

## Chapter 10

# A Peek at the Future Internet

**Abstract** The Internet “connectivity machine” is the generative engine of our modern digital society. It has been the launching pad of the Web (now the Web 2.0), truly the largest and most versatile information system ever built. While the Web phenomenon relentlessly continues, scientists worldwide are now living the dream of yet a more generative next-generation network. This chapter explores some prominent research directions, discussing the *Internet of Things*, *context-aware networks*, *small world networks*, *scale-free networks*, *autonomic networks*, *dependable networks*, the *privacy vs. security* dichotomy and the two facets of *energy-efficient networks*.

*The best way to predict the future is to invent it*

Alan Key, computer scientist

### 10.1 The Fourth Networking Principle: Beyond Mere Connectivity

In [Chap. 2](#), we introduced the three fundamental principles of networking: *connect*, *discover* and *stay connected*. It is now time to argue that the next-generation networks should go beyond mere connectivity.

Networks are currently engineered in layers, going from the lower *physical* layer up to the *application* (the seventh) layer. Each layer has specific responsibilities (for instance, layer three, the network layer, is in charge of *route computation*) and dedicated interfaces with the adjacent layers. This “insulation” between layers makes networks more manageable and facilitates the appearance of new applications. Layers make it easy to focus on specific functionalities without having to

worry about the whole system. In fact, the marvelous Internet applications that we use today are probably the direct consequence of the layering model: the programmers could focus on the application logic without having to master the lower layers.

However, inter-layer insulation comes with a downside: it limits our ability to introduce new optimization mechanisms. If we keep the network layer isolated, the routing and transport functions cannot promptly take into account the requirements arising from the physical network. What is worse, *packet routing* does not adapt to the applications or to the user's context. For instance, we cannot implement content-based routing on the IP layer.

The advances made at the network edges, such as P2P networking, have revealed the potential of *context-aware* networking. At the same time, the realization of context-aware networks at the application level (as in P2P) is not ideal. The damage that P2P applications cause to the network is now well documented. On the other hand, IP networks are not always capable of meeting the delivery deadlines of the real-time P2P systems (such as P2P IPTV). In fact, we can now observe a trend whereby *cloud* services such as *YouTube* are becoming more prominent.

Imagine what we could achieve if the network itself could take into account requirements and constraints arriving from the other layers. We could route packets based on the type of content, the user's context or the recipient's preferences. The network would be able to spot communication patterns and allocate resources accordingly. Routing algorithms would be based on a *probabilistic* approach rather than on the current *deterministic* approaches that do not work under dynamic conditions.

Context-awareness is the extra gear that is missing in the Internet and a crucial mechanism for the realization of the next-generation Net. The upcoming networks will not be completely autonomic,<sup>1</sup> but will certainly have to be more adaptive regarding a variety of perturbations.

## 10.2 Internet of Things: Sense and Influence Your Environment

The time when the Internet was for the sole use of computers is over. Our technology roadmap is going towards the *Internet of Things* (IoT) [1, 2], a digital infrastructure where anything having any kind of network interface will be part of the Net. The convergence between the conventional stationary Internet and the cellular network has given tremendous impulse to the digital society [3]. Even greater breakthroughs will come from the interconnection of everyday objects, sensors and actuators.

---

<sup>1</sup> Autonomic networks are envisioned to be able to *self-configure*, *self-heal*, *self-optimize* and *self-protect* with minimal human intervention, according to the autonomic computing principles.

The realization of the IoT poses ambitious scientific hurdles, though it certainly has enormous potential. With virtually anything on the Net, from the domestic appliances to clothing and biometric sensors, the network will suddenly assume a “massive” scale.

Yet the biggest challenge will probably come from the huge functional diversity among the devices. RFIDs<sup>2</sup> can do very little in terms of networking, but give a cheap way to locate a myriad of objects. Multiple sensors may collaborate to provide environmental monitoring information, but will have substantial computational and energy constraints. Intelligent camera systems may solve complex surveillance problems, though they will incur severe traffic onto the network.

The size and diversity of the IoT cannot be handled by the current IP protocol [4]. On the other hand, the IoT will be able to rely on a wealth of contextual information that will enable greater routing intelligence. The IoT will not only propagate contextual information “where” and “when” it is needed, but it will also make use of the context to better operate the network itself.

Once we make the move to attaching anything to the Net, the network will become the largest control system ever built. The network’s “things” will provide *sensory*, but also *transducing* and *actuation* capabilities. Actuators, for example, motors, pneumatics and hydraulics, can move objects and pump fluids. Electrical relays can switch on the heating system or turn off the lights.

The transducers will further enhance the network’s self-sufficiency. Researchers are making progress in the area of energy-harvesting transducers that can capture small but usable amounts of energy from the environment. This energy can be used to run sensors and network interfaces.

The next-generation network will be able to *grasp* and simultaneously *influence* its environment. Scientists are investigating the paradigm shift required to make the most of these new capabilities.

## 10.3 Small, Large Networks

There is no doubt that the Net is getting bigger, more complex and increasingly dynamic. At the same time, the perturbations created by emerging applications are more and more intense and erratic. The Net is a complex system that is constantly changing and expanding. The routing protocols must keep everything connected; they must discover short paths across such a massive network.

One way to keep large networks “small” is to increase the number of links, making the network denser. This is easier said than done. Adding new capacity on

---

<sup>2</sup> Radio-frequency identification (RFID) is a technology that uses communication via radio waves to exchange data between a reader and an electronic tag attached to an object for the purpose of identification and tracking.

the physical network is costly. In fact, the current Net is relatively sparse; it has a number of links roughly of the same order of magnitude as the number of nodes.

Things get more complicated if we try scaling up the network while at the same time ensuring “stability.” Suppose we can add new links. How do we know which node pairs would benefit the most from the extra capacity? Where do we add capacity in a constantly changing network? How can we make this choice automatically?

Ironically, while the *computer networks* community has created a marvelous yet complex digital ecosystem, fundamental breakthroughs have also been achieved beyond the technologists’ circle. Physicists, biologists, mathematicians and sociologists have been studying biological [5] and neural networks [6] that are far more complex than the present Internet [7, 8]. Thus, understanding the properties of the “natural” networks should be the starting point for those who are rethinking the Internet [9–11].

Perhaps one of the most remarkable discoveries is the *small-world* phenomenon, which is present in most complex networks [7]. Apparently, the networks resulting from a natural evolution process are able to build short paths, irrespective of the number of nodes. A fascinating yet not fully proved theory is that in natural networks, any node is, on average, six hops away from any other node—this is known as the “six degrees of separation” property or “small-worldness”.

Another outstanding property of natural networks is known as *scale-freeness* [7]. Scale-free networks exhibit the same interconnectivity distribution, no matter how big the network grows. While *small-worldness* is key to scalability, *scale-freeness* is crucial for robustness and stability.

The mechanics of small-world and scale-free networks is not fully understood. However, scientists have already unveiled several mysteries. We have enough knowledge to start designing routing protocols that can make a large network “small.”<sup>3</sup> We know that a well-designed network must have short paths. This can be achieved if the network has the “right” mixture of low- and high-degree nodes and of weak and strong links [12].<sup>4</sup>

Scientists have discovered a number of counter-intuitive properties that have significant potential for the re-design of routing protocols. For instance, weak links play a crucial role in reducing the network diameter as they build long-distance bridges between nodes that would otherwise be poorly connected. Because of their nature, weak links tend to be transient. It seems to defy logic, but scientists have discovered that it is precisely this volatility that makes weak links so crucial in kicking the network out of sub-optimal configurations. Weak links make it possible to propagate signaling information more rapidly and towards areas that would

---

<sup>3</sup> Recent literature describing the properties and mechanisms of small-world and scale-free networks is included in our “References” section.

<sup>4</sup> A link is “weak” when its addition or removal does not significantly change the mean value of a target measure (P. Csermely, “Weak Links”, Springer 2009).

otherwise not be reached. Weak links hold the secret of *stability*. However, weak links cannot exist without the strong ones. In fact, the natural networks have a continuous spectrum of link strengths.

Extensive studies of complex networks have unveiled how difficult it is to pursue multiple performance goals. Network *speed* and *stability* are often conflicting targets. It is a myth that networks' diameter can be merely reduced by increasing the average node degree. Nodes with a large number of neighbors are called *hubs*. Hubs multiplex traffic; so they are important. However, hubs come with a problematic side effect. They make the network vulnerable. Hubs have huge responsibilities; so if they are attacked, large portions of the network are affected. Hubs not only propagate genuine data, but also speed up the spreading of computer viruses or any other destabilizing agent.

Ironically, hubs and strong links help to improve transmission speed, but do not play a positive role when it comes to stability and robustness. Another counter-intuitive finding is that in addition to weak links, *bottlenecks* can also help make networks more *robust*. Bottlenecks limit the network throughput, but often generate new weak links. Bottlenecks force networks to re-distribute the load and trigger a rewiring process that is crucial in protecting networks against cascading failures. Scientists such as Motter have proved that a selective removal of network elements makes the network more robust.<sup>5</sup>

One of the problems of the current routing protocols is that they strive for a "uniform" network. They pursue routing efficiency but neglect other essential properties. Looking at the most complex natural networks, we see that they are not only transmission-efficient, but also tolerant to incredible amounts of failures, errors, noise and dynamics. Small-world, scale-free networks have a mix of randomness, nestedness,<sup>6</sup> disuniformity, volatility and unpredictability. They have a variety of nodes (hubs,<sup>7</sup> rich clubs,<sup>8</sup> VIP clubs,<sup>9</sup> leaves and bottlenecks) and links (bridges, weak and strong links). As part of their evolution, the natural networks have learned how to orchestrate this variety of elements and respond to new forms of perturbations.

---

<sup>5</sup> A.E. Motter, Cascade control and defense in complex networks. Phys Rev Lett 93, 098701.

<sup>6</sup> *Nestedness* indicates the hierarchical structure of networks. Each element of the top network usually consists of an entire network of elements at the lower level. Nestedness helps us to explain the complexity of networks.

<sup>7</sup> *Hubs* are connection-rich network elements.

<sup>8</sup> In hierarchical networks, the inner core becomes a *rich club* if it is formed by the hubs of the network. For example, in the Internet, the routers form rich clubs.

<sup>9</sup> In VIP clubs, the most influential members have low number of connections. However, many of these connections lead to hubs.

## 10.4 Manage the Autonomics

Networks are becoming increasingly complex and heterogeneous. Networks are nested within networks, virtualized, overlaid, sub-netted. Some sections of the Internet are “managed,” e.g., by network operators or ISPs. However, there is a steep increase in “unmanaged” networks (e.g., wireless home networks), “spontaneous” networks (e.g., *ad hoc* networks) and “content-driven” networks (e.g., P2P networks). Several researchers are investigating how to bring the power of the natural evolutionary networks into the Net [5, 6, 13]. By mimicking biological mechanisms, the “bio-inspired” computer networks promise efficiency, robustness, scalability, but also “adaptivity” and “evolvability.”

In the future, big chunks of the Net will be “autonomic” [3, 14]. Networks will be able to learn how to respond to new kinds of perturbations. They will be able to absorb and disperse the bad signals whilst transmitting the good ones. They will be resilient to viruses, failure or catastrophic events.

Many networks will be self-managed [2, 15], though human intervention will still be needed. It will be necessary to incorporate higher-level management mechanisms to manage the complex entangle of autonomic elements. There is a possibility that the introduction of sophisticated automatisms will generate new problems in terms of signaling, stability, security and trust. The multiplicity of autonomic systems will interact, influencing each other. How can we ensure that such interactions do not degenerate or create interferences or instabilities?

Just as in the evolutionary networks within nature, the different sub-systems of the future Internet will morph over time. However, computer networks are influenced by multiple factors that we have not yet learnt how to master. The evolution of the Net is affected in different ways by technology, but also by economic, political, legal and social elements. Until we find out how to realize a self-sustained digital ecosystem, we shall continue to need human intervention for purposes such as global optimization, regulatory obligations, law enforcement, business and provision of quality levels [16, 17]. Thus, for many years to come, it will still be necessary to monitor the autonomics and possess a means to influence it positively.

## 10.5 Dependable Networks

As the Net is used more and more for time-constrained applications, we are left to deal with a critical question: how *reliable* is the Net? We mentioned earlier that the typical packet-loss rate is in the order of 8–10% (internettrafficreport.com). However, even though so many packets are dropped, we can still run a variety of applications [18]. This has been made possible by innovating the applications rather than trying to introduce better network mechanisms. The innovation has taken place on the network’s edges through techniques such as *caching*, *adaptive coding*, *scalable coding* or *P2P transmission* (to mention just a few) [19–24].

Yet, the transition from the current *best-effort* network to a more *dependable* Net will be unavoidable if the unrelenting trend towards extreme *ubiquity* and *mobility* continues. At present, networks put little effort into delivering packets on time. When a packet is dropped, the IP layer has the tendency to forget about it and move on with normal life. This means that not much is done in the core network, apart from buffering the packets during congestion periods. However, *buffering* is not the ultimate solution. It is just a temporary patch that has the ability to deal with transient problems. The very heart of the network, the all-optical trunks, is not even able to perform any buffering.<sup>10</sup> Also, by buffering a packet, we shield it from congestion while, at the same time, incurring extra latency.

The existing network mechanisms concerned with *congestion* and *packet loss* are rudimentary. Packets are dropped unpredictably. When a loss is detected at the application layer (e.g., through TCP or within the application), we can try to recover the packet by requesting a retransmission. Yet, just like buffering, *retransmission* affects the communication latency. What is worse, there is no way to determine whether the retransmitted data can in fact meet its delivery deadline. Obviously, a “failed” retransmitted packet (one that reaches the application too late and is unusable) incurs unnecessary traffic. Also, if a packet is dropped due to congestion, chances are that the retransmitted packet will suffer the same destiny. Thus, packet retransmission, as such, does not provide a solid answer to “reliable” transmission and is potentially a counter-productive measure (retransmissions worsen congestion).

The key reason why the Net does not offer robust transmission is lack of parallelism. If a path is congested, the Net tries to find a diversion, and it does so pretty slowly. The lesson learned from P2P applications is that a much better approach is to seek alternative sources. There is huge data redundancy in the Net; therefore, it does not make sense to only transmit via point-to-point channels. Exemplar transmission mechanisms are *chunk-based* transport, *multi-layered* transport, *redundant-data* transport and *location-dependent* transport such as in cloud services.

The foundations of dependable networks lie on intelligent routing and transport mechanisms that incorporate *parallelism*, *context-awareness* and *content-awareness*. Significant research efforts are currently directed towards such a *cross-layer routing* approach [25].

## 10.6 The Fine Line Between Freedom, Security and Privacy

Many people today trust the Net with their most private data. To make a transaction, we post our credit card details and other personal data. While we browse through an e-shop, we actually leave traces of our preferences. Blogging and twitting are vehicles for people to express opinions, which, in some countries, may

---

<sup>10</sup> Optical buffering is currently one of the major hurdles in the realization of all-optical networks, which would lead to a substantial increase in network capacity.

lead to persecution or prosecution. On the other hand, monitoring, tracing and logging over the Net are required for the purposes of *law enforcement* and *cybercrime prevention* [26].

Thus, a most controversial issue is how to balance freedom, security and privacy [27]. A number of technical as well as legal tools have been developed for the purpose of (and in the name of) security. For instance, telecom providers must be able to supply so called *legal intercepts* in response to a court order. Similarly, ISPs are required to disclose to the judge the personal whereabouts of alleged cybercriminals.

However, within the Net, there is only a very fine line between security, crime and prosecution: the very same security tools may be misused by cybercriminals or by totalitarian regimes [28].

The Net is not well equipped to protect our privacy. Thus, a number of techniques are being developed to tackle the issue in a radical way, for example, through anonymity-support services [29, 30]. Clearly, if the identity of a blogger is hidden to the ISP, he can voice his opinion online without fear of being persecuted. Yet again, anonymity works against security because it allows cybercriminals to hide.

Looking at the present technology, there is no apparent solution to the “freedom-privacy-security” clash. This is possibly because the Net, that is, the primary handler of sensitive data, is totally oblivious to the problem. The IP is geared for “sharing” more than it is for “securing” data. It comes with some raw mechanisms for encrypting packets, but is oblivious to the issues of *freedom*, *privacy*, and *security*. Unlike any other complex network (e.g., the biological networks), the Net has no self-defense mechanisms. The result is that a predominant fraction of the Internet traffic today relates to *viruses*, *spam*, *polluted content*, and *malicious software*. The Net does not know how to identify and slow down the propagation of “bad” data whilst accelerating the distribution of the “good” one.

The consequences are dramatic. An estimated 80% of emails are spam, which costs businesses in the range of \$20.5 billion annually, a figure that will soon rise to \$200 billion (spamlaws.com). Identity theft hits around \$10 million Americans a year and costs businesses about \$200 billion a year. Similarly astonishing figures relate to viruses and the other plagues of the Net.

Despite the significant attention by the policy-makers, the critical issues surrounding freedom, privacy and security are still partly in the hands of the cybercriminals. This complex issue must be tackled at a global scale and in every element of the digital society. The next-generation network can no longer remain out of the problem.

## 10.7 Energy-Efficient Networks

Harvard scientists estimate that today “the whole ICT sector produces as much greenhouse gases as all airline companies together” [31]. An increasing fraction of energy is consumed by the large data centers—1000 *Google* searches burn about



as much energy as driving 1 km with a car. The network itself takes a large toll. A 2007 study by *Telecom Italia* unveiled that its network absorbed over 2TWh, representing 1% of the total national demand, which ranked the company as the second largest energy consumer (after the *National Railways*).<sup>11</sup>

As much as they have become crucial to the global economy, today's networks are not at all eco-friendly. They are always ON and burn energy even when they are on standby. The energy consumption of an Internet connection is dominated by the access network, particularly the broadband access lines. The deployment of fiber-to-the-home (FTTH) will lead to substantial improvements (optical transmission is more efficient than electrical). Substantial effort is in fact directed towards all-optical networks, but many fundamental issues still remain open: how can we build all-optical routers if we do not know how to construct suitable optical buffers?

In parallel to the research efforts on the “physics” of networks, significant breakthroughs are required on the “soft” aspects. Improving the routing architectures along the lines indicated earlier in this chapter (*context-awareness, small-worldness, autonomicity, parallelism* etc.) will be a priority.

Another dimension of energy-efficiency [32] is created by the convergence between the conventional networks and the emerging variety of wireless networks. These span beyond the confines of WiFi, WiMax and the cellular networks. Spontaneous, opportunistic connectivity along the concepts of *ad hoc networks* and *IoT* will surely gain importance. In this context, energy-efficiency is required at a different level, not just to save the planet. The emerging edge-network will comprise a range of battery-operated terminals that will participate in the complex routing game. Terminals will *source, filter, clean, store, relay* and *terminate* data. The terminals will play a key role in differentiating between “good” and “bad” data, filtering spam, eradicating viruses, aggregating data and help to propagate it reliably. In this way, the “edge” networks will help to keep the traffic local; they will have the ability to spot communication patterns, self-regulate and minimize their energy consumption. This vision of *cognitive networking* is debated passionately at the present, although we do not yet know how to realize autonomic networks that are also controllable, stable and reliable.

## 10.8 No Matter What, the Network will Remain Generative

We started this book writing about the “generative” power of the Internet [33]. On its conception, the Internet had not been designed in view of the phenomenal applications it is still sparking. Today, the search giant *Google* is valued at \$200

---

<sup>11</sup> C. Bianco, F. Cucchietti, and G. Gri, “Energy consumption trends in the next generation access network—a telco perspective,” International Telecommunications Energy Conference, INTELEC, Sep. 30–Oct. 4, Rome, Italy, 2007.

billion and the social network *Facebook* is worth \$50 billion.<sup>12</sup> Yet neither application was in the minds of the Internet architects, Robert Kahn and Vint Cerf.

Along with *creativity*, comes the urge to protect it from spam, viruses, computer hackers and the lot. Many attempts to protect our digital assets have resulted in measures that have, at times, restrained the “generativity” of the Net. For instance, we have seen a periodic alternation between those who support an “open” networked environment (one that gives wide freedom to individuals to manipulate their terminals, as in *Linux*) and those who are prepared to sacrifice this freedom in exchange for a greater sense of security (as in the video game consoles which do not allow any customization by the customer).

Nevertheless, even this emerging form of an “appliancized” network has not actually stopped the generativity of the Net. The iPhone/iPad phenomenon has proved that *device tethering* does not always confine our inventiveness. The apple store had 50,000 applications available in 2009 and 330,000 in January 2011, with a rate of 600 new applications submitted every day.<sup>13</sup> In comparison with other open platforms such as *Google Android*, we observe a counter-intuitive phenomenon: the sense of security instilled by a *tethered* network does occasionally surpass the sense of freedom instilled by an *open* network.<sup>14</sup>

Despite the unexpected developments of the last decade, the Internet “connectivity machine” has not seen many changes since its conception. Yet, it has continued to be the “generative” engine of our digital society. Scientists worldwide are now living the dream of yet a more generative next-generation network.

## References

1. Chaouchi H (2010) The internet of things: connecting objects. Wiley-ISTE
2. Kim S, Choi M, Ju H, Ejiri M, Hong J (2008) Towards management requirements of future internet. Challenges for next generation network operations and service management. Springer, pp 156–166
3. Liotta A, Liotta A (2008) P2P in a regulated environment: challenges and opportunities for the operator. *BT Technol J* 26:150–157
4. Akyildiz IF, Vuran MC (2010) Wireless sensor networks. Wiley
5. Farooq M (2010) Bee-inspired protocol engineering: from nature to networks. Springer, Heidelberg
6. Haykin S (2008) Neural networks and learning machines. Prentice Hall, New Jersey
7. XiaoFan W, Guanrong C (2003) Complex networks: small-world, scale-free and beyond. *IEEE Circuits Syst Mag* 3:6–20
8. Dressler F, Akan O (2010) Bio-inspired networking: from theory to practice. *IEEE Commun Mag* 48:176–183

---

<sup>12</sup> Source The Economist, 8–14 January 2011.

<sup>13</sup> Source <http://148apps.biz/app-store-metrics/>

<sup>14</sup> As of January 2011, the number of *android* devices has surpassed the number of iPhones. However, the number of iPhone apps is significantly larger.

9. Buchanan M (2003) *Nexus: small worlds and the groundbreaking theory of networks*. W.W. Norton & Company
10. Gammon K (2010) Four ways to reinvent the Internet. doi:[10.1038/463602a](https://doi.org/10.1038/463602a)
11. Clark DD, Partridge C, Braden RT, Davie B, Floyd S, Jacobson V, Katabi D, Minshall G, Ramakrishnan KK, Roscoe T, Stoica I, Wroclawski J, Zhang L (2005) Making the world (of communications) a different place. *SIGCOMM Comput Commun Rev* 35:91–96
12. Csermely P (2009) *Weak links: the universal key to the stability of networks and complex systems*. Springer
13. Dhillon S (2008) *Ant routing, searching and topology estimation algorithms for ad hoc networks*. Delft University Press
14. Papadimitriou D (ed) (2009) *Future internet—the cross-ETP vision document*, v. 1.0. <http://www.futureinternet.eu>
15. Jennings B, van der Meer S, Balasubramaniam S, Botvich D, Foghlu M, Donnelly W, Strassner J (2007) Towards autonomic management of communications networks. *IEEE Commun Mag* 45:112–121
16. Agboma F, Liotta A (2010) Quality of experience management in mobile content delivery systems. *J Telecommun Syst* (Special issue on the Quality of Experience issues in Multimedia Provision, 14 pages, Springer; Online First, 24 June 2010). doi:[10.1007/s11235-010-9355-6](https://doi.org/10.1007/s11235-010-9355-6)
17. Menkovski V, Exarchakos G, Liotta A, Sánchez AC (2010) Quality of experience models for multimedia streaming. *Int J Mobile Comput Multimedia Commun (IJMCMC)* 2(4):1–20. doi:[10.4018/jmcmc.2010100101](https://doi.org/10.4018/jmcmc.2010100101)
18. Handley M (2006) Why the Internet only just works. *BT Technol J* 24:119–129
19. Alhaisoni M, Liotta A (2009) Characterization of signaling and traffic in Joost. *Peer-to-peer Netw Appl* 2:75–83
20. Alhaisoni M, Liotta A, Ghanbari M (2009) Improving P2P streaming methods for IPTV. *Int J Adv Intell Syst* 2:354–365
21. Alhaisoni M, Ghanbari M, Liotta A (2010) Scalable P2P video streaming. *Int J Bus Data Commun Netw* 6:49–65
22. Alhaisoni M, Ghanbari M, Liotta A (2010) Localized multistreams for P2P streaming. *Int J Digit Multimed Broadcasting* 2010:1–13
23. Alhaisoni M, Liotta A, Ghanbari M (2010) Resource-awareness and trade-off optimization in P2P video streaming. *Int J Adv Media Commun* 41:59–77 (special issue on High-Quality Multimedia Streaming in P2P Environments)
24. Alhaisoni M, Liotta A, Ghanbari M (2010) Resilient P2P streaming. *Int J Adv Netw Serv* 3:209–219
25. Iannone L (2009) *Cross-layer routing and mobility management in wireless mesh networks*. VDM Verlag
26. Liotta A, Liotta A (2011) *Privacy in pervasive systems: legal framework and regulatory challenges. pervasive computing and communications design and deployment: technologies trends and applications*. Idea Group Publishing
27. Mackinnon R (2010) Liberty or safety? Both-or neither (spectral lines). *IEEE Spectr* 47:10
28. Rennhard M (2004) *MorphMix—a peer-to-peer-based system for anonymous internet access*. Shaker Verlag GmbH, Germany
29. Leavitt N (2009) Anonymization technology takes a high profile. *Computer* 42:15–18
30. Clarke I, Miller S, Hong T, Sandberg O, Wiley B (2002) Protecting free expression online with Freenet. *IEEE Internet Comput* 6:40–49
31. Bianco C, Cucchietti F, Griffa G (2007) Energy consumption trends in the next generation access network—a telco perspective. *Int Telecommun Energy Conf* 737–742
32. Restrepo J, Gruber C, Machuca C (2009) Energy profile aware routing. *IEEE Int Conf Commun* 1–5
33. Zittrain J (2009) *The future of the internet and how to stop it*. Yale University Press, London

Networks for Pervasive Services  
Six Ways to Upgrade the Internet  
Liotta, A.; Exarchakos, G.  
2011, XVIII, 162 p., Hardcover  
ISBN: 978-94-007-1472-4