Requirements For Future Internet Architecture

(draft-FIA-Requirements-r.0.6.3)

December 2011

Editor: TaeWan You, ETRI {twyou _at_ etri.re.kr}

Summary

This document describes fundamental requirements and principles for Future Internet Architecture (FIA) developed by Architecture Working Group (AWG) of Future Internet Forum (FIF). This document includes various requirements and design principles for FIA from several technical perspectives. Also, general requirements and principles are developed based on them. Finally, the document provides the recommendation for Future Internet Research.

Contributors

Name	Affiliation	Contact	Contributions
Woojik Chun	ETRI	wjchun_at_etri.re.kr	Requirements and Principles
SeokJoo Koh	KNU	sjkoh_at_knu.ac.kr	Technical Requirements – Mobile perspective
MyeongWuk Jang	SAIT	myeong.jang_at_samsung.com	Technical Requirements – Content-centric perspective
TaeKyoung Kwon	SNU	tkkwon_at_snu.ac.kr	Technical Requirements – Mapping system perspective
SangJin Jeong	ETRI	sjjeong_at_etri.re.kr	Technical Requirements – Green networking perspective
SangWoo Lee	ETRI	ttomlee_at_etri.re.kr	Technical Requirements – Security perspective
HeeYoung Jung	ETRI	hyjung_at_etri.re.kr	Overall
Antonio Marcos Alberti	INATEL, Brazil	Antonioalberti_at_inatel.br	Overall

TABLE OF CONTENTS

[Editor's Note: the document is still in draft version, so many parts of texts are tentative. whole texts may be revised by further contributions]

1. INTRODUCTION

The Internet has been working for longer than 40 years successfully without major change of the architecture. However, the great success of the Internet has faced many challenges including technical and non-technical issues. Network links became almost a million times faster than earlier and wireless are more common technology of the Internet. It will be anticipating that the number of Internet nodes has been increased tremendously to more than 100 billion, and new applications and services have emerged by responding to user's new demands. Around each person there are about 3000-5000 objects [38]. The total connected objects would be up to 100 trillion, and current internet architecture is not able support all objects. Therefore lots of world-wide activities are going on to address the limitations of current Internet and to build a Future Internet Architecture [35] [36]. Hence, in recent years several research communities are addressing the fundamental limitations of the current Internet and its architecture. Future Internet must be carefully designed that must be flexibly to adapt the continuous changing in networks. The Future Internet (FI) is expected to be a holistic communication and information exchange ecosystem, which will interface, interconnect, integrate and expand today's Internet, public and private intranets and networks of any type and scale, in order to provide efficiency, transparency, interoperability, flexibly, time saving and security services to humans and systems, while still allowing for tussles among the various stakeholders without restricting considerably their choices.

Recently, several research organizations have devoted to define future internet architecture. Some of them are significantly mentioned in this draft such as FIA in USA [8], NetSE in USA [9], FIND in USA [10],GENI in USA [11], AKARI in Japan [12], Future Internet in Korea[13]. However, in Europe, a significant part of the Information and Communication Technology (ICT) of the Framework Program-7 has been devoted to the Future Internet [14] starting in 2006 with the EIFFEL initiative [52]. Meanwhile, there is several large/integrated and small/targeted research projects are already running and early results have been published.

FIF AWG believes that the first step to develop Future Internet Architecture (FIA) should be the establishment of appropriate requirements and/or principles. In the context, FIF AWG develops the requirements and principles for the design of FIA by considering various technical perspectives.

This document describes the requirements and principles for the Future Internet Architecture. The document composes three parts. Firstly, the document addresses technical requirements and principles by gathering various requirements from specific technical perspectives. Secondly, general requirements and principles for FIA are drawn by extracting some common features from these technical requirements and principles. Finally the document will suggest some recommendations for the research on FIA.

1.1 Scope

The scope of this document includes the following items:

- Collect various requirements and principles from several technical perspectives.
- Identify general requirements and principles based on considering the collected requirements and principles.
- Provide the recommendation for FIA Research

2. DEFINITIONS AND ABBREVIATIONS

2.1 Terms and Definitions

2.1.1 ARCHITECTURE

It is a set of functions, states, and objects/information together with their behaviour, structure, composition, relationships and spatial-temporal distribution. The specification of the associated functional, object/informational and state models leads to an architectural model comprising a set of components (i.e. procedures, data structures, state machines) and the characterization of their interactions (i.e. messages, calls, events, etc.) [36]

2.1.2 REQUIREMENT

It is an outlined indispensable conditions and terms such as Objectives and goals. Which is determined a specific need that any stakeholders of the Future Internet wish to achieve. We have considered six general terms that should be satisfied in the Future Internet architecture. These terms are discussed in Section 3.1.

2.1.3 PRINCIPLES

It is involved in determining the fundamental of network topology, routing mechanism cost of transmission, and time invariant laws underlying the working of an engineered artefact. It's resolving the size of the components used and suggests normative rules to design Future Internet architecture (FIA).There are several general principles that need to consider additional improvement of FIA designing. These terms are discussed in Section 3.2.

2.1.4 FRAMEWORK

It provides an innovative conceptual model of the architectural process and diversity to obtain an entire operation in the architecture which is defined under the guideline of the principles but not mandate. Framework utilizes hot spots according to the specific needs and requirements of the system architecture. Hence, it is always flexible for further extension.

2.2 Abbreviation and acronyms

AWG	FIF Architecture Working Group
FIF	Future Internet Forum in Korea
FIA	Future Internet Architecture
ISP	Service Provider
CP	Content Provider
Telco	Telecommunication Corporation
IPTV	Internet Protocol Television
DDoS	Distributed Denial of Services
QoS	Quality of Service
HTTP	Hypertext Transfer Protocol
MIP	Mobile IP
HA	Home Agent
LMA	Local Mobility Anchor
PMIP	Proxy MIP
DTN	Delay Tolerant Network
LM	Location Management
ID	Identifier
LOC	Locator
CDN	Content Delivery Network
FIB	Forwarding Information Base
DNS	Domain Name System
DNSSEC	DNS Security Extensions
PKI	Public Key Infrastructure
DHT	Distributed Hash Table
GHG	Greenhouse Gas

EU	European Union
GPS	Global Positioning System

3. REQUIREMENTS AND PRINCIPLES

[Editor's Note: The clause contains tentative contexts, text may be revised by further contributions]

Over the last few years no. of internet users/services are exponential increasing and the size of the Internet capabilities are presumably saturating. In the internet of the future, there will be far more devices, a lot more computing on the go, and many new applications with compared to the Internet of today. To prepare for a far more versatile future Internet, our goals are focused around Scalable, Secure, Sensitive, Seamless, Sustainable and Smart in a unified global communications network. As we know the goal of the original Internet architecture was to develop an effective technique for multiplexed utilization of existing interconnected networks. Therefore, in any case we need to expend the size and capability of the current internet so internet will never be comprised of a single network technology. The internet architecture needs to be able scale for that we need to combined public and private networks. The goal of the original Internet architecture was to develop an effective technique for multiplexed utilization of existing interconnected networks [44]. The future internet architecture require with several fundamental detailed such as FI must support multiple types of communication services, accommodate variety of networks, continue despite loss of networks or gateways, permit distributed management of its resources, permit host attachment with a low level of effort, accountable and cost effective. The requirements of the FIA can be satisfied neither at the same time nor with the same significance selection by the present Internet architecture.

3.1 General Requirements

The current Internet architecture was designed for static and well-managed flat network topology to support packet switching, layering, collaborating networks, intelligent end-systems and end-to-end argument. As Internet evolved from a small research network to a worldwide information network as a growing diversity of commercial, social, ethnic, and governmental interests led to increasingly conflicting requirements among the competing stakeholders. Therefore, the improvement of current internet, we should redefine internet requirements with respect to new applications and technologies as well as various interrelated

perspectives such as networks and infrastructure perspective, services perspective and media and information perspective. To prepare for a far more versatile future Internet, our goals are focused around six S folds such as Scalable, Secure, Sensitive, Seamless, Sustainable and Smart in the development of a unified global communications network. We have explained in brief about six "S" into the following subsections.

3.1.1 SCALABLE

Many limitations of the current Internet are originated by excessive growth of the Internet in terms of bandwidth, number of hosts and users, and volume of contents. The well-known “IPv4 address deficiency problem” is a typical example of the scalability issues. As the Internet grows in the number of users and its application area, the scalability issue becomes more serious. The future Internet has to be flexible enough to cope with potential growth of the number of users, contents, services, and devices as well as explosive growth of traffic. The now-trendy concept of Big Data usually implies ever-growing hordes of data, including unstructured info posted on Facebook and Twitter, and ways of gleaning intelligence from all of it to create business opportunities. The concept, however, also carries with it risks for anyone opening up about themselves on the Internet and raises questions about how to handle this big data in the future Internet in scalable ways. Hence, It is the ability of a network (hardware or software) to continue to function well when it (or its context) is changed in size or volume in order to meet a user need or rescale in a larger size of networks.

3.1.2 SEAMLESS

The Future Internet is needed to provide consistent access mechanism to support diverse network and communication paths on the different administration domains, mobility through even heterogeneous networks. In order to provide seamless network access services to the communicating entity, including users, devices, data, and applications. The following terms are considering in the development of seamless system to support upcoming technologies.

- **Mobility**: In the present scenario of the Internet technology, If an IP host is mobile, then its IP-address will be broken whenever it switches to a new IP subnet. The FI should support the mobility of IP hosts without breaking end-to-end connectivity. Hence, for FIA, we should consider seamless mobility where ID and Locator are separate to support heterogeneous wireless networks, Multi-homing hosts, mobility control, data delivery and protocol separation of data delivery.

-

- **Distribution of processing, storage, and control functionality and autonomy** (organic deployment): These are addressed by current architecture (concerning storage and processing several architectural enhancements might be required e.g. for the integration of distributed but heterogeneous data and processes).

- **Transparency** is only concerned with the end-to-end service between the terminal/host. In the current Internet service is the connectivity when the notion of "service" is not embedded in the architectural model of the Internet.

3.1.3 SENSITIVE

The Future Internet pursues integration of not only traditional wired and wireless networks but also easily support various new types of networks such as sensor, service and content aware, social networks. The designing of FIA, we should sense that what might be important to develop for sensitive network environment to support multiple data traffic, real-time streaming in an independent entity. Sensitivity is the ability of a test to correctly identify the ability of networks which is sensitively support following issues in a particular domain that are easily fixed with a particular technique.

- **Context Sensitive** is circumstance of network in a sensitive manner through careful planning, consideration of different perspectives, and tailoring designs to particular network setting. Context sensitive uses a collaborative interdisciplinary approach that includes early involvement of key stakeholders to ensure that transportation projects are not only “moving safely and efficiently,” but are also in harmony with the natural, social, economic, and cultural environment.

- **Content-Sensitivity** is a networking process that has to process data at various node of a network. These nodes cooperate with each other to satisfy requests for content by end users, transparently moving content to optimize the delivery process. Content-sensitive can take the form of reducing bandwidth costs, improving end-user performance or increasing global availability of content. Hence, content-sensitivity classification should be based on security of the relevant data to the lifecycle for a specific domain. The relevant content processing facilities are depending the requirement of the users.

- **Time-Sensitivity** is tuning of the minor software/hardware system component which is high-precision timing for packet injections into the network, or require packet level traffic measurements with accurate timing by alleviated. However, creating a large number of connections, in order to model traffic in networks closer to the core of the

Internet, with thousands of flows sharing each link, is not a trivial task. The difficulty of such modelling becomes even more obvious when one desires to capture the heterogeneity in link capacities, with only a limited number of physical machines [5].

- **Power-Sensitive** is the fundamentally important especially to the operation of wireless communication and quality of services maintenance. To design FIA, we should be kept power sensitive network architecture to minimize power consumption and prolong battery life of wireless network. That would be good to mitigate interference and increase network capacity. Moreover, by controlling its transmitter power each link can autonomously probe (interact with) the rest of the network and observe its collective reaction by monitoring the interference induced on its receiver such as admission control, channel selection and switching, and handoff control.

- **Genericity** is addressing to support multiple data traffic such as non/real-time streams, messages, contents etc., independently. That is reinforced to migration of mobile network to IPv6 Internet, IPTV moving to Internet TV, etc. otherwise leading to segmentation and specialization per application/service. It is the shared infrastructure partitioning/divisions, which is independently support to the host/terminal.

3.1.4 SECURE

One of the fatal problems in the current Internet is lack of security features. For strengthening the security capability some encryption mechanisms, such as IPsec and sHTTP, are patched. However, those can only protect content privacy but cannot solve network related security issues such as DDoS (Distributed Denial of Services). Thus, security must be considered form the early stage of the Future Internet architecture design. Since how secure communications must be kept is dependent on the how much they trust peers and communication environment, security and trustworthy are two sides of the same coin in the development of FIA. We should consider following terms during the development of a secure FIA.

- **Accountability** is the involvement of used resources and security without impeding user privacy, utility and self-arbitration that should be held responsible for its own specific actions. Once the entity process has passed and later traceable execution process on entity so that the causes are accountability which is determined afterwards.

- **Reliability** is the capacity of the Internet to perform in accordance to what it is expected to deliver to the end-user/hosts while coping with a growing number of

users with increasing heterogeneity in applicative communication needs. Hence, it the ability of a system or component to perform its required functions under stated conditions for a specified period of time.

- **Robustness/stability, resiliency, and survivability** are especially suitable for interplay and dynamic behaviour of a definite organizational architecture. It is quantifiable behaviour of a system, which is remaining close to original state after small perturbations. Hence, global dependability and security framework of the network are needed for resilience, self-healing, and dynamic content and volatile environments. The immense systems of ever-evolving networks of computers and mobile devices. Which are needed to support and provide Ambient Intelligence? That has the necessary resilience and survivability, despite any residual development and physical faults, interaction mistakes, or malicious attacks and disruptions [21].
- **Security and Trustworthy** is highly desirable computing systems that are inherently secure, available, reliable and authenticity of all traffic into the internet carriers. Trustworthy computing has to meet trust from user's point of view. There are few basic key questions such as is the technology there when I need it? Does it keep my confidential information safe? Does it do what it's supposed to do? And do the network who server and user the business that provides it always do the right thing? However, the more works on this requirement has discussed in Security WG.

3.1.5 SMART

One of the well-known principles of the current Internet is the “end-to-end” principle, where most of intelligent functions have to be deployed in end systems while keeping networks as simple and dummy as possible. This principle has contributed for graceful evolution of the Internet. However, diverge and differentiated applications of the Future Internet would require much sophisticated management over the communication infra. That is, a network itself should perform its role intelligently by classifying the traffics, prioritizing requirements, and allocating resources, and also it must be equipped with advanced management capability such as self-configure, self-healing, self-adjust, etc. Smart network means autonomous distributed system which is automatic capable of auto restoration to construct a network. To support an automatic restoration, we should follow the following points in the development of smart networks.

- **Proactive service and support** uses several mechanism and processes to get information about network before its routing process. These mechanism and processes are varying for best support to each and every single network.
- **Manageability (distributed, automated, and autonomic operation)** is a self-managing system (software or hardware component) that is autonomously tries to keep its parameters within a desired range and follow high-level policies such as

configuration, discovery, monitoring and proactive identification to overcome the rapidly growing complexity of computing systems management.

- **Autonomous** is the unit of route policy, either a single network or a group of networks that is control by a common network administrator on behalf of a single administrative entity. An autonomous system is also sometimes referred to as a routing domain and assigned a globally unique number. Therefore, an autonomous system shares routing information with other autonomous systems using the Border Gateway Protocol (BGP) and networks within an autonomous system communicate routing information to each other using an Interior Gateway Protocol (IGP).
- **Ability of Diagnosis (root cause detection and analysis)** is detrimental to corporation between internet users and providers. The Internet does not allow hosts to diagnose potential problems. The network offers little feedback for hosts to perform root cause discovery and analysis.

3.1.6 SUSTAINABLE

The primary reason why the Future Internet must be considered in the clean-slate manner is that the original principles of the current internet can no more satisfy newly arisen requirements. So the architecture for the Future Internet must be flexible enough to fulfil the requirements to be appeared as well as already identified. Also, it must be evolvable to accept new technologies and applications without interference among existing services. To design a sustainable system, we must need to support following terms.

- **Flexibility** (capacity to adapt/react in a timely and cost-effective manner when internal or external events occur that affect its value delivery) is the ability of a system to respond to uncertainty in a manner such as potential internal or external changes in a time and cost effective manner. Uncertainty can create both risks and opportunities in a system, and it is with the existence of uncertainty that flexibility becomes valuable.

- **Evolvability** (of time variant components) is an evolution to enhance their ability to discover effective adaptations and frequency of genetic variation to enhance its evolvability. It is the ability to accurately reproduce the best genetic arrangements that have been discovered in the past, and the ability to discover new and better genetic arrangements through the testing of variants by trial and error.

- **Energy efficiency** is the increasing demand of improving efficiency of network and reducing the energy consumption and greenhouse gas emissions. In order to meet the demand, FIA should provide a way to reduce energy required to carry out a given task while maintaining the same level of performance.

- **Virtualization** : A promising technology to reduce energy consumption is the virtualization of substrate resources to enable secure sharing of powered-on resources. It enables dynamic sharing of virtualized resources to reduce energy consumption. The aim is to self-adjust required resources accordingly to variations on service and applications usage.

3.2 Architectural Principles

[Editor's Note: The whole parts of text are still tentative, it may be revised by further contributions]

This clause describes desirable alternatives and additional improvement of the current architectural improvement components. FIA will be a convergence of wired and wireless networks technologies that can consist billions of networking devices with different networking interfaces. As we know, the current internet principals are based on layering, network collaborating, packet switching, connectionless network, end-to-end principles and connection oriented transport but it has to support mobility, multi-homing, privacy, path preference selection, etc., which should be resolved in FIA. The principals of FIA are directly derived from the design requirements such as social, economic and policy forces rather than technological aspects. The FIA is often to adapt the most significant global challenges in a holistic way. We need to consider following points into the development of FIA.

3.2.1 KEEP IT AS SIMPLE AS POSSIBLE

Future Internet should support large-scale interoperability for that KISP (Keep It as Simple as Possible) principle should follow which is based on famous quote by Albert Einstein: "Make everything as simple as possible, but not simpler". But sometimes complex problems require complex solutions and the FI will be providing non-trivial functionality in many respects. Therefore, designers should keep in mind when selecting from among many technologies and integrating them in order to enable diverse uses, simplification is the most important principle Because complex systems are generally more difficult to manage and less reliable since more things can go wrong at any given time. The guiding principles of the current Internet architecture policy would be continue and consider following terms into account when designing the FIA [7].

- **Simplicity and cost-effectiveness**: more data is needed but simplicity seems to be progressively decreasing. Note that simplicity is explicitly added as design objective to -at least- prevent further deterioration of the complexity of current architecture

(following the "Occam's razor principle" key design principle). Indeed, lowering complexity for the same level of performance and functionality at a given cost is key objective.

- **Globally Unique Identification** is a distributed system with a unique reference number without significant of central coordination across space and time. The connectivity between two nodes have established on basis of node ID that should be globally unique and fixed in the network. The size of the ID (identifier) and propagation process must be sufficiently improbable in practice. Therefore, ID can be used to reliably identifying for multiple purposes.

- **ID-based bus** is the better option to support network access and control. ID-based Bus technique doesn't need mapping services during the communication (packet is transferring) between two entities. A globally unique ID is distributed to all communication entities (host, services, and contents) that are plug into the network Bus to provide well-defined interface. In this case ID's are location independent but ID must be bounded to the location to ID management. Hence, the management of the global ID we need to design well-structured network architecture because if there are no structures than the ID explosion chances are very high. ID-based Bus techniques has provide well-defined interface to reduce the issues of scalability and network performance.

-

3.2.2 POLYMORPHIC NETWORKS

In contrast of current Internet their all devices are fitted in same protocol suite but the future Internet should be polymorphic where one could implement, and deploy its new network protocols or cooperation schemes without disturbing other working protocols. Therefore, heterogeneous communication paradigms can be accommodated into the same framework without rising routing and addressing to the application such as peer-to-peer networks, overlay networks, VPN, spontaneous networks. The following network architectures are applicable to support polymorphic network into the FIA development.

- **Heterogeneous network** is typically composed of multiple architectures and communication technologies. It offers wide variety of communication and coverage in the environment such as wireless network which provides a service through a wireless LAN and is able to maintain the service when switching to a cellular network.

- **Network virtualization** is a method of combining the available resources in a network by splitting up the available bandwidth into channels, each of which is independent from the others, and each of which can be assigned (or reassigned) to a particular server or device in real time. It intended to optimize network speed, reliability, flexibility, scalability, and security for powerful way to run multiple networks, at the same time over a shared substrate. Therefore, We consider the role of virtualization to support multiple architectures simultaneously as a long-term solution for the future Internet. However, the difficulty is the requirement of resource separation at a certain level of isolation. Because most of the infrastructures have the potential to support virtualization, there's no need to change them as well as the service providers can operate their own virtual network that is up to their own needs such as throughput, latency or security. For the operation and management of virtual network to its best, there should be additional parties such as Virtual Network Providers for assembling virtual networks between multiple providers and Virtual Network Operators for the installation and operation. Moreover, there should be supporting architecture and standardized interfaces so that it is easily manage for each level of each related parties.

- **Support of heterogeneous wireless network** is to reduce the unnecessary handover occurrences in the network the heterogeneous network must be fixed limited number of Received Signal Strength (RSS), Location, Multi-parameter based on QoS, Signal-to noise and Interference ratio. The network can cooperate with mobile user to provide seamless mobility support in order to highly multimedia Quality-of-Service (QoS) constraints.

- **Support independent network** is a way to represent a hierarchical tree structure because parent at top and child at the bottom. In a hierarchical structure parent node is one step higher than child node in the same branch and the Peer-to-peer (P2P) computing or networking is a communication model which deals with the establishment of multimedia communication network/file sharing network by partitioning the tasks between peers. In such a network, each peers share a portion of their own resources (e.g. processing power, storage capacity) to facilitate the service provided by the network. In this network, a peer can initiate a request as well as it can respond to a request from the other peers in the network. Therefore, the hierarchical structured domains have composed parent-child relationship to support efficient forwarding routing mechanism in a large networks.

3.2.3 DESIGN FOR TUSSLE

We suggest that the reality of tussle implies the need for network designers to think explicitly about tussle and the design requirements it implies [42]. Based on design principal, FI should not organized by one particular Internet stakeholder over another. FI should be capable of supporting flexible business models where multiple stakeholders can participate in an open environment that supports and encourages innovation and participation without barriers. The FI should support a greater participation of individuals, communities and small businesses alongside larger and more established organizations. The FI should enable all providers of content, services or other forms of added value to receive appropriate compensation for their contribution. The FI should support a greater participation of individuals, communities and small businesses alongside larger and more established organizations. As a computer science discipline, we focus on design principles that deliver such virtues as performance, robustness, scalability and manageability in the face of complexity, component failures, growth, and other challenges. We need to think about tussle in the same way: as an important and central aspect of design. As we do so, we may come to recognize design strategies driven by the growing tussle among between different Internet players [7].

3.2.4 MODULAR APPROACH

Modularity is an important design principle; its goal is to design systems so that modules can be optimized independently of other modules because in a case if one module fails then it does not affect other modules. A modular application can dynamically load and unload modules at runtime, completely separate applications in their own right, which interact with the main application and other modules to perform some set of tasks. Each modules are self-contained that can replace or add anytime without affecting the rest of the system. Therefore, we should consider following terns to design a specific modular into the FIA.

- **Decompose** is the common concept of tactic to divide into sub-module in the same structure and analyse the issues of each modules. To analyse the full cost, we need to combine all modules. The benefit of the decomposition is to concentrate in a specific module for understand, design and manage complex interdependent systems.

- **Recursion** is a method where the solution to a problem depends on solutions to smaller instances of the same problem. The power of recursion evidently lies in the possibility of defining an infinite set of objects by a finite statement. In the same manner, an infinite number of computations can be described by a finite recursive program, even if this program contains no explicit repetitions [Wikipedia].

- **Vertical and/or Horizontal Layering** is an isolated access network from the service layer to aid the access of multimedia and voice applications from wireless and wire line terminals. It means services do not need their own control functions it is supported by control common horizontal layer to reduced cost and complexity.

- **Separation of Identifier and Locator** is very important point for mobility support to a node. As we know a name is often used as an identifier of the node that the name denotes. To be used as an identifier, a name must be unique in a given scope but this is not always guaranteed. For non-unique names to be used as identifiers their scopes may be limited or name must be attributed. Current internet is overloading of IP address due to scalability issues because each IP address carrying an identity and location information's of the node. Therefore, if we replace IP-address into two separate fold ID and LOC (locator) then node easily moves to other location at any time without interrupting communication connectivity. Where ID (identifier) is a unambiguously identity of the node and locator is a symbol which used for pointing specific positions on a given space. Note that,

- **Separation of control plane and data plane** as we know the current internet has combined control plane and data plane into same plane and the data and control traffics are routed without distinction as shown in the IP and ICMP protocols. Hence, if data plan may consist of the wireless links with relatively low bandwidth and unreliable transmissions, whereas the control plan is high bandwidth to provide reliable transmissions. According to communication mechanism result are differ but it need should be same. Then, we need to separate control plan and data plan and design an affected with better performance in the network.

3.2.5 INTRINSICALLY SECURE

Future Internet should be designed so to effectively support intrinsically security function. Hence, if somehow network security accident such as DDoS happens then the traceability of original attacker is required to cope with next accident and to claim responsibility for the attacks. A network should have the functionality on achieving location information or identifier of the malicious host or hacker for traceability of malicious activity. Hence, it should consider following terms to design a secure FIA.

- **Self-certifying ID** is a global and decentralized ID distributed system that is providing transparent encryption of communications and authentication into the IMS (ID-mapping server) which is uniformly accessed by any server.

- **Self-management** is the process by which computer systems shall manage their own operation without human intervention. Self-management includes functionality required for self-configuration, self-optimisation, self-healing and self-protection.

- **Trustworthy network** is defined as a network which intrinsically support mutual authentication of the network entities and content integrity. Hence, the developments of trustworthy networks are strongly related to protect their privacy and personal data. To support interoperability and standardization is given when appropriate, to strengthen the societal impact of the technology results such as coherently address security, trust and privacy from a technological, economic, legal and social perspective.

- **Intrinsic security** is possible for an entity to validate and communication with the correct entity without demanding access to external databases, information, or configuration.

3.2.6 ENVIRONMENTAL AWARENESS

Future Internet architecture needs to be environmentally designed so that the architecture design, resulting implementation and operation of Future Internet can minimize their environmental impact, such as the consumption of materials and energy and reducing greenhouse gas emissions. Following terms are required to consider into the developing of FIA [41].

- **Green networking** is the practice of selecting energy-efficient networking technologies and products, and minimizing resource use whenever possible. Energy Efficient Components Improvements in the energy efficiency of networking equipment components have been slow, due to the high costs of designing equipment with energy-saving technologies and the increasing number of functions that switches perform in the network that require more power. Such as energy-efficient CPU, server, peripheral and reduced recourse consumption as well as proper disposal of electronics waste. The green networks are including virtualization, server consolidation, more energy efficient products, remote administration, video conferencing for travel etc.

- **Improving Energy Efficiency** is available in two way to reduce the stress of their equipment by using the most efficient components and other is seeking to first

optimize network traffic across the network. By using rapid heat-dissipating raw materials, highly efficient power supplies, intelligent cooling systems, and advanced silicon solutions. Hence. There are significant equipment-level improvements in energy efficiency of all networking and IT equipment.

- **Power Management Capabilities** is widely needed to include in phase of designing to reduce the energy wasted by a computer. The advent of high-density computing equipment has sent power usage soaring. As a result, power consumption and other "green" issues are fast becoming the information technology (IT) industry's biggest challenge. Inevitably, as these concerns grow, focus will broaden to all types of IT equipment, settling on one of the thirstiest devices; the local area network (LAN) switch, which can consume several thousand watts. Hence, in a large network domain that wasted of energy quite significant so we need to consider in an initial stage of FIA to support an power management mechanism.

3.2.7 EVOLUTIONAL DEPLOYMENT

Sustainable networks are being flexible enough to continuously evolve, develop, extend and response to changing societal requirements. A sustainable network are allowing for environmental and societal developments over many decades. Hence, the sustainability of the FI will rely on its ability to be scalable, available and reliable in a resource- and cost efficient manner. The FIA must be designed to support universal communication that will overcome the obstacles of language, culture, distance, or physical ability which exist in the current Internet (CI). There are following general evolution terns which is consider into the development periods [7].

- **Internets of services are** needed to support flexible and rely on its ability to be scalable, available and reliable in a resource-and cost efficient manner. So, FI should be able to provide openness to users to facilitate the creation of new applications along with the ability for multiple entities, which are implemented according to certain common rules, to communicate with each other (interoperability).

- **Internet of Thing** is going to generate a huge amount of data that can be captured and accessed by today's technologies. Since there are more things on the Internet than people on the Internet. With the use of the IoT, we can easily manipulate data to get information, from information to get knowledge and knowledge to wisdom. We have a lot of systems connected by IoT but these systems are not isolated but controlled by each other.

- **Reconfigurability** is a behaviour capability of a system that can compute and reconnection in a time and run time. Dynamic reconfigurablity denotes the capability of a dynamically reconfigurable system that can dynamically change its behaviour during run time.

4. TECHNICAL PERSPECTIVES

This clause describes specific requirements and technical principles to make realization of Future Internet Architecture (FIA) from specific technical perspectives.

4.1 Mobile perspective

4.1.1 SPECIFIC REQUIREMENTS

To effectively support the mobility in Future Internet, the following specific requirements should be considered in the design of Future Internet architecture.

4.1.1.1 PROVISION OF MOBILITY FUNCTIONALITY IN THE BUILT-IN FASHION

It is envisioned that mobile users now become the key driver toward future Internet with explosive growth of the number of subscribers of 2G/3G cellular systems and other wireless data systems, and that there will be much more mobile/wireless users than wired ones. However, it is noted that the current Internet was originally designed for fixed hosts, rather than for mobile ones, which has enforced to develop the extensional features to Internet, in the patched-on fashion, in order to support the mobile environments, as shown in the examples of Mobile IP (MIP). However, such patched-on approach seems to be just a temporal heuristic rather than a sustainable solution to the mobility issues to future Internet.

Accordingly, the mobility functionality should be provided in the design of Future Internet in the built-in fashion rather than in the patched-on way.

4.1.1.2 PROVISION OF LOCATION MANAGEMENT AND HANDOVER CONTROL

To support the mobility functionality, the Future Internet should be designed to provide the location management and handover control.

The location management function is used to keep track of the movement of a user in the network and to locate the user for data delivery. It is noted that the location management function is used for supporting the prospective ‘incoming’ call to the mobile user. The LM

functionality includes the location registration/update and location query (for user data transport). The location registration/update function is to keep track of the current location of a user. The location query function is to locate the user for data communication.

The handover control function is used to provide the 'service continuity' for the 'on-going' session of the moving user by minimizing data loss and handover delay during handover. With the help of the handover control function, a mobile user can seamlessly continue the data communication during the session, even though it changes its location (or IP address) in the network.

4.1.1.3 PROVISION OF SCALABILITY TO MOBILITY CONTROL

Most of the mobility schemes in current Internet are based on a centralized mobility anchor, such as Home Agent (HA) of Mobile IP (MIP) or Local Mobility Anchor (LMA) of Proxy MIP (PMIP). The centralized control, however, tends to inject unnecessary data traffic to Internet core, and thus the data traffic explosion problem becomes more severe. Moreover, the centralized approach is vulnerable to a single point of failure or attack.

Accordingly, the scalability to mobility control should be provided in the design of Future Internet for effective mobility support and for avoiding the traffic explosions.

4.1.1.4 SUPPORT OF ROUTE OPTIMIZATION

In the centralized mobility control of current Internet, the routing path through a centralized anchor tends to be longer, which results in non-optimal routes and performance degradation.

Accordingly, the route optimization in the mobility control should be provided in the design of Future Internet.

4.1.1.5 SUPPORT OF MULTI-HOMING HOSTS

In the future Internet environment, it is expected that a host with multiple interfaces will be very common, in which the host may be connected to two or more wireless networks (e.g. wireless LAN or 3G wireless network, etc).

Accordingly, the Future Internet should be designed to effectively support the multi-homing hosts with multiple network interfaces.

4.1.1.6 SUPPORT OF HETEROGENEOUS WIRELESS NETWORKS

The current Internet assumes a common IP protocol stack over all Internet nodes according to the famous hourglass model. However, networks environment will become more heterogeneous, which are ranged from simple lightweight networks to highly reliable networks. For instance, wireless networks are likely to have quite diverse characteristics from sensor networks to cellular networks. In the meantime, the backbone network is evolving to full optical network with very high bandwidth.

Accordingly, the future Internet should be designed to effectively support the network heterogeneity and diversity.

4.1.1.7 SUPPORT OF OPPORTUNISTIC WIRELESS LINKS

The current Internet was designed based on a stable connection between host and network. However, in mobile environment, the connection is subject to dynamics of the network, in particular, due to high error rates and intermittent connections, depending on characteristics of wireless links.

Accordingly, special considerations should be taken for lossless and reliable communications in such wireless network environments, as shown in the example of the Delay Tolerant Network (DTN).

4.1.1.8 SUPPORT OF IDLE/SLEEP-MODE HOSTS

In current Internet, it is implicitly assumed that a host is always active so that it can receive the incoming packets at any time. However, it may not be true in a certain mobile/wireless environment. For instance, mobile hosts such as smart phone may be in idle, dormant or sleep mode frequently where they may not response immediately for incoming packets. This inactive condition of mobile hosts brings unacceptable packet loss. In addition, the power saving is the most essential requirement for mobile hosts. However, we note that the current Internet protocols have been designed without any special consideration on this issue.

Accordingly, the Future Internet should be designed to effectively support the idle/sleep mode hosts.

4.1.1.9 SUPPORT OF NETWORK MOBILITY

Future Internet is envisioned to include moving networks as well as moving terminals. Some of typical example platforms for moving networks could be bus, train, ship, air plane and so on. Such moving networks may require the seamless services.

Accordingly, the Future Internet should be designed to effectively support the network mobility, which is called 'network mobility'. This network mobility may require the different features from the host mobility.

4.1.1.10 SUPPORT OF SERVICE/PERSONAL MOBILITY

In addition to the host and network mobility issues, the services mobility and the personal mobility need to be supported in the Future Internet environments. The services mobility can be applied for a specific service, i.e., the ability of a moving object to use the particular (subscribed) service irrespective of the location of the user and the terminal. The personal mobility represents the mobility for those scenarios where the user changes the terminal used for network access at different locations. The ability of a user to access telecommunication services at any terminal on the basis of a personal identifier, and the capability of the network to provide those services delineated in the user's service profile.

Accordingly, the Future Internet should be designed to effectively support the services mobility and the personal mobility.

4.1.2 TECHNICAL PRINCIPLES

4.1.2.1 SEPARATION OF IDENTIFIER AND LOCATOR

In current Internet, an IP address has overloaded semantics as Identifier (ID) and Locator (LOC). In mobile environment, however, the location of mobile host is likely to continue to change by movement. This means that the static allocation of LOC (IP address) to a host may become problematic in mobile networks. In the meantime, the ID needs to be kept persistently (without change) to maintain an on-going sessions against movement of a host. Accordingly, ID and LOC should be separated to support the mobility in future Internet. That is, an identifier should be used only to identify an object in the viewpoint of service provisioning, whereas a locator should be used so as to effectively locate the object and to deliver packets in the network.

Another critical concern is that IP address, as an ID, is allocated to a network interface of a host, rather the host itself. Accordingly, if a host has multiple interfaces, multiple IP addresses must be allocated to a single host. This may give serious inefficiency to a multi-homing host, since the same host has to use different IDs for communication. Therefore, ID needs to be allocated to a host itself rather than its network interface.

As for the allocation of LOC or IP address, it does not make sense to allocate IP address to a mobile host, since it may continue to move on. Accordingly, in mobile environments, it is suggested that an address or LOC should be allocated to a certain fixed node in the network, rather than the host itself.

4.1.2.2 ID-BASED GLOBAL COMMUNICATION AND LOC-BASED LOCAL DELIVERY

With host ID and network LOC, the ID-based global communication and LOC-based local delivery is considered for effective mobility control. That is, the end-to-end communication between two hosts will be performed only with their host IDs, whereas data packets will be delivered to an end host by using the associated network LOCs, possibly through one or more transit networks. Such LOCs may be local or private IP addresses, and each of transit networks may use different routing schemes within its domain.

For this purpose, each host has a globally unique ID, by which global communication is accomplished. In the meantime, various LOCs can be used for packet delivery in each network. Each LOC is used locally in the networks, without any assumption on global uniqueness of LOC.

In addition, in Future Internet, the protocols used for data delivery in access and backbone networks need to be separated. In future Internet environment, each access network and the backbone network may have quite different characteristics. For example, access networks might consist of the wireless links with relatively low bandwidth and unreliable transmissions, whereas the backbone network will be the optical network with high bandwidth to provide reliable transmissions. Accordingly, the protocol requirements for the access and backbone networks may be quite different. This implies that the protocols used in the access network need to be designed by considering the wireless link characteristics, whereas the protocols used in the backbone network may be designed to be as simple as possible by considering the optical networks.

The access networks should be able to guarantee easy access of users, whereas the backbone network is primarily purposed to provide effective delivery of packets. In this context, we need to separate the protocols used for access and backbone networks in the design of Future

Internet. In particular, we also note that the current IPv4/v6 protocols may be used in the backbone network, as an incremental approach (or a tentative solution) to deployment of future Internet. This is because the backbone network is quite difficult to replace with a completely new protocol at a stretch, compared to the access network. This approach will also be helpful for migration from the current Internet to the clean-slate future Internet.

4.1.2.3 Separation of Control Plane and Data Plane

In most of current Internet protocols, data delivery and control function are integrated and implemented at the same devices, and the data and control traffics are routed along the same path, as shown in the IP and ICMP protocols. The control information for signalling is mission-critical and thus needs to be delivered more urgently and more reliably, compared to normal user data. In this context, it is desired that the control functionality should be separated from the data transport functionality, as seen in the 3G or 4G wireless mobile communication systems.

4.1.2.4 Distributed Mobility Control

To effectively distribute the data traffic in the network, the future Internet shall be designed to provide a distributed mobility control. In the distributed mobility control, the route optimization will be intrinsically supported, and this can also mitigate the problem of a single point of failure to a local network. For this purpose, a centralized mobility anchor needs to be distributed to two or more locally distributed mobility anchors.

4.2 Content-centric perspective

4.2.1 Specific Requirements

4.2.1.1 Provision of user-oriented Content Naming Scheme

Host addresses, such as IP addresses and MAC addresses, were introduced to connect devices and were used by computer experts, but the current Internet is mainly used by general users to access content. While a host address represents the location of a device, users are interested in content. Therefore, the addressing/naming scheme in networking should be changed from host addressing to content naming. Also, the content name should be easy to use by general users. Domain names are currently used for the similar purpose.

While a name in content-centric networking usually identifies a piece of content, a name can also represent multiple pieces of content (e.g., movies directed by Steven Spielberg), a person

(e.g., talk with Steven Spielberg), or a group of people (e.g., chat with actors of Jurassic Park). etc. Multiple different names may represent the same content (e.g., the Jurassic Park movie, the Jurassic Park movie directed by Steven Spielberg, the dinosaur movie directed by Steven Spielberg, etc.). Therefore, a name or names in the future Internet should be able to identify any entity or a group of entities.

4.2.1.2 SUPPORT OF EFFICIENT CONTENT ACCESS

While the host address-based networking is an efficient way to send a packet to a device, it causes inefficiency when retrieving content. When the same content exists on multiple devices, the addressed host may not be the best device to access the content. If general users can access what content they want, it is not important for them where the content comes. Therefore, content should be transferred from the nearest host in the communication space. Also, when a device has multiple connectivities, such as WiFi, cellular, and Bluetooth, the best connectivity should be used to get content quickly. Network traffic is changing from time to time, and thus, networking path should also be changed to escape traffic congestion. That is, networking should dynamically adopt the given environment and its change to support efficient content access.

4.2.1.3 FAIR SUPPORT OF MASSIVE CONTENT DISTRIBUTION

A video on demand service, such as YouTube and NetFlix, and a real-time video transferring service, such as IPTV, are significantly increasing the traffic of the Internet. Especially, an explosive increase of users to access certain content, such as a big match in the World Cup game, during the short time period causes serious traffic congestion in networks closed to its content server. The CDN (Content Delivery Network) service can reduce the number of same packets over the same physical link using local servers. However, the CDN service does support personal content which is not located on servers registered to the service, even though the content is required by numerous users at the same time. Also, the shared links between a local server and multiple client devices deliver the same packets. Therefore, massive content distribution should be supported by networking nodes without external servers to reduce network traffic for any content either on a server or a personal device.

4.2.1.4 SECURE NETWORKING

Major requirements of secure networking have been described in Section 4.5.

In content-centric networking, a name is given to access content. This name does not mean the location of the content. The content may exist on multiple devices and/or routing nodes;

the content is delivered from any device holding the content. In such a networking environment, sever protection and channel protection mechanisms cannot be enough to guarantee that the content is correct and secure. Therefore, the integrity of content should be provided with the signature of the content creator. Also, in order to allow only authorized/authenticated users to access content, the content should be encrypted with a security key.

4.2.2 TECHNICAL PRINCIPLES

4.2.2.1 HIERARCHICAL CONTENT NAMING

The size of a routing table in content-centric networking may be proportional to the number of content prefixes which are used to forward packets; as the number of content prefixes increases the size of the routing table also increases. It is assumed that the number of content prefixes will be larger than the number of devices. Thus, the size of FIB(Forwarding Information Base) table in content-centric networking will be larger than that of FIB in the current Internet. To effectively reduce the size of FIB, aggregation of names is necessary. Therefore, names should be hierarchically structured to support aggregation of content names.

4.2.2.2 DIRECT NAME-BASED PACKET FORWARDING

A domain name is easier for general users to identify a host than a host address. However, it introduces inefficiency in networking. Because the current packet forwarding nodes cannot directly handle domain names, a given domain name should be changed to an IP address through an external DNS (Domain Name System) server before delivering a packet to a destination device. Networks should directly process a name of content without the support of such external servers.

4.2.2.3 TIME-SHIFTED MULTICAST

To avoid transferring same packets over the same physical link, a packet forwarding node should know what packets the node delivers. By knowing the history of content requesting packets, the node can avoid to send the same content requesting packets to other devices. When the node receives the corresponding content, it will duplicate and send the content to the requesting devices. Also, if the node stores content being delivered on its cache, the node will send the stored content to devices that request the same content. It is called time-shifted multicast.

4.2.2.4 STRATEGY-BASED PACKET FORWARDING

When there are multiple candidates for networking, some of them may be used (e.g., multiple connectivities of a device, multiple paths from a content requesting device to a content providing device, multiple sources for same content, etc.). To select a candidate, various networking strategies may be applied: Select-All, Best-Fit, Round-Robin, etc. The future Internet should support various strategies to fit well user intention.

4.3 Mapping system perspective

The mapping system in the Future Internet may have to support a variety of mapping services. That is, when a user (or a host) sends a query with a key to the mapping system, it should reply with the value that corresponds to the given key. The current mapping system in the Internet is the DNS, which is host-oriented, and mainly used for mapping between domain names and their corresponding IP addresses. The DNS requires individual hosts to be connected to the global Internet, and potentially has the scalability issue. For instance, the popularity of .com implies that its registry operator (i.e. VeriSign) should handle a large amount of query traffic. Also, if it is used to provide the mapping between identifiers and locators of mobile hosts, it should be provisioned for dynamic updates of the entries.

4.3.1 SPECIFIC REQUIREMENTS

4.3.1.1 FLEXIBILITY

The mapping system may have to support a wide variety of key-value mapping. One of the crucial key-value mapping is the locator update of mobile hosts for mobility support. Also, to mitigate the routing scalability, the mapping of endpoint identifiers to their routing locators can be supported by the mapping system. Another potentially important usage is the mapping from content names (or content identifiers) to their locators, which is similar to trackers in BitTorrent systems. There may be other usages or requirements of the mapping system in the Future Internet. It should be able to be extended to support other naming or mapping functionality.

4.3.1.2 AVAILABILITY/RESILIENCY

It should not have a single point of failure/bottleneck. According to some DNS measurements, a substantial portion of the DNS traffic is often lost. The workload on the servers in the mapping system should be balanced and distributed. Also, a failure of a single server or component in the mapping system may have to be recovered without noticeable disruption.

4.3.1.3 RESPONSE TIME

The mapping of key-value pairs may be replicated globally or locally. In this way the response from the mapping system may be returned to potential solicitors timely, so that the delay of resolution does not affect the applications and services.

4.3.1.4 AUTHENTICITY/INTEGRITY

The mapping information of the key should be trustworthy. We may leverage the DNSSEC or Resource PKI. Whether this issue is handled in the AWG or security WG needs further discussions.

4.3.1.5 ABSENCE OF GLOBAL CONNECTIVITY

The mapping system may have to be able to operate even without its global connectivity. For instance, sensor networks, ad hoc networks, and delay tolerant network may operate individually without connectivity to the global Internet. The mapping system may need to support operations locally in an autonomic manner.

4.3.2 TECHNICAL PRINCIPLES

4.3.2.1 HIERARCHICAL OR FLAT STRUCTURES

One of the main principles that should be considered in designing a mapping system is that whether the main structure is hierarchical or flat. The DNS has the tree structure, which has the problem of a single point of failure/bottleneck. The weakness is augmented by adding redundant nodes (and links) to enhance resiliency (e.g. 100+ root server machines) and has been extended with high availability. If the mapping system has a tree structure, the lessons from the DNS operations should be taken into account. A flat structure, like distributed hash table (DHT) is also possible for a mapping system. Even though it is more resilient by nature, its performance issue (e.g. delay) should be solved. Some combination of tree and flat structures may be possible.

4.3.2.2 CACHING FRIENDLINESS

The mapping system may have to be designed in the anticipation of caching the mapping data. That is, in-network nodes (say routers) or end-hosts may cache the value that corresponds to a key. The workload on the mapping system will be significantly mitigated, and the lookup delay will also be reduced.

4.3.2.3 LOCALITY OR POPULARITY

Not all the data in the mapping table will be equally accessed. For instance, in the cases of mobility, there is often the locality between the corresponding host and mobile host. If the mapping system provides the location of content files, there will be popular files and unpopular files. The mapping system can be efficiently or cost-effectively designed and operated if the disparity among the mapping data is exploited.

4.4 Green networking perspective

This subsection investigates Future Internet architectural requirements from the perspective of green networking or energy-efficient networking [43].

Improving energy efficiency and reducing the greenhouse gas (GHG) emissions have become a global agenda recently. European Union (EU) has announced that EU will reduce the GHG emissions by 20 percent until 2020. Korean government also has declared the reduction of GHG emissions by 4 percent in compared with those of 2005 until 2020. It has been investigated that ICT industry emitted 2 percent of man-made GHG and consumed 4% of global electricity consumption in 2008, so efficient operations become important for reducing energy consumption in ICT industry. Therefore, Future Internet should be designed by considering the energy efficiency and energy consumption in network.

4.4.1 SPECIFIC REQUIREMENTS

4.4.1.1 CONSIDERATION OF ENERGY IN NETWORKS

In order to achieve more improvement in energy efficiency, it is necessary to consider energy efficiency in network. First of all, energy efficiency should be considered during network planning and dimensioning. The planning includes how to replace electronic networks with more energy efficient networks such as optical networks and accomplish more reduction in energy consumption for data transfer. Also, network protocols used in network should be designed in order to establish a reliable connection but at the same time be energy efficient and these energy-aware network protocols should be used in not only core networks, but also access networks. Finally, optimized transmission and access methods such as advanced wireless channel management methods should be supported in wireless access networks.

4.4.1.2 INCREASED ENERGY EFFICIENCY IN NETWORK EQUIPMENTS

In order to increase the energy efficiency of network, the energy efficiency of network equipments should be initially considered. There are several methods to increase the energy efficiency of equipments, including network interface proxying, rate adaptive link control, etc. More specifically, network equipments need to support energy saving mode i.e., sleep mode, in order to reduce energy consumption and network interfaces should support energy management mechanisms such as adaptive link rate and sleeping mode. In addition to that, network equipments should have mechanisms allowing single pieces of equipment to go idle for some time, as transparently as possible for the rest of the networked devices. And, network equipments should have different energy consumption (or cost) profiles that a device may exhibit as a function of its utilization level. Also, from the hardware's point of view, network equipments need to utilize low power electronics for reduce energy consumption and efficient battery technology should be deployed in nodes in case of battery-powered equipments. Finally, in order to effectively control and manage the energy consumption in equipments, energy management functions should be deployed in network and equipments.

4.4.2 TECHNICAL PRINCIPLES

4.4.2.1 SUPPORT OF NETWORK VIRTUALIZATION

Network virtualization is a technology that enables the creation of logically isolated network partitions over shared physical networks so that heterogeneous collection of multiple virtual networks can simultaneously coexist over the shared networks. This includes the aggregation of multiple resources in a provider and appearing as a single resource [44].

Network virtualization technology can decrease the resource consumption and energy consumption of networks by changing the overall architecture of networks. This technology enables network operators to deploy multiple virtual networks on a physical network. This reduces necessary physical resources for constructing networks, e.g., optical fibre or copper cable, which generally reduces energy consumption. Also, this technology regroups a set of mechanisms allowing more than one service to operate on the same piece of physical resource, thus improving the hardware utilization. This opens possibility to lower energy consumption because a single machine under high load generally consumes less energy than several lightly loaded ones. Also, network virtualization can support resource consolidation which regroups underutilized devices to reduce the energy consumption [44].

4.4.2.2 SUPPORT OF SELECTIVE NETWORK CONNECTIVITY

Networked devices often stay on because the Internet Protocols assume that the devices are always-on. So, it prevents other devices from saving energy because entering the energy saving loses network connectivity. At some point devices will go into sleep and they need to do extra work to join the network again. Therefore, it is necessary to provide intelligence for maintaining network presence in an entity in the networks other than the network devices.

Proxying is a mechanism allowing single pieces of equipment to go idle for some time, as transparently as possible for the rest of the networked devices. A network proxy is an entity that maintains full network presence for a sleeping device and the sleeping device appears to other devices as fully operational. Edge devices can go idle in order to avoid supporting network connectivity tasks (e.g., periodically sending heartbeats, receiving unnecessary broadcast traffic, etc.). These tasks may have to be taken over by other nodes, such as proxies, momentarily faking identity of idle devices, so that no fundamental change is required in network protocols.

Therefore, controlling sleep mode of networked devices should be supported in order to increase energy efficiency of the devices.

4.4.2.3 SUPPORT OF UTILIZATION PROPORTIONAL ENERGY USAGE

Energy consumption on network devices, especially an Ethernet link is largely independent of its utilization. During the idle interval, the devices or Ethernet links are used to continuously send and receive traffic that is not destined to the devices in order to keep network connectivity or to preserve synchronization. Furthermore, energy consumption of a link mostly depends on the negotiated link capacity rather than actual link load. Therefore, devices with different energy consumption profiles have emerged. The devices may show energy consumption as a level of a function of their utilization levels.

These different profiles offer different optimization opportunities. Energy-agnostic devices, whose energy consumption is constant, independently of their utilization, represent the worst case. Such devices are either on and consume the maximum amount of energy, or off and inoperative. In contrast, fully energy-aware devices exhibit energy consumption proportional to their utilization level. Between these two extreme situations, there exist an infinite number of possible intermediate profiles, for instance the single-step and multi-step cases, whose energy consumption coarsely adapts to their load. Single step devices have two operation modes while multi-step devices have several performance thresholds.

One of the well-known technologies is adaptive link rate in Ethernet devices. Adaptive Link Rate, to which most of the effort in green networking has been devoted up to now. These techniques, following the proportional computing paradigm, are designed to reduce energy consumption in response to low utilization in an on-line manner. Techniques can be either considered to be link-local or network-global depending on the network layer they pertain to, as well as on the scale of the network involved and the need for interaction between elements (in which case, they also apply the selective connectedness principle). A considerable number of works have explored this solution, and the IEEE Energy Efficient Ethernet Task Force is moving toward its standardization as IEEE 802.3az [4-3].

Therefore, the energy consumption of network devices should be proportional to the utilization level of the devices in order to effectively reduce energy consumption.

4.5 Security perspective

4.5.1 SPECIFIC REQUIREMENTS

To effectively support the security in Future Internet, the following specific requirements should be considered in the design of Future Internet architecture.

4.5.1.1 MALICIOUS-PACKET-FREE ARCHITECTURE

The various forms of malware such as botnets are emerging as the most serious threat against network security as they provide a distributed platform for several illegal activities such as launching distributed denial of service attacks against critical targets.

Accordingly, the Future Internet should be designed to effectively support that there are no malicious packets such as the data from a spoofed host in the network.

4.5.1.2 BUILT-IN SECURITY

The current Internet was originally designed for open and scalable network. This feature makes it possible to deploy the Internet very successfully. In particular, the Internet Protocol (IP) was designed to support ease of attachment of hosts to networks. However, this feature results in the lack of security. In particular, there is no inherent support in the IP layer to check whether a source is authorized or not. Therefore, security function was added into the original Internet as an additional or optional layer such as IPSec. However, this add-on solution cannot solve the problem fundamentally.

Accordingly, the Future Internet should be designed to support the security function intrinsically.

4.5.1.3 TRACEABILITY OF MALICIOUS ACTIVITY

When network security accident such as DDoS happens, the traceability of original attacker is required to cope with next accident and to claim responsibility for the attacks. Traceability of malicious activity means that the network should have the functionality on achieving location information or identifier of the malicious host or hacker.

Accordingly, the Future Internet should be designed to support traceability of a malicious activity.

4.5.1.4 USER PRIVACY

User privacy is hot issue in today's network environment. The privacy information includes personal identification data such as social security number and e-mail ID. In addition, it includes location data of an user such as GPS information of a smart phone. The customer's personal information on service provider should be handled confidentially by adopting cryptographic encryption and secure audit technology. Also, service providers cannot achieve normal user's private information including location data without the prior consent.

Accordingly, the Future Internet should be designed to support user privacy.

4.5.1.5 CONSIDERATION OF SYSTEM AVAILABILITY

The security function should be developed in consideration with system availability. Security problem is big issue nowadays because the security features has been developed without taking into account the availability. For example, the system with security function such as firewall and IDS shows lower performance compared to the system without security function. This makes it hard to deploy the security function in the whole network.

Accordingly, the Future Internet should be designed to develop security function in consideration with system availability.

4.5.2 TECHNICAL PRINCIPLES

4.5.2.1 SELF-CERTIFYING IDENTIFICATION

Future Internet should support the built-in security which allows an entity to validate that it is communicating with the correct entity without needing access to external databases information, or configuration. The use of self-certifying identifiers for network entities can provide intrinsic security. The self-certifying identifier can be defined as an identifier which is proved without relying on any global trusted authority. One example for the self-certifying identifier of the network entity is the public key of the network entity or the hash of the public key. With the self-certifying identifier the Future internet should support mutual authentication of the respective host. In addition, the Future Internet should support integrity and validity of the content that a user requests.

4.5.2.2 USER-CENTRIC IDENTITY MANAGEMENT

Future Internet should support user-centric identification management which allows users to have control over their identity information as it's collected and stored. In addition, users should be able to know and restrict who might use the data for what purposes.

4.5.2.3 TRUST DOMAIN MANAGEMENT

The Future Internet should support trust domain management. The domain can be defined as logical or physical communication group in the whole network. The trust domain can be defined as the domain which is composed of the entities trust each other. Entities outside of the trust domain should have high level of security policies to communicate each other. However, entities inside of the trust domain can have low level of security policies. Future Internet should support the built-in security which allows an entity to validate that it is communicating with the correct entity without needing access to external databases information, or configuration. The use of self-certifying identifiers for network entities can provide intrinsic security.

5. RECOMMENDATIONS

[Editor's Note: The section will be described after maturing the draft document]

6. REFERENCES

[1] T. Zahariadis, et al., “Towards a Future Internet Architecture,” Lecture Notes in Computer Science, Vol. 6656/2011, pp. 7-18, 2011.

[2] Raj Jain, Arjan Durresi, Subharthi Paul, "Future Internet Architecture: Design and Deployment Perspectives", IEEE Communication Magazine, July 2011.

[3] J. Pan, S. Paul, R. Jain, "A Survey of Research on Future Internet Architectures, "IEEE Communications Magazine, Vol. 49, No. 7, July 2011, pp. 26-36

[4] S. Paul, J. Pan, R. Jain, "Architectures for the Future Networks and the Next Generation Internet: A Survey," Computer Communications, UK, Volume 34, Issue 1, 15 January 2011, Pages 2-42

[5] J. Pan, R. Jain, S. Paul, C. So-In, "MILSA: A New Evolutionary Architecture for Scalability, Mobility, and Multihoming in the Future Internet," IEEE Journal on Selected Areas in Communications, Vol. 28, No. 8, October 2010

[6] S. Paul, R. Jain, J. Pan, "A Future Internet Architecture Based on De-conflated Identities," Proceedings of IEEE Globecom 2010, Miami, FL, December 6-10, 2010

[7] Future Media Internet Architecture, “Future Media Internet Architecture Think Tank” FMIA-TT reference model (v1.0), 1 March 2011. (White Paper)

[8] D. Clark, L. Chapin, V. Cerf, R. Braden, R. Hobby, "Towards the Future Internet Architecture", IETF Network Working Group,RFC-1237, Dec. 1991.

[9] D.D. Clark, The Design Philosophy of the DARPA Internet Protocols, ACM SIGCOMM Computer Communications Review, Vol. 18, No. 4, Aug. 1988, pp. 106-114.

[10] R. Braden, D.D. Clark, S. Shenker, and J. Wroclawski, "Developing a Next-Generation Internet Architecture", ISI white paper, 2000

[11] Nicholas Bambos, "Toward Power-Sensitive Network Architecture in Wireless Communications: Concepts, Issues, and Design Aspects", IEEE Personal Communications, June 1998.

[12] Neda Beheshti, Yashar Ganjali, Monia Ghobadi, Nick McKeown, Jad Naous, Geoff Salmon," Time-Sensitive Network Experiments, University of Toronto SNL Technical Report TR08-UT-SNL-04-30-00.

[13] A. Feldman, Internet Clean-Slate Design: What and Why?, ACM SIGCOMM Computer Communications Review, Vol. 37, No. 3, July 2007, pp. 59-64.

[14] NSF: http://www.nsf.gov/pubs/2010/nsf10528/nsf10528.htm

[15] PIMS: http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503325

[16] FIND: www.nets-find.net

[17] GENI: www.geni.net/?p=1339

[18] AKARI: akari-project.nict.go.jp/eng/overview.htm

[19] FIF: mmlab.snu.ac.kr/fiw2007/presentations/architecture_tschoi.pdf

[20] FI: http://www.future-internet.eu/

[21] CORDIS:http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_RCN=8376495

[22] NSF Future Internet Architecture Project, http://www.nets-fia.net/.

[23] Named Data Networking Project, http://www.named-data.net.

[24] MobilityFirst Future Internet Architecture Project, http://mobilityfirst.winlab.rutgers.edu/.

[25] NEBULA Project, http://nebula.cis.upenn.edu.

[26] eXpressive Internet Architecture Project, http://www.cs.cmu.edu/~xia/.

[27] OpenFlow Switch Consortium, http://www.openflowswitch.org/.

[28] The FP7 4WARD Project, http://www.4ward-project.eu/.

[29] FIRE: Future Internet Research and Experimentation, http://cordis.europa.eu/fp7/ict/fire/

[30] GEANT2 Project, http://www.geant2.net/.

[31] JGN2plus- Advanced Testbed Network for R&D, http://www.jgn.nict.go.jp/english/index.html.

[32] China Education and Research Network, http://www.edu.cn/english/.

[33] CERNET2 Project, http://www.cernet2.edu.cn/index_en.htm.

[34] Internet 3.0 project, http://www1.cse.wustl.edu/~jain/research/index.html.

[35] The Network of the Future Projects of EU FP7, http://cordis.europa.eu/fp7/ict/future-networks/home_en.html.

[36] Future Internet Assembly, http://www.future-internet.eu/home/future-internet-assembly.html.

[37] Domingue, J. & et. al, " The Future Internet Assembly published its third book titled: "The Future Internet, Future Internet Assembly 2011: Achievements and Technological Promises", a book published by Springer, July 2011

[38] Infographic, Cisco, http://www.ditii.com/2011/08/23/infographic-cisco-50-billion-things-on-the-internet-by-2020/

[39] D.D. Clark, The Design Philosophy of the DARPA Internet Protocols, ACM SIGCOMM Computer Communications Review, Vol. 18, No. 4, Aug. 1988, pp. 106-114

[40] A. Feldman, Internet Clean-Slate Design: What and Why?, ACM SIGCOMM Computer Communications Review, Vol. 37, No. 3, July 2007, pp. 59-64

[41] ITU-T Recommendation Y.3001 (2011), Future Networks: Objectives and Design Goals.

[42] D.D. Clark, et at all, “Tussle in cyberspace: defining tomorrow's Internet,” IEEE/ACM Transactions on Networking, Vol.13, Issue 3, June 2005.

[43] George Koutitas and Panagiotis Demestichas, “A Review of Energy Efficiency in Telecommunication Networks,” Telfor Journal, Vol. 2, No. 1, 2010.

[44] D. Clark, et at all, “Towards the Future Internet Architecture,” IETF RFC 1287, December 1991.

[45] Ashok Anand et al., "XIA: An Architecture for an Evolvable and Trustworthy Internet," CMU-CS-11-100, Jan. 2011

[46] David G. Andersen et al., "Accountable Internet Protocol (AIP)," In Proc. ACM SIGCOMM, Seattle, WA, August 2008.

[47] T. Li, et al. Recommendation for a routing architecture. IETF RFC 6115, February 2011.

[48] R. Moskowitz, et al. Host Identity Protocol. IETF RFC 5201, April 2008.

[49] R. Atkinson. ILNP concept of operations. IETF Internet Draft, draft-rja-ilnp-intro-11.txt, July 2011.

[50] D. Farinacci, et al. Locator/ID Separation Protocol (LISP). IETF Internet Draft, draft-ietf-lisp-15, July 2011.

[51] Homepage of Mobile Oriented Future Internet (MOFI), http://www.mofi.re.kr.

[52] Homepage of EIFFEL, http://www.fp7-eiffel.eu/

[Editor's Note: Requirements are not limited to above items. Additional requirements will be added according to contributions. Any contribution to FIF AWG is welcome: architecture@fif.kr or twyou@etri.re.kr]
