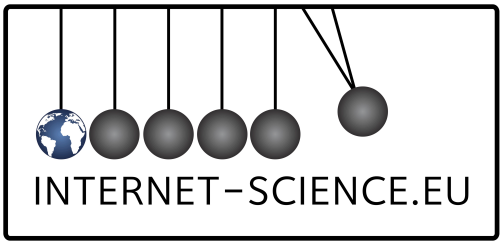

**ICT - Information and Communication Technologies**




**FP7-288021**

**Network of Excellence in Internet Science**

# Survey on Internet Science Research

**Due Date of Deliverable: 29/02/2012**

**Actual Submission Date: 30/04/2012**

**Start date of project:** December 1st 2011 **Duration:** 42 months

**Organisation name of lead contractor for this deliverable: CERTH**

**Editors: Anna Satsiou, Leandros Tassiulas**

**Contributors:** Anna Satsiou (CERTH), Raffaele Bruno (CNR), Andrea Passarella (CNR), Karl Aberer (EPFL), Thanasis Papaioannou (EPFL), Stephan Neuhaus (ETH), Bart Lannoo (IBBT) , Mathieu Tahon (IBBT), Sofie Verbrugge (IBBT), Marlies Van der Wee (IBBT), Rob Heyman (IBBT-SMIT), Jo Pierson (IBBT-SMIT), Andrea Scharnhorst (KNAW), Paolo Dini (LSE), Simone Basso (NEXA), Raimondo Iemma (NEXA), Federico Morando, (NEXA), Ioannis Stavrakakis (NKUA), Ian Brown (OXF), Christian Doerr (TUDelft), Fernando Kuipers (TUDelft), Piet Van Mieghem (TUDelft), Huijuan Wang (TUDelft), Heiko Niedermayer (TUM), Javier Aracil (UAM), Chris Marsden (UESSEX), Alberto Schaeffer-Filho (ULANC), Michael Till Beck, (UNI PASSAU), Andreas Fischer (UNI PASSAU), Gergö Lovasz (UNI PASSAU), Michael Niedermeier (UNI PASSAU), Kai Samelin (UNI PASSAU), Thomas Plagemann (UIO), Jonathan Cave (WARW).

Project Information

| | |
|---|---|
| **PROJECT** | |
| Project name: | Network of Excellence in Internet Science |
| Project acronym: | EINS |
| Project start date: | 01/12/2011 |
| Project duration: | 42 months |
| Contract number: | 288021 |
| Project coordinator: | Leandros Tassiulas – CERTH |
| Instrument: | NoE |
| Activity: | THEME ICT-20011.1.1: Future Networks |
| **DOCUMENT** | |
| Document title: | Survey on Internet Science Research |
| Document type: | Report |
| Deliverable number: | D13.1 |
| Contractual date of delivery: | 29/02/2012 |
| Calendar date of delivery: | 30/04/2012 |
| Editors: | Anna Satsiou, Leandros Tassiulas |
| Workpackage number: | 13 |
| Workpackage title: | Dissemination and Cooperation |
| Lead partner: | CERTH |
| Dissemination level: | PU |
| Version: | FINAL |
| Total number of Pages: | 84 |
| Document status: | FINAL |

**TABLE OF CONTENTS**

# 1. Executive Summary

This deliverable seeks to provide an Internet Science Survey. Since "Internet Science" is still more of an ultimate goal of this NoE than "a reality", this survey aims at presenting the different and usually unsynchronized efforts to study and understand Internet from different perspectives and disciplines. In this way it will serve as an important starting point to on one hand provide a cohesive view of the Internet research and on the other hand motivate and enable research towards making Internet a unifying discipline that although borrows some of its principles from other well-established sciences, has also its own particular fundamental laws and principles, similar to any other empirical science. Towards these goals, this deliverable presents the major Internet research drives that have been pursued so far, while next version, i.e., D13.2 related to the Roadmap of Internet Science will provide the future directions of Internet Science Research based on this study and the findings of this NoE.

The organisation of the deliverable is based on the evidence that Network Science and Web Science consist the two major Internet research drives followed by more recent research interest on (i) investigating how the Internet can support sustainability at planetary scale, (ii) how to deal with the new privacy and security issues brought up by the penetrating to Internet technologies, like cloud computing, sensor networks and Internet of things, and (iii) the various legislation and standardisation issues arisen as the Internet evolves.

# 2. Introduction

Human history has been shaped by networks: biological networks transferring enzymes and connecting cell elements; road networks transporting not only goods but culture; cultural networks, where information is elaborated among groups of people and transferred from generation to generation; economic networks (distribution networks, stock markets, etc.) where goods, services and information are exchanged in order to coordinate production, satisfy needs and generate (or appropriate) wealth; the power grid (among the most extensive man-made networks), which caters for the generation, transport and distribution of electric power. *The Internet is just a newcomer in this long sequence of networks, with some quite special features though.*

The emergence of the Internet as a new technology coincides with two other large-scale processes: globalization [2, 3] and the raise of the information society [4, 5]. Since its inception, the Internet has evolved from a purely technical artifact, in which all creators shared a common goal of interconnecting computers globally, to a central element of our social fabric through a combination of design and evolution by emergence. The designed elements mainly reflect principles from Computer Science and Communication, or more generally Information and Communication Technologies (ICT). On the other hand, the emergence of the web, especially in its more 'bottom-up' and social aspects (e.g. web 2.0), demonstrate that the design paradigm provides an inadequate basis for either the analysis of the Internet as it exists or even for the design of future aspects, and it has already provided ample evidence that the Internet cannot be studied and its potential cannot be fully exploited by using concepts from the area of ICT only.

It is importance to realize that "the Internet" in fact is a complex system in itself, composed by different layers (Fig. 1).

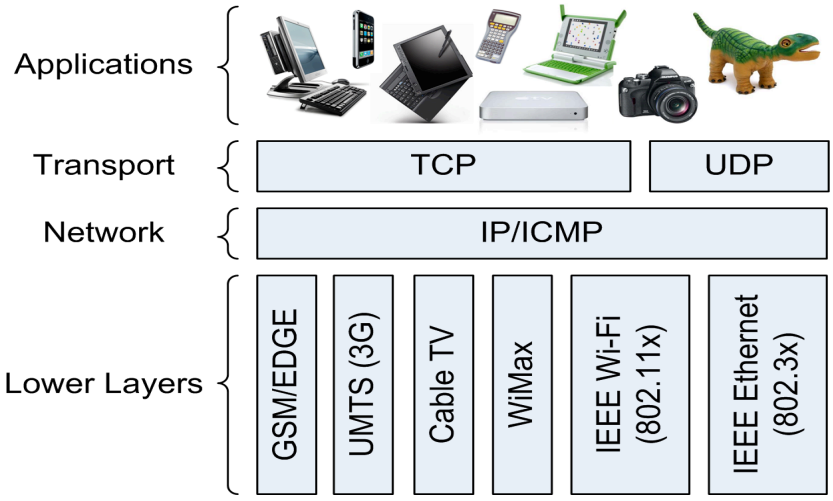



Fig. 1: Internet layers - Source: http://dret.net/lectures/web-fall10/img/network-convergence.png

The evolution of the Internet, as of any other network, is shaped by the human interaction that happens using it. Sociologists have long noted the importance of structure and function of inter-human and mimetic networks. Social networking, currently experiencing an explosive growth in its evolution and penetration, greatly evidences the above. Therefore, it is not surprising that the Internet is also impacting human interactions in a twofold manner: human activity shaping the network ("forward direction") and network impacting on human behaviour ("backward direction"). For instance, two relevant dimensions that have been deeply affected by the emergence of web-based networks' structures and its implications can be identified in new facets of knowledge generation (wikis, e-science, online education, distributed R&D, open innovation, peer-based production, online encyclopedias, user generated content) and new models of knowledge circulation and distribution (e-journals, open repositories, Creative Commons licenses, academic podcasting initiative, etc.).

The milieu that the Internet of today operates in has attracted various and diverse players from the commercial, government and civil society domains, which alternatively can be grouped into Internet providers, users and regulators (including co-regulators, and industry-led self-governance arrangements). Given the increasing number, power and disparity of these players, the complexity of their interactions and the plasticity of their roles, duplication, gaps and contention come as no surprise.

The results, however, can be surprising: well-intentioned actions that produce perverse consequences, disproportionate influence and discontinuous change, and emergent behaviour (including startling innovations) that may not even be perceived until fully developed and irreversible. The evolution of the Internet in the technological sense (to say nothing of the less-tangible cognitive, informational, societal, economic and political networks it supports) is often based on socio-economic 'fitness' rather than technological superiority, and it proceeds in 'punctuated' fashion (with periods of gradual and 'localised' change interspersed with shorter periods of widespread and disruptive change).

Another striking feature of the Internet is its tremendous generative power, stemming from the embedded architectural openness and the 'constitutional' end-to-end principle. This reflects the initial situation in which intelligence and trust could safely be left to the users of the Internet and to the edge devices through which they gained access. To further their collective ability to pursue improvements, the network itself was meant to be as flat, as simple and as open as possible – not least because more complex forms of facilitation within the Internet itself were technologically challenging.

However, the situation has changed; end users are no longer fully cognisant, no longer let alone in control of their devices, as the network itself can play a much more active role in managing collective problems. In their seminal work [1], Clark et al. recognise that struggle is as important in technology as in economic and political systems, suggesting that "we, as technical designers, should not try to deny the reality of the tussle, but instead recognize our power to shape it". Although meant for the technical people, this mandate pertains to all the communities that influence the various aspects of development of the Internet, many of which already recognise that their shaping decisions are moves in a game rather than acts of sovereign design. In consequence, the methodologies and techniques

developed by these communities are structurally consistent with the 'new' scientific perspective called for by Clark et al.

As soon as the Internet emerged as a technical and social-cultural phenomena, it has been studied from different perspectives**.** The Association of Internet Research held her first conference in 2000, and is since that active as "an academic association dedicated to the advancement of the cross-disciplinary field of Internet studies." [http://aoir.org/]. Internet research is devoted studying the practices using the Internet, but can be as diverse as designing web crawlers to study webspheres [6,7,8] and ethnographic studies in Second Life [9,10] to name only two examples.

The last 20 years have seen repetitive efforts in creating one commonly shared platform for Internet Science and/or Internet Research, accompanied by consolidation and professionalization inside of existing disciplines and yet again attempts to re-integrate disciplinary perspectives. This Network of Excellence is situated in this cycle of differentiation and re-integration as an important integrative moment. It aims at an exchange of knowledge about the Internet consolidated in rather isolated studies in different disciplines and perspectives.

***This survey aims at presenting the different and usually unsynchronized efforts to study and understand Internet from different perspectives and disciplines*****.** Major Internet research drives have been so far through Network Science and Web Science, also considering sustainability and legislation/standardisation issues and the interaction with the emerging new technologies (e.g., Internet of Things, cloud computing etc.) and the related security and privacy challenges.

# 3. Network Science Perspective

This perspective and the enormous literature associated with Network Science (e.g. [1]) have their origins in mathematics, physics, biology and allied natural sciences. It is primarily concerned with phenomenological description based on graph-theoretic properties interpreted as large-scale system outcomes of random processes. For example, physicists apply statistical mechanics to graph theory to analyse the implications of universal statistical features such as power laws in the measurement, modelling, and assessment of network structure and behaviour [2]. Among the central questions are:

1. whether complex system properties (e.g. reliability, robustness, performance, efficiency, adaptability, etc.) can be traced to (classes of) network structure;
2. whether structure and behaviour can be explained by universal laws – for example, to what extent can emergent 'global' properties not accounted for by reductionist or macro-level analysis be explained by such 'local' properties as self-organisation;
3. whether systems can be designed, engineered, organised, constructed, reinforced, managed, complemented or 'nudged' to improve their performance in an uncertain world by minimising vulnerabilities and endogenous collapse e.g. by producing 'robust yet fragile' geometries or adaptability.

One can identify different Network Perspectives [55] reaching from the impact of a network to one individual up to analyzing global properties of whole networks. Methods differ with respect to the different granularity of network analysis, and also to which scientific discipline takes most interest and claims most legitimacy explaining certain aspects. Concerning Internet science all different perspectives re-appear as becomes visible in the next section. What holds for Internet Science as well as for network science as one of its major theoretical approach is that one discipline alone is not longer capable to take care of understanding and managing network caused effects on individual behaviour and societal laws in the era of the Internet.

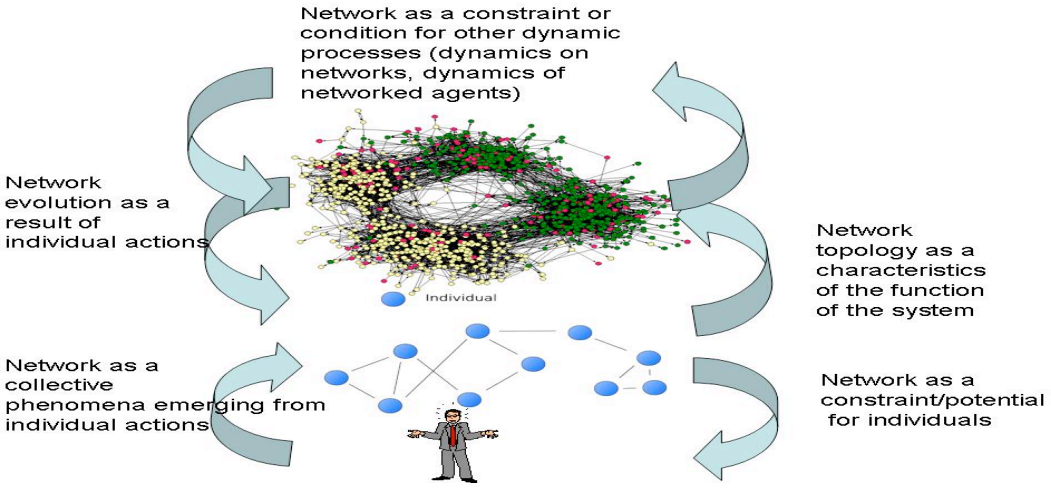



Fig. 2: Network as object of investigation and as boundary condition for other systems - on various levels (from micro to macro)

## 3.1 *Research Directions*

Strongly motivated by remarkable universal phenomena observed in many different complex networks ranging from the Internet, transportation networks, telephony networks, power grids, financial networks to social networks, we believe that the beginning of the third millennium will be typified by a transfer of knowledge of dynamic processes in living material to self-made and engineered structures, based on the principles of network science.

What tools and underlying theories can be applied? Beside descriptive languages, extensive computer simulations and measurements, network science mainly relies on graph theory for its topological structure, on probability theory to express characteristic properties such as the degree and eigenvalue distributions and on dynamic systems theory to describe the processes on the network (such as e.g. virus spread [3] and synchronization [4]). In these fields, progress is still being made: (a) new bounds on spectral and topology metrics, (b) asymptotic scaling laws, (c) new extremal graphs, (d) physical phenomena (coupling, synchronization, percolation, self-criticality, emergent and collective behavior and other, generally, non-linear processes). Although the main ambition is to understand networks via mathematical deductions, very often computer simulations are needed to scan the first order behavior, in order to direct analysis towards the correct path. Finally, measurements of real-world networks benchmark the quality of a new theory.

One of the high-level main drivers is the construction of a complex networking framework that combines several disciplines and application domains and that targets the right level of abstraction to find coherent and universal processes in these complex networks or systems. On a small scale, the details are overwhelmingly different: nodes in a complex network such as molecules in biology, computers or routers or hand-held devices (such as the Iphone) in the Internet, neurons in the brain, companies in an economic network, etc. Yet, the art is to “look” at the right scale of aggregation to cope with the complexity, surmount the distracting origin of microscopic differences and to “see” the beauty of invariants (such as the universal characteristics mentioned above).

Aiming at the ultimate goal of transferring robust and self-adaptive behavior in nature to man-made infrastructures, equipped with tools of cross diverse disciplines, we would like to address the following potentially transformative and continuously developing themes facing diverse complex networks.

### 3.1.1 Efficient Network characterisations

After about 13 years of extensive research on complex networks, numerous metrics have been proposed to quantify different topological properties. Examples are the degree of a node, the betweenness of a link, the hopcount of a shortest path from i to j, the clustering coefficient, the edge/link connectivity, etc. We refer to [5, 6] for a quite extensive discussion and comprehensive list of graph metrics and to [7] for additional properties. Another type of metrics are spectral metrics [8]

such as the largest eigenvalue of the adjacency matrix (spectral radius) and the algebraic connectivity, which are powerful characterisers of dynamic processes on networks such as virus spreading and synchronization processes.

These metrics are, however, correlated. Determining a small representative set of properties that largely determine all the other metrics considered, will greatly reduce the computation time in characterizing large complex networks, e.g. social networks and anatomical brain networks and will help to discover the network properties that influence the network's function the most [14]. Moreover, network optimization problems can be simplified if the set of network properties to be optimized can be reduced.

#### 3.1.1.1 Characterisation of nodes' importance: the Betweenness Centrality case

Revealing key properties of large network structures lies in the core of complex systems modeling and analysis. Central to this task is the role of centrality metrics originally introduced in social sciences [34]. They are used as graph-theoretic tools defined either on the nodes or edges of a (social) graph and aim to provide a measure of their relative significance or "social" standing. Different measures have been introduced to capture a variation of a node's importance [35], like ability to reach numerous nodes via relative short paths or popularity among others. Betweenness (BC), the most commonly used centrality metric, assesses the extent to which a network node lies on shortest paths linking all other node pairs. Betweenness centrality calculations are involved in a wide range of network science studies ranging from traffic analysis and network vulnerability to attacks [36] to cascading failures [36] and epidemics [38]. The computation of betweenness centrality, however, typically demands global information about all network nodes and their interconnections. The distribution and maintenance of this information is problematic in large scale networks. Moreover, availing increasingly larger datasets of network snapshots (e.g. OSNs, Internet maps) has turned much of the research effort to the BC approximations techniques.

A relevant thread involves the extrapolation-based BC estimation. Brandes and Pich [39] proposed a technique which is able to estimate the betweenness centrality of each network node by extrapolating values from a small subset of path computations. The pivots i.e., the source nodes from which the shortest path computations are initiated from, affect the achieved quality of the approximation; a random pivot selection is shown to perform better than deterministic strategies. Even if the method provides low-cost BC approximations it is prone to overestimates of the BC values of nodes lying close to the pivots. To improve over these overestimates, Geisberger et al. [40] introduced a scaling factor to modulate the BC estimates of network nodes with respect to their distance from the pivots. The method is shown to perform better over networks with unique shortest paths while being less accurate in the general case.

Posing constraints to the length of the considered shortest paths that are taken into account for the centrality computations leads to the notion of k-Betweenness Centrality [35, 41]; exploring paths of lengths at most equal to k offers yet another approximation of standard BC with cost bounded by the average number of edges present in the k-neighborhood of nodes. An alternative approach to

approximations yet of less complex computation for assessing node centrality may be based on a node's ego network; that is the subgraph involving itself, its 1-hop neighbors, and their interconnections. Nodes can acquire a local estimate of their centrality value through egocentric measurements [42] in their immediate locality. The approximation can then rely on the positive correlation between the two BC counterparts.

### 3.1.2 Dynamic Processes on Networks

Apart from the topological structure of a complex network, the network processes constitute the heart of network science: they determine why the network is built or created and they give value to a complex network. Examples of network processes or services are the transfer of IP packets in the Internet, the transport of cars in a road network, the interaction between functional brain regions, the spread of rumors and news in a social network, etc. A general topic in complex network theory is the dynamics of processes on the graph, of which virus spread [9] and synchronization [7,8] are reasonably well-understood examples. In most cases, we are interested to know whether the process is stable, whether phase-transitions [10] or forms of self-organisation occur and how the process behaves when the network grows (scaling laws) or is modified (removal or adding of subgraphs). In summary, the effect of the topology (graph) on the functioning (process) of network is an important theme. Immediately related to this theme is the association of relevant topology metrics to the function of the network.

### 3.1.3 Network Metrics through Distributed Measurements: the Net Neutrality Example

A relevant thread of applied research concerns the creation of metrics about Internet connections and quality of service on the basis of distributed measurements [15, 16, 17, 18]. Despite the availability of similar metrics for ICT companies and/or Internet Service Providers, both independent researchers and regulators frequently lack access to such data and/or to independent data in this domain [19]. Examples of policy domains where these metrics are crucial include the debate about Network Neutrality [20, 21].

State of the art network neutrality research tools either focus on detecting a specific blockage technique [22, 23, 24, 25, 26], or measure general quality metrics and try to identify unfair treatments by analyzing the results of many quality tests [27, 28, 29, 30, 31, 32]. Orthogonal to the two main lines of network neutrality tools is Measurement Lab, which provides a distributed worldwide server platform that hosts network measurements tools [33].

### 3.1.4 Network Co-evolution

A considerably more difficult class of problems is the study of the interaction between the processes on the network and the underlying network itself. For example, a virus spreads in a network and the

protection against the virus can consist of installing anti-virus software in computer networks or of vaccinations or medicines in a human social network. These actions do not change the underlying topology. However, adjusting the topology by avoiding contact with infected nodes (e.g. computers or humans) leads to another type of protection that requires the understanding of the coupling between graph and process (or function of the complex network). The last type of dynamics also receives increasingly more interest as most of our infrastructures are coupled [11]. For example, nearly all complex networks need energy, while the influence of digital communication to control these infrastructures increases. A failure occurring in the electricity distribution or in the control communication network may introduce failures or undesired behaviour in the functioning of the complex network. Such cascade effects are poorly understood.

Another theme is to understand how biological processes in nature achieve such an amazing adaptivity and resilience against external factors. For example, the Alzheimer disease is only diagnosed with certainty when over 80% of the links in the brains are destroyed. What is the way biological networks evolve? Which topological processes (such as rewiring, creation, deletion of links) are determining the network structure during the lifetime of an organism?

The flip-side of networks is the processes that take place within the nodes. Also here we can learn a great deal from nature, for example how the metabolic processes and transduction pathways taking place *within* neuronal cells are related to the synchronisation *between* neurones. A great deal of work has been done in modelling cytoplasmic and transcription processes inside the cell as the basis of new models of computation, for example through artificial chemistries [43, 44]. The more promising approaches are introducing more structure in artificial chemistries through algebra, for example chemical organisation theory [45]. The algebraic perspective on computation has been around for a long time [46], but until recently only extremely simple systems could be analysed due to the lack of adequate computational tools. This has recently changed [47], enabling the analysis of a range of real cellular and chemical networks [48, 49, 50] as well as networks of automata [51]. The work discussed in [52], in particular, seeks to connect the finite group structure of automata derived from particular metabolic and regulatory pathways to the Lie group structure of the non-linear dynamical systems derived from the same (bio)chemical rate equations. Because Lie groups are related to the integrability of (non-linear) dynamical systems, whereas the simple non-abelian groups (SNAGs) found in the corresponding automata can encode universal finitary computation (if greater than $A_5$) [53, 54], there is an interesting possibility to connect self-organising behaviour of metabolic networks with some of the computational properties of their corresponding discrete models.

# 4. Dimension of the "Web"

Network Science neither holistically captures phenomena, methods and insights from the social sciences perspectives, nor the dimension of the 'web' and the various associated repercussions with generation and retrieval of content in the Internet. These aspects are instead taken into account by the Web Science Trust started in 2006 between MIT and University of Southampton to bridge and formalize the social and technical aspects of the World Wide Web. The exact scope of Web science is still -intentionally- largely undefined. Some initial areas of interest are: social networks, collaboration, understanding online communities, analyzing the human interactions inherent in social media, developing "accountability" and other mechanisms for enhancing privacy and trust on the Web.

## 4.1 *Virtual Communities*

### 4.1.1 Online Social Networks

In the last years we witnessed a massive diffusion of online social networks (henceforth OSN) (e.g., Facebook, Twitter, etc.). The growing number of new communication paradigms introduced by these services is changing the way individuals interact and link to each other. Moreover, OSN are fostering the availability of a huge amount of data concerning social relationships between people that can be used to analyse human behaviours.

Sociologists and anthropologists have largely studied social relationships in humans from two different points of view. On the one hand, personal network analysis starts with an individual - called ego - and studies the relationships this individual has with other people - called alters. Many researchers refer to the networks formed from the ensemble of this relationships as *personal networks* or *ego networks* [8,9,10]. On the other hand, social network analysis studies the relationships existing between people inside a bounded population or community (e.g., researchers community, movie directors community, etc) [11,12,13]. Whilst social network analysis puts more emphasis on the key features of the whole network (e.g., topology, centrality, etc), personal network analysis focuses on the relevant features of ego's social relationships.

Human ego networks formed "outside" the OSN world has been deeply investigated and some of the key features of these networks have been identified [14,15,16]. Ego networks are considered important as they determine the properties of social networks from the standpoint of the single individuals. In particular, "tie strength" - the importance of the social relationship between two individuals - is found to be one of the most important features of ego networks and it is what makes social networks really "social" [8,17]. Indeed, tie strength has shown to play a key role in the study of both types of social networks. For example, previous authors demonstrated that tie strength plays a central role in the diffusion of information between people in social networks [8,13,24].

Studies on the properties of OSN are becoming increasing popular, as there is still lack of understanding of their key features, and of their impact on social relationships between individuals. Some authors recently studied the properties of the entire Facebook network, considering all the unweighted links existing between individuals [18,19]. Some work has been done to analyse OSN characteristics from the user's point of view [20]. Other authors studied the influence of OSN on the "social well being" [21,22]. Although the work done so far evinced many important aspects of OSN, the relation between the social behaviour of users and tie strength in virtual environments has not been fully discovered yet (initial results have been presented in [28]). Estimating the strength of social ties is clearly important for a number of social aware services, such as data dissemination, community detection, etc. Unfortunately, direct measures of social ties - i.e., quantitative measures taken without explicitly asking individuals - are not possible neither in human social network nor in OSN, as tie strength depends also on emotional factors that are not directly measurable. Nevertheless, using interaction variables - such as the frequency of contacts - has proven effective in estimating tie strength in human social networks [16]. This approach has still to be fully explored in OSN.

In [8] Granovetter proposes a definition of tie strength based on the combination of the amount of time, the emotional intensity, the intimacy and the reciprocal services which characterise the relationship. The author also identifies a first distinction between the different properties of strong and weak ties, with the former being useful for emotional and financial support and the latter for the acquisition of new ideas coming from groups of people socially far from ego. This distinction has been confirmed by many experiments performed on different types of social networks [11,13,24]. Our results indicate - through a rigorous analysis based on PCA techniques - that the composition of tie strength in Facebook in terms of factorial dimensions is similar to that found in human ego networks [8,17].

In [25], a first detailed characterisation of tie strength in human social networks is derived using an analytical model. The results of this work evinced the presence of two main dimensions of tie strength, having to do with the time spent in a relationship and the "depth" of the relationship. Moreover, the results indicate that "emotional closeness" or "intensity" of a relationship are the best indicators of tie strength and the frequency of contact only partially explains this concepts. Despite this relevant finding, many authors consider only the frequency of contact as tie strength estimator [13,24,27]. Moreover, other authors do not take tie strength into account to analyse OSN properties. For example, recent papers presented an analysis of the properties of Facebook entire network, considering all the unweighted links existing between people [18,19]. The results presented by the authors of these papers indicate that the average distance between any two people in Facebook is 4.74 links. This means that information circulating in Facebook could reach any arbitrary users in, on average, less than five jumps. From this perspective, it seems that Facebook is forcing the famous "six degrees of separation", empirically confirmed in human social networks by the Milgram's experiment [26], to become five, or even four in virtual environments. However, as these studies do not take tie strength into consideration, the actual behaviour of social aware services might be different, as tie strength plays a significant role, for example, in determining the trust between individuals and thus the willingness of cooperating.

#### 4.1.1.1 Extracting and Understanding Data from Online Social Networks

Some research work has focused the attention on the possibility of deducing social tie strength from OSN data [23]. The idea of the work in [23] is to validate the findings in [25] using Facebook data to estimate tie strength. A model is built from a set of explicit evaluations of tie strength collected with a survey distributed to participants of the experiment. Some limits of such approach can be ascribed to the presence of too many variables in the regression model, which can lead to overfitting. Moreover, the model presented in [23] is not tested on a test set and its predictive power remains unknown.

Work in [28] attempted to address some of these issues, by analysing the properties of several interaction variables from a Facebook dataset. This initial analysis has shown remarkable similarities between the shape of the distributions of interaction variables (messages, posts, like, etc.) and the typical shapes of tie strength indicators in human social networks. This suggests that similar properties can hold in both types of networks. A detailed investigation of this subject is currently ongoing.

Breadth First Search (BFS) and Depth First Search (DFS) are two social data extraction techniques, described in Cormen et al. [70]. In both techniques the graph is crawled node per node adding all discovered nodes to a list of nodes to visit. The difference between BFS and DFS is based on the procedure of how the next visited node is selected. In BFS the first node of this list is selected to be visited next and removed from the list, whereas in DFS the last node in the list is selected and marked as visited. Both techniques are leading the crawling procedure towards the inner core of the network due to the friendship paradaxon. This paradoxon, first observed by Field [71] states originally that your friends having more friends than you, will force a crawl towards nodes having a high centrality in the network. A related effect, noted by Kurant et al. [72] describes that BFS and DFS are introducing a bias towards high degree nodes for an incomplete traversal of the network. Some recent work has also introduced new methods of collecting social data, such as the snowball method [68] which creates bias subsets, or incremental community-driven sampling, such as mutual friend crawling [69], used for steered data collection.

One of the fundamental issues for extracting social data from the Internet is how to capture and analyze terabytes of data from the network in a scalable manner. In certain cases, it is mandatory to extract information from the network traffic itself. On the one hand, there is the issue of capturing high-speed data (10 Gbps) and, on the other hand, it has to be captured in a hard disk and subsequently analyzed. A high-speed driver has been developed that allows capturing more than 14 million packets per second with no loss [65]. In combination with well-known standard RAID cards it is capable of dumping data to hard disk at more than 8 Gbps. This allows building a traffic sniffing and data repository on Commercial Off-The-Shelf hardware, which is very benefitial in terms of cost and scalability.

It is also worth mentioning that GPUs (Graphical Processing Units) are gradually being adopted as co-processors for data analysis. As it turns out, such devices allow massively processing network data in

parallel and they are very cost-effective. Actually, the GPU market volume is huge (they are mainly used in the video game industry) and the economies of scale are significant [66].

There are many examples of data mining techniques using GPUs. In all of them there is a gain in speed and power efficiency, at a relatively low cost when compared to traditional grid computing approaches [67].

### 4.1.2 Open Government Data and Civic Hacking

Increased transparency of public and private bodies and wider democratic participation by citizens represent key challenges that can be faced within new models of interaction enabled by the Internet. For instance, the (potential) 'data deluge' from Public Administrations, corporations and social streams calls for the participation of virtual communities of actors that cooperate on making relevant information meaningful and further disseminate it, also by mixing and linking data streams from different sources. Such 'civic hacking' initiatives allow citizens to be better informed on preminent issues - from the way governments use incomes from taxes to the carbon footprint levels in a given geographical area - supporting participation and better decision-making. Indeed, analysing the functioning role and potential obstacles hindering the work of such communities seems particularly interesting [1]. Relevant research from Benkler [2], Lessig [3] and Ostrom [4] - just to mention a few well-known contributors - highlight the role of cooperation and the ways cooperative behaviour can be (self-)governed and enabled, especially when dealing with a common pool of resources and, in particular, with information commons in a digital environment. Other recent research covers different possible frameworks of reuse of Public Sector Information (Open Government Data). However, some more specific aspects specifically related with civic hacking initiatives grounded on cooperative reuse of (Open) Data by virtual communities are anything but played out. Some important research threads are: (i) the 'democratization' of the so-called Big Data, so that communities can access and re-use data with transparency-oriented purposes; (ii) the openness degree - under a technical and legal viewpoint - of the data supplied by private and public sector bodies [5], [6]; (iii) the systems of 'checks & balances" to be adopted within communities that better enable 'civil hacking' activities to reach their full potential [4].

### 4.1.3 Governance and self-organisation as examples of social entrepreneurship

With the increasing consumer-citizen use of the Internet, new services and new business models have been created for those users [29-31]. There are many user-created environments in which bottom-up rules have claimed to be set [32]. Their regulatory effect is voluntary and not supported or recognised by government [33-35], the closest approach being 'acknowledgement' that they exist [36], neither a vote of support nor a condemnation. Some display far greater responsiveness to empowering users to create and regulate content, using Social Networking Sites (SNS) and virtual worlds as well as mash-ups and other techniques collectively constituting the Web2.0 phenomenon. Some offer increased security and protection from harmful content for users who desire, or in any case receive, 'walled

gardens' less open Internet experiences. Examples include proprietary platforms: games console and many mobile networks.

Difficulties with self-organisation include variously: user inertia to default settings; the decision by e-commerce providers to make websites almost impossible to use selectively for average users; and 'The myth of the super-user', the belief that users are technically competent and will self-select [37-38]. The economic fundamentals driving Web2.0 are that broadband has become ubiquitous for many. With UGC, the user is enabled to 'pull' content and even adapt and mix content into a 'mash-up'. A mash-up is a combination of existing media reworked into a new and innovative type. An example might be remixing music tracks, or the integration of maps into classified directories that GoogleMaps performs. 'Data mashing' makes innovative 'recombinant' uses of existing media, e.g. remixed music tracks or the integration of maps with other information. Examples of Web2.0-type applications are varied:

1. P2P sharing networks (such as *KaZaa* and *BitTorrent*);
2. Photo-sharing sites (such as *Flickr*);
3. Video sharing sites (such as *YouTube* and *DailyMotion*);
4. Online games (such as *World of Warcraft);*
5. Public SNS (such as *MySpace, Facebook* and *Bebo*);
6. Blogs and Wikis, including *Wikipedia*, a user-generated encyclopedia and *WikiLeaks*, a whistleblowers' site;
7. Executive SNS such as LinkedIn and ASmallWorld.

The range of SNS is broad, but easily divided into those that are open to anyone, and exclusive 'walled garden' invitation-only sites. In terms of UGC, we can distinguish online games from the more interactive virtual worlds, the former generally making modifications to a mass media gaming software package, the latter involving modification including writing of new code for the 'virtual world'. Blogs and Wikis are collaborative author tools which are largely UGC. The regulation of these systems takes place at corporate and user level, in the same way as Usenet sites were first regulated in the early 1990s [39-40]. That does not mean that there is no innovation in their regulatory structure: virtual worlds, for instance, have built up elaborate self-regulatory models.

Media sharing services are not communities as such, and there is less interaction between members and therefore little regulated behaviour specific to the networks, except copyright and other unauthorised or inflammatory content that is subject to Notice and Take Down (NTD). I show the various types of social network modeling against their commercial or public (as opposed to private) characteristics.

Social networking on the Internet did not begin with Web2.0 and note bulletin boards (Usenets, which have a long history, substantially predating the formation of the IETF) and Intranets predate the commercial Internet. P2P programmes have carried advertising in the past, notably Kazaa. Note that professional networks such as LinkedIn, and monetized virtual world 'SecondLife', are more

professional in character than advertising-driven mass market social networks and aggregation sites, such as Bebo or YouTube. Blogs are predominantly non-commercial in character, though those with highest readerships may syndicate advertising. It is clear from the description of the number of users and viewers of SNS that, as a mass phenomenon, it would not be possible to regulate the posters of content directly. On the Internet, as earlier discussed, the content host (typically an ISP but not in these cases) is subject to a NTD regulatory regime. This does not require *ex ante* regulation, but does require content hosts to 'take down' users' content which they have been informed (given 'notice') either breaches law or otherwise offends against their terms of use. There is thus a shift of liability. ECD provides for clarification of the applicable liability regime to internet intermediaries (with no strict liability), sets out the exoneration conditions for certain types of intermediary activity (transmission and/or storage of third party content) and does not affect the liability of the actual content provider (which is left to national law). The host's limited liability is to ensure that users are only able to use the service under conditions or terms that explicitly permit the content host to take down material that is illegal, often extending this power to material that is offensive, of an unsuitably adult nature, and so on.

Take the example of video-sharing site, YouTube. On YouTube, the editorial controller, if such exists, is the person who posts the content. For regulatory purposes, YouTube users post the content and the YouTube website reacts *ex post* on receiving complaints regarding breaches of copyright or offensive content [41]. This is fundamentally different to traditional broadcast regulation, where the editorial controller (the broadcaster) is responsible for the content *ex ante* – before it is offered to the public. While it is true that opportunity presents problems and solutions [42], it also allows for what I term 'Regulation 2.0', mass user self-regulation via Web2.0 tools to report abuse, flag and label content. SNS have membership and usage rules, which entitle them to suspend or expel members accordingly. Members can report and even rate the content or comments of others. There is substantial self-policing by residents of these communities.

The self-regulatory approach of 'virtual worlds' is worth consideration as an alternative to the *ex ante* broadcast/*ex post* Internet regulatory distinction [43-44]. In an online game, it is possible for the administrator to respond to inappropriate behaviour by a member by the online equivalent of a community punishment [45]. The alternatives to direct enforcement are: to rely on a form of indirect liability against content hosts, and to reply on the media literacy and self-policing of online communities, whether YouTube or Second Life. Enforcement can only be undertaken successfully by the content host. Mayer-Schonberger and Crowley [44] see four scenarios for virtual world regulation:

1. Virtual world providers will serve as regulators by enforcing the terms of their contracts with users to prevent cyber-fraud and ensure proper behaviour,
2. Governments could try to block their citizens from using virtual worlds that don't abide by government restrictions and regulations (although this will never be 100% effective, just as governments have not been able to completely block access to Web sites),
3. Government may try to minimize the real-world impact of virtual worlds by, for instance, banning the sale of virtual goods for real-world currency, or

4. "Real-World Assisted Virtual World Self-Governance," governments provide support for mechanisms where by users of virtual worlds can agree upon and enforce their own "community standards" and rules of conduct.

Richter has recently compared types of social entrepreneurship as regulatory techniques [46-48], in a pioneering approach to self-organisation as a "solution from outside the regulated environment through entrepreneurship and innovation, and relies on the forces of the market to become effective" [49]. He explains that social entrepreneurs can be more effective and more efficient than regulation (or else go out of business) [50], but that "Further efforts are required to ensure participation, transparency, and public accountability, and to avoid regulatory fragmentation" [49]. Social entrepreneurship as a tool to regulate has only recently emerged as part of the Third Sector [46], or Big Society approach to private provision of formerly charitable or state activities [51]. In 2005, the British government's Office of the Third Sector allowed for the Community Interest Company (CIC) with a regulator [52]. Richter argues that "the existing framework of social entrepreneurship can be extended to entrepreneurial organisations providing innovative and market-based solution to environments in which regulation and market self-regulation have failed to provide a social good" [49]. This separates them from non-business policy entrepreneurs [53-54]. Spear and Bidet state: "The entrepreneurs are citizens, not the state, the decision-making power is not based on capital ownership, the participatory nature involves those affected by the venture, profit distribution is limited, and finally the venture explicitly aims at benefiting the community." [55] Social enterprises can be Type 1 (local) or Type 2 (macro) according to Nicholls [56], with the Fair Trade movement a classic established example of the latter. Richter states that "production of social value with market-based solutions and entrepreneurial innovation are sufficient to differentiate social entrepreneurship from profit-maximising models of entrepreneurship, from philanthropy, from institutionalised and state-backed forms of civil society engagement, from CSR, and from policy entrepreneurship [49]".

As Richter states [49], there are three governmental approaches to encourage social entrepreneurship, to cooperate in problem and solution definition as might be argued was the case with CC-Brazil and involvement of Minister Gilberto Gil, as a customer for such solutions as in OCL models which I described as 'Regulation 2.0' [57], and finally the creation of a market for social entrepreneurship as with the UK CIC, where the "market regulator should develop and enforce minimum standards for transparency, accountability, and participatory solution design, create an arbitration panel for citizen complaints, encourage independent performance reviews, and push for the interoperability of solutions to preserve competition [58]". He also argues that in the absence of a CIC regulator, "legal logic under *Marsh vs. Alabama* [59] allows the application of basic constitutional rights to private providers of public infrastructure and could also be extended to require transparency and due process rules for the private regulatory activities by Creative Commons"

Whether one agrees with Latzer that it is 'self-organisation' - there being no multiparty self-regulatory body - or side with Price and Verhulst in terming it self-regulation [60], there is a particular feature to a single corporate policy negotiated internally rather than through external discussions. First, it is not transparent inasmuch as self-regulation may be so. Second, it is conducted for internally validated

reasons: a mixture of profit-maximisation via brand enhancement (making the product distinctively better regulated than others), via corporate governance (performing pro bono socially beneficial duties as a means to securing corporate distinction), or because as monopoly or oligopoly player, it is in a position to rule-make rather than rule-take vis-a-vis its competitors i.e. it is not obliged to conduct a 'race to the bottom' in welfare terms. This leaves to one side the unusual category of social entrepreneur, a regulatory actor of such obscurity that few academics have investigated the phenomenon until recently [61-63]. In a commercial service, such as Facebook, users have Terms of Use proscribed by the service owner. This is not a new phenomenon, except in the degree to which UGC is generated, and users consider the service owner's brand associated with that third party content. AOL's branded portal in the mid-1990s was the most successful site on the Internet, as Facebook is in 2011. The type of governance that applies to these organisations is either charitable status or corporate governance rules. For some, it is the legal status as a charity that its board of directors must observe, which provides a very low baseline of compliance [64]. Lessig offers a summary of the legal position of the iCommons organisation , as a UK charity with majority non-US citizens on its board [39]. In the case of corporate governance, the main obligation on the board of directors is the fiduciary duty to pursue the most beneficial course for shareholders.

## 4.2 *Trust and Reputation*

Trust and Reputation are "notions" borrowed by our social life to serve many critical Internet aspects from p2p communications [1-11], cooperation in ad hoc networks [12-14], data integrity and authentication in sensor networks [37-39, 47], web services' selection [15-25], to relationships and access control in social networks [26-35].

An extensive investigation of related research indicates that there are many definitions of "trust" and "reputation" and sometimes these terms are used interchangeably. However, most of the times trust is used as a subjective (local) measure of trustworthiness, while reputation is used to define the global trustworthiness of a user as perceived by all the users in the network, usually as an average of all users' opinions about the particular one. That means that a user may trust another one despite the latter's bad reputation.

### 4.2.1 Enforcing cooperation in P2P and ad hoc networks

In p2p networks, they have been extensively investigated to distinguish and avoid malicious peers by applying suitable provider selection mechanisms [1-3]. A lot of work [4-7] was also focused to provide simple incentive mechanisms to enforce collaboration between peers by controlling not only the provider selection policy but also the client selection policy. Reputed, thus contributive, peers are rewarded by receiving preferential treatment, while misbehaving peers are punished by not being served. Reputation-based allocation policies [8,9] have also been proposed to decide about the different levels of offered resources to different peers, in contrast to just decide whether to serve one peer or not, and to account for their different needs (expressed service demands). Reputation-based

incentive mechanisms have been proposed not only to foster cooperation among users of file sharing systems [4-6,9] but also of p2p grids [8], wireless neighborhood communities [10] and internet sharing communities [11] in a p2p fashion. The objective of the latter communities is to both provide free and good quality Internet access to its users anywhere inside it, and protect their home connection resources by letting them the allocation control. Many reputation-based incentive mechanisms have also been proposed for ad hoc networks [12-14] to motivate nodes to cooperate and forward packets on behalf of others in order to maintain a low packet latency and loss rate in the network.

#### 4.2.2 Helping consumers to take decisions over web services

Trust and Reputation systems also play a decisive role in consumers' decisions [15] over services provided in the Internet and several reputation systems have been employed by successful commercial applications in the Web, such as eBay's Feedback Forum [16], Amazon's rating system [17], etc. Reputation systems are also used in expert sites like AllExperts [18], AskMe [19] and Advogato [20] to rate the experts, in product review sites like Epinions [21] and BizRate, in discussion fora like Slashdot [22] and Kuro5in [23], and to support suppliers and subcontractors agreements, like Open Ratings [24]. PageRank algorithm [25] employed by Google search engine can also be seen as a reputation system since it ranks a page based on the number of hyperlinks pointing to it, which can constitute the reputation of the page.

#### 4.2.3 Trust and Reputation in web-based social networks

Trust and Reputation systems in web-based social networks have been used either for rating users' recommendations/reviews or for access control (e.g., which users in the network are allowed to access my data). As an example of the first category we mention FilmTrust [26] which is a website that provide movies' information based on a trust network. Users provide their reviews and ratings for films, and the website uses the reviews of trusted friends (and friends of friends) to display a custom rating for each movie to a user. Trust in this context also implies similar film tastes between users.

The approach that is most commonly adopted is that trust relationships are dependent on personal relationships; since two people may be affiliated in more than one way (e.g., friends and colleagues), there also may be more than one trust relationship between them, according to the context of their personal relationship. For example, user A may count on B as a loyal friend but not have confidence on his work. In the vast majority of social networks (Facebook [28], MySpace [29], Friendster [30] etc), a user cannot discriminate the type and the strength of the trust relationship with all other members of his network. Some web-based social networks, though, allow their members to (i) determine different relationship types with other users (the case of LinkedIn where different types such as "colleague", "classmate", "business partner" etc. are possible), (ii) determine how much they trust other members, creating different trust relationships. This can be done either by expressing recommendations (the case of LinkedIn [31]) or by grading others in different trust levels (the cases of Orkut [32] and RepCheck [33]). Orkut gives their members the ability to rate personal trust while

RepCheck allows for both personal and business trust. Works in [27], [34] and [35] denote authorized users in terms of the minimum trust level and maximum length of the paths connecting the requestor and the resource owner. Plus, work in [27] prevents forging of fake relationships by requiring that relationships are established only with the mutual consent of the involved members; moreover, it supports access control not only based on the trust level and length of paths connecting two nodes but also based on the type of their relationship.

On the other hand, social networks can be used to extract users' reputations, considering that most reputable users are the most highly connected. NodeRanking algorithm [36] deduces the reputations of users similar to the pagerank algorithm, with the difference that it uses the social network topology in contrast to the topology of the web page links. However, [36] depends on an a priori knowledge of the relationships between users on top of which the social network is built, which is usually difficult to acquire.

#### 4.2.4 Trust and Reputation for Sensor Networks

Trustworthy is defined in this context as: secure, reliable and resilient to attacks and operational failures; guaranteeing quality of service; protecting user data; ensuring privacy and providing usable and trusted tools to support the user in his security management [40]. This in turn includes requirements like security [41][42] and safety that also need to be carefully addressed in WSNs. Especially functional safety, which guarantees the detection and controlling of failures in a system to remain in a safe state [43][44][45] has to be part of a WSN concept, especially when this system should provide critical functions in unattended operation in hazardous environments, where no security perimeter is present. Current solutions in this area are self-tests [46] or reputation concepts [37-39], [47], which enable a sanity-checking of sensor data. While the reliability of sensor networks is always an important goal, the privacy of sensed data can vary heavily depending on the WSN's purpose. Environmental data can for example be publicly available, while data revealing personal information should only be accessible by very few individuals. An especially obvious case can be found in the area of wireless body area networks (WBANs), which are used for patient health monitoring. Here, methods like secure and dependable distributed data storage and fine-granular distributed data access control can be used to secure the privacy of the user [48] against unauthorized access.

#### 4.2.5 Shielding against Sibyl Attacks in opportunistic networks

This section was adapted from [72].
We believe that one of the emerging game-changing technologies will be opportunistic networks. These will change the way people communicate by allowing direct one-hop communications between handheld devices carried by human beings while on the move. Users will be involved in participatory interactions with their surrounding using applications (e.g., mobile social networking, content distribution [49], flea-markets, micro-blogs) enhancing the experience of real-world social networks

with digital and ubiquitous features. With these applications, users will publish their input or services (e.g. content, sold objects, blog entries) and subscribe based on their solicitations. Inputs will disseminate from their authors to consumers through relays in a delay-tolerant epidemic fashion from hop to hop using mobility without routing per se. While areas of operations are mainly developing countries, for no fixed wireless infrastructure is required, urban citizens will also enjoy a free and open network that made the success of the Internet at its early stage.

In the absence of a central regulating authority, infrastructure-based and hard cryptographic solutions are rarely available, and are often traded for threshold cryptography [50] or PGP-like chains [51]. One prevailing solution used to secure interactions between possibly unknown users is *trust*. For instance, it is often considered in recommendation systems based on ratings, where trust relies on (i) the service (or content) quality provided by others and (ii) trust in other users' opinions having similar taste. This trust, however, requires interactions between users in order to be established. What is more, pure opportunistic networks cannot ensure a one-to-one binding between an identity and a user. Compared to real-world social networks, their digital counterparts allow easily generating fake identities, known as sybil users [52]. These sybils can then obtain a higher degree of influence in the system. Trust must hence be considered at a more fundamental level. In this section, we consider the most basic level of trust that can and must be achieved in opportunistic networks, i.e., social trust: the belief that an identity is genuine and that the user's intentions are honest.

A sybil attack [52] describes the attempt to create many identities in order to gain larger influence in a reputation system, abandon bad reputation or evade responsibility of his/her actions. In order to detect such attacks, Piro et al. [56] observe that sybil users can only communicate serially and thus cause much fewer collisions at the MAC layer. SybilGuard [57] considers that sybil users have only a few trust relationships which can be highlighted by carefully observing the social graph. Location-based sybil detection is also an effective measure [58] but requires specialized hardware.

Reputation systems are ideal targets for sybil attacks [59], [60]. These systems rely on disseminated user ratings to enable informed selection of content by estimating a prospective source's reputation beforehand. Liars or sybil liars try then to influence ratings in the system about a user or a service. The similarity of direct and received ratings may be evaluated to assess trust in future opinions [61], [62]. To avoid the manipulation of ratings, Quercia et al. propose to store them in tamper-proof tables certified by witnesses [63], [64]. Since one cannot prevent users from generating multiple identities, one way to limit the influence of sybils is to proactively establish trust in the identities being genuine. In classical networks, trust is established by a certificate authority (CA) through a public key infrastructure (PKI) [65]. In a pure opportunistic network this approach is useless since no fixed infrastructure and thus no authorities can be assumed. The CA duty can, however, be distributed to nodes which can generate their own credentials and sign certificates of others when paired. Following this track, Capkun et al. [66] allows users to build certificate chains similar to PGP under the assumption of unconditional transitivity of trust along the chain paths. Other approaches limit trust exclusively to consciously selected friends [55] (non-transitive) or small groups [67].

Besides crypto-related approaches, trust establishment can leverage mobility properties and network structures using the rich set of complex social network tools. For instance, community detection algorithms extract the underlying structure with the highest modularity when fed with a network topology [68], [69], [70]. Distributed versions for opportunistic networks such as proposed by Hui et al. [54], [71] classify users in different categories, e.g., friends, familiar strangers, and strangers. Each category can be assigned different trust values, for example in order to choose trustworthy forwarders in DTNs. This approach, however, defines strict categories and was not designed with security in mind especially against sybil attacks.

## 4.3 *Identity and Privacy*

The increasing number of social network users, as the emergence of large data farms for cloud computing services or the design and implementation of complex architectures of sensors and devices, permit to collect a huge amount of data concerning identified or identifiable subjects. In many cases the informational power that is related to these databases is in the hand of a limited number of entities, big private companies or governments. This concentration on power is due both to the role that the subject assumes in the data flow and to the availability of technical and human resources for the analysis of the information.

From this point of view, considering the existing relationship between big private companies and governments, it is evident that identity, trust and privacy should also be considered taking into account the possible consequences in terms of social control and the effects of solutions of trusted digital identities on individuals and groups.

The EU proposal for a General Data Protection Regulation offers some means to protect individual privacy, although it does not seem counteracting effectively the existing asymmetry between the data subject and the owner of big data. Possible measures to reduce these risks may arise from the adoption of privacy by design techniques, but it is also necessary to reflect on a global agreement, at an international level, in order to control and limit the informational power that derives from mass data collecting and data mining. From this perspective an interesting research thread is represented by the analysis of the relationship between social control and digital identity, in order to define the existing risks and the possible solutions.

### 4.3.1 … in Online Social Networks

The recent boom of social networking platforms has lead to a dramatic shift in how people behave, spend their time and interact with others, but it has also opened new venues to mine, and potentially misuse, information about ourselves and our lifestyle. Activities of users and their interactions with their friends are for example now analyzed to obtain personal profiles, which can be used for marketing activities, but also help companies determine whether a customer can be deemed “influential” and should consequently receive a better treatment than others [20]. Information on relationships, personal habits and interests can be taken into account when assessing risks and rates

when applying for health insurance [21], and face recognition performed on photos stored in online social media allows the re-identifications of persons in other contexts, such as identifying passerby's in camera recordings to deliver targeted billboard advertisements [22].

In consequence, much research has recently started to identify issues related to how information is leaked by social networks, which dangers for privacy exist, and how it is possible to maintain privacy. Gross and Acquisti [23] analyzed patterns of information revelation in OSNs and privacy implications in the "early" stage of Facebook. An amazingly high number of 89% of users in their dataset provided their real name. Other attributes like phone number, birthday, home town, address etc. were also given by the majority of the users. Different techniques to infer private information like reidentification of users by analyzing the postal code and their birthday are presented. Face re-identification to identify users on different sites or even identity theft of the users social security number was shown to be feasible. The basic information provided by the user (normally picture and name - information requested by most social networks) is enough to identify a person [6]. A solution based on "Virtual Social Networks" has been proposed in [9].

The role of third party sites in tracking users of OSNs and obtaining private information is investigated by Krishnamurthy and Wills [24, 25]. In most cases, a user has no possibility to control all applications that track profile data. Users are not aware which data is accessed by them and what the different services do with this data.

The possibility for involuntary personal information leakage in current social networks is highlighted in [37], e.g. by means of certain OSN features like annotating or tagging user photos, and its effects are demonstrated in [34]. Even though very few OSN users (only 6% [44]) trust strangers with their personal information, operators allow strangers to access a user's profile; e.g., Facebook allows any application developer to access a user's profile.

Apart from the social network providers, the users themselves may undermine the privacy of other participants, e.g., when their common contacts have to be exchanged [1,3,5,7,8]. Multi-Party-Computation techniques are especially relevant, when thinking about the arising paradigm shift that leads from a direct bilateral communication between individuals to a communication structure involving an un-trusted third party. This party is able to generate large amounts of personalized information using data mining algorithms. Because of that, it is required to develop and also implement privacy preserving mechanisms into the currently omnipotent social networks [6, 10].

Lockr system [38] improves the privacy of centralized and decentralized content sharing systems. It allows users to control their own social information by decoupling the social networking information from other OSN functionality using social attestations, which act like capabilities. However, these social attestations are used only for authentication and authorization is enforced using separate authorization policies. Persona [39] uses attribute-based encryption to realize privacy-preserving OSNs. The attributes a user has (e.g., friend, family member, colleague) determine what data he can access. The NOYB approach [33] adopts a novel approach for preserving content privacy. They

observe that if users address their privacy issues themselves by hosting encrypted content on OSNs, they could be expelled from the OSN by the OSN operator. Hence, they propose to replace users profile content items with “fake” items randomly picked from a dictionary. NOYB encrypts the index of the user's item in this dictionary and uses the ciphered index to pick the substitute. On the other hand, flyByNight [40] encrypts the users' content that hosts on the OSN.

Because of the knowledge about friendships in OSN and the fact that those relations are mostly built between individuals having similar interests it is still possible to infer private attributes of a user from his friends even if the user has a profile which is not visible to everyone. McPherson et al. [26] discussed “homophily” as a concept that limits individuals to connect only to others having similar attributes. The strongest divisions are based on race and ethnicity followed by age, religion, education, occupation and gender. Hence, ties between non-similar users are either not constructed or dissolve at a higher rate. This leads to social niches in the social space.

He et al. [27] constructed a Bayesian network assuming that direct neighbors have a higher overlap than users multiple hops away. It is shown that privacy can be indirectly inferred via social relations and mathematically over multiple hops. He et al. use an influence strength which is defined as the conditional probability (P(A|B)) that user A has an attribute given a friend (B) has the same attribute. By using friendship information and group attendance information, Zheleva and Getoor [28] showed for different OSNs that it is possible to infer private attributes using group and friendship information. Blenn et al. [29] further demonstrate that it is feasible to reconstruct large parts of private profiles from social networking sites; in consequence the current practice of privacy protection by obfuscation needs to be reevaluated.

It is evident that the term “privacy” lacks a clear definition in social networks. What is even more daunting is that even if a definition is used, it is impossible to explain user disclosure practices on social media [45] or why they are against a certain Facebook innovation, but never change their settings accordingly [46]. In order to better understand what users are doing in terms of disclosure on social media, we need to expand our scope to trade-offs that influence disclosure decisions beyond privacy. Christofides et al. found that popularity was a more important driver to disclose personal information [47]. Social media (and web related services in general) are not using adequate measures to inform users [48]. They are in fact nudging uses to neglect informing themselves and changing privacy settings accordingly [49]. These design decisions are commercially motivated because targeted advertising is the biggest (and usually only) revenue stream of social media.

As described, it is usually vague to identify which data are sensitive and how they could be protected. In addition, the type and origin of the adversarial entities can be misleading. Consider the following example, where the social network provider (Facebook) is a semi-trusted party, acting as a relaying between the users and additional third parties. Facebook can play the role of both the social network and platform provider, while Zynga plays the role of the third party using Facebook's platform to offer games. The users do not want their data to be sent on not fully-trusted entities like Zynga; however they have to provide some data like their name and friends that play the game in an unmodified state.

On the other hand, Zynga has to rely on Facebook that it will provide the authentic data in order to offer the users their expected experience. In this example, Facebook is not considered adversarial, but a semi-trusted third party [2] in the sense that it does not conspire with either of the users or Zynga.

#### 4.3.1.1 Privacy Preserving of OSNs in a p2p manner

Recently, the issue of using decentralized infrastructures for organizing OSNs in a privacy-preserving manner, was addressed by the research community [30], [35], [41], [31]. PeerSon [41] adopts encryption mechanisms for content storage and access control enforcement. It uses a two-tier architecture in which the first tier is a DHT, which is used as a common storage by all participants. The second tier consists of peers and contains the user data. The DHT stores the meta-data required to find users. Peers connect each other directly, exchange the content, and then disconnect.

[35] addresses privacy in OSNs by storing profile content in a P2P storage infrastructure. Each user in the OSN defines his own view ("matryoshka") of the system. In this view, nodes are organised in concentric rings, having nodes at each ring trusted by the nodes in its immediate inner ring, with the user node being the center of all rings. The user's profile data is stored encrypted at the innermost ring, which is accessed by other users through multi-hop anonymous communication across this set of concentric rings. In the DHT, an entry for a user with the list of nodes in the outermost ring is added. Thus, [35] achieves both content privacy (using encryption) and anonymity of searcher and hosting nodes, yet limited content discovery and profile availability.

In [30], a decentralized OSN, Vis-a-Vis is proposed, where a user's profile content is stored at his own machine called as virtual individual server (VIS). VISs self-organise into P2P overlays, one overlay per social group what has access to content stored on a VIS. Three different storage environments are considered: cloud alone, P2P storage on top of desktops, a hybrid storage, and their availability, cost, and privacy trade-offs were studied. In desktop-only storage model, a *socially-informed replication scheme* was proposed, where a user replicates his content to his friend nodes and delegates access control to them. However, normally, a uses trusts only a fraction of his friends to the extent of delegating access control enforcement.

In [31], a decentralized OSN infrastructure is proposed organised over a P2P overlay. Users delegate access control to their trusted friends, while profile replication is employed for improving availability. Different profile placement algorithms have been proposed based on different criteria and profiles are indexed by a privacy-preserving DHT [panacea] for data searchability.

Tribler [42] is a P2P file sharing application which exploits friendship relationships, tastes and preferences of users to increase the performance of file sharing. However, in Tribler, users host their own profile and therefore profile placement for high availability and low access or consistency cost are not considered. Finally, LifeSocial [43] is a P2P-hosted OSN where users employ public-private key pairs to encrypt profile data that is stored in a distributed way and is indexed in a DHT. Friends can read a user's profile based on a symmetric key that is encrypted with their public keys.

#### 4.3.2 …in Internet of Things, clouds and sensor networks

The "old" Internet, where data were mainly provided by single servers (machines) and used by clients (humans) is currently undergoing several drastic paradigm shifts, triggered by the numerous advances in fields like miniaturization, internetworking as well as cost-effective production of devices. New concepts have been originated from cloud computing to the Internet of Things as well as intelligent wireless sensor devices that are integrated into the global network and provide environmental data not only to human clients, but also to each other, to autonomously achieve an added value. In the following we briefly discuss the identity and privacy issues that have been arisen with the advent of each of these technologies.

**Internet of Things**: RFID and similar tags are becoming ubiquitous in logistics, access controls and a wide range of other applications. There has been some research into privacy-friendly tags, which can only be read by those possessing the appropriate cryptographic keys [11, 12]. There has also been some consideration of public policy options to encourage the adoption of such systems, including the use of European codes of practice [13] and other regulatory options for protecting privacy in remotely-readable tag systems [14].

**Clouds**: Consumers, businesses and government agencies are making increasing use of remote storage and computing resources over the Internet. Where personal data is being stored or processed, this can raise significant privacy issues. Research has focused on improving the security of "cloud" servers using techniques such as strongly enforced virtualisation [15]; and on allowing encrypted data to be processed, reducing the ability of server administrators or intruders to access original data - although it seems that this approach has some severe limitations [16].

**Sensor networks**: Tiny low-powered sensors and actuators are becoming increasingly pervasive in all kinds of environments, both dedicated (e.g. pollution detectors, heart monitors) and contained in more general-purpose devices (such as smartphones). The "Safeguards in a World of Ambient Intelligence" project defined a number of "dark scenarios" that imagined how this technology could develop in ways that damage social values such as privacy and trust [15], as well as legal safeguards to prevent these scenarios from coming about [16],[17].

### 4.4 *Semantic Networks*

Semantic (overlay) networks (SON) [1] extend on the idea of clustering related data in a structured overlay network for efficient retrieval. We assume that the semantics of information objects, either structured data or unstructured content, are given by a model that allows to express semantic proximity, i.e., whether two objects have a similar meaning. This model is given by mapping of the information objects into a metric space, in which the distance function captures the semantic proximity. Resources and interests of nodes can then be equally modeled as points or regions in such a semantic space. The overall goal of constructing semantic networks is to extend or modify an overlay network structure, such that semantic locality is achieved. As a result, nodes with similar resources or

interests are better connected. This has two effects. Nodes can find more likely content relevant to their needs in their immediate neighborhood. And when searching for a specific type of content, the results tend to be clustered in a region and can thus be more efficiently retrieved. The notion of semantic networks applies to Semantic Web, Webforms/ Linked Open Data, Web Trust, semantic mapping, and more.

According to [1], different types of features can be used to characterise the semantics of a resource, as follows:

1. Categorization. Resources are assigned with one or more predefined categories. The categories can be application-specific or be taken from some general-purpose classification schemes or ontologies.

2. Full text description. Resources are annotated using a full text description. The semantics of such a full text description is usually derived from the statistical features of the text such as the tf-idf measure used in full text retrieval.

3. Multimedia features. If the resources consist of media files, such as image or audio, feature vectors can be extracted using content analysis tools.

The concept space may exhibit some additional internal structure. The two most common cases found for the construction of semantic overlay networks are:

1. Flat concept spaces. They exhibit no internal structure.

2. Hierarchical concept spaces. Organise the concepts in an hierarchical structure, either a tree or a tree with some additional relationships such as terminological relationships.

More general internal structures such as lattice structures or general graph structures can be envisaged but have so far not been adopted in the construction of semantic overlay networks. Finally, and most importantly, the concept space is equipped with a similarity function that measures the semantic similarity of two concepts and is at the heart of creating an overlay network structure with strong locality properties.

We find the following two basic classes of similarity functions among categories:

1. Boolean similarity function. This type of function can only distinguish whether a given concept is present or not. Though simple, it is used in some cases.

2. Real-valued similarity function. This type of function assigns real values in the interval [0, 1] to pairs of concepts and enables a rich structuring of the concept space. From the similarity functions for single concepts, in general, similarity functions for concept sets are derived. For the case of boolean similarity function, this may result in more complex similarity measures for concept sets.

When using flat concept spaces [2, 3], the similarity among two concepts c1 and c2 degenerates to the equality function, such that sim(c1, c2) = 1 iff c1 = c2, i.e., a Boolean similarity function. For sets of concepts, related, for example, to collections of queries or resources, a profile can be derived by constructing the frequency distribution of the concepts in the sets. Similarity among concept sets can then be computed similarly as similarity for term frequency vectors in full text retrieval using the cosine similarity measure.

Hierarchical categorization has been widely used [4, 5, 6, 7]. The hierarchies are taken from domain specific ontologies, e.g., the ACM topic hierarchy, generic ontologies, such as Wordnet, or one of the abundant hierarchical categorizations found on portal sites on the Web. With hierarchical categorization, the problem of determining the similarity among two concepts becomes more complex. Sophisticated methods are used to define similarity of concepts by exploiting the hierarchical structure of the concept space. Examples of such measures are shortest path distance, weighted path distance, GM distance (relies only on the height of the concepts in the hierarchy) [50]. For comparing the set of concepts related to a query Q with the set of concepts related to a peer profile R, the similarity metric in [5] can be employed. Additionally, for comparing profiles of different peers, the similarity function in [8] can be applied.

Concepts extracted from text or media files are usually represented as vectors in high-dimensional feature spaces [8, 9]. Similarity among concepts is then computed in the simplest case as the cosine similarity among the feature vectors. More sophisticated similarity measures are found in particular for text retrieval, such as generalized tf-idf measures or similarity measures based on language models [10].

According to [1] the approach to constructing a semantic overlay network is to a certain extent orthogonal to the choice of the concept space and its similarity metrics. A first distinction can be made with respect to the criterion used to establish links between peers that are semantically close, i.e., the semantic clustering strategy. Three main approaches can be distinguished here.

1. Interest-Resource clustering. Peers create preferably links to peers that hold resources of interest to them, typically to peers that have provided useful answers to queries earlier. As a result, peers can more easily find relevant resources and peers with common interest profiles tend to cluster around peers holding related resources.

2. Resource-Resource clustering. Peers create preferably links to peers that hold similar resources. As a result, peers with similar types of resources tend to cluster and access to resources of a specific type is localized and thus more efficient.

3. Interest-Interest clustering. Peers create preferably links to peers that have requested similar types of resources the peer is interested in. In this way, peers obtain links to recommenders that might be particularly knowledgeable where to locate specific types of resources.

A second distinction can be made with respect to the mechanism that is used to create the semantic overlay network. Here we can distinguish two main classes of approaches:

1. Protocol-driven overlay network creation. The connectivity of an existing, typically unstructured, overlay network is augmented or modified through protocols that implement preferential attachment to peers with related interests or resources. In this way, initially unstructured overlay networks are gradually transformed into increasingly structured overlay networks that cluster semantically related peers.

2. Mapping to a structured overlay network. The concept space is mapped to the identifier space of a structured overlay network, by preserving the proximity of semantically close concepts. This assures that semantically related peers are clustered with the structured overlay network. With this approach, the structure of the semantic overlay network is explicitly specified and structural properties and performance characteristics can be given.

## 4.5 *Economic Perspective*

The economic perspective considers the implications of "network externalities" on economic outcomes (including innovation), the importance of specific interaction structures for trading, communication and other outcomes, and the competitive and efficiency consequences of (primarily physical) transportation, energy and communication networks. There is a growing field of research between economics and network theories [10]. Innovation networks have been studied extensively in modern economics, in particular in fields as institutional economics and evolutionary economics. Empirical observations show the role of collaboration in R&D driven industries in innovative sectors such as biotechnology [11]. Knowledge becomes embedded in networks rather than remaining an exclusive resource for some economic players [12]. Networks of interaction create a new specific locality between firms. From an economic point of view, the question arises, how "neighbourhoods" in knowledge exchange networks and "neighbourhood" in a geographical sense are related to each other. It has been discussed widely that the "death of the distance" is a myth and that regional innovation systems do play a role even in a globalized economy where internet seems to make local encounter superfluous [13]. However, interestingly there seems to be a correlation between hubs of Internet traffic and clusters of innovative firms [14]. The emergence of the Internet both enables and requires new forms of collaboration. As an example, the structure of large scale collaboration in software development (around the globe) has been discussed from a complex networks perspective [15]. While there is in general an emphasis on the surplus resulting from economic networks, it is also evident that collaboration does not come without costs. In some cases this cost-factor can even lead to a breaking down of networks (dying and not evolving, growing networks) [16].

### 4.5.1 Background

In a technical sense, the internet is a network, allowing transportation of data in between different physical locations. This technical development, the emergence of computer networks and the internet

in general, not only had revolutionary implications on the telecommunications domain, but changed our everyday life drastically. Telecommunication networks and connectivity have influenced the way people communicate, look for information, spend their free time etc.

Indirect effects are effects for one actor, caused by actions of another actor. General examples include air pollution (negative indirect effect) or the effect a large investment project can have on national employment rate (positive indirect effect). Specific indirect effects resulting from the presence of a fast and stable internet connection are for instance e-Health services that make sure that elderly can stay longer at home, e-Government services, which result in large savings in the administration expenses of a city and many more. Indirect effects also include network externalities, i.e. when the advantage of subscribing to the service or buying the good increases when the number of users becomes higher (e.g. the telephone network: the more people owning a telephone, the more valuable the network becomes to all) [1],[2].

Although it becomes widely accepted that these effects have a (positive) influence on society, they are usually not taken into account when investigating cost-benefit analyses of deployments of new and faster internet networks. This section will identify the most important effects for the sectors of society under influence, and give first quantification results from previous literature studies.

### 4.5.2 Identification of sectors, services and effects

Getting to a good and complete overview of all important effects requires a systematic approach of identification. Starting from the society as-a-whole, different sectors that can be influenced by the internet, should be enumerated: eBusiness, eGovernment, eHealth, eEducation and eEntertainment. Note that the "e-" is included in every sector, indicating the implicit changes caused by the presence of a fast and stable broadband connection. Also, note the "fast and stable broadband connection" definition instead of purely referring to "the internet", as some services and effects can be observed as soon as an internet connection is present, while others only make sense if the connection is fast and stable enough to support e.g. high-quality video or security.

The next paragraphs will describe the different sectors briefly, and try to give an indication of the most important effects these sectors experience. Where available, results from previous literature and studies will be included to give a first estimate of the monetary value of these effects.

#### 4.5.2.1 eBusiness

The Business sector could benefit significantly from the availability of a fast and stable broadband connection, both at the office and at the employee's home. When thinking of eBusiness and its advantages, one mainly mentions the possibilities to work from home (also referred to as teleworking) and the opportunities that arise from high-quality videoconferencing.

Teleworking reduces traffic and saves in commuting time, which entails huge savings in fuel costs and gives the employee more free time. Columbia Telecommunications Corporation calculated a decrease of 649 miles and 25.5 hours per employee per year (for the region of Seattle in the VS) [2]. Climate Risk saw an opportunity of decreasing the number of business trips by one third [3]. Plum Consulting agrees that, through using HD videoconferencing, 10% of flights used for business travel, could be avoided [4].

#### 4.5.2.2 eGovernment

eGovernment (or electronic government) is a platform that allows to offer city administration and other public services through an application running over the internet. This so-called e-counter reduces the number of visits to the administrative center of the city, and enhances the quality of the services offered. On a larger scale, these kinds of services can also be used for online filing of other types of requests, e.g. taxes (already operational in Belgium via TaxOnWeb [5]).

Previous studies showed that the large savings could be primarily found in time reductions and reallocation of administrative personnel. Price Waterhouse Coopers [6] calculated that, in the UK, granting driving licenses online instead of through the traditional manner would save 35 minutes (5 minutes online time versus 40 minutes traditional time – 37 minutes travel time and 3 minutes waiting time). Furthermore, postal and process costs could also severely be reduced (€1.06 per application). The same study concluded that the British government could save about €5 per customer when filing its tax returns online.

Another study performed by the Flemish Ministry of Finance and Planning investigating the effects of requesting building permits online [7] resulted in savings of about €12 million for the Flemish municipalities, mainly by reallocating the time of the administrative personnel (4-6 hours saved per building permit).

#### 4.5.2.3 eHealth

Structural changes in the health sector – transforming into eHealth – could entail huge savings in both care and personnel costs. These savings can be found especially in healthcare for chronic illnesses, elderly and people living in remote areas.

Currently, the highest healthcare costs for hospitals are to be found in taking care of the long-term, chronically ill people and elderly. These need constant monitoring, and currently, this is only possible in hospitals in most of the cases. A study performed by Columbia Telecommunications Corporation [2] calculated that the average hospital stay could be reduced from 14.8 to 10.9 days, that the number of visits to general practitioners could be decreased with 10% and emergence visits with 63%. Furthermore, monitoring equipment could bring back the average stay in care homes for elderly from 2.5 years to about 6 months, entailing savings of $50 000 per person. Price Waterhouse Coopers [6] also calculated that applying telemedicine for the chronically ill could bring down the costs per patient from $1166 to $335 per year.

#### 4.5.2.4 eEducation

Offering courses online and/or making use of videoconferencing tools for educational purposes are the most important effects of broadband to be mentioned in the education sector. University student are hereby offered the opportunity to follow lectures online (the Open University concept, already applied in the Netherlands [8]), or students can actively participate in a lecture given by a professor at another physical location using the tele-classing system (already operational in a cooperation between the universities of Ghent and Brussels in Belgium).

Some previous studies indicate that the availability of ICT improves the results of students after the age of 16 years, and increases the percentage of higher educated student with 1% [6]. The New Zealand Institute [9] further estimated that having courses available online will reduce travel costs with 20%.

#### 4.5.2.5 eEntertainment

The last sector that is to be noted to have a large impact from the internet is the entertainment sector. Gaming gets a totally new dimension when it becomes possible to directly compete with fellow gamers in an online, real-time environment. Social relationships with relatives abroad are much easier to maintain, and information retrieval becomes much faster and broader by being able to search for it on the World Wide Web.

The eEntertainment sector is probably most directly impacted by the internet, but advantages for the society are not easily calculated, they mostly refer to individuals' perspectives. Therefore, this sector is not of main focus in most previous studies, and results are based on estimates, rather than actual savings calculations.

### 4.5.3 Research directions

It is beyond doubt that the internet already had a huge effect on our everyday life, and that the current and upcoming developments in ICT will have a large impact on the way of living in the future. Technical upgrades of networks require typically a high upfront investment, and are frequently postponed with the argument that the "normal" customer revenues don't cover these investments completely. This chapter gave an indication of other kinds of "revenues" (mostly cost savings) that the internet and availability of broadband connections could entail, and that could help to fill the "revenue gap" for future investments in ICT networks.

Future research directions include the potential quantification of these revenues/savings for the different sectors listed above. Both macro-economic (top-down) as well as case specific (bottom-up) approaches can be used.

### 4.6 *Game theoretic Perspective*

The game theoretic perspective shares with Network Science a focus on graph theoretic representations, but focuses on deliberate rather than random dynamics and distinguishes behavioural choices at nodes from decisions to make, break, use or alter network links. There are several related approaches. Roughly, one considers the behaviour of individuals in networked environments (e.g. the way 'local' interactions with network neighbours influence strategic choice and evolution of conventions (Kandori-Mailath-Rob [10], Young [13], [14], Morris [11], etc.); another considers players' strategic choice of network connections (Aumann and Myerson [1], Jackson-Wolinsky [8], etc.). These are not wholly distinct; in games of communication (e.g., Dutta and Jackson [3]), messages dispatched through the network create linkages (at least of awareness). At a deeper level, the network perspective changes the interpretation of the basic elements of a game itself; players may have diffused, overlapping, shared or otherwise 'networked' identities, preferences, powers of action (individual, linkwise, groupwise) and information. Indeed, it is reasonable to consider rational individuals as networks in themselves. Four further observations that contribute to a synoptic view of the extensive related literature are:

- Game theory is based on assumptions of rational behaviour, but rationality itself may have a 'network' character. For instance, the cognitive framing approach of Bernheim and Rangel [2] (inter alia) codifies rationality as: identifying a range of alternatives; associating with each a range of possible consequences; evaluating these 'packages', 'bundles' or 'lotteries over' consequences; and picking the best. Clearly, the awareness attached to the first two steps depends on a framing that can be visualised as a network of attention or salience. Even evaluation and choice (or at least implementation) have a stepwise character by which immediate consequences give rise to indirect or wider impacts. Both in the 'real' world and in the mind of the player, these are themselves networked and (in the actual play of the game) affected by the choices and behaviour of others to whom the player is linked.

- The literature analysing behaviour in networks tends to treat network structures as fixed; the 'evolution of conventions' or games of network formation literature tends to treat the payoffs to different structures as fixed (at least in aggregate as a 'value function' that can be parcelled out to the players through an allocation function or explicit processes of negotiation or bargaining or conflict). These are clearly 'corners' of a more general model in which both structural and behavioural change occur at very different time-scales; removing this temporal isolation produces some quite startling and novel effects. This has implications for Internet dynamics as well - these seem to show punctuated equilibrium behaviour, where long periods of gradual and local structural change are interspersed with brief episodes (triggered by events like the Arab Spring or technological or service changes) of rapid and widespread alteration - and by periods when behaviour changes faster than structure interspersed with periods of structural change when behavioural habits change little if at all.

- Most models assume (with the exception of a few recent and simplified examples) that players in network formation games know the structure of the networks they inhabit. If they do not, the model changes radically. For example, in the standard 'agreeing to disagree' model, players' information about the state of the world is summarised in personal partitions on a common state space (typically the unit interval with a partition into some Borel subsets). These partitions are common knowledge; players communicate by means of an observable signal or language that maps events (elements of the field generated by the join of the individual partitions) into public signals or actions (e.g. moves in a game that maximise conditional expected payoff). If the players form a clique, the dynamics converge - at each stage players refine their beliefs based on the signals emitted by all players and their personal partitions get finer and finer in a perfectly predictable way. If the players are in a network, this process becomes divergent - to interpret a neighbour's moves at the second and subsequent rounds means forming a conjecture about what that neighbour's neighbours might have done or said - and thus a diverging network of conjectures. The situation is even more complex if the player does not know to whom his neighbours are linked - in this case the incomplete information (partition) on the states of the world and strategy choices must be complemented by a partition on the set of possible networks.

- In competitive settings that are typically approached in game-theoretic terms, nodes may exhibit a broad range of *behaviors* reflecting different perceptions, or even philosophical life stances when actors coincide with humans, as to what is "rational", "sensible", and "useful" to them or their fellow nodes. Moreover, their actions are also a function of the particular conditions, *e.g.,* time pressure and availability of knowledge/information about what their competitors do. Therefore, nodes may chose to consistently prioritize their *individual utility,* inline with the practices of *homo economicus*, or behave more altruistically and prioritize the *social welfare*, as *homo reciprocans* would do. Likewise, when they share common knowledge about the practices and priorities of their competitors, they might be capable to optimize their actions according to the norms of classical rationality; whereas, under tight decision-making deadlines and partial knowledge, their decisions may be driven by more heuristic considerations and be influenced by the local environment. Indeed, important insights to the process of human reasoning and decision-making have come over the last decade from the field of *cognitive psychology* [15, 16]. The magnitude and the intertwining of different determinants (such as needs, preferences, biases) on individual judgments have been the subject of research that attempt to dig specific brain regions, probing human decision–making mechanisms. In particular, the respective literature on cognitive science suggests that people draw inferences (*i.e.,* predict probabilities of an uncertain event or assess the relevance/value of incoming information), exploiting *cognitive heuristics*. These results relax the assumption of *classical rationality* and contrast the icon of super-calculator mind that decides after fully enumerating all possible actions and their repercussions.

### 4.6.1 Game-theoretic resource allocation

The resource allocation problem in game-theoretic terms has attracted interest from various disciplines under different contexts. Research studies on network – enabled nodes' transactions devise auction-based schemes to address the challenge of *resource* (energy, bandwidth and storage space) *sharing* among multiple networking users [26, 27]. In the same vein, transportation research exploits fundamental normative concepts aiming to systematically analyze phenomena on traffic flows (i.e., parking spot *resource assignment* [24, 25]).

In the following we present several proposed game theoretic resource allocation methods in p2p, cloud computing and ad-hoc networks to control the allocation and in some cases motivate cooperation among competing users.

#### 4.6.1.1 …in P2P networks

One crucial matter in p2p systems is the need for cooperation between peers. However, it is a social phenomenon, reported as "tragedy of the commons" [36] that most of the users are reluctant to cooperate, and only a small number of them are willing to share their resources, as there is a natural incentive for users only to consume but not contribute to a community.

The same phenomenon is known as "free riding" in the context of file sharing systems, like Gnutella, Napster and Kazaa. In Gnutella, for example, it was reported in 2000 [37] that 70% of all users do not share files and nearly 50% of all file requests are satisfied by the top 1% of sharing nodes. In 2005, a new report [38] indicated that 85% of Gnutella users are free riders.

Several game-theoretic protocols have been proposed to control the allocation and even motivate cooperation in the network. In [39] the Resource Biding Mechanism with Incentive and Utility (RBM-IU) is proposed according to which the server solves an optimization problem seeking to maximise the allocated bandwidth to each competing peer according to its contributions to the network and its reported bandwidth demands. The more contributive a peer is in the network the better QoS it will receive as an acknowledgement of its cooperative behabiour; therefore cooperation is enforced. The game theoretic model of the system of the competing peers who can strategically report their bandwidth demands in order to maximize their pay off has proved to have a Nash equilibrium.

A similar model is presented in [40]. Peers strategically determine the upload portion they decide to dedicate for serving other peers, rewarding the best contributors characterised by a reputation metric. The reputation of a peer is determined by the upload bandwidth dedicated to the network and determines its payoff. A simulation study has showed that the continuous interaction of peers result in efficient equilibria.

In [41] and [42] a game formulation among client-server pairs is considered. A peer acting as a client may or may not request a file, while acting as a server can choose to allow downloads or ignore requests, following a decision function that tends to penalize free riding behavior. This function,

together with the repetition of the game allows for the existence of equilibria other than the inefficient noncooperative ones of the classical prisoner's dilemma.

#### 4.6.1.2 …in Cloud Computing

Foster et al. [17] abstract cloud computing as "A large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualised, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet". As such, cloud computing emerges as a promising utility for large-scale computing and data storing whereby node resources are offered over the Internet as scalable and on-demand services [18,19]. Indeed, within the cloud abstraction the term "computing resources" refers to both the applications delivered as services as well as the system hardware and software in the datacenters that provide those services [28].

Within this dynamic and decentralized web-based cloud computing environment, researchers have questioned how automated system management, workload scheduling and virtualisation techniques can efficiently allocate resources among competing cloud consumers, namely complex cloud-based applications consisting of multiple subtasks that communicate each other. The intuitive decision to request and use resources at minimum cost (e.g., amount of money for the consumed resources), combined with the constrained, even scarce, cloud-based services, highlight the game-theoretic dynamics behind the cloud resource allocation problem. In [20] the authors present a QoS-constraint resource selection framework seeking to provide scheduling solutions in face of specific QoS requirements. Market-based treatment of the resource allocation problem can be found in [21, 22, 23]. Drawing on different criteria for resource allocation, the authors seek to couple resource utilization with nodes' (consumers' and providers') welfare.

#### 4.6.1.3 … in Wireless Ad hoc Networks

Ad hoc networks are characterised by a dynamic topology and often high node mobility providing an infrastructure-less but also volatile mean for multi-hop communications. Since no centralised control is usually present in ad hoc networks, networking operation like routing must be performed by the nodes of the network. However, since nodes have limited energy resources, they would inherently decline to cooperate, resulting in the degradation if not collapse of the network.

Works in [43]-[48], apply game theory to study the nodes' cooperative or not behavior in these networks. The nodal interactions can be represented in general as prisoner's dilemma where the strategy is to forward or reject an incoming packet. While mutual cooperation yields better result for all the nodes, the Nash equilibrium is non-cooperation, i.e. not forwarding packets. However the common conclusion is that repeated interactions of nodes, together with the adoption of proper reactive strategies of nodes can employ more effective equilibria, which is the general result of repeated game theory.

Work in [47] and [48] further investigates the impact of malicious nodes in the overall operation of the network. Malicious nodes can have a much more severe impact than the selfish ones, because they

obtain utility not only by maximizing their own benefit (as selfish nodes do) but also by destroying network operation at the expense of the legitimate nodes who are considerably damaged by ignorantly transacting with malicious nodes.

### 4.6.2 Game theoretic market entry

Next to the application of game theory in resource allocation, game theory also offers methodologies to assess the competitive interactions of market participants in broadband deployments. As has been indicated by [29], game theory is "aimed at modeling situations in which decision makers have to make specific actions that have mutual, possibly conflicting, consequences".

As such, the competition between different operators, service providers or vendors can be modeled by means of a payoff matrix. This matrix has a payoff (e.g. Net Present Value) for all players for each possible combination of strategies. This is called the strategic form of the game and allows finding an equilibrium in the game. An equilibrium is a set of strategies (one for each player) at which players are not inclined to change their strategy. Different equilibrium concepts have been proposed in the field of game theory. The most commonly known equilibrium is the Nash equilibrium (NE), which is defined as a situation in which no player can gain by unilaterally changing its strategy. In a pure NE, each player will use a pure strategy, whereas in a mixed NE, the players can play mixes (probabilistic combinations) of strategies [29]. It is often assumed that a game with fully rational players (using this equilibrium as criterion) is expected to result in one of the NEs being chosen.

In techno-economic analyses of broadband deployment, game theory has only been applied in a limited number of studies. In [30], the viability of a 3G introduction was studied under different market circumstances, where both dominant operators and new entrants compete for market share using different price setting strategies. A comparable price game was researched in [31] for competing wireless operators using a different access technology (3G and WiFi). Other publications focus on competition between wireless operators using other than price strategies [32] or on the competition between fixed broadband network operators [33].

A more recent field of techno-economics tries to combine game theory and real option analysis through the concept of option games [34]. Large investment projects are of particular interest for this domain, since uncertainty and competition can largely impact the result of the techno-economic analysis [35].

# 5. Security, Resilience and Dependability Aspects

The Internet and data communication networks in general, serve increasingly critical applications, ranging from financial transactions and business operations to support specialized security operations, earlier undertaken by mission-specific networks. As a consequence, the impact of all types of failures in their operation, whether due to human mistakes or software/hardware faults, as well as political decisions and increasingly intelligent and orchestrated, malicious attacks can be dramatic for economies and societies as a whole. Therefore, a very important Internet science research direction is the study of the security, resilience and dependability of the Internet.

## 5.1 *Research Directions*

The Internet of the future faces a wide number of challenges and threats. These range from traditional security issues over new attacks to privacy issues in an increasingly networked environment. As the Internet itself is becoming more ubiquitous, the damage from possible attacks increases in magnitude. Threats like botnets or Denial of Service attacks are already affecting millions of devices. This will become even more severe, if concepts like the Internet of Things become a reality [1].

On the other hand, the Internet increasingly hosts critical services which need to be protected. Information served over the Internet in real-time is nowadays an economic building block. As such, the failure of services like the Web or DNS can lead to huge economical damage. The failure of services can even become life-threatening, as in the example of emergency calls performed with Voice over IP (VoIP). This leads to an inherent need for network and service resilience [2].

### 5.1.1 Challenges in today's Internet for critical infrastructures

While the Internet seems to be quite robust for typical end-user applications like web browsing or messaging, other more critical applications may not work in such an environment without risk [3]. Routing failures are one reason for outages that may take longer than applications may allow. The reaction to failures in intra-domain routing can take several 100 ms [4]. The situation is even worse for inter-domain routing. BGP reaction to routing failures can take up to several minutes [5]. Furthermore, maintenance errors or attacks can have severe impact on Internet routing. Pakistan Telekom accidentally blocking Youtube in large parts of the world is one example [6]. Another example for misconfiguration made Cisco routers crash when they received BGP update messages [7]. These examples also illustrate another weakness of the current Internet. It lacks security by design. Authentication protocols are not essential part of the infrastructure, but built on top, mostly on application layer. This allows ARP spoofing, forging of BGP updates or DNS responses [8], and many other threats to the Internet's security and, thus, the security of an important critical infrastructure. Spam is another example, where the misuse of a service accounts for up to 90 % of the traffic of the service. This is also related to the problem that the congestion of the network cannot be controlled. An attacked peer cannot tear down undesired traffic. This also has implication for traffic engineering as

fixed demands and traffic matrices do not account for unexpected attack traffic [9]. Centralization of services is another issue. Imagine a failure at Google. Many people rely on their services and for most people such a shutdown may be a shutdown from the Internet as they will not be able to search the WWW as they are used to [10].

### 5.1.2 Cloud Computing and Virtualised Environments

Network virtualisation is currently being investigated as a possible route towards a future Internet. Security in this area, however, has to be studied further [11]. It is yet unclear, whether the security benefits will outweigh the security drawbacks. While virtualisation allows operators to confine different networks in their own environment, the compartmentalization is not perfect [12]. If this technology is adapted in the future Internet, it will require careful planning of virtualised networks [13]. With regard to resilience, virtualisation can be used to increase the availability of Internet services, ensuring that a service remains operable even in the event of network failures [14].

Cloud computing is recently becoming part of the critical infrastructure of the Internet in supporting government and industry service operations. Cyber-security and resilience in the cloud must address emerging vulnerabilities associated with the characteristics of such environments, including: (a) the collocation of computation and confidential data of multiple users (multi-tenancy), (b) potential exploits in hardware virtualisation technologies, and (c) requirements of processing elasticity [15]. Alongside new vulnerabilities, more traditional and established security threats are expected to take new forms in a cloud environment [16], including abuse of resources, malicious insiders, malware propagations, and account hijacking.

In particular, [17] has investigated a multi-level network resilience approach to online security and resilience by looking into extended systems aspects. This research takes into account system and device aspects as well as users and their interactions with the network. Multi-level network resilience is characterised by the end-to-end monitoring of Internet threats, at both edge and core networks (horizontally), and at different layers of the protocol stack (vertically). This ranges from the analysis of low-level traffic data to the investigation of high-level vulnerabilities in end-systems.

### 5.1.3 Network and Service Resilience Management

Resilience management encompasses the traditional FCAPS (fault, configuration, accounting, performance, and security) functionalities. The nature of the attacks and challenges a network may face typically requires the use of mechanisms across various layers of the protocol stack, across a number of administrative domains, and across heterogeneous infrastructures. Therefore, ensuring the resilience of a network requires the systematic design and evaluation of resilience strategies, and the capture of best practices and experience of network operators into reusable resilience configurations.
Central to this strategy is the management and reconfiguration of interacting detection and remediation mechanisms operating in the network infrastructure [18]. An active research topic is the investigation

of how management policies [19] can be used to control the operation of these mechanisms, and how they should be reconfigured in the face of new types of challenges or changes in their operational context, e.g., high resource utilisation, or performance degradation. Recently, [20] has proposed the notion of multi-stage resilience strategies, in which the policy-based configuration of a set of detection and remediation mechanisms is dynamically refined as new information about challenges becomes available.

Further, [21] has defined a framework and process for the design and evaluation of network resilience management. The framework enables (1) the offline evaluation of resilience strategies to combat several types of challenges, (2) the generalisation of solutions for coping with different challenge behaviours into reusable resilience configurations, called patterns, and (3) the rapid deployment of appropriate patterns when challenges are observed at run-time. For the offline evaluation, a policy-based resilience simulator [22] has been used, which is based on an integration between the OMNeT++ network simulator [23] and the Ponder2 policy framework [24]. The toolset supports the simulation of a range of network challenges, and the reproduction of the policy-driven interactions between the mechanisms used to combat such challenges. The simulation environment is valuable for the understanding of the different challenge profiles and candidate mitigation strategies, before they are implemented on physical devices in the network. By capitalising on successful resilience configurations, one can derive generalised patterns for different challenge behaviours. Patterns thus support the notion of reusing tested solutions for known problems when building strategies for network resilience. Furthermore, a promising research direction is the application of such techniques in the context of resilience in clouds and virtualised environments, considering the types of challenges and attacks specific to these environments.

### 5.1.4 Analyzing and Modelling of Network Robustness

A network consists of a topology specifying the nodes and their inter-connections (“links”). Networks are of interest because of the dynamic process for which the network is designed. Examples are power transport and information transport.

The huge complexity in communications networks (due to a multi-layer protocol suite, different aggregation levels, missing service metrics that adequately capture and define robustness properties, and a dynamically changing and uncertain topology) illustrates why, at present, a framework to compute network robustness is still lacking.

A wealth of procedures to evaluate and improve network robustness has been proposed over the last 50 years. A literature overview of the proposed frameworks for resilience (here as well called robustness) is presented by Cholda et al. [25]. The first approach to network robustness was in the context of network reliability [26], [27], [28], [29], primarily aiming at connectivity measures, both deterministic and probabilistic. Network nodes and links are weighted with failure (survival) probabilities and graph theoretic tools together with Boolean logic techniques are used to compute the

connectivity between arbitrary network endpoints (terminal reliability) [26], [27], [28] and for the network as a whole (network reliability) [29]. The probability of a graph to remain connected after a number of network component failures is studied using graph percolation in [30], [31] and reliability polynomials in [32], [33]. Recently, attention has been given to the study of power law network's reliability [34], [35], [36], since Faloutsos et al. [37] showed that the degree distribution of the Internet topology follows a power law. Graph connectivity aspects in assessing network vulnerability are discussed in [38]. Overall, reliability studies are a valuable tool to address the risk for network disconnectivity via stochastic models. However, reliability studies present two drawbacks. First, reliability studies are shown not to be optimal due to the irregular stress cycles of network elements [39]. Second, these studies ignore the multi-level service nature of networks.

Performance concerns, on the other hand, are explicitly treated in the performability framework, introduced by Meyer in [40]. The term performability was initially launched to cover a class of unified performance-reliability measures [40], but soon evolved to a more general theory and tools assessing the capability of systems to perform in the presence of faults [41]. Performability studies have been trying to incorporate the impact of lower level system processes to higher-level application performance. However, the emphasis of performability work is not on the network topology: higher levels of abstractions, modeled by stochastic Petri nets and Markovian chains, are necessary to compute performability.

Modern network theory has been integrated with dynamic system's theory to understand the influence of network topology on the performance of a network's function or service, which is in general a complex dynamic process upon a network. This allows the evaluation and further improvement of the robustness of a network with respect to its function. For example, the largest eigenvalue $\lambda_1(A)$ of the adjacency matrix A, called the spectral radius of the graph, plays an important role in dynamic processes on graphs, such as the SIS (susceptible-infected-susceptible) virus spreading [42] and the Kuramoto type of synchronization process of coupled oscillators [43] and percolation. The SIS type of network infection features a phase transition at the epidemic threshold $\tau c=1/(\lambda_1(A))$: when the effective infection rate $\tau>\tau c$, the network is infected, whereas below $\tau c$, the network is virus-free. The more curious aspect is that the same type of phase-transition occurs at the coupling strength $gc=1/(\lambda_1(A))$ in a network of coupled oscillators, above which oscillators synchronize. Besides these well understood processes, the association between network topology features and the performance of a network's remains still as a challenging question.

# 6. Sustainability Perspective

Latest Research on the Internet seeks to investigate how the Internet can relieve the main problems affecting sustainability at planetary scale, including Greenhouse gas (GHG) emissions, energy production, sustainable lifestyles and the related problem of climate change. This research dimension is very important towards the definition of the Internet Science.

Energy sustainability, especially energy efficiency, has gained increased interest in the past years, promising sustainability, reduced costs, and environmental gains. There is already a broad literature on the subject and several surveys have appeared, e.g. a recent survey by [1], [2] and [3].

Internet Science and Sustainability are linked through two major challenges: First, the Future Internet architecture has to be energy-efficient itself. Second, Internet technologies should be used to enable world sustainability.

## 6.1 *Towards an energy-efficient Internet*

The worldwide usage of Internet services causes huge power consumption: For ensuring a solid communication infrastructure, a lot of different devices, e.g., routers, servers, and clients have to be deployed and need to be turned on. So, one question is how the current Internet infrastructure could be enhanced or replaced by better, more energy-efficient solutions.

This might be either done by a clean slate approach, i.e., by implementing a completely new architecture, or by improving existing techniques. Virtualisation (e.g., see [4] and [5]) is often seen as a key technology for the future Internet: Multiple Machines can be migrated, even on-line, to a single physical host. This might be more energy-efficient than deploying the services on several hosts and is therefore reasonable in times the service is only rarely requested (e.g., at night). Therefore, in the context of future Internet technologies, virtual networks could be used that are embedded into the physical topology in an energy-efficient way.

Existing work on making the Internet more energy efficient can broadly be classified into:

1. Measuring and modeling energy consumption
2. Virtualisation based consolidation approaches
3. Dynamic rate adaptation
4. Energy-aware traffic engineering
5. Energy-efficient network design

### 6.1.1 Measuring and modelling energy consumption

When measuring and modeling energy consumption, it is also essential to lay out priorities. On the short term, access networks and customer premise equipment deserve our attention as they are by far

the largest energy consumers in the network. This is mainly due to the high number of devices present in this area of the network. However, as we shift towards higher capacity access networks, the core networks will also need to be able to carry this capacity at a reasonable energy consumption. Hence, on a longer term, also these networks should be investigated [43].

The specs for networking equipment usually mention some energy consumption values, although often only for a specific (e.g., best case/worst case) operating condition. These values may be sufficient for high-level energy-aware network design, but may be too coarse for energy-aware network management that has to take into account an accurate and detailed view of the energy consumption of the specific network in operation. This kind of information is often missing from papers, partly because it is considered too equipment specific, and partly because this information is only publicly available for a limited number of devices. Moreover, even if these values are available, it is not always clear if these values are representative average for similar equipment or not. Substantial differences in power consumption per equipment type have been observed in different papers, due to different sources. In response to these issues, in [44] reference power consumption values are proposed (based on a collection of vendor data sheets) for core network equipment such as IP/IMPLS routers, transponders and optical line amplifiers.

Since energy consumption may depend on the dynamic traffic load and its characteristics, the consumption pattern may also vary dynamically and consequently needs to be measured frequently in order to be able to "steer" the energy consumption, for instance via traffic engineering algorithms. Similarly, modelling energy consumption and adopting a benchmark aids in designing and comparing energy-aware techniques.

Often it is assumed that there is a linear relation between energy consumption and traffic demand. Ricciardi et al. [6] argue that often energy consumption relates to traffic load and consider 3 cases: (1) the idle energy model composed of a fixed part and a part that is linearly increasing with the amount of traffic, (2) the fully proportional model where there is no energy consumption in absence of traffic, and (3) the energy-agnostic case that always consumes a fixed amount of energy irrespective of the amount of traffic.

In general, energy-efficiency techniques and models are expected to be able to give good rules of thumb, but "greening" a network will also require energy measurements and tailor-made solutions.

### 6.1.2 Virtualisation based consolidation approaches

Virtualisation is often seen as a key technology for the future Internet. Instead of using the physical hardware directly, it is accessed through a virtual abstraction layer. Software is installed at this virtual level; the actual access to the real underlying hardware is managed by the virtualisation technology. Multiple virtual machines can be installed at the same physical host. They can be migrated, even on-line, to another physical host.

The consolidation of multiple virtual machines onto the same host might be more energy-efficient than deploying the services on several hosts and is therefore reasonable in times the service is only rarely requested (e.g., at night), because, in this case, it is unlikely that the consolidation results in a reduction of quality of service (QoS) [4], [5]. Additionally, one can also look at the potential of virtualised servers of replacing high computing capacity at the user premises. By replacing desktop and laptop computers with lightweight thin clients and migrating the processing to a data center, large efficiency gains can be realized. Moreover, due to a better server management, longer equipment life cycles can be realized resulting in an overall carbon footprint reduction. Another possible application of virtualisation is the use of a Virtual Home Gateway, where the CPE processor is partly or completely moved to a central server [45]. Multiple subscribers can share the processor in time and more efficient router hardware is available in the network, resulting in a more efficient power use.

In the context of future Internet technologies, whole network topologies could be virtualised. Various networks could then be embedded into a physical network infrastructure. At the side of the network infrastructure provider, consolidation techniques could then be used to reduce the power consumption level of the physical infrastructure by switching off unnecessary devices [28].

### 6.1.3 Dynamic rate adaptation

The energy consumption of a device in general depends on the rate at which it operates, where higher rates usually correspond to higher energy values. If the rate of a device can be configured dynamically, reducing the rate in times of low traffic demands may save power (e.g., see [7]).

Switching off nodes and links is considered to be an extreme form of rate adaptation and clearly also generates the biggest savings in the rate adaptation spectrum. However, it also comes at greater risks in terms of network robustness and Quality of Service (QoS). Operating a network at its bare capacity minimum is most energy efficient, but conflicts with the notion of having redundant devices for resiliency purposes. Similarly, over-provisioning as a means to provide QoS, results in higher energy levels. Research is needed to find a proper balance between switching off or adapting the rates of nodes and still offering sufficient robustness and QoS performance.

Also in wireless devices, sleep modes offer a promising reduction strategy. When comparing the increasing capacity needs for wireless devices and the limited reach over which these capacities can be provided, always-on wireless networks will become unsustainable. Hence, a novel access network, combining lightweight base stations with intensive sleep mode algorithms, is required to be able to provide these high capacities.

### 6.1.4 Energy-aware traffic engineering

Energy-aware traffic engineering (possibly in tandem with QoS routing) relates to finding paths in a network that use a minimum amount of energy. For instance, while load balancing was often considered good practice to reduce congestion levels, aggregating traffic on as few paths as possible may be more energy efficient (since the idle devices could be switched off or operated in sleeping mode). Another approach may be to queue (at the expense of some extra delay) packets at the edge of the network and transmit them as bursts of packets over the network to impose a more energy-favorable traffic pattern.

Typically, router hardware will have a certain idle power specified. This is the power requirement when no (external) traffic is processed. Energy consumption increases with bandwidth, but there may not be a one-to-one relation, since, in addition to bulk bandwidth, also traffic characteristics such as packet size or type (IP or MPLS) may influence power requirements [46]. Idle power in most cases is a fairly high part (~90%) of the total maximum power dissipation. On the other hand, when looking at Ethernet technology, which is seeing adoption in carrier-grade networks, it is possible to reduce power down to 25% of the maximum rated peak consumption simply by adjusting line rates (e.g., 100 Mbps – 1 Gbps – 10 Gbps) to carried traffic volume [47][48] (compare to dynamic rate adaptation above). This would suggest a similar idle power for layer 2 equipment of ~25% of maximum power dissipation. Given this dependency of power requirements on traffic volume and characteristics, energy-aware traffic engineering therefore focuses on routing as well as optimal filling of network links, taking into account power characteristics and/or models of devices.

In [49], the effect of multilayer traffic engineering and its interaction with hardware improvements related to energy-efficiency are examined. Power scaling, where the entire power requirements are reduced through iterative CMOS technology improvements, and architectural improvements leading to lower idle power are compared, in order to indicate how multilayer traffic engineering reduces energy requirements for both cases and how device power characteristics improve these.

Work in [50][51] continues with multilayer traffic engineering, looking at the impact of energy-aware routing and lightpath establishment for diurnal traffic variations; the difference between peak and off-peak traffic volumes can be quite large (e.g., 4:1) as shown in [52][53]. Multilayer traffic engineering is shown to lead to savings in power requirements of more than 40% during off-peak hours, using rerouting and switch-off. Taking into account the power characteristic of equipment when devices of varying energy efficiency are used in a network can provide an additional 10%+ reduction.

Many of the related papers focus on aggregating traffic based on different energy models. Their approach is often fairly similar: either a traffic matrix is assumed and an Integer Linear Program (ILP) is proposed, e.g. [8] and [9] or dynamic traffic is considered and a shortest-paths-like algorithm is deployed on a network with a certain energy cost per node/link, e.g., [10], [11] and [12]. Less work is available on actual implementations and experiments to obtain insights into the gain of energy-efficient traffic engineering in practice.

### 6.1.5 Energy-efficient network design

Properly thinking about and designing a network will be the best foundation for green networking. However, network design is a complex problem, with many constraints. For instance, new equipment may be more energy efficient or adaptable than old equipment. Which equipment to use/replace, where to place it (some locations may be closer to cheap energy sources or may be in areas of low temperature – thus saving on cooling), and how to connect it are decisions that have to be made in light of costs, physical constraints and traffic load forecasts. Power-hungry IP routers could be optically bypassed through optical cross-connects, while multiple intermediate solutions are possible where IP routers are still used at certain points to groom (i.e. bundle) traffic to optimize channel capacity usage [54]. Although design problems are complex, they do not have to be solved instantly and hence exact solutions (e.g., via an ILP) may be feasible or well-performing heuristics can be devised, e.g., see [13] and [14].

The above classification of the type of work on energy efficiency is fairly generic and hence can be considered in different contexts. For example, information-centric networking may dynamically deploy caching in the network to provide the requested content from a location as close as possible to the user, thereby alleviating the transport network and the originating server, which on its turn may reduce energy. Or, with respect to carbon emissions, a follow the sun/follow the wind paradigm could be applied to data centers. Data centers are then powered by renewable energy source, with very low carbon emissions, and jobs and data is dynamically migrated across large geographical areas to where renewable power is available [55]. To reap the “energy” fruits of such a novel networking paradigm, new energy-aware algorithms might have to be developed.

## 6.2 *Internet for energy-efficient power provisioning*

Several mechanisms have been discussed related to how evolving Internet technologies can help to increase the sustainability inside the power grid itself and to build a power grid that is really "smart". New ways to save energy are explored by looking at a whole ecosystem consisting of energy providers, data centers, and end users of data centers. On one hand, data centers can have a great impact on the emergence and avoidance of peak loads in the power grid. Currently, peak loads in the power grid can only be compensated by highly responsive power plants which, in general, are ecologically (and economically) expensive. On the other hand, energy providers can reduce the impact of such peaks by balancing the energy sources based on their flexibility and $CO_2$ emissions, including renewable energy sources, which have traditionally been difficult to fully integrate into the power grid due to their unpredictability. Therefore, ways to adapt the energy consumption of data centers based on the current load in the power grid or the availability of renewable energies should be investigated. This will help the energy provider to avoid peaks and integrate renewable energy sources into the power grid, respectively, by an intensive communication between the energy provider and its customers. The All4Green project [27] actively investigates in this.

It is true that the use of Internet technologies in current power provisioning is very limited. However, for certain appliances like street lighting or electric storage heaters, utility companies can remotely control when to switch them on or off. Also, to ensure grid stability, since 2012 all renewable energy power plants in Germany which exceed a peak power generation capability of 30kW are required to be equipped with remote control devices.

Instead of using IP-based communication, load control is realized by using ripple control in many countries. Ripple control uses the electricity grid of the utility to communicate with frequency sensitive relays triggering circuit breakers. Technically, the utility creates a ripple control signal by superimposing higher frequency signals onto the standard 50 Hz grid power signal. These control signals are usually in the range from 100 Hz to 2000Hz. On the client side, the control signals are decoded and can be used to trigger relays that switch the power to certain devices.

### 6.2.1 Role of AMI and multi-agent systems in smart grids

In addition, in the smart grid there will be a massive adoption of distributed generation technologies, especially based on renewable sources, which will dominate more traditional forms of large-scale centralized generation. Furthermore, a significant portion of the grid users will be energy prosumers. As a consequence the smart grid must be a fully bidirectional electric network where, in principle, power flows could be "routed" over circuit paths established between any pair of grid points [15]. On one hand, this will induce a profound technological transformation of the existing electricity delivery infrastructure, especially at the distribution system level, to accommodate bidirectional power flow patterns. On the other hand, a pervasive two-way communication backbone, called *advanced metering infrastructure* or *AMI*, must be established amongst smart meters and other energy management units, which is needed to collect the huge amount of status information from all grid devices, and to realize innovative demand-side control applications, such as demand response [16]. It is intuitive to notice that reliability and delay concerns will become more serious as the communication network of the smart grid becomes more complex and widely deployed, because a larger volume of data will need to be distributed to various applications. However, most of the communicating devices interconnected by the smart grid will be tiny embedded devices with low computing and storage capabilities. Therefore, new network architectures and communication protocols able to meet the QoS requirements of smart grid applications while guaranteeing low-cost deployment, easy network maintenance and better communication reliability, should be investigated [17], [18]. For instance, there is a large body of work that envisions an extensive use of both infrastructure-based and self-organizing wireless technologies e.g. see [19] and [20]. In addition, wireless technologies are necessary to allow the integration of mobile units (e.g., electric vehicles) in the smart grid infrastructure. However, there is no doubt that the large variety of different usage cases for the smart grid will necessarily require the exploitation of multiple types of communications technologies.

It is also important to observe that the transition to the smart grid will necessarily bring about significant changes to the way management and control applications will be implemented in the power

systems. Indeed, it is expected that the smart grid will embrace a fully decentralized control model where multiple different energy management systems (EMSs) should interact with each other [21]. Then, the control applications will make autonomous but coordinated decisions in order to achieve a desired control objective based on the real-time information provided by the AMI. For instance, there will be EMSs to control energy usage in homes and to support demand response applications, for the optimal operation of microgrids and virtual power plants, for the efficient integration of electric vehicles into the smart grid, etc. Furthermore, with the massive deployment of distributed generation from intermittent renewable resources and the wide adoption of electric vehicles, there is an increasing consensus in the power engineering community that in the smart grid some management and control functionalities should be de- centralized and moved to the periphery of the grid [22]. Several technologies can be considered to implement fully distributed, autonomous EMSs, but multi-agent systems (MAS in short) have received much attention in the research community, e.g. see [23] and [24] for a survey, and there is a large body of papers that have developed multi-agent systems for a variety of application scenarios, including power system restoration, fault diagnosis, management of distributed energy resources, demand-side management, management of energy storage systems, optimization of electric vehicle operations, etc.

However, there are several technical issues which must be addressed in order to be able to effectively use this technology in real-world deployments. For instance, to guarantee scalability it is necessary to define flexible, extensible, and open architectures, where agents can be easily added or removed, and agent interactions are not fixed at design time. An example is provided in [25], where a three-layered architecture is proposed to manage energy resources while reducing architecture complexity. In addition, it is also essential to use implementation approaches and standards that can ensure that agents are able to cooperate, irrespective of their different capabilities and functions, or of the platforms used to develop them [26].

### 6.2.2 Demand-Response Systems definitions and Non Intrusive Load Monitoring (NILM)

Demand Response (DR), Demand Side Management (DSM), or Price-responsive demand are essentially different ways of achieving the same end result, i.e. to make the users' demand respond to the state of the grid so that available capacity or resources may be shared efficiently and peak loads can be alleviated. User demand is regulated through variable pricing, financial (dis)incentives, or explicit/direct load control so that demand matches supply. Although demand-side strategies are more popular in the power sector today, they are also used in other domains such as transportation (e.g. congestion pricing).

Demand Side Management (DSM) has traditionally been used as a broad term involving the management of electricity demand through various means. These means include activities affecting the load shape (shedding load, shifting load or activating on-site generation) and various other energy efficiency measures the purpose of which is to steadily reduce the load level.

The first proposed NILM system "required no intrusion to the residence" [29] and was coupled to the power circuits which enter the house or flat. NILM is enabled by voltage sensing (VS) transformers. Digital AC monitors sample current and voltage signals with a preferable rate at least once per second, and identifies real and reactive power, which is consumed by the residence. On the next step this information is used to calculate admittance, which can be used as appliance identifying characteristic. Scaler normalizes admittance signals. Net change detector unit distinguishes between steady state condition and changing condition, when an appliance was just launched or shut down. Finally cluster analysis unit detects frequently observed changes, which most likely correspond to certain appliance turning on or off. The number of points in the cluster (per time) indicates how frequently appliance was used.

NILM systems still carry much similarity with the architecture [29]. According to [30] the main steps of most NILM systems work in following two steps:

1. The detection of transitions. This step is usually done using statistical change detection.
2. The classification of transitions. This step often uses library of labeled transitions.

Although this view is simplified comparing to [29], it shows the major challenges of NILM. Ongoing research in NILM area aims at both improving the time and accuracy of transition detection and improving the accuracy of classification.

In order to distinguish appliances, NILM systems rely on power signatures – distinct features of appliance energy consumption. Taxonomy of power signatures was summarized in the paper [31]. Some further classification details can be found in the paper [32]. According to [32] the systems can be split into two broad categories, i.e., transient and steady-state approaches. Monitors using a steady-state approach distinguish appliances by their steady-state power consumption. Those monitoring devices have relatively modest computational requirements and have been practical for some time. The transient approach identifies appliances by examining the full detail of their transient behavior. Implementations of transient NILMs have typically used custom hardware, such as the parallel computer or the digital signal processor–personal computer combination.

The working appliance can be identified indirectly, by analyzing the activity of the user and deducing what appliance does user need to proceed with the activity. Some of the activity recognition techniques, like [33, 34], were used for appliance management in order to reduce the power consumption. The work in [35] employs another approach to activity recognition classification and views it from the perspective of employed sensors. According to [35] the approaches for classification of activities of daily living can be generally classified into two categories. First category is based on the use of visual sensing devices, like cameras. This category employs computer vision methods in order to process visual observations for activity monitoring. The second category uses sensor networks for activity recognition. Activity models are produced by applying data mining and machine learning techniques to the sensor data. Learnt models are the basis of activity recognition.

### 6.3 *Cyber-Physical Systems*

Sustainability requires the need to detect and react to events in the real world, which is the core concern of Cyber-Physical Systems (CPS). Therefore, this section gives a brief introduction and the current state respectively shortcomings of science and engineering of CPS.

Sensors and actuators have for several years successfully been used for automation tasks in, e.g., elevators, temperature control, cars, and trains. This generation of sensors has been designed for particular applications with very few control parameters. Recent developments are promising an abundance of new (wireless) sensors and actuators that become smaller, more energy efficient, more intelligent, and provide more sensing/actuating and processing capabilities. Furthermore, these devices are accessible through communication networks including the (Future) Internet. This change constitutes the start of a new computing era. From the very beginning of computing, each computing device (mainframe, PC, smart phone) has a set of Input/Output devices directly attached to it, like keyboard and monitor, for human computer interaction. Interaction between the environment and computers has only been indirect through the mediation of humans. However, networked sensors and actuators will change this drastically, because computation will more and more interact directly with the environment through these devices without a "human in the loop" to form smart environments, also called Cyber Physical Systems (CPS). Already today many promising application domains are identified, including eHealth, environmental monitoring, smart buildings, smart grid, manufacturing, transport and logistics and many others. Thus, smart environments can help to solve some of the major challenges society is facing, like the demographic change and aging in Europe, and sustainable ecosystems and environments. J.M. Wing (Carnegie Mellon University and National Science Foundation) goes even beyond this and predicts that: *"Cyber Physical Systems will be everywhere, used by everyone, for everything"* [36].

In this context, the development of new innovative applications with networked sensors and actuators is the most obvious research task. However, there are much more fundamental challenges to be solved. To identify these challenges we briefly discuss the simple question: What makes smart environments *smart*? Sensors and actuators only convert signals. For example, sensors typically convert an analogue signal in the real world to a digital signal, like temperature or luminance to integer values. To interpret values from sensors and to react to events through actuation requires additional computing. It is exactly this computation, which makes smart environments smart. However, the development of the necessary software is a major bottleneck for smart environment development, because there are three core properties of smart environments that increase the difficulty of their efficient development. First, every smart environment is different, i.e., in Ambient Assisted Living (AAL) every residential home is different and of course every resident is different. Second, smart environments are dynamic systems typically caused by mobility of users and devices. Third, smart environments are complex systems comprising many components like radios, network protocols, operating systems, data fusion and data aggregation, as well as middleware components like data stream management systems and complex event processing systems, and applications. Since the application domains are very different, recent projects are typically "hard wiring" a single solution for a particular application domain and a

particular environment. Re-use of partial solutions across different application domains is rarely happening and the development of self-adapting applications and systems is very hard. Adaptation across system layers, i.e. cross-layer optimization [37], violates today's engineering principles and adaptive smart environments will break the layered system model. This has recently been pointed out by A. Lee (Stanford University) "*to fully realize the potential of CPS, the core abstractions of computing need to be rethought*" [38], and Conti et al. "*there is a need to deeply rethink the modelling and architecting of future pervasive systems*" [39].

Recent programs and activities to address these shortcomings include the most recent call for proposals from the National Science Foundation [40] which aims to "*By abstracting from the particulars of specific systems and application domains, the CPS program aims to reveal cross-cutting fundamental scientific and engineering principles that underpin the integration of cyber and physical elements across all application sectors.*" Bogdan and Marlescu [41] aim to lay new foundations for a science of CPS design by identifying the main characteristics of communication workload of realised CPS systems being self-similar and non-stationary. Based on this insight they present a statistical physical model to define a new optimal control problem. Another step towards "Science and Engineering of Cyber-Physical Systems" is the Dagstuhl Seminar 11441 [42]. Several challenges and open problems are identified.

# 7. Standards Policy and Internet Science

Clark et al. [1] recognise that struggle or "tussle" between different interests is as important in technology evolution as in economic and political systems, suggesting that "we, as technical designers, should not try to deny the reality of the tussle, but instead recognize our power to shape it." As Greenstein [2] advises standards bodies, "doing the tussle" can create more robust and widely adopted industry standards. Although a mandate for the technical community, this can be easily extended to the legal regulatory communities that directly shape the various aspects of Internet development, many of which already recognise that their shaping decisions are moves in a game rather than acts of sovereign design. Design choices in code can be as normative as law - decisions have to be made on the values that code embeds [3].

Most progress has happened with technical protocol development within companies (and arguably open source communities), where coordination ("tussle") problems are less complex than in legislatures. Code has continued to morph rapidly even as legislation has tried to adapt. Investor certainty and democratic participation in legislative processes are arguably enhanced by the leisurely speed of legislation, contrasted with the rapid - but slowing - progress of Internet standards in which only technical experts can realistically participate.

There is an extensive history of competition policy in favour of open technology standards that long predates the Internet [4] but the evidence of extensive network effects and innovation that can rapidly tip markets has helped focus policymakers' attention on the potential for using interoperability as a solution to the competition and innovation problems that emerge. As competition policy provides for interoperable remedies, governments have set great store by the success of open standards as solutions for the well-known entrenchment of dominant Internet commercial actors using network effects [5],[6]. Bar et al [7] observed that "Interconnection is binary – you are either connected or not – but interoperability comes in degrees and presupposes a higher level of logical compatibility": the higher the compatibility, the greater the interoperability.

What should an open standard contain? Dolmans [8] suggests that an established 'common standard' which is truly open allows the "best of breed" components from different manufacturers to be combined, with maximum efficiency. To qualify as "open," he argues that a standard must meet a number of open conditions:

- access to the decision-making process
- transparent and undistorted procedures
- published, pro-competitive goals
- published, objective, relevant criteria for technology selection
- no over-standardisation

Most critical is access to the standard, which he argues includes open information on blocking patents (cause of much patent thicket litigation in smartphones and tablet computing); no unjustified refusal to license; fair reasonable and non-discriminatory (FRAND) pricing [9], [10]: Paragraphs 285-291.

Dolmans [8] suggests that royalty-free licensing is advisable in the software arena – allowing both open source and proprietary software to compete on quality and functionality. However, the telecommunications sector uses FRAND licensing, given the price and complexity of standard-setting efforts. He states that: "Mandating royalty-free licensing would likely recreate a tragedy of commons and discourage innovation, while allowing IPR owners to charge at will could create a tragedy of anticommons. To strike the right balance, therefore, a contract of mutual restraint is necessary." This argues for a mixed market and against uniform royalty-free pricing [6].

The European Commission's thinking on interoperability and code has developed through the course of the Microsoft, Intel and Rambus cases ([9]: chapters 5-6). Neelie Kroes was Competition Commissioner from 2005-9, and signalled more intervention on interoperability: "I will seriously explore all options to ensure that significant market players cannot just choose to deny interoperability with their product" [11]. She argues that the lengthy Microsoft case has lessons for action: "Complex anti-trust investigations followed by court proceedings are perhaps not the only way to increase interoperability. The Commission should not need to run an epic antitrust case every time software lacks interoperability."

Kroes' solution to the Microsoft dilemma - solving the antitrust problem long after the competitors have died - is to require *ex ante* interoperability evidence, which had not previously been available except through antitrust suits: "Whereas in ex-post investigations we have all sorts of case-specific evidence and economic analysis on which to base our decisions, we are forced to look at more general data and arguments when assessing the impact of *ex-ante* legislation." She argues for a potential future legislative proposal, which would impose an *ex ante* requirement imposed to publish interoperability information.

Microsoft and Intel's settlements illustrate a general point about smart structural remedies under competition policy – network effects demand very effective trans-Atlantic cooperation plus policy formed from research into global information technology. This applies the Lessig 'code is law' analysis but with Braithwaite and Drahos' international coordination regulatory approach applied to the overall information environment (Braithwaite and Drahos 2000 [12], Drahos with Braithwaite 2002 [13]). Note the forerunners of the suggested policy direction are 1980s data protection and 1990s cryptography cooperation.

If free and open source software have not proved a significant competitive check on information monopolists, that raises a significant regulatory challenge which must be met by governments, to create interoperability in those dominant actors' own software. Kroes [11] set out a radical agenda to ensure interoperability in European ICT procurement and regulation, drawing on procedural frustrations in the Microsoft case. It is in five parts:

- a new standard setting framework;
- new horizontal agreement guidelines to establish more transparency in licensing standards (EC 2011 [10]: Chapter 7);
- a common framework for ICT procurement;
- a new European Interoperability Framework (EIF); and
- intervention in competition cases to establish a principle of interoperability, including via *ex ante* requirements.

The EIF is a second version of a much less ambitious 2003/4 first version of the framework. EIF Version 2.0 was adopted by the College of Commissioners, "as of a higher status and importance than EIF version 1" which was more guidance than instruction. EIF2.0 has been very severely criticized by open source advocates, with the EC accused of regulatory capture by large software companies, and the interoperability requirements substantially watered down (Moody 2010 [14]).

The new standard-setting framework was established by end-2010, intended to result in a widening of participation from European telecoms standards body ETSI to more Internet-based standards bodies, W3C and IETF in particular, arguably about twenty years too late (ITU 2010 [15]). She explains that her proposal benefits these 'truly open' standards with two paths to approval: "via a fast-track approval of their standards through a process hosted by a traditional European standards body such as ETSI, or through the assessment of these bodies' compliance with certain criteria regarding notably openness, consensus, balance and transparency." On licensing standards, she notes the Commission draft horizontal agreements guidelines of 2009, which came into force in January 2011, and aid in allocating FRAND pricing for accessing essential technologies (EC 2011). Kroes does not argue for uniformity: "Standard-setting for software interoperability is not the same as setting a new standard for, say, digital television or mobile telephony." She continues to suggest strategic action to encourage open standards. This suggests an additional legislative requirement that government support for standards must rely on best practice in licensing including royalty terms.

Kroes' agenda embraces research funding and government IT procurement. European law requires governments to ensure they open public procurement contracts above a minimum size to all European firms, to encourage the development of the single European market (Directive EC/2004/18 [16]). As government spending is about half of European GDP, this opens the largest single information technology market to interoperability. Member states that fail to register procurement contracts with the European Commission are subject to infringement actions and ultimately court proceedings, though this implementation has not been as rigorous as it might be. Market-setting procurement European Commission policy can be used to pursue EIF2.0.

On IT procurement by European governments, Kroes suggests "detailed guidance on how to analyse a technology buyer's requirements in order to make best use of ICT standards in tender specifications". Governments became unintentionally locked into proprietary technology for decades. An IT vendor 'cartel' was alleged by government buyers on both sides of the Atlantic in 2011, publicly voicing their

frustration at the limited choices available. EIF 2.0 contains a 'comply or explain' requirement if government buyers do not adopt an available open standard, which follows the practice in Kroes' own country, Netherlands.

In the first phase, the European Commission [17] adopted the Communication, to "establish a common approach for Member States public administrations, to help citizens and businesses to profit fully from the EU's Single Market." The EC four prong strategy is 1. Common frameworks in support of interoperability, 2. Reusable generic tools, 3. Common services (operational applications and infrastructures of a generic nature to meet user requirements across policy areas), and 4. Analysis of the ICT side in the implementation of new EU legislation. As Ganslandt [18] argues, the four prongs are not likely to be sufficient without a more effective enforcement strategy. The European Parliament (COD/2011/0150 [19]) responded to the standards strategy by proposing direct funding for SMEs (small and medium sized enterprises) and civil society to participate in the standards which underpin the entire strategy, confirming a multi-stakeholder approach to be adopted, though substantial disagreement ensured in Committee over whether 'balanced', 'relevant' or 'appropriate' representation be established and financially supported. These proposals are promising but no conclusions can be drawn, as they are both ambitious and yet to be implemented in practice.

# 8. Conclusions

In this deliverable we presented a survey on Internet Science Research, investigating the various related research threads and trends. It is evident that although a great interest and effort exists from different disciplines, current Internet research lacks an integrated approach; the disciplines remain somewhat "stove piped" in different silos. This *fragmentation* in research in the various associated fields and disciplines represents the primary reason behind the fact that development in the Internet and other disciplines occurs in a highly unsynchronized manner. What is missing is to *bring together these many solutions and approaches into a holistic and coherent scientific framework* with associated evaluative and design methodologies. This holistic approach can be used to understand Internet development, and to harness the creatively destructive force of the tussles of the Internet to stimulate the productive consequences of the Internet, improve its resilience and robustness and use the combined technological and human systems of the extended Internet to address wider societal, environmental, economical and other objectives in a holistic manner.

In the quest of addressing this need for a scientific understanding of what is the Internet today, one should observe that networks in their broadest view, e.g. in form of human networks, roads, postal service and telephony have a very long history. However, it is only during the past years, with the development of online social networks, an increased understanding of complex systems and the wide availability of the Internet, that one could identify some common principles among these historical networks and the newcomer Internet. This observation underlines the call for an Internet Science to become a unifying discipline that borrows some of its principles from other well-established sciences as computer science, physics, economics, social science, etc. and has also its own particular fundamental laws and principles, similar to any other empirical science.

*Next version of this deliverable called "Internet Science-Going Forward" will delve into these necessities, seek to indicate directions for a holistic approach of Internet Science and provide a Roadmap to Horizon 2020.*

# 9. References

## 9.1 *Section 2 - Introduction*


1. D. Clark, J. Wroclawski, K. Sollins, and R. Braden, Tussle in cyberspace: defining tomorrow's Internet, IEEE/ACM Transactions on Networking, 13(3), pp. 462-475, 2005.
2. http://plato.stanford.edu/entries/globalization/.
3. P. R. Krugman, Geography and Trade 1994, MIT Press 1991.
4. F. Webster, Theories of the Information Society, London Routledge 1999.
5. S. Wyatt, Technology and inequality : questioning the information society, London Routledge 2000.
6. M. Thelwall, Link Analysis: An Information Science Approach. Academic Press, 2004.
7. M. Thelwall, Introduction to Webometrics: Quantitative Web Research for the Social Sciences. San Rafael, CA: Morgan & Claypool (Synthesis Lectures on Information Concepts, Retrieval, and Services, Vol. 1, No. 1, 2009.
8. J. Fry, Studying the Scholarly web: How disciplinary culture shapes online representations. Cybermetrics 10(1), 2006. http://www.cybermetrics.info/articles/v10i1p2.html.
9. S. Antonijevic, L. Gurak, Trust in Online Interaction: An Analysis of the Socio-Psychological Features of Online Communities and User Engagement, International Conference Cultural Heritage Online, Florence, Italy, pp. 65-69, 2009.
10. S. Antonijevic, From Text to Gesture Online: A Microethnographic Analysis of Nonverbal Communication in the 'Second Life' Virtual Environment, Information, Communication, and Society, 11 (2): London: Routledge, 1, pp. 211-238, March 2008.


## 9.2 *Section 3 – Network Science Perspective*


1. T. Lewis, Network science: theory and practice, John Wiley and Sons, 2009.
2. R. Albert, A.L. Barabasi, Statistical mechanics of complex networks, Rev. Mod. Phys. 74.
3. P. Van Mieghem, J. Omic, and R. E. Kooij, Virus spread in networks, IEEE/ACM Transactions on Networking, 17(1):1-14, February 2009.
4. J. G. Restrepo, E. Ott, and Brian R. Hunt, Onset of synchronization in large networks of coupled oscillators. Physical Review E, 71(036151):1-12, 2005.
5. S. Baccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang, Complex networks: Structure and dynamics. Physics Reports, 424:175-308, 2006.
6. L. Da F. Costa, F. A. Rodrigues, G. Travieso, and P. R. Villas Boas, Characterisation of complex networks: A survey of measurements, Advances in Physics, 56(1):167-242, Februari 2007.
7. P. Van Mieghem, Performance Analysis of Communications Systems and Networks, Cambridge University Press, Cambridge, U.K., 2006.
8. P. Van Mieghem, Graph Spectra for Complex Networks, Cambridge University Press, Cambridge, U.K., 2011.
9. P. Van Mieghem, J. Omic, and R. E. Kooij, Virus spread in networks, IEEE/ACM Transactions on Networking, 17(1):1-14, February 2009.

10. S. H. Strogatz, From Kuramoto to Crawford: exploring the onset of synchronization in populations of coupled oscillators. Physica D, 143:1-20, 2000.
11. J. G. Restrepo, E. Ott, and Brian R. Hunt, Onset of synchronization in large networks of coupled oscillators. Physical Review E, 71(036151):1-12, 2005.
12. S. N Dorogovtsev and A. V. Goltsev, Critical phenomena in complex networks, Reviews of Modern Physics, 80:1275-1335, October-December 2008.
13. S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, Catastrophic cascade of failures in interdependent networks, Nature Letters, 464:1025-1028, April 2010.
14. Li, C., H. Wang, W. de Haan, C. J. Stam, P. Van Mieghem, The Correlation of Metrics in Complex Networks with Applications in Functional Brain Networks, Journal of Statistical Mechanics: Theory and Experiment (JSTAT), November 2011.
15. Bauer, D. Clark, W. Lehr, Understanding broadband speed measurements, MITAS project white paper, June 2010.
16. J. C. De Martin, A. Glorioso, The Neubot project: A collaborative approach to measuring internet neutrality, IEEE International Symposium on Technology and Society, Fredericton (Canada), DOI 10.1109/ISTAS.2008.4559763.
17. S. Basso, A. Servetti and J. C. De Martin, The network neutrality bot architecture: a preliminary approach for self-monitoring of Internet access QoS, IEEE 16th International Symposium on Computers and Communications, DOI 10.1109/ISCC.2011.5983857.
18. http://measurementlab.net/
19. http://netindex.com/
20. J. Palfrey, and J. Zittrain, Better Data for a Better Internet, Science, volume 334, number 6060, 2011.
21. M. Lemley and L. Lessig, "The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era," Ucla L. Rev., vol. 48, p. 925, 2000.
22. R. Beverly, S. Bauer, and A. Berger, "The internet is not a big truck: toward quantifying network neutrality," Passive and Active Network Measurement, pp. 135–144, 2007.
23. Switzerland Network Testing Tool - Electronic Frontier Foundation. [Online]. Available: https://www.eff.org/pages/switzerland-network-testing-tool
24. M. Dischinger, A. Mislove, A. Haeberlen, and K. Gummadi, "Detecting bittorrent blocking," in Proceedings of the 8th ACM SIGCOMM conference on Internet measurement. ACM, pp. 3–8, 2008.
25. NNMA-NNSquad Network Measurement Agent. [Online]. Available: http://www.nnsquad.org/agent
26. N. Weaver, R. Sommer, and V. Paxson, "Detecting forged TCP reset packets," Proc. of NDSS, Citeseer, 2009.
27. M. Tariq, M. Motiwala, and N. Feamster, "NANO: Network Access Neutrality Observatory," in Proceedings of ACM HotNets, Citeseer, 2008.
28. Y. Zhang, Z. Mao, and M. Zhang, "Ascertaining the Reality of Network Neutrality Violation in Backbone ISPs," in Proc. of ACM HotNets-VII Workshop, 2008.
29. WindRider – A Mobile Network Neutrality Monitoring System. [Online]. Available: http://www.cs.northwestern.edu/ ict992/mobile.htm

30. BISMark – Monitor and Manage Your Home Network. [Online]. Available: http://projectbismark.net/signup.html
31. Grenouille.com - la meteo du net depuis 2000. [Online]. Available: http://www.grenouille.com/
32. R. Prasad, C. Dovrolis, M. Murray, and K. Claffy, "Bandwidth estimation: metrics, measurement techniques, and tools," Network, IEEE, vol. 17, no. 6, pp. 27–35, 2003.
33. http://measurementlab.net/
34. L. C. Freeman, "A set of measures of centrality based on betweenness," Sociometry, vol. 40, no. 1, pp. 35–41, 1977.
35. S. P. Borgatti, M.G. Everett, "A graph-theoretic framework for classifying centrality measures.", Social Networks 28(4): 466-484, 2006.
36. P. Holme et al., "Attack vulnerability of complex networks", PhysRev E.65, 056109, 2002.
37. A. Vespignani, "Predicting the behavior of tecno-social systems." Science. 325, no. 5939: 425-428, 2009.
38. L. Dall'Asta et al. , "Vulnerability of weighted networks" J. Stat. Mech. P04006, 2006.
39. U. Brandes and C. Pich, "Centrality estimation in large networks," in Intl. Journal of Bifurcation and Chaos, Special Issue on Complex Networks Structure and Dynamics, 2007.
40. R. Geisberger, P. Sanders, and D. Schultes, "Better approximation of betweenness centrality," in Proceedings of the Ninth Workshop on Algorithm Engineering and Experiments (ALENEX), 2008.
41. D. E. K. Jiang and D. Bader, "Generalizing k-betweenness centrality using short paths and a parallel multithreaded implementation," in ICPP'09, Vienna, Austria, September 2009, pp. 542–549.
42. P. Pantazopoulos, , M. Karaliopoulos, and I. Stavrakakis, "Assessing the value of localized centrality metrics," Tech. Rep., April 2011. [Online]. Available: http://cgi.di.uoa.gr/~istavrak/publications.html
43. W. Banzhaf, Artificial chemistries towards constructive dynamical systems. Solid State Phenomena 97-98, pp. 43-50, 2004.
44. P. Dittrich, Artificial Chemistry, in Meyers, RA (Ed.), Encyclopedia of Complexity and Systems Science, Springer, pp. 326-344, 2009.
45. P. Dittrich, P. Speroni di Fenizio, Chemical organisation theory, Bulletin of Mathematical Biology, Vol 69, N 4, pp. 1199-1231, 2007.
46. K. Krohn, J. Rhodes, Algebraic Theory of Machines. I. Prime Decomposition Theorem for Finite Semigroups and Machines, Transactions of the American Mathematical Society, Vol 116, pp. 450-464, 1965.
47. A. Egri-Nagy, CL. Nehaniv, SgpDec - software package for hierarchical coordinatization of groups and semigroups, implemented in the GAP computer algebra system, Version 0.5.19, 2010. http://sgpdec.sf.net.
48. A. Egri-Nagy, CL. Nehaniv, J. Rhodes, MJ Schilstra, "Automatic Analysis of Computation in Biochemical Reactions," *BioSystems*, Vol 94, Issues 1-2, pp. 126-134, 2008.
49. A. Egri-Nagy, CL. Nehaniv, "Hierarchical coordinate systems for understanding complexity and its evolution with applications to genetic regulatory networks", *Artificial Life*, Vol 14, No 3, pp. 299-312 (Special Issue on the Evolution of Complexity), 2008.

50. A. Egri-Nagy, CL. Nehaniv, "Algebraic Properties of Automata Associated to Petri Nets and Applications to Computation in Biological Systems", *BioSystems*, Vol 94, Issues 1-2, pp. 135-144, 2008.
51. P. Dömösi, CL. Nehaniv, Algebraic Theory of Automata Networks. Philadelphia: SIAM, 2005.
52. P. Dini, CL Nehaniv, A. Egri-Nagy, MJ Schilstra, Algebraic Analysis of the Computation in the Belousov-Zhabotinksy Reaction, in Lones, *IPCAT2012: 9th International Conference on Information Processing in Cells and Tissues*, Springer LNCS 7223, Cambridge, UK, 30 March-2 April, pp. 216-224, 2012.
53. WD Maurer, J. Rhodes, A property of finite simple non-Abelian groups, Proc. Amer. Math. Soc., Vol 16, pp. 552-554, 1965.
54. G. Horváth, Functions and Polynomials over Finite Groups from the Computational Perspective, PhD thesis, University of Hertfordshire, 2008.
55. A. Pyka, A. Scharnhorst, Network perspectives on innovations: Innovative networks – network innovation, Innovation Networks, Springer Berlin et al., 2009.

## 9.3 *Section 4 –Dimension of the "Web"*

### 9.3.1 Section 4.1 – Virtual Communities

1. G. Aichholzer, H. Burkert, Public Sector Information in the Digital Age. Between Markets, Public Management and Citizens Right, In EE, Celtenham, 2004.
2. Y. Benkler, The Penguin and the Leviathan: How Cooperation Triumphs over Self-Interest, Crown Business, 2011.
3. L. Lessig, Code and Other Laws of Cyberspace (also in its second version, 1999 and 2006 respectively).
4. C. Hess, E. Elinor Ostrom, Ideas, Artifacts and Facilities: Information as a Common-Pool Resource, Cited: 66 Law & Contemp. Probs. 111, 2003.
5. C. Bizer, T. Heath B-L. Tim, Linked Data - The Story So Far, in The International Journal on Semantic Web and Information Systems, pp. 1-22, vol. 5, issue 3, 2009.
6. M. van Echooud, B. van der Wal, Creative commons licensing for public sector information. Opportunities and pitfalls, v.3, Institute for Information Law, University of Amsterdam, 2008.
7. D. Bollier, Viral Spiral: How the Commoners Built a Digital Republic of Their Own, New Press, 2009
8. M. S. Granovetter, The Strength of Weak Ties, The American Journal of Sociology 78, pp. 1360-1380, 1973.
9. S. G. Roberts, Constraints on Social Networks, in: Social Brain, Distributed Mind (Proceedings of the British Academy), pp. 115–134, 2010.
10. S. G. Roberts, R. I. Dunbar, T. V. Pollet, T. Kuppens, Exploring variation in active network size: Constraints and ego characteristics, Social Networks 31, pp. 138–146, 2009.
11. P. S. Dodds, R. Muhamad, D. J. Watts, An experimental study of search in global social networks, Science 301, pp. 827–9, 2003

12. M. E. J. Newman, D. J. Watts, S. H. Strogatz, Random graph models of social networks, Proceedings of the National Academy of Sciences of the United States of America 99 Suppl 1 pp. 2566–2572, 2002.
13. J. Leskovec, E. Horvitz, Planetary-Scale Views on an Instant- Messaging Network, Technical Report, 2007.
14. W.X. Zhou, D. Sornette, R. a. Hill, R. I. M. Dunbar, Discrete hierarchical organisation of social group sizes., in: Biological sciences, volume 272, pp. 439–44.
15. R. I. M. Dunbar, S. Roberts, Communication in Social Net- works: Effects of Kinship, Network Size and Emotional Close- ness, Personal Relationships 18, pp. 439–452, 2011.
16. R. A. Hill, R. I. M. Dunbar, Social network size in humans, Human Nature 14 pp. 53–72, 2003
17. P. V. Marsden, K. E. Campbell, Measuring Tie Strength, Social Forces 63 pp. 482–501, 1984.
18. J. Ugander, B. Karrer, L. Backstrom, C. Marlow, The Anatomy of the Facebook Social Graph, CoRR abs/1111.4, 2011.
19. L. Backstrom, P. Boldi, M. Rosa, J. Ugander, S. Vigna, Four Degrees of Separation, CoRR abs/1111.4, 2011.
20. K. N. Hampton, L. S. Goulet, L. Rainie, P. Kristen, Social networking sites and our lives, Technical Report, Pew Internet & American Life Project, 2011.
21. M. Burke, C. Marlow, T. Lento, Social Network Activity and Social Well-Being, in: international conference on Human factors in computing systems, pp. 2–5.
22. N. B. Ellison, C. Steinfield, C. Lampe, The Benefits of Face- book Friends: Social Capital and College Students Use of Online Social Network Sites, Journal of Computer-Mediated Communication 12, pp. 1143–1168, 2007.
23. E. Gilbert, K. Karahalios, Predicting tie strength with social media, in: International conference on Human factors in com- puting systems, ACM Press, New York, New York, USA, 2009.
24. J. Onnela, J. Saramaki, J. Hyvonen, G. Szabo, D. Lazer, K. Kaski, J. Kertesz, A. Barabasi, Structure and tie strengths in mobile communication networks., in: National Academy of Sciences of the United States of America, volume 104, pp. 7332– 7336.
25. P. V. Marsden, Core Discussion Networks of Americans, Amer- ican Sociological Review 52 pp. 122–131, 1987.
26. J. Travers, S. Milgram, An Experimental Study of the Small World Problem, Sociometry, 1969.
27. B. Goncalves, N. Perra, A. Vespignani, Validation of Dunbar's number in Twitter conversations, Networks 2011.
28. V. Arnaboldi, A. Passarella, M. Tesconi, D. Gazz`e, Towards a Characterisation of Egocentric Networks in Online Social Net- works., in: R. Meersman, T. S. Dillon, P. Herrero (Eds.), OTM Workshops, volume 7046 of Lecture Notes in Computer Science, Springer, pp. 524–533, 2011.
29. M. Priest, The Privatisation of Regulation: Five Models of Self-regulation, Ottawa Law Review Vol.29, pp. 233-301, 1997.
30. R. A. Spinello, Regulating Cyberspace: The Policies and Technologies of Control, Greenwood Publishing, Westport, London, 2002.
31. Mayer-Schönberger, Viktor and Malte Ziewitz, Jefferson Rebuffed, Columbia Science and Technology Law Review, Vol.8, pp.188-238 at p.225, 2007.
32. T. Wu, When Code Isn't Law, Virginia Law Review Vol.89, No.4, pp.679-751, 2003.

33. P.Richard, Economic Analysis of Law, 7th ed., Wolters Kluwer, New York, 2007.
34. R. C. Ellickson, Order without law – How neighbors settle disputes, Harvard University Press at p.208, 1991.
35. E. A. Posner, Law and Social Norms: The Case of Tax Compliance Virginia Law Review Vol.86, No.8, pp.1781-1819.
36. IDATE–TNO–IViR, User Created Content: Supporting a participative Information Society at http://ec.europa.eu/information_society/eeurope/i2010/docs/studies/ucc-annexes.pdf, 2008.
37. C.R. Sunstein, Switching the default rule, New York University Law Review Vol. 77, pp. 106-34, 2002.
38. J. Weinberg,Rating the Net, Hastings Communications and Entertainment Law Journal Vol. 19, pp. 453-82, 1997.
39. L. Lessig, Guest Blog Post: Lawrence Lessig, For The Record II at http://blogs.law.harvard.edu/palfrey/2010/07/11/guest-blog-post-lawrence-lessig/, 2010.
40. J. Goldsmith, T. Wu, Who Controls the Internet? Illusions of a Borderless World, Oxford University Press, 2006.
41. Viacom International, Inc. v. YouTube, Inc. No. 07 Civ. 2103, 2010.
42. European Network Information Security Agency, Security Issues and Recommendations for Online Social Networks, ENISA Position Paper No.1: at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf, 2007.
43. C. Ondrejka, Aviators, Moguls, Fashionistas and Barons: Economics and Ownership in SecondLife, available at http://ssrn.com/abstract=614663, 2004.
44. V. Mayer-Schonberger, J. Crowley, Napster's SecondLife?: The Regulatory Challenges of Virtual Worlds, Northwestern University Law Review Vol. 100, No. 4, http://www.vmsweb.net/attachments/pdf/NWLR100n4.pdf, 2006.
45. Source:http://secondlife.com
46. A. Giddens, The Third Way: The Renewal of Social Democracy, Polity Press: Cambridge, 1998.
47. G. Mulgan, C. Landry, The other invisible hand: Remaking charity for the 21st century, Demos: London, 1995.
48. G. Kelly, G. Mulgan, S. Muers. Creating Public Value: An analytical framework for public service, Cabinet Office, UK Government, London, 2002.
49. W. Richter, 'Better' Regulation Through Social Entrepreneurship? Innovative And Market-Based Approaches To Address The Digital Challenge To Copyright Regulation, Thesis submitted for the Degree of Doctor of Philosophy, Oxford Internet Institute, Oxford University, 2010.
50. J. Robinson, Navigating Social and Institutional Barriers to Markets: How Social Entrepreneurs Identify and Evaluate Opportunities in Johanna Mair, Social Entrepreneurship, Hampshire: New York, 2006.
51. A. Nicholls, A. H.Cho, Social Entrepreneurship: The Structuration of a Field in Alex Nicholls (ed.) Social Entrepreneurship, Oxford University Press, at p.102, 2006.
52. CIC Regulator, Guidance – Overview of a Community Interest Company available at http://www.cicregulator.gov.uk/Leaflets/OverviewLeafletMarch2008.pdf, 2008.
53. J. W. Kingdon, Agendas, Alternatives, and Public Policies, Little Brown and Company, Boston, 1984.

54. M. Schneider, P.Teske, Toward a Theory of the Political Entrepreneur: Evidence from Local Government, American Political Science Review Vol.86, No.3, pp.737–747, 1992.
55. R. Spear, E. Bidet, The role of Social Enterprise in European Labour Markets, EMES working paper series 3/10 at p.8, 2003.
56. A. Nicholls, What is the Future of Social Enterprise in Ethical Markets? Office of the Third Sector available at http://www.cabinetoffice.gov.uk/third_sector/Research_and_statistics/social_enterprise_research/think_pieces.aspx, 2007.
57. C. Marsden, Beyond Europe: The Internet, Regulation, and Multi-stakeholder Governance—Representing the Consumer Interest? Journal of Consumer Policy Vol.31, Iss.1, pp.115–132, 2008.
58. J. Braithwaite, Regulatory Capitalism: How It Works, Ideas for Making It Better, Cheltenham: Edward Elgar, 2008.
59. J. Zittrain, ICANN: Between the Public and the Private – Comments before Congress, Berkeley Law Technology Journal Vol.14, pp. 1070-1094, 1999.
60. M. Price, S. Verhulst, Self-Regulation and the Internet, Amsterdam: Kluwer, 2005.
61. C. Leadbeater, The Rise of the Social Entrepreneur, Demos, London, 1997.
62. J. Emerson, F. Twersky, New Social Entrepreneurs: The Success, Challenge and Lessons of Non-profit Enterprise Creation, Roberts Foundation, California, 1996.
63. J. Thompson, The world of the social entrepreneur in International Journal of Public Sector Management, Vol.15, No. 5, pp. 412–431, 2002.
64. A. Prakash, M. Gugerty, Trust but verify? Voluntary regulation programs in the nonprofit sector, Regulation & Governance, 4(1), pp. 22-47, 2010.
65. P.M. Santiago del Río, J. Ramos, J.L. García-Dorado, J. Aracil, A. Cuadra-Sánchez and M. Cutanda-Rodríguez, "On the processing time for detection of Skype traffic", 2nd International Workshop on Traffic Analysis and Classification (IWCMC2001-TRAC), Istanbul, Turkey, July 2011.
66. S. Han, K. Jang, K. Park and S. Moon. PacketShader: Massively Parallel Packet Processing with GPUs to Accelerate Software Routers, USENIX NSDI poster, San Jose, California, April 2010.
67. X. Cui, J. St. Charles, The GPU Enhanced Parallel Computing for Large Scale Data Clustering, International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2011
68. S. H. Lee, P.J. Kim, H. Jeong. Statistical properties of sampled networks. Physical Review E, 73, 2006.
69. N. Blenn, C. Doerr, B. Van Kester, P. Van Mieghem, Crawling and Detecting Community Structure in Online Social Networks using Local Information, Networking 2012.
70. T. Cormen, Introduction to algorithms. MIT electrical engineering and computer science series, MIT Press, 2001.
71. S. L. Feld, "Why Your Friends Have More Friends Than You Do," American Journal of Sociology, vol. 96, no. 6, pp. 1464–1477, 1991.
72. M. Kurant, A. Markopoulou, and P. Thiran, "On the bias of BFS (Breadth First Search)," in Teletraffic Congress (ITC), 2010 22nd International, pp. 1–8, IEEE, 2010.

### 9.3.2 Section 4.2 - Trust and Reputation


1. S. D. Kamvar, M. T. Schlosser, and H. Garcia Molina. The EigenTrust algorithm for reputation management in P2P networks. Proc. 12th ACM International Conference World Wide Web (WWW), pp. 640–651, May 2003.
2. S. Marti and H. Garcia-Molina. Limited Reputation Sharing in P2P Systems. In Proc. Of ACM Conference on Electronic Commerce, pp. 91–101, 2004.
3. L. Xiong, L. Liu, PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities. IEEE Transactions on Knowledge and Data Engineering, 16(7):843–857, 2004.
4. Th. G. Papaioannou and G. D. Stamoulis. Reputation-based Policies that Provide the Right Incentives in Peer-to-Peer Environments. Computer Networks (Special Issue on Management in Peer-to-Peer Systems: Trust, Reputation and Security), Elsevier, 50(4):563–578, 2006.
5. H. T. Kung and C. H. Wu. Differentiated Admission for Peer-to-Peer Systems: Incentivizing Peers to Contribute their Resources. In Proc. of the Workshop on Economics of Peer-to-Peer Systems, June 2003.
6. N. Andrade, M. Mowbray, A. Lima, G. Wagner, and M. Ripeanu. Influences on Cooperation in BitTorrent Communities. Proc. ACM SIGCOMM, August 2005.
7. L. Mekouar, Y.Iraqi, and R.Boutaba. A contribution-based service differentiation scheme for peer-to-peer systems. Peer-to-Peer Networks and Applications journal, Springer, 2(2), June 2009.
8. A.Satsiou, L.Tassiulas. Trust-Based Exchange of Services to Motivate Cooperation in P2P Networks, Peer-to-Peer Networking and Applications Journal, Springer, 4(2), pp. 122-145, April 2011.
9. A.Satsiou, L.Tassiulas. Reputation-based Resource Allocation in P2P Systems of Rational Users. IEEE Transactions on Parallel and Distributed Systems, 21 (4), pp. 466-479, April 2010.
10. P.Antoniadis, B.Le Grand, A.Satsiou, L.Tassiulas, R.Aguiar, J.Barraca, and S.Sargento. Community Building over Neighbourhood Wireless Mesh Networks. IEEE Technology and Society, special issue on Potential and Limits of Cooperation in Wireless Communications, 27(1):48–56, 2008.
11. A.Satsiou and L.Tassiulas. Reputation-based Internet Sharing in Wireless Neighborhood Community Networks. In Proc. of the IEEE International Conference on Communications, May 2010.
12. Y. Rebahi, V. Mujica, D. Sisalemin. A Reputation-Based Trust Mechanism for Ad Hoc Networks. 10th IEEE Symposium on Computers and Communications, 2005.
13. S. Jianhua, M. Chuanxiangin, A Reputation-based Scheme against Malicious Packet Dropping for Mobile Ad Hoc Networks. Proc. IEEE International Conference on Intelligent Computing and Intelligent Systems, 2009.
14. S. Abbas, M. Merabti, D. Llewellyn-Jones, D. Llewellyn-Jonesin. The Effect of Direct Interactions on Reputation Based Schemes in Mobile Ad hoc Networks. IEEE Consumer Communications and Networking Conference, 2011.
15. A. Josang, R. Ismail, C. Boyd. A survey of Trust and Reputation Systems for Online Service Provision, Decision Support Systems, 43(2), pp. 618-644, 2007.
16. http://ebay.com/

17. http://www.amazon.com/
18. http://www.allexperts.com/
19. http://www.askmecorp.com/
20. http://www.advogato.org/trust-metric.html
21. http://epinions.com/
22. http://slashdot.org/
23. http://www.kuro5hin.org/
24. http://openratings.com
25. L. Page, S. Brin, R. Motwani, and T. Winograd. The PageRank Citation Ranking: Bringing Order to the Web. Technical report, Stanford Digital Library Technologies Project, 1998.
26. http://trust.mindswap.org/FilmTrust/
27. B. Carminati, E. Ferrari, A. Perego. Enforcing Access Control in Web-based Social Networks, ACM Transactions on Information and System Security, Volume 13 Issue 1, October 2009.
28. http://facebook.com
29. http://www.myspace.com/
30. http://friendster.com
31. http://www.linkedin.com
32. http://www.orkut.com
33. http://repcheck.com
34. S.R. Kruk, S. Grzonkowski, H. C. Choi, T. Woroniecki, A. Gzella, D-FOAF: Distributed identity management with access rights delegation. In The Semantic Web – ASWC, LNCS, vol. 4185. Springer, pp. 140–154, 2006.
35. H.C. Choi, S. R. Kruk, S. Grzonkowski, K. Stankiewicz, B. Davis, J.G. Breslin, Trust models for community-aware identity management. In Identity, Reference, and the Web Workshop, IRW, Online: http://www.ibiblio.org/hhalpin/irw2006/skruk.pdf, 2006.
36. M. J. Pujol, R. Sanguesa, and J. Delgado. Extracting reputation in multi agent systems by means of social network topology, In Proc. of Int'l Conf. on Autonomous Agents and Multi-Agents Systems, pp. 467-474, 2002.
37. W. Zhang, S.K. Das, Y. Liu. A Trust Based Framework for Secure Data Aggregation in Wireless Sensor Networks, Proc. Of IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, 2006.
38. S. Ozdemir, Functional reputation-based reliable data aggregation and transmission for wireless sensor networks, Computer Communications, Vol. 31, No. 17, pp. 3941–3953, November 2008.
39. H. Chen, Task-based Trust Management for Wireless Sensor Networks, International Journal of Security and Its Applications, Vol. 3, No. 2, April 2009.
40. European Commission C(2011)5068, Objective ICT-2011.1.4 Trustworthy ICT, footnote 11, 2011.
41. E. Shi, A. Perrig, "Designing secure sensor networks," Wireless Communications, IEEE , vol.11, no.6, pp. 38- 43, Dec. 2004.
42. A. Perrig, J. Stankovic, D. Wagner, Security in wireless sensor networks. Communications of the ACM, 47(6), 53 – 57, 2004.

43. G. Hoblos, M. Staroswiecki, A. Aitouche, Optimal design of fault tolerant sensor networks, IEEE International Conference on Control Applications, Anchorage, AK, pp. 467–472, September 2000
44. D. Nadig, S.S. Iyengar, A new architecture for distributed sensor integration, Proceedings of IEEE Southeastcon'93, Charlotte, NC, April 1993.
45. C. Shen, C. Srisathapornphat, C. Jaikaeo, Sensor information networking architecture and applications, IEEE Personal Communications, pp. 52–59 August 2001.
46. R. Zhang, Z. Zilic, K. Radecka, "Energy efficient software-based self-test for wireless sensor network nodes," VLSI Test Symposium, Proceedings. 24th IEEE, April 30 2006-May 4 2006.
47. Z. Taghikhaki, M. Sharifi, "An Efficient Algorithm to Detect Faulty Reading in Wireless Sensor Network Using the Concept of Reputation," Computational Intelligence for Modelling Control & Automation, 2008 International Conference on , pp.969-974, 10-12 Dec. 2008.
48. M. Li, W. Lou, K. Ren, "Data security and privacy in wireless body area networks," Wireless Communications, IEEE , vol.17, no.1, pp.51-58, February 2010.
49. G. Karlsson, V. Lenders, and M. May, "Delay-tolerant broadcasting," IEEE Transactions on Broadcasting, vol. 53, March 2007.
50. J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing robust and ubiquitous security support for mobile ad hoc networks," ICNP, 2001.
51. P. R. Zimmermann, The Official PGP User's Guide. MIT press, 1995.
52. J. R. Douceur, "The sybil attack," in IPTPS, 2002.
53. A. Chaintreau, P. Hui, C. Diot, R. Gass, and J. Scott, "Impact of human mobility on opportunistic forwarding algorithms," IEEE TMC, vol. 6, 2007.
54. P. Hui, E. Yoneki, S. Y. Chan, and J. Crowcroft, "Distributed community detection in delay tolerant networks," MobiArch, 2007.
55. S. Capkun, J.-P. Hubaux, and L. Buttyan, "Mobility helps peer-to-peer security," IEEE TMC, vol. 5, 2006.
56. C. Piro, C. Shields, and B. N. Levine, "Detecting the sybil attack in mobile ad hoc networks," in Securecomm and Workshops, 2006.
57. H. Yu, M. Kaminsky, P. B. Gibbons, and A. D. Flaxman, "Sybilguard: Defending against sybil attacks via social networks," IEEE/ACM ToN, vol. 16, 2008.
58. A. Tangpong, G. Kesidis, H. yuan Hsu, and A. Hurson, "Robust Sybil Detection for MANETs," in ICCCN, 2009.
59. S. Buchegger and J.-Y. Le Boudec, "A Robust Reputation System for Peer-to-Peer and Mobile Ad-hoc Networks," in P2PEcon, 2004.
60. D. Quercia, S. Hailes, and L. Capra, "B-trust: Bayesian trust framework for pervasive computing," in iTrust, 2006.
61. J. Liu and V. Issarny, "Enhanced reputation mechanism for mobile ad hoc networks," in iTrust, 2004.
62. K. Walsh and E. G. Sirer, "Experience with an object reputation system for peer-to-peer filesharing," in NSDI, 2006.
63. D. Quercia, S. Hailes, and L. Capra, "Lightweight distributed trust propagation," in ICDM, 2007.
64. D. Quercia, S. Hailes, and L. Capra, "MobiRate: Making Mobile Raters Stick to their Word," in UbiComp, 2008.

65. R. Housley, W. Ford, W. Polk, and D. Solo, “Internet x.509 public key infrastructure certificate and crl profile,” 1999.
66. S. Capkun, L. Buttyan, and J.-P. Hubaux, “Self-organised public-key management for mobile ad hoc network,” IEEE TMC, vol. 2, 2003.
67. Y. Lin, A. Studer, H. Hsiao, J. McCune, K. Wang, M. Krohn, P. Lin, A. Perrig, H. Sun, and B. Yang, “SPATE: Small-group PKI-less Authenticated Trust Establishment,” in MobiSys, 2009.
68. M. E. J. Newman, “Fast algorithm for detecting community structure in networks,” Physical Review E, vol. 69, 2004.
69. V. D. Blondel, J.L. Guillaume, R. Lambiotte, and E. Lefebvre, “Fast unfolding of communities in large networks,” Journal of Statistical Mechanics: Theory and Experiment, 2008.
70. A. Clauset, “Finding local community structure in networks,” Physical Review E, vol. 72, 2005.
71. P. Hui, J. Crowcroft, and E. Yoneki, “Bubble rap: Social-based forwarding in delay tolerant networks,” in MobiHoc, 2008.
72. S. Trifunovic, C. Anastasiades, F. Legendre, Social Trust in Opportunistic Networks, Second IEEE International Workshop on Network Science For Communication Networks (NetSciCom'10), San Diego, CA, USA, March, 2010.

#### 9.3.3 Section 4.3 – Identity and Privacy

1. E. De Cristofaro, M. Manulis, B. Poettering, Private Discovery of Common Social Contacts, ACNS 2010, (eprint.iacr.org/2011/026.pdf)
2. H. C. Pöhls, A. Bilzhause, K. Samelin and J. Posegga, Sanitizable Signed Privacy Preferences for Social Networks, In Proc. of GI Workshop on Privacy and Identity Management for Communities - Communities for Privacy and Identity Management, DICCDI 2011.
3. L. Huang et al., Privacy-Preserving Friend Search over Online Social Networks (eprint.iacr.org/2011/445)
4. N. B. Ellison, C. Steinfield, C. Lampe. The Benefits of Facebook Friends: Social Capital and College Students Use of Online Social Network Sites.
5. B. Zhou and J. Pei, Preserving Privacy in Social Networks Against Neighborhood Attacks.
6. A. Narayanan, V. Shmatikov, "De-anonymizing Social Networks", Security and Privacy, 30th IEEE Symposium, pp.173-187, 17-20 May 2009.
7. G. Ateniese, E. De Cristofaro, G. Tsudik: (If) Size Matters: Size-Hiding Private Set Intersection. Public Key Cryptography, pp. 156-173, 2011.
8. L. Marconi, M. Conti, R. Di Pietro: CASSANDRA: a probabilistic, efficient, and privacy-preserving solution to compute set intersection. Int. J. Inf. Sec. 10(5), pp. 301-319, 2011.
9. M.Conti, A. Hasani, B. Crispo, Virtual private social networks. CODASPY, pp. 39-50, 2011.
10. R. Gross, A. Acquisti, Information revelation and privacy in online social networks, pp. 71-80.
11. A. Juels, S.A. Weis, Defining Strong Privacy for RFID. Pervasive Computing and Communications Workshops, pp. 342-347, 2007.
12. M. Langheinrich, A Survey of RFID Privacy Approaches. Personal and Ubiquitous Computing 13(6), pp. 413, 2009.

13. S. Spiekermann, The RFID PIA - Developed by Industry, Agreed by Regulators, in Privacy Impact Assessment: Engaging Stakeholders in Protecting Privacy, Springer Verlag, Dodrecht, 2011.
14. S.L. Garfinkel, R. Pappu, RFID privacy: an overview of problems and proposed solutions. IEEE Security & Privacy, pp. 34-43, May-June 2005.
15. G. Anthes, G. Security in the cloud. Communications of the ACM, 53(11), November 2010.
16. M. Van Dijk, A. Juels, On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing. Proceedings of the 5th USENIX conference on Hot topics in security, pp. 1-8, 2010.
17. P. Ahonen, et al,Safeguards in a World of Ambient Intelligence. Springer Verlag, 2010.
18. J. Cas, Ubiquitous Computing, Privacy and Data Protection: Options and Limitations to Reconcile the Unprecedented Contradictions. In Gutwirth, S. et al. (eds.) Computers, Privacy and Data Protection: An Element of Choice, pp.139-169, 2011.
19. P. De Hert, S. Gutwirth, A. Moscibroda, D. Wright, G. Gonzalez Fuster, Legal safeguards for privacy and data protection in ambient intelligence. Personal and Ubiquitous Computing, 13(6), pp. 435-444, 2009.
20. A. Miller, Untangling the social web, The Economist, September, 2010.
21. L. Scism and M. Maremont, Insurers test data profiles to identify risky clients. Wall Street Journal, November, 2010.
22. N. Singer. Face recognition makes the leap from sci-fi. New York Times, November, 2011.
23. R. Gross and A. Acquisti, Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society, WPES '05, pp. 71–80, New York, NY, USA, 2005.
24. B. Krishnamurthy, C. E. Wills. Characterizing privacy in online social networks. In Proceedings of the first workshop on Online social networks, 2008.
25. B. Krishnamurthy, C. E. Wills, On the leakage of personally identifiable information via online social networks. SIGCOMM Comput. Commun. Rev., 40:112–117, Jan. 2010.
26. M. McPherson, L. S. Lovin, and J. M. Cook. Birds of a Feather: Homophily in Social Networks. Annual Review of Sociology, 27(1):415–444, 2001.
27. J. He, W. Chu, and Z. Liu. Inferring Privacy Information from Social Networks. In Intelligence and Security Informatics, volume 3975 of Lecture Notes in Computer Science, pages 154–165. Springer-Verlag, Berlin/Heidelberg, 2006.
28. E. Zheleva and L. Getoor. To join or not to join: The illusion of privacy in social networks with mixed public and private user profiles. In 18th International World Wide Web Conference, pp. 531–531, April 2009.
29. N. Blenn, C. Doerr, N. Shadravan, P. Van Mieghem, How Much do Your Friends Tell About You? Reconstructing Private Information from the Friendship Graph, Social Networking Sites 2012.
30. A. Shakimov, A. Varshavsky, L. P. Cox, and R. Caceres, Privacy, cost, and availability tradeoffs in decentralized osns, in Proc. of the WOSN, 2009.
31. R. Narendula, T. G. Papaioannou, and K. Aberer. My3: A highly-available P2P-based online social network. In Proc. of IEEE P2P 2011.

32. A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, Measurement and analysis of online social networks, in Proc. of the 7th Internet measurements conference, 2007.
33. S. Guha, K. Tang, and P. Francis, Noyb: privacy in online social networks, in Proc. of the WOSP, Seattle, WA, USA, 2008.
34. B. Krishnamurthy and C. E. Wills, On the leakage of personally identifiable information via online social networks, in Proc. of the WOSN, 2009.
35. L. A. Cutillo, R. Molva, and T. Strufe, Privacy preserving social networking through decentralization, in Proc. of the WONS, 2009.
36. R. Narendula, T. G. Papaioannou, and K. Aberer, Panacea: Tunable privacy for access controlled data in peer-to-peer systems, in Proc. of International Teletraffic Congress (ITC-22), 2010.
37. I.F. Lam, K.-T. Chen, and L.-J. Chen, Involuntary information leakage in social network services, in Proc. of the 3rd International Workshop on Security, 2008.
38. A. Tootoonchian, S. Saroiu, Y. Ganjali, and A. Wolman, Lockr: better privacy for social networks, in Proc. of the CoNEXT, 2009.
39. R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, Persona: an online social network with user-defined privacy, in Proc. of the ACM SIGCOMM, 2009.
40. M. M. Lucas and N. Borisov, Flybynight: mitigating the privacy risks of social networking, in Proc. of the WPES, 2008.
41. S. Buchegger, D. Schioberg, L.H. Vu, and A. Datta, Peerson: P2p social networking: early experiences and insights, in Proc. of the ACM EuroSys Workshop on Social Network Systems, 2009.
42. J. A. Pouwelse, P. Garbacki, J. Wang, A. Bakker, J. Yang, A. Iosup, D. H. J. Epema, M. Reinders, M. R. van Steen, and H. J. Sips, Tribler: a social-based peer-to-peer system: Research articles, Concurr. Comput. : Pract. Exper. , vol. 20, no. 2, pp. 127-138, 2008.
43. K. Graffi, P. Mukherjee, B. Menges, D. Hartung, A. Kovacevic, and R. Steinmetz, Practical security in p2p-based social networks, in Proc. of the IEEE LCN, October 2009.
44. A.Acquisti and R.Gross, Imagined communities: Awareness, information sharing, and privacy on the facebook, in Proc. of the PET, 2006.
45. Liu, Y., Gummadi, K. P., Krishnamurthy, B., Mislove, A., Analyzing Facebook Privacy Settings: User Expectations vs. Reality, IMC '11, Berlin: ACM, pp. 61–70, 2011.
46. Lange, R., & Lampe, C. , Feeding the Privacy Debate: An Examination of Facebook, The annual meeting of the International Communication Association, Quebec: ICA, p.26, 2008.
47. Christofides, E., Muise, A., & Desmarais, S. , Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? Cyberpsychology & Behavior, 12(3), pp. 341–345, 2009.
48. McDonald, A. M., & Cranor, L. F. , The cost of reading privacy policies. ISJLP, 4, pp. 543–897, 2009.
49. Heyman, R., Pierson, J., & Picone, I., 3.1.1: Mapping and in-depth analysis of corporate profiling techniques. EMSOC deliverable, Brussels: IBBT-SMIT, p. 150, 2011. Retrieved from http://emsoc.be/wp-content/uploads/2012/01/SMIT_VUB_EMSOC_rapport.2011.pdf.

### 9.3.4 Section 4.4 – Semantics Networks


1. K. Aberer, Peer-to-Peer Data Management (chapter 5), Morgan & Claypool Publishers, 2011.
2. E. Michlmayr, A. Pany, G. Kappel. Using taxonomies for content-based routing with ants. Comp. Netw., 51(16):4514–4528, 2007.
3. J. M. Tirado, D. Higuero, F. Isaila, J. Carretero, A. Iamnitchi, Affinity p2p: A self-organizing content-based locality-aware collaborative peer-to-peer network. Comp. Netw., 54(12):2056–2070, 2010.
4. A. Crespo, H. Garcia-Molina, Routing indices for peer-to-peer systems, In Proc. 22nd Int. Conf. on Distributed Computing Systems, pp. 23–33, 2002.
5. P. Haase, R. Siebes, F. van Harmelen, Peer selection in peer-to-peer networks with semantic topologies. In Semantics for Grid Databases, First International IFIP Conference on Semantics of a Networked World, volume 3226 of Lecture Notes in Computer Science, pp. 108–125, Springer Berlin / Heidelberg, 2004.
6. W. Penzo, S.Lodi, F. Mandreoli, R. Martoglia, S. Sassatelli, Semantic peer, here are the neighbors you want! In Advances in Database Technology, Proc. 11th Int. Conf. on Extending DatabaseTechnology, pp. 26–37, 2008.
7. C. Schmitz, Self-organisation of a small world by topic. In LWA 2004: Lernen - Wissensentdeckung- Adaptivität, pp. 303–310, 2004.
8. P. Raftopoulou, E. Petrakis, icluster: a self-organizing overlay network for p2p information retrieval. In Proc. 30th European Conf. on IR Research, pp. 65–76, 2008.
9. C. Doulkeridis, K. Norvag, M.Vazirgiannis, Desent: decentralized and distributed semantic overlay generation in p2p networks. IEEE Journal on Selected Areas in Communications, 25(1):25–34, 2007.
10. C. Xiang Zhai, Statistical language models for information retrieval: A critical review. Found. Trends Inf. Retr., 2:137–213, March 2008.


### 9.3.5 Section 4.5 – Economic Perspective


1. M. Sobolewski, M. Czajkowski, Network effects and preference heterogeneity in the case of mobile telecommunications markets. Telecommunications Policy Vol. 36 Issue 3, April 2012.
2. Columbia Telecommunications Corporation Benefits beyond the balance sheet: Quantifying the business case for Fiber-to-the-Premises in Seattle. Report for the City of Seattle, September 2009.
3. Mallon, K., Johnston, G. Burton, D. and Cavanagh, J., Towards a High-Bandwidth, Low-Carbon Future: Telecommunications-based Opportunities to Reduce Greenhouse Gas Emissions. Climate Risk Report, 2007.
4. Plum consulting A framework for evaluating the value of next generation broadband. A report for the Broadband Stakeholder Group, June 2008.
5. Tax on Web – http://www.taxonweb.be
6. Price Waterhouse Coopers Final Report: Technical assistance in bridging the “digital divide”: A cost-benefit analysis for broadband connectivity in Europe, 6 October 2004.

7. Gazet van Antwerpen Digitale Bouwaanvraag sneller en goedkoper. Press release of July 28th, 2011. Available from: http://www.gva.be/nieuws/economie/aid1066065/digitale-bouwaanvraag-sneller-en-goedkoper.aspx.
8. Open Universiteit Nederland. Available from: http://www.ou.nl/.
9. The New Zealand Institute Defining a broadband aspiration: how much does broadband matter and what does New Zealand need?, 2007. Presentation available from: http://www.nzinstitute.org/Images/uploads/Broadband%20aspiration%20Sept%202007.pdf.
10. König, M and S. Battiston, From Graph Theory to Models of Economic Networks. A Tutorial. Networks, Topology and Dynamics. Vol. 613. Berlin, Heidelberg: Springer Berlin Heidelberg. pp. 23-63, 2009.
11. Gilbert, N. and Pyka, A. and Ahrweiler, P, Innovation networks - a simulation approach Journal of Artificial Societies and Social Simulation 4(3), 2001.
12. Saviotti, P. 2009, Knowledge Networks: Structure and Dynamics. In: Pyka A., Scharnhorst, A, Innovation Networks, Springer, Berlin et al, pp. 19-41, 2009.
13. K. Frenken, J. Hoekman, S. Kok, R. Ponds, F. van Oort, and J. van Vliet. 2009. Death of distance science? A gravity approach to research collaboration". In: Pyka A., Scharnhorst, A, Innovation Networks, Springer, Berlin et al., pp. 43-57, 2009.
14. Vinciguerra, S., Frenken, K., Valente, M., The geography of Internet infrastructure: An evolutionary simulation approach based on preferential attachment. *Urban Studies* 47(9): 1969-1984, 2010.
15. Markus Michael Geipel: Dynamics of Communities and Code in Open Source Software. PhD Thesis Dissertation ETH No. 18480, 2009.
16. Michael D. Konig, Stefano Battiston and Frank Schweitzer. 2009. Modeling Evolving Innovation Networks. In: Pyka A., Scharnhorst, A, Innovation Networks, Springer, Berlin et al., pp. 187-268, 2009.

### 9.3.6 Section 4.6 – Game Theoretic Perspective

1. Aumann, R. and R. Myerson "Endogenous formation of links between players and coalitions: An application of the Shapley value" in A. Roth (Ed.), The Shapley Value, Cambridge Univ. Press, Cambridge pp. 175–191, 1988.
2. Bernheim, D. and A. Rangel, "Addiction and Cue-Triggered Decision Processes" *The American Economic Review* 94(5): 1558-1590, 2004.
3. Dutta, B. and M. Jackson, "The stability and efficiency of directed communication networks" Rev. Econ. Design 5: 251–272, 2000.
4. Ellison, G., "Learning, local interaction, and coordination. Econometrica 61, pp. 1047–1071, 1993.
5. Galeotti, A. and S. Goyal "The law of the few" *American Economic Review* 100: 1468-1492), 2010.
6. Galeotti, A., Goyal, S., Jackson, M. O., Vega-Redondo, F. and Yariv, L., "Network Games" *Review of Economic Studies* **77**: 218–244, 2010.

7. Jackson, M. and A. Watts, "The Evolution of Social and Economic Networks" *Journal of Economic Theory* 106 (2): 265-295, 2002.
8. Jackson, M. and A. Wolinsky "A strategic model of social and economic networks" *Journal of Economic Theory* 71: 44–74, 1996.
9. Jackson, M. and B. Rogers, "Relating Network Structure to Diffusion Properties through Stochastic Dominance" *Advances in Theoretical Economics* **7**(1): 1–13, 2007..
10. Kandori, M., Mailath, G., Rob, R. "Learning, mutation and long-run equilibria in games" *Econometrica* 61: 29–56, 1993.
11. Morris, S., "Contagion" *Rev. Econ. Stud.* **67** (1): 57–79, 2000.
12. Page, F. and M. Wooders, and S. Kamat, "Networks and Farsighted Stability" *Journal of Economic Theory* 120(2): 257-269, 2005.
13. Young, H.P., "The evolution of conventions" *Econometrica* 61:57–84, 1993.
14. Young, P., "The Economics of Convention" *The Journal of Economic Perspectives* 10(2): 105-122, 1996.
15. D. G. Goldstein and G. Gigerenzer, "Models of ecological rationality: The recognition heuristic," *Psychological Review*, 109(1):75–90, 2002.
16. E. Shafir and A. Tversky. Decision making, "*Invitation to Cognitive Science: Thinking*," pages 77–109, 1995.
17. I. Foster, Y. Zhao, I. Raicu and S. Lu , "Cloud Computing and Grid Computing 360-Degree Compared," Grid Computing Environments Workshop, 2008.
18. A. Goscinski, M. Brock, "Toward dynamic and attribute based publication, discovery and selection for cloud computing," Future Generation Computer Systems , vol. 26, pp. 947-970, July 2010.
19. S. Wang, Z. Zheng, Q. Sun, H. Zou and F. Yang, "Cloud model for service selection," IEEE INFOCOM Workshop on Cloud Computing, April 2011.
20. G. Wei, A. V. Vasilakos, Y. Zheng, and N. Xiong, "A game-theoretic method of fair resource allocation for cloud computing services," The Journal of Supercomputing, November 2010.
21. F.Teng, F. Magoulès, "A New Game Theoretical Resource Allocation Algorithm for Cloud Computing," 5th International Conference Grid and Pervasive Applications, 2010.
22. S. Zaman and D. Grosu, "Combinatorial Auction-Based Allocation of Virtual Machine Instances in Clouds," IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), 2010.
23. W-Y Lin, G-Y Lin, H-Y Wei, "Dynamic Auction Mechanism for Cloud Resource Allocation," 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing (CCGrid), 2010.
24. R. Arnott, "Spatial competition between parking garages and downtown parking policy," Elsevier Transport Policy, November 2006.
25. D. Ayala, O. Wolfson, B. Xu, B. Dasgupta, and J. Lin, "Parking slot assignment games," 19th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems, 2011.
26. G. Iosifidis and I. Koutsopoulos, "Double auction mechanisms for resource allocation in autonomous networks," IEEE Journal on Selected Areas in Communications, 2010.

27. G. Iosifidis, and I. Koutsopoulos, “Challenges in Auction Theory Driven Spectrum Management”, IEEE Communications Magazine, Vol. 49, No. 8 Aug. 2011.
28. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A view of cloud computing,” Communications of the ACM, April 2010.
29. Felegyhazi, M., & Hubaux, J.-Pierre, Game Theory in Wireless Networks : A Tutorial. Access, 2007.
30. Katsianis, D., Gyürke, A., Konkoly, R., Varoutas, D., & Sphicopoulos, T., A game theory modeling approach for 3G operators. NETNOMICS Economic Research and Electronic Networking, 8(1-2), 71-90, 1998.
31. Lannoo, B., Tahon, M., Van Ooteghem, J., Pareit, D., Casier, K., Verbrugge, S., Moerman, I., et al., Game-theoretic evaluation of competing wireless access networks for offering Mobile Internet. Competition and Regulation in Network Industries, 2nd Annual conference, Proceedings, 2008. Retrieved from: http://biblio.ugent.be/input/download?func=downloadFile&fileOId=1001177
32. Tahon, M., Lannoo, B., Ooteghem, J. V., Casier, K., Verbrugge, S., Colle, D., Pickavet, M., et al., Municipal support of wireless access network rollout: A game theoretic approach. Telecommunications Policy, 35(9-10), pp. 883-894, 2011.
33. Casier, K., Lannoo, B., Van Ooteghem, J., Verbrugge, S., Colle, D., Pickavet, M., & Demeester, P. Game-theoretic optimization of a fiber-to-the-home municipality network rollout. Journal of Optical, 1(1), 30, 2009.
34. Smit, H., & Trigeorgis, L., Strategic Options and Games in Analysing Dynamic Technology Investments. Long Range Planning, 40(1), pp. 84-114, 2007.
35. Ferreira, B. Y. N., Kar, J., & Trigeorgis, L., Option Games The Key to Competing in Capital-Intensive Industries. Harvard Business Review, (March), pp. 101-108, 2009.
36. G. Hardin, The tragedy of the commons, Science 162, pp. 1243–1248, 1968.
37. E. Adar and B.A. Huberman, Free Riding on Gnutella, First Monday, 5(10), 2000.
38. D. Hughes, G. Coulson, and J. Walkerdine. Freeriding on Gnutella Revisited: the Bell Tolls, IEEE Distributed Systems Online, 6(6), June 2005.
39. R. T. B. Ma, S. C. M. Lee, J. C. S. Lui, D. K. Y. Yau, “Incentive and service differentiation in P2P networks:a game theoretic approach”, IEEE/ACM Trans. Netw. 14(5): 978-991, 2006.
40. B. Mortazavi, and G. Kesidis, “Model and simulation study of a peer-to-peer game with a reputation-based incentive mechanism”, Technical Report, 2006.
41. K. Lai, M. Feldman, I. Stoica, and J. Chuang,“Incentives for Cooperation in Peer-to-Peer Networks”, Proc.1st Workshop on Economics of Peer-to-Peer Systems, 2003.
42. M. Feldman, K. Lai, I. Stoica, J. Chuang, “Robust Incentive Techniques for Peer-to-Peer Networks”, Proc. 5th ACM Conference on Electronic Commerce, 2004.
43. A. Urpi, M. Bonuccelli, and S. Giordano, “Modeling cooperation in mobile ad hoc networks: a formal description of selfishness,” Proc. of the 1st Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, March 2003.
44. V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, R. R. Rao “Cooperation in wireless ad hoc networks,” Proc. of IEEE INFOCOM, vol. 2, pp. 808-817, April 2003.

45. M. Felegyhazi, L. Buttyan, and J.-P. Hubaux, “Equilibrium analysis of packet forwarding strategies in wireless ad hoc networks the dynamic case,” Proc. of the 2nd Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, March 2004.
46. M. Felegyhazi, L. Buttyan, and J. P. Hubaux, “Nash equilibria of packet forwarding strategies in wireless ad hoc networks,” IEEE Transactions on Mobile Computing, vol. 5, no. 5, pp. 463476, 2006.
47. G. Theodorakopoulos, and J. S. Baras, “A Game for Ad Hoc Network Connectivity in the Presence of Malicious Users,” Proc. of IEEE GLOBECOM, 2006.
48. G. Theodorakopoulos, and J. S. Baras, “Enhancing Benign User Cooperation in the Presence of Malicious Adversaries in Ad Hoc Networks”, 2nd IEEE Communications Society/CreateNet International Conf. on Security and Privacy in Comm. Netw. (SecureComm), 2006.

### 9.4 *Section 5 - Security, Resilience and Dependability Aspects*

1. Marias, G. F., Barros, J., Fiedler, M., Fischer, A., Hauff, H., Herkenhoener, R., Grillo, A., Lentini, A., Lima, L., Lorentzen, C., Mazurczyk, W., de Meer, H., Oliveira, P. F., Polyzos, G. C., Pujol, E., Szczypiorski, K., Vilela, J. P. and Vinhoza, T. T. V., Security and privacy issues for the network of the future. Security Comm. Networks, 2011.
2. J.P.G. Sterbenz, D. Hutchison, E.G. Cetinkaya, A. Jabbar, J.P. Rohrer, M. Schöller, and P. Smith, “Resilience and survivability in communication networks: strategies, principles, and survey of disciplines”, Computer Networks, Special Issue on Resilient and Survivable Networks, Vol. 54, N° 8, pp. 1245-1265, June 2010
3. N. Kammenhuber, A. Fessi, G. Carle, "Resilience: Widerstandsfähigkeit des Internets gegen Störungen–Stand der Forschung und Entwicklung.", Informatik-Spektrum, Springer-Verlag, 2010.
4. Goyal, M. and Ramakrishnan, K.K. and Feng, Wu-Chi, "Achieving faster failure detection in OSPF networks". In IEEE International Conference on Communications (ICC), 2003.
5. Teixeira, Renata and Shaikh, Aman and Griffin, Tim and Rexford, Jennifer, "Dynamics of hot-potato routing in {IP} networks". In SIGMETRICS Perform. Eval. Rev., Volume 32, Number 1, 2004.
6. RIPE NCC, "YouTube Hijacking: A RIPE~NCC RIS case study", http://www.ripe.net/news/study-youtube-hijacking.html.
7. Renesys Blog, "Longer is not always better", http://www.renesys.com/blog/2009/02/longer-is-not-better.shtml.
8. V. Ramasubramanian, E. Gün Sirer , "Perils of Transitive Trust in the Domain Name System". In Proceedings of the ACMInternet Measurement Conference (IMC) 2005.
9. H. Wang, H. Xie, L. Qiu, Y. Richard, Y. Yin Zhang, A. Greenberg, "COPE: Traffic Engineering in Dynamic Networks", ACM SIGCOMM 2006.
10. N. Kammenhuber, J. Luxenburger, A. Feldmann, G. Weikum, "Web Search Clickstreams". In Proceedings of the ACM Internet Measurement Conference (IMC), Rio de Janeiro, 2006.
11. Cohen, F. The Virtualisation Solution. IEEE Security and Privacy, IEEE Computer Society, 8, pp. 60-63, 2010.

12. Ristenpart, T.; Tromer, E.; Shacham, H. & Savage, S. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds CCS '09: Proceedings of the 16th ACM conference on Computer and communications security, ACM, pp. 199-212, 2009.
13. Fischer, A. & De Meer, H. Position Paper: Secure Virtual Network Embedding. Praxis der Informationsverarbeitung und Kommunikation, 34, pp. 190-193, 2011.
14. Fischer, A.; Fessi, A.; Carle, G. & De Meer, H. Wide-Area Virtual Machine Migration as Resilience Mechanism. Proc. of the International Workshop on Network Resilience: From Research to Practice (WNR2011), IEEE, 2011.
15. Grobauer, B.; Walloschek, T.; Stocker, E.; , "Understanding Cloud Computing Vulnerabilities," Security & Privacy, IEEE , vol.9, no.2, pp.50-57, March-April 2011. doi: 10.1109/MSP.2010.115.
16. Luis M. Vaquero, Luis Rodero-Merino, and Daniel Morin. 2011. Locking the sky: a survey on IaaS cloud security. Computing 91, 1, pp. 93-118, January 2011.
17. Angelos Marnerides, Cyriac James, Alberto Schaeffer-Filho, Saad Yunus Sait, Andreas Mauthe, Hema Murthy. "Multi-level network resilience: traffic analysis, anomaly detection and simulation". In: ICTACT Journal on Communication Technology, Special Issue on Next Generation Wireless Networks and Applications. Vol. 2, n. 2. 2011.
18. P. Smith, A. Schaeffer-Filho, A. Ali, M. Schöller, N. Kheir, A. Mauthe, D. Hutchison. "Strategies for Network Resilience: Capitalising on Policies". In: Proceedings of the 4th International Conference on Autonomous Infrastructure, Management and Security (AIMS 2010), ser. LNCS. Zurich, Switzerland. Springer, pp. 118-122, June 2010.
19. M. Sloman and E. Lupu, “Security and management policy specification,” IEEE Network, vol. 16, no. 2, pp. 10–19, Mar.-Apr. 2002.
20. Y. Yu, M. Fry, A. Schaeffer-Filho, P. Smith, and D. Hutchison, “An adaptive approach to network resilience: Evolving challenge detection and mitigation,” in DRCN’11: 8th International Workshop on Design of Reliable Communication Networks, Krakow, Poland, pp. 172 –179 October 2011.
21. A. Schaeffer-Filho, P. Smith, A. Mauthe, D. Hutchison, Y. Yu and M. Fry, "A Framework for the Design and Evaluation of Network Resilience Management". To appear in: Proceedings of the 13th IEEE/IFIP Network Operations and Management Symposium (NOMS 2012), Maui, Hawaii, USA. April 2012.
22. A. Schaeffer-Filho, P. Smith, and A. Mauthe, “Policy-driven network simulation: a resilience case study,” in SAC’11: 26th Symposium on Applied Computing. Taichung, Taiwan: ACM, , pp. 492– 497, March 2011.
23. A. Varga and R. Hornig, “An overview of the OMNeT++ simulation environment,” in SIMUTools ’08: Proceedings of the 1st International Conference on Simulation Tools and Techniques. Marseille, France: ICST, pp. 1–10, 2008.
24. K. Twidle, E. Lupu, N. Dulay, and M. Sloman, “Ponder2 - a policy environment for autonomous pervasive systems,” in POLICY ’08: IEEE Workshop on Policies for Distributed Systems and Networks. Palisades, NY, USA: IEEE Computer Society, pp. 245–246, 2008.

25. P. Cholda, A. Mylkeltveit, B. E. Helvik, O. J. Wittner, and A. Jajszczyk. A survey of resilience differentiation frameworks in communication networks. IEEE Communications Surveys, 9(4):32.54, 2007.
26. O. Wing, P. Demetriou. Analysis of Probabilistic networks. IEEE Transactions on Communication Technology, Vol. 12, pp. 38-41, September 1964.
27. R. Wilkov. Analysis and design of reliable computer networks. IEEE Transactions on Communications, Vol. 20, No. 3, pp. 660-677, June 1972.
28. S. Rai and K. K. Aggarwal. An efficient method for reliability evaluation of a general network. IEEE Transactions on Reliability, Vol. 27, No. 3, pp. 206-211, August 1978.
29. V. Li and J. Silvester. Performance analysis of networks with unreliable components. IEEE Transactions on Communications, Vol. 32, No. 10, pp. 1105-1110, October 1984.
30. H. L. Frisch and J. M. Hammersley. Percolation processes and related topics. SIAM Journal on Applied Mathematics, vol. 11, no. 4, pp. 894-918, 1963.
31. M. F. Sykes and J. W. Essam. Exact critical percolation probabilities for site and bond problems in two dimensions. Journal of Mathematical Physics, vol. 5, no. 8, pp. 1117-1127, 1964.
32. M. Chari and C. J. Colbourn. Reliability polynomials: A survey. J.Combin. Inform. System Sci, vol. 22, pp. 177-193, 1998.
33. S.-C. Chang and R. Shrock. Reliability polynomials and their asymptotic limits for families of graphs. J.STAT.PHYS., vol. 112, p. 1019, 2003.
34. L. Page and J. Perry. Reliability polynomials and link importance in networks. Reliability, IEEE Transactions on, vol. 43, pp. 51-58, Mar 1994.
35. P. Holme, B. J. Kim, C. N. Yoon and S. K. Han. Attack vulnerability of complex networks. Physical Review E, vol. 65, p. 056109, 2002.
36. D. S. Callaway, M. E. J. Newman, S. H. Strogatz and D. J. Watts. Network robustness and fragility: Percolation on random graphs. Physical Review Letters, vol. 85, p. 5468, 2000.
37. M. Faloutsos, P. Faloutsos and C. Faloutsos. On power-law relationships of the internet topology. SIGCOMM, pp. 251-262, 1999.
38. T. H. Grubesic, T. C. Matisziw, A. T. Murray and D. Snediker. Comparative Approaches for Assessing Network Vulnerability. International Regional Science Review, Vol. 31, pp. 88-112, 2008.
39. M. Cushing, J. Krolewski, T. Stadterman and B. Hum. U.S. army reliability standardisation improvement policy and its impact. IEEE Transactions on Components, Packaging, and Manufacturing Technology. Part A, vol. 19. No. 2, pp. 277-278, 1996.
40. J. F. Meyer. On evaluating the performability of degradable computing systems, IEEE Transactions on Computers, Vol. C.29, No. 8, pp. 720-731, 1980.
41. J. F. Meyer. Performability: a retrospective and some pointers to the future. Performance Evaluation, Vol. 14, pp. 139-156, 1992.
42. P. Van Mieghem, J. Omic and R. E. Kooij. Virus spread in networks. IEEE/ACM Transactions on Networking, Vol. 17, No. 1, pp. 1-14, 2009.
43. J. G. Restrepo, E. Ott and B. R. Hunt. Onset of synchronization in large networks of coupled oscillators. Physical Review E 71, 036151, 2005.

### 9.5 *Section 6 – Sustainability Perspective*


1. Y. Zhang, P. Chowdhury, M. Tornatore, and B. Mukherjee, “Energy Efficiency in Telecom Optical Networks,” IEEE Communications Surveys & Tutorials, Vol. 12, 2010.
2. R. Bolla, R. Bruschi, F. Davoli, and F. Cucchietti, “Energy Efficiency in the Future Internet: A Survey of Existing Approaches and Trends in Energy-Aware Fixed Network Infrastructures,” IEEE Communications Surveys & Tutorials, Vol. 13, No. 2, pp. 223 - 244, 2011.
3. Aruna Prem Bianzino, Claude Chaudet, Dario Rossi, and Jean-Louis Rougier, “A Survey of Green Networking Research,” IEEE Communications Surveys & Tutorials, Vol. 14, No. 1, pp. 3 - 20, 2012.
4. G. Lovasz, A. Berl, and H. De Meer, “Energy- and Performance-Aware Resource Management in G-Lab and Future Internet Infrastructures,” Proc. of the 11th Wuerzburg Workshop on IP: Joint ITG, ITC, and Euro-NF Workshop on “Visions of Future Generation Networks” (EuroView 2011), 2011.
5. Y. Wang, E. Keller, B. Biskeborn, J. van der Merwe, and J. Rexford, “Virtual Routers on the Move: Live Router Migration as a Network-Management Primitive,” Proc. of ACM SIGCOMM, August 2008.
6. S. Ricciardi, D. Careglio, F. Palmier, U. Fiore, G. Santos-Boada, and J. Solé-Pareta, “Energy-oriented models for WDM networks,” Proc. of ICST Broadband Communications, Networks, and Systems (Broadnets), 2010.
7. S. Nedevschi, L. Popa, G. Iannaccone, S. Ratnasamy, and D. Wetherall, “Reducing Network Energy Consumption via Sleeping and Rate- Adaptation,” Proc. of the 5th USENIX Symposium on Networked Systems Design and Implementation, USENIX Association Berkeley, CA, USA, 2008.
8. E. Yetginer and G.N. Rouskas, "Power efficient traffic grooming in optical WDM networks," Proc. of IEEE GLOBECOM, Honolulu, Hawaii, November 2009.
9. Y. Chen and A. Jaekel, "Energy efficient grooming of scheduled sub-wavelength traffic demands," Optical Fiber Communication Conference (OFC), Los Angeles, California, March 6, 2011.
10. S. Zhang, D. Shen, and C-K Chan, "Energy efficient time-aware traffic grooming in wavelength routing networks," Proc. of IEEE GLOBECOM, Miami, USA, December 2010.
11. M. Xia, M. Tornatore, Y. Zhang, P. Chowdhury, C.U. Martel, and B. Mukherjee, "Green provisoning for optical WDM networks," IEEE Journal of Selected Topics in Quantum Electronics, vol. 17, no. 2, March-April 2011.
12. S. Yang and F.A. Kuipers, "Energy-Aware Path Selection for Scheduled Lightpaths in IP-over-WDM Networks," Proc. of IEEE SCVT, Ghent, Belgium, November 22-23, 2011.
13. G. Shen and R. S.Tucker, "Energy-Minimized design for ip over wdm networks," IEEE/OSA J. Optical Commun. Netw., vol. 1, no. 1, pp. 176--186, June 2009.
14. X. Dong, T. El-Gorashi, and J.M.H. Elmirghani, "Energy-ffficient IP over WDM networks with data centres," Proc. of IEEE Transparent Optical Networks (ICTON), 2011.
15. H. Farhangi, The path of the smart grid, IEEE Power and Energy Magazine 8 (1), pp. 18–28, 2010.

16. Z. Fadlullah, M. Fouda, N. Kato, A. Takeuchi, N. Iwasaki, Y. Nozaki, Toward Intelligent Machine-to-Machine Communications in Smart Grid, IEEE Communications Magazine 49 (4) pp. 60–65, 2011.
17. V. Gungor, B. Lu, G. Hancke, Opportunities and Challenges of Wireless Sensor Networks in Smart Grid, IEEE Transactions on Industrial Electronics 57 (10), 3557–3564, 2010.
18. D. Wang, Z. Tao, J. Zhang, A.A. Abouzeid, RPL Based Routing for Advanced Metering Infrastructure in Smart Grid, in: Proc. of IEEE ICC'10, 2010.
19. D. Niyato, L. Xiao, P. Wang, Machine-to-Machine Communications for Home Energy Management System in Smart Grid, IEEE Communications Magazine 49 (4), pp. 53–59, 2011.
20. J. Gao, Y. Xiao, J. Liu, W. Liang, C. Chen, A Survey of Communica-tion/Networking in Smart Grids, Future Generation Computer Systems 28, pp. 391–404, 2012.
21. F. Wu, K. Moslehi, A. Bose, Power System Control Centers: Past, Present, and Future, Proceedings of the IEEE 93 (11), pp. 1890– 1908, 2005.
22. S. Keshav, C. Rosenberg, How Internet Concepts and Technologies Can Help Green and Smarten the Electrical Grid, in: Proc. of ACM SIGCOMM workshop on Green networking, pp. 35–40, 2010.
23. S. McArthur, E. Davidson, V. Catterson, A. Dimeas, N. Hatziargyriou, F. Ponci, T. Funabashi, Multi-Agent Systems for Power Engineering Applications – Part I: Technologies, Standards, and Tools for Building Multi-agent Systems, IEEE Transactions on Power Systems 22 (4), pp. 1753–1759, 2007.
24. S. McArthur, E. Davidson, V. Catterson, A. Dimeas, N. Hatziargyriou, F. Ponci, T. Funabashi, Multi-Agent Systems for Power Engineering Applications – Part II: Technologies, Standards, and Tools for Building Multi-agent Systems, IEEE Transactions on Power Systems 22 (4), pp.1753–1759, 2007.
25. M. Lu, C. Chen, The design of multi-agent based distributed energy system, in: Proc. of IEEE SMC, pp. 2001–2006, 2009.
26. V. Catterson, E. Davidson, S. McArthur, Issues in integrating existing multi-agent systems for power engineering applications, in: Proc. of Conf. on Intelligent Systems Application to Power Systems'05, 2005.
27. All4Green project: http://net.fim.uni-passau.de/all4green
28. Juan F. Botero, Xavier Hesselbach, Michael Duelli, Daniel Schlosser, Andreas Fischer and Hermann De Meer, "Energy Efficient Virtual Network Embedding" IEEE Communications Letters.
29. George W. Hart, Edward C. Kern, Jr., Fred C. Schweppe. Non-intrusive appliance monitor apparatus. US patent 4858141, 1989.
30. Goncalves, Hugo, Adrian Ocneanu, Mario Berges. "Unsupervised Disaggregation of Appliances using Aggregated Consumption Data". KDD 2011 Workshop on Data Mining Applications for Sustainability, San Diego, CA, USA, 2011.
31. G. W. Hart, "Nonintrusive appliance load monitoring," Proceedings of the IEEE, vol. 80, no. 12, pp. 1870-1891, Dec. 1992.

32. S. R. Shaw, S. B. Leeb, L. K. Norford, and R. W. Cox, “Nonintrusive Load Monitoring and Diagnostics in Power Systems,” IEEE Transactions on Instrumentation and Measurement, vol. 57, no. 7, pp. 1445-1454, Jul. 2008.
33. Ferscha, A., Emsenhuber, B., Gusenbauer, S., Wally, B., Klein, C., Kuhmunch, C. and Mitic, J. PowerSaver: Pocket-Worn Activity Tracker for Energy Management. Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.160.8037.
34. Jonghwa Choi, Dongkyoo Shin & Dongil Shin, Research and implementation of the context-aware middleware for controlling home appliances. IEEE Transactions on Consumer Electronics, 51(1), pp.301– 306, 2005.
35. L. Chen, C. Nugent, and H. Wang, “A Knowledge-Driven Approach to Activity Recognition in Smart Homes,” IEEE Transactions on Knowledge and Data Engineering, vol. 23, no. 2, 2011.
36. Wing J. M.: “Cyber-Physical Systems Research Challenges”, National Workshop on High-Confidence Automotive Cyber-Physical Systems, Troy, MI, USA, April 2008.
37. Lindeberg, M., Kristiansen, S., Plagemann, T., Goebel, V: “Challenges and Techniques for Video Streaming Over Mobile Ad-hoc Networks”, Multimedia Systems Journal, Vol. 17(1), 2011.
38. Lee, E. A.: "Cyber Physical Systems: Design Challenges". Int. Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing (ISORC 2008), Orlando, Florida, USA, May, 2008.
39. Conti, M., Das, S., Bisdikian, C., Kumar, M., Ni, L., Passarella, A., Roussos, G., Troester, G., Tsudik, G., Zambonelli, F., “Looking ahead in pervasive computing: Challenges and opportunities in the era of cyber-physical convergence”, Pervasive and mobile computing, Elsevier, Vol. 8, 2012.
40. http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286
41. Bogdan, P., Marculescu, R., “Towards a Science of Cyber-Physical Systems”, IEEE/ACM 2nd Int. Conference on Cyber Physical Systems, Chicago, USA, April 2011.
42. Giese, H., Rumpe, B., Schaetz, B., Sztipanovits, J., “Science and Engineering of Cyber-Physical Systems” Report from Dagstuhl Seminar 11441, Dagstuhl, Germany, 2011.
43. W. Vereecken, W. Van Heddeghem, M. Deruyck, B. Puype, B. Lannoo, W. Joseph, D. Colle, L. Martens, and P. Demeester, “Power consumption in telecommunication networks: overview and reduction strategies”, IEEE Communications Magazine, 49(6):62 –69, June 2011.
44. W. Van Heddeghem, F. Idzikowski, W. Vereecken, D. Colle, M. Pickavet, and P. Demeester, “Power consumption modeling in optical multilayer networks”, Photonic Network Communications, January 2012.
45. P. Vetter, L. Lefevre, L. Gasca, K. Kanonakis, L. Kazovsky, B. Lannoo, K. L. Lee, C. Monney, X.-Z. Qiu, F. Saliou, A. Wonfor, “Research Roadmap for Green Wireline Access”, accepted for ICC 2012, workshop on Green Communications and Networking, Ottawa, Canada, June 10-15, 2012.
46. J. Chabarek, J. Sommers, P. Barford, C. Estan, D. Tsiang, and S. Wright, “Power awareness in network design and routing,” Proc. of IEEE INFOCOM, Phoenix, Arizona, pp. 457–465, April 2008.
47. B. Nordman, et al. “Reducing the Energy Consumption of Networked Devices,” IEEE 802.3 tutorial, San Francisco, July 2005.

48. Cisco Systems, Ethernet Power Study of Cisco and Competitive Products, Cisco public white-paper, 2008.
49. B. Puype, W. Vereecken, D. Colle, M. Pickavet and P. Demeester, "Power Reduction Techniques in Multilayer Traffic Engineering," IEEE Transparent Optical Networks (ICTON), São Miguel, Azores, Portugal, June 2009.
50. B. Puype, D. Colle, M. Pickavet and P. Demeester, "Energy Efficient Multilayer Traffic Engineering", ECOC 2009, Vienna, Austria, September 2009.
51. B. Puype, D. Colle, M. Pickavet and P. Demeester, "Multilayer traffic engineering for energy efficiency," Photonic Network Communications, Vol. 21, No. 2, pp. 127-140, April 2011 .
52. K. Cho, K. Fukuda, H. Esaki and A. Kato, "Observing slow crustal movement in residential user traffic." ACM CoNEXT, Madrid, Spain, December 2008.
53. M. Afanasyev, T. Chen, G.M. Voelker, and A.C. Snoeren, "Analysis of a mixed-use urban wifi network: when metropolitan becomes Neapolitan," 8th ACM SIGCOMM Con-ference on Internet Measurement (IMC'08), Vouliagmeni, Greece, pp. 85–98, October 2008.
54. W. Van Heddeghem, M. De Groote, W. Vereecken, D. Colle, M. Pickavet and P. Demeester, "Energy-Efficiency in Telecommunications Networks: Link-by-Link versus End-to-End Grooming", ONDM 2010, Kyoto, Japan, February 2010.
55. W. Van Heddeghem, W. Vereecken, D. Colle, M. Pickavet and P. Demeester, "Distributed Computing for Footprint Reduction by Exploiting Low-Footprint Energy Availability", Future Generation Computer Systems [Green Computing special issue] Vol 28 Issue 2, pp. 405–414, February 2012.

### 9.6 *Section 7 – Standards Policy and Internet Science*

1. Clark, David D., Wroclawski, John, Sollins, Karen R., Braden, Robert "Tussle in cyberspace: defining tomorrow's Internet." *IEEE/ACM Transactions on Networking* 13 (3): 462–475, 2005.
2. Greenstein, Shane, "Standardisation and Coordination". IEEE Micro. 30:3 May-June at 6-7 2010. ISSN: 0272-1732.
3. Brown, Ian, Clark, David and Trossen, Dirk, "Should Specific Values Be Embedded In The Internet Architecture?" *Proceedings of the Re-Architecting the Internet workshop*. New York: ACM Press, 2011.
4. Kahin, B. and Abbate, J., *Standards Policy for Information Infrastructure*. Cambridge, Mass: MIT Press, 1995.
5. Pitofsky, Robert "Self Regulation And Antitrust." Prepared Remarks of the Chairman, Federal Trade Commission, D. C. Bar Association Symposium, February 1998.
6. Lemley, Mark A. and McGowan, David, "Legal Implications of Network Economic Effects." California Law Review 86: 479-611, 1998.
7. Bar, F., Borrus, M., Steinberg, R. "Islands in the bit-stream: mapping the NII interoperability debate." Berkeley Roundtable on the International Economy Working Paper # 79. BRIE, Berkeley, CA., 1996. Available at: http://www-rcf.usc.edu/fbar/Publications/islands-in-the-bitstream.pdf.
8. Dolmans, Maurits, "A Tale of Two Tragedies – A plea for open standards." *International Free*

*and Open Source Software Law Review* 2 (2): 115-136, 2010. Available at http://www.ifosslr.org/ifosslr/article/view/46/72

9. Coates, Kevin, *Competition law and regulation of technology markets*. Oxford: Oxford University Press, 2011.
10. EC, "Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements." Official Journal C 11 of 14.1.2011.
11. Kroes, N, "Address at Open Forum Europe 2010 Summit: 'Openness at the heart of the EU Digital Agenda' Brussels." Speech 10/300, June 2010.
12. Braithwaite, J. and Drahos, P., *Global Business Regulation*. Cambridge: Cambridge University Press, 2000.
13. Drahos, Peter and Braithwaite, J., *Information Feudalism: Who Owns the Knowledge Economy*? New York: Free Press, 2002.
14. Moody, Glyn., "European Interoperability Framework v2 - the Great Defeat". *Computerworld* 17 December, 2010. Available at http://blogs.computerworlduk.com/open-enterprise/2010/12/european-interoperability-framework-v2---the-great-defeat/index.htm
15. ITU, "FG-FN Output Document 77." Focus Group On Future Networks 8th FG-FN meeting: 28 November-3 December 2010.
16. Directive 2004/18/EC, Directive on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts. OJ L 134, p. 114, 30.4.2004.
17. EC, "Communication: Towards interoperability for European public services." December 2010. Available at http://ec.europa.eu/isa/strategy/index_en.htm
18. Ganslandt Mattias, "Completing the Internal Market", December 2010. Available at http://www.talkstandards.com/completing-the-internal-market/
19. COD, European standardisation (COD/2011/0150:) (amending Directives 89/686/EEC, 93/15/EEC, 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/105/EC and 2009/23/EC), 2011. Dossier of the committee IMCO/7/06240 at http://www.europarl.europa.eu/oeil/FindByProcnum.do?lang=2&procnum=COD/2011/0150.