Virtual Energy Information Network: A Resilience Perspective

Andreas Berl*, Michael Niedermeier*, Andreas Fischer*, Hermann de Meer*, David Hutchison†

*University of Passau, Innstr. 43, 94032 Passau, Germany
{andreas.berl, michael.niedermeier, andreas.fischer, hermann.demeer}@uni-passau.de

†School of Computing and Communication Systems, Lancaster University, Lancaster, LA1 4WA, United Kingdom
d.hutchison@lancaster.ac.uk

Abstract

Increasing demand in energy consumption, missed modernisations, and the increasing difficulties in predicting power production due to volatile renewable energy sources (e.g., based on wind or sun) impose major challenges to the power grid. Power supply and power demand are closely interconnected with the need to maintain the power grid in a stable state while a sufficient quality of power. This requires energy-relevant information to be exchanged through the so called Energy Information Network. Communication, however, is challenging within the Energy Information Network due to privacy, security, resiliency, and quality-of-service requirements. Particularly, the resilience of communication within the Energy Information Network needs to be considered to maintain the power grid in a stable and controlled state. This paper suggests a Virtualised Energy Information Network (VEIN), where the Energy Information Network is divided into multiple virtual networks that run over a common substrate network. Furthermore, this paper discusses benefits of this approach in terms of privacy, security, and resilience and points out open research questions.

1. Introduction

The Smart Grid[1] faces big challenges, such as achieving energy efficiency, integrating decentralised power generation based on renewable power sources, reducing CO_2 emissions, or decreasing the proportion of nuclear power production, while the worldwide energy consumption is still steadily increasing [2]. Power supply needs to match power demand very closely at all times to maintain a high level of power quality and to keep the power grid[2] in a stable state. Power needs to be delivered free of disruptions or disturbances, so that voltage, current, and frequency do not cause failure or mis-operation of end-user's equipment [4]. Losses of up to 24 billion dollars per year [5] have been caused by insufficient power quality in the USA in recent years. Instabilities of the power grid can lead to blackouts, causing high economic, ecological, and social costs.

To cope with these challenges, a fine-granular monitoring of energy consumption, distributed energy production, and the current state of the power grid needs to be established. To achieve this, the Smart Grid uses an Information and Communication Technology (ICT) based infrastructure to collect, analyse, and process energy-related data. This ICT-based communication infrastructure is called *"Energy Information Network"* in this paper. The Energy Information Network is based on various access technologies (e.g, powerline, mobile communication, or fiber) and provides the required interconnection between metering, accounting, production, transport, and distribution of power. The interconnection of grid technology and ICT, however, leads to new security challenges and adds an additional layer

[1] "The term 'Smart Grid' refers to a modernization of the electricity delivery system so it monitors, protects and automatically optimizes the operation of its interconnected elements – from the central and distributed generator through the high-voltage transmission network and the distribution system, to industrial users and building automation systems, to energy storage installations and to end-use consumers and their thermostats, electric vehicles, appliances and other household devices. The Smart Grid will be characterized by a two-way flow of electricity and information to create an automated, widely distributed energy delivery network. It incorporates into the grid the benefits of distributed computing and communications to deliver real-time information and enable the near-instantaneous balance of supply and demand at the device level." [1]

[2] "An electrical grid is an interconnected network for delivering electricity from suppliers to consumers. It consists of generating stations that produce electrical power, high-voltage transmission lines that carry power from distant sources to demand centers, and distribution lines that connect individual customers." [3]

of technology that can potentially be attacked, malfunction, and eventually fail. The power grid, which was typically isolated from other networks in the past, will get directly or indirectly connected to public networks, such as the Internet, opening it for IT-based attacks [6] and privacy issues [7].

This paper considers security, privacy, and resilience within Energy Information Network and suggests a *Virtualised Energy Information Network (VEIN)* that is based on network virtualisation technologies. On one hand, network virtualisation allows the embedding of the Energy Information Network into already available networks (both private and public) while still providing security. The embedded network is completely separated from traffic that is running over other networks. On the other hand, the virtualisation is able to provide additional resilience to the Energy Information Network: network resources can be dynamically allocated or modified if required, virtual network elements can be migrated to other physical locations to overcome disturbances of the network, and different access technologies can be combined to aggregated virtual links to achieve fault tolerance.

The remainder of this paper is structured as follows: Section 2 introduces the Energy Information Network of the Smart Grid and discusses its challenges in detail. Section 3 describes VEIN, a network virtualisation-based communication approach. Section 4 discusses open research questions, Section 5 elaborates on related work, and Section 6 concludes the paper.

2. Energy Information Network: Data Exchange and Arising Challenges

The Energy Information Network is needed to support the supply of high quality power without disruptions in the future. This infrastructure enables energy providers, particularly in the distribution network, to better monitor and regulate the power grid. To do so, large amounts of sensitive data need to be exchanged between the power grid's participants. Such data flows have, depending on their origin, target, and content, very different properties and requirements. The following list names some household-related examples with varying requirements:

- **Monitoring:** Power consumption and distributed power generation (e.g., power produced by photovoltaic cells) is monitored in fine granular time intervals by smart meters. On one hand, this data is very useful for energy providers to gain insight in power distribution and consumption processes and for detecting problems in the power grid. On the other hand, this kind of data potentially reveals private information (e.g., user behaviour in households) and needs to be secured.

- **Billing:** Energy consumption and distributed energy generation is monitored for billing purposes (typically with longer time intervals than for grid monitoring). This data, which is usually sent to a billing company once a month, has strong integrity requirements, besides being privacy-relevant.

- **Energy management:** Some devices in households are controllable with respect to the current availability of power in the grid (demand-response management), e.g., heating or air-conditioning. Also the remote activation and deactivation of power supply for households should be possible in the future (e.g., if new tenants move in a house). Signaling information for energy management is crucial for the grid's stability. It needs to have high integrity and often has Quality-of-Service (QoS) constraints.

Technologies used to exchange information in the Energy Information Network are a widely discussed topic. The data transfer within the household (between smart appliances, smart meters, and the gateway) can be achieved using ZigBee, Ethernet, WLAN or Bluetooth for instance. It is important to see that the communication between those devices needs to be resilient, as it can be interrupted due to interferences or due to manipulations of users (e.g., to steal energy). For this paper, however, mainly access technologies suited for the communication between households and energy providers are of concern. The gateway gathers information of smart meters and smart appliances and is responsible for the communication between household and other Smart Grid participants (e.g., the energy distributor). It is not yet quite clear, where the gateway will be located in the Smart Grid. Location possibilities are, e.g., within the smart meter, as a separate device at the power consumer, or within the transformer that distributes power to consumers. The gateway may also act as energy management system for home automation, or even be a multi-utility gateway, responsible for water and gas metering. Possible communication technologies to cover the path from household to energy provider are, e.g, powerline, UMTS, fiber optics, or DSL. The most suited access technology still is not finally agreed upon and has to be evaluated based on several factors, such as the associated costs, the available bandwidth, delay, and availability of the transmission link [8].

Particularly, the use of a public network for transmitting energy-related data is a highly interesting approach. Households are typically connected to the Internet, while other alternative communication paths (as dedicated fiber cables) may often not be available. If Smart Grid communication is running over a public network, several challenges arise. Energy-related communication streams have strong and varying requirements in terms of privacy, security, resilience, and QoS within the Energy Information Network. Security-relevant or privacy-infringing information should not be distributed openly over insecure links. Instead, this kind of data needs to be kept confidential, e.g. via encryption or anonymization. Energy management information (controlling power consumption or production) is time-critical. Decentralised power generation, for instance, has to be rapidly down-regulated to maintain a stable grid condition, if there is a power surplus in the grid. The Internet, however, relies on a ”best effort” service strategy, being not able to guarantee maximum delay properties. Finally, resilience is a major issue of the Energy Information Network. Energy-related data needs to be transmitted in spite of disturbance or interference, e.g., during critical situations in the power grid (e.g., localised blackouts).

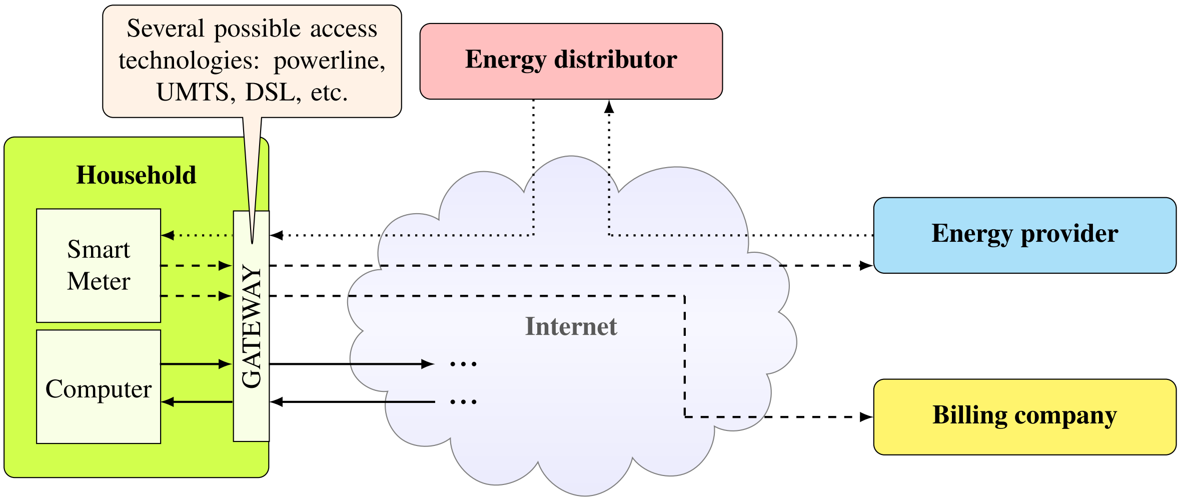

Figure 1: Currently proposed data exchange in the Energy Information Network

Figure 1 illustrates several logical communication paths of the Energy Information Network over the Internet. This example encompasses households, the energy provider, an energy distributor, and a billing company. Transmissions of monitored energy consumption/production data are illustrated as *dashed lines*. Transmissions of energy management data which are used, e.g., to signal smart meters or field devices (such as power substations, distribution automation, or condition monitoring) are illustrated as *dotted lines*. Transmissions of non-power grid related data, such as common Internet network traffic are illustrated as *solid lines*. If the Smart Grid communication is done using the Internet as medium, the gateway is most likely a generic cable or DSL router without any QoS guarantees. In the example of Figure 1, all traffic is sent though the Internet. The illustrated gateway sends privacy-, security-, and resiliency-critical energy-related data together with other common Internet traffic, leading to the challenges that have been discussed in this section.

3. VEIN - Virtualised Energy Information Network

Network virtualisation offers a promising approach to deal with challenges that were discussed in Section 2. This section discusses how network virtualisation can be applied to increase communication privacy, security, and resilience in the Smart Grid by introducing VEIN, a Virtualised Energy Information Network.

3.1. Network Virtualisation Concepts

Network virtualisation is the approach of setting up various virtualised networks on top of a common substrate network [9]. The virtualised networks are separated from each other and each of the networks has its own set of network resources. Virtual networks can be used to provide an abstract way of communication, regardless of the physical underlay that is actually used. In particular, a communication channel can be initialised with specific properties, such as QoS or security. This is done by appropriately combining and/or partitioning network resources. Network resources in this context are network nodes and the links that interconnect them. These are virtualised in order to get virtual nodes and virtual links. Multiple virtual nodes can be running on a single substrate node. Virtual links can be a combination of substrate resources, where a single virtual link is comprised of several substrate links. This partition and combination of resources can be used to increase communication resilience. Virtual nodes, e.g., can be migrated to counter the effects of faulty substrate nodes [10]. Virtual links, e.g, can combine multiple substrate paths to provide fallback resources in case a single substrate path fails.

3.2. Virtualising the Energy Information Network

The concept of network virtualisation can be used to run the Energy Information Network over public infrastructure. Virtual networks can be created on demand and will cater to the requirements of the data connections, as explained in Section 2. Virtualisation can provide a means to combine the various characteristics of different communication technologies to increase overall resilience. In particular, the flexibility of virtualised network resources can be used for dynamic remediation [10] in case of upcoming challenges. Also, network virtualisation can provide automatic management techniques, which can adjust the properties of a virtual link according to the needs of the communication partners. In detail, the usage of VEIN would achieve three important goals simultaneously:

1. **Readily usable technology:** Public networks (e.g., the Internet) can be utilised to build up / extend the Energy Information Network. The Internet provides a specific kind of resilience: Big parts of the Internet's infrastructure can fail without leading to a complete failure of the Internet [11]. Internet packets are re-routed through the remaining infrastructure. Although, as the Energy Information Network is co-located with other Internet traffic, network virtualisation can provide a clear separation between different kinds of virtual networks.
2. **Fail-over mechanisms:** Network virtualisation is able to provide a higher level of resilience in terms of fault tolerance to the Energy Information Network. Links can be aggregated to virtual links, comprising different access and transmission technologies.
3. **Fine-grained confidentiality:** Network virtualisation can be used to set up dedicated encrypted virtual links on demand between any two communication partners. This is an important tool to support the specific confidentiality and privacy needs of energy metering information. Moreover, by adjusting security appropriately, public infrastructures can be used as a fall-back communication facility in case more trustworthy equipment fails.

A VEIN example is depicted in Figure 2, where two virtual networks have been set up. Both virtual networks are used for the transmission of energy-related data and are embedded in a public substrate network. *"Virtual network 1"* is used to transmit monitoring and billing data of the household. In this virtual network, privacy and the integrity of data is of major concern, therefore, the virtual links that are used in this network should provide data encryption and authentication. *"Virtual network 2"* is used to transmit energy management data in this example. This data has high resilience and QoS requirements, in addition to integrity and security. Resilience and QoS requirements can be realised by setting up virtual links over highly reliable substrate links. Several redundant communication channels may be combined to virtual links to further increase resilience.

4. Open Research Questions

Network virtualisation offers several advantages which can be highly beneficial in the context of Smart Grid communication. However, there are still multiple research questions that have to be answered before a wide-scale deployment of VEIN can be considered:

- Various communication streams are present in the Energy Information Network that have different individual requirements in terms of privacy, security, resiliency, and QoS. The following questions need to be answered: Who needs to transfer energy-related information to whom? What are concrete requirements of these communication streams? How can these requirements be modeled through virtual networks?

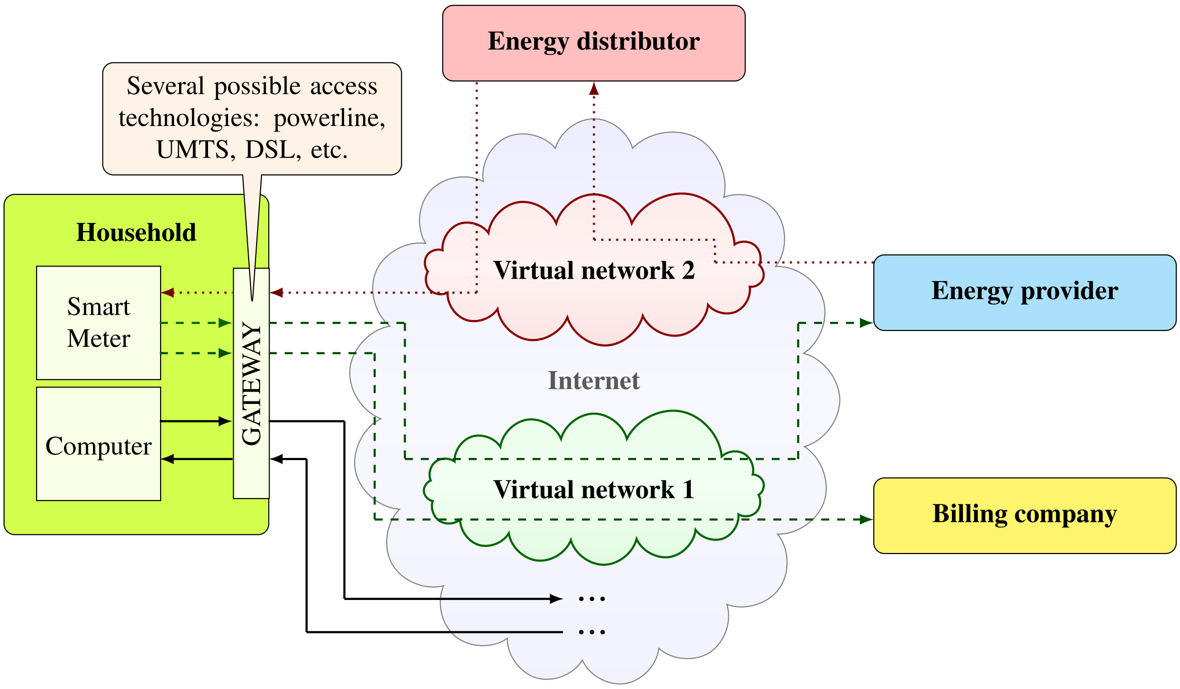

Figure 2: Data exchange in the Energy Information Network using VEIN

- Network virtualisation provides us with a set of useful methods that can be used to realise VEIN, such as the creation, duplication, or migration of network elements, the aggregation of physical links, or, more general, the embedding of virtual networks in physical networks. It needs to be investigated how these available methods can be used to support the (changing) requirements of the Energy Information Network.

- The aggregation of multiple access and transmission technologies within VEIN needs to be investigated. Multihoming and link aggregation are highly interesting topics to achieve resilience. Also, a possible sharing of access and transmission technologies (e.g., among physical neighbors) needs to be investigated.

- The impact of virtualisation on the functional safety of the overall Energy Information Network is an important factor that needs to be investigated. If several communication streams are running virtualised over a single physical hardware link, a failure of this link could severely impair the overall reliability. In this case, it is important to not only consider the normal operation of the grid, but also to consider critical situations, such as maintenance, brownouts, or blackouts and their effect on the Energy Information Network.

- Finally, VEIN introduces a virtualisation layer to the Energy Information Network, which adds complexity and new possible attack vectors. Implications of the virtualisation layer and the overhead of such a system need to be analysed in detail.

5. Related Work

Amin [12] describes the necessity for a self-healing, resilient smart grid with a particular focus on high-voltage networks. Claudia Eckert et. al [13], [14] describe the Smart Grid, its communication infrastructure and security challenges. They describe security architectures for the private customer and distribution network domain. Berl et. al [15] discuss current status, challenges, and future developments of the power grid. Particularly, the trade-off between energy efficiency and security is investigated with respect to control systems and smart metering. The Smart Grid is often described with properties as self-healing, highly reliable, optimised energy management, resilient to cyber attacks and real-time pricing [16]. Further general information on Smart Grid technologies and arising challenges can be found in [17], [18] and [19]. Smart Grid security related research covering privacy and security in smart meter environments are, for instance, analysed by [20] and [21], concluding that privacy enhancing technologies, such as anonymisation or data aggregation have to be applied. While the resistance to attacks should be one of the key characteristics of the Smart Grid, this goal is hardly achievable in a real-life implementation of a Smart Grid due to several reasons, which are addressed in [22], [23], or [24].

Network virtualisation has been discussed in the context of Future Internet approaches for some time now. Network virtualisation can be used to instantiate a number of different virtual networks on the same substrate network [25], [9]. Feasibility of this concept has been demonstrated already [26]. In terms of security, network virtualisation can be seen from two sides. On the one hand, it can be used to add security. For example, Davy et al. [27] discuss how secure virtual links can be set up dynamically between communicating parties. On the other hand, network virtualisation also has its own security problems, which have to be taken care of [28]. Marias et al. [29] discuss generic virtualisation problems in the Future Internet. Fischer and De Meer [30] point out potential security problems when planning virtual networks.

6. Conclusions

This paper has discussed privacy, security, and resiliency issues of the ICT-based Energy Information Network. VEIN, a network virtualisation based approach has been suggested, in which the Energy Information Network is composed of several separate virtual networks that are embedded in a common network substrate. Although energy related traffic is routed over the public Internet together with other traffic in this approach, VEIN is able to provide a secure separation between traffic flows. Additionally, VEIN is able to provide a high level of resilience in terms of fault tolerance, as it allows for a transparent aggregation of access and transmission technologies within virtual links. Finally, this paper has discussed open research questions that need to be worked on to realise a network virtualisation based Energy Information Network.

Acknowledgements

The research leading to these results was supported by EC's FP7 Network of Excellence EINS (grant no. 288021) – in particular JRA7 on resilience of critical infrastructures – and by "Regionale Wettbewerbsfähigkeit und Beschäftigung", Bayern, 2007–2013 (EFRE) as part of the SECBIT project.

References

[1] D. V. Dollen, Report to nist on the smart grid interoperability standards roadmap, Tech. rep., National Institute of Standards and Technology (NIST) (2009).

[2] A. Battaglini, J. Lilliestam, C. Bals, A. Haas, The supersmart grid, in: European Climate Forum, Potsdam Institute for Climate Impact Research, 2008.

[3] S. M. Kaplan, Electric power transmission: Background and policy issues, Tech. rep., Congressional Research Service (2009).

[4] B. Kennedy, Power quality primer, McGraw-Hill Professional, 2000.

[5] E. P. R. Institute, Estimating the cost and benefits of the smart grid, http://my.epri.com/portal/server.pt?Abstract_id=000000000001022519 (March 2011).

[6] N. Falliere, L. O. Murchu, E. Chien, W32.Stuxnet Dossier, Tech. rep., Symantec (2011).

[7] P. McDaniel, S. McLaughlin, Security and privacy challenges in the smart grid, IEEE Security and Privacy 7 (2009) 75–77.

[8] A. Yarali, S. Rahman, Smart grid networks: Promises and challenges., JCM 7 (6) (2012) 409–417.
URL http://dblp.uni-trier.de/db/journals/jcm/jcm7.html#YaraliR12

[9] N. M. K. Chowdhury, R. Boutaba, A survey of network virtualization, Computer Networks 54 (5) (2010) 862 – 876. doi:DOI:10.1016/j.comnet.2009.10.017.

[10] A. Fischer, A. Fessi, G. Carle, H. De Meer, Wide-area virtual machine migration as resilience mechanism, in: Proc. of the International Workshop on Network Resilience: From Research to Practice (WNR2011), IEEE, 2011, pp. 72–77. doi:10.1109/SRDSW.2011.16.

[11] M. Omer, R. Nilchiani, A. Mostashari, Measuring the resilience of the global internet infrastructure system, in: Systems Conference, 2009 3rd Annual IEEE, 2009, pp. 156–162. doi:10.1109/SYSTEMS.2009.4815790.

[12] M. Amin, Challenges in reliability, security, efficiency, and resilience of energy infrastructure: Toward smart self-healing electric power grid, in: Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE, July, pp. 1–5. doi:10.1109/PES.2008.4596791.

[13] C. Eckert, Sicherheit im Smart Grid – Eckpunkte für ein Energieinformationsnetz.

[14] C. Eckert, C. Krauss, Sicherheit im Smart Grid – Sicherheitsarchitekturen für die Domänen Privatkunde und Verteilnetz unter Berücksichtigung der Elektromobilität.

[15] A. Berl, M. Niedermeier, H. De Meer, Smart Grid Considerations- Energy Efficiency vs. Security, in: A. Hurson (Ed.), Green and Sustainable Computing: Part II, Vol. 88 of Advances in Computers, Elsevier B.V., 2013, pp. 159 –198. doi:10.1016/B978-0-12-407725-6.00004-6.

[16] R. E. Brown, Impact of Smart Grid on distribution system design, Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century, IEEE (2008) 1–4.

[17] S. M. Amin, B. F. Wollenberg, Toward a Smart Grid: power delivery for the 21st century, Power and Energy Magazine, IEEE 3 (5) (2005) 34–41.

[18] H. Farhangi, The path of the Smart Grid, Power and Energy Magazine, IEEE 8 (1) (2010) 18–28.

[19] J. En-Bo, Smart Meter System Design in Smart Grid Advanced Metering Infrastructure AMI, Tech. rep., Electrical Measurement & Instrumentation (2010).

[20] E. L. Quinn, Smart Metering and Privacy: Existing Laws and Competing Policies, Social Science Research NetworkHttp://ssrn.com/paper=1462285.

[21] A. Cavoukian, J. Polonetsky, C. Wolf, SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation, Whitepaper, http://www.futureofprivacy.org (2009).

[22] A. R. Metke, R. L. Ekl, Smart Grid Security Technology, Tech. rep., Motorola, Inc. (2010).

[23] W. F. Boyer, S. A. McBride, Study of Security Attributes of Smart Grid Systems – Current Cyber Security Issues, Tech. rep., Idaho National Laboratory, Critical Infrastructure Protection / Resilience Center (2009).

[24] A. Lee, T. Brewer, Smart Grid Cyber Security Strategy and Requirements, Tech. rep., The Cyber Security Coordination Task Group, Advanced Security Acceleration Project – Smart Grid (2009).

[25] N. Feamster, L. Gao, J. Rexford, How to lease the internet in your spare time, ACM SIGCOMM Computer Communication Review 37 (2007) 61–64.

[26] J. Rubio-Loyola, A. Astorga, J. Serrat, W. K. Chai, L. Mamatas, A. Galis, S. Clayman, A. Cheniour, L. Lefevre, O. Mornard, A. Fischer, A. Paler, H. De Meer, Platforms and Software Systems for an Autonomic Internet, in: Proc. of the IEEE Global Communications Conf. (IEEE GLOBECOM 2010), 2010.

[27] S. Davy, C. Fahy, L. Griffin, Z. Boudjemil, A. Berl, A. Fischer, H. de Meer, J. Strassner, Towards a policy-based autonomic virtual network to support differentiated security services, in: International Conference on Telecommunications and Multimedia (TEMU 2008), Ierapetra, Crete, Greece, 2008.

[28] J. Sahoo, S. Mohapatra, R. Lath, Virtualization: A survey on concepts, taxonomy and associated security issues, in: Computer and Network Technology (ICCNT), 2010 Second International Conference on, 2010, pp. 222–226. doi:10.1109/ICCNT.2010.49.

[29] G. F. Marias, J. Barros, M. Fiedler, A. Fischer, H. Hauff, R. Herkenhoener, A. Grillo, A. Lentini, L. Lima, C. Lorentzen, W. Mazurczyk, H. de Meer, P. F. Oliveira, G. C. Polyzos, E. Pujol, K. Szczypiorski, J. P. Vilela, T. T. V. Vinhoza, Security and privacy issues for the network of the future, Security and Communication Networks 5 (9) (2012) 987–1005. doi:10.1002/sec.384.

[30] A. Fischer, H. De Meer, Position paper: Secure virtual network embedding, Praxis der Informationsverarbeitung und Kommunikation 34 (4) (2011) 190–193. doi:10.1515/piko.2011.040.