Freiburger Studien zur Netzökonomie 21

Günter Knieps | Volker Stocker [eds.]

The Future of the Internet

Innovation, Integration and Sustainability

Nomos

Freiburger Studien zur Netzökonomie

Prof. Dr. Günter Knieps, Universität Freiburg

Volume 21

Günter Knieps | Volker Stocker [eds.]

The Future of the Internet

Innovation, Integration and Sustainability

Nomos

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.d-nb.de

ISBN 978-3-8487-6080-0 (Print)
978-3-7489-0209-6 (ePDF)

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN 978-3-8487-6080-0 (Print)
978-3-7489-0209-6 (ePDF)

Library of Congress Cataloging-in-Publication Data
Knieps, Günter / Stocker, Volker
The Future of the Internet
Innovation, Integration and Sustainability
Günter Knieps / Volker Stocker (eds.)
245 pp.
Includes bibliographic references.

ISBN 978-3-8487-6080-0 (Print)
978-3-7489-0209-6 (ePDF)

1st Edition 2019

No responsibility for loss caused to any individual or organization acting on or refraining from action as a result of the material in this publication can be accepted by Nomos or the editors.

Table of Contents

Internet of Things (IoT), heterogeneous virtual networks and the future of the Internet

Günter Knieps[1]

Abstract

The Internet of Things (IoT) makes it necessary to rethink the future role of the Internet. Different physical network services (e.g. shared mobility services, smart rail services, smart energy services) require different implementations of virtual networks, all based on QoS requirements for data packet transmission within mobile and fixed broadband networks. The focus of this chapter is on the heterogeneity of virtual networks for a large variety of physical network services. The heterogeneity of relevant dimensions of virtual networks is analyzed, specifically considering heterogeneous QoS requirements of all-IP bandwidth capacities, heterogeneous sensor network requirements, heterogeneous geopositioning services as well as heterogeneous data processing and cloud computing. A basic goal of network virtualization is to bundle the end-to-end responsibility for privacy and security concerns regarding the virtual side of IoT applications in the hands of the provider of the virtual networks.

Keywords: Internet of Things, Economics of virtual networks, Smart networks

[1] University of Freiburg, Chair of Network Economics, Competition Economics and Transport Science; guenter.knieps@vwl.uni-freiburg.de

1. Introduction

Smart networks may be considered as an "envelope concept" focusing on the combination of Information and Communication Technologies (ICT) with traditional infrastructure networks providing physical network services. Smart bidirectional metering, sensors, actuators and remote control by interactive machine-to-machine communication, in combination making up the so-called Internet of Things (IoT),[2] are becoming increasingly important on the road towards smart networks (European Commission, 2015; OECD, 2012, 2013a, 2013b). The IoT makes it necessary to rethink the future role of the Internet. Real-time two-way communication between sensors and actuators as well as communication between physical and virtual networks is gaining importance, e.g. the remote tactile steering or control of an object via the Internet. For example, vehicles in a platoon need to be connected with 1-2 ms latency and thus have very low latency tolerance. Other examples requiring very low latency guarantees are remote driving and real-time control of microgrids. Hence ICT based steering and control of physical networks are becoming increasingly important in the future IoT.

The focus of this chapter is on IoT applications which are characterized as smart physical network services. The interaction between physical networks and ICT is challenging the industrial organization of network industries (Knieps, Bauer, 2016). On one hand, a fundamental change is taking place in traditional network industries and physical network services, with real-time, location aware and adaptive network capacity allocation becoming particularly relevant. On the other hand the traditional communication and entertainment oriented Internet is challenged to meet the ICT requirements of smart network industries and more general of the app economy.

The chapter is organized as follows: In the subsequent section 2 the design principle of IP based virtual networks required for various physical networks and for a large variety of physical network services is characterized. In section 3 the basic dimensions of virtual networks are considered. The intrinsic heterogeneity of virtual networks is analyzed, based on innovative entrepreneurial combinations of the heterogeneous dimensions of

[2] The term Internet of Things (IoT) most probably dates back to Kevin Ashton, who pointed out the particular relevance of the physical world compared to the virtual ICT world: "Ideas and information are important, but things matter much more" (Ashton, 2009, p. 1).

virtual networks. In particular, heterogeneous Quality of Service (QoS) bandwidth capacities, heterogeneous sensor networks, heterogeneous geopositioning requirements, heterogeneous (big) data processing capacities and heterogeneous security requirements are identified. In section 4 a concluding outlook is provided.

2. *IoT and the evolution of IP based virtual networks*

2.1. The complementarity between physical networks and virtual networks

From a network economic point of view the conceptual differentiation between services of physical network infrastructures (e.g. roads, railways, electricity networks) and complementary virtual networks based on ICT services is important (Knieps, 2017c). Different physical network services (e.g. shared mobility services, smart rail services, smart energy services) require different implementations of virtual networks, all based on QoS requirements for data packet transmission within mobile and fixed broadband networks. Virtual networks may be interconnected with other virtual networks (e.g. ubiquitous sensor networks) or via the all-IP Internet with other actors. For example, within a microgrid the aggregator must bundle the prosumer consumption and generation decisions within the different home networks and communicate the real-time import/export decisions to the wholesale distribution network operator. Home networks may also use multipurpose broadband communication architecture, not only for electricity applications based sensors but also for other communication requirements, e.g. entertainment (Knieps, 2017a).

2.2 IP based virtual networks

The Archimedean point of virtual networks is the evolution of the IP towards the universal network protocol for internetworking: the IP as the common network layer protocol for interconnecting many different networks, for instance cable, fixed and mobile communication networks etc. (Tanenbaum, Wetherall, 2011, pp. 424 ff.). Alternative broadband access networks, such as mobile access networks, fixed telecom access networks, or cable access networks are characterized by convergence towards all-IP networks (Knieps, Zenhäusern, 2015, pp. 339 ff.; Knieps, Stocker, 2016).

Based on the well-established concept of Next Generation Networks (NGN)[3] the concepts of Future Networks (FNs) and network virtualization have been developed, emphasizing the need for advanced traffic management to realize a wide scope of application services and heterogeneous network architectures on a common multipurpose ICT infrastructure (ITU-T, 2012, p. iv). Traditional specialized communication networks are thus challenged by the concept of network virtualization: "Network virtualization is a method that allows multiple virtual networks, called logically isolated network partitions (LINPs), to coexist in a single physical network" (ITU-T, 2012, p. 2).

Virtual networks provide the necessities for increasingly important end user demand for a wide scope of heterogeneous application services requiring heterogeneous ICT support. Different virtual networks require different QoS bandwidth capacities offered by traffic service providers. Service continuity may also require multiple interconnected virtual networks. Property rights and decision competency for the traffic service providers are different from those for the virtual networks providers. Whereas traffic service providers are offering QoS guaranteed bandwidth capacities for QoS requirements driven by IoT applications, virtual network providers combine specific QoS bandwidth capacities with other ICT components (virtual resources), such as sensoring, geopositioning, or data processing, to build a virtual network tailored for the requirements of complementary physical applications. Heterogeneous virtual networks have been analyzed for microgrids (Knieps, 2017a), smart sustainable cities (Knieps, 2017b), shared mobility services (Knieps, 2018a), and networked vehicles (Knieps, 2018b). Different (single purpose specialized) virtual networks may seamlessly cooperate without interoperability requirements between different traffic service providers. Cooperation between different virtual networks can serve as a substitute for interoperability agreements between different traffic services providers (Knieps, 2017c, pp. 243-246).

[3] An NGN is defined as follows: "A packet-based network able to provide telecommunication services and able to make use of multiple broadband QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users." (ITU-T Y.2001, 2004, p. 2).

3. Heterogeneity of virtual networks

Virtual networks for a large variety of physical network services are based on the following dimensions:

- All-IP based real-time and adaptive broadband communication networks
- IP based sensor networks
- Global navigation satellite systems and their overlay position correction networks
- (Big) Data processing, cloud computing and fog computing
- Privacy and security

The IoT application driven variety of virtual networks is based on entrepreneurial combinations of the different dimensions of virtual networks. In the following the heterogeneity requirements for the different dimensions of virtual networks are elaborated.

3.1 Heterogeneity of QoS requirements of all-IP bandwidth capacities

Due to the unified standardized Internet Protocol IP, different stationary and mobile broadband technologies can be used for data packet transmission in the future all-IP Internet. Utilization dependent user fees are also becoming indispensible for data packet transmission in the all-IP Internet. The prioritization of data packets within different QoS classes for providing deterministic or stochastic QoS guarantees necessitates access controls, and concomitant price and quality differentiation for different quality classes. Traffic services providers can use the resultant revenues, in addition to the fixed connection fees, for investment in broadband capacities. Heterogeneous traffic classes without deterministic QoS guarantees are characterized in Babiarz et al. (2006). A hierarchy of heterogeneous stochastic QoS classes can be established in such a way that the highest classes are Expedited Forwarding (EF), followed by Assured Forwarding (AF) and Default Forwarding (DF) providing the lowest “Low Priority Data service class” (for non-real time and elastic traffic). For deterministic QoS guarantees, see Ash et al. (2010).

The economic incentives for QoS differentiation traffic classes can only be analyzed if the entrepreneurial QoS potentials and related traffic architectures are taken into account. Prioritization of data packets can take place within the DiffServ architecture, enabling a hierarchy of traffic classes without deterministic QoS guarantees (Knieps, 2011). The Generalized DiffServ architecture provides the open set of flexible multipurpose traffic architectures supporting a variety of heterogeneous QoS classes required for different application services (Knieps, 2015, p. 739). Traffic QoS requirements cannot be considered from the perspective of IoT only, but have also to take into account all other application services provided within an all-IP network infrastructure. For deterministic QoS guarantees two complementary mechanisms are required: Firstly, admission control and associated priorities, secondly development of service restoration priority levels based on the criticality of services. As important network performance criteria delay, jitter and packet loss parameters are specified for stochastic and deterministic QoS guarantees. The hierarchy of traffic classes (implemented by admission control) is based on a monotone relation of more strictly defined QoS parameters with increasing opportunity costs of bandwidth capacity. The hierarchy of restoration priority is based on a monotone relation of opportunity costs of bandwidth capacity usage due to different restoration priority parameters.

The heterogeneous requirements of different deterministic and stochastic traffic qualities can be implemented by means of NGN, allowing the entrepreneurial search for QoS architectures and subsequent incentive compatible pricing schedules (Knieps, 2015; Knieps, Stocker, 2016). A well-defined hierarchy of traffic classes with different deterministic traffic quality guarantees is defined for NGN bandwidth allocations (Ash et al., 2010). It has been shown that QoS pricing for a hierarchy of deterministic traffic classes can be derived in an incentive compatible manner (Knieps, 2017c). The hierarchy of traffic classes is based on a monotone relation of opportunity costs of bandwidth capacity usage due to different QoS classes as well as restoration priority parameters. Network capacity (bandwidth) is allocated to each quality class (channel) separately, including the required reserve capacity due to the required restoration priority parameter to guarantee the deterministic parameters (delay, jitter, packet loss). Price and QoS differentiation pricing and investing rules for a hierarchy of deterministic QoS guarantees are derived, resulting in the following insights: The price for packet transmission increases with required traffic quality, because variable costs increase with traffic quality. For higher quality classes marginal cost functions are shifted upwards, resulting (ceteris paribus) in higher package charges.

3.2. Heterogeneous sensor network requirements

Heterogeneous sensor networks with strongly different characteristics can be differentiated, such as 6LoPan sensor networks (low costs, low speed) and camera based sensoring (high volume, very delay sensitive/tactile). During the last two decades there has been an evolution towards IP based sensor networks. Based on these standards for sensor networks, the innovation potentials of different virtual networks, which are complementary for the heterogeneous smart infrastructure services, can be realized. The important goal is to connect the metering and sensor networks to the all-IP Internet.

An important area for sensor networks is focused on low-cost, low-speed ubiquitous communication between devices based on low rate wireless networks with low transfer rates and very limited communication range. The IEEE 802.15.4. standard[4] specifies the physical layer as a required precondition for two major networking protocols, 6LoW PAN and ZigBee IP (Kushalnagar et al., 2007). Characteristics of Low-Power Wireless Personal Area Networks (LoWPANs)[5] are wireless sensors with small packet size, low bandwidth and Reduced Function Devices (RFDs). The benefits of IP v6 are the large address space, since a large number of devices are involved, as well as the seamless connectivity to other IP based networks without translation gateways (Kushalnagar et al., 2007). Interconnection can take place on the basis of existing IP network infrastructure. Even if different network carriers apply different QoS traffic architecture, only a mapping between the traffic classes of different carriers is required; emulation techniques like translation gateways are not necessary. Virtual networks can be designed by application providers based on the different QoS architectures of different traffic service providers.

The advantages of compatibility with the IPv6 network standard come at a cost. They require additional fragmentation due to the constraints regarding the size of the Maximum Transmission Unit (MTU) and lead to lower data rates. Since IPv6 requires the support of much larger packet

[4] IEEE 802.15 WG (Working Group) develops Wireless Personal Area Network (WPAN) standards for short distance wireless networks, https://standards.ieee.org/develop/wg/WG802.15.html

[5] “A LoWPAN is a simple low cost communication network that allows wireless connectivity in applications with limited power and relaxed throughput requirements. A LoWPAN typically includes devices that work together to connect the physical environment to real-world applications, e.g., wireless sensors.” (Kushalnagar et al., 2007, p. 1).

sizes than the largest IEEE 802.15.4. frame size, a LoWPAN fragmentation and reassembly adaptation layer must be provided at the layer below IP, because a full IPv6 packet does not fit in an IEEE 802.15.4 frame (Montenegro et al., 2007).

ZigBee Alliance and IETF are cooperating on the design of an open standard named ZigBee IP. The basic strategy is to use IPv6 whenever possible and introduce required modifications. A protocol has been defined to compress IPv6 datagrams and send them over 802.15.4 radio link. IPv6 Neighbor Discovery has been modified to find the IP addresses of directly reachable neighbors; there was also a protocol developed for allowing neighbors to exchange data. ZigBee IP: IEEE 802. 15. based specifications are using 6LoWPAN header compressions as a high level communication protocol. ZigBee IP, the IPv6 based standard for wireless sensor networks, enables multipurpose applications, not only for virtual microgrids but also for virtual networks supporting smart city IoT applications and smart water networks.

In contrast, tactile ad hoc radio networks require high data rates and high mobility. For these applications the tactile Internet with high throughput requirements and ultra-low latency guarantees combined with big data processing is required. The ultra-low latency requirements of the tactile Internet can be implemented within next generation 5 G networks, enabling multipurpose-driven different IoT applications such as networked vehicles, water sensors located within agricultural areas, or security cameras (Brake, 2016, pp. 2-6). Camera based sensoring (which involves high volumes of data) is implemented with compressor functions, combined with big data processing for networked vehicles applications (Knieps, 2018b).

3.3 Heterogeneous geopositioning services

In Intelligent Transport Systems as well as in other application areas of the IoT, in addition to real-time transmission, spatially differentiated data collection with an ever increasing positioning accuracy becomes increasingly important. Thus satellite navigation systems gain increasing significance. The geopositioning Overlay-System EGNOS (European Geostationary Navigation Overlay Service) is fundamentally an enhanced infrastructure system in the form of a satellite based differential GPS or Galileo. EGNOS improves accuracy and reliability by correcting the measurements in the GPS, respectively Galileo navigation systems. Galileo enhancement is based on the accurate positioning of mobile vehicles. EGNOS combined with digital cellular technologies enables a large variety of real-time and locational tailored applications in the app economy. Various EGNOS based applications are evolving, such as airport approach control, networked driving, intermodal local traffic (e.g. bus on demand services), entering ports in conditions of reduced visibility, and location based services within the city. The EGNOS infrastructure consists of three geostationary satellites and a network of ground stations. EGNOS has been founded by an agreement between the European Space Agency (ESA), the European Commission (EC) and Eurocontrol (the European Organisation for the Safety of Air Navigation).

Three categories of EGNOS services are provided:[6]

(1) Safety of Life (SoL), enabling safety critical transport applications with particular focus on aviation applications
(2) Open Service (OS) enabling improving position accuracy for applications where safety is not critical
(3) EGNOS Data Access Service (EDAS) providing additional services such as the EGNOS information broadcast through the GEO Signal In Space (SIS). Access to EDAS servers enables additional performance, in particular regarding the QoS of data packet transmission in real time and within guaranteed delay boundaries not available via the use of best effort Internet.[7]

EGNOS provides its services, which can be received throughout Europe, free of charge. The full transmission of data provided by EDAS Servers is IP based, either via best effort Internet or by point to point direct link guaranteeing higher performance. The costs of direct communication access lines are borne by the users.[8]

EGNOS can be used in all areas where precise geopositioning is of particular importance, such as aviation, networked/autonomous driving, rail traffic control, navigation in smart cities, or agriculture. Geopositioning systems differ from those of broadband infrastructures insofar as there is no rivalry in the receiving of positioning data. Because of this perfect non-rivalry in consumption, the financing target cannot be met through utiliza-

[6] https://gssc.esa.int/navipedia/index.php/Category:EGNOS_Services

[7] https://www.gsa.europa.eu/egnos/edas/condition-use-edas

[8] https://gssc.esa.int/navipedia/index.php/EGNOS_Data_Access_Service_(EDAS)

tion dependent user fees. Government financing thus seems to be the obvious solution.

3.4 Heterogeneous data processing and cloud computing

The collection, processing and transmission of large volumes of real-time and location aware data may become an important ICT component in many IoT applications. In the context of smart cities and Intelligent Transportation Systems speed sensors and high-resolution cameras are collecting large volumes of real-time traffic data, enabling intelligent traffic management. Platforms for networked driverless vehicles depend on ultra-delay sensitive adaptation to road traffic conditions within the nearby local environment. The design of big data virtual networks enables the combination of big data analysis for sensor-compressing with ultra-low latencies in data transmission, taking into account strict positioning requirements (Knieps, 2018b, pp. 5 f.).

The question as to where to locate the data processing leads to the division of labor between cloud computing and fog computing. The result may depend on different criteria, including data processing, bandwidth consumption, latency requirements and security and safety. Fog computing within the edge cloud is focused on local, highly distributed computing concepts (e.g. Bonomi et al., 2012, pp. 13 f; Chang et al., 2014, p. 346). The ultra-low latency requirements of networked automated vehicles result in the necessity of combining the highest QoS traffic class for bandwidth capacity with fog computing (Knieps, 2018b). The literature on big data, cloud computing and fog computing leaves open the question of how to allocate the decision competence among the different actors involved. However, the concept of the big data virtual network requires that the end-to-end responsibility and the decision competence to combine the required ICT components rest with the virtual network provider.

3.5 Heterogeneous e-privacy and security requirements

A basic goal of network virtualization is to bundle the end-to-end responsibility for privacy and security concerns regarding the virtual side of IoT applications in the hands of the provider of the virtual network.[9] Virtual networks should not create security externalities and in particular not cause disruptions to other virtual networks or physical networks. Authentication, authorization, and accounting of virtual resources are required, preventing the abuse of virtual resources and malicious attacks (ITU-T, 2012, p. 12). Privacy protection and security measures are relevant within all dimensions of virtual networks. The advantage of IP based virtual networks is their ability to benefit from the efforts of the IETF to develop security measures for data packet transmission. The focus of Internet Protocol Security (IPsec) is on the security of the IP protocol located at the network layer, avoiding attacks on protocols.[10] In contrast, attacks on users are largely independent from protocol details. The disaggregated approach to security concepts differentiates between security measures on the network layer, the transport layer and the application layer. The basic principle of network layer security architecture is the split between time-consuming authentication and the key exchange protocol step; this also establishes a security architecture on one hand and the actual data traffic protection on the other hand (Baker, Meyer, 2011). Whereas security requirements regarding confidentiality (unauthorized disclosure), integrity (data integrity and data origin authentication) and availability (mitigating denial-of-service attacks) are typically required on all layers, heterogeneous implementations of security mechanisms combining network layer security with application layer security are up to the security requirements of different applications (Baker, Meyer, 2011, pp.10 ff.). There are many ways in which IPsec can be implemented with heterogeneous granularity as regards the security service provided (Kent, Seo, 2005, p. 10).

In addition to the requirements, which must be met by the network architecture of an all-IP Internet, there are important challenges from a data

[9] "Since LINPs created by network virtualization are isolated and independently managed, conventional security considerations for non-virtualized networks should be independently applied to each LINP too. In addition to that, a security problem of an LINP should not be spread to other LINPs." (ITU-T, 2012, p. 6).

[10] "IPsec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, detection and rejection of replays (a form of partial sequence integrity), confidentiality (via encryption), and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection in a standard fashion for all protocols that may be carried over IP (including IP itself)." (Kent, Seo, 2005, p. 5).

privacy protection (e-privacy) and cyber security point of view, due to the increasing relevance of spatially differentiated real-time traffic data. In this context the principle of Geographic Location/Privacy (Geopriv) architecture has been developed: "A central feature of the Geopriv architecture is that location information is always bound to privacy rules to ensure that entities that receive location information are informed of how they may use it." (Barnes et al., 2011, p. 4).

Heterogeneous security requirements are also identified in the context of cloud computing, with a particular focus on data isolation, data protection and confidentially protection. Different cloud computing services require heterogeneous security mechanisms in order to avoid conflicts between different protection requirements (ITU-T, 2015, p. 12). Fog computing at the edges has particular protection requirements compared to cloud computing, because the fog devices are faced with a higher threat potential, which is typically not expected in the central cloud (Stojmenovic, Wen, 2014, p. 5). Security and privacy are also considered of particular importance for the 5 G networks of the future (Brake, 2016, p. 5). A disaggregated approach to security mechanisms within 5 G networks has been proposed, with a particular focus on the role of network slicing and heterogeneous application-specific security mechanisms (Ericsson, 2017, p. 8).

4. Conclusions

The IoT poses new challenges for the Internet of the future. Real-time transmission as well as spatially differentiated data collection are growing in importance. The transition from a narrowband best effort Internet to a multi-purpose Internet with active traffic management based on all-IP broadband infrastructure with QoS differentiated bandwidth capacities gains increasing relevance. All-IP broadband infrastructures endowed with the Generalized DiffServ architecture function as General Purpose Technologies (GPTs) for applications and services driven by innovational complementarities between Internet applications (e.g. search engines, PC software) and traffic services (Knieps, Bauer, 2016, p. 45). The IoT strongly enlarges the scope of applications and services. The entrepreneurial development of heterogeneous virtual networks is driven by the requirements of new markets for IoT applications, such as microgrids, shared mobility services and smart city concepts, requiring traffic architectures in an all-IP broadband network that provide stochastic and deterministic QoS guarantees (Knieps, 2017c). The potentials of a GPT for ICT based complementary innovations between traffic services and IoT based applications should therefore not be hampered by network neutrality regulation (Bauer, Knieps, 2018).

References

Ash, G., Morton, A., Dolly, M., Tarapore, P., Dvorak, C., & El Mghazli, Y. (2010), Y.1541-QOSM: Model for Networks using Y.1541 Quality-of-Service Classes, RFC 5976.

Ashton, K. (2009), That ´Internet of Things´ Thing – In the real world, things matter more than ideas, RFID Journal, 22 June, https://www.rfidjournal.com/articles/view?4986

Babiarz, J., Chan, K., & Baker, F. (2006), Configuration Guidelines for DiffServ Service Classes, RFC 4594.

Baker, F. & Meyer, D. (2011), Internet Protocols for the Smart Grid, RFC 6272.

Barnes, R., Lepinski, M., Cooper, A., Morris, J., Tschofenig, H., & Schulzrinne, H. (2011), An Architecture for Location and Location Privacy in Internet Applications, RFC 6280.

Bauer, J.M., & Knieps, G. (2018), Innovational Complementarities and Network Neutrality, Telecommunications Policy, 42,172-183.

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012), Fog Computing and Its Role in the Internet of Things, MCC, August 17, Helsinki.

Brake, D. (2016), 5 G and Next Generation Wireless: Implications for Policy and Competition, Information Technology & Innovation Foundation (ITIF), June, 1-22, www.ITIF.org.

Chang, H., Hari, A., Mukherjee, S., & Lakshman, T.V. (2014), Bringing the Cloud to the Edge, IEEE INFOCOM Workshop on Mobile Cloud Computing, 346-351.

Ericsson (2017), 5G Security: Scenarios and Solutions, Ericsson White Paper, Uen 284 23-3269, June.

European Commission (2015), A Digital Single Market Strategy for Europe, Brussels, 6.5. 2015, COM (2015)192 final.

ITU-T (2004), Next Generation Networks – Frameworks and functional architecture models: General overview of NGN, Recommendation ITU-T Y.2001.

ITU-T (2012), Framework of network virtualization for future networks, Recommendation ITU-T Y.3011.

ITU-T (2015), Security framework for cloud computing, Recommendation ITU-T X.1601.

Kent, S., & Seo, K. (2005), Security Architecture for the Internet Protocol, RFC 4301.

Knieps, G. (2011), Network neutrality and the Evolution of the Internet, International Journal of Management and Network Economics, 2(1), 24-38.

Knieps, G. (2015), Entrepreneurial traffic management and the Internet Engineering Task Force, Journal of Competition Law & Economics, 11(3), 727-745.

Knieps, G. (2017a), Internet of Things and the Economics of Microgrids, in: F. Sioshansi (Ed.), Innovation and Disruption at the Grid`s Edge, Amsterdam et al.: Academic Press/Elsevier, 241-258.

Knieps, G. (2017b), Internet of Things and the economics of smart sustainable cities, Competition and Regulation in Network Industries, 18(1-2), 115-131.

Knieps, G. (2017c), Internet of Things, future networks and the economics of virtual networks, Competition and Regulation in Network Industries, 18 (3-4), 240-255.

Knieps, G. (2018a), Network Economics of Shared Mobility, Network Industries Quarterly, 20(3), September, 9-12.

Knieps, G. (2018b), Internet of Things, big data and the economics of networked vehicles, Telecommunications Policy, https://doi.org/10.1016/j.telpol.2018.09.002

Knieps, G., & Bauer, J.M. (2016), The Industrial organization of the Internet, in J.M. Bauer & M. Latzer (Eds.), Handbook on the Economics of the Internet, Cheltenham et al.: Edward Elgar, 23-54.

Knieps, G., & Stocker, V. (2016), Price and QoS differentiation in all-IP networks, International Journal of Management and Network Economics, 3(4), 317-335.

Knieps, G., & Zenhäusern, P. (2015), Broadband network evolution and path dependency, Competition and Regulation in Network Industries, 16(4), 335-353.

Kushalnagar, N, Montenegro, G. & Schumacher, C. (2007), IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals, RFC 4919.

Montenegro, G., Kushalnagar, N., Hui, J., & Culler, D. (2007), Transmission of IPv6 Packets over IEEE 802.15.4. Networks, RFC 4944.

OECD (2012), Machine-to-Machine Communications: Connecting Billions of Devices, OECD Digital Economy Papers, No. 230, OECD Publishing, http://dx.doi.org/10.1787/5k9gsh2gp043-en.

OECD (2013a), Building Blocks for Smart Networks, OECD Digital Economy Papers, No. 215, OECD Publishing, http://dx.doi.org/10.1787/5k4dkhvnzv35-en.

OECD (2013b), The App Economy, OECD Digital Economy Papers, No. 230, OECD Publishing, http://dx.doi.org/10.1787/5k3ttftlv95k-en

Stojmenovic, I., & Wen, S. (2014), The Fog Computing Paradigm: Scenarios and Security Issues, Proceedings of the 2014 Federated Conference on Computer Science and Information Systems, IEEE, ACSIS, Vol. 2, DOI: 10.15439/2014F503, 1-8.

Tanenbaum, A.S, & Wetherall, D.J. (2011), Computer Networks, 5th ed., Boston et al.: Prentice Hall.