Architecture for Delivery of Virtualized Network Functions

Tomáš Halagan[*]
Institute of Applied Informatics
Faculty of Informatics and Information Technologies
Slovak University of Technology in Bratislava
Ilkovičova 2, 842 16 Bratislava, Slovakia
tomas.halagan@stuba.sk

Abstract

The main aim of this dissertation is the creation of a new architecture that interconnects several domains. The network elements of these domains are controlled by Software Defined Networking technology (SDN), and these domains also contain virtualized network functions (NFV), so the term SDN/NFV domain is used in the work further. The SDN/NFV domain combines all the benefits that both technologies bring, creating a fully automated domain to deliver network functions in virtualized form. These SDN/NFV domains can be implemented in a different way. Currently there are existing solutions from Cisco, Juniper, HPE, IBM, Metaswitch and many others containing various SDN controllers, various other applications helping to manage the SDN/NFV domain. The result of the research is a new architecture for interconnection and transparent management of different SDN/NFV domains. The proposed solution has been successfully verified using the Petri Color Mathematical Modeling Tool.

Categories and Subject Descriptors

C.2.1 [**Computer communication networks**]: Network Architecture and Design—*Distributed Networks*; C.2.2 [**Computer communication networks**]: Network Protocols

Keywords

SDN, Software-defined Networking, NFV, Network Functions Virtualization, Network Architecture, Interconnect, NFV Federation

1. Introduction

Today's computer networks are undoubtedly one of the most widely used means of communication that has gained tremendous popularity among all layers of users. Through computer networks a widespread public Internet network is spreading. Internet allows to exchange of information between different autonomous systems all around the world.

Networks of Internet and Network Service Providers use established mechanisms that are the result of network standardization, and have only partially changed since their inception - negligible. Surveys unambiguously show the tendency of the huge growth of computer networks, also due to the huge number of connected devices around the world[5]. This trend requires ever higher demands on the networks and their provided features.

The work includes a description of two emerging technologies - Software-Defined Networks and Virtualization of Network Functions. These technologies offer many advantages that can benefit from not only Internet and Network Service Providers but also users themselves and basically our entire society of people. In spite of the huge research done by many subjects, very little work is focused on the use of programmability of networks to interconnect autonomous systems and the use of this programmable feature to provide applications and services in virtualized form. No significant research has been carried out in the field of data center integration, which can be done through these two technologies. The benefits of this interconnection are significant and need to be taken into account.

The aim of this dissertation is to create a universal architecture that can be deployed in different domains of Software-Defined Networks and Domains of Virtualized Network Functions, which can be arbitrarily combined. This concept makes it possible to take advantage of the already-known benefits that these technologies provide, as well as the benefits that are new and identified in this work. The work includes a description of two emerging technologies - Software-Defined Networks and Virtualization of Network Functions, offering many benefits that can benefit not only Internet and network service providers but also users themselves and basically our entire company of people. In spite of the huge research done by many subjects, very little work is focused on the use of programmability of networks to link autonomous systems and the use of this programmable feature to provide applications and services in virtualized form. No significant research has been carried out in the field of data center integration, which can be done through these two tech-

[*]Recommended by thesis supervisor: Assoc. Prof. Ivan Kotuliak
To be defended at Faculty of Informatics and Information Technologies, Slovak University of Technology in Bratislava, 2017.

nologies. The benefits of this connection are considerable and need to be taken into account.

2. General Issues of Computer Networks

Today's times could be characterized as times of informatics and information technologies, computers, computer networks. By 2015, around 5 billion people will be connected to the global public Internet network, more than 4 billion people will use network services through mobile devices, and more than 2 billion people will use broadband fixed Internet connections. Claus G. Gruber[5] has the following assumptions as well as the assumption that network traffic will have a growth rate in the coming years from 40% to 200% compared to today's network traffic. For this reason, it is relevant to evaluate the state of the current computer networks and other elements that are an integral part of it. Internet expansion has promoted and accelerated the use of mobile devices such as laptops, mobile phones, tablets. Mobile users' requirements are many times more demanding than those of users with fixed network connections, especially when it comes to accessibility at any time, anywhere[13]. For that reason, today's networks must be adaptable and agile, providing not only high service availability but also their quality.

One of the most successful models of today's networks is the Open System Interconnection (OSI)[3] architecture that allows the network to be layered - split into layers. The modularity that has been achieved by this layering leads to a better understanding of the entire system of networks. Repeated use of the same lower layers for applications and services reduces their development costs. Layering simplifies network design but leads to the creation of a large number of robust scalable protocols on the Internet. However, multi-layer network diversification suffers from the lack of flexibility and sup-optimality that is caused by the impossibility of exchanging information between layers as shown in the work [14]. Reducing this complexity is especially important for researchers who require real-world networking tests and experiments, for revolutionary ideas, innovative ideas and improvements.

At present, there is practically no way to experiment with new network protocols, device settings to the extent that this experiment gains credibility for broad deployment in Internet Service Provider (ISP) networks and Network Service Provider (NSP) networks). For the sake of clarity - Internet service providers are particularly interested in internet access, internet traffic, domain name registration, ”Web hosting”, usenet discussion system. Network service providers are essentially business entities that provide or sell services such as network access and bandwidth by accessing part of their infrastructure or accessing the network access point. Quite often, network service providers are considered to be Internet service providers, but in principle they are the ones who provide access to backbone networks and services.

Authors at [10] confirm that a huge number of networking devices already deployed uses the same network infrastructure with the same network protocols being used for decades are a huge barrier to the entry of innovative solutions, development and research into computer networks. As a result of this common approach, the fact that many new ideas from the research community are untested, unverified, unpracticed.

It is important to note that the Internet project has been built for research. However, architects building an Internet infrastructure did not realize the possibility of coming to the giant networks we have today. Security, mobility, network flexibility has never been solved, as in the time of Internet formalization the computers were not mobile and the researchers wanted to unceremoniously spread new ideas through open environments. The vision of the perfect Internet environment has begun to disappear with an ever-increasing number of network users. A number of basic concepts have not changed since their creation. With the rapid development of information technology, the public Internet computer network is unable to meet emerging requirements. Obviously, today's networks need a new proposal that is better suited to new trends.

The following chapters will outline the general issues facing today's networks of Internet Service Providers and Network Service Providers as well as two current technologies to address these general issues in more detailed contours.

2.1 Costs of the Computer Networks

The operation and maintenance of computer networks, since their very creation, requires a large amount of costs that can generally be broken down as follows:

- Investment so-called CAPEX - Capital expenses, these are costs of a one-off nature, that must be spent on purchasing a certain material, tangible, intangible and financial assets, which includes[2]:
  - Technical resources, hardware by type of resources (servers, end stations, routers, cable distributions, etc.)
  - Software, i.e. License fees and updates
  - Individual applications and other software resources
  - Buildings and workplaces for new procurement and not for rent
- Non-investment so-called Operating, OPEX - Operative expenses, costs continuously to be spent on the management, operation, maintenance and development of resources, also includes the costs associated with the collection of certain services, namely:
  - Purchased services - application and infrastructure services, communication services, consulting services, customization, implementation, integration, prophylaxis
  - Post-warranty service, training, help desk, marketing
  - Personal expenses - wages, qualification increases, insurance
  - Buildings and workplaces if it is a rental
  - Consumables
  - Other and overhead costs - travel, interpretation.

There are countless small, larger or fatal problems with network devices that are dedicated to a specific function[12]. These problems, on the one hand, reduce their guaranteed service life and operation and, on the other hand, these devices require a huge amount of interventions, repairs, maintenance that must be carried out by administrators or service technicians - these operations are related to operating costs, ie OPEX. - ————————

2.2 Operational Complexity

In the work *Managing Complexity of Information Systems The value of simplicity* [7], the authors outlined the fact that the heterogeneous environment of information systems is growing. Employees of companies, and especially end-users, often work in heterogeneous environments, using different technologies, programming languages, business applications, and operating systems. Because of this situation, operational complexity is considerable. That's why the Internet service providers, network service providers, as well as other key organizations and businesses perceive this high complexity as one of the most important problems of the present.

Operational complexity concerns in particular all sales units, called stock keeping unit (SKU), which NSPs and ISPs provide. As part of the provision of this unit, it is also the warranty period for which this unit needs to be maintained, repaired, and thus the operating costs incurred[11]. Direct pride goes with the more diverse SKUs, the more complex the salesperson or the provider has to make. For this reason, the operational complexity is the highest in telco telecommunications operators, as the occurrence of multiple SKUs is in those networks in the order of thousands.

3. New Approaches in Computer Networks

Looking at the above-mentioned problems, it is necessary to think about an innovative approach to networks, in the best case to realize a change in the basic architecture of the networks. In the following sections the new approaches in computer networks will be described.

3.1 Software-defined Networking

The basic idea of SDN networks, and at the same time the biggest benefit, is the separation of the network structure and the network configuration in the way that the management and management functionality is located in the central control element in the issue called SDN Controller. This separation of the control and data network allows for more flexible and flexible network management.

SDN technology enables innovation in the network design and management. This innovative network approach has been brought to the community's awareness just a few years ago and since then, SDN technology has been the number one topic for computer systems and networks.

The sketch of the basic architecture of SDN technology shows the figure 1, where it is possible to distinguish between three layers of SDN technology similarly to the works [6], [8]:

- Application plane - This layer includes all the applications and services that are needed to program the network topology. Apps can meet various logical features such as securing consistent policies, securing the configuration of specific network devices for seamless delivery and service delivery, routing computing applications based on network line parameters, and so on.

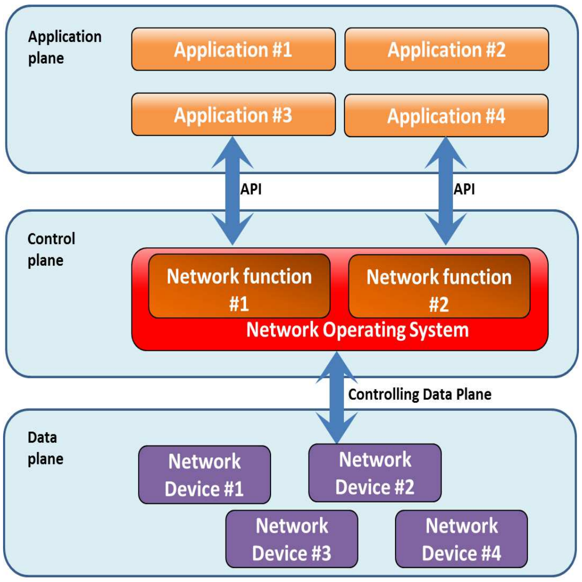

Figure 1: Basic architecture of SDN technology.

- Control plane - Replaces the basic decision logic that each network device previously had. Through the control layer, it is possible to centrally manage the switching, routing and configuration of all devices in the network.
- Data plane - Contains hardware network devices that have basic packet recognition capabilities according to flows and their transmission based on instructions contained in the flow table. If an unknown packet is delivered to the machine, it will be sent to the control unit and decides where the packet will popup or discard. The control unit can also complete the flow tables of the network devices in question so that the packet can be transferred to the target by the correct network path.

This paper contains only basic information about SDN. Further information e.g. about OpenFlow protocol being used in the SDN networks and SDN history may be found in [1], [9].

3.2 Network Functions Virtualization

Telco operator networks, Internet or network service providers networks contain a number of proprietary hardware devices, and have caused the above described general network problems in computer networks. There are CAPEX, OPEX problems, operational and time complexity for deploying and maintaining new or existing network services. The emerging network virtualization technology, widely named as Network Functions Virtualization (NFV) aims to address these issues.

The European and American continent has announced the emergence of a new Industrial Specification Group (ISG) under the auspices of the European Telecommunication Standards Institute (ETSI), a global leader in the development of standards for information and communication technologies, such as Information and Communication Technologies ICT). It is this specification that deals with the standardization of NFV technology.

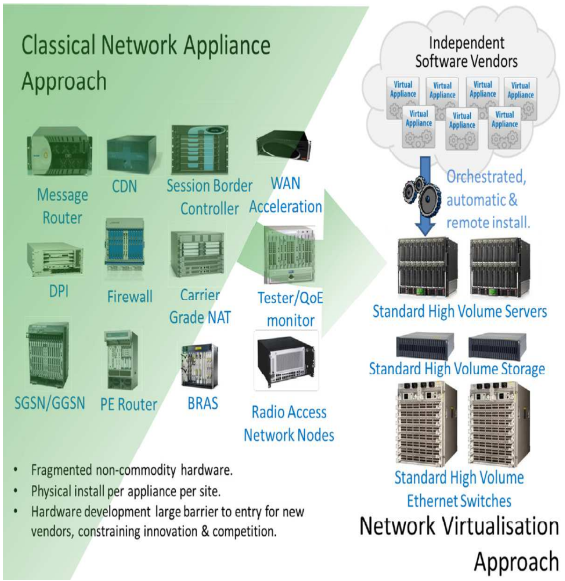
Classical Network Appliance Approach
Message Router
CDN
Session Border Controller
WAN Acceleration
DPI
Firewall
Carrier Grade NAT
Tester/QoE monitor
SGSN/GGSN
PE Router
BRAS
Radio Access Network Nodes
• Fragmented non-commodity hardware.
• Physical install per appliance per site.
• Hardware development large barrier to entry for new vendors, constraining innovation & competition.
Independent Software Vendors
Virtual Appliance
Orchestrated, automatic & remote install.
Standard High Volume Servers
Standard High Volume Storage
Standard High Volume Ethernet Switches
Network Virtualisation Approach

Figure 2: NFV technology in nutshell[4]

The nascent idea of the NFV technology shown in the figure 2 is to virtualize a number of network devices of different types and place them on industry standardized servers located in data centers.[4].

3.3 Evaluation of Current State of the Art

Current research and development in the area of SDN technology is predominantly centered on one network that contains one central element - the SDN control unit, which is dedicated to network management. This network achieves elasticity and flexibility, thanks to simple programmability. This important feature of SDN networks uses applications that communicate directly through the northern interface with the SDN control unit. All this miracle takes place on a single network that communicates directly with the public network infrastructure. In other words, SDN networks lack an idea that could fully exploit the basic feature of programmability from another network.

The same research and development is being implemented in the field of NFV technology to provide networked functions in virtualized form, to connect them, as well as to all the orchestration and management of these virtualized network functions. All this effort is focused on the independent development of the NFV domain that is self-sufficient.

We can talk about a number of subjects that are affected by SDN and NFV. With regard to SDN networks, network service providers (NSPs) and Internet (ISP) services, telco network operators, as well as other major corporate network solution companies are currently involved. Software-controlled networks find their way in the home, small or bigger companies, companies, datacenters and telecom operators for their directness and simplicity. As far as NFV networks are concerned, the telecom operators' networks for which the technology is standardized and deployed are most affected, as well as all other virtualized services provided. In summary, SDN and NFV technology is very hot topic not only discussed but also considered as future concept of all computer networks.

The field research demonstrates the complementarity of SDN and NFV technologies. SDN technology provides a unique feature of network programmability, NFV technology provides a unique virtualization capability for network services. Identified problems are the combination of these two properties, the combination of two SDN and NFV technologies. The NFV domain will provide orchestration and management of virtualized services, complex service maintenance, but a solution for automated use of a virtualized service, and does not provide proper customer network setup.

4. Thesis Objectives

This section provides a definition of the thesis objectives that the work is focusing on, and a basic sketch of the design for their solution.

The vision is to enable automated provision of virtualized network services to end-customers who are part of a network managed by SDN technology. In order to achieve a fully-fledged provision of virtualized network service to a customer, SDN and NFV domain collaboration is needed. This results in the problems described in the subchapters below.

4.1 Proposal of the SDN and NFV Domain Interconnection Architecture

- **Objective No.1 - Specification of the NFVi control unit functions** In this case, it is an NFV control unit that has the ability to communicate with another NFV control unit located in a remote domain. These units are labeled with the letter "i", in a matter called "interconnect" or linking. First of all, it is necessary to answer the question whether it is possible to use the currently designed and functioning SDN control units for the purposes of the NFVi control unit, or it is necessary to specify and design a new NFVi control unit. Currently, there is no control unit that would manage the administration and orchestration of virtualized network services beyond the logical network domain - domain. It is important that this controller can handle SDN devices. It is assumed that the logical network connections between virtualized network services will be implemented through SDN technology and thus the SDN control unit. This idea strengthens me and aims to extend the SDN of the controller to the functionality necessary for the administration and orchestration of virtualized network functions.

- **Objective No.2 Interconnect between multiple NFVi control units** The communication between NFVi control units can be understood as communication between two SDN controllers. In the present state of the art, there is no way to communicate in a standardized format between SDN control units. It is important for this communication to ensure that the SDN communications (SDN forwarder) switches are set up correctly to ensure the availability of virtualized network functionality.

- **Objective No.3 Proposal of a Data Model**

Protocol and Management Messages for Proper Communication between SDN - NFV Domains
In the current state of the art, there is no standard for communication between the SDN and the NFV domain. The concept of communication between these domains was not designed by anyone. ETSI seeks to enforce orchestration and virtual network management in its architecture - in a domain that is further subdivided into individual subdomains for the needs of virtualization itself and its maintenance. However, there is no sketched and mentioned linking of an SDN domain with an NFV domain. For this reason, it is necessary to design management reports that will serve to communicate and exchange information between SDN and NFV domains. A further specification of these messages will be included in the proposal.

4.2 Proposal of Interconnecting SDN/NFV Domains

An important aspect for interconnecting the SDN/NFV domains is in particular the reliability of the link. This is meant to resume interconnection in the event of a random incident, which may be, for example:

- Network issues - packet discards due to reduced network quality through which a connection is made - packet outages
- Software and Hardware Issues - Dropouts and Interface Disorders

The solution to the problem should cover these basic most frequently occurring situations and re-interconnect automatically after the failure.

- **Problem No.4 Proposal of architecture for creating the interconnection between two and more SDN/NFV Domains**
  Interconnecting multiple SDN/NFV domains may be important in terms of expanding available resources as well as a way to avoid a single failure point in data centers. It can be assumed that the service provider will operate multiple data centers. It is for this reason that the service provider will require the connection of these data centers in order to allow the exchange of important information between the data centers.
  Attractive is the idea of consolidating financial resources to build infrastructure in places where a particular user either does not have a deployed network technology with sufficient network and computing parameters or simply does not have it at all in that location. In this case, it is possible to establish a link between two independent entities on the basis of a predetermined contract - an agreement on the conditions for the provision, sharing or lending of existing infrastructure. If such agreement is to be established, it is important to be able to specify what will be the subject of providing infrastructure not only on paper but also in practice - ideally as automated as possible without the administrator's intervention, in the less ideal case, reduce the time needed to establish domain and deployment of customer service. The consolidation of funds may also involve the migration of such network services where the risk or threat of leakage of sensitive data has not been identified. For a better idea, for example, a public cloud, which has a significantly lower cost of running network services as a dedicated cloud with precisely set parameters and service protection, can serve. Of course, this idea is only relevant if its application is possible, ie in the case of the aforementioned network services, where there is no risk of leakage of sensitive data.

- **Problem No.5 Proposal of continuous operation - providing virtualized network functions**
  It is important to say that the correct identification and selection of the infrastructure can lead to a reduction in a downtime and increase in the availability of services and thus to the observance of the service level agreement (SLA). For software products, in case of SDN and NFV we can definitely talk about, it is important to create real-time software backups to identify when and under what circumstances the system should be restored. The SDN, NFV, or NFVi controllers are software products that can run on secure infrastructure, and this infrastructure may protect them in certain degree against their downtime. Of course, only a layer of infrastructure is protected, not a software layer, where a huge amount of potential threats are opened - software error, reduced functionality due to the dropout of a particular communicating module, a configuration error that did not occur immediately, an unexpected outage caused by inconsistent treatment of all possible scenarios. In the field of software products, there are already some mechanisms that address service failure, but to provide virtualized network services, it is necessary to define and implement such algorithm, a system, a model that guarantees a loss-free operation, or a drop in the character unnoticed - within a few seconds. This issue has not yet been addressed in SDN networks.

5. Proposal of Architecture for Delivery of Virtualized Network Functions

Due to complexity of the individual problems formulated, this dissertation thesis is strictly focused on the proposal of the architecture for the interconnection of several SDN/NFV domains.

The proposed architecture consists of two domains that are hierarchically separated and have their own distinctive function in architecture, and are as follows:

- Core Domain Management (CMD) - This Domain serves solely to manage the connections created between SDN/NFV domains. Within this domain, there are specified messages to establish, maintain, or terminate the link.
- SDN / NFV Domain (SND) - This domain has the virtualized network functions itself and therefore does not only exchange management messages with the Core Management Domain, but also exchange data among other SND domains that have been interconnected through the Core Management domain.

Controlling messages exchanged between domains of different or the same hierarchy are defined in the INT protocol, whose design and specification is incorporated in this dissertation works as well. Architecture proposal respects existing SDN or SDN domains where virtualized network features are deployed. In both types of domains has an SDN controller that serves for proper routing - setting up a network path, or setting forwarders. Above the SDN controller there is an NFVi controller that directly communicates with both the SDN controller across the northbound interface and with the other NFVi controller via the East-West interface. It is important to say that this communication is going through INT module, which includes various drivers for transparent communication with different SDN/NFV domains. Various SDN/NFV domains are in this assumption domains that have been designed - implemented by using various techniques supporting different types of communication for the internal purposes of a specific domain. In principle, it can be domains implemented by various key companies such as Juniper, HPE, Cisco, IBM, a domain that today can not communicate with each other. A precondition for successful communication is the driver that should be developed by the company that created / made the domain for coverage of all features and proper support. INT module will therefore be a modular system that will support drivers as plug-ins. Based on the domain identification, a suitable driver will be used that will correctly support all features of the domain. In this way, it is virtually possible to link any SDN/NFV domain implemented over any infrastructure, or even devices directly designed for the delivery of virtualized network services.

5.1 Core Management Domain

As mentioned above, due to the complexity of the solution, the newly created architecture consists of two hierarchically different domains. The Core Management Domain is hierarchically superior, and serves to access, create, manage, and interrupt SDN/NFV domain connections as well as CMD domains.

NFV Management is a feature present only in the CMD domain and serves all customers, administrators, and other legitimate users to access the management of either one or more SDN/NFV domains. The domain linking options are as follows:

- CMD <-> CMD - Interconnecting hierarchically and organizationally identical CMDs in order to achieve high availability or interconnection of hierarchically identical, but organically distinct CMD domains - such as interconnecting domains of different companies and creating an SDN/NFV federation
- CMD <-> SND - linking hierarchically different domains to interconnect multiple SND domains in an organization. To interconnect the SND domains of different providers, firstly the CMD domains interconnection has to be made.

5.2 SDN/NFV Domain

The proposed architecture respects the existing SDN topologies as well as the already implemented NFV solution - in this case we are talking about the SDN/NFV domain. Such domain may already include an SDN controller for controlling and changing network topology, a NFV orchestration for the management and orchestration of virtualized network services. For the correct creation of interconnections between domains, it is necessary to incorporate the NFVi controller as described above. Just thanks to this component, it's possible to enable transparent communication and profit from the benefits that this interconnection offers.

6. Verfication of Proposed Architecture

Since the architecture of the proposed solution is complicated and the design itself requires multi-entity collaboration, the Petri Network, namely the Color Petri Network, was designed to verify the solution. This type of network belongs to high-level networks offering much wider system modeling, processes and features. An important fact is that it is in the Color Petri Network that it is possible to model data types, work with data, model functions, and integrate their calculations into network states. The undoubted advantage of such networks is the better clarity, the visibility of individual token types, which can be distinguished by colors. An example may be the sending and receiving of packets, where each location, transition, edge, function, mark is indicated by a specific color.

Other network specifics are described in the following subsections.

6.1 The color scale of proposed Coloured Petri Network

As mentioned above, the individual parts of the proposed Petri Color Network are marked with colors as follows:

- All processes related to the transmission, generation and receipt of the packet are marked in red. The RECEIVE_HELLO function is also marked with this color that processes the received packet.
- The state of the physical interface and its associated processes are marked with a purple color. This status is important for the entire network that switches to clean mode in the event of an interface failure, so the link reboots and creates a resume.
- The NFV database records and the associated processes are marked in green. WRITE_TO_NFV_DB is also marked with this color through which the entire write to the database is controlled.
- When two CMDs are interconnected to high availability, the processes for maintaining a backup domain are activated in blue. In this case, the backup algorithm provides a backup domain that can operate in full mode operation
- The processes related to the IP address setting on the INT module are marked with a brown color.
- For proper operation of the proposed network, it is necessary to maintain auxiliary variables such as the number of neighboring domains, temporary memory for storing the resulting link, and the like.

7. Conclusions

In assessing the fulfillment of objectives I would like to highlight the following for each individual thesis objective:

- **Specification of the NFVi control unit functions** - in the work, the NFVi functions of the control unit are specified. The functionality and reliability of the NFVi unit has been verified in the proposed Petri Color Network.

- **Interconnect between multiple NFVi control units** - In the proposed architecture, the Core Management Domain was specified in the proposed architecture. Functionality and reliability of Core Domain Management has been verified in the proposed Petri Color Network.

- **Proposal of a Data Model Protocol and Management for Proper Communication between SDN - NFV Domains** - dissertation thesis describes comprehensive INT protocol that defines simple management messages for the proper establishment and maintenance of interconnection of multiple SDN - NFV domains. The correctness of the protocol was verified in the proposed Petri Color Network.

- **Proposal of architecture for creating the interconnection between two and more SDN/NFV domains** - Interconnection of multiple SDN/NFV domains of different levels is defined and the verification of this interconnection was successfully verified in the proposed Petri Color Network.

- **Proposal of continuous operation - providing Virtualized Network Functions** - Because of the robustness and complexity of a problem that addresses a different issue, this problem was not addressed in this work.

References

[1] A. K. Adrian Lara and B. Ramamurthy. Network innovation using openflow: A survey. *IEEE Communications Surveys & Tutorials*, 16(1):493 – 512, August 2013.

[2] B. J. Bashker D., Cascio W. *How to Apply HR Financial Strategies (Collection)*. Pearson Education, Inc., New Jersey, 2013.

[3] J. Day and H. Zimmermann. The osi reference model. *Proceedings of the IEEE*, 71(12):1334 – 1340, Dec 1983.

[4] M. C. et al. Network functions virtualisation: An introduction, benefits, enablers, challenges & call for action. *ETSI, white paper*, 2012.

[5] C. G. Gruber. Capex and opex in aggregation and core networks. *Optical Fiber Communication*, 5(1):1–3, May 2009.

[6] J. K. Hyunmin Kim and Y.-B. Ko. Developing a cost-effective openflow testbed for small-scale software defined networking. *Advanced Communication Technology (ICACT), 2014 16th International Conference on*, 16(1):758–761, Feb 2014.

[7] P. P. Lemberger and M. Morel. *Managing Complexity of Information Systems: The Value of Simplicity*. John Wiley & Sons, London, 2013.

[8] K.-H. N. Myung-Ki Shin and H.-J. Kim. Software-defined networking (sdn): A reference architecture and open apis. *ICT Convergence (ICTC), 2012 International Conference on*, 12(1):360–361, Dec 2012.

[9] J. R. Nick Feamster and E. Zegura. The road to sdn: An intellectual history of programmable networks. *ACM SIGCOMM Computer Communication Review*, 44(1):87–98, August 2014.

[10] e. Nick McKeown. Openflow: Enabling innovation in campus networks. *In: SIGCOMM Computer Communication Review*, 38(5):69–74, Jan 2008.

[11] T. F. Nir Kshetri and D. C. R. Torres. *Big Data and Cloud Computing for Development: Lessons from Key Industries and Economies in the Global South*. Taylor & Francis, New York, 2017.

[12] Y. Tits. Lack of standardization concerning interfaces between network equipments. *Electricity Distribution (CIRED 2013)*, 22(2):1–4, June 2013.

[13] Z. Z. Yu Wu and F. Lau. Cloudmov: Cloud-based mobile social tv. *IEEE Transactions on Multimedia*, 15(4):821 – 832, Jan 2013.

[14] e. a. Zaborovsky. Network complexity: Cross-layer models and characteristics. *In: Telecommunications*, 3(1):1 – 6, Jan 2007.

Selected Papers by the Author

P. Podhradský, E. Mikóczy, M. Soriano, P. Helebrandt, T. Halagan, I. Drozd Future networks - Concepts, architectures and services In *ed. Bratislava : Slovak University of Technology, 2015. CD-ROM, 104 s. ISBN 978-80-227-4522-2.*

T. Halagan, T. Kováčik, P. Trúchly, A. Binder. Syn flood attack detection and type distinguishing mechanism based on counting bloom filter. In *Third IFIP TC 5/8 International Conference, ICT-EurAsia 2015*, and 9th IFIP WG 8.9 Working Conference, CONFENIS 2015, Held as Part of WCC 2015, Daejeon, Korea, October 4-7, 2015, proceedings. 1. vyd. Cham : Springer, 2015, p. 30-39. ISBN 978-3-319-24314-6.

T. Halagan, T. Kováčik. Modification of TCP SYN flood (DoS) attack detection algorithm. In Numerical modelling and simulation : international interdisciplinary PhD workshop IIPhDW, Tatranske Matliare, Slovak republic, 20-22 May 2014. 1. vyd. Warsaw : Elektrotechnical institute, 2014, ISBN 978-83-61956-29-7.

T. Halagan, I. Kotuliak. NFV Federation. In ICETA 2016. 14th IEEE International conference on emerging elearning technologies and applications. November 24 - 25, 2016. Danvers : IEEE, 2016, p. 79-84. ISBN 978-1-5090-4701-7.

L. Kaplán, T. Halagan. Development sketch-based tool for creation and scaling of virtualized SDN infrastructure. In ICETA 2015. IEEE 13th, *International Conference on Emerging eLearning Technologies and Applications* , pages 189–194, IEEE, 2015, ISBN 978-1-4673-8533-6