Architecture Requirements of the Future Internet

Invited Paper

Tapio Frantti
VTT Technical Research Centre of Finland
P.O. Box 1100
FI-90571 Oulu
FINLAND
tapio.frantti@vtt.fi

Jyrki Huusko
VTT Technical Research Centre of Finland
P.O. Box 1100
FI-90571 Oulu
FINLAND
jyrki.huusko@vtt.fi

Reijo Savola
VTT Technical Research Centre of Finland
P.O. Box 1100
FI-90571 Oulu
FINLAND
reijo.savola@vtt.fi

Ville Könönen
VTT Technical Research Centre of Finland
P.O. Box 1100
FI-90571 Oulu
FINLAND
ville.kononen@vtt.fi

ABSTRACT

The current Internet architecture curls around an original conversational model developed in the 1970's. New solutions were for a long-time built on that framework. However, the current architecture is not able to meet *optimally* challenges posed by new access technologies, applications and services any more. In this paper, the purpose is to bring a new clarity to the architectural issues of the Future Internet by abstract reasoning. The paper explains the importance of architecture and introduce an architecture gap (problems and bottlenecks) in the current Internet as well as some essential requirements for a new architecture. The choice of requirements set by emerging and new challenges may be the most critical issue determining the new architecture. Therefore, the development of the new architecture should be guided by an understanding of the requirements. On the basis of requirement analysis we also propose a new architecture framework, which aim is to provide greater functionality, lower costs and increased adaptability for different types of communication for the Future Internet.

Keywords

Future Internet, networking architecture, mobility, security, authentication

1. INTRODUCTION

After decades since its invention (see Fig. 1), new uses and abuses, are pushing the Internet into realms that its original design not anticipated. Long time continued freezing of the current architecture and developing overlay solutions for it may serve a short-term purposes, but may significantly impair the long-term flexibility of the Internet, too. The fact that in the past decades, we also have learnt a lot about networking and packet switching arises a question that 'is this the way we would design the Internet if we were to start it now?'. Accordingly, the research questions of the Future Internet can be stated as: 'Is it possible to change the Internet architecture in a planned way, so as to achieve a long-term goals?'

Generally the aim in the Future Internet research is to invent and demonstrate a global communications network and related services that will be qualitatively better than today's Internet[4],[5]. At the moment there are several ongoing Future Internet programs recently started in the US, Europe, and Asia like GENI (Global Environment for Network Innovations)[5] and FIND (Future Internet Network Design)[4] in US, NWGN (NeW Generation Network)[6] in Japan and some EU FP7 funded projects such as 4ward[1] and Trilogy[3] around the topic. GENI is an experimental facility being planned by the NSF (National Science Foundation), in collaboration with the research community. The research challenge is to understand how to design and build the Future Internet that achieves its potential. FIND is a major new long-term initiative of the NSF NETS research program. The aim of it is to research how would we reconceive tomorrow's global network today, if we could design it from scratch? NWGN is NICT's (National Institute of Information and communication Technology) new generation network project, which focuses on next generation network architecture issues. 4WARD is an example of EU FP7 IP projects which research, *e.g.*, new architecture and protocols for Future Internet.

Future Internet research also arises a new research 'philosophy'. Currently in the Internet research there are questions like: 'can X work over packet switched networks?' or 'can we transfer M/G/T bits/s to the end user?'. Instead newer questions are more like: 'can we make reliable network?', 'can non-technical users use it without developing amateur sys-admins skills? (auto/zeroconfiguration,

Mobimedia 2008 July 7-9, 2008, Oulu, Finland.
Copyright 2008 ICST ISBN 978-963-9799-25-7
DOI 10.4108/ICST.MOBIMEDIA2008.4073

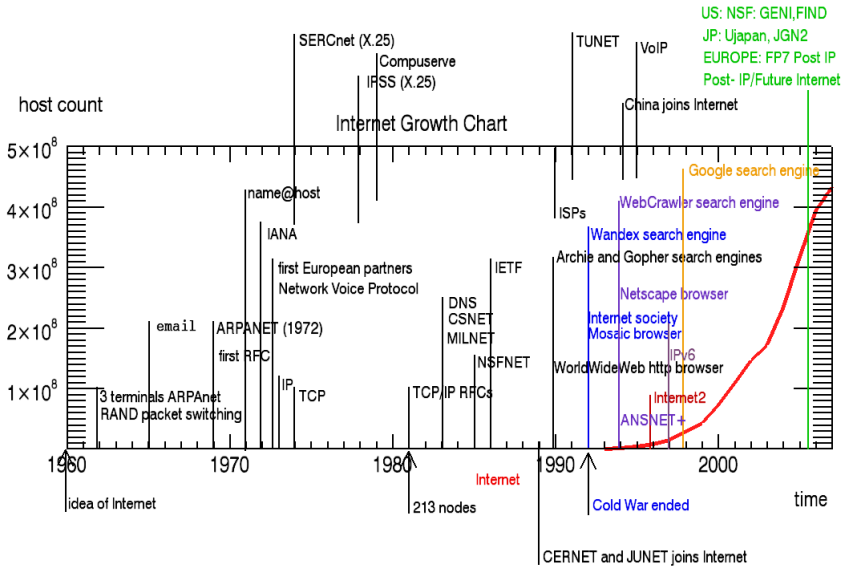

Figure 1: The Internet timeline from the idea to the beginning of the Future Internet programs.

autonomous computing, self-healing networks)' or 'can social and financial damage inflicted through networks be prevented (viruses, spam, identity theft, privacy violations)'?

In this paper, the purpose is to bring a new clarity to the architectural issues of the Internet by abstract reasoning. In Section 2 we present a literature review of the architecture research approaches. The Section 3 considers and analyses challenges of the Future Internet due to wireless access technologies, mobility, and new computing technology as well as challenges set by security, trust and privacy issues. In Section 4 it is presented architectural scenario of the Future Internet and outlined an architecture framework for the Future Internet. Section 5 discusses how Future Internet architecture framwork meets the challenges. Finally conclusions are drawn in Section 6.

2. LITERATURE REVIEW

The term *network architecture* is used to describe a set of abstract principles for technical design of protocols and communication mechanisms for computer networks. A computer network architecture presents a deliberate choices from many design alternatives, where these choices are informed by an understanding of the requirements. The purpose of the architecture is to provide a coherent and consistent decisions and to ensure that the requirements are met.[9]

Computer networking, on the other hand, is an engineering discipline concerned with communication between computer systems. Communicating computer systems constitute a computer network which generally involves devices capable of being networked and some of them also to relay information.

Many recent research efforts are trying to define new architectural principles that are more flexible, support cross-layer interaction and facilitate network as well as service composition. The planned architecture should meet the needs of an ever-expanding global network with a multitude of technologies used by billions of end terminals, and accessed a diverse range of applications and services each with its own unique mobility, QoS and security requirements.

In the current Internet architecture, it has been noticed that it is difficult to realize such network enhancements like IPv6, IPSec, MobileIP or multicast. In addition, the exponential growth of the Internet has shown its architectural deficiences such as support for seamless mobility, security vulnerabilities, address shortage, and lack of support for QoS to name a few. Even if a number of solutions have been proposed for these problems, they can be described only as a patchwork to fill architectural holes. Most of them have also come out in an uncoordinated fashion with the new problems of their own and similar functionality re-appearing over and over again in different protocols and layers. This kind of ad hoc problem solutions can even endanger the operations and performance of the whole system.

For instance, Network Address Translation (NAT) was proposed to resolve shortage of IPv4 addresses as well as some security issues but it also changed the original end-to-end architecture to the client-server architecture. In the end-to-end principle, protocol operations should be defined to occur at the end-points of a communications system instead of intermediate nodes (servers). End-to-end principle has been very essential to Internet architecture since its conception and has also led to the model of a minimal network with smart terminals.

IPSec was designed to secure IP datagrams and it has found widespread use. However, it is unsuitable with high user mobility due to constant re-establishment of IPSec tunnels. Mobile IPv6 has tried to address this problem by integrating IPSec procedures with the Binding Update process, but the approach is still clearly untenable in the long-run.

The role-based architecture proposes to get rid of the strict layering of protocols and replacing them with functional units (roles) organised arbitrarily for greater flexibility and richer interactions between protocols [8]. [8] refers to the notion of components (modular protocol units or ser-

vices) that can be flexibly composed according to the particular application and user requirements. The approach focuses on protocols and their component, but do not really consider an overall architecture. The recursive networking architecture [12] applies a generic meta-protocol to all layers to make cross-layer interactions cleaner and to avoid multiple instantiation of the same functionality at different layers. The metaprotocol is configured according to the individual requirements of the respective layer. In architectural work of FARA [10], the approach is also based on the layering principle and the main idea is to decouple end-system names from network addresses. The PlutArch proposal [11] facilitates inter-connectivity between networks which are based on different architectural principles using gatewaying functions. The Autonomic Network Architecture (ANA) project [2] also concentrates on an architecture that includes different types of networks with autonomic behaviour.

In the literature references mentioned above, the proposed architectures are rather generic and high-level without actually specifying how they could be used to realize a communication system. This motivates the need for defining an architectural framework that is generic and flexible enough to accommodate diverse networking architectures and at the same time has sufficient level of detail to make it usable for instantiating specific communication networks. In this paper, we bring a new clarity to the architectural issues of the Internet and explains the importance of architecture and introduce an architecture gap in the current Internet as well as some essential requirements for a new architecture. According to the requirement analysis we propose a new architecture framework, which aim is to provide greater functionality, lower costs and increased adaptability for different types of communication for the Future Internet.

3. CHALLENGES OF THE FUTURE INTERNET

Challenges underlying the original Internet include, for example, end-to-end acknowledgements, connectionless packet delivery, reliable transport service, universal interconnection, and network technology independece. Examples of emerging new challenges for the future networking are security, wireless access technologies and mobility, and new computing technology, see Table 1. Security is at the limit of its extensibility due to known vulnerabilities lurking in the Internet (DoS, worms, malware, spams). Wireless is starting to dominate in many forms and the Internet architecture should support flexible, efficient, and highly dynamic mobility. Nodes also must be able to change their attachment point to the Internet and applications must be able to discover and adapt to varying characteristics of wireless links. In the next 10 years with new computing technology most of the computers will be small sensors and actuators and it will be odd if Internet in 10 years does not take into account the needs of the majority of the computers then deployed. This also due to fact that the whole world is becoming networked (sensors, consumer electronic devices, embedded processors and other devices with limited computational and space resources), *i.e.*, 'Internet of Things' will emerge arising scale and diversity challenges.

3.1 Architectural challenges

The choice of requirements may be the most critical issue determining a new architecture and the development of an architecture should be guided by an understanding of the requirements. The Internet has imminent, medium and long–term architectural problems. Imminent architectural problems include, for example, spam, security, DDoS (Distributed Denial of Service), and applications deployment problems. Examples of medium–term architectural problems are congestion, routing, mobility, multihoming, and architectural ossification. Long–term problems are related to, *e.g.*, address space, how to connect billions of small devices together, and how to minimize redundancy in communication mechanims, see Table 2. In generally a network architecture should specify, *e.g.*,:

Table 1: Emerging new challenges for the future networking.

Challenge	Example challenge
Security	malware, spams
Wireless access technologies	local mobility
Mobility	seamless mobility
New computing technology	sensors, actuators
'Internet of Things'	network of consumer electronic devices

1. what entities are named
2. how to perform and inter-relate naming, addressing and routing functions
3. how communication functions are arranged to form protocols
4. how network resources are divided between flows
5. where security boundries are set and how they are enforced
6. how management boundries are drawn
7. how QoS issues are handled.

The original Internet architecture included also, *e.g.*, a connectionless packet-forwarding, least-common-denominator data delivery service at the network layer, and fixed-size numerical addresses with a simple hierarchy that are applied to physical network interfaces. The last one made possible to overload both naming and routing to a node, too. However, it is not straighforward to use an architecture to create technical design and such a mapping in a mechanical fashion is practically impossible. The architecture provides only a set of abstract principles against which each technical design decision can be checked, *i.e.*, architecture sets a sense of direction. It guides technical development such as protocol design in a consistent direction.

3.2 Architectural gap in the current Internet

A new architecture should provide greater functionality, lower costs and increased adaptability for different types of communication [7]. In a protocol design of the new architecture, the starting point and the main goal is to minimize the bottleneck effect of the current Internet at network layer as depicted in Fig. 2. The aim is that with well planned protocol design, different functionalities can be distributed into the system more efficiently and at the same time to minimize the redundancy in the whole communication chain.

Table 2: Architectural challenges for the future networking.

Short term challenge	Medium term challenge	Long term challenge
spam	congestion	address space
DDoS	routing	how to connect billions of devices together
application deployment	mobility	minimize redundancy in communication mechanims

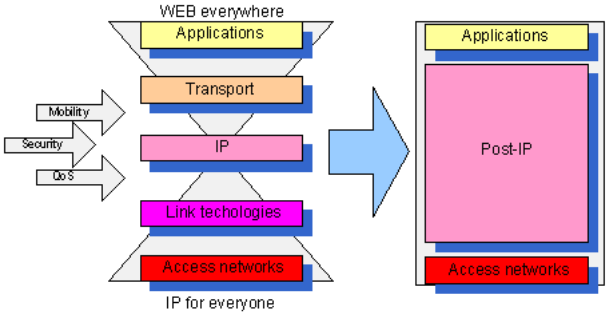

Figure 2: Bottleneck problem of the current Internet.

3.3 Security, privacy and trust

Security, privacy and trust issues sets own requirements for a new network architecture. This due to fact that security issues should be considered in the very early stages of technological development in order to be able to develop proactive architectural and system-level security solutions, see Table 3. On the other hand, a network architecture sets a sense of direction for security, privacy and trust design solutions, which can be seen as main enablers for the Future Internet and the future applications. Services also play an important role in defining the security, trust and privacy requirements of the Future Internet. It can be seen from the history of technological development that communication networks and devices are often re-used for purposes for which they were not originally developed, causing major security problems in many cases. The basis of current Internet itself is another example of this kind of lack of clear view of the future use scenarios during the original architectural design when security was not seen as the primary design objective. Consequently, a number of factors in the current security environment of the Internet provide would-be attackers with significant advantages over security solutions. An attacker needs to find only a single vulnerability whereas the defenders must try to eliminate all vulnerabilities. Powerful attack tools, including automated tools for malicious actions, are now freely available for downloading over the Internet by anyone who wants them, and little skill is required to use them. The resources - including training and equipment - needed to launch potentially harmful attacks are not only readily available but relatively inexpensive compared to the costs of securing systems, networks and information and, responding to attacks.

Moreover, in present system solutions, authorization decisions are made usually depending on user needs. The increasing complexity of Internet together with the increased need of context-awareness and adaptability will make hierarchical role-based authorization more popular. The roles can be 'hard coded' in the functionality to the Future Internet architecture.

Currently, also the biggest botnets in Internet might have hundreds of thousands if not millions of nodes. As the quality of malware implementation will continue to increase, it will become more and more silent and deadly. The Future Internet should have enough countermeasures for botnets and other kinds of sophisticated malware 'hard coded' to the architectural choices.

3.4 From 'Connectivity by Default' to Publish-Subscribe?

In the design of the Future Internet, one must consider changing the original 'Connectivity by Default' paradigm to a more controlled form of connectivity. The default connectivity is causing a lot of security breaches of today such as several denial of service (DoS) attacks and has implied to the use of firewalls. One possible direction would be to design connectivity to publish-subscribe paradigm. The design of architecture for Future Internet should ensure that reactive secure solutions such as firewalls would not be needed anymore.

3.5 From authenticity of addresses to authenticity of content

Physical addressing (like IP addresses) will not have so important role in the architecture of Future Internet. More and more of the content will be available using peer-to-peer communication and the actual physical location of the data is not important. However, authenticity of the content will play a major role. Therefore, several relevant research questions arise in this context such as 'Where should the authentication take place?' and 'Should Digital Right Management (DRM) support be included in the authentication process?'.

3.5.1 Location of the authentication module

Relations between subscribers and publisher can be either long-term or short-term. As an example, consider a relationship between a newspaper publisher and its subscriber. The customer relationship is usually quite a long-term in its nature whereas the actual content of the product, *i.e.*, a newspaper is consumed only once. Different validity periods of the authentication keys lead to challenging key management issues. For some application, a local key management system is adequate whereas for some other application the global system is more suitable.

3.5.2 Communication peer identification vs. content authentication

Content authentication has its own technical challenges for the new architecture. For example, frequently changing content set special requirements for the authentication system. Fundamentally, necessity of the content authentication depends on the nature of the content. For several applications, only provider (publisher) authentication is enough. Therefore, it should be clarified if such authentication is actually needed in the design of communication system or is

the external system enough.

3.5.3 *Digital rights management*

Some of the content, *e.g.*, multimedia streams, are commercial and rights for their usage are usually granted by the publisher. However, Digital Right Management systems should be implemented on the lowest possible level of the communication systems for achieving the best possible security. The co-operation between communication system specific DRM and the whole system level DRM should be clarified for the new network architecture.

3.6 Ubiquitous computing and communication peer identity

As we progress, step by step, towards the Ubiquitous Computing Age, we will have more and more infrastructureless, mobile and dynamic networks. There are huge challenges for identity management in this kind of usage environment of the current and Future Internet, *e.g.*, critical applications such as payment services will be used routinely. Currently, there are no good solutions for the identity management in this mixture of computation, communication and peer-to-peer activity. One possible solution might be to use a new kind of 'mini' Certificate Authorities for identification services. Combining mobility and identity management brings challenges for the design of communication mechanisms, too. Use of 'universal' identifiers will be encouraged in the future, and a paradigm shift from device authentication to user authentication is needed to take into account in a new network architecture.

Together with the increase of peer-to-peer and infrastructureless communication solutions, it becomes more and more important to trust the communication peers, devices and networks. Automated and certificate mechanisms are needed in the Future Internet to ensure the trust.

3.7 User privacy

The Internet already stores a lot of information on individuals. The architectural solutions in the Future Internet should guarantee enough user privacy. Special mechanisms should be developed to combat unauthorized publication of private information in the Internet.

Table 3: Security challenges for the future networking.

Proactive system-level security solutions
Publish-subscribe paradigm
Authencity of the data content and provider
Key management systems
Digital right management
Identity management
User authentication
User privacy guarantee
Automated and certificate mechanism for trust
Countermeasures for botnets
Hierarchical role-base authorization

4. ARCHITECTURE FRAMEWORK OF THE FUTURE INTERNET

In the next generation Internet, importance of the just-in-time service provisioning increases. It is foreseen that for instant service provisioning with guaranteed QoS (Quality of Service) and QoE (Quality of Experience) the protocols and communication mechanisms, *i.e.*, architecture should be well designed and optimized, see Table 4.

Currently, *e.g.*, multimedia delivery and mobility management mechanisms need to rely on cross-layer communication with inherent deficiencies for the improvements. At the same time new middleware functionalities are introduced to improve, for example, security and communication reliability, which implies increased complexity on cross-layer information controllers and managers, and protocol communication and hierarchies. However, information needs to be transferred also through the network, not only inside the protocol stack, expanding the overhead of communication dramatically, which gives way for the new protocol architecture framework solution (see Fig. 3).

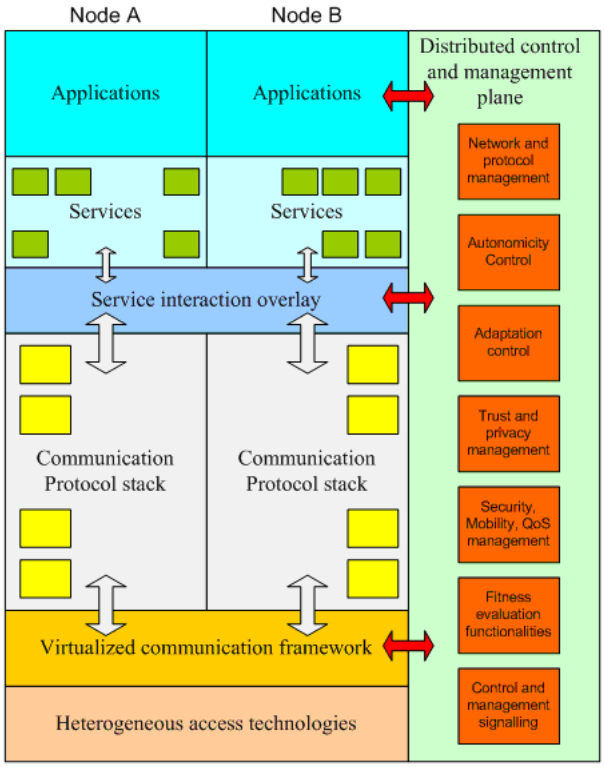

Figure 3: New protocol architecture framework.

The proposed architecture framework illustrates the basic elements for the communication architecture for Future Internet. It utilizes the virtualization of the access technologies in order to provide seamless network connectivity, and the application/service interaction overlay to fulfill the communication requirements for information dissemination in the network. In order to provide system level adaptation and dynamic protocol configuration in the management and control plane, the communication protocol stack benefits from the dynamic management and control functionalities through the communication framework and interaction overlay (dark arrows in the Figure 3). Distributed control and management plane is designed to fultill the requirements set for the architecture in the Tables 1-3. The Table 4 presents the properties of the architecture framework.

The interaction overlay fulfills, *e.g.*, the requirements of

information dissemination and the virtualized communication framework provides the required functionalities for multi-access. New protocol architecture enables overall improvement of the scalability, minimization of the redundancy in a protocol stack and real-time control signalling for emerging needs. The presented approach with inherent real-time signalling entities in control and management signaling plane enables instant connection establishment and optimized just-in-time type service provisioning. Real-time signalling here means that control information is transmitted, if necessary, at once even one control bit a time (without conventionally collecting a bunch of them before transmission) for immediate actions in the communication system.

Table 4: Properties of the future networking architecture framework.

Just-in-Time (JIT) service provisioning
QoS
QoE
Virtualized access technologies for seamless network connectivity
Application/service interaction overlay
System level adaptation
Dynamic protocol configuration
Dynamic control and management functions
Real-time control signalling

5. DISCUSSIONS

The development of an architecture for the Future Internet should be guided by an understanding of requirements. Generally set of challenges of the Future Internet due to wireless access technologies, mobility, and new computing technology as well as challenges set by security, trust and privacy issues. Especially, security is at the limit of its extensibility due to such vulnerabilities as DoS, worms, malware, and spams. The connectivity is also causing a lot of security breaches of today which give a way for a different types of connectivity directions like publish-subscribe paradigm. These due to fact that security issues should be considered already in the architecture development in order to be able to develop proactive system-level security solutions. In addition, the fact that whole world is becoming networked ('Internet of Things') will emerge arising scale, identification, authorization and diversity challenges. Other examples of architectural problems are congestion, routing, mobility, multihoming, architectural ossification, problems related to address space and how to connect billions of small devices together. A new architecture should also provide greater functionality, lower costs, minimize redundancy, enable instant connection establishment and optimized just-in-time type service provisioning and increase adaptability for different types of communication. It should also take into the consideration different validity periods of the authentication keys, which lead to challenging key management issues. In future networks amount of content also increases and the authenticity of the content will play a major role instead of the physical location of data. The co-operation between communication system specific DRM and the whole system level DRM should also be clarified for the new network architecture.

It is not straighforward to mechanically map requirements to architecture design likewise it is not straighforward to use an architecture to create technical design. The architecture guides technical development such as protocol design in a consistent direction but it provides only a set of abstract principles against which each technical design decision can be checked.

Properties of the future networking architecture framework are represented in Table 5. Reliability can be defined as the ability of a network to maintain or restore an acceptable level of performance. Therefore, the presented solution should include sufficient QoS/QoE provisioning. Autoconfiguration can roughly bethough to be network's ability to configure itself without user intervention. The presented solution should have functions for autoconfiguration in various places. The architecture framework should include autoconfiguration management functionalities. The communication networks should be able to recover (self-healing) itself from network or system failures. Damage prevention is closely related to the self-healing. Security, such as authentication, privacy, and trust functionalities should be build-in features in the model. Dynamic protocol model provides suitable ways to handle varying traffic conditions in an effective way (congestion control). Due to the dynamic nature of the protocol model, it is suitable for handling mobility issues such as routing. Several connections can be attached to a service in the proposed model for implementing multihoming service. Proposed system does not fix the address space and therefore several possible protocols can be used, *e.g.*, IPv6. Signaling inside and between layers is inherently compatible for wireless access.

6. CONCLUSIONS

In this paper we discussed the underlying challenges of the original Internet and presented one possible architecture framework model as an abstract level solution. Advantages of the proposed approach are build-in cross-layer information delivery, build-in network security properties and less amount and real-time delivery of control information. Disadvantages includes more complicated implementation especially for small-scale devices.

Future Internet research arise a new kind of philosophy with new kind of research questions such as 'can we make reliable network?'. According to the new philophy we presented challenges in the present Internet architecture and the means how the Future Internet meets these challenges. the proposed framework solution solves the main challenges in a very high abstraction level. In future research we will model our architecture framework solution in NS-2 simulation environment for more concrete solution.

7. REFERENCES

[1] 4ward project page. http://www.4ward-project.eu.
[2] Autonomic network architecture project web page. http://www.ana-project.org.
[3] Eu fp7 ist trilogy project. http://www.trilogy-project.org.
[4] Find project web page. http://www.nets-find.net/.
[5] Geni project web page. http://www.geni.net.
[6] Nict's nwgn projects. http://akari-project.nict.go.jp/document/INFOCOM2007.pdf.
[7] R. Braden, D. Clark, S. Shenker, and J. Wroclawski. Developing a next-generation internet architecture.

Table 5: Challenges in the Internet architecture with the desciption how the Future Internet Protocol model meets these challenges.

Reliability	QoS/QoE provisioning.
Autoconfiguration	Distributed functionality inside the protocol model.
Self-healing and damage prevention	Functionalities can be replicated inside the system in the case of damage.
Autonomous computing	Protocol components are autonomous units, which support autonomous services.
Security issues	Management system includes authentication, privacy and trust functionalities.
Congestion	Dynamic protocol model is able to meet requirements of variable conditions.
Routing	Dynamic protocol model and signalling support routing in mobile and volatile environments.
Mobility	Dynamic nature of the protocol model supports inherently mobility issues.
Multihoming	Components can be added dynamically to support multiple connections.
Address space	Proposed system does not dictate physical address space. Several protocols can be used.
Wireless access	Inter- and intralayer signalling is compatible for wireless access.

Internal Whitepaper, MIT Laboratory for Computer Science, 2000.

[8] R. Braden, T. Faber, and M. Handley. From protocol stack to protocol heap: role-based architecture. *ACM SIGCOMM Computer Communication Review*, 35(1), 2003.

[9] V. Cerf and R. Kahn. A protocol for packet network intercommunication. *IEEE Trans on Comm*, Com-22(5):637–648, 1974.

[10] D. Clark, R. Braden, A. Falk, and V. Pingali. Fara: Reorganizing the addressing architecture. In *Proceedings of the ACM SIGCOMM workshop on Future directions in network architecture*, 2003.

[11] J. Crowcroft, S. Hand, R. Mortier, T. Roscoe, and A. Warfield. Plutarch: An argument for network pluralism. In *Proc. of the Workshop on Future Directions in Network Architecture (FDNA) at ACM SIGCOMM 2003*, 2003.

[12] J. Touch, Y. Wang, and V. Pingali. A recursive network architecture. Technical Report ISI-TR-2006-626, ISI Technical Report ISI-TR-2006-626, December 2006.