distinguish management approaches by the *organisational model,* structured into centralised, weakly distributed and strongly distributed approaches. This model is helpful in a coarse categorisation of paradigms in network management and to distinguish between traditional and more comprehensive approaches.

Centralised paradigms with *no distribution* include e.g. SNMPv1 as described in [RFC1155], and generally consider a single manager only. *Weakly distributed* approaches with a hierarchical structure, composed of a few managers whose function is mainly limited to collecting data, includes, among others, SNMPv2 [RFC1441] and SNMPv1 in conjunction with Remote Monitoring (RMON) [RFC2819]. While the former introduces the concept of intermediary managers and communication between these, the latter includes the concept of monitors and probes and goes one step further in distributing management functionality, allowing decisions to be made outside the agent and local to an occurring anomaly [BoutabaAndXiao2002a].

These and related traditional approaches do not meet many of the requirements stated in Chapter 2 For instance, due to the management capabilities being located outside the network within dedicated managers, these systems have only very limited scalability and are vulnerable to failures that could render the management subsystem of a network non-functional (robustness). Furthermore, heterogeneity is a major issue due to the coexistence of e.g. SNMP and CMIP in different network domains (IP versus Telecom) [MartinFlatinEtAl1999a].

More comprehensive management approaches are *strongly distributed,* including *hierarchical* and *cooperative* paradigms. In the following we will focus on this third group and first discuss a number of general management architectures, followed by major projects with significant contributions to autonomous network management. We then state some enabling technologies, paradigms and models that should be considered in the design of INM architectures. We then conclude briefly our discussions.

ASA – Autonomic Service Architecture

The authors of [ChengEtAl2006a] introduce the *Autonomic Service Architecture (ASA)*, a framework for autonomic management of service delivery over IP networks. This research addresses both service and network management, introducing different levels of abstraction where services are built on top of virtual and physical resources. The concept of virtual resources allows simplifying resource management providing a uniform interface for all the heterogeneous physical resources, such as routers, links and storage devices.

The design of ASA has the main goal of enabling autonomic management of resources so that Service Level Agreements (SLA) between service providers and customers are guaranteed anytime. All management functions are performed by entities called Autonomic Resource Brokers (ARB), which are organised in a hierarchical structure and interact with underlying virtual resources and other ARBs. The authors show how ASA can be applied to the management of DiffServ/MPLS networks and propose an autonomic resource sharing scheme, in which the spare capacity in underloaded SLAs can be borrowed by overloaded SLAs.

The main advantage of ASA is that it is a generic architecture, which encompasses different abstraction layers and heterogeneous resources. However, it is characterised by a high level

of complexity, both in the hierarchical structure of the management entities and in the internal structure of such entities as well.

FOCALE – Foundation Observation Comparison Action Learn Reason

The *FOCALE* autonomic network management architecture is presented in [JenningsEtAl2007a, MeerEtAl2006a]. It emphasises the use of information and ontological modelling to gather knowledge about network capabilities and constraints and to get an abstract representation of vendor specific functionalities. This approach also accentuates the role of policies as a way to express business rules that determine how resources in the network should be used and optimised.

One main goal that drove the design of the architecture is to make it adaptive to changes in the environment, business rules and user requirements. To achieve this, FOCALE uses two control loops: a maintenance control loop used when no irregular behaviour is found, and an adjustment control loop, when actions have to be performed or new policies have to be introduced. Moreover, machine reasoning and learning techniques are addressed, in order to analyse knowledge collected into information and data models and automatically generate new knowledge. FOCALE is a distributed architecture, so that it foresees that each network element can incorporate the autonomic management software. Lastly, integration of bio-inspired algorithms into FOCALE is also a future objective.

The FOCALE system is characterised by a high level of autonomy, in that human interaction is only foreseen in the definition of business goals. However, the system is very complex and therefore difficult to understand in case of unforeseen failure of the management system itself. In case of unanticipated situations due to changes in the environment or the development of technologies, some assumptions on which the system is based could be violated and it could become difficult to make modifications in the system to make it aware of new possible conditions. Complexity can also have negative effects as far as security is concerned, making it more and more hard to handle. The goal of an INM solution should be rather the design of an autonomous system which is kept as simple and flexible as possible, providing a balanced level of autonomy and abstract interfaces to allow interactivity with the system.

MANNA – A Management Architecture for Wireless Sensor Networks

Besides these comprehensive management architectures, Ruiz et al. present a management architecture which is targeted specifically to wireless sensor networks [RuizEtAl2003a]. The *MANNA management architecture* utilises models of network conditions, which give an abstract vision of the system. A model representing a given aspect of the network provides the conditions for executing a management function according to management policies. The distribution of management functionalities in the network distinguishes between manager, agent and management information base (MIB). Management can be conducted in a centralised, distributed or hierarchical way, according to the application running on the wireless sensor network, and the locations of manager and agents depend on the kind of wireless sensor network.

The design of the MANNA architecture takes into account specific characteristics of wireless sensor networks, such as energy limitations, high frequency of faults and frequent reconfiguration. Therefore, it should be considered as an approach limited to this particular kind of networks.

Ambient Networks

The Ambient Networks (AN) project was an integrated project (IP) of the Sixth Framework Programme [AhlgrenEtAl2005a, NiebertEtAl2005a, AmbiNetProject]. The project aimed at an innovative, industrially exploitable mobile network solution, which enables the composition of networks across business and technology boundaries in order to make efficient use of infrastructure resources and to stimulate new business developments and growth in the wireless domain.

Of relevance to the research topics addressed by 4WARD In-Network Management are especially the work addressing context, policy and network management [Giaffreda 07]. The project advocated for management approaches that are dynamic, distributed, adaptive, self-managing, self-policing and autonomous responsive to the changes in the networking and context. The functionality of the context management work [Mathieu 07] includes:

- Linking together with appropriate publish-subscribe mechanisms the context clients with the context sources
- Keeping context information up to date and consistently stored across distributed nodes
- Implementing appropriate dissemination mechanisms for the efficient distributed storage of context information
- Providing context clients with the right protocol suite that enables them to query context sources

The work on policy management [Ohlman 06] focused on access control policies by using XACML as policy language.

Policies are stored on two levels. Policies related to node resources are stored on the node itself. Policies related to an Ambient Network are stored in a distributed database accessible to all nodes within the AN.

The network management work contains three contributions. First, it presented a solution for composition management. [Akhtar 07] Its functionality is to manage the logical structure of the control space of composing (and de-composing) networks. The proposed solution supports different types of compositions.

Second, a contribution in the field of self-configuration: a building block that provides general services to other functional blocks to correctly accomplish their configuration tasks [Nunzi 07]. Its main purpose is to guarantee stability of a certain configuration over time and to avoid oscillations. The general problem is that concurrent changes generated by different blocks, can provide results not expected.

Third, in the field of monitoring, an algorithm [Gonzalez 07] that provides an estimation of network-wide variables with the required accuracy and minimal overhead. (Monitoring distributed systems involves the fundamental trade-off between accurate estimation of a variable and the generated overhead). This algorithm creates a self-organizing layer that interconnects management processes on the network devices. This self-organizing layer is scalable, robust and adaptive to networking condition changes.

FP6-IST-27489 ANA – Autonomic Network Architecture

The *Autonomic Network Architecture (ANA)* project is an integrated project (IP) of the Sixth Framework Programme within Priority FP6-2004-IST-4 Situated and Autonomic Communications (SAC) [Sestinim2006a, JelgerEtAl2007a, ANAProject]. The goal is to design and develop a novel network architecture beyond legacy Internet technology that can demonstrate the feasibility and properties of autonomic networking. The ANA architecture will facilitate self-* features such as self-configuration, self-optimisation, self-monitoring, self-management, self-repair, and self-protection.

Of relevance to the research topics addressed by 4WARD In-Network Management are especially the work addressing principles, mechanisms and proof-of-concepts for autonomic network self-management at the node and compartment level. This encompasses functions for monitoring, self-optimisation and resilience.

The goal of the ANA monitoring architecture is to include monitoring as integral part in the network architecture (make it a “first class citizen”). This implies that a set of new requirements has to be addressed: monitoring needs to be dynamic, adaptive and

programmable. In contrast to traditional approaches, monitoring must not assume a priori knowledge about the network itself, but instead monitoring functions may be placed and configured dynamically in the network. For this to happen it is required that modules explore the available monitoring support in their environment at runtime.

Besides performing conceptual work, ANA puts emphasis on prototypical realisation. The architecture relies on the paradigm of functional composition of modules at runtime. A number of functional blocks, called ANA bricks in the project's terminology, are currently under development, including e.g. components for packet capturing, sampling and system monitoring. Typical applications would include management tasks such as adaptive traffic monitoring and management, mobility prediction, self-optimisation and stabilisation, cross-layer optimisation, and measurement-based resilience.

The problem field addressed by ANA is somehow close to the topics addressed in 4WARD InNet Management, because they both aim at increasing the level of automation into the network. Nevertheless ANA should be regarded as a generic architecture for autonomic devices, while InNet Management will leverage on a tight coupling of management functions with the services deployed on a device, like virtualisation of resources or generic paths.

EUREKA/CELTIC Project Madeira

The *EUREKA/CELTIC Project Madeira* [MadeiraProject] developed a distributed network management system (including interworking fault and configuration applications) with self-forming logical overlay topologies that demonstrate performance and scalability for managed WLAN networks of large dimension based on a non-hierarchical peer-to-peer paradigm. This enables self-managed services and network elements of increased scale, heterogeneity and transience.

The Madeira project researched and developed a distributed architecture and framework based on the peer-to-peer paradigm, developed application and data modelling and manipulation functionality and performed detailed case studies on fault management and configuration management based on a common scenario. Furthermore Madeira developed a solution to secure Madeira framework, performed an extended scalability study to improve the framework and developed several demos.

While Madeira developed a peer-to-peer management overlay, 4WARD will place the network management functionality *into* the network, significantly minimizing the need for external management functionalities in the nodes' functionalities. For example, much of Madeira's solutions were supporting fault and performance management, but they did not go towards a general approach for self-configuration in heterogeneous networks. Also, Madeira assumes a single network domain (P2P) while 4WARD assumes also multiple domains.

5.1 Enabling Technologies, Paradigms, and Models for In-Network Management

Complementary to the discussed projects and architectures a variety of enabling technologies, paradigms and models can be identified, which have been previously proposed as potential candidates in the implementation of network management frameworks. In the following, some prominent fields are discussed in more detail.

Distributed object computing (DOC) supports strong distribution of management tasks by its inherent object-oriented approach, and is adapted for network management primarily by OMG's CORBA and Microsoft's Distributed COM (DCOM) [BoutabaAndXiao2002a, Pavlou2007]. DOC supports interoperability of heterogeneous network management protocols, such as SNMP and CMIP [BoutabaAndXiao2002a]. DOC-based technologies are also of interest with respect to certain levels of transparency, e.g., location and replication transparency provided by CORBA [Pavlou2007a], which is attractive when considering abstractions such as the Network of Information considered in 4WARD's WP6.

Code mobility and *management by delegation* are essential mechanisms enabling the transfer of components of applications at runtime between nodes. While *weak mobility* does not allow retaining state and data between code relocations, strong mobility, implemented in the form of mobile agents, allows suspending a program at the source node and resuming it at the target node upon code migration [BoutabaAndXiao2002a]. According to [Pavlou2007a], the Scripting Management Information Base (MIB) [RFC3165] and the Command Sequencer [ITU-X-753] are two approaches that support the delegation of scripts and also compiled programs (in the former case). One more key contribution regarding mobile agents is presented in [BellavistaEtAl1999a]. The authors present a mobile agent framework for system management with a specific focus on security and interoperability, which can inspire the work of INM with regards to these requirements.

The paradigm of *Intelligent Agents* originate from the domain of artificial intelligence (AI) and go beyond mobile agents in that they exhibit forms of intelligent behaviour. They provide inherent autonomy in their tasks, such as pro-activeness and self-learning. Intelligent agents are considered to have large potential as enablers of autonomic network management architectures [BoutabaAndXiao2002a]. A not-so-recent but still highly valuable presentation of the state-of-the-art of intelligent agents in network management is presented in [CheikhrouhouEtAl1999a]. However, with increased autonomy and complexity, intelligent agents and the environment they are applied to become prone to complex security issues. For example, it is difficult to determine to which extent they actually may exercise their autonomy [BoutabaAndXiao2002a]. Furthermore, their operation may be incomprehensible to the outside, in particular, in the event of unpredicted failures in which a user is confronted with a complex situation that he or she is unable to asses, let alone to determine steps to direct the system back into a state that is consistent with abstract management policies that may exist.

Expert Systems also originate from the domain of AI and they attempt to incorporate human knowledge into their programming in order to even further facilitate autonomy [Gupta2006a]. Their application to network management has been considered e.g. in [CronkEtAl1998a, KumarAndVenkatara1997a], with a focus on fault diagnosis, without considering the execution of corrective actions [Gupta2006a] and thus breaking the autonomous network control loop. Similar to Intelligent Agents, Expert Systems tend to be incomprehensible to users if they capture complex situations, and they may also not be able to consider every eventuality that may occur, in particular, when deployed to new environments. The example of TCP and its assumptions regarding packet loss is an example of this problem [MortierAndKiciman2006a].

Active networks allow programs to be injected into network components, which run customised tasks on the data passing through these components. They are especially attractive in the realisation of real-time adaptations and thus, the implementation of real-time capable control loops, because they allow fast task adaptation at run-time [BoutabaAndXiao2002a]. However, similar to intelligent agents and expert systems, they introduce major security concerns [MurphyEtAl2001a]. In addition, they require more heavy-weight support in both hardware and software [Gupta2006a] and raise performance issues, among others.

In computing, an *ontology* is a structure of concepts or entities within a domain, organised by relationships. Standardisation of formal ontology languages by the W3C [BernersLeeEtAl2001a] has created the technical foundation for supporting (semantic) interoperability in heterogeneous and evolving systems and networks [WangEtAl2004a] [MasuokaEtAl2004a] [BelecheanuEtAl2004a]. An ontology consists of a set of axioms that assert one or more relationships between classes and/or properties (e.g., subsumption). In other words an ontology consists of classes (characteristics or concepts of individual things) and properties (relationships between or about things). The class hierarchy tree in an ontology is a set of concepts with equivalence or sub-/super-class semantic relationships between them, thus it is organised as a class taxonomy.

A major drawback of the proposed management approaches and architectures concerns *security*: either security issues are not considered or they are included as an additional feature in a later stage of the development process. Absence of security features protecting the network against threats, malicious attacks and unauthorised users make unlikely large deployment and practical applications of management approaches. This is particularly true for mobile agents, where code is moved from one network element to another one. In this case rigorous access control to the resources is required to allow the execution of the code.

In traditional management applications for Internet, security is based on the SNMP version 3 [Stallings1998a]. This protocol provides in fact a complete security framework, including access control on management information and a key distribution mechanism. SNMP v3 is highly modular, and divided in two subsystems. Privacy (encryption) and authentication functions are performed by the Security Subsystem. So far this subsystem can address the following threats: unauthorised management operations performed by altering, reordering, delaying messages or assuming the identity of an authorised entity, and learning the values of managed objects and events observing message exchanges. The Access Control Subsystem provides authorisation services to control access to MIBs for the reading and settings of management objects. The complexity of such a modular design limited the adoption of SNMP v3 in operative networks and it is disabled or only partly implemented on most of today's devices.

Policy-*based Network management (PBNM)* [Sloman1994a, AgrawalEtAl2005a] is a paradigm developed originally to reduce the administrative complexity of reconfiguring a device and/or a network to adapt to fluctuating conditions of the business and the infrastructure. The dynamic changes within business and the infrastructure, allied with the ever enlarging number of heterogeneous devices within a network [Strassner2004_Policy01], makes the manual process of network configuration quite cumbersome and intricate. PBNM aims to decrease this complexity and the related cost by automating, to some degree, the reconfiguration. Fujitsu solves the problem of complexity and cost of adapting constantly to changing situations with TRIOLE, which enables operation management without human involvement. With TRIOLE, consistency between the business level and the node level is achieved through a policy control architecture, where system configuration is updated automatically according to SLA changes. The policy levels in TRIOLE are business, system, control and execution. Their autonomic control loop includes analysis, design/verification, operation and monitoring [Triole2004_Policy03]. However, TRIOLE does not consider automating system configuration to adapt to changing infrastructure, nor self-organisation of new network infrastructure. The Policy Technologies group at the IBM T.J. Watson Research Centre has recognised this connection and has developed the Policy Management for Autonomic Computing (PMAC) technology. This PMAC technology is embedded within software applications. An "autonomic manager" tool can make decisions based on policies (business rules), created by the developer to make applications capable of self-managing and self-configuring [Alphaworks_Policy02]. Motorola's autonomic networking for seamless mobility responds to both changing conditions in the business and in the network infrastructure with self-awareness and business-driven adaptation with the policy continuum [Strassner_Policy04]. Motorola's autonomic system is self-governing where the system senses changes in itself and its environment, determines the effect of the changes on the business policies, executes changes to be made if business policies are violated and subsequently observes the results [Strassner2005_Policy05]. Zhang et al [ZhangEtAl2003_Policy06] targeted wireless networks, proposing a policy-based management architecture to manage QoS in an integrated UMTS and WLAN environment. Chadha et al [ChadhaEtAl2004_Policy07] proposed a management architecture for mobile ad-hoc networks, based on the IETF PCIM policy model [MooreEtAl2001_Policy08]. However, this model does not take into account context information that may improve policy decisions in different network environments.

A variation of an applied policy management system is "policy based mobility management" [FanEtAl2007_Policy09]. It corresponds technically with the classical PBNM in that is uses

control cycles and a policy language, but it applies these concepts to resource and mobility management in a heterogeneous access network.

A different kind of policy system is the PCC (policy and charging control) of 3GPP Release 6/7 [3GPP_Policy10]. It consists of PCRF (P&C rule function) and PCEF (P&C enforcement function) subsystems and enables operator controlled QoS and QoS adaptation according to subscriber service requirements, resulting in optimised usage of network resources.

The relevance of *biologically-based models* is likely to increase, as many self-* properties characteristic of autonomic management in network systems can already be found in nature [DobsonEtAl2006a, AgoulmineEtAl2006a]. Biological mechanisms are powerful and highly evolved and they are able to adapt in a varying environment. Some specific biological mechanisms are identified in [AgoulmineEtAl2006a], which resemble accurately the requirements of network management, for instance homeostasis as the ability to maintain system equilibrium and the immune system as a natural defence mechanism of the human body to respond to foreign invaders.

There is a lot of work in biology-inspired self-organisation; applying these ideas to network management has been done for example by the authors of [BalasubramaniamEtAl2006a]. They established a mapping between biologic organisms and communication systems, based on the analogy of a cell with a device and a collection of cells with a communication system. The hierarchical organism architecture, namely formed by layers like organism, tissue, cell, protein, is translated into a hierarchy of policies; a bio-inspired Policy Based Management (bioPM) for autonomic communications systems is developed based on this organisational model. In [LeibnitzEtAl2006a] a biologically inspired technique towards self-adaptive routing for overlay networks is proposed. The technique supports adaptation for packet stream in response to changes in the metrics of the path through the concept of multi-path routing.

Several of these innovative approaches based on biological principles are being studied. Bio-inspired methods are considered to be included in the FOCALE architecture as well [JenningsEtAl2007a], as presented previously. The compatibility of such biologically inspired models with the existing network architectures and classical approaches is still unclear and it has to be investigated and proved. Their applicability in the networking domain is still object of current research. A survey on design patterns from Biology for distributed computing is contained in [BabaogluEtAl2006a].

Using *economic theory* as a basis for network management has been proposed as an alternative approach [BoutabaAndXiao2002a]. Network services could be modelled as an open market model and the result would be a self-regulating network, without the presence of any formal management network infrastructure. It is a form of policy based network management, in which policies follow the economic policy model. However, this approach is in a very early stage and has not been elaborated and analysed in detail so far.

While most approaches focus on taking actions reactively based on the detection of e.g. faults, *predictive network management* methods are still in their beginnings [Gupta2006a], and only considered with respect to resource usage, e.g. in [BushAndKalyanaraman2006a, BushAndKulkarni2001a].

5.2 Concluding Remarks

This section presented a general assessment of the state-of-the-art related to INM.

First of all, it is evident that traditional approaches do not sufficiently support many fundamental requirements, like scalability, autonomy, and heterogeneity. However, these approaches are widely found in today's network environments and need to be accounted in for any approach to autonomous network management. While 4WARD's INM pursues a clean slate approach, it will take into consideration existing and legacy systems that currently coexist in a heterogeneous networked world (voice, data) and support their seamless evolution into a holistic manageable future network architecture.

Second, only few architectural and project-related solutions exist that provide a more general approach to autonomic network management. While some are highly complex (e.g. ASA [ChengEtAl2006a], FOCALE [JenningsEtAl2007a]), others focus on specific network environments (e.g. MANNA [RuizEtAl2003a] in WSNs, Madeira [MadeiraProject] in P2P). These approaches provide valuable insights into network management in different domains, and they shall be considered in the design of 4WARD's INM architecture and algorithms. We are further convinced that only within an integrated project of the magnitude of 4WARD it will be possible to exploit the potential of radically new concepts, such as generic paths and networks of information.

Finally, a large number of enabling technologies, paradigms and models exist that have been considered in the design of network management, but their individual benefits and drawbacks as well as their interplay and mutual compatibility in a network management approach is yet to be understood. 4WARD's INM will assess such issues in the analysis of its architecture and algorithms, and carefully balance required functionality, beneficial autonomy and other quantities with overall system complexity, in order to provide a "clean and lean" management facility that is still comprehensible and tangible to the outside user.

Chapter 6 Selected In-Network Management Scenarios and Use Cases

The idea to define scenarios and use cases (UCs) is mainly twofold. First of all, scenarios/use cases will highlight the importance of In-Network Management, why it is needed and what the requirements for In-Network Management solutions will be. They show what the current limitations in network management are and what can be achieved by implementing In-Network Management.

Afterwards, the UCs will be used to evaluate the efficiency and quality of results achieved within the project based on evaluation criteria and pre-defined metrics. Such a scenario based evaluation not only allows to judge on the quality of results efficiently and in a structured manner, but can also give some quantitative results. Finally use cases might provide potential demo scenarios to demonstrate the advantages of In-Network Management.

6.1 Scenario Selection Process and Template Structure

Within the first month, multiple scenarios and use cases have been defined in this work package touching different perspectives and views of future networks.

The scenarios describe the environment in which a set of use cases can be defined. We distinguish scenarios in accordance to technologies in use and administrative structures. Since there are a wide variety of diverse networks we have to focus on a few selected ones meaning the most relevant scenarios as reference for the development of In-Network Management solutions

Therefore, it was necessary to decrease the number of scenarios/UCs, restructure and merge contents. We based the selection process on the need to comply with following requirements.

- Requiring management technologies beyond the current state of the art (e.g. prohibitive scale, timeliness requirements, overhead/costs)
- Reflecting future network structures and environments (e.g. (network) mobility, ad-hoc, mesh, context-aware service, sensor networks)
- Supporting future business models (multiparty control, user content...)
- Addressing application challenges (critical infrastructures, security, privacy issues)
- Capability of demonstrating benefits of self-organisation principles
- Showing overall 4WARD vision (supporting 4WARD overall scenarios, allowing for strong cooperation with other work packages)

After getting input from all partners for various merged and re-structured proposals, three of them remained for the first step and were taken as basis for a voting process. The voting showed the consistency of partners, as the most frequently selected proposal for merged scenarios could get around 80% of all votes. The finally selected proposal with a set of 4 scenarios will be presented in the following.

In order to get a similar and consistent description for all scenarios and use cases a template was provided containing sections that were filled for each scenario and use case description.

The template consists of the following elements:

- Scenario Description

  A short overview of scenario is given that is setting the scene; it describes the area of concern with its main characteristics and features, and lists challenges that are encountered in this context.

- Network Environment

Details what networking technologies are relevant, but also looks at issues of control and management in this environment: determines whether it allows for a more centralised or a distributed and self-organising management approach; identifies the parties that can exercise administrative control.

- Key Challenges

  The future Internet will be characterised by broader heterogeneity in its networking technologies and higher dynamicity and changes in comparison to today's networks. For each scenario the specific challenges that arise in this context are explained.

- Detailed Use Case Description

  From the broad scope of management tasks that are required within the setting of the scenario, a few use cases are selected, which are analysed in detail. They allow for a more concrete examination of management problems that need to be addressed, and for which In-Network Management is expected to provide effective solutions.

- Further Use Cases

  Possible Use Cases within this network environment are briefly described, pointing out further research issues that might need elaboration.

- State of the Art

  Relevant state of the art for the specific problem area is presented that lists promising approaches and techniques which can be applied to the use case. Depending on the maturity of the approach, some products may be available on the market. However in most cases development may be further behind in the pipeline: there may be already mature technological solution available which could be turned into products; or it may be still an area of more basic research where first promising scientific solution exist which however still need further development.

- Limitations of Traditional Approaches

  Discusses causes why traditional management is insufficient or inefficient in that particular use case, and provides a rationale and motivation for new approaches that need to be followed.

- Expected Benefits from In Network Management

  Analyses from various Perspectives what are the benefits that can be gained by following an In-Network Management approach

- Requirements

  Identifies aspects such as required functionality, information that need to be collected and exchanged between entities, non-functional factors like timeliness, reliability, costs or security. It will be important input when developing In-Network Management and defines evaluation criteria for the proposed solutions.

- Relationship with other WPs

  Identifies commonalities and common interests with the work undertaken in other work packages and areas of cooperation

6.2 Scenario 1: Self-Management in wireless multi-hop networks

This scenario describes problems, challenges and requirements of In-Network Management in wireless Multi-Hop environments such as Mobile Ad-Hoc Networks (MANETs), Wireless Mesh Networks (WMNs) or Sensor Networks. The unique characteristic of this scenario is that there is no central administrative control. Nodes belong to different users and are under the administrative control of each individual user.

6.2.1 Network Environment

The need to get access to information, e-mails, or even just to be connected to the Internet is increasing day by day. Users want to enjoy such services no matter where they are or whether they stay at the same location. This desire emphasises the importance of wireless connectivity where fixed connections is not available.

Types of networks, e.g. Phone, Freifunk, Car-to-Car and others clearly show an increasing interest in community communication. This way it is feasible to expect that future communication networks will not be just composed of a few administered domains, but also of multiple self-organizing wireless networks such as Mobile Ad-Hoc Networks (MANETs) or Wireless Mesh Networks (WMNs).

Hence, wireless network elements communicate and exchange different kinds of data (file transfer, streaming, sensed information, control information, etc.) without the need of existing infrastructure. In the following those network elements will be also referred as mobile nodes, which might act as sending/receiving stations as well as data forwarding nodes (routers). They exhibit different capabilities such as transmission range, mobility schemes or even computation power and establish any kind of communication fully autonomously.

6.2.2 Key Challenges

The key challenges in wireless multi-hop networks are the following:

- Changing network conditions
  In a wireless multi-hop network conditions can change by multiple reasons, such as different mobility schemes (e.g. rather static or quite mobile) that might change from one second to another one, changing weather conditions or even the density of nodes. Network nodes have to change their routing behaviour according to situation changes.

- Correlation of information from different sources
  Transmission conditions for wireless networks are different than for fixed ones. For In-Network Management in wireless networks it is important to gather information from different layers (e.g. link quality, SNR or bandwidth) and include them in the decision making process. Also configuration can take place at multiple layers (e.g. changing radio channels or routing). Therefore cross-layer-functionalities are of advantage.

- Scalability:
  The increasing number of network nodes leads to an increasing importance of scalability as wireless multi-hop network tends to collapse due to interferences. Changes in transmission power (transmission range), channel switching, reducing control information broadcastings and multi-path routing are some possible techniques to stabilise possible network communication.

6.2.3 Detailed Use Case Description

Situation-aware adaptive multi-path routing in wireless multi-hop networks

Based on the assumption that wireless multi-hop networks as a part of a Future Internet will be used and composed by multiple devices with different behavior (e.g. wireless routers, laptops, mobile terminals, etc.) the network situation will constantly change and hence exhibit heterogeneous characteristics (e.g. dense, congested, mobile, etc.). To be able to optimize the overall network performance it seems obvious that network nodes must be able to fully self-adapt if the network situation changes. This way, a routing protocol must not only take action and change its strategy when the node itself changes its behavior, e.g. from static to mobile, but also when neighboring nodes or even a local cluster experience changing network conditions.
This directly implies the importance for nodes to determine their current local network situation therefore they are able to adapt their routing behaviour accordingly. Hence, responsibility of the In-Network Management approach is not just to deal with self-adaptive functionality, but also to establish situation awareness as a decision basis. Such functionality has to offer monitored network state information and will be a main part of the In-Network Management architecture. Its task will be not limited to routing functionality, but to support any In-Network Management functionality and application that is interested in any network state information.

Figure 3 visualises the need of situation awareness pointing out the aspect of mobility in wireless multi-hop networks. It also shows the impact of multipath routing techniques when data destined for the same node will be split up and sent via different network access routers, e.g. due to network usage constraints.

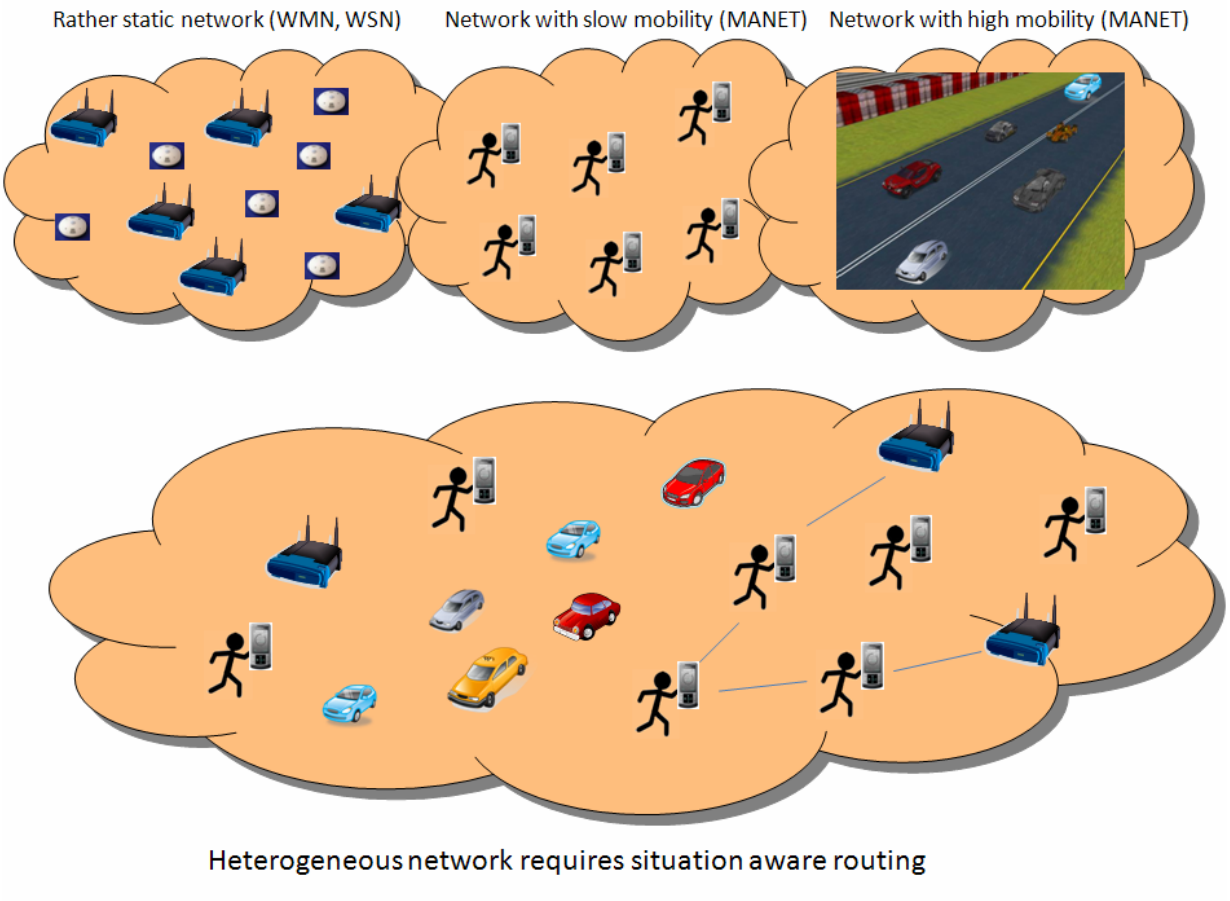

Figure 3: Different types of wireless multi-hop networks

6.2.4 Further Use Cases

This section describes further use cases that can occur in the given scenario but have not been elaborated as reference use case.

Clustering of sensor networks

Managing sensor network is a real challenge, though doing so in a centralised manner is inappropriate for a few reasons:

- There are a huge number of sensors, possibly thousands of them in one geographic region.
- A central management entity cannot communicate with all sensors, as most of them are not within transmission range. Relaying messages between the central entity and out-of-range sensors is an inappropriate approach; a large amount of hops is required, clogging the network capacity with relay information, and shortening the battery lifetime of each sensor.
- Configuring the sensors to operate at a specific mode is desired, due to changes in network state, environmental state (i.e. measurement thresholds), or outside alarms, but is unfortunately impossible

A distributed approach for managing the sensor network is more appropriate. Sensors operate in a cluster, where they can effectively communicate with each other, skipping transmission of redundant data, and reconfiguring themselves as needed. Clusters can communicate with nearby clusters when external information must be conveyed (i.e. external alarms)

Car-to-Car Communication

Prospective cars tend to be equipped with wireless communication interfaces being able to establish communication e.g. by using WLAN. They may exchange traffic information such as arising traffic jams or even accidents and thus might help to inform the police or an ambulance in case of emergencies.

Multi-path Routing

Two well known problems in wireless communication are the limitation of transmission bandwidth and instability of connections. These shortcomings even get worse when data is sent via multiple hops and nodes are used as relays. Firstly, due to interferences nodes do have to synchronise themselves with their neighbouring nodes when data shall be transmitted. Secondly, the probability of route breaks and thus the instability of routes steps up with increasing number of hops. Multi-Path routing is a possibility to increase the transmission throughput and enables better connection stability by using multiple paths to the destination at the same time.

Applying multiple Routing Metrics according to a Node's Situation

Due to the nature of the wireless medium network elements are not bound to a certain location and thus might move around in idle mode as well as during ongoing communications. Hence routing protocols should be able to adapt their routing metrics based on mobility patterns. A similar adaptation should be implemented for the computation of routes (e.g. number of hops where routing information are exchanged) based on the current network situation (e.g. traffic patterns and mobility).

6.2.5 State of the Art

Traffic forwarding in wireless networks is a well known problem and a very challenging issue, as there arise much more problems than in fixed networks [LBCL05] [RoMM03] [YaWK03] [IaKS03] [LuNT03]. Over years much academic research has been done in this area and there exist various proposals and surveys trying to overcome those problems. Due to the high degree of autonomicity and the need for self-management, such as self-healing or self-configuration, wireless multi-hop networks are one of the most interesting and challenging types of networks within this area. Networks belonging to this group namely are Mobile Ad-Hoc Networks (MANETs), Wireless Mesh Networks (WMNs), and Wireless Sensor Networks (WSNs). In the past most academic research has been done for network environments of MANETs. However, in the meantime MANETs are not arguably the most important wireless multi-hop environment anymore. Reality has shown an increasing interest in Wireless Mesh Networks (WMNs) [AkWW03][AkWa02] with a major interest to establish Internet connectivity in rarely uncovered areas. The changed focus seems to be reasonable as there are already WMNs in community usage. Even providers do have an increasing interest in such networks and hope for business models in the future as well.

Anyway, regardless of the specific network environment, most existing routing techniques can be basically split into two groups of routing protocols, namely pro-active and reactive.

Pro-active protocols

Pro-active routing protocols (also referred as table-driven) try to provide each node with a total view of the network. To achieve this goal, each network node exchanges its routing information with its neighbouring nodes periodically and tries to maintain an up-to-date routing table. By nature of this up-to-date routing table those approaches allow to immediately transmitting data to a destined node without the need to look for a route previously; thus allow data transmission without any further delay. Furthermore, by reason of continuous periodic routing updates there is no need to maintain and take care for selected routes separately. However, of course the actuality of routing information directly depends on the broadcast time interval of control information, meaning how often routing information is exchanged. Unfortunately, exchanging such control information periodically also wastes network resources as there is mostly no need to have knowledge about the reachability of all nodes within the network. Moreover, nodes often do not have to transmit any data, too, thus do not need any routing information at all.
Some approaches that belong to this group are e.g. DSDV [PeBh02] and OLSR [CHCB04].

Reactive protocols

Reactive routing protocols neither try to maintain an up-to-date routing table that matches with the current network topology nor do they send routing information periodically. In case that a node requires a path to a destination, the source initiates a route discovery process. Consequently, reactive MANET routing protocols are also referred as (source-initiated) on-demand routing protocols. Contrary to pro-active routing protocols they do not consume network resources by periodically sending control packets and just request route information to the intended destination node. This way, they do not have a view of the network, but just path information to the destination they are interested in. On the other hand, due to the fact that routes have to be discovered before data can be transmitted reactive protocols suffer from a sending delay when the transmission is started. They also have to support a further mechanism called route maintenance to be able to take care for routes that are used for ongoing sessions.
Protocols that belong to this group are e.g. DSR [JoMa02] and AODV [PeRo02].

Further routing protocols

Some proposals try to minimise the shortcomings of pro-active and reactive protocols by combining both approaches. ZRP [Haas01] is a well known protocol that belongs to this group of hybrid-protocols by restricting the number of hops routing information are exchanged pro-actively. Another interesting approach to overcome those problems is a proposal [BoKo02] that is based on DSDV and adapts its broadcasting behaviour of routing information according to the network usage; meaning that just active routes are maintained in a pro-active manner.

Routing metrics

Most protocol research in the past has been done based on the path weighting metric "minimum hop count". In the meantime various new routing metric have been proposed. The most well known one is called Expected Transmission Count (ETX) [CABM04]. It is based on the probability of transmission errors which lead to retransmissions and thus minimises the average amount of transmissions that a packet needs to reach the destination. Further metrics such as "Medium Time Metric" (MTM) [AwHR03], "Expected Data Rate" (EDR) [PaKa02], or WCETT [DrPZ03] try to extend the idea of ETX by using further parameters and functionalities such as interferences, Channel Switching, and link speeds. A well known research shows the importance and dependency of routing metric and performance [DrPZ03].

Multi-Path Routing

One major problem in wireless networks is to increase the network throughput by reason of low transmission rates. Hence a convenient possibility to increase the throughput for a given transmission is to use multiple paths to the network. In case of wireless multi-hop networks such a strategy could lead to an immense increase of network throughput as it can reduce arising intra-flow interferences by multiple times [MuTG03][NaNA03][YYWL05][TsMo02].

References

Routing Protocols

[PeBh02] – C. E. Perins, P. Bhagwat, "Highly dynamic destination-sequenced distance vector (DSDV) for mobile computers", in ACM SIGCOMM'94, pp. 234-244, Aug. 1994

[CHCB04] – T.H. Clausen, G. Hansen, L. Christensen, G. Behrmann, „The Optimized Link State Routing Protocol, Evaluation Through Experiments and Simulations", Proceedings of IEEE Symposium on Wireless Mobile Communications 2001, September 2001

[JoMa02] – D. B. Johnsen, D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", Mobile Computing Kluwer Academic Publishers, 1996

[PeRo02] – C. E. Perkins, E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing", in Proceedings of Mobile Computing Systems and Applications, February 1999

[Haas01] – Z. J. Haas, "A New Routing Protocol for the Reconfigurable Wireless Networks", in Proceedings of IEEE ICUPC'97, October 1997

[BoKo02] – R. V. Boppana and S. P. Konduru, "An Adaptive Distance Vector Routing Algorithm for Mobile, Ad Hoc Networks", IEEE INFOCOM 2001

Multiple proposals of different routing metrics

[CABM04] – D. S. J. De Couto, D. Aguayo, J. Bicket, R. Morris, "A High-Throughput Path Metric for Multi-Hop Wireless Routing", MOBICOM '03

[AwHR03] – B. Awerbuch, D. Holmer, H. Rubens, "The Medium Time Metric: High Throughput Route Selection in Multi-rate Ad Hoc Wireless Networks", Proceedings WONS Conference 2004

[PaKa02] – J. C. Park and S. K. Kasera, "Expected Data Rate: An Accurate High-Throughput Path Metric For Multi-Hop Wireless Routing", Sensor and Ad Hoc Communications and Networks, 2005. IEEE SECON 2005

[DrPZ03a] – R. Draves, J. Padhye, B. Zill, “Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks” – MobiCom’04

[DrPZ03b] – R. Draves, J. Padhye, B. Zill, “Comparison of Routing Metrics for Static Multi-Hop Wireless Networks”, SigComm’04

Multi-Path routing

[MuTG03] – S. Mueller, R. P. Tsang, and D. Ghosal, “Multipath routing in mobile ad hoc networks: issues and challenges,” in Performance Tools and Applications to Networked Systems, M. C. Calzarossa and E. Gelenbe, Eds., vol. 2965 of Lecture Notes in Computer Science, pp. 209–234, Springer, Berlin, Germany, 2004.

[NaNA03] – N. S. Nandiraju, D. S. Nandiraju, D. P. Agrawal, „Multipath Routing in Wireless Mesh Networks“, Mobile Adhoc and Sensor Systems (MASS) 2006

[YYWL05] – Y. Yuan, H. Yang, S. H. Y. Wong, S. Lu, W. Arbaugh, “ROMER: Resilient Opportunistic Mesh Routing for Wireless Mesh Networks”, The 1st IEEE Workshop on Wireless Mesh Networks (WiMesh) 2005

[TsMo02] – J. Tsai, T. Moors, “A Review of Multipath Routing Protocols: From Wireless Ad Hoc to Mesh Networks”,

Miscellaneous about routing in MANETs/WMNs

[LBCL05] – J. Li, C. Blake, D. S. J. De Couto, H. I. Lee, R. Morris, “Capacity of Ad Hoc Wireless Networks”, MobiCom 2001

[RoMM03] – E. M. Royer, P. M. Melliar-Smith, L. E. Moser, “An Analysis of the Optimum Node Density for Ad hoc Mobile Networks”, IEEE International Conference on Communications 2001

[YaWK03] – Y. Yang, J. Wang, R. Kravets, "Designing Routing Metrics for Mesh Networks", IEEE Workshop on Wireless Mesh Networks, WiMesh, 2005

[IaKS03] – L. Iannone, R. Khalili, K. Salamatian, S. Fdida "Cross-Layer Routing in Wireless Mesh Networks", 1st International Symposium in Wireless Communication Systems (ISWCS'04)

[LuNT03] – H. Lundgren, E. Nordström, C. Tschudin, „Coping with Communication Gray Zones in IEEE 802.11b based Ad hoc Networks“, WoWMoM‘02

Surveys on Wireless Mesh Networks

[AkWW03] – Ian F. Akyildiz, Xudong Wang, Weilin Wang: Wireless Mesh Networks: A Survey. Computer Networks 47:445-487, 2005. (Elsevier)

[AkWa02] – I. F. Akyildiz, X. Wang, “A Survey on Wireless Mesh Networks”. IEEE Communications Magazine, 43(9):S23--S30, 2005. (IEEE)

6.2.6 Limitations of Traditional Approaches

Current techniques just take a rather static situation into account, e.g. either there is mobility or nodes just rarely change their location. Moreover, most approaches just use one input parameter or one routing metric to decide on the optimal routing path. Similarly, not using multi-path routing techniques meaning just to have one routing path between source and destination node, is a constraint of most approaches that often lacks efficient network resource usage and increased network stability. Another problem is the incompatibility of offered information from different vendors - unfortunately, there is no specified standard which vendors do have to follow and thus identical values of the same parameter could reflect different network conditions. However, a node’s network situation should be taken into account for routing and thus it is required to gather, combine and use such information. This will enable reflecting a node’s situation and thus allowing an adaptation of important routing parameters, metrics, etc.

6.2.7 Approaches and Techniques

The most important part is establishing a situation-aware framework that offers needed information in a standardised way via its interfaces (e.g. collecting and distributing information via IPFIX). Consequently, offered information can be requested and used by protocols or services as they are needed. This way it will be possible to enhance route selection processes of routing protocols. Routing protocols could use a set of routing metrics, which can be adapted and weighted according the nodes or even networks situation. As that situation aware information also offers a much better view of parts of the network, routing techniques such as multi-path routing could be used more efficiently increasing the network throughput and the stability of the network.

- Collecting, gathering, combining and exporting situation aware information via standardised interfaces (e.g. via IPFIX) and thus establishing situation awareness
- Developing new routing metrics
- Change/Adapt/Weight routing metrics and protocol behaviour according to a node's and network’s situation (e.g. mobility scheme, cross-traffic)
- Computing multiple routes to a destination and distributing traffic via multiple routes

6.2.8 Expected Benefits for Situation-aware Adaptive Multi-path Routing

Future networks tend to be mobile and possibly are composed of multiple ad-hoc networks; hence self-managed nodes that deal with upcoming network problems are indispensable. Roughly the same applies for routing in such multi-hop environments as well, as there is a strong interest to optimise and achieve efficient and situation aware routing. The adaptive multi-path routing based on path metrics increases communication reliability and available bitrates in end-to-end communications. Additionally, due to the traffic dispersion among multiple paths the network could be balanced more efficiently.

6.2.9 Requirements

As previously mentioned the establishment of situation awareness will be one of the most important parts to support In-Network Management with needed information and thus enable such paradigm. However, in order to be able to facilitate situation awareness to the In-Network Management, at least, the following requirements have to be fulfilled.

- Nodes have to monitor network traffic and gather lower layer information (e.g. SNR)

- Nodes need to interact, meaning that they have to exchange control and routing information among each other. Such information exchanging needs to be done in a standardised way (e.g. via IPFIX)
- Establishing situation awareness (e.g. recent information about a node's neighbourhood)
- Offering those “situation-aware information” to other network functions, e.g. information about link speed, network usage/congestion, mobility, SNR, link quality, etc.

6.2.10 Relationship with other WPs

- WP1-BIRD: Heterogeneous network architectures could imply new business cases.
- WP2: Architectural specifications have to take into account support for network heterogeneity (WMNs, WSNs, MANETs)
- WP5: Parts of the contribution namely are definition of new routing metric or adaptation of existing ones, changing of protocols, or multi-path routing techniques, which should be aware of research that will be done around the topic of “generic path establishment”
- WP6: Sensor networks might comply with NetInf guidelines.

6.3 Scenario 2: Large Operator

This scenario describes problems, challenges and requirements of In-Network Management in a large operator environment. The unique characteristic for this scenario is that there is a common administrative control. All network nodes belong to one operator. The operator has access and can control the nodes.

The Large Operator scenario does not address interoperability between operators. Clearly, service provisioning and maintenance of a service carried out by more than one operator introduces additional level of complexity. In-Network Management problems that are related to a single operator are sufficiently challenging, unsolved as of yet, and for this reason should be the first priority.

6.3.1 Network Environment

- Wired, wireless, and mobile networks, supporting voice, video, and data services, are gradually converging towards an all IP heterogeneous network. This heterogeneous network is gradually changing; nodes are added, creating new topology with increased bandwidth requirements, and legacy networks evolve. Along this gradual evolution, sudden changes may occur to the network, due to failure, malfunction, attack, or congestion
- Operators strive to ensure end-to-end connectivity (E2E) which clearly crosses the core and access networks boundaries. While the core and the access networks are very different from each other, network adaptation must be effectively addressed, seamlessly ensuring E2E connectivity. Network adaptation should be performed in a collaborative manner.
- Networks are growing at tremendous pace, supporting ever growing user base and types of services and technologies. Centralised network management becomes complex and unmanageable. A centralised management entity cannot cope with the amount of processing required and the expected short response time; its bandwidth and performance are increasingly insufficient. It seems that a distributed approach is the only way to support such growing demands, effectively keeping the network operational and healthy. Monitoring, anomaly detection, and adaptations can be performed autonomously in each section of the network, in a timely manner.
- Traffic metrics fluctuate dynamically, affected by the re-adapted topology of the network, and by traffic demand. Traffic demands also vary, affected by the type of services required at any given time, the time of the day, the location (residential or office area), and gradual demographic changes. Those network characteristics must be taken into consideration, in order to maintain an operational and optimally-utilised network.

6.3.2 Key Challenges

General challenges for large network operators with respect to network management include

- Scalability: This is one of the biggest challenges organisations that operate large and complex networks face if they do so in a centralised way.
- Efficient and economic network utilisation: Because of fierce competition between network operators, economic usage of the network is essential and network management has to provide support for this.
- Traffic engineering: Efficient traffic analysis are important for any operator to optimize its resource utilization, overcome upcoming bottlenecks and to even detect network problems in advance

- Security: The core-network offered by the operators is a vital part of the Internet; it needs to be as much reliable as possible and thus must be protected from any attacks, e.g. DoS
- Cross-layer delivery: Exchanging cross-layer information, e.g. to create shortcuts via certain source and destination nodes allows to increase resource utilization and network performance

Operational challenges

- Effective and dynamic network adaptation to changes.
- Definition of information models and protocols for In-Network Management.
- Fast adaptation. The detection of the network event and the reaction (network adaptation) must be prompt, minimizing service/network downtime.
- Maintain network connectivity between any nodes, any service; effective detection of node failure, link failure, congestion
- Ensure network survivability. Network survivability is the ability for communication networks to graciously recover from failures and to maintain a certain level of revenue as well as QoS level.
- Avoid network congestion in any segment over the whole network.
- The ability to forecast future events that require network management operations: changes in traffic patterns (time of day, location, increased demand, etc.), or possible failure points. When possible, such proactive approach takes corrective actions before the anomaly occurred, thereby keeping the network operational in the most effective manner.
- Delivery of High-quality TV and video delivery over the converged all IP packet-switched network. It is required to have stringent availability and reliability, and support for QoS (e.g. guaranteed minimum bandwidth, maximum delay, jitter, etc). Such QoS parameters must be enforced end-to-end; from the streaming server, via all intermediate nodes, and all the way to the consumer. When failure or congestion occurs in one of the components on the path, it is desired not to rely only on IP routing protocols to restore the path, but rather to employ pre-arranged protection mechanisms at layer 1-2 (i.e. backup paths, with reserved capacity, ensuring QoS requirements and speedy recovery).

6.3.3 Detailed Use Case Description

Network adaptation to traffic pattern changes and failure

The operator's network experiences frequent changes; users join or leave the network, add or remove services on the fly, move from one place to another, or form ad-hoc connections. Network nodes are exposed to ever changing load requirements and QoS requests. Nodes or links might fail, due to hardware problems, loss of power, cable cuts, frequency interferences, bad configuration, or a malicious attack, just to name a few.

The network is expected to be collectively aware about changes in traffic load and about a failure of an entity (a node, a link, or multiplicity of them at any combination). This is done in a distributed manner, and involves collaboration with the neighbouring nodes, by means of embedded measurement implementation. Every node, or a designated node in a local area, monitors the state of its neighbouring nodes/links, and measures the load on those links, and the health of the link to neighbouring nodes. When congestion is detected over one link, or when a link is not operational, following an accurate and precise diagnosis, the node is able to recover by means a collaborated effort, executing the appropriate action; re-routing the traffic

away from the problem, in an autonomous manner, and without manual intervention from a remote network manager.

The detection and the corrective actions are handled in a local manner, close to the problematic entity. Figure 4 demonstrates the adaptation process.

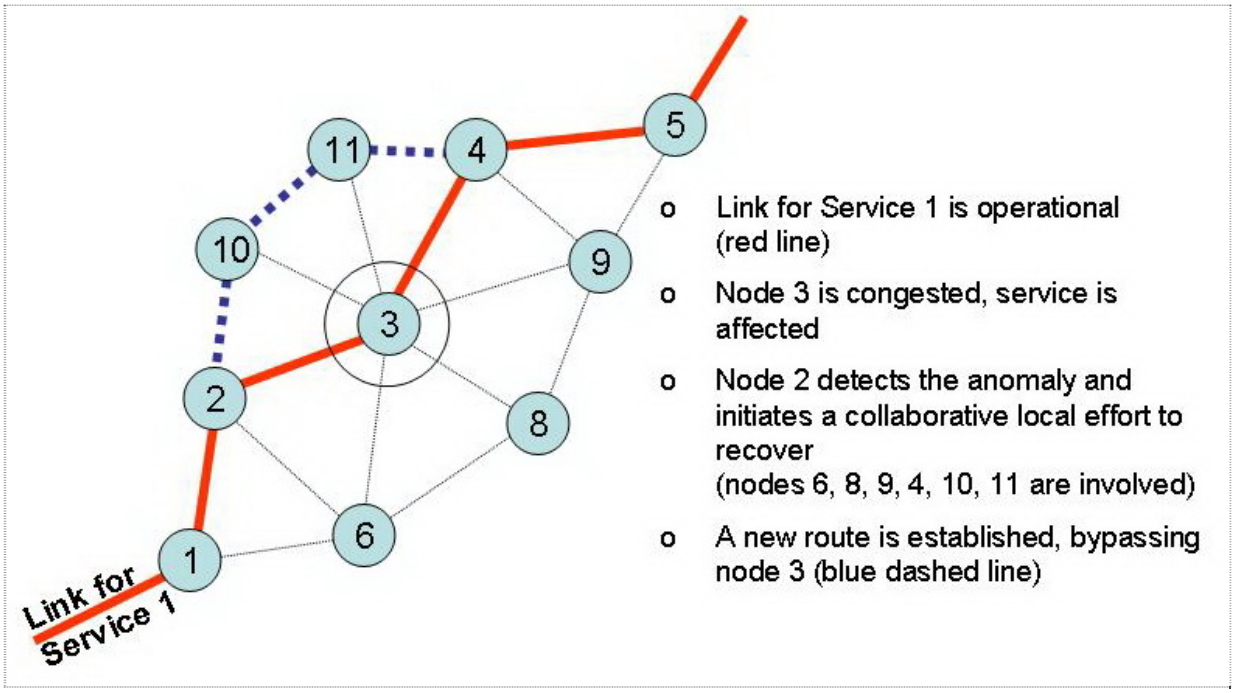

Figure 4: A pictorial demonstration of the network adaptation process

6.3.4 Further Use Cases

- **Coping with fluctuated traffic metrics**: As already explained, traffic metrics fluctuate dynamically, due to topology changes and traffic demands, which also fluctuate, due to different services offered, the time of the day, location (residential or business), and natural demographic changes. Inadequate routing planning could lead to congestion, failure, and denial of service. The deployment of permanent, semi-permanent or dynamic virtual links (e.g. IP/MPLS, T-MPLS, PBB) should be taken into consideration, in order to address different states of the network.
- **Dynamic service provisioning:** Provisioning a new service to a new subscriber involves a lot of manual setup and configuration. It is desirable that such provisioning will be handled dynamically; once initiated, the sequence of all operations will be automatically executed, instantly and successfully completing the provisioning.

6.3.5 State of the Art

Network Survivability

Network survivability is the ability for communication networks to graciously recover from failures and to maintain a certain level of revenue as well as QoS level. The failures can come in the form of nodes or link failures (permanent failures), or transient failures (due to maintenance process). The ability for the communication network to recover from failures in the most efficient manner is important for network operators to maintain a certain level of revenue while maximising the customers QoS level, and minimising the rejection rate.

The research into network survivability has been investigated extensively, and can be separated into proactive as well as reactive techniques. The majority of the research work has worked extensively in proactive mechanisms. One good example of proactive recovery mechanism is the work presented by [PSwAt05], where the authors proposed a pre-computed path backup for MPLS networks. The solution is not ideal for network traffic that changes very often, where a slight change in primary path traffic will lead to computation of a new backup path. The solution relies on a network with surplus spare capacity that can accommodate secondary paths without affecting other pre-existing primary paths. A more unconventional methodology for proactive routing was a work developed by [LWM06], who proposed a biologically inspired technique towards self-adaptive routing for overlay networks. The technique supports adaptation for packet stream in response to changes in the metrics of the path through the concept of multi-path routing. The concept is based on creating a number of primary paths and secondary paths between a source and destination pair. The solution proposed supports mechanisms to switch from primary path to secondary paths when the primary path encounters congestion or instability. The authors have proposed a number of differential equations for each of the path and using the concept of attractor-selector technique to choose the most appropriate path.

A very good example of reactive routing mechanism was investigated by [ALASJFDL02], who employed a technique of manipulating the parameters of existing paths in the event of link or node failures for MPLS network. The solution leads to high signalling overhead. And is very time consuming and, therefore, is not appropriate for maintaining a high level of customers QoS due to the amount of time required to perform the reactive routing process. . In [SaKV06], a reactive routing process was developed using the Merging Point of recovery Optimisation (MPO) for discovery of merging point nodes for re-routing in the event of node or link failures. The solution is based on broadcasting recovery messages to upstream nodes that will establish a re-routing path that routes around the failed region of the network. The proposed solution optimally determines the closest merging point node through an optimisation function that minimises the hop count as well as the round trip notification, and is performed in real time which avoids the need of proactive route discovery. The other advantage of this technique is also the ability for the network to recover by considering the current load of the network. However, the solution is not de-centralised and requires for each node to have knowledge of the network topology. This knowledge is required for the nodes to route the recovery messages to the appropriate upstream nodes. The solution does not comply with the requirements of autonomic based future internet that implement distributed signalling in the event of network failure.

In [KHCGL06], the authors developed a distributed combination of a reactive and proactive re-routing technique in the event of network failures. This is a hybrid approach and is based on determining a re-routing strategy based on a fixed traffic demand matrix. Each node evaluates the alternate route to re-route the packet stream in the event of detected failures downstream. The approach also integrates policies that allow the nodes to evaluate returning packets to determining anomalies in certain sections of the networks

The Spare Capacity Allocation (SCA) [WoMi05] method aims to minimise the added capacity required by the backup paths in MPLS network. Many papers proposed an Integer Linear Program (ILP) whose output is the set of backup paths that can fully restore the traffic on the primary paths [LTV07]. Most solutions focus on approximation algorithms, since finding an optimal solution to an ILP is computationally hard. One approach is based on a Genetic Algorithm [MeTi00] and utilises crossover and mutation operators to evolve "good" solutions towards optimality. These operators force disjoint backup paths to share their bandwidth. The algorithm is able to detect completely new paths and can also deal with nonlinear cost functions. Only a few papers proposed approximation algorithms with performance guarantees for the SCA problem or its variants. Both offline and online approximations are

presented. These algorithms are based on approximation algorithms for the Steiner network problem.

Other works concentrate on non-SCA criteria. Several heuristics are proposed for minimizing restoration time and bandwidth consumption. Examples of criteria used in the heuristic search includes, (i) reduction of the backup path length as well as the bandwidth consumption for discovered paths, (ii) minimising delays of the primary and back-up paths, and (iii) determining the paths using the throughput information between specific source and destinations. In one work, a Fully Polynomial Time Approximation Scheme (FPTAS) technique is used based on the primal-dual approach is developed. The proposed algorithm separates an existing demand matrix into sub-matrixes, each of which will be used to evaluate the primary and backup paths.

[PSwAt05] – P. Pan, G. Swallow, A. Atlas, “Fast Reroute Extensions to RSVP – TE for LSP Tunnels,” RFC 4090, May 2005.

[ALASJFDL02] – J. Ash, Y. Lee, P. Ashwood-Smith, B. Jamoussi, D. Fedyk, D. Skalecki, L.Li, , “LSP Modification using CR-LDP”, RFC 3214, January 2002.

[SaKV06] – W. Sa-Ngiamsak, P. Krachodnok, R. Varakulsiripunth, “A Recovery Scheme for QoS Guaranteed Mobile IP over MPLS Network”, Proceedings of the 1st IEEE International Symposium on Wireless Pervasive Computing Conference, Phuket, Thailand, January 2006.

[LWM06] – K. Leibnitz, N. Wakamiya, M. Murata, “Biologically inspired Self-Adaptive Multi-path routing in overlay networks”, Communications of the ACM, vol. 49 (3), March 2006.

[KHCGL06] – A. Kvalbein, A. F. Hansen, T. Cicic, S. Gjessing, O. Lysne, "Fast IP Network Recovery using Multiple Routing Configurations", in Proceedings of 25th IEEE International Conference on Computer Communications, Barcelona, April 23rd - 29th, 2006.

[WoMi05] – I. Woungang, S. Misra, “Spare Capacity allocation design schemes in self-healing ATM networks”, in Proceedings of IEEE Communications, Computers, and Signal Processing, Victoria, B.C. Canada, August 2005

[LTV07] – Y. Liu, D. Tipper, K. Vajanapoom, “Spare Capacity Allocation in Two-Layer Networks”, IEEE Journal on Selected Areas in Communications, Vol. 25 (5), June 2007, pp. 974 – 986.

[MeTi00] – D. Mehdi, D. Tipper, “Some approaches to solving a multi-hour broadband network capacity design problem with single-path routing”, Telecommunication Systems, vol. 13 (2), 2000, pp. 269 – 291.

In-Network Traffic Engineering

In-Network Traffic Engineering is used by large operators to optimise network utilisation. This is commonly done as an offline and centralised process to optimise routing for failure and non-failure state of the network. Numerous papers exist both from theoretical and practical perspective that describe the state of the art in traffic engineering.

Cooperative Anomaly Detection

Denial-of-service attacks, or briefly DoS attacks, are network traffic events organised and controlled by a malicious party to cause damage to a network or remote host or to prevent it from operating in the way it was intended.

Vulnerability attacks exploit existing software flaws. Many of these attacks can be prevented by either upgrading broken software or filtering particular signatures using Intrusion Detection Systems such as [Roes99]. Nonetheless they remain a serious and ongoing threat. [MoVS01]

Flooding attacks on the other hand overwhelm the victim's resources. Because there is rarely a way to distinguish the useful requests from the unwanted, it can be extremely difficult to defend against these attacks. [MoVS02] Any limited resource of a system may be attacked. This shows in how far vulnerability to DoS attacks is inherent to any system: As long as there exists any kind of resource that is a) limited and b) shared between multiple users, it will always be possible for a user to claim part of this resource (or even all of it), thus reducing the availability for other users.

A common approach to intrusion detection is to define an attack as an abnormal and noticeable deviation of some statistic of the monitored network traffic workload. Most of the attack detection techniques include an evaluation of a different statistic of network traffic or other network or host events [CKBR06]: Change-point detection algorithms [ThJi03] isolate a traffic statistic's change caused by attacks. To identify and localise a DoS attack, the Cusum identifies deviations in the actual versus expected local average in the traffic time series. If the difference exceeds some upper bound, the Cusum's recursive statistic increases for each time series sample; State-based Intrusion Detection [ViKe99] analyses the state changes in different parts of hosts and the network; Principle Component Analysis (PCA) [LaCD04] allows to identify anomalies in a large set of metrics by reducing them to a smaller feature vector while retaining a maximum of information.

A specific challenge in the 4WARD architecture and the proposed scenarios will be to correlate intrusion detection information from a large number of sources, in a distributed fashion. [AbTa03] and [CAMB02] for example have studied this process on server log data and intrusion events from common IDS systems. The current approaches however assume a cooperative, often central data collection process. In the 4WARD architecture, we envision a decentralised co-operative approach based on different distributed computation models.

On the one hand, less critical operations can be performed using a weaker trust model and gossip protocols [JeBa06], which allow a participant to get a general overview of the strategies, reactions and impressions of the other actors in fulfilling their objectives. On the other hand, where stricter security requirements exist, smart contracts [Szab97][Szab04] and distributed validation permit a group of actors to reliably decide on a joint defence strategy.

[Roes99] – M. Roesch. Snort - lightweight intrusion detection for networks. In LISA '99: Proceedings of the 13th USENIX conference on System administration, pages 229–238, Berkeley, CA, USA, 1999. USENIX Association.

[LaCD04] – A. Lakhina, M. Crovella, C. Diot. Diagnosing network-wide traffic anomalies. ACM SIGCOMM, Portland, August 2004.

[ViKe99] – NetSTAT: A Network-based Intrusion Detection System, Giovanni Vigna and Richard A. Kemmerer, Journal of Computer Security vol. 7/1999

[AbTa03] – Abad, Taylor et al. "Log Correlation for Intrusion Detection: A Proof of Concept", Proceedings of ACSAC 2003, United States

[CAMB02] – F. Cuppens, F. Autrel, A. Miège, and S. Benferhat. "Correlation in an intrusion detection process". In Securite des Communications sur Internet (SECI'02), Sep. 2002.

[MoVS01] – "Inferring Internet Denial-of-Service Activity" authored by David Moore, Geoffrey Voelker, and Stefan Savage. Published in proceedings of the 2001 USENIX Security Symposium (Best Paper Award).

[MoVS02] – Quantitative Network Security Analysis, David Moore, Geoffrey M. Voelker and Stefan Savage, CAIDA.org project NSF-01-160

[ThJi03] – Anomaly Detection in IP Networks, Marina Thottan, Chuanyi Ji, IEEE Transactions on Signal Processing, Volume: 51, Issue: 8, Aug. 2003, Pages: 2191 – 2204

[JeBa06] – Márk Jelasity and Ozalp Babaoglu. T-Man: Gossip-based overlay topology management. In Sven A. Brueckner, Giovanna Di Marzo Serugendo, David Hales, and Franco Zambonelli, editors, Engineering Self-Organising Systems: Third International Workshop (ESOA 2005), Revised Selected Papers, volume 3910 of Lecture Notes in Computer Science, pages 1–15. Springer-Verlag, 2006.

Congestion Control:

One task of current transport layer protocols is to avoid network congestion. Multiple protocols and techniques have been specified, though the most well known and used one is the Transmission Control Protocol - TCP [Post04]. As the transport layer usually runs on a user's machine and not within the network itself. Hence, today's network congestion control is realised in end-to-end manner and network elements such as routers are not able to deal with it on its own.

[Post04] – Jon Postel, "Transmission Control Protocol", RFC 793, September 1981

Information on autonomic management:

The vision of Autonomic Management is to be able to manage future communication networks with minimal human intervention [KeWa05]. This capability is required for future communications networks, which will witness large scale networks that are composed of dynamic and heterogeneous network devices that are integrated to form the whole system. This capability will be only possible through the concept of self-governance, where communication devices (AE - Autonomic Element) will be able to exhibit self-* properties (e.g. self-management, self-learning, self-optimising, self-healing).

A set of challenges for designing Autonomic Communication Systems, was presented in [ABBSLD06]. These challenges includes, the ability to simplify the administrator's task by automating the decision making process, and enabling the users to manage such system in a pervasive manner. The paper presented different architectures that support the design, implementation and deployment of autonomic systems. In [JSBBFDJ07], the FOCALE autonomic network management architecture was developed. The architecture manages the network in an autonomous manner through Policy Based Management system, allowing the network to exhibit self-governance. The architecture also addresses mechanisms for policies refinement, where business policies can be refined to low level network policies. The network adaptation will be performed through control loops that consider various environmental changes, where these changes may include changes by the user, business goals, and environmental conditions (e.g. changes in topology – failures or expansion of topology). The architecture is based on the use of knowledge management to interpret context information from the underlying networks, which are then controlled by policies to ensure that the changes made to the underlying network is performed within certain constraints. At the same time the self-* capabilities, which are controlled by the constraints of the policies, are performed using Bio-inspired algorithms [BBDOFS07].

Prehofer and Bettstetter [PreBe05] have defined self-organisation as a system-wide adaptive structure with no external or central dedicated control entity, where individual entities interact with each other in a peer-to-peer fashion. They outlined four design paradigms for achieving self-organisation, which includes establishing local behaviours rules to achieve global properties by distributing responsibility among individual entities, exploit implicit and conflict detection information to coordinate between entities (e.g. deduce current information to draw new information), avoid maintaining long-lived state information especially dynamic networks, and protocols that are adaptable to changes within the environment. [YaTh05] proposed a self-optimizing, self-healing architecture for QoS provisioning in Differentiated services. The architecture employs a model free Reinforcement Learning (RL) approach to counter the

dimensionality problems of large state spaces found in conventional Dynamic Programming (DP) techniques. Although the methodology avoids the need for an accurate model of the environment by providing the agents with learning enforcement to reach optimality, the architecture is not suitable for dynamic networks. [LDPC03] proposed an autonomic monitoring system based on the resource model concept where the monitoring tool models and implements the aspect of the entities as objects. These objects are then used to evaluate raw data in order to detect, predict and correct any abnormal behaviour. The reference model lays out the critical path of a system or application and matches the current condition to the predefined path in order to determine the root problem and perform any necessary corrections. However, the monitoring tool is limited to single machine fault detection rather than network system environments. At the same time, although the operational phase and monitoring phase do provide autonomic behaviour, the design and deployment requires manual intervention.

[BBVB06] – Bahati, R.M.; Bauer, M.A.; Vieira, E.M.; Baek, O.K.; Chang-Won Ahn, "Using policies to drive autonomic management", International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2006. WoWMoM 2006.

[JSBBFDJ07] – B. Jennings, S. van der Meer, S. Balasubramaniam, D. Botvich, M. O' Foghlu, W. Donnelly, J. Strassner, "Towards autonomic management of communications networks", IEEE Communications Magazine, Volume 45, Issue 10, October 2007 Page(s):112 - 121

[ABBSLD06] – N. Agoulmine, S. Balasubramaniam, D. Botvich, J. Strassner, E. Lehtihet, W. Donnelly, "Challenges for Autonomic Network Management", accepted for 1st conference on Modelling Autonomic Communication Environment (MACE), Dublin, Ireland, October 2006

PreBe05] – C. Prehofer, C. Bettstetter, "Self-organisation in Communication Networks: Principles and Design Paradigms", IEEE Communications Magazine, July 2005

[YaTh05] – D. Yagan, C.-K. Tham, "Self-Optimizing Architecture for QoS Provisioning in Differentiated Services", In Proceedings of the Second International Conference on Autonomic Computing (ICAC' 05), Seattle, WA, USA, June 2005.

[LDPC03] – G. Lanfranchi, P. Della Peruta, A. Perrone, D. Calvanese, "Toward a new landscape of systems management in an autonomic environment" IBM Systems journal, vol. 42. no. 1, 2003.

[BBDOFS07] – S. Balasubramaniam, D. Botvich, W. Donnelly, M. Ó Foghlú, J. Strassner, Bio-inspired Framework for Autonomic Communication Systems, (Editors Falko Dressler and Iacopo Carreras) in "Advances in Biologically Inspired Information Systems: Models, Methods, and Tools", Studies in Computational Intelligence, Springer Verlag, 2007

[KeWa05] – J. O. Kephart, W. E. Walsh, "An Artificial Intelligence Perspective on Autonomic Computing Policies", In Proceedings of the 27th International Conference on Software Engineering, St. Louis, Missouri, USA, 2005.

Information Theory

Information theory answers some of the fundamental questions in communications: the ultimate data compression limit and the ultimate transmission rate. These issues are studied both for single and for multiple channel communications.
One of the most recent research topics in this area is network coding, originally proposed by R.W.Yeung and Z.Zhang in 1999, as an alternative to routing.

[AhlswedeEtal2000] The core notion of network coding is to allow and encourage mixing of data at intermediate network nodes. This approach is in contrast to traditional ways of operating a network where it is wanted to avoid collisions of data streams as much as possible. This technology provides a way to boost throughput, scalability and efficiency of everything from content distribution to wireless networks. Network coding is essentially an algorithm that proponents say can potentially more than double network throughput while also improving reliability and resistance to attacks. It helps to distinguish a variety of different types of traffic, and prioritises them helping to increase the capacity of the network.
[FragouliEtal2006] There are two main benefits of this approach: potential throughput improvements and a high degree of robustness. Robustness translates into loss resilience and facilitates the design of simple distributed algorithms that perform well, even if decisions are based only on partial information.
[DobsonEtAl2006a] New coding advances at the application level will strongly influence the design and evolution of future algorithms for communication systems. Specific new families of codes are Digital Fountain codes and Network Coding. These are already influencing the next generation of algorithms for peer-to-peer content distribution.
[ShamaiVers2007] Fountain codes are currently employed for reliable and efficient transmission of information via erasure channels with unknown erasure rates. The rateless property of these codes allows them to perform well in highly dynamic networks.

[ShamaiVers2007] – Shamai, Shlomo, Telatar, I. Emre, and Verdn, Sergio, "Fountain Capacity", IEEE Transactions on Information Theory, Vol.53, N.11, pp.4372-4376, November, 2007

[Dimakis2006] – Dimakis, Alexandros G., Prabhakaran, Vinod, and Ramchandran, Kannan, "Decentralized Erasure Codes for Distributed Networked Storage", IEEE Transactions on Information Theory, Vol.52, N.6, pp.2809-2816, June, 2006

[FragouliEtal2006] – Fragouli, Christina, Boudec, Jean-Yves Le, and Widmer, J¨org, "Network Coding: Na Instant Primer", ACM SIGCOMM Computer Communication Review, Vol.36, N.1, pp.63-68, January, 2006

[OceanStore] – The OceanStore Project, http://oceanstore.cs.berkeley.edu/

[AhlswedeEtal2000] – R. Ahlswede, N. Cai, S.-Y. R. Li and R. W. Yeung, "Network information flow," IEEE Trans. on Information Theory, vol. 46, pp. 1004-1016, Jul 2000.

[LiYeungCai2003] – S.-Y. R. Li, R. W. Yeung and N. Cai, "Linear network coding," IEEE Trans. Inform. Theory, vol. 49, pp. 371-381, Feb 2003.

6.3.6 Limitations of Traditional Approaches

- Scalability (e.g. the number of e2e paths a head end router can manage or the size of the network for which a complex measurement task can be done).

- Network Survivability: The traditional approaches have largely concentrated on proactive techniques to support re-routing in the event of failures. Proactive techniques usually rely on determining secondary paths that is set in the event of failures.

    - The biggest problem with proactive solutions is that, the re-routing process is not load sensitive. Those backup paths are pre-arranged and assigned at the time the primary path is established. Therefore, in the event of traffic demand changes, the re-routing process may not consider the new traffic conditions of neighbouring nodes during re-routing. Clearly, this is not an acceptable solution, considering fluctuating traffic loads.

  - Spare Capacity Allocation (SCA), a method that aims at minimizing the added capacity required by the backup paths in MPLS network, is not practical for network operators who have a fixed capacitated network, and want to maximise their revenue (i.e. establish as many paths possible on a given network capacity). Also, as explained above, another drawback of the SCA optimisation for network operators is that the cost associated with an established LSP does not depend on the load imposed on the selected route. In other words, there is no incentive for addressing congestion and implementing load balancing.

  - Inefficient and non-optimised utilisation of network resources.

- Overprovision of network resources, resulting in possible congestions at some network locations, and denial of service/session that are otherwise can be sustained.

- Slow reaction time to change, slow restoration of service. Until a corrective action is taken, the service is not fully operational, which means potential revenue loss and unsatisfied customers.

- Manual intervention required too frequently due to topology changes, or network evolution. That means that personnel-related expenses are higher than optimal, and network adaptation is not automated and is not fast.

- Generic paths and virtualisation concepts are not fully exploited. With higher level of abstraction, the network adaptation process has more resources to use, without being too much aware about the underline implementation.

- Non optimal utilisation of network resources when network congestion is handled end-to-end. In an end-to-end congestion handling, the whole route is replaced, even though some sections of the original route are very responsive and not overloaded. In the proposed scheme, recovery is local to the problem; the fix is implemented only at the congested area, and only the congested nodes or links are replaced.

- Centralised detection of network anomalies usually requires manual intervention, which is inherently slow to react, and sometimes unreliable.

6.3.7 Approaches and Techniques

- Distributed In-Network Management seems to be the only feasible way to effectively cope with scalability and diversity of services. Centralised network management becomes complex and unmanageable. A centralised management entity cannot cope with the amount of processing required and the expected short response time; its bandwidth and performance are increasingly insufficient.
  Monitoring, anomaly detection, and adaptations can be performed autonomously in each section of the network, in a timely manner.
- Local responsibility and recovery: a cluster of nodes, designated nodes, neighbouring nodes.
- Decentralised information flows among neighbouring nodes
  - Cost/Value based priority model for traffic flows that is considered on a finer granularity (i.e. a link by link, or a node by node). If a specific node is required for another higher-profit service, the network is adapted by rerouting the less-profitable service away from that node.

  - Context-sensitive filter generation near the anomaly source. Local recovery means that nodes have better knowledge about their neighbours, (i.e. the context), and if such node misbehave (e.g. flood the network), its neighbours are at the best position to promptly detect it and filter out the bad streams, before other sections of the network are affected.

- Collaborative collection of information (embedded measurement). A network problem cannot be fixed, unless it is accurately detected. Via a collaborated effort, knowledge is built more accurately from partial raw information that is available at each node.
- Anomaly detection at the appropriate layer
  - Application-layer attacks
  - Misbehaved host
  - Congestion and denial of service control
- Cooperative decision making and reaction to abnormal conditions. A single node cannot detect a network anomaly, and react (adapt), without involving its neighbour id the process.
- Self-adaptation to traffic changes and topology changes (adding/removing one node, node malfunction)
- Re-routing, in case of network failure or network congestion. Traffic should be diverted to an alternate route.
  1. Continuously. Re-routing should be continuously considered, in order to ensure effective network utilisation.
  2. Re-routing process must be concluded in timely manner. This includes both the time it takes to detect the need for re-routing, and the time it takes to select the alternate route and to switch to it.
  3. Ensuring that the route discovery process is sensitive to varying and changing traffic load. Communication networks experience frequent traffic changes.
  4. Ensuring that the re-routing process is performed with different priorities and QOS parameters for the different traffic types. Furthermore, the re-routing process should be aware about changes of bandwidth per QoS class. This ensures that revenue is maximised, and the customer's satisfaction is maintained

  A possible approach towards mitigating deficiencies in current network stability is to develop a reactive distributed technique that can support efficient re-route discovery in the event of failures or congestion. This technique facilitates cooperation of nodes, collectively discovering a new route, locally bypassing the detected anomaly. The alternate route is load sensitive. Using reactive based routing, can support various traffic demand changes, and allows swift route discovery and handover in an efficient manner.

  Another approach is to reserve an MPLS backup path implementing local recovery, replacing the broken/congested elements only. This can be handled in a distributed manner autonomously, in the area where the fault/congestion occurred.
- Traffic handling can be handled by the network itself (where routing takes place) and not in a higher layer based on end-to-end techniques. In other words, load balancing and routing are implemented by the same network entity with strong ties between both functions.

- For delivery of High-quality TV and video over the all IP packet-switched network, a circuit-switching emulation over a packet-switching network can be an effective way to address the QoS and high-bandwidth needs. In such emulation (e.g. MPLS network), a network path is permanently established, and stays active as long as all the nodes and the links in the path are operational. When failure or congestion occurs in one of the components on the path, it is desired not to rely only on IP routing protocols to restore the path, but rather to employ pre-arranged protection mechanisms at layer 1-2 (i.e. backup paths, with reserved capacity, ensuring QoS requirements and speedy recovery).

6.3.8 Expected Benefits for Large Operator Networks

- Increased network stability and survivability. A reactive distributed routing approach results in a swift recovery process that can be performed in a very short period of time without affecting other non-immediate neighbouring nodes during route discovery and handover. Frequent traffic demand changes can be permitted without affecting the re-routing process. In such cases, the operators will only have to set the priority between traffic types (depending on the revenue that have been set), to allows routes to be discovered with different priorities. Minimal disruptions will occur for customers whose traffic flows are affected by the failures. Such approach minimises possible service downtime or revenue loss, while retaining customer's satisfaction.
- Reduced information and processing necessary for network adaptation, as compared with centralised management entities. Only information that is local to the area experiencing the anomaly is required for network adaptation (or, in other words, the size of the "situation-awareness domain is smaller). Only neighbouring nodes are involved in the process.
- Reduced/no manual intervention when network topology is changed. The local area affected recovers autonomously. Recovery is faster, manpower is reduced. In other words, performance is increased at a reduced management overhead.
- Dynamic adaptation of policy changes (e.g. for traffic engineering).
- The number of paths (and the number of services) supported at a given MPLS-like network capacity can be increased (better network utilisation, revenue is maximised).

6.3.9 Requirements

- Implementation of a distributed interactive process between neighbouring nodes, a collaboration effort to monitor the network, make decisions, and take actions: detect network anomaly, discover an alternate route, and seamlessly handover. Distributed network adaptation should minimise computation load on each node. The route discovery must address traffic prioritisation among traffic types, QoS, and SLAs, such that the alternate route performs as expected/provisioned.
- A collaboration effort between nodes, to optimise traffic metrics as a function of time, geographical position, system policies and business objectives.
- Information models and protocols to support such collaboration are required.
- Nodes must have adequate local resources: storage for data aggregation and processing power for distributed calculations.
- Network adaptation must be at least as reliable as the centralised approach.
- Substantially faster network adaptation (as compared with the centralised approach), without manual intervention, at least for the "normal" set of network anomalies and congestion.
- Reduced computation loads and management information flows (as compared with the centralised approach).
- Traffic differentiation (revenue based, service classification, emergency channels)
- Detection of anomalies and role based interaction.

- Knowledge about network resources and network usage.
- Knowledge about how generic paths are built, how they are identified, and how to control them.

6.3.10 Relationship with other WPs

WP2: consistency with WP2-proposed architecture, principles and concepts.

WP3 Network Virtualisation: the abstraction of network resources, locally used for network adaptation. The adaptation process should be able to use the abstracted view of the network, which is then mapped to real objects.

WP5 Generic paths: re-routing in the control plane. Generic paths are eventually translated into real paths. The adaptation process should be able to perform in both environments; physical paths, or generic paths. Re-routing can be implemented as a modification to the generic path.

WP6 Network of information: information-centric network management, and network adaptation. NetInf proposed data-centric network architecture; the network is made of collection of objects, and a set of operations that creates them, publish them, and manages them. Clearly, management activities for this network architecture should be in line with what is proposed in this scenario.

Specifically, network monitoring of such network, and call control of real-time video/voice calls are two functions that are should be addressed, and made consistent in both WP4-large operator scenario, and WP6 NetInf ideas.

Scenario 3: Home Networks

6.3.11 Scenario Description

New capabilities are required in the network to meet the levels of reliability and easy-to-use expected in a future home environment. A characteristic feature is the dynamic interaction between different players – users, service providers, equipment providers, etc.- which will play an important role in future home networks, but which is not possible with today's equipment. In such environment, network management is invisible to the end-user but nevertheless ensures smooth operation of the network while optimising resource (including energy) consumption.

In order to illustrate the range of applications covered by future home networks, we list some areas where we expect significant support from networked devices in the home:

- Situation & context-aware services
  The current context is automatically detected and corresponding profiles are activated to control home privacy, e.g. what message notifications are enabled during dinner times or night times etc.
- Leisure & entertainment
  Real-time interaction for high-definition 3D gaming, TV allowing for new forms of interactivity with integrated support of information services. Social networking support includes video-enabled status updates transmitted in real-time.
- Work environment at home for job and education

  Secure connectivity to cloud computing and other infrastructure as a service resources (storage, collaboration tools, etc.) provided by the employer or educational institution.
- Surveillance technology for security and protection against intrusions, but also support in supervising e.g. small kids or pets
- Sensors for monitoring local facilities and utilities enhanced with intelligent supporting services
  e.g. keeping track of food items and their consumption date and providing dinner recipes suggestions; checking in stock heating fuel and observing competing supplier prices

6.3.12 Problem Description

During the last years, more and more attention has been paid to Home Networks. The home network is becoming a heterogeneous and complex environment composed of highly diverse set of hardware and software; different services can be offered to the users in the home, not only IP connectivity and delivery of voice and video, but also home automation and home security for example. These trends give rise to new issues and management challenges.

First of all, the job of installing, optimizing and maintaining the home network becomes more and more expensive and increasingly difficult. Users are willing to buy new technological devices for their home, but they do not want to face installation or interoperability problems, which they are most probably not able to solve by themselves. Today operators are able to manage and configure their networks but their control does not extend to within the home.

In order to cope with the problems related to this emerging new entity, the home network, there is the need to find a long term solution which addresses configuration and management issues. Furthermore the home network itself should be able to detect and cope with changes and modifications by itself without always requesting information and actions from the outside. The approach is to incorporate management capabilities in the devices themselves, allowing them to perform all the necessary steps to automatically manage themselves and to interact with the other devices in the environment in a flawless way.

However, despite these management capabilities are embedded in the devices, operator support for management purposes in the home might be necessary as well. An open issue is to find out to what extent the operator should extend its control to the home network, and what is the level of autonomy that the home network can achieve in managing itself without external coordination. It is clear that the more autonomous the home network is, the smaller the management load for the operator will be. In any case, the management operations must be seamless to the users in the home.

This includes automatic, dynamic policies that adapts to the current situation the family is in. For example, content filtering based on source or sender should be adapted for the current situation, policies for who will be able to get through to the family during the dinner should be automatically enforced.

Due to the growth of complexity in home networks and the number of home networks, management of a multitude of home networks is very challenging for the operator. Traditional approaches like TR-69 for provisioning and controlling of DSL routers are centralised and this will result in scalability problems.

In addition to installation and configuration of home networks, QoS provisioning is becoming a key issue as well. Inside the home many devices compete for the usage of available resources. In order to guarantee the appropriate QoS to all devices, it should be investigated how the devices within the home can coordinate their operations in such a way to automatically administer the resources inside the home. Furthermore, to make this scenario complete, for the operator another challenge is to provide and optimise QoS to areas consisting of a great number of home networks. The distribution and allocation of available resources within a group of home networks, like in a neighbourhood, is still to be investigated. This can be seen in situations, where there are a lot of bandwidth intensive needs with different requirements. Here, extra capacity has to be started and synchronised by the house to provide best possible experience for the family. This includes negotiation of capacity with the outside world and different providers.

In this context, considering an agglomerate of home networks located in proximity to each other, a question is if the home networks themselves can cooperate and interact in order to share resources, share content and perhaps coordinate the reception of content. This interrelationship could be either indirectly managed by an operator or occur in a peer-to-peer style.

An additional complication is that in the home several operators could be present, if the family has made different subscriptions. This makes management inside the home more challenging, in that the devices in the home interact with different operators. Management of the home network should then be shared or coordinated among these operators. Moreover, a device could perform routing decisions based on different factors, like cost, QoS and availability. Handover management between different operators is also an issue when devices move or experience varying connectivity. GSM, UMTS, SAE/LTE, WiMax) with the home networks is another challenge in this scenario.

Furthermore, the family and the home will have on-the-fly, ad-hoc interactions with many providers, where some of them may be very short-term, while other may last for years.

Besides the discussed challenges that arise with future home network environments, a critical issue concerns the aggregated energy consumption of the set of involved devices. Many devices around the home that do not have network connectivity are expected to integrate such functionality in the near future. The power drawn by including only an always-on mode for this functional part of each individual device would aggregate over time to an energy consumption that must not be neglected anymore, even if many individual devices remain in low-power stand-by modes during periods of low activity.

In an environment with little or no self-management capabilities no interaction takes place between devices and in certain cases they could simply be turned off completely (e.g., when

nobody is at home). The trend towards In-Network Management implies that devices must take on more responsibilities in order to carry out management tasks in an autonomous and distributed way. Taking more responsibilities may imply that each device must carry out more resource-consuming management tasks by itself, which could potentially make it more difficult to operate in low-power modes. Care should be taken when designing the functionality of the management plane so that it does not become too compute or communications intensive.

In particular cases, such as scenarios with real-time requirements, low-power modes would be even more difficult to maintain. Device reactions to external stimuli must be prompt, and waking up from a low-power mode may simply take too long thus affect SLAs. This problem can already be seen in devices that are used in home networks today, for example, sophisticated WLAN routers or cable receivers, which contain advanced logic and even operating systems that need time to assume their fully operational mode. Furthermore, In-Network Management also requires an increased level of self-awareness, which requires monitoring functionality that must be active on at least a subset of a home network's devices. This should introduce additional criteria related to energy efficiency in the design of protocols and functionality.

The problem of energy-efficient operation consists of minimising resource consumption through on-the-fly adjustments that are sensitive to the overall context and a particular situation (saving energy by means of exploiting the context of users, personal habits and preferences for example) and intelligent energy management by means of exploiting algorithmic and technological choices at design time, while assuring all the QoS and reliability requirements are met.

For example, the house could autonomously prepare the home to suit the family (i.e. adjusting temperature, lights etc.) in anticipation of the arrival of the first family members. It might start adjusting the temperature about 20 minutes before the arrival while the lights can be turned on as the car pulls up the driveway. Since only rudimentary connectivity has been switched on during the absence of the family additional capacity has to be initiated by the house as family members arrive.

6.3.13 Network Environment

The dynamic growing home networks are becoming increasingly heterogeneous, as the environment includes several devices with single or multiple functionalities. Initially they included classical TV sets, PCs connected to an ISP and phones (mobile and fixed), each of them bringing services provided by different operators. Nowadays the triple/quad play offer of an operator may compete with alternative solutions from other service providers. Furthermore, the new devices presented in **Error! Reference source not found.** (such as set-top boxes, IP phones/ videophones, wireless phones, laptop computers, IP cameras, access points, gateway devices, routers, consumer electronics, sensors) have multiple functions. They are more and more transformed into heterogeneous wireless networks: e.g. narrowband wireless for in-home sensors and broadband for media services. Outside the home ISPs have managed to compete with traditional telecom operators, by offering cellular phones and mobile Internet via their wireless access networks. Also, multiple operators may reach the home network simultaneously, which need to be either selected automatically or manually by the subscribers. Traditional WAN technologies are accompanied now by MAN, WMAN, WWAN for inter-home networks, whilst inside a house the LAN is frequently complemented by WLAN, PAN and sensor networks.

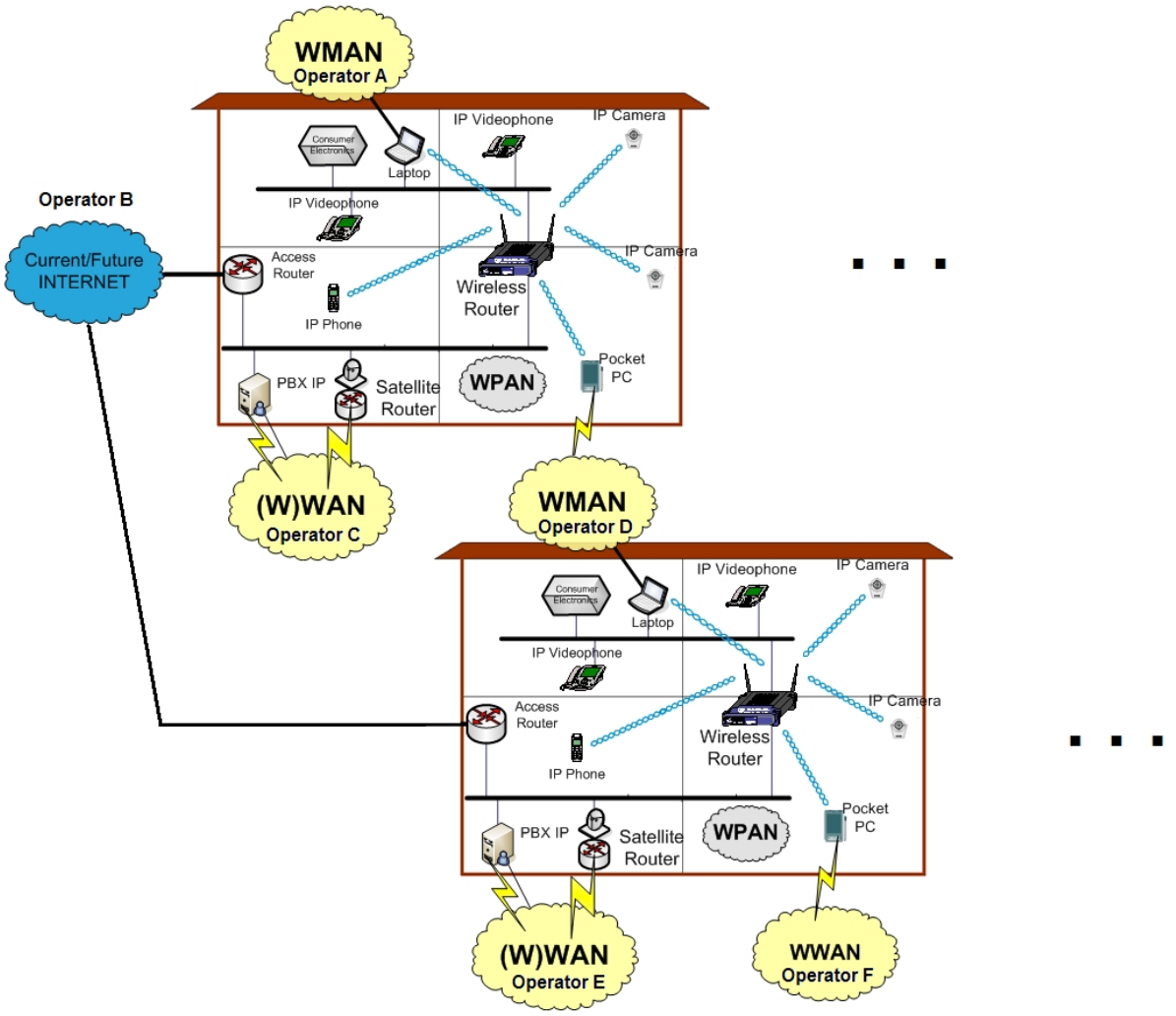

Figure 5: An example of multiple devices and network technologies within, to-and-from, and between different Home Networks

6.3.14 Key Challenges

Home Networks can be seen as an "emerging organisational entity" that has not existed in this dimension before (exception: small offices) and there are many of them (not as many as the individual people, but as many as there are "homes" or "families" evidently). Management (install, control, optimise, modify, balance) of a multitude of these new home networks is challenging, as the traditional approaches (currently centralised) may generate bottlenecks. The typical example is TR69 for provisioning/ controlling DSL routers. We will below list a few key challenges we have identified in this scenario:

1. One of the key challenges foreseen in this scenario is the **dynamic interaction between different players** - operators, service providers, equipment providers, etc.-, which will play an important role in future home networks, but is not possible with today's management paradigms.
2. Another challenge is to find the right algorithms (out of a multitude of existing, e.g. ad-hoc, mesh) and architecture for this management task, especially when trying to find the right balance between the level of autonomy (nice for the operator because this reduces his management task load) and control (not nice for both the operator and the home network owners). Where is the optimal level between these? A challenge can be

seen in **distributing available resources**, both wireless spectrum and fixed line capacity within the neighbourhood (e.g. a house with 10 home networks), while trying to be cost efficient (particularly when we expect growth of bandwidth by a factor of 100). A combination of this bullet and the bullet above is how to automatically optimise resources shared by many homes when there are different owners of different networks.

3. It is a challenge to **provide QoS** not only within the individual home network (many different devices), but also within areas consisting of multiple home networks. How can these be structured and configured/optimised? If today we are using DSLAM access concentrators, tomorrow the approach will it be all-fibre, but with the same hierarchical structure for backhaul/core networking?
4. There is also a big challenge in defining **when to connect the mobile subscriber's devices (phones) to home networks:** when is it beneficial to re-direct an ongoing data or voice call over the user's own or someone else's home network. Also what will be the relationship between the large-coverage mobile networks (GSM, UMTS, SAE/LTE, WiMAX) with the home networks?
5. Another challenge is obviously **security (both in the routing and privacy sense)**. While sharing the bandwidth (and available resources in general) might be beneficial, the user wants to be sure that unauthorised parties cannot have access to parts of their network where they shouldn't. The question is how to control it, how much control should the user have and how much the operator(s)? The typical home user doesn't want to waste time with tweaking security settings; he/she just wants to be sure that his/her private data and devices are safe. How to find and provide the balance between privacy and openness?
6. Finally, regarding energy consumption, the key challenge can be stated as the **minimisation of the overall energy consumption** in the home network that potentially interacts with operators and other home networks, while at the same time maintaining In-Network Management functionality that is able to meet QoS requirements. This is especially challenging due to the fact that self-management tasks may be highly diverse, making it more complex to devise powerful strategies that are able to significantly reduce overall energy consumption.

It should be noted that minimising overall energy consumption is a generic challenge in the modern world, related to many other activities in addition to network management. The traditional design of network management systems focused on methods that would facilitate only a unique task: supervise, control and administer the network. Next-generation network management systems (or In-Network Management planes) need to be aware of applications outside their immediate field of operation that would require services in ways not related to the standard FCAPS. A key challenge in this context is how to integrate, at design time, such interfaces that would expose information for outside consumption and be able to accept commands from applications. Solutions can be a really simple publish-subscribe mechanism, but if there is no central directory how would one find this information? Do we need to devise specialised mechanisms for this, or the existing means of the system would allow it right from the beginning? Could we use NetInf in this context? How to best serve all these new consumers (and perhaps, why not, producers) of information while still keeping the overall energy optimisation goal?

6.3.15 Detailed Use Case Description

6.3.15.1 Green IT

- Shutdown most of the wireless access points to save power when nobody at home (or in a given room)
- Wake-on-LAN-style functionality to replace the standby function of non-core electric/electronic devices
- Mobile phone as a tracking device (turning on lights in the house or garden) and remote control (TV, stereo, garage door)
- Power-saving communication modes adapting the power consumption of the device to the type of network traffic

This use case envisages a home equipped with an energy management system (HEMS).

The HEMS senses the level of activity in the house such as number of people present, their location and situational context and activates relevant devices in the vicinity, while unneeded appliances are sent to a low energy consumption mode or completely shut down to zero consumption depending on the likelihood of anticipated usage.

Late at night, when all family members in the home are asleep, the HEMS operates in minimum energy consumption mode where only the very essential home network functions are maintained such as some basic monitoring of the fridge temperature, heating adjustments, and some minimum networking functionality.

The system monitors for triggers and hints of activities of persons in the house. E.g. when someone gets up in the morning, and turns on the light in the bedroom (= manual trigger), it serves as an indication for the HEMS to switch some devices / network components in a higher level of awareness /faster reaction time (for example, from hibernation to standby). For example, the person tracking subsystem could be activated, but only in those parts of the home where tracking is required (e.g. bedroom, hallway, bathroom at first, and only the coarse-grained tracking functions). While the person moves through the home the tracking subsystem adjusts activity levels of devices in the house to be active only in those regions where it is relevant. For example, a detailed location tracking in the kitchen is only required once a person enters, and this subsystem should only be brought up then.

It is expected that energy management will in fact not change the habits of a user, but do energy management that is transparent to the user.

State-of-the-Art and Limitations (Specific to Green IT Use Case)

Energy (power) management is highly relevant in wireless sensor networks due to fact that nodes have extremely limited resources, in particular, battery capacity. A large body of work has focused on management solutions on the different protocol layers, such as energy-efficient MAC protocols [YeEtAl2002a], routing protocols [MannEtAl2005a], and tracking (application layer, e.g. [DuAndLin2005a]), and also, energy management architectures [JiangEtAl2007a]. These solutions are targeted to the specific environment of wireless sensor networks and are in most cases highly application-specific.

[YeEtAl2002a] – Wei Ye, John Heidemann and Deborah Estrin: *An Energy-Efficient MAC protocol for Wireless Sensor Networks.* In Proceedings of INFOCOM 2002, pp.1567-1576, New York, NY, USA, 2002.

[MannEtAl2005a] – Raminder P. Mann, Kamesh R. Namuduri and Ravi Pendse: *Energy-Aware Routing Protocol for Ad-Hoc Wireless Sensor Networks.* EURASIP Journal on Wireless Communications and Networking, **5**(5):635-644. Hindawi Publishing Corp.

[DuAndLin2005a] – X. Du and F. Lin: *Efficient Energy Management Protocol for Target Tracking Sensor Networks.* Proceedings of the 9th IFIP/IEEE International Symposium on Integrated Network Management, pp. 45-58, Nice, France, May 2005.

[JiangEtAl2007a] – Xiaofan Jiang and Jay Taneja and Jorge Ortiz and Arsalan Tavakoli and Prabal Dutta and Jaein Jeong and David Culler and Philip Levis and Scott Shenker: *An Architecture for Energy Management in Wireless Sensor Networks.* ACM SIGBED Review (Special Issue on the Workshop on Wireless Sensor Network Architecture), 4(3):31-36, 2007.

Due to the limited energy resources of small devices, energy management is also crucial in pervasive computing. For example, Spectra monitors the usage of application resources and, depending on resource availability, is able to determine where to execute components of an application [FlinnEtAl2002a]. The authors of [MokEtAl2007a] propose a methodology to save energy in pervasive home networks, emphasizing that always-on connectivity is vital to establish such networks. While both works consider balancing performance and quality with energy consumption in the realm of pervasive environments, they do not consider the interfacing of these networks between one another or operator networks.

[FlinnEtAl2002a] – J. Flinn, Park SoYoung and M. Satyanarayanan: *Balancing Performance, Energy, and Quality in Pervasive Computing.* In Proceedings of the 22nd International Conference on Distributed Computing Systems (ICDCS'02), pp. 217-226, 2002.

[MokEtAl2007a] – Hyung-Soo Mok, Sung-Yong Son, Jun Hee Hong and Sanghoon Kim: *An Approach for Energy-Aware Management in Ubiquitous Home Network Environment.* In Proceedings of the 5th IFIP WG 10.2 International Workshop (SEUS 2007), pp. 293-300, Santorini Island, Greece, May 2007. Springer Lecture Notes 4761.

A number of power-saving techniques in wired ICT equipment, specifically, in LAN technology, considers, among others, scaling in link-speed [GunaratneEtAl2005a],, low-power modes [GuptaEtAl2007a], and dynamic link shutdown [GuptaEtAl2007b]. Further, [Simunic2005a] surveys power saving techniques for wireless LANs. While these techniques focus on LAN technology, home networks will typically be highly heterogeneous in terms of ICT equipment, and it remains to be analysed with of such techniques are applicable in these networks.

Besides these investigations a variety of power management technologies are promoted by industry, including e.g. ACPI (Advanced Configuration and Power Interface) [ACPISpec] and Intel's SpeedStep which allows for the adaption of processor speed by software. While these technologies are targeted to PCs and workstations, many devices in the home network will have very limited interfaces to energy savings (e.g. only differentiate by stand-by and on) and possibly not support these technologies in the first place.

[ACPISpec] – *Advanced Configuration and Power Interface Specification.* Revision 3.0a, December 30, 2005.

[Simunic2005a] – T. Simunic: Power Saving Techniques for Wireless LANs. In Proceedings Design, Automation and Test in Europe, pp. 96-97, March 2005.

[GunaratneEtAl2005a] – Chamara Gunaratne, Ken Christensen and Bruce Nordman: *Managing Energy Consumption Costs in Desktop PCs and LAN Switches with Proxying, split TCP Connections, and Scaling of Link Speed.* International Journal of Network Management, 15:297-310, 2005.

[GuptaEtAl2007a] – Maruti Gupta and Suresh Singh: *Using Low-Power Modes for Energy Conservation in Ethernet LANs.* In Proceedings of the 26th IEEE International Conference on Computer Communications (IEEE INFOCOM 2007), pp. 2451-2455, Anchorage, AK, USA, May 2007.

[GuptaEtAl2007b] – Maruti Gupta and Suresh Singh: *Dynamic Ethernet Link Shutdown for Energy Conservation on Ethernet Links.* In Proceedings of the 2007 IEEE International Conference on Communications (ICC'07), pp. 6156-6161, June 2007.

In addition to the discussed proactive energy saving approaches, some commercially available monitoring products focus on monitoring energy- and power-related parameters, such as electricity consumption. For example, the ScatterWeb Meter Reading Solution allows getting data in real-time from distributed meters into an analysing application. Such tools, however, focus on collection and visualisation of relevant data and users still play an active role in deciding on energy savings strategies. Furthermore, they require dedicated measuring equipment, which is cost-intensive and which requires its own deployment and management. Rather, energy management shall be embedded within INM itself.

6.3.15.2 Plug'n'Play

As use case we consider a self-configuring TV with embedded In-Network Management capabilities; therefore, it is able to reach automatically a fully functional state, without requiring human support. Once it has been turned on, it performs all the necessary steps to get to the operative state:

The device announces its presence and capabilities in the new network and interacts with the other devices already present in the network, discovering their presence and capabilities. It will, for example, find out that another TV and a video recorder are present in the other room.

The device is able to cooperate with the other devices in order to receive configuration information for accessing the required wired and wireless resources for reception of TV content. This auto configuration mechanism includes identifying and selecting the route for connectivity towards external network environments, Service Provider discovery, and Services discovery. In this procedure, authentication mechanisms are included, in order to prevent any unauthorised device to attach to the network.

The described operations are performed without the intervention of the user. She can simply select the program she would like to see and start watching it.

When the user starts watching TV, the device automatically coordinates and optimises its reception of bandwidth within the home network, since other devices are active at the same time and have intensive bandwidth requirements as well..

This use case covers mainly the following concepts:

- Automatic configuration
- Resource control and optimisation

Automatic configuration allows for device to be Plug and Play to the network environment, in other words it can become a part of the network without the need of human support. Currently devices lack of automation and interoperability and the user cannot simply plug them in and expect them to be operative. In the case of problems, for example incorrect configuration or conflicts with other devices in the network, the user has to intervene, perform configuration manually and troubleshooting. However, the average user is not able and does not want to do that; in most of the cases he will contact the help desk and ask for help. This implies high costs for the operator to provide support and dissatisfaction of the user because he cannot immediately use his device. By embedding auto configuration capabilities in all the devices, a device can be arbitrarily attached to the home network and become integral part of it. However, the plug and play functionality is not restricted to the case of plugging in a new device: also when a device leaves the network, the other devices must be informed of the new status of the network and a reconfiguration of the network might be necessary, in order to always keep the network in the most suitable and optimised configuration. **Error! Reference source not found.** shows the new capabilities enabled by In-Network Management in comparison to the case without plug and play mechanisms.

Resource control and optimisation is necessary to provide the appropriate QoS to each device. The members of the family make use of a wide range of services, for instance IPTV, VoIP, online gaming, interactive conferences, which have different requirements as concerns QoS. Providing QoS to the end users is essential because users have very high expectations, especially when they buy a service with guaranteed QoS. As a consequence, the resources in the home need to be controlled and properly managed, for example fixed line capacity and wireless spectrum. Nowadays operators do not have control on the home network, since it is hidden behind a residential gateway. Therefore, resource management and optimisation mechanisms need to be introduced in the home. Introducing more intelligence in the home devices themselves so that they can coordinate the usage of the resources can be a way forward to make the resources in the home self-managed. For instance, when more devices are using the wireless spectrum at the same time, they must coordinate themselves in order not to interfere with each other. To achieve this, nodes must exchange announcements about services, quality and resources required and available respectively.

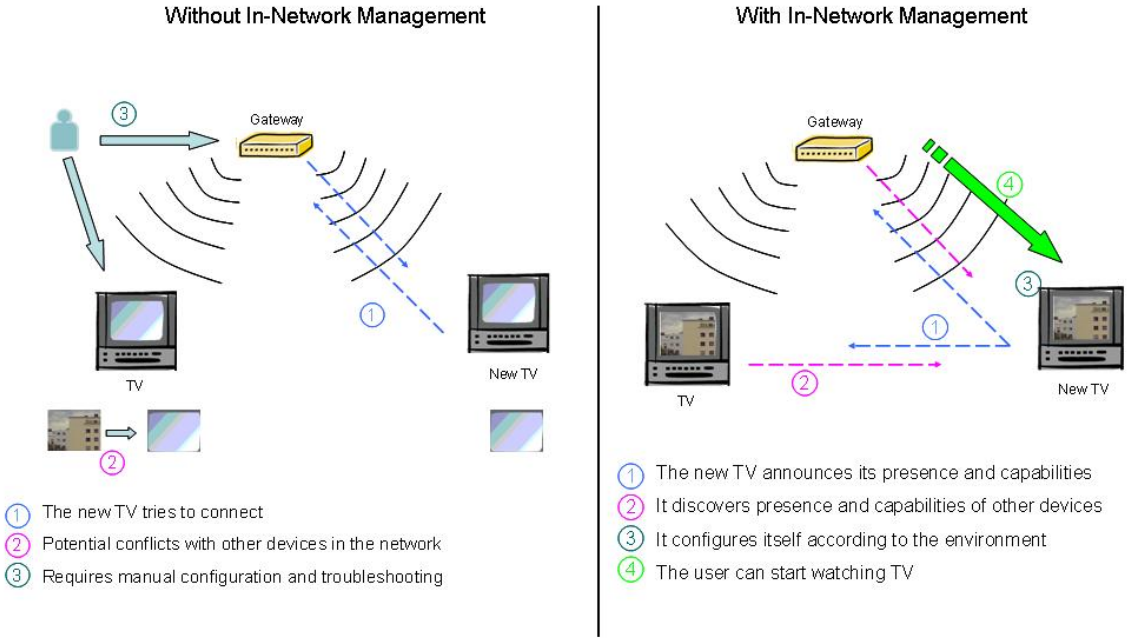

Figure 6 New capabilities enabled by In-Network Management in Plug and Play use case

6.3.16 Further Use Cases

Anomaly detection

One network element (e.g. television) causes increased network traffic (e.g. continuous network flooding) due to an internal protocol failure. By monitoring and information gathering, another network element realises this failure and informs other network elements nearby about this misbehaviour. To protect the network, the group of these network elements decides that this malfunctioning node should not be part of the network anymore and thus eliminates it from their routing tables.

6.3.17 State of the Art

6.3.17.1 The Home Gateway Initiative HGI

The Home Gateway Initiative (HGI) is an organisation that defines guidelines and specifications for broadband Home Gateways using the standards of other standard bodies. HGI's work is in particular oriented to the automation and management of the Home Network, by providing a remote management service to the Home Gateway in the first place, and to the devices beyond the Home Gateway at the customer's premise with a lesser extent. HGI aims to provide the requirements for a generic Home Gateway, although the primary access technologies envisioned are DSL and fibre. HGI identifies the Home Gateway as the central point of the management architecture, for its location at the end of the broadband access network. The main goals of the overall architecture are managing the Home Network on behalf of the customer and providing broadband services to any device in the home. The HGI architectural model assumes the presence of a single Home Gateway controlled by the operator and connected to a single Access Network. The HGI approach is based on the work of DSL Forum and in particular on the CWMP protocol specified in TR-069. HGI defines an entity named Remote Management System (RMS), which includes the Auto Configuration Server (ACS) capabilities introduced in the DSL Forum specifications and foresees the usage of the corresponding CWMP protocol. Home Gateway and end devices are also figured to interact to accomplish functionalities such as device discovery and configuration, the latter restricted to devices that are compliant to the CWMP protocol. Some Quality of Service management mechanisms are included in the HGI specifications as well. The basic principle of operation is based on the Home Gateway, which is supposed to inspect some header fields of the incoming and outgoing packets, in order to provide a packet-by-packet service classification. Currently HGI is extending its specifications with interworking with IMS and NGN core networks. http://www.homegateway.org/

6.3.17.2 TR69 for automatic DSL provisioning

TR-069 (short for Technical Report 069) is a DSL Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. It is a bidirectional SOAP/HTTP based protocol and it provides communication between CPE and Auto Configuration Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework. http://www.dslforum.org/techwork/tr/TR-069.pdf

6.3.17.3 The UPnP Forum

Universal Plug and Play (UPnP) http://www.upnp.org/ is a set of computer network protocols promulgated by the UPnP Forum. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and corporate environments. It is based on IP, HTTP, Web browsing, XML and SOAP (Simple Object Access Protocol) and GENA (General Event Notification Architecture).

Making use of UPnP technology, a device can dynamically join a network, obtain suitable network configuration parameters like an IP address, communicate its capabilities and get to know about the presence and capabilities of other devices attached to the network. Moreover, the device can easily leave the network without leaving any inappropriate state behind. UPnP provides communication between devices, managing it in a distributed manner, under the control of control devices in the network. UPnP AV (Audio and Video), group within the UPnP forum, has defined an UPnP AV Architecture, which provides media distribution services in the home. It targets home environments with consumer electronic equipment such as TVs, VCRs, DVD players and PCs. The main goal is to enable the AV content to flow between devices in the customer's network. http://upnp.org/standardizeddcps/default.asp

6.3.17.4 DLNA initiative

Digital Living Network Alliance (DLNA) is a collaboration of consumer electronics, computing industry and mobile device companies, which aims to define a set of industry design guidelines that enable different digital devices to interoperate, especially in Home Networks. The DLNA vision is that of a customer's Home Network formed by a multiplicity of digital devices; each device can store, access and play different forms of digital media and the device management intelligence is distributed throughout the Home Network. DLNA guidelines address the challenges of devices to be easy to install and able to interoperate with other devices without requiring to be configured by the customer. To accomplish these tasks, every DLNA device is provided with a networking component called Device and Service Discovery and Control, which enables devices on the Home Network to automatically self-configure networking properties and to discover the presence and capabilities of other devices on the network. Control and collaboration between devices and media management is also carried out by this component. DLNA identified in UPnP as the suitable framework for the support of these mechanisms. http://www.dlna.org/home

6.3.17.5 Devices Profile for Web Services DPWS

The Devices Profile for Web Services (DPWS) defines a minimal set of implementation constraints to enable secure Web Service messaging, discovery, description, and eventing on resource-constrained devices. Its objectives are similar to those of UPnP but, in addition, DPWS is fully aligned with Web Services technology and includes numerous extension points allowing for seamless integration of device-provided services in enterprise-wide application scenarios. DPWS builds on the following core Web Services standards: WSDL 1.1, XML Schema, SOAP 1.2, WS-Addressing, and further comprises WS-MetadataExchange, WS-Transfer, WS-Policy, WS-Security, WS-Discovery and WS-Eventing. http://www.ws4d.org/ http://schemas.xmlsoap.org/ws/2006/02/devprof/

6.3.17.6 OMA-DM; Open Mobile Alliance Device Management

OMA DM specification is designed for management of small mobile devices such as mobile phones, PDAs and palm top computers. The device management is intended to support: provisioning, configuration of device, software upgrades, and fault management. OMA DM uses XML for data exchange, the sub-set defined by SyncML. The device management takes place by communication between a server and the client. It is designed to support and utilise any number of data transports such as: physically over both wireline (USB, RS-232) and wireless media (GSM, CDMA, IrDA or Bluetooth) transport layers implemented over any of WSP (WAP), HTTP or OBEX or similar transports.
http://www.openmobilealliance.org/tech/wg_committees/dm.html

6.3.17.7 OWL-S; based on OWL (Web Ontology Language)

OWL-S is an ontology built on top of Web Ontology Language (OWL) by the DARPA DAML program. Within the OWL-based framework of the Semantic Web, for describing Semantic Web Services. It enables users and software agents to automatically discover, invoke, compose, and monitor Web resources offering services, under specified constraints. Semantic models are a promising approach to integrate different protocols UPnP, TR-069, OMA-DM.
http://www.daml.org/services/owl-s/

6.3.18 Limitations of traditional approaches

If a new PnP device has to be integrated into the home network, the configuration still involves the system administrator. This is opening the question on who is the system administrator in the family (father, mother, son....?). It would be preferable if this question can be avoided. Regarding the currently used devices, they are indeed able to advertise about the services provided but there is a complete lack of security and trust relationships (i.e. an Internet-based video-camera can perform video surveillance but it should trust the other nodes). Having nowadays multiple function devices replacing the single use ones, they are not able to discover all neighbours. Furthermore the new devices claim and use resources in an un-

coordinated way (e.g. today's WLAN frequency selection is chaotic and impacts bandwidth in a negative way). Although it is needed the current home networks cannot cooperate with other home networks or operators, as they are hidden behind home gateways (NAT/firewalls). Supposing inherent security threats of (U)PnP will be solved in the near future, another limitation will arise. The packets exchanged within the home network are not able to select themselves the proper route to destination (within active networks).

6.3.19 Approaches and Techniques

The possible approach is to have a PnP device acting as self-organised node, with embedded self-descriptive management functions and self-routing mechanisms. This means they should be able to select among different WAN/LAN technologies, protocols and paths. Inter-working with all other self-organised nodes could be realised by advertising the existence of each new node, the services offered (intra- and inter-home networks) and also the resources they would occupy.

6.3.20 Expected Benefits from In-Network Management for Home Networks

The home network will be completely scalable, according to particular wishes of the inhabitants. In-Network Management will avoid unexpected costs for installation, configuration and maintenance of new devices (both operators and owners will benefit of it). The customers will be encouraged to demand new services according to their immediate needs and the operators should optimally fulfil their requests. It may not be necessary any more for future operators to provide every single household with their own DSL; instead, maybe only the house is provided with the "bit-pipe" while inside, the rest is self-organised, even between different families.

6.3.21 Requirements

Multicasting the status and capabilities information for each node is currently used in existing home networks and it will remain a required functionality. The new techniques requested are related to self-routing (i.e. an information object selects itself the proper route to destination), self-separation of administrative domains and ownership, self-management of available resources. Having In-Network Management available, it will become very comfortable to support all type of devices (laptop, mobile phone, PDA, video-camera, TV set, PC, consumer electronics, sensors, etc), all legacy technologies (UMTS, WiMAX, WiFi, PSTN, Gigabit Ethernet, Bluetooth, IEEE 802.15.4, etc). Everything should have complete functionality 24/7 (including self-healing) with power saving capabilities. By establishing and detecting trust relationships, the nodes will prevent intruders to gain access to personal data.

6.3.22 Other Required Functionalities

- Manage a multitude of home networks
- Do not manage it in a central way; instead manage them via some components that perform the tasks and act for operator(s) and users
- These components should be located within every home network
- Distribution means that the components can be spread over all home networks and over all the participating devices

6.3.23 Relations to other WPs

- WP2 is responsible for the overall new architectural principles and concepts. Since INM and the home network scenario wants to have network management and control as a key building block in the architecture and concepts from the very beginning we need to cooperate and influence this work from day one. Furthermore the home network scenario imposes new requirements on the architecture and principles that must be included by NewAPC.
- WP3 is investigating novel ways of sharing resources to enhance efficient use of these resources through virtualisation. The home network scenario shows multiple instances

where virtualisation will be used, and hence also some requirements on what virtualisation has to support.

- WP5 deals with forwarding and multiplexing for generic paths. In the home network scenario we highlight many situations where this functionality is required to enhance the utilisation of the resources within the home, as well as using multiple accesses to-and-from the home to cope with dynamicity and changing environments.
- WP6 looks at information-centric issues. INM and the home network scenario both provides a lot of information about the networks and resources, as well as uses this and other information to control the networks and their surroundings. Examples here are the adjustment of the house temperature based on when the family is expected to come home and the refill of fuel in the home.

6.4 Scenario 4: Large-scale adaptation in response to dramatic events (DEFCON)

6.4.1 Scenario Description and Network Environment

The future Internet will be critical to society in the sense that it must never completely fail and must at least provide basic services all times. The widely differing operating conditions that the future Internet will face during its lifetime mandate mode-switching mechanisms, i.e., mechanisms for rapid switching among global network configurations in response to global conditions inside or outside the network.

We envision a set of levels of readiness for the management plane, similar to the “defence readiness condition” (DEFCON) of the USA Armed Forces. The level of readiness is determined by the networking conditions.

The scenario centres around global or domain-wide reconfiguration of network, network services and network control mechanisms, which are triggered by internal or external events. Events are global conditions, such as sudden significant damage to network infrastructure, large-scale cyber attacks on the network control plane, network instabilities, and threshold crossings of global metrics or network health indicators. Such events are detected by InNet Management functions in the management plane. Global reconfiguration means switching the network from one mode to another. This might affect the configuration on all (or a large number of) networks nodes and is achieved by InNet Management functions in the management plane.

This scenario considers two types of use cases. First, disaster scenarios that include major disruptions of the network infrastructure. Second, the self-adaptation of network control mechanisms triggered by a global performance parameter crossing a critical threshold.

The unique characteristic for this scenario is that there is a sudden and severe change in the environment that requires a complete re-configuration or even new initialisation of the network. The scenario covers the most extreme challenging case for In-Network Management and can be used as stress-test scenario.

6.4.2 Key Challenges

- Scalability. This is a key challenge in management solutions for large and dynamic networks
- Adaptability. Management solutions need to adapt to changing networking conditions, such as node failures and topology changes.

6.4.3 Detailed Use Case Description

6.4.3.1 Recovering from major drop in service quality

This use case considers dramatic (and rare) events, which need a rapid response action by the management plane, but whose root cause might not be determined in a short time-scale.

Scene 1: We are continuously monitoring (performed in a decentralised fashion) the network-wide distribution of the throughput for users watching a live football game on the web. The game video is distributed using an Akamai-like approach.

Scene 2: A critical threshold is crossed. More than 10% of end-users get a throughput below 300 kbps (those indicated with a red arrow), considered to be insufficient. Moreover, a runaway behaviour is detected: the percentage of end-users experiencing quality degradation is increasing steadily. (Figure 7)

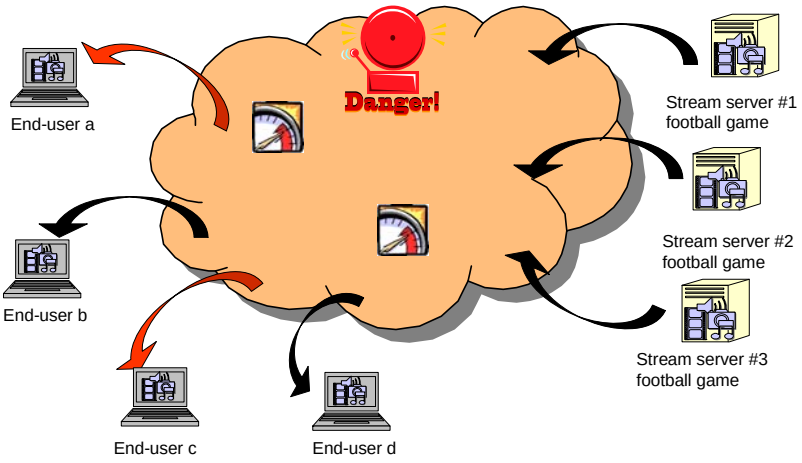

Figure 7 Scene 2: The Management Plane detects a drop in the service quality for a number of end-users (red arrows)

Scene 3: This causes the (distributed) management plane to take action. In order to detect the root cause, it starts monitoring a range of other metrics, such as server peak load values and server load distribution.

Scene 4: Based on the available information (possibly incomplete), the Management Plane determines that the potential causes for the quality drop could be (1) several of the servers assigned to this event are unreachable, (2) a sudden increase in the number of end-users watching the game.

Scene 5: This triggers three actions (Figure 8):

- 1) problem stabilisation: assignment of five clusters from a reserve pool to the distribution of the football event.
- 2) problem diagnosis: a deeper root cause analysis is started
- 3) problem notification: an alarm is sent to management station

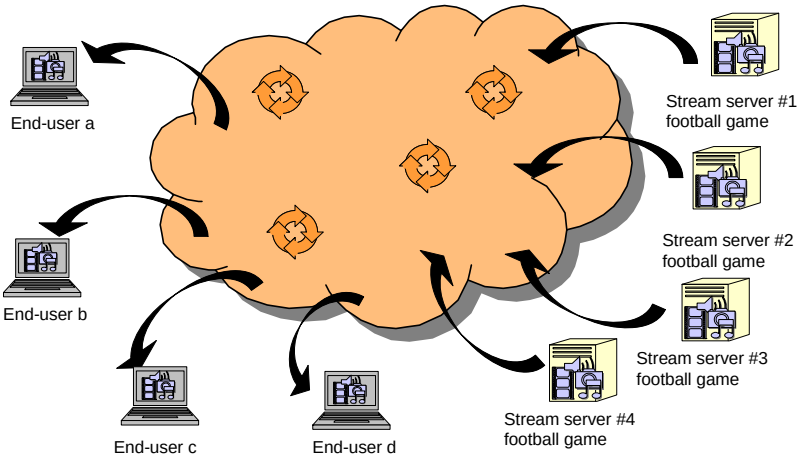

Figure 8 Scene 5: The Management Plane stabilises the problem by assigning more servers to the video distribution. Service quality recovers.

6.4.3.2 Creating communication services for emergency operations

Emergency situations arise in real life in case of catastrophes or big accidents and the Future Internet might play an important role in the creation of new instruments to help the community in such situations. In fact the diffusion of networked devices in different environments of users' life can be used to provide effective help in emergency situations like not possible today. This use cases highlights the need for enhanced management capabilities in the devices to enable this type of services.

In emergency situations it is required to provide timely information to the community, such as warning messages about the coming danger or directives about a proper behaviour. Today many of these operations require manual assistance, because media channels (e.g. television programs in homes, hotels, or public areas, web pages, mobile telephone messages) must be manually initiated to deliver the proper emergency information. Additionally, there is no guarantee that the network is able to provide the delivery of that information, because the network itself is not aware of new emergency condition around. In bad situations, safety messages cannot be delivered to the interested people or injured people cannot get access to emergency services.

As exemplary situation, this use case considers the emergency situation arose from an earthquake in an urban area. Given the diffusion of portable devices and networked equipment in general, different communication channels exist to bring emergency information. The expected capability from the network is to assure that all these devices and their infrastructure is able to adapt their behaviour to assure the emergency services.

When the earthquake is sensed, for example from the sensors distributed in the urban area, the network management plane is informed of the emergency; as a consequence, a series of configuration changes are enforced. In a hotel, the local distribution of TV contents is interrupted and guests' TV sets are connected to media content servers, reporting the emergency in place. Different actions can be involved in this process, like the remote activation of the TV sets, the interruption of all internal web traffic and reconfiguration of the gateway towards the network operator.

Outside the building, the mobile wireless networks are also adapted to give priority to emergency communication. Base stations around the affected area adapt their QoS

scheduling mechanism, so that common call requests are given low priority and resources are reserved for emergency services.

Figure 9 compares the behaviour of the network in an urban area during emergency situations, like an earthquake. Currently, people residing in a building are notified of the emergency situation through their TV sets; the emergency messages must be manually sent with the TV control system, located at the ground floor. Additionally, the cellular network can become overloaded due to an exceptionally high number of calls; as a consequence, people needing assistance might not reach emergency facilities, like a hospital emergency number. Given this scenario, INM can provide the means to support two main functions. The first one is the tight coupling of the TV system with emergency services, so that manual intervention is not required to distribute emergency messages to TV sets. Secondly, the cellular network can be quickly adapted to change access control mechanisms; in this way, people with urgent needs would be given priority.

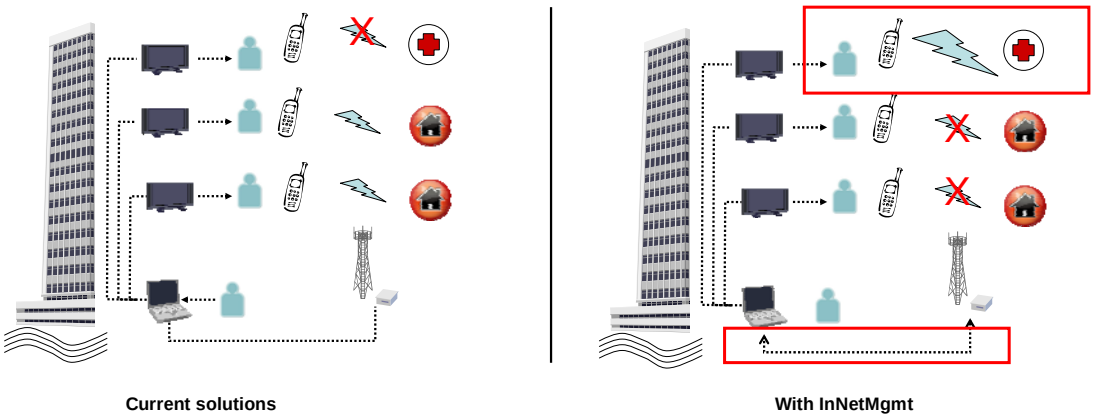

Figure 9 Comparison of network emergency situations.

6.4.4 Further Use Cases

Next we include some classes of further potential use cases

- Major disruption of network infrastructure caused by natural disasters (earthquake, tsunami), war-like events, large-scale cyber attacks politically/economically-motivated (major policy decisions possibly based on this kind of events). For example, as a result of massive cyber-attack, 40% of net equipment is infected by a virus and needs to be shutdown. In response all non-critical video and audio communication is shut-off and 50% of the network capacity is assigned to network re-configuration, recovery, and connection re-establishment, and 30% or the remaining resources to key core services.
- Self-optimisation of a network control mechanism based on global state information and performance objectives. An example is switching MANET routing schemes, based on global metrics, such as: mobility and average path length.
- Monitoring and recovering from major network instabilities/failures due to external circumstances (drastic shift in load patterns, runaway behaviour by classes of network applications, instable feedback loops).
- Network rejuvenation, including distributed maintenance, generic testing, and distributed garbage (collection of global network objects, such as, virtual circuits), in response to reaching specific aging threshold.

“Collapse and recovery of VoIP service due to feature interaction in connection with operating system update”

A network operator runs a widely used VoIP service. The VoIP service relies on a coordination protocol, a distributed data structure such as a distributed hash table. The coordination protocol runs on top of a large network of servers running some dialect of Windows. Windows is updated, to include some new feature which interacts badly with a communication service used by the coordination protocol. This feature interaction causes the VoIP service to fail locally, and it also gives rise to a substantial amount of recovery traffic, to attempt to rebuild the coordination data structure, which is now partially broken. A management station observes that a lower threshold on VoIP traffic is crossed, indicating something is not right. In order to determine the root cause the management plane starts monitoring recovery traffic and observes a substantial increase. It now decides to stabilise the situation by:

a) Sandboxing the recovery traffic

b) Activating a backup VoIP service, to reroute new calls to that service, instead of the more advanced and efficient, newer version.

The sandboxing and alternative service activation are automatically configured on each server. Having done this the manager decides to aggregate possible event correlates per server, across the entire network. It turns out that service failure log entries and OS update event log entries are strongly correlated. It then decides to roll back the OS updates. By global monitoring of the appropriate aggregates the network manager observes that the rollback causes recovery traffic and amount of failure log entries to decrease, and it can then start routing calls to the new service again.

6.4.5 State of the art

Decentralised Network monitoring

Recently, there has been significant research in real-time monitoring of macroscopic network metrics (such as the quality threshold discussed in one of the use cases above). A key aspect in those works is the control of fundamental trade-off in monitoring: quality of the estimation versus the required monitoring resources. Achieving high quality estimations requires significant amounts of resources, and limited resources possibly mean low quality estimations. The quality of estimation includes two aspects. First, the accuracy: how close the estimation is to the actual value. Second, the latency: how long it takes to present an estimation of the current aggregate to the monitoring station(s).

In the literature, we can find different instantiations of this trade-off. We can classify them into three categories: latency vs. overall traffic [Inta00] [Kris02] [Kris02b] [Madd02], maximum error vs. overall traffic [Boul03] [Corm05] [Deli04] [Inta02][Shar04], and accuracy vs. storage requirements [Babc02] [Cons04] [Fang98] [Nath04].

Most of the proposed approaches in this research area have been evaluated using simulation. Examples of schemes that have been evaluated through a prototype implementation in the context of fixed networks are [Gonz07] and [Olst03]. [Madd02] and [Zhao03] report on implementations of real-time monitoring of macroscopic metrics in the context of sensor networks.

[Inta00] C. Intanagonwiwat, R. Govindan, and D. Estrin, “Directed diffusion: A scalable and robust communication paradigm for sensor networks”, In Sixth Annual International Conference on Mobile Computing and Networking (Mobicom), Boston, USA, August 2000.

[Kris02] B. Krishnamachari, D. Estrin, and S. Wicker, “The impact of data aggregation in wireless sensor networks”, In International Workshop of Distributed Event-Based Systems, Vienna, Austria, July 2002.

[Kris02b] B. Krishnamachari, D. Estrin, and S. Wicker, “Modelling data-centric routing in wireless sensor networks”, Technical Report CENG 02-14, USC Computer Engineering, 2002.

[Madd02]S.R. Madden, M.J. Franklin, J.M. Hellerstein, and W. Hong, “TAG: a tiny aggregation service for ad-hoc sensor networks”, In Fifth Symposium on Operating Systems Design and Implementation, Boston, USA, December 2002.

[Boul03] A. Boulis, S. Ganeriwal, and M. B. Srivastava, “Aggregation in sensor networks: an energy - accuracy tradeoff”, Elsevier Ad-hoc Networks Journal (special issue on sensor network protocols and applications), pages 317–331, 2003.

[Corm05] G. Cormode, M. Garofalakis, S. Muthukrishnan, and R. Rastogi, “Holistic aggregates in a networked world: distributed tracking of approximate quantiles”, In ACM SIGMOD International Conference on Management of Data, Baltimore, USA, June 2005.

[Deli04] A. Deligiannakis, Y. Kotidis, and N. Roussopoulos, “Hierarchical in-network data aggregation with quality guarantees”, In 9th International Conference on Extending Database Technology (EDBT), Crete, Greece, March 2004.

[Inta02] C. Intanagonwiwat, D. Estrin, R. Govindan, and J. Heidemann, “Impact of network density on data aggregation in wireless sensor networks”, In 22nd International Conference on Distributed Computing Systems, Vienna, Austria, July 2002.

[Shar04] M. A. Sharaf, J. Beaver, A. Labrinidis, and P. K. Chrysanthis, “Balancing energy efficiency and quality of aggregate data in sensor networks”, ACM International Journal on Very Large Data Bases, 13(4):384–403, December 2004.

[Babc02] B. Babcock, S. Babu, M. Datar, R. Motwani, and J. Widom, “Models and issues in data stream systems”, In 21st ACM Symposium on Principles of Database Systems, Madison, USA, June 2002.

[Cons04] J. Considine, F. Li, G. Kollios, and J. Byers, “Approximate aggregation techniques for sensor databases”, In 20th International Conference on Data Engineering, Boston, USA, March 2004.

[Fang98] M. Fang, N. Shivakumar, H. Garcia-Molina, R. Motwani, and J. D. Ullman, “Computing iceberg queries efficiently”, In 24th Int. Conf. Very Large Data Bases (VLDB), New York City, USA, August 1998.

[Nath04] S. Nath, P. B. Gibbons, S. Seshan, and Z. Anderson, “Synopsis diffusion for robust aggregation in sensor networks”, In Second ACM Conference on Embedded Networked Sensor Systems, Baltimore, USA, November 2004.

[Gonz07] A. Gonzalez Prieto, R.Stadler "A-GAP: An Adaptive Protocol for Continuous Network Monitoring with Accuracy Objectives", IEEE Transactions on Network and Service Management (TNSM), Vol. 4, No. 1, June 2007

[Olst03] C. Olston, J. Jiang and J. Widom, “Adaptive Filters for Continuous Queries over Distributed Data Streams”, ACM SIGMOD 2003, San Diego, USA, June 2003.

[Zhao03]J. Zhao et al., “Computing aggregates for monitoring wireless sensor networks”, 1st IEEE International Workshop on Sensor Network Protocols and Applications, Anchorage, USA, May 2003.

Self-configuration

While the existing work on real time autonomic self-configuration has a narrow focus, there are some works on configuration of management algorithms [Liot99] [Liot02] [Chen02] [Zhu01] [Mart99]. Those works aim at determining the appropriate configuration for different management tasks and networking scenarios. A key result in this area is the lack of a silver

bullet. Different networking conditions require different configurations. An interesting parallelism the business management is stated in [c5]. Large businesses are run very differently from small ones. Similarly, the appropriate configuration for a network has to be based on its characteristics. Along the same idea, as the economic situation changes, businesses must adapt their decisions. Similarly, networks need to adapt to changing networking conditions. While this set of works are a good starting point and provide some design guidelines, they are far from our objective of an autonomic self-configuring management plane, since self-configuration is not the focus of those works.

[Liot99] A. Liotta, G. Knight, G. Pavlou, On the Performance and Scalability of Decentralised Monitoring Using Mobile Agents, in Active Technologies for Network and Service Management, Proceedings of the 10th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management (DSOM '99), Zurich, Switzerland

[Liot02] A. Liotta, G. Pavlou, G. Knight, Active Distributed Monitoring for Dynamic Large-scale Networks, Proceedings of the IEEE International Conference on Communications (ICC'01), Helsinki, Finland, Vol. 5, pp. 1544-1550, IEEE, June 2001

[Chen02] T. Chen, S. Liu, "A model and evaluation of distributed network management approaches," IEEE J. on Selected Areas in Communications, vol. 20, May 2002

[Zhu01] Y. Zhu, T. Chen, S. Liu, "Models and analysis of trade-offs in distributed network management approaches," 7th IFIP/IEEE Int. Symp. on Integrated Network Management (IM 2001), Seattle, May 14-18, 2001

[Mart99] Jean-Philippe Martin-Flatin, Simon Znaty and Jean-Pierre Hubaux, “A Survey of Distributed Enterprise Network and Systems Management Paradigms”, Journal of Network and Systems Management, Volume 7 , Issue 1, March 1999.

Emergency services

The support for emergency services in IP networks has been recently receiving some attention from some standardisation bodies. Both 3GPP and IETF are considering extensions to support emergency service in their architectures. [3GPP_Tech] provides an analysis of requirements to deliver emergency services in the 3GPP systems and defines some extensions to the signalling schemes. [RFC5012] provides a similar analysis study for services based on SIP. Both the studies are clearly targeting specific architectures, and they do not provide generic mechanisms to reconfigure the network globally.

[3GPP_Tech] – 3GPP Technical Specification Group Services and System Aspects; Earthquake and Tsunami Warning System Requirements and Solutions (ETWS); Solution Placeholder TS 22.168 (Release 8) V0.1.0 (2008-01).

[RFC5012] – Internet Engineering Task Force (IETF): *Requirements for Emergency Context Resolution with Internet Technologies.* Request for Comments (RFC) 1155. January 2008.

6.4.6 Limitations of traditional approaches

Real-time monitoring of fast-changing network environments is not feasible today since the costs are prohibitive using today’s management approaches.

At the same time, real-time automatic reconfiguration has been addressed to date only for a small set of functionality (e.g., routing). Most aspects of reconfiguration have not been studied to date and reconfiguration is generally done manually on a per-device basis.

Emergency situations are today handled manually and require coordination between human operators of different organisational entities, like local and country authorities, network

providers and media services. A recent effort to support emergency services, especially targeting the cases of earthquakes and tsunamis, is currently investigated in [3GPP_Tech]. This document captures the importance of emergency capabilities in next generation networks, but the purpose of the document is clearly limited to a specific type of networks and relies on an operations controlled centrally by the network operator. The extension to this capability to a heterogeneous network, where different types of devices need to collaborate like shown in Figure 9, is therefore not possible.

6.4.7 Approaches and Techniques

In order to achieve the functionality described in this scenario, we will develop the "InNet Management" paradigm, which includes:

- Real-time monitoring, which is self-tuning and adaptive to a changing network environment. It is fundamental to develop robust & real-time techniques for measuring and monitoring aggregate network state
- Techniques for management decentralisation to support scalability and fast reaction time
- Efficient distributed management algorithms that adapt to network conditions and enable self-* capabilities

It is also required to engineer techniques for the network to automatically adapt to policy decisions and changes in operational environments. This potentially means changing control parameters in all network components. This has to be in real-time and conducted in a safe manner.

6.4.8 Expected Benefits for Large-scale Adaptation

A set of capabilities that are not possible for today's Internet, but will be a fundamental requirement for the critical infrastructure of society in the future.

INM will provide means to switch the behaviour of the network with the following schemes:

- The configuration change would happen quickly, within the range of few seconds within a wide area network or a second in a local area network.
- Additionally the configuration would be enforced consistently over the different devices. For example QoS profiles would be mapped consistently in different places of the network, so that the delivery success of critical end-to-end services or broadcast messages is guaranteed. Additionally, the correct media with the necessary reliability would be chosen based on the current conditions. Accounting processes could also be informed of a critical situation, like an emergency situation.
- The success of the configuration would be guaranteed on different external conditions. In case where a network connection does not provide the expected characteristics in terms of timeliness or reliability, the best alternative connection would be discovered and selected. Eventually, this would be achieved through a learning phase, performed during the plug-and-play phase or periodically.

6.4.9 Requirements

A distributed management architecture, whereby each network device participates in the management tasks by running management processes.

Access to local variables at the managed nodes. This can be realised through a variety of mechanisms and requires a well-defined interface.

The quick switching of a network-wide behaviour at different scales requires some pre-constructed relationships between the devices. It is therefore required that the devices run some self-discovery mechanisms and maintain internally a topology of the components required for the fast switching.

Additionally, it is required that a device is aware of the current network conditions, like delay times or reliability of the link between the other components. This would allow choosing the best mechanism to disseminate the configuration change. In general, the new capabilities are expected to work on links of different reliability, but the device should be aware of the probability of error related to the link. On the other side it is clear that the limitations of the physical link would have an impact on the overall performances of the fast switching mechanism; for example a considerable transmission time over a noisy wireless channel would inevitably impact the time to complete a re-configuration process.

Besides the conditions of the link, the characteristics of the other devices might play a role on the performance of the switching mechanism. A device with limited computational power or in an energy-saving mode would affect the time to achieve a consistent global configuration. Also in this case, the new management capabilities can mitigate the impact of such bottlenecks, but physical characteristics, like the time to wake-up of an a device in power-save mode, poses a lower boundary on the fast switching mechanism.

A common information model and a security framework would also be required to allow the collaborative mechanism between devices.

6.4.10 Relations to other WPs

WP1, business innovation, the functionality presented in this scenario is of critical business value.

WP2: consistency with WP2-proposed architecture, principles and concepts. The management plane of the architecture has to support DEFCON capabilities

WP3 Network Virtualisation: the abstraction of network resources, locally used for network adaptation. DEFCON functions will reconfigure the virtual networks following global policy decisions triggered by network disruptions.

WP5 Generic paths: re-routing in the control plane. DEFCON functions will be responsible for reconfiguring generic paths.

WP6 Network of information: information-centric network management, and network adaptation. NetInf proposed a data-centric network architecture; the network is made of collection of objects, and a set of operations that creates them, publish them, and manages them. Network states described in this scenario can be modelled as NetInf objects.

Chapter 7 Evaluation Criteria for In-Network Management

Ideas, concepts, methods and architectures developed within INM will be evaluated in months 16-24 of the 4WARD project and the results will be presented in a final document. The goal of the evaluation is to prove the feasibility of INM as well as to identify and quantify improvements that can be achieved by applying INM. The scenarios defined in Chapter 6 of this document serve as one basis for this evaluation. Further evaluation criteria, such as additional scenarios, use cases or requirements may be added later as appropriate during the ongoing work of the 4WARD project.

This document provided first material to verify the benefits of INM, because the scenarios highlighted problem cases where traditional approaches cannot be efficiently adopted. As a result, the scenarios defined a set of requirements and expected benefits that will guide the construction of the new INM framework. In other words, the problem cases presented in this document will be regarded as checkpoints to compare INM with respect to traditional approaches.

An important aspect in the definition of a new management architecture, like INM, is the two-fold impact on the Future Internet. One direction will bring incremental benefits with respect to traditional approaches. It is expected that the new management functions will be more efficient, for example they will control and limit the traffic consumption of maintenance processes. The other direction is more challenging and goes along the line of introducing new enhanced capabilities in the Future Internet which cannot be supported today. This impact cannot be evaluated against existing approaches or existing operative networks at all, but analysis studies and proof-of-concepts prototypes will instead be more suitable for this purpose.

Given the variety of the purposes of the INM framework, the evaluation will use different instruments to meet the different requirements, as explained in the following:

- **Analysis.** Different mathematical studies will be conducted to model the main characteristics of the new architecture and assess complexity of management operations. For example scalability and robustness properties can be modelled and predicted through mathematical instruments.
- **Simulations.** Simulations will be conducted to evaluate a range of performance parameters of INM in practical configurations of an operative network. The results will provide quantitative results about increased performances of INM. In those cases where a new capability is investigated, the simulations will provide initial expected behaviour of the new solutions.
- **Demonstrator.** A prototype will be implemented at the end of the project to assess practical feasibility of a selected set of functionalities of the INM. The demonstrator will exemplify capabilities and applicability of INM by implementing a set of functions that overcome limitations of traditional network management paradigms. The demonstrator will serve as a proof of concept and will provide an evaluation of the effectiveness of the solutions when running a network as well as their usability in practical operations.

The evaluation will give an exhaustive assessment of the advanced capabilities of INM with respect to the following criteria:

- **General feasibility**. It will be shown that the overall INM can meet practical deployments in the Future Internet.
- **Proof-of-concept**. It will be shown a selected set of new capabilities on a demonstrator, so that their behaviour and usability on an operative network can be assessed.
- **Increased performances**. It will be shown that INM will increase performances of management operations with respect to a selected set of the requirements; some of these

requirements have been identified already in this document and additional ones might be collected during the 4WARD project. The use of analysis and simulations will provide quantitative results on these requirements, e.g. reduction of traffic overhead or dimension of the managed network.

It is expected that the selection of criteria discussed in this chapter will produce an extensive and robust evaluation for the document planned for month 24 and will include all the novel capabilities developed within the INM framework.

Chapter 8 Conclusion

The current document concentrated on a set of scenarios and use cases that were chosen as being representative for the challenges encountered in the future Internet. The idea was to come up with a set that is small enough to be studied in depth, but also varied between each other to cover a wide spectrum of technological and non-technological aspects that need to be considered within network management in the future Internet. As a result of an evaluation process 4 scenarios have been selected, and the final candidates comprise self-management in wireless multi-hop networks, management requirements in the networks of a large operator, management needs of home networks environments, and management strategies for preserving network availability under extreme conditions.

The scenarios serve as a kick-off activity for the research in the 4WARD In-Network Management framework. The scenarios were carefully selected to allow for comprehensive analysis of the problem space that needs to be addressed by network management in the future Internet. The scenarios have been examined with respect to current state-of-the-art in order to help to identify promising methods and techniques to be applied in the In-Network Management architecture. The scenarios set up an evaluation framework for the results developed within this work package. By concentrating on concrete environments and situations as described in the use cases we gain evaluation criteria and define measurable objectives for the solutions proposed by In-Network Management, and provide a blueprint for defining demonstration and testing environments in later stages of the project work. The scenarios create a common language and focus for the various approaches examined with the parallel tasks within the work packages. They also represent a common ground for integration and cooperation between work packages.

References

[AgoulmineEtAl2006a] – Nazim Agoulmine, Sasitharan Balasubramaniam, Dmitri Botvitch, John Strassner, Elyses Lehtihet and William Donnelly: *Challenges for Autonomic Network Management.* 1st IEEE International Workshop on Modelling Autonomic Communications Environments, Dublin, Ireland, October 2006.

[AgrawalEtAl2005a] – D. Agrawal, K. W. Lee, and J. Lobo, "Policy-Based Management of Networked Computing Systems," IEEE Commun. Mag., Oct. 2005, vol. 43, no. 10, pp. 69–75.

[AhlgrenEtAl2005a] – *Ambient Networks: Bridging Heterogeneous Network Domains.* In Proceedings of the IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications, Volume 2, pp. 937-941, September 2005.

[Akhtar 07] – N. Akhtar et al., "Network Composition: A Framework for Dynamic Internetworking between Networks", IEEE ChinaCom 2007, China, Shanghai, 22-24 August 2007

[Alphaworks_Policy02] – http://www.alphaworks.ibm.com/tech/pmac

[AmbiNetProject] – Ambient Networks. Supported in part by the European Commission under its Sixth Framework Programme. http://www.ambient-networks.org/

[ANAProject] – Autonomic Network Architecture (ANA). Project funded by the European Union Information Society Technologies Framework Programme 6 (EU IST FP6). http://www.ana-project.org/

[BabaogluEtAl2006a] – O. Babaoglu et al.: Design Patterns from Biology for Distributed Computing. ACM Transactions on Autonomous Adapt. Sys., **1**(1):26-66, September 2006.

[BalasubramaniamEtAl2006a] – Sasitharan Balasubramaniam, Keara Barret, William Donnelly, Sven van der Meer and John Strassner: *Bio-inspired Policy Based Management (bioPBM) for Autonomic Communications Systems.* Seventh IEEE International Workshop on Policies for Distributed Systems and Networks (Policy 2006), pp. 3-12, 2006.

[BelecheanuEtAl2004a] - Belecheanu, R., Jawaheer, G., Hoskins, A., McCann, J.A., Payne, T., "Semantic web meetings autonomic ubicomp" in Proceedings of the Workshop on Semantic Web Technology for Mobile and Ubiquitous Applications, Hiroshima, Japan, 2004.

[BellavistaEtAl1999a] – Paolo Bellavista, Antonio Corradi and Cesare Stefanelli: *An Open Secure Mobile Agent Framework for Systems Management.* Journal of Network and Systems Management, **7**(3):323-339, 1999.

[BernersLeeEtAl2001a] – Berners-Lee, T., Hendler, J., Lassila, O., "*The Semantic Web*", Scientific American, May 2001.

[BoutabaAndXiao2002a] – Raouf Boutaba and Jin Xiao: *Network Management: State of the Art.* Proceedings of the IFIP 17th World Computer Congress (WCC'02) – TC6 Stream on Communication Systems: The State of the Art. IFIP Conference Proceedings Vol. 220, pp. 127-146, Montréal, Québec, Canada, 2002. ISBN: 1-4020-7168-X. Kluwer, B. V. Deventer, The Netherlands.

[BushAndKalyanaraman2006a] – S. F. Bush and S. Kalyanaraman: *Management of Active and Programmable Networks.* Journal of Network and System Management, **14**(1):1-5, March 2006.

[BushAndKulkarni2001a] – S. F. Bush and A. B. Kulkarni: Active Networks and Active Virtual Networks Management Prediction: A Proactive Management Framework. Norwell, MA: Kluwer, 2001.

[ChadhaEtAl2004_Policy07] – R. Chadha, H. Cheng, Y.H. Chend, J. Chiang, A. Ghetie, G. Levin, H. Tanna, "Policy-Based Mobile Ad Hoc Network Management", In Proceedings of the Fifth IEEE Workshop on Policies for Distributed Systems and Networks (POLICY'04), New York, USA, June 2004.

[CheikhrouhouEtAl1998a] – Morsy M. Cheikhrouhou, Pierre Conti and Jacques Labetoulle: *Intelligent Agents in Network Management: A State-of-the-Art.* Networking and Information Systems, **1**(1):9-38, 1998.

[ChengEtAl2006a] – Yu Cheng, Ramy Farha, Myung Sup Kom, Alberto-Leon-Garcia and James Won-Ki Hong: *A Generic Architecture for Autonomic Service and Network Management.* Computer Communications, **29**(18):3691-3709, November 2006.

[CronkEtAl1998a] – T. Cronk, B. Callahan and L. Bernstein: Rule-Based Expert Systems for Network Management and Operations. IEEE Network, pp. 11-21, September 1998.

[DobsonAndMcDermid1989a] – J. E. Dobson and J. A. McDermid: *A Framework for Expressing Models of Security Policy.* IEEE Symposium on Security & Privacy, Oakland, California, May 1989.

[DobsonEtAl2006a] – Simon Dobson, Spyros Denazis, Antonio Fernández, Dominique Gaïti, Erol Gelenbe, Fabio Massacci, Paddy Nixon, Fabrice Saffre, Nikita Schmidt and Franco Zambonelli: *A Survey of Autonomic Communications.* ACM Transactions on Autonomous and Adaptive Systems, 1(2):223-259, December 2006.

[ENERGyProject] – Empowered Network Management (ENERGy). http://www.itea-energy.eu/

[FanEtAl2007_Policy09] – Fan, C. et. Al, “Managing Heterogeneous Access Netowrks Coordinated policy based decision engines for mobility management”, 32nd IEEE Conference on Local Computer Networks (LCN 2007)

[Giaffreda07] – R. Giaffreda et al., " Context, Network and Policy Management for Ambient Networks", Ambient Networks Deliverable FP6-CALL4-027662-AN P2/ D22-D2, December 2007, available at www.ambient-networks.org.

[Gonzalez 07] – A. Gonzalez Prieto, R.Stadler "A-GAP: An Adaptive Protocol for Continuous Network Monitoring with Accuracy Objectives", IEEE Transactions on Network and Service Management (TNSM), Vol. 4, No. 1, June 2007

[Gupta2006a] – Ankur Gupta: *Network Management: Current Trends and Future Perspectives.* Journal of Network and Systems Management, **14**(4):483-491, December 2006.

[ITU-X-753] – Information Technology – Open Systems Interconnection, command Sequencer for Systems Management. ITU-T Recommendation X.753, 1998.

[JelgerEtAl2007a] – Christophe Jelger, Christian Tschudin, Stefan Schmid and Guy Leduc: *Basic Abstractions for an Autonomic Network Architecture.* In Proceedings of the 1st IEEE WoWMoM Workshop on Autonomic and Opportunistic Communications (AOC'07), Helsinki, Finland, June 2007.

[JenningsEtAl2007a] – Brendan Jennings, Sven van der Meer, Sasitharan Balasubramaniam, Dmitri Botvich, Mícheál Ó Foghlú and William Donnelly: *Towards Autonomic Management of Communications Networks.* IEEE Communications Magazine, **45**(10):112-121, October 2007.

[KumarAndVenkatara1997a] – G. Kumar and P. Venkatara: Artificial Intelligence Approaches to Network Management. Recent Advances and a Survey. Computer Communications, **20**(1):1313-1322, 1997.

[LeibnitzEtAl2006a] – K. Leibnitz, N. Wakamiya and M. Murata: Biologically Inspired Self-Adaptive Multi-Path Routing in Overlay Networks. Communications of the ACM, **49**(3), March 2006.

[MadeiraProject] – Madeira. http://www.celtic-madeira.org/index.html

[MartinFlatinEtAl1999a] – Jean-Philippe Martin-Flatin, Simon Znaty and Jean-Pierre Hubaux: *A Survey of Distributed Enterprise Network and Systems Management Paradigms.* Journal of Network and Systems Management, **7**(1):9-26, 1999. Springer.

[MasuokaEtAl2004a] – Masuoka, R., Labrou, Yannis, Parsia, B., Sirin, E., "Ontology-Enabled Pervasive Computing Applications", IEEE Intelligent Systems, Sept-Oct 2004, pp 68-72.

[Mathieu 07] – B. Mathieu et al. "Autonomic Management of Context-Aware Ambient Overlay Networks", IEEE ChinaCom 2007, China, Shanghai, 22-24 August 2007

[MeerEtAl2006a] – Sven van der Meer, Willie Donnelly, John Strassner, Brendan Jennings and Mícheál O Foghlú: *Emerging Principles of Autonomic Network Management.* 1st IEEE International Workshop on Modelling Autonomic Communications Environments, Dublin, Ireland, October 2006.

[MooreEtAl2001_Policy08] – Moore, B., Ellesson, E., Strassner, J., Westerinen, A., "Policy Core Information Model - Version 1 Specification", RFC3060, February 2001

[MortierAndKiciman2006a] – Richard Mortier and Emre Kiciman: *Autonomic Network Management: Some Pragmatic Considerations.* Proceedings of the 2006 SIGCOMM Workshop on Internet Network Management, pp. 89-93, Pisa, Italy, 2006.

[MurphyEtAl2001a] – S. Murphy, E. Lewis, R. Puga, R. Watson and R. Yee: Strong Security for Active Networks. IEEE OPENARCH 2001.

[NiebertEtAl2005a] – Norbert Niebert, Mikael Prytz, Andreas Schieder, Lars Eggert, Nick Papadoglou, Frank Pittmann and Christian Prehofer: *Ambient Networks: A Framework for Future Wireless Internetworking.* In Proceedings of the IEEE 61st Semiannual Vehicular Technology Conference (VTC 2005 Spring), Stockholm, Sweden, May/June 2005.

[Nunzi 07] – G. Nunzi, S. Schuetz, M. Brunner, "Design and Evaluation of Distributed Self-configuring Load-Balancing", 10th Symposium on Integrated Network Management, Munich, Germany, 21-25 May 2007

[Ohlman 06] – B. Ohlman, "Requirements for Policy Framework for Ambient Networks", Wireless World Research Forum- WWRF16, Shanghai, China, April 26-28, 2006

[Pavlou2007a] – George Pavlou: *On the Evolution of Management Approaches, Frameworks and Protocols: A Historical Perspective.* Journal on Network and Systems Management, **15**(4):425-445, December 2007. Springer.

[RFC1155] – Internet Engineering Task Force (IETF): *Structure and Identification of Management Information for TCP/IP-based Internets.* Request for Comments (RFC) 1155. May 1990.

[RFC1441] – Internet Engineering Task Force (IETF): *Introduction to Version 2 of the Internet-Standard Network Management Framework.* Request for Comments (RFC) 1441, April 1993.

[RFC2819] – Internet Engineering Task Force (IETF): Remote Network Monitoring Management Information Base. Request for Comments (RFC) 2819, May 2000.

[RFC3165] – Internet Engineering Task force (IETF): Definitions of Managed Objects for the Delegation of Management Scripts. Request for Comments (RFC) 3165, August 2001.

[RuizEtAl2003a] – Linnyer Beatrys Ruiz, José Marcos Nogueira and Antonio A. F. Loureiro: *MANNA: A Management Architecture for Wireless Sensor Networks.* IEEE Communications Magazine, **41**(2):116-125, February 2003.

[Sestinim2006a] – Fabrizio Sestinim: Situated and Autonomic Communication – an EC FET European Initiative. ACM SIGCOMM Communication Review, **36**(2):17-20, April 2006.

[Sloman1994a] – M. Sloman, "Policy Driven Management for Distributed Systems," J. Net. Sys. Mgmt., vol. 2, no. 4, Dec. 1994, pp. 333–60.

[Stallings1998a] – William Stallings: SNMPv3: A Security Enhancement for SNMP. IEEE Communications Surveys, Forth Quarter 2008.

[Strassner2004] – Policy01] Strassner, J., "Autonomic Networking - Theory and Practice", IEEE Tutorial, Dec 2004

[Strassner_Policy04] – Strassner, J. "Policy-Based Network Management", Morgan Kaufmann Publishers, ISBN 1-55860-859-1

[Strassner2005_Policy05] – J. Strassner, "Autonomics: A Critical and Innovative Component of Seamless Mobility", Motorola Technology Position Paper, 2005, http://www.motorola.com/mot/doc/5/5978_MotDoc.pdf

[Triole2004_Policy03] – "TRIOLE Executive Whitepaper", Edition 1, May 2004, www.fujitsu.com/downloads/TRIOLE/pdf/e_wpe.pdf

[WangEtAl2004a] – Wang, J., Jin, B., Li, J., "*An ontology-based publish/subscribe system*". In proceedings of the 5th ACM/IFIP/USENIX International Conference on Middleware, 2004.

[ZhangEtAl2003_Policy06] – W. Zhang, Y.S. Gan, K.J. Loh, K.C. Chua, "Policy-Based QoS Management Architecture in an Integrated UMTS and WLAN Environment", IEEE Communications Magazine, November 2003

[3GPP_Tech] – 3GPP Technical Specification Group Services and System Aspects; Earthquake and Tsunami Warning System Requirements and Solutions (ETWS); Solution Placeholder (Release 8) V0.1.0 (2008-01).

[3GPP_Policy10] – 3GPP TS 23.203, "Policy and charging control architecture", http://www.3gpp.org/ftp/Specs/archive/23_series/23.203/23203-800.zip

Glossary

The Terminology chapter contains acronyms and short definitions of the key concepts that are specific for the document. Common terminology will be available in a 4WARD Terminology document.

- **Autonomic management**

An autonomic management system is a system that exhibits self-* capabilities for the management tasks, including self-healing, self-optimisation, self-configuration, self-adaptation, etc.

- **Automated management**

Management tasks and the management control cycle are executed in an automated way, i.e., without human intervention. Automated management can be distributed or centralised. (Note that there is no general agreement in the research community about the distinction between automated and autonomic management.)

- **In-Network Management**

In-Network Management is a paradigm whereby management tasks are executed inside the managed system, i.e., inside the network. A characteristic is that nodes in the managed system (generally management processes in or close to network elements) interact with each other in a peer-to-peer fashion. In-Network Management enables “management by exception”, which means that outside management stations are contacted only if a exceptional (and rare) condition occurs in the network, and outside intervention is required.

- **Management plane**

An abstraction of management functionality in a network or system. In the case of In-Network Management, the management plane resides inside the managed system, which means it is realised as part of the network infrastructure. To enable In-Network Management in large network, the management plane must be self-organizing.

- **Management protocol**

In the traditional sense, a management protocol defines rules and data formats that allow management entities to interact in order to execute management tasks. A well-known management protocol is SNMP, which defines how management entities outside the network interact with agents inside the network elements. Traditionally management protocols rely on manager/managed roles. To realise In-Network Management, new types of management protocols are needed, which govern the interaction between management entities inside the network and are based on peer-to-peer paradigm. The core of such protocols are distributed algorithms that solve computational tasks, typically involving monitoring and control actions.

- **Management Policy**

A management policy expresses a set of rules that serve to govern the behaviour of the management plane in order to obtain some business or operational goals.

- **Distributed management**

With the management protocol exhibiting a peer-to-peer communications model the management plane can become transient in nature allowing when necessary a group of network infrastructure elements with similar In-Network Management capabilities and goals to connect with each other and directly access In-Network Management operations and data.

- **Scalable management system**

A management system is scalable if the performance objectives (such as overhead in terms of processing, or communication resources, or response time) for a specific management task

grows sub-linearly with system complexity metrics (such as system size, number of users, number of services, number of servers).

- **Real-time monitoring**

Real-time monitoring makes local state information from network devices available to management tasks inside or outside the management plane, at a time scale of a few seconds or sub-seconds. In the context of large networks, aggregation is a key (and non-trivial) monitoring technique, permitting to achieve scalability. To realise real-time monitoring for large-scale, dynamic networks, the monitoring task must be decentralised.

- **Situation Awareness**

Describes the knowledge and understanding about the current situation. It forms the basis for making sound decisions. Typically it consists of three steps. First critical factors in the environment which are relevant for the decision are perceived (Perception). Then it is inferred what those factors mean for the decision maker's goals (Inference). Based on the gathered information one then tries to predict what may happen in the near future (Prediction).