

Introducing Neutral Access Networks

Alessandro Bogliolo
Information Science and Technology Institute
University of Urbino
Urbino, Italy 61029
Email: alessandro.bogliolo@uniurb.it

Abstract—Open access networks (OANs) have been recently proposed as a mean for bridging digital divide and enhance Internet penetration by enabling a fair competition among Internet service providers on a shared access infrastructure.

This paper introduces the concept of *neutral access networks* (NANs), which are a special class of OANs conceived to grant positive externality to the shared infrastructure. Externality creates a positive feedback loop among users, service providers, and network operators which increases market penetration, motivates the development of new services, and promotes the deployment of new access networks.

NANs are presented and discussed in terms of business models, market penetration, usage patterns, external benefits, technical feasibility, and legal issues.

I. INTRODUCTION

Aggregate IP traffic is doubling every two years [1], Internet is becoming more and more integrated into our lives [2], and broadband connectivity is considered to be a top priority worldwide. Nevertheless, there is a stagnation in the broadband market due either to the *lack of supply* (incumbent operators are not motivated to support bandwidth-intensive innovations, while new entrants cannot afford the investments required to create their own access networks) [3], or to the *lack of demand* (stagnation in what users can do with networks ultimately leads to a stagnation in users' demand for networks) [4]. Race, gender, education, purchase power, cultural background, and technical ability are additional determinants of broadband access [5], [6], that affect individuals' perception of network potentials, the willingness to pay for bandwidth, and the ability to fully exploit it [7].

According to the Broadband Working Group of the MIT Communications Futures Program, there is a so-called *broadband incentive problem* that comes from the inadequacy of the prevailing business model, which is based on *vertical integration* and on *flat-fee* pricing models [4].

Price is important both to understand the market and to shape it [5]. Flat rates were introduced in the narrow-band era to encourage penetration, but they induce user behaviors which are not correlated with the costs they impose to network operators. The diffusion of bandwidth-intensive applications and the extreme diversity of broadband traffic might induce operators to apply arbitrary restrictions on user behavior in order to monetize additional usage [4], ultimately violating neutrality and hampering innovation at the application level.

Vertical integration, on the other hand, originated from the monolithic structure of early telephone networks [3]. Nowa-

days it is still applied by most network operators in the attempt of realizing scope economies between physical access and online services [4]. Vertical integration, however, has several drawbacks: it limits innovation (by introducing dependences among different layers), it hampers competition (by raising entry barriers), it increases bandwidth costs (by reducing statistical resource sharing), and it endangers neutrality (by allowing incumbent operators to apply their own access policies) [3]. From a technical point of view, vertical integration fails in transposing to the business model the benefits of the layered nature of the network, based on TCP/IP and ISO/OSI models.

Liberalization of telecommunications was not sufficient, per se, to create a true competition, because of the tremendous advantage of incumbent operators owning (or controlling) the local access infrastructures, which account for 80% of network costs in fixed deployments [8]. Regulations were then introduced in many countries in order to create the conditions for a fair competition by forcing the sharing of fixed access infrastructures (by means of *local loop unbundling*, *line sharing*, or *bitstream access*) [9]. In 2006 broadband penetration in countries with access sharing regulations was more than twice larger than in countries without [10].

The advent of wireless access technologies (*WiFi*, *Hiperlan*, *WiMAX*) and the allocation of significant public funding to address digital divide, is offering the opportunity for deploying new access networks. In order for such networks to make the difference, however, they have to be designed, deployed, and managed by avoiding vertical integration. The need for new business models able to separate network access from service provisioning and to enable a fair competition on a shared infrastructure is particularly apparent in case of access networks subsidized by public money and deployed with the main purpose of maximizing public utility [8], [11]. The concepts of *operator-neutral networks* (ONNs) [12] and *open access networks* (OANs) [3] were introduced to answer this need.

OAN model encompasses a layered network architecture and a set of usage and trusting rules [3]. The OAN acts as an intermediary between users and services and it is composed of three main layers, represented in Figure 1: *access islands* (the local access infrastructures), *operator-neutral backbone* (the common infrastructure), and *service providers* (the entities providing online services, including Internet access) [8]. Battiti *et al.* introduced two sets of rules to be adopted in OANs in order to allow the network: *i)* to freely grow with needs and

opportunities (*anyone should be allowed to add access points and to extend the shared part of the OAN*) and *ii*) to enable a fair competition among operators (*all service providers must be offered the same conditions*) [3]. An additional rule of thumb can be derived from the working definition of *infrastructure sharing* (as opposed to the concept of *roaming* [13]) provided by Barceló *et al.*: An access network is shared if it contains independent edge routers for all the service providers that operate on it [8].

The aim of OANs is to realize a win-win scenario providing freedom of choice for users, freedom of service development for providers, and sharing opportunities for network deployment and maintenance costs. Schewick conducted a thorough analysis of the economic implications of open access policies [14].

Although the concept of OAN is independent of the access technology of choice, most of the testbeds deployed so far are municipal and academic *wireless* networks [11], [15], [16]. Motivation is three-fold. First, many wireless access networks have been deployed from scratch in the last years to address digital divide issues. New networks are much more suitable to be used as testbeds than existing ones. Second, wireless access technologies enable the deployment of public hot spots, which allow nomadic end users to associate to the network without incurring last-mile costs. Nomadic users are the ideal target for OANs since they are usually not registered with local operators. Third, many wireless access networks are subsidized by public funding and controlled by public institutions. This provides an additional motivation for operator neutrality and a suitable answer to the cumbersome question about *who should own, operate, and maintain an operator-neutral access network* [12].

Due to the above observations, the deployment of public wireless hot spots granting open access to a broadband network (possibly based on fixed access lines) can be regarded as a part of the OAN model [17]. A comparative analysis of the technical solutions available to implement wireless OANs is provided by Barceló *et al.* [8], who come to the conclusion that there are many viable solutions (evaluated in terms of security, maturity, scalability, and convenience), but the perfect sharing technology does not exist.

Sharing the access infrastructure, enabling horizontal scope economies, offering a fair playground for competition in broadband services, are not the only benefits of an OAN. In fact, the adoption of an open access policy also grants some *externality* to the access network, which represents an added value per se.

This paper is aimed at discussing the socio-economic potential of shared access networks, and the technical issues to be addressed to fully exploit it. Since neutrality is the key feature of the open access networks discussed in the rest of the paper, they will be hereafter called *neutral access networks* (NANs).

II. FROM OAN TO NAN

The main goal of an OAN is sharing the access infrastructure in order to realize scope economies and enable

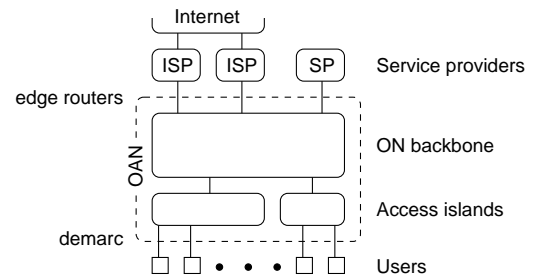


Fig. 1. Open Access Network (OAN) architecture.

competition. The OAN is nothing but an intermediary (that should be as *transparent* as possible) between users and service providers. The ideal sharing technology should give the end user the freedom of choosing among different service providers and the perception of connecting directly to the provider of choice. From a service provider perspective, the ideal sharing technology should combine the economic advantage of cost sharing with the distinguishing features of a proprietary network.

In the OAN architecture, service providers are represented as edge routers granting access to services which are external to the access network. In the typical case of an Internet service provider (ISP), the service provided is Internet connectivity with a given service level agreement (SLA). The technical solutions analyzed by Barceló *et al.* for the implementation of OANs [8] are aimed at allowing the user to register with the providers in order to gain access to their services. This vision introduces a beneficial separation between network access and services, but it does not change too much the business model of service providers, nor the motivation of the users for entering the network.

The NAN model retains the benefits of OAN, while making the access network *visible* (rather than *transparent*) to the end users. This is done by delivering a sizeable set of services directly within the access network, in order to make them available to all users before they register with a service provider and go through a specific edge router. In a NAN, users are no longer viewed as subscribers.

III. NEUTRAL ACCESS NETWORK MODEL

A. NAN business model

Among the commercial models that have been proposed in the context of OANs [3], [15], [16], [17], the *service-oriented* model is the most appropriate to be applied in a NAN. End users have commercial relationships only with service providers, that in turn pay a share of their revenue to the OAN organization. The share is then distributed among the stakeholders (real estate owners, investors, and technical operators) to cover operating costs and investments. Different cost models can then be applied, possibly based on *long run incremental cost* (LRIC) estimates [18] as recommended by the European regulatory framework.

According to the service-oriented model, users do not have to pay to enter the NAN. As discussed in the Subsection III-D, this is a sizeable advantage in terms of market penetration. Depending on the access technology in use, however, a non-negligible one-time cost can be associated with the so called *customer-premises equipment* (CPE) required to physically connect to the network. Referring to Figure 1, CPEs could be represented at the user side of the *demarcation point* (demarc).

In vertically-integrated access networks CPEs are usually provided by the operators and their costs are covered either by the activation fee or by the monthly rate paid by the subscribers. This model, however, does not apply to OANs, where service providers have no control on the infrastructure and network operators have no commercial relationships with end users.

Unless the CPE is integrated in users' terminals (as in case of WiFi), CPE provisioning and installation is a barrier that has to be overcome by the end user in order to gain access to an OAN. Two solutions can be envisaged: *i*) motivating the end user to overcome the barrier by paying for his/her own CPE, or *ii*) finding third-party motivations and resources for demolishing the access barrier by subsidizing the CPEs. In both cases, network externality and scope economies may help finding the required motivations.

B. NAN externality

Externality is a term used in economics to denote the (positive or negative) effect induced by an action (or decision) on third-party stake-holders who are not directly involved in it. A positive externality occurs whenever a new node/user/service is added to a network since it increases the networking opportunities for all other users. The positive externality is apparent in the Internet, while it is not in vertically-integrated access networks, in which it is limited to low-cost internal communications offered by some ISPs to their subscribers. In case of under-provisioned access networks, external diseconomies may also occur because of bandwidth bottlenecks: The larger the number of subscribers the lower the speed of their Internet connection.

NANs are characterized by a positive externality since they are full-fledged networks by themselves. The entry of a new user into the NAN has a beneficial effect for all other users since it enhances their communication potentials and it helps reaching the critical mass of users required to incentivize the provisioning of new services and the extension of the access infrastructure. Similarly, the entry of a new service provider has a spillover benefit for all other providers since it induces new users to enter the shared marketplace and it contributes covering the costs of the infrastructure. Finally, the extension of the infrastructure (possibly consisting in the deployment of new access islands owned and/or managed by new operators) has a positive effect on the usage of the existing infrastructure since it increases networking opportunities, ultimately affecting users' motivations to become part of the network.

In other words, all the entities involved in a NAN add to the value of the NAN, and benefit from its value.

C. NAN usage patterns

The breakdown of Cisco's traffic forecasts [1] provides useful elements to envisage the potentials of NANs. According to Cisco, in fact, the exponential growth of aggregate IP traffic (which is doubling every two years) accompanies sizeable changes in usage patterns and users' behaviors. In particular: *i*) consumer IP traffic grows faster than business IP traffic; *ii*) there is a higher growth in metro networks than in backbone networks; *iii*) in 2011 43% of IP traffic will be *non-Internet traffic* (i.e., traffic generated by the delivery of video services over IP within operators' networks) which accounted for only 18% in 2006; *iv*) P2P traffic will decrease as a percentage of overall consumer Internet traffic (from 62% in 2006 to 43% in 2011); and *v*) Internet video streaming will grow as a percentage of consumer Internet traffic (from 9% in 2006 to 30% in 2011).

All the above elements suggest that access networks are gaining importance not only to provide Internet access, but also to deliver IP services which are local to the network, or made accessible within the network. Also, a significant shift is observed from business traffic to consumer traffic.

NANs provide a suitable answer to these trends while also promoting the development of new services and the emergence of new usage patterns. The main novelties, to this purpose, are the opportunity of delivering online services to users who don't need to register with any ISP, and the possibility of exploiting the territorial dimension of the access islands. Active citizenship, tourism, digital inclusion, and proximity marketing are some of the fields that could benefit from access network neutrality.

D. NAN penetration

As stated in the introduction, broadband penetration is hindered not only by the lack of access infrastructure, but also by the lack of demand. Many people do not subscribe to any ISP just because they have not enough motivation to pay a flat fee before even knowing which services they will really use. The limited market penetration, in its turn, is a deterrent to invest in the deployment of broadband infrastructures in sparsely populated regions.

NANs may have higher penetration than traditional access networks for several reasons. First, because they are open to users who are not subscribers and who possibly pay only for the services they really benefit from. Second, because they may contain online services (like tourist information, local news and advertising, IP-TV) which are more actual and easier to understand than "Internet connection" for people who are not familiar with the Internet. Third, because they enable the development of public online services delivered for free. Fourth, because of the externality discussed in Section III-B, which makes it convenient for all the stake-holders to involve more people in the network.

All the above observations are based on positive externality, which is a distinguishing feature of NANs. Externality occurs, however, if there are suitable infrastructures, a sufficient number of users, and a sizeable pool of online services. If this is

not the case, either venture capitals or public investments are required to reach the critical mass needed to trigger positive externality.

To this purpose, it is worth noting that NANs are more suitable to be subsidized than traditional access infrastructures, since: they provide more guarantees of fair competition and public utility, they can be used to deliver public services and implement social policies, and they make it easier to trigger the positive externality required to guarantee network development and long-term sustainability.

IV. NEUTRAL ACCESS NETWORK IMPLEMENTATION

NANs are OANs with enhanced externality. This section discusses the technical requirement and the legal issues raised by this additional feature.

A. Technical aspects

Many technical solutions exist to implement operator-neutral access networks and many of them can be also applied to NANs. However, they are not equally capable of granting positive externality to the access networks.

A thorough analysis of the available technologies is beyond the scope of this work, which is a position paper introducing the concept of NANs and discussing their key features independently of the technology in use. Nevertheless, practical examples are useful to point out the impact of implementation choices on network neutrality, and to outline the minimum requirements that must be satisfied by any enabling technology.

Significant examples of technical solutions are provided by Barceló *et al.* [8]. Although the comparative analysis they provide is focused only on wireless OANs, the set of solutions they present is rich enough to support our discussion. Solutions include: *i*) DHCP relay (each user receives IP configuration from the SP he/she is registered to [19]); *ii*) tunneling (users associate with the OAN without authentication, but they need to authenticate to establish a virtual tunnel towards the SP of choice [11]); *iii*) SSID separation (each access point broadcasts multiple *service set identifiers* to create separate 802.11 wireless LANs for the SPs); *iv*) CAPWAP VLAN differentiation (users are assigned to SP-specific VLANs based on their 802.11i authentication [20]); and *v*) IPMS-WLAN interworking (the same WLAN is used to allow the user to gain access to different *public land mobile network operators* [21]).

Even if significant differences exist in terms of security, scalability, maturity, and convenience [8], all the above technologies provide feasible solutions to allow the users to register with the SP of choice through a shared infrastructure. However, most of them (namely, DHCP relay, SSID separation, CAPWAP, and IPMS) make the access network so transparent to the end user that they fail in creating a true NAN. The user receives SP-specific IP configuration based either on the MAC address of its terminal, on the credentials used for 802.11i authentication, or on the SSID of choice. Although the same infrastructure is shared by many SPs, the user is required to make a choice before even entering the network, so that he/she

is treated as a subscriber and he/she does not perceive any service but the ones offered by the SP he/she subscribed to. Needless to say, this impairs externality. In addition, DHCP relay and SSID separation suffer from scalability issues, while CAPWAP and IPMS are still immature.

Among the above mentioned techniques, tunneling [11] is the only one granting visibility to the shared infrastructure, since it allows unauthenticated users to connect to the network, to take advantage of internal services, and eventually establish a tunnel with the provider of choice. In addition, tunneling is almost independent of the network architecture and it minimizes the coordination effort among the entities involved. This is done, however, at the cost of losing in *convenience* [8], since tunneling clients are not pre-installed on most terminals and they are not sufficiently user-friendly to be widely accepted.

An alternative solution has been developed by the University of Urbino and tested in its wireless campus. The access network is open to unauthenticated users, who are dynamically assigned with private IPs. A subnet is used to publish internal services directly available within the access network, while a captive portal redirects the users to a predefined landing page whenever they attempt to access an external URL which is not white-listed. The landing page contains a link to the internal web portal, which grants access to all the local services available. Moreover, the landing page of the captive portal allows the end user to choose among several edge routers (managed by different SPs/ISPs) to gain access to external services. As the user makes his/her choice, a source-based policy route is dynamically created on the captive portal to route across the selected edge router all the traffic originated from the private IP assigned to the user. The same solution is adopted to manage both nomadic users connected to public hot spots and residential users directly connected to the Hiperlan backbone by means of CPEs. VPN tunnels are also used as a second choice.

In general, NANs should be implemented in order to support unauthenticated connection to the shared network, direct access to internal services, and authenticated access to external services. In addition, they should guarantee independence from access technology, minimize the technical commitment among the entities involved, and guarantee scalability.

B. Legal aspects

The possibility of granting access to unauthenticated users before they register with a SP in one of the main strengths of NANs. Dealing with unauthenticated users, however, raises legal issues the solution of which requires a paradigm shift in the responsibility chain.

Telecommunication networks and online services are often used to break the law. Typical Internet crimes include defamation, copyright infringement, and security fraud. Although the *intermediary liability* of Internet operators for the misconduct of their users is a controversial matter [22], [23], SPs must provide the technical support required to detect and prosecute law infringements. Moreover, ISPs are subject

to telecommunication data retention directives (such as the 2006/24/EC adopted by the European Community in March 2006) which impose them to identify their users and to track Internet transactions in order to enable anti-terrorism control.

Internet users are liable for their acts on the Internet, but they are hidden behind their *digital identities*, so that network operators and SPs need to be involved in order to trace back the digital identities to users' *real identities*.

Authentication is the process of claiming a digital identity by presenting valid (and unique) credentials. *Registration* is the process of obtaining a digital identity and the credentials required to claim it. We call *strong registration* a registration process which provides a digital identity uniquely associated with a real identity, confirmed (either directly or indirectly) by a valid personal ID.

In the vertical model typical of telecommunication operators, ISPs are responsible for the strong registration of their customers and for keeping track of the (static or dynamic) association between users and IPs. On the other hand, online services are published on the Internet, so that any user has to obtain a public IP from an ISP in order to take advantage of them. As a result, the user responsible for an offending transaction can be identified according to the following responsibility chain:

offending transaction \xrightarrow{SP} public IP \xrightarrow{ISP} user's identity

The key advantage of this responsibility chain is that SPs are allowed to adopt weak registration procedures that do not entail the acquisition of verified personal data (unless they are strictly required because of the nature of the online service provided).

Assume that some online service (e.g., e-mail) has been used to commit a crime (e.g., defamation). Once the crime has been reported, a timestamp and a source address (uniquely identifying the SP managing the online service) are taken from the offending transaction. The logs maintained by the SP are then used to obtain the IP address the user connected from, which uniquely identifies the ISP he/she used to connect to the Internet. At this point, traffic logs maintained by the ISP are used to obtain the digital identity of the user, while registration logs are required to go up to his/her real-world identity (according to the personal ID he/she exhibited to obtain the digital identity).

In a NAN, online services are directly exposed to unauthenticated users who are assigned with private IPs. Users are not identifiable unless they authenticate with credentials obtained by means of a strong registration procedure. As a consequence, SPs need to assume direct responsibility for the identification of their customers. It is worth noticing that in this scenario ISPs are nothing but SPs who provide Internet access through their edge routers.

Imposing strong registration to gain access to online services represents a big change in the behavior of both Internet users and SPs, which might end up hindering service accessibility and usability.

The solution to this problem is twofold. First, passive services delivered for free (like tourist information, news, advertisements, proximity services, broadcasting) do not require user authentication. Second, open standards can be adopted to enable ID portability by separating service provisioning from ID provisioning [24]. Third-party entities, called *ID providers* (IDP), can come into the picture to take care of users' registration and authentication, while allowing the SPs to implement their own authorization and accounting policies. According to the principle of *federated identity* [25], multiple IDPs can cooperate in the same network providing uniform authentication services to their users. In a NAN, IDPs could be responsible for the implementation of strong registration and authentication procedures made available to all SPs in order to guarantee user identification according to the following chain:

offending transaction \xrightarrow{SP} digital ID \xrightarrow{IDP} user's identity

Even the ISPs operating on the NAN could take advantage of the identity management services made available by IDPs. In this case, the identification of an Internet user responsible for a malicious use of an online service involves the SP who made the service available on the Internet, the ISP who granted Internet access from the NAN, and the IDP who provided authentication and registration services.

offending transaction \xrightarrow{SP} public IP \xrightarrow{ISP} digital ID
digital ID \xrightarrow{IDP} user's identity

As a side benefit, ID portability would allow each individual to use the same credentials to authenticate with different providers, thus reducing the *password fatigue* caused by the proliferation of virtual identities belonging to the same person.

V. CONCLUSION

A new model of access network, called *neutral access network* (NAN), has been introduced. NANs retain the benefits of open access networks in terms of fair competition and infrastructure sharing, while inducing positive externality in order to enhance market penetration, motivate development, and reach sustainability.

The NAN model has been motivated, presented, and discussed, and the main implementation issues have been addressed in the paper.

The feasibility of the proposed model has been tested on the *Urbino wireless campus* testbed [11], while economic experiments are under development to evaluate the effects of externality.

ACKNOWLEDGMENT

The authors would like to thank Andrea Seraghiti, from the University of Urbino, Italy, and Jaume Barceló and Jorge Infante, from the Universitat Pompeu Fabra, Barcelona, Spain, for many useful discussions.

REFERENCES

- [1] Cisco, "Global ip traffic forecast and methodology," *Cisco White Paper*, 2008.
- [2] ITU, "digital.life - itu internet report 2006," International Telecommunication Union, Tech. Rep., 2006.
- [3] R. Battiti, R. Lo Cigno, M. Sabel, F. Orava, and B. Pehrson, "Wireless LANs: From WarChalking to Open Access Networks," *Mobile Networks and Applications*, vol. 10, pp. 175–287, 2005.
- [4] Broadband Working Group, "The broadband incentive problem," *MIT Communications Futures Program White Paper*, September 2005.
- [5] K. Flamm and A. Chaudhuri, "An analysis of the determinants of broadband access," *Telecommun. Policy*, vol. 31, no. 6-7, pp. 312–326, 2007.
- [6] J. E. Prieger and W.-M. Hu, "The broadband digital divide and the nexus of race, competition, and quality," *Information Economics and Policy*, vol. 20, no. 2, pp. 150 – 167, 2008.
- [7] S. J. Savage and D. M. Waldman, "Ability, location and household demand for internet bandwidth," *International Journal of Industrial Organization*, vol. In Press, Corrected Proof, 2008.
- [8] J. Barceló, A. Sfairpoulou, and B. Bellalta, "Wireless open metropolitan area networks," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 12, no. 3, pp. 34–44, 2008.
- [9] European Commission, "Unbundled access to the local loop. dg information society working document," European Commission, Tech. Rep., 2000.
- [10] S. Turner, "Broadband reality check ii: The truth behind america's digital decline," *Free Press*, 2006.
- [11] A. Bogliolo, "Urbino wireless campus: A wide-area university wireless network to bridge digital divide," in *Proceedings of AccessNets-07*, 2007, pp. 1–6.
- [12] V. Kordas, E. Frankenberg, S. Grozev, B. L. N. Zhou, and B. Pehrson, "Who should own, operate and maintain an operator neutral access network?" in *LANMAN2002: IEEE Workshop on Local and Metropolitan Area Networks*, 2002.
- [13] B. Anton, B. Bullock, and J. Short, "Best current current practices for wireless internet service provider (wisp) roaming," Wi-Fi Alliance, Tech. Rep., 2003.
- [14] B. van Schewick, "Towards an economic framework for network neutrality regulation," *Journal on Telecommunications and High Technology Law*, vol. 5, pp. 329–392, 2007.
- [15] J. Barceló, C. Macán, J. Infante, M. Oliver, and A. Sfairpoulou, "Barcelona's open access network testbed," in *Proceedings of IEEE Tridentcom*. IEEE, 2006.
- [16] L. Berthilsson, *StockholmOpen - Roles, Requirements and Economic Models*, ser. MS Thesis. IT University of Kista, 2003.
- [17] J. C. Francis, N. Elnegaard, T. G. Eskedal, and R. Venturin, "Business opportunities of open broadband wireless access networks," in *Proceedings of Int'l Workshop on Broadband Wireless Access for Ubiquitous Networking*, 2006.
- [18] L. Rodriguez de Lope and K. Hackbarth, "Cost model for bitstream access services with qos parameters," *Journal of Universal Computer Science*, vol. 14, no. 5, pp. 653–672, 2008.
- [19] R. Droms, "Dynamic Host Configuration Protocol," *RFC 2131*, 1997.
- [20] P. Calhoun, M. Montemurro, and D. Stanley, "CAPWAP Protocol Specification," *IETF Intern Draft*, 2008.
- [21] 3GPP TSG Service and System Aspects, "3GPP system to WLAN interworking; System description (Release 8)," *3GPP TS 23.234 V8.0.0*, 2008.
- [22] K. A. Taipale, *Secondary Liability on the Internet: Towards a Performative Standard for Constitutive Responsibility*, ser. Working Paper Np. 04-2003. Center for Advanced Studies in Science and Technology Policy, 2003.
- [23] T. J. Mann and S. R. Belzley, *The Promise of Internet Intermediary Liability*, ser. Law and Economics Working Paper No. 045. The University of Texas School of Law, 2005.
- [24] N. Ragouzis *et al.*, *Security Assertion Markup Language (SAML) V2.0 Technical Overview*, ser. OASIS Draft. OASIS, 2007.
- [25] T. scavo *et al.*, *Shibboleth Architecture - Technical Overview*, ser. Working Draft 02. Internet2, 2005.