Cross-Domain Network Slicing for Industrial Applications

Vasileios Theodorou*, Konstantinos V. Katsaros*, Andreas Roos†, Ermin Sakic‡§, Vivek Kulkarni‡
*Intracom Telecom, Greece, †Deutsche Telekom AG, Germany, ‡Siemens, Germany, §TUM, Munich, Germany
Email:*{theovas, konkat}@intracom-telecom.com, † Andreas.Roos@telekom.de, ‡{ermin.sakic, vivekkulkarni}@siemens.com

***Abstract*—Building on virtualization and programmability, 5G networks aim for concurrent support of application domains with different functional and QoS requirements, both across and within vertical domains. Towards these requirements, network slicing mechanisms allow the management and orchestration of the underlying pool of resources, typically within a single administrative domain. However, in several occasions, verticals are expected to have a large geographical footprint, often crossing the administrative borders of multiple network domains, placing a subsequent functional requirement for cross-domain orchestration. In this paper we describe our approach on cross-domain slicing operations for the case of Industrial Applications with strict and flexible QoS requirements, with a particular focus on Wind Power plant *networks*. We describe the design of our SDN-based orchestration TRL-7 prototype and further provide a detailed look on the testbed prepared for measurements in an operational Wind Power plant in Brande, Denmark.**

***Keywords*—5G, Slicing, SDN, Wind Turbine, IoT**

I. Introduction

Recently, intensive effort has been devoted towards the realization of 5G networks, aiming at substantially differentiated next generation network capabilities. Perhaps of utmost importance, 5G networks are aimed to enable the management and orchestration of the underlying resources towards network behavior tailored for specific sectors of economic activity and the industry, the so-called *verticals*. Through means of virtualization and programmability, 5G networks are expected to enable the assembly of the required resources and functionality for various co-existing types of verticals, on top of the same physical infrastructure, which in many cases is extended to the physical world with new types of devices e.g., sensors and actuators in the context of the Internet-of-Things. The resulting *network slices* then "*provide only the traffic treatment that is necessary for the use case, and avoid all other unnecessary functionality. The flexibility behind the slice concept is a key enabler to both expand existing businesses and create new businesses*" [1].

Network management in large industrial wind power plants is a distinctive application domain of particular importance, due to its economic, ecologic and social impact. Managing a large number of wind turbines and an ever growing number of locally hosted applications and data sources requires dynamic connectivity and bandwidth shares. New value-added services will further require application specific network configuration to reflect the stakeholder's access rights and communication requirements. Active and proactive power production will require flexible management of Distributed Energy Resources (DERs) and energy storage capacities based on per-minute saturation of market and actual pricing model. Furthermore, external stakeholders such as grid operators require insight into the capabilities of the Wind Power plant in order to utilize its capabilities, e.g., production and consumption of reactive energy when there is insufficient wind etc. The Wind Power plant operators, on the other hand, require the wholesale market pricing state available to them at all times. Data mining and pattern matching techniques for early fault recognition and identification of irregularities will result in a wide range of additional scenarios requiring automated setups and configuration of deterministic network services to provide the necessary sensor data for processing in externally or internally hosted data analytics appliances.

It becomes obvious that a wide set of applications with different Quality of Service (QoS) requirements, are expected to be supported by the underlying network infrastructure. Though QoS support mechanisms have been under investigation and development for decades [2], the expected state of affairs in 5G networks will introduce unique challenges. Diverse QoS requirements will need to be supported under the same, but often also under different service administration realms. Different service providers/stakeholders are expected to operate on network slices of the same infrastructure e.g., wind turbine firmware update by vendor *vs.* energy regulation by distribution system operator (DSO). At the same time, the physical footprint of the services will in some cases cross the administrative borders of network operators, as is the case of remotely operated industrial Wind Power plants. As such, the network slicing related management and orchestration operations will need to cross the network operator administrative borders as well.

In this paper we present the cross-domain network slicing solution developed in the context of the EU-funded research project VirtuWind. Other research initiatives have set similar objectives, such as the 5GEx Project[3], presenting however a particular focus on Network Functions Virtualization (NFV) aspects and targeting a wide range of use cases. Our work takes a rather focused approach, targeting industrial applications, and in particular the management of remote industrial Wind Power plants. Our network slicing solution builds on a logically centralized framework based on Software Defined Networking (SDN) principles, presenting a lightweight and readily deployable alternative to related approaches. We present the design of our solution along with software and system level details of the developed TRL-7 prototype. We then provide details on the testbed we have established in an existing Wind Power plant in Brande, Denmark, which aims to serve our evaluation efforts planned to be completed in future.

II. Cross-domain slicing in VirtuWind

A. Industrial Wind Park Requirements

The control applications of an industrial wind park are managed by Supervisory Control and Data Acquisition (SCADA) systems. SCADA is typically placed in the close proximity to the controllers and actuators, inside a private network infrastructure. Additionally, industrial wind park networks expose external interfaces for remote services such as maintenance access, energy regulation and grid response. Customized access for different stakeholders means the access for a particular service has a limited time duration or constrained number of devices or constrained industrial-grade QoS requirements or any of those combinations, and poses the requirement for traffic and resource isolation across networked applications. We henceforth briefly detail these requirements.

Remote Access for Maintenance Purposes: SCADA applications requiring remote access are the management of the wind turbine equipment and monitoring applications which carry video/audio data used for supervising the area inside and around the turbine, especially useful for the remote support of technicians in offshore turbines *e.g.*, to visually check the rotor position in an offshore wind turbine, prior to hoisting technicians by helicopter. The converged surveillance and control applications are both transmitting over the same physical network, most often over fibre, but sometimes also radio links.
View Isolation for Audit, Surveillance and Maintenance: Integration of different vendors equipment both in terms of networking devices *e.g.*, switches and utility devices such as Wind Turbine Generator (WTG) appliances, puts a requirement for the isolated access to the assigned devices for maintenance by different vendors. Typical wind power plant stores must also provide for the isolated and reliable access to operational data to various clients and customers *e.g.*, regulatory personnel accessing operational and production logs.
Quality of Service: Typically, internal field level control traffic requires real-time guarantees in terms of end-to-end delay and bandwidth allocation *e.g.*, for high vibration level alarms. Sensor data must be also securely and reliably aggregated and transmitted to the outside domains for remote analytics. Several cross-domain SCADA control services require strict end-to-end delay bounds and reliable delivery e.g., grid regulation signaling. Remote video surveillance has relaxed end-to-end latency requirements, but requires relatively high bandwidth shares and specific security and isolation network properties to be in place. In a converged network, both the voice/video and control applications data is transmitted over the same physical network, and thus needs appropriate prioritization and granular traffic filtering at the control-domain site.

B. A Logically Centralized Approach

The principles of network slicing constitute a beneficial enabler for the described industrial application environment and the corresponding requirements. Traffic isolation and support for QoS differentiation emerge as the basic building blocks, with technical solutions readily available for many years now (*e.g.*, [2]). What comes next is the ability to orchestrate these technical solutions on an inter-domain level. However, crossing the administrative borders of multiple Network Service Providers (NSPs) poses the challenge of an inter-domain coordination mechanism that realizes the required network slices, while preserving the operational autonomy of each NSP.

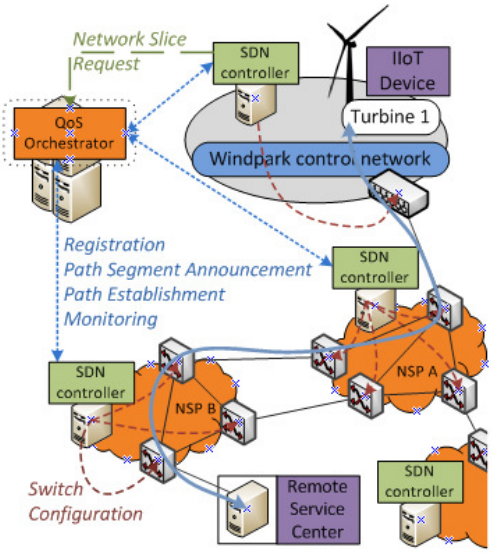


Fig. 1: Inter-domain deployment scenario and high-level interactions.

To this end, the EU research project Virtuwind [4] has designed and implemented a complete solution building on the principles of Software Defined Networking (SDN) [5]. A two-level hierarchical structure allows the management and control of the underlying network resources (see Figure 1). On the first level, a logically centralized SDN Controller entity per NSP is responsible for the management and orchestration of the intra-domain network. This includes the local transmission technologies and QoS mechanisms (e.g., DiffServ, 802.1p, MPLS). Each network operator controls and manages its network infrastructure utilizing the locally selected set of technologies, that need not be the same across the inter-domain network. SDN Controller instances are also further considered for the management and control of the network within the wind park. On the next hierarchy level, a logically centralized entity i.e., the *QoS-Orchestrator*, is responsible for the coordination of individual NSP operations, as described later in this section.

The VirtuWind solution applies the aforementioned two-level hierarchy structure to the network slicing process as well. Namely, each NSP has at least one network slice prepared with a predefined set of ingress and egress points and QoS attributes *e.g.*, bandwidth, delay, latency, packet loss. Such network slices are prepared by local means of orchestration (*i.e.*, by the local SDN Controller) and are aimed to be offered as constituent *path segments* of the end-to-end inter-NSP network slices offered for the support of industrial applications. In this way, NSPs need not engage in the configuration of their intra-domain forwarding substrate on a per industrial application network slicing request. All predefined network slices are registered with the QoS-Orchestrator. On the next hierarchy level, the QoS-Orchestrator creates network slices for specific industrial application requests by selecting and stitching together individual predefined NSP network slices. Obviously, the capacity of the individual predefined NSP slices allows the support of multiple industrial application service requests. To this end, upon the establishment of an industrial

application network slice, the availability of a path segment of the constituent NSP-level network slices is updated at the QoS-Orchestrator level.

Control plane. The VirtuWind approach is realized in three phases.

Registration phase: NSPs register their SDN controllers to the QoS-Orchestrator through he exchange of *Registration Request/Reply* messages, which include exchanged credentials to be used for authentication and authorization in future requests.

Path Segment Announcement phase: Each NSP SDN controller announces its network resources, which the NSP is willing to contribute in order to enable the QoS-enabled inter-domain end-to-end connectivity service, in the form of path segments. A path segment is mainly described by the path segment identifier, ingress-node, egress-node, QoS requirements, time constraints and price, and essentially constitutes a pre-configured network slice. The phase is completed through the exchange of authenticated/authorized *Path Segment Offer Request/Reply* messages.

Path Establishment phase: When an end-to-end connectivity request arrives from an industry SDN controller, the QoS-Orchestrator calculates the end-to-end (E2E) path and requests the respective NSP SDN controllers to configure their networks accordingly.

An industrial application *e.g.*, video surveillance, requests an E2E path by sending a *QoS Connectivity Request* to the local (usually Industry domain) SDN controller and from that point on to the QoS-Orchestrator. This message contains the source and destination points, flow matching information, as well as the QoS requirements and the time constraints. The QoS-Orchestrator evaluates this information and computes a path based on up-to-date path segment information from each intermediate NSP SDN domain controller. To calculate the path, the QoS-Orchestrator considers the capabilities of currently available path segments at each NSP along the potential paths of communication. When there are multiple viable paths, the QoS-Orchestrator can select a path based on other parameters such as cost. Once a valid path is selected, the QoS-Orchestrator triggers the path segment instantiation at each SDN Controller of the NSPs involved in the QoS enabled end-to-end path. Subsequently, the SDN controllers instantiate their network path segment with the announced QoS capabilities and duration, and finally individually provide a status feedback about the network path segment establishment to the QoS-Orchestrator. The QoS-Orchestrator then informs the SDN controller who initiated the process about the final outcome (success/failure). Only then, the communication between the end-points may begin.

Periodically during the established service's lifetime, each SDN domain reports monitoring information to the QoS-Orchestrator, to ensure that the QoS agreed for each inter-domain flow is satisfied. Proactive resilience is supported through fast failover and/or the establishment of redundant paths. Link and node failures are also reactively propagated to the local NSP SDN Controller, so as to optimize the recovery paths yielded by fast failover. If the failure cannot be handled by an SDN controller *e.g.*, it involves an inter-domain link, it is propagated to the QoS-Orchestrator, which restarts path establishment on the updated (inter-domain) network graph.

Data plane. The described orchestration mechanism aims at the realization of E2E network slices across the involved domains without imposing limitations or placing strong functional requirements on the exact forwarding or QoS support technologies adopted within each NSP. In this respect, the resulting forwarding configuration primarily focuses on the configuration of border routers or switches. As illustrated in Figure 2, the baseline VirtuWind solution builds on GRE Tunneling [6], with a single tunnel established between unique pairs of egress-ingress NSP end points. During the Path Segment Announcement phase, NSP SDN Controllers advertise the identifiers for the registered Path Segments, mapping one-to-one to forwarding identifiers *e.g.*, MPLS labels or VLAN IDs. During the Path Establishment phase, the QoS-Orchestrator generates a unique GRE Tunnel Key [7] for the E2E service. The GRE Tunnel Key is used by border nodes to distinguish different E2E service flows within the same GRE Tunnel, allowing all these flows to use the same inter-NSP link (GRE Tunnel) but follow different Path Segments within each domain (both egress and ingress). This approach provides the flexibility to differentiate the treatment of service flows subject to their QoS requirements, while keeping the granularity of the GRE Tunnels to a topological scale *i.e.*, in the order of the number of distinct border router pairs. This is enabled by the introduction of a $<$*GRE Tunnel, GRE Tunnel Key*$>$ to/from *Path Segment Identifier* mapping at each border node, with Path Segment Identifiers specified by each NSP individually i.e., an MPLS Label or a VLAN ID.

The presented VirtuWind solution follows a logically centralized approach, in an analogy to the SDN paradigm. This approach has been the result of a careful consideration of several design aspects, also in the light of alternative distributed approaches with bilateral inter-NSP negotiations. Our assessment concluded that the centralized approach presents significantly lower complexity as it confines control plane communications only between NSPs and the QoS-Orchestrator, thus scaling regardless the topology characteristics, as opposed to bilateral signaling between densely connected NSPs. The simplicity of the centralized approach also facilitates the establishment of the necessary trust for both the unbiased selection of Path Segments and the corresponding revenue sharing. This becomes clearer when considering the role of the QoS-Orchestrator as a trusted third party (similar to IXP operators or trusted certificate authorities), as opposed to the bilateral NSP interactions, where the Path Segment selection and revenue sharing is subject to a distributed agreement between biased actors i.e., competing NSPs.

III. VirtuWind Prototype

The VirtuWind solution has been developed in a full-fledged prototype, aimed to validate and evaluate our design in an existing wind park setting. In this context, we first describe the software architecture of the developed prototype and subsequently present our testbed environment, situated in Brande, Denmark.

A. Software Architecture

The VirtuWind prototype (Figure 3(a)) builds on the OpenDaylight SDN Controller, with a series of components supporting different features of the solution, in a modular

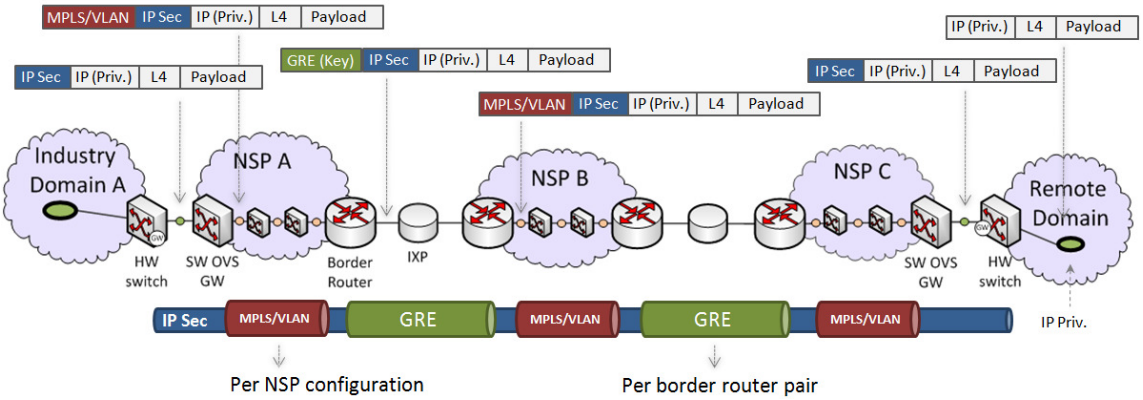


Fig. 2: Exemplary cross-domain data plane configuration.

approach. The prototype also supports operations targeted for the network environment within each wind turbine, which are out of the scope of this paper. Apart from the VirtuWind SDN Controller, a stand-alone QoS-Orchestrator prototype has been separately developed. Due to paper length limitations we provide only a short description of each component of the architecture.

QoS-Orchestrator
Orchestration Manager: Provides an interface towards the SDN controllers of individual domains for all control plane traffic (refer to Section II-B).
Path Manager: Computes an inter-domain path for each E2E request received by an industrial SDN controller, by maintaining a network topology map of the participating inter-connected domains and the received path segment offers (offered network resources) through the Orchestration Manager.
Security Manager: Provides authentication and authorization for inter-domain related requests (registration, path segment announcement, path segment instantiation and monitoring) sent by the underlying SDN controllers.
Web Portal: Provides a graphical interface to the maintained QoS-Orchestrator parameters, showing registered domains, received path segment offers, instantiated E2E paths as well as monitoring information.

Virtuwind SDN Controller
QoS Negotiator: Interfaces the QoS-Orchestrator for all control plane interactions (see Section II-B) *e.g.*, path establishment requests.
Security Manager: Provides authentication and authorization for requests received by the QoS-Orchestrator.
Path Manager: Manages network slice bootstrapping and domain-level reactive resilience, currently supporting MPLS and VLANs. It also monitors the QoS parameters of network slices to be reported to the QoS-Orchestrator.
Resource Monitor: Presents the physical topology to the Path Manager along with network status events (*e.g.*, link failure) and performance parameters *e.g.*, latency, packet loss.
Resource Manager: Acts as the interface between Path Manager and the physical infrastructure.
User Interface: Allows management and administration of NSP domains. It exposes the network topology, the QoS parameters of path segments and details on established flows and corresponding industrial traffic.

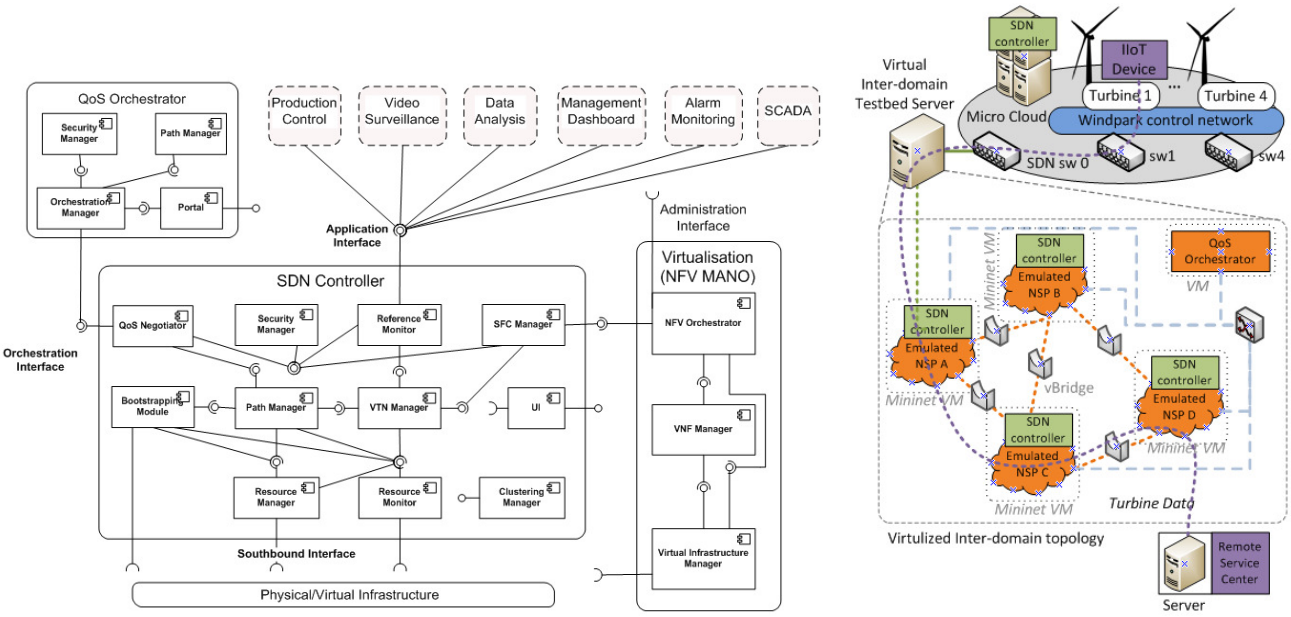
B. Wind Park Testbed in Brande

Reaching a high Technology Readiness Level (TRL), namely TRL-7, the VirtuWind prototype has been deployed in a real wind park site located in Brande, Denmark, with the purpose of validating its functionality in real, operational conditions. The Brande wind park testing environment has been extended to support the inter-domain features of VirtuWind. Obviously, these features target and require the availability of inter-connected SDN-enabled NSPs providing QoS-enabled connectivity between the Brande intra-domain environment and a remote service center. As this is currently practically infeasible on top of the public Internet, the project has targeted the development of a realistic emulated environment.

The virtualized testbed is realized on top of a hardware (HW) server. The HW server resources are virtualized through Linux Ubuntu 16.04 Virtual Machines (VMs), with each one instance corresponding to a single, emulated NSP. NSP domain emulation is supported through the instantiation of Mininet, which realizes each domain's topology through interconnected Open vSwitch (OVS) instances. The virtualized testbed supports an interconnection of four individual domain topologies. Each domain topology is designed to reflect common connectivity scenarios found within network operators that feature multiple paths between end-points. Each domain peers with other domains through edge switches.

All NSP domains are inter-connected as shown in Figure 3(b). The QoS-Orchestrator responsible for calculating a requested E2E inter-domain path is running in a separate VM. In order to establish an E2E inter-domain path, the Brande wind park network (industry domain) and a Remote Service Center, realized as a single application server, are connected to the inter-connected NSP domains. The industry domain is connected to NSP A, while the Remote Service Center is connected to NSP D. In each of the NSP domains and the industrial domain, an SDN controller is instantiated and registered to the QoS-Orchestrator.

Based on the established testbed, validation and evaluation efforts are planned towards important KPIs, both on the control



(a) VirtuWind system architecture

(b) Inter-domain testbed in Brande.

Fig. 3: VirtuWind System: (a) software prototype architecture, (b) the deployed testbed in Brande, Denmark.

plane, including service establishment time, service availability, failure detection and recovery times, and the data plane i.e., ensuring conformance to QoS requirements including bandwidth, packet loss, latency, jitter. As these efforts are ongoing at the time of this paper writing, Figure 4, shows a preliminary view of the cumulative distribution function (CDF) of the recovery/path optimization time for link failures handled reactively by local SDN Controllers. As expected, measurements show a high average value (2.4 sec) as path optimization involves the communication of the network with the SDN Controller and the subsequent calculation and establishment of an alternative, in the presence of the observed failure, optimal path.

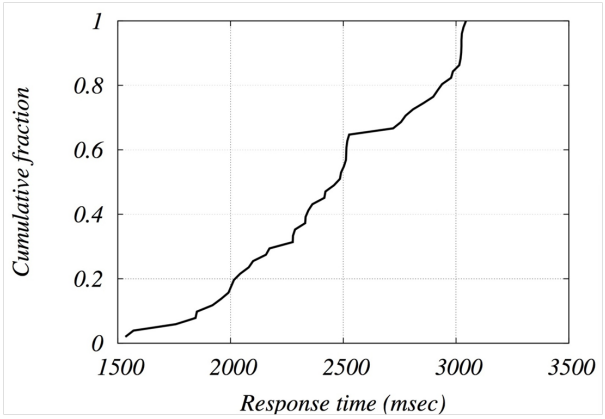


Fig. 4: Recovery/path optimization time: reactive, NSP SDN Controller scheme.

ACKNOWLEDGMENT

This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 671648 (VirtuWind).

REFERENCES

[1] NGMN, "NGMN 5G White Paper," 2015. [Online]. Available: http://bit.ly/2BGEH0Q

[2] D. Vali, S. Paskalis, L. Merakos, and A. Kaloxylos, "A survey of internet QoS signaling," *IEEE Communications Surveys Tutorials*, vol. 6, no. 4, pp. 32–43, Fourth 2004.

[3] EU Project 5GEx, "5GEx: 5G Exchange," 2015-2018. [Online]. Available: http://www.5gex.eu/

[4] EU Project VirtuWind, "Virtual and programmable industrial network prototype deployed in operational Wind park," 2015-2018. [Online]. Available: http://www.virtuwind.eu/

[5] W. Xia, Y. Wen, C. H. Foh, D. Niyato, and H. Xie, "A survey on software-defined networking," *IEEE Communications Surveys Tutorials*, vol. 17, no. 1, pp. 27–51, 2015.

[6] D. Farinacci, T. Li, S. Hanks, D. Meyer, and P. Traina, "Generic Routing Encapsulation (GRE)," Internet Requests for Comments, RFC Editor, RFC 2784, March 2000, http://www.rfc-editor.org/rfc/rfc2784.txt. [Online]. Available: http://www.rfc-editor.org/rfc/rfc2784.txt

[7] G. Dommety, "Key and Sequence Number Extensions to GRE," Internet Requests for Comments, RFC Editor, RFC 2890, September 2000.