Published in: NetSoft 2018 - 4th IEEE International Conference on Network Softwarization
DOI: 10.1109/NETSOFT.2018.8460110

Network Slicing for Critical Communications in Shared 5G Infrastructures - An Empirical Evaluation

Fabian Kurtz, Caner Bektas, Nils Dorsch, Christian Wietfeld
Communication Networks Institute, TU Dortmund University, Otto-Hahn-Strasse 6, 44227 Dortmund
Email: {fabian.kurtz, caner.bektas, nils.dorsch, christian.wietfeld}@tu-dortmund.de

***Abstract*—Increasing automation in systems such as Smart Grids (SGs), Intelligent Transportation, the Internet of Things (IoT) and Industry 4.0, involves the need for robust, highly capable Information and Communication Technology (ICT). Traditionally, to meet diverging use case requirements regarding network data rate, delay, security, reliability and flexibility, dedicated communication infrastructures are employed. Yet, this is associated with high costs and lengthy roll-out times. Therefore it is desirable for multiple tenants to share one Physical Network (PN). However, this may compromise service guarantees, potentially violating Service Level Agreements (SLAs). Network slicing aims to address this challenge by transparently dividing one common infrastructure into multiple, logically independent networks. Thereby tenants are isolated from one another, ensuring the fulfillment of hard performance guarantees. As slicing is central to realizing the potential of 5G networks, this work presents a novel approach based on Network Function Virtualization (NFV) and Software-Defined Networking (SDN) driven queueing strategies. The developed solution is comprehensively evaluated with realistic traffic in a physical testing environment. Highly demanding critical infrastructure use cases, with multiple service levels per slice, are used to validate performance and demonstrate functionalities such as dynamic data rate allocation.**

I. Introduction

Developments such as the emergence of Smart Grids, largely driven by a shift to renewable energy resources, Intelligent Transportation Systems (ITSs) with self-driving cars and the IoT place increasing demands on ICT. Traditionally, such Critical Infrastructures (CIs) require dedicated communication networks to meet their specific, diverging requirements [1]. However, this methodology incurs high costs and communication resources can not easily be deployed and scaled according to demand. Hence, 5G proposes to instantiate multiple, virtual networks, so called network slices, on top of one underlying, shared (public) Physical Network (PN) [2]. This approach aims to provide independent networks, meeting the requirements of individual use cases, while reducing costs and configuration overhead. For slicing in 5G architectures the three main categories Enhanced Mobile Broadband (eMBB), Massive Machine Type Communication (mMTC) and Ultra-Reliable Low Latency Communication (uRLLC) have been defined, as shown in Figure 1 [3][4]. Due to their relevance for CI, the latter two are the main focus of this paper, while eMBB is used to generate bulk traffic. Although network slicing is crucial to fulfill the performance targets of 5G, currently no standard has been selected. Therefore, this work introduces a novel solution for CI communications in shared 5G infrastructures. By building on SDN and the European Telecommunications Standards Institute (ETSI) NFV architecture, we demonstrate the ability to provide hard service guarantees. A dedicated SDN controller for Management and Orchestration (MANO) provides individual slices, each in turn managed by its own controller. This strategy not only facilitates multiple tenants to share the same PN, but also enables new business models. Hence, clients such as SG Distribution System Operators (DSOs) can either configure network resources by themselves or utilize a fully managed slice via SDN's northbound Application Programming Interface (API). As slices are isolated from one another, overloads, e.g. caused by Distributed Denial of Service (DDoS) attacks or misconfiguration, are shown to have no impact on other slices. Also, flexible data rate allocation is demonstrated, allowing excess network capacity to be utilized by other traffic flows according to their priority. Beyond a scalability and performance evaluation, we validate our approach empirically by way of a real-world application scenario based on ITS Floating Car Data (FCD) [5] and IEC 61850 [6] SG traffic requirements. This paper is structured as follows: Section II provides an overview of related work. Next, Section III details three key aspects of this publication. First the general concept of 5G network slicing architectures is described. Subsequently, requirements of critical infrastructure communications are presented. Lastly, our NFV and SDN driven network slicing concept is detailed. Section IV introduces the employed testing methodology and evaluation scenarios. Afterwards, Section V discusses results, highlighting performance and scalability observations.

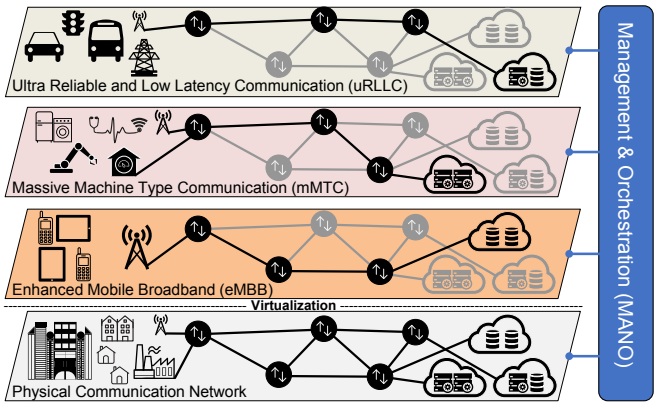

Figure 1: Overview of a Sliced 5G Communication Network

978-1-5386-4633-5/18/$31.00 ©2018 IEEE

II. Related Work

Related work presented in the surveys of [2], [7], [8], [9] and [10] emphasizes the importance of SDN and NFV for network slicing. Also general challenges and possible solutions are identified, yielding comprehensive overviews of the topic. Theoretical works meanwhile mostly focus on specific aspects of slicing, such as [11] who also identify NFV as key enabling technology. Approaches for slice selection and routing between Virtual Network Functions (VNFs) are developed in [12]. The interplay of cascading SDN controllers in sliced architectures is the focus of [13]. Algorithms, for example regarding optimized allocation of available network resources, are studied in [14], [15] and [16]. In contrast, we focus on an empirical evaluation of physical communication links resource sharing, as required by slicing. Works which implement slicing technologies, often employ or extend FlovVisor [17], a transparent proxy between OpenFlow (OF) switches and multiple SDN controllers. Among these studies [18] and [19] concentrate on slice management, respectively security aspects. An extension of FlowVisor with a general Quality of Service (QoS) scheme based on flow redirection is presented in [20]. Other solutions constitute a more flexible and universal basis for slicing, by building on SDN and NFV. Yet, Virtual LANs (VLANs) are mostly used as a means for traffic separation, a concept similar to FlowVisor. Management functionalities such as slice (de-) provisioning are discussed in [21]. [22] and [23] provide further works in this area, using an OpenDaylight controller [24]. An analysis of fast slice failover strategies is given in [25], while [26] describes challenges and solutions of Radio Access Network (RAN) slicing via LTE [27] and IEEE 802.11 [28] air interfaces. However, contrary to this paper, these works don't harness the potential of SDN and NFV fully, thus increasing system complexity and overhead. In summary, no work fully addresses the challenges of allocating available physical communication resources to virtual network slices in an efficient and dynamic manner. Hence, this paper not only develops a technical solution to network slicing suitable for deployment in current SDN and NFV enabled communication infrastructures, but also verifies the approach by a thorough, empirical performance evaluation.

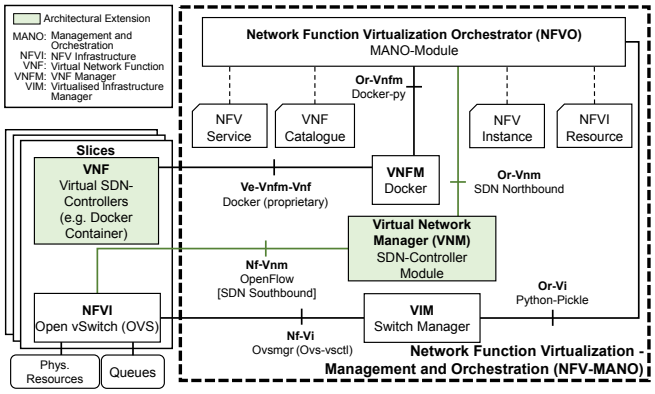

Figure 2: Extended ETSI NFV Architecture including Components of the Proposed Network Slicing Solution

III. Software-Defined Networking and Network Function Virtualization Based 5G Slicing

This section first introduces the concept, requirements and architectural framework of 5G network slicing. Next, the challenges of CI communications, particularly in shared infrastructures, are discussed. Afterwards we present our approach to slicing and illustrate its implementation.

A. 5G Network Slicing - Architecture and Concept

As illustrated by Figure 1, the next generation of mobile communication (5G) proposes the virtualization network resources. Through this multiple isolated network partitions, called slices, are created. This facilitates the deployment of use cases with differing demands on the same physical communication infrastructure. In this context, 5G distinguishes three main categories. eMBB is aimed at data rate intensive services (up to $20Gbps$) such as ultra high resolution video, fixed wireless broadband or Augmented (AR) and Virtual Reality (VR). With the emergence of IoT devices and Industry 4.0, inter-machine communication increases significantly. Although per user user rates are low, a massive number of devices physically distributed over large areas poses its own challenges. An example of this is Smart Metering in SGs, i.e. the automated collection of energy generation and demand down to customer or even device level. Hence, such mMTC use cases require a dedicated network (slice) to meet their performance targets. The third major scenario included in 5G addresses mission critical, latency sensitive applications, termed uRLLC services. An example are ITSs with FCD based vehicle-to-X communication. End-to-end delays below $1ms$ have to be guaranteed at all times, enabling fast control loops and thus reactions. Protection mechanisms for electric power transmission in SGs, as outlined in the next section, constitute another example of uRLLC. To meet these diverging requirements networks need to support slicing. Therefore NFV and SDN are widely considered key components of upcoming 5G infrastructures [2]. Figure 2 presents the generic NFV architecture defined by ETSI, extended with modules of our approach to network slicing. Leveraging these technologies, we illustrate our slicing concept in the following sections.

B. Requirements of Critical Infrastructure Communications

Modern critical infrastructures increasingly rely on ICT to reliably fulfill their requirements. However, dedicated networks are frequently required to provide the necessary level of performance, traffic isolation and manageability. Hence, network slicing is an ideal solution to these challenges. To be viable, the demands of CI communications in terms of data rate, latency, reliability and more have to be met. In this regard ITSs are a prominent field of application. Driven by the shift to increasing levels of driving automation, incrementally more FCD traffic is generated. FCD contains for instance information about vehicle location, direction of travel, speed and other status data. By exchanging these messages between vehicles or transmitting it via e.g. cellular networks to cloud infrastructures for analysis, road traffic can be optimized and

accidents reduced. As no general industry standard specifying packet size and Inter-Transmission Time (ITT) exists, we utilize values from literature [5]. Assuming a scenario in which vehicles travel on a highway at $130\frac{\text{km}}{\text{h}}$ a 5G uRLLC compliant end-to-end delay of $1ms$ equals a traveled distance of $\sim 3.6cm$. Conversely, passenger internet access for business or entertainment purposes, as an example for eMBB applications, is not as latency but more data rate sensitive than FCD.

Another especially challenging CI are SGs. The increasing share of renewable energies calls for powerful monitoring and control solutions. Therefore, stable operation necessitates pervasive, robust communication infrastructures. Electric utilities such as Transmission System Operators (TSOs) need to protect their high-voltage power lines and substations against faults, relying on Wide Area Monitoring Protection and Control (WAMPAC) and Supervisory Control and Data Acquisition (SCADA) systems. For this purpose inter- and intra-substation communication utilizes the IEC 61850 [6] protocol as developed by the International Electrotechnical Commission (IEC). The standard defines three main messages types aimed at different tasks. Manufacturing Message Specification (MMS) is employed to configure electrical grid devices. In contrast, Sampled Values (SV) and Generic Object Oriented Substation Events (GOOSE) are used for transmitting measurements, respectively events. Both are encapsulated directly into IEEE 802.3 Ethernet frames [29], allowing packet sizes of 64 to $1518Bytes$. Moreover, the maximum allowed end-to-end latency is defined at 3 to $10ms$ (depending on the exact application), with typical packet rates between $4,000$ and $12,800$ messages per second in the case of SV. Thus, this application requires a uRLLC network slice for stable operation. Smart Metering is another SG use case, typically employed by DSOs, for which a set of different communication protocols is available. A mMTC network slice is suitable for this application, as data rates and ITTs are comparatively low, while millions of devices can be deployed.

C. An NFV and SDN driven Approach to Network Slicing

Our approach to network slicing builds on NFV and SDN, to meet 5G's functionality and performance targets. Traditional communication infrastructures integrate services such as load balancing, firewalling and intrusion detection in custom hardware appliances. In contrast, NFV decouples hard- and software, abstracting functionalities into VNFs running on Commercial Off-The-Shelf (COTS) server platforms, e.g. in clouds. Thus mass-produced computing, storage and switching components can be used to flexibly deploy, scale and chain network services as needed by 5G communication. SDN is closely related to the concept of NFV. Typically decentralized devices such as routers handle packet switching as well as network control. In SDN dedicated Data Plane (DP) devices, i.e. switches without any routing capability, perform physical data forwarding. Hence, routing is centralized on the Control Plane (CP) via a so-called SDN controller. Thereby control decisions are based on a global instead of local network states, while CP and DP can be upgraded independently. Thus, performance as well as efficiency are increased, and the network can be configured centrally and flexibly, meeting the requirements of dynamic use cases such as CIs. The DP is configured via the southbound API, mostly by way of the de facto standard OF protocol [30]. Multiple controllers are linked through the east-, respectively westbound APIs, enabling scalability. Applications interface with the SDN controller over the northbound API, re-configuring communication according to service requirements. For both APIs no pervasive standard is currently available. SDN and NFV are complementary approaches, as the controller can dynamically route traffic flows between VNFs, while being deployed as VNF itself.

While many approaches to slicing build on VLANs for sharing physical communication resources, we build on queueing strategies (in this case Hierarchical Token Bucket (HTB)) in combination with SDN and NFV, as depicted by Figure 2. Open vSwitch (OVS) [31], an open-source virtual multilayer switch, is deployed on all bare-metal or virtualized DP devices of the network. On this basis our SDN-MANO controller creates a main bridge in each switch, which includes the respective physical ports. Next, one bridge per slice is added or removed as needed, as shown by Figure 3. These slice bridges contain virtual ports, which are nested within the main bridge. The MANO controller serves as an orchestrator, dynamically instantiating slice controllers (e.g. via Docker [32]), which can potentially be optimized for individual use cases. When traffic enters the DP, i.e. the main bridge, our MANO controller assigns packets, e.g. via their protocol or other criteria supported by OF, to the respective slice bridge. There the slice's controller routes packets to their virtual destination port, where the flow is mapped to the main bridge's proper QoS queue and physical port. These actions are repeated on each hop to the destination. Flows which match no slice are classified as best effort traffic. Although Ethernet is used in combination with queues to share the PN's available data rate, the presented approach can be adapted to other technologies. While we focus on wired 5G communication, provisions are made to ensure compatibility with air interface slicing technologies.

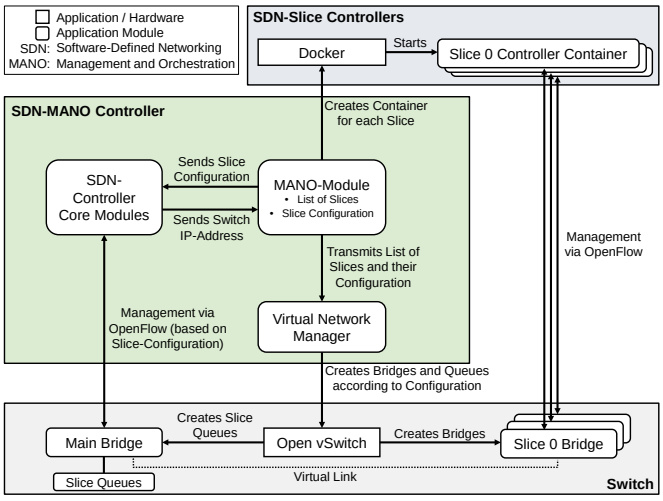

Figure 3: The Developed Network Slicing Architecture

IV. Testing Environment and Evaluation Scenarios

This section provides a detailed description of the varied scenarios under study and the corresponding testing setup.

A. Testing Environment

The testing setup consists of 13 identical servers, each equipped with an Intel Xeon D-1518 Central Processing Unit (CPU) (four cores at 2,2GHz), 16GB of RAM and six 1GBase-T Ethernet ports from two Network Interface Cards (NICs) (four: Intel I350, two: Intel I210). All devices utilize Ubuntu Server 16.04.3 LTS (v4.13.0-32-generic x86-64 Kernel) as Operating System (OS). Three computers are deployed as virtual switches by running Open vSwitch version 2.5.2, and thus constitute the sliced data-plane evaluated in this paper. As can be seen from Figure 4, six servers are assigned in pairs to the three use cases studied in this work and set up as hosts to either send or receive traffic over the sliced network. Another four machines act as SDN controllers, three of which employ Floodlight (v1.2) [33], managing the Smart Grid, Intelligent Transport and Best Effort Slices. The remaining device runs Ryu (v4.19) [34] and acts as SDN-MANO controller, creating slices for orchestration by the other controllers. To avoid any interference of measurements on the solution under study, three distinct networks are used: out-of-band control, maintenance and the sliced data-plane. Maintenance (not depicted in Figure 4) and control communication are each handled via a Zyxel GS1900-24E switch. The Precision Time Procotol (PTP) [35] is employed to synchronize all devices within the testing setup, yielding a mean clock deviation of $16\mu s$ and $152\mu s$ at maximum. With the exception of the real-world application scenario given in IV-B3, User Datagram Protocol (UDP) traffic loads are created with iPerf2 community edition (v2.0.10) [36]. For assessing our solution's overhead, we determine the maximum performance of the testing setup without slicing. Ethernet framesize at OSI model layer 2 is $1512Byte$ (from here on referred to as layer 2 data rate). We use this as a point of reference, as our solution is embedded on this level. Performance evaluations (Section IV-B1) operate on layer 4, resulting in a payload (i.e. goodput) of $1470Byte$. Thus, the maximum usable layer 4 data rate is 97.2% of the layer 2 data rate, i.e. $97.2Mbps$ goodput on a $100Mbps$ queue. Measurements are repeated at least 100 times with a minimum duration of $1\,\mathrm{min}$ per run. Dependent on payload size and ITT, latencies without slicing range from $0.25ms$ to $1ms$.

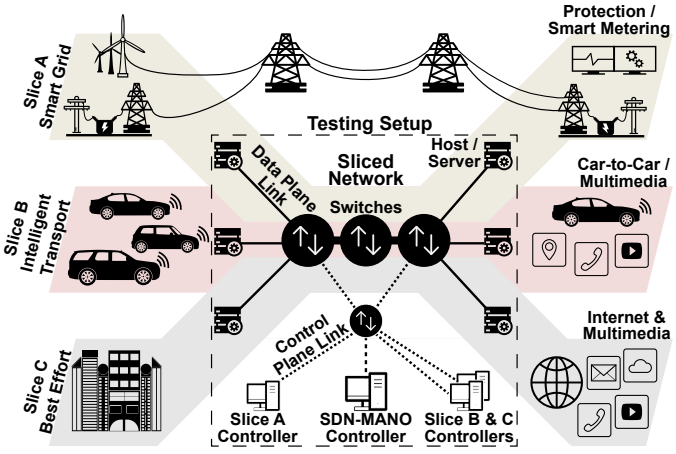

Figure 4: Evaluation Scenario within the Testing Setup

B. Evaluation Scenarios

The scenarios on which the evaluation of the developed network slicing solution is based are as follows:

1) Scenario A - Performance Study: For evaluating the performance of our end-to-end slicing solution, we focus on several key aspects resulting from 5G and CI communication requirements. Therefore, delay and data rate for varying degrees of network load are studied. On this basis we determine the overhead of our approach, to highlight the efficient use of available resources. This is facilitated by the use of $100Mbps$ Ethernet, which avoids any possible limitations of the evaluation setup interfering with the general concept, while also affording us the option to closely monitor CPU load during testing. Furthermore the isolation, i.e. independence of different slices is verified. This is particularly important to preclude any detrimental effects of errors or overloads in one virtual infrastructure on other tenants sharing the same PN. Hence, slice utilization is stepwise increased beyond the limit of 97.2% layer 4 goodput. This effectively represents a case in which a tenant transmits with a higher data rate, e.g. due to a DDoS attack, than allocated (i.e. rented or bought slice capacity). Misconfiguration by the PN operator is studied as well. Here two slices, with their combined maximum data rate exceeding the PN's capabilities, are used simultaneously.

2) Scenario B - Scalability Analysis: To represent an approach viable for deployment in large-scale, multi-tenant communication infrastructures, we demonstrate our solution's scalability in the following. Ideally end-to-end delays should not be influenced by the number of concurrent slices and their traffic load. Accordingly we analyze delay performance for no, 2, 8 and 16 slices. Available data rate is shared equally among all virtual networks, with traffic streams configured to utilize 100% slice capacity. Thereby any increase in delay can be attributed to side-effects of our solution, instead of overloads caused by congestion. Moreover, we validate slice isolation and end-to-end delay stability. This is achieved by subjecting seven out of 21 slices to UDP based traffic with data rates above the allocated limit. Contrary to scenario A, $1Gbps$ Ethernet is used to stress test concept and testing setup.

3) Scenario C - Critical Infrastructure Communication: Based on the challenging requirements of CI communications, we devise a testing scenario including real-world traffic flows such as FCD of ITSs and the IEC 61850 SG protocol. Both use cases are equally important and hence are allocated slices of the same priority, including dedicated SDN controllers. SG protection and FCD are classified as uRLLC 5G services and are assigned the highest priority in their corresponding slices. To demonstrate our solution's ability to discern different traffic

Table I: Slices and Traffic Flows of the CI Comm. Scenario

Slice (Descending Priority)	Use Case	5G Service Class	Priority within Slice	Hard Min. Data Rate [Mbps]	Max. Delay [ms]
Smart Grids	Protection (IEC 61850)	uRLLC	Highest	50	1
	Smart Metering	mMTC	High	200	20
Intelligent Transportation Systems	Floating Car Data	uRLLC	Highest	100	1
	Passenger Internet	eMBB	Low	450	10
Best Effort	Multimedia	None	Lowest	None	100

classes within a slice, Smart Metering (representing mMTC), as well as passenger internet (eMBB) are included in the related slices. Also, a best effort slice is present, handling multimedia traffic. As such it does not map directly to a 5G service class or impose strict delay boundaries. However, it transmits with a continuous data rate of $950Mbps$, roughly maximum the layer 4 goodput of the shared, physical $1Gbps$ DP network. As the slices has the lowest priority, it is thus overloaded whenever another slices consumes data rate. The different packet flows are started one after another, thereby taking away data rate from the lower priority best effort traffic. In contrast FCD and IEC 61860 protection flows are assigned hard guarantees, e.g. as required by SLAs, due to their criticality. Thereby we showcase the option of our solution to either impose hard data rate limits or assign network capacity dynamically. Additionally we increase FCD and protection traffic data rate limits during the test run, highlighting the ability to quickly and seamlessly re-configure slices on demand. Slices and their traffic flows, including minimum guaranteed data rates as well as maximum tolerable delays, are given in Table I. It is to be noted, that the given data rates are achieved by bundling multiple traffic flows. Although e.g. a single Smart Metering or FCD transmission does not require $200Mbps$, such an order of magnitude is commonly reached in aggregate due to the large number of simultaneously transmitting devices found in real-world deployments.

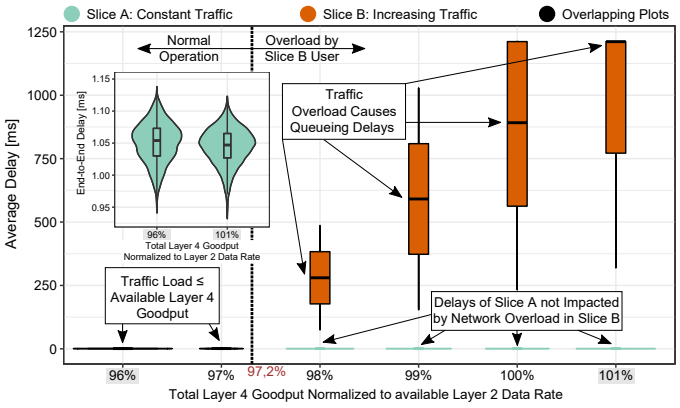

Figure 5: End-to-End Delays of Two Slices for Varying Traffic Loads, Including Overloads in Slice B

V. Evaluation Results

Evaluation results of the previously detailed slicing solution, obtained with the aid of our physical testing environment, are presented and discussed in the following sections.

A. Delay and Data Rate Performance

Figure 5 shows the end-to-end delays of two slices for varying traffic loads. Slices A and B share a physical $100Mbps$ Ethernet network fairly and transmit UDP traffic. As discussed in Section IV-A, some data rate is consumed by protocol headers. In effect 97.2% of layer 2 data rate remains as layer 4 goodput, regardless of the chosen approach. Hence, at 96% to 97% Slice A and B have a median end-to-end delay of $1.05ms$ with an variance of ca. $\pm 0.05ms$. However, if a data rate exceeding Slice B's allocation is forced into the network, an overload is created. While Slice A stays at its assigned limit (97.2% layer 4 goodput normalized to layer 2 data rate), the traffic of Slice B is increased in 1% steps. As indicated in Figure 5, this user-driven overload (e.g. due to a DDoS attack) leads to a sharp rise in delays, with medians up to $1,212ms$ at 101% load. Crucially the observed delays in Slice A remain unaffected, even compared to no slicing, as shown by the enlarged violin plots. Hence, slice isolation is demonstrated.
Misconfiguration by the PN operator is illustrated by Figure 6. Here, Slice A has an allocated queue data rate (i.e. layer 2 data rate) of $40Mbps$, effectively yielding $38.9Mbps$ on layer 4. The total sum of queue data rates (x-axis) should not exceed the theoretical maximum layer 2 data rate of a $100Mbps$ Ethernet link. This maximum is the ratio between frame sizes at layers 2 and 1, which yields $\frac{1512Byte}{1532Byte} = 98.7\%$. As Slice B's available queue data rate increases in $1Mbps$ steps, the queues' total sum eventually exceeds the $98.7Mbps$ limit, representing a misconfiguration. In that case Slice B tries to utilize resources that do not exist. Accordingly the 97.2% layer 4 goodput is no longer obtainable for Slice B, as A consumes the HTB mechanism's tokens. Hence, Slice A's data rate remains stable while B can not use its assigned capacity and stagnates at $56.9Mbps$, which is below 97.2% of the configured $60Mbps$ queue data rate. No overhead in terms of achieved throughput is observed, confirming expectations.

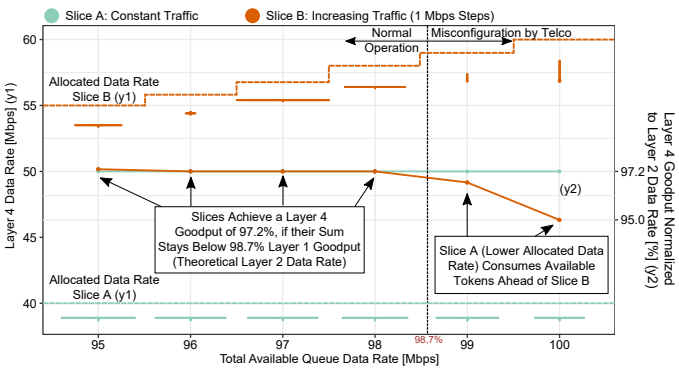

Figure 6: Impact Analysis of Misconfiguration by the Physical Communication Network Operator, i.e. Slice Provider

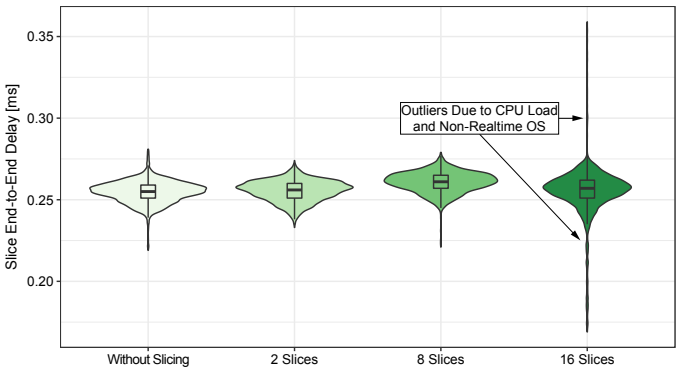

Figure 7: Effect of Multiple Slices on End-to-End Delays

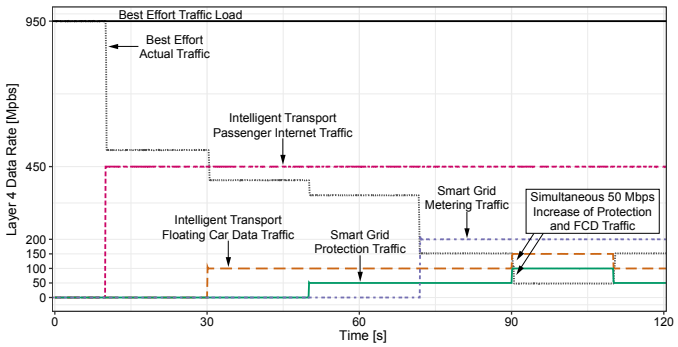

Figure 9: Critical Infrastructure Communication Scenario - Data Rate Allocation and Slice Isolation

B. *Scalability of the Proposed Slicing Solution*

Figure 7 shows the presented slicing solution's scalability. End-to-end delays of a dedicated and several sliced networks ($1Gbps$ capacity) is given. Data rate is allocated fairly, with all slices idle but one. Delays remain stable up until sixteen concurrent slices, at which point outliers of up to $0.36ms$ occur. Investigations reveal this to be a result of CPU context switches, necessitated since the employed hardware provides a maximum of eight threads and queues. Outliers down to $0.17ms$ are likely caused by the non-realtime OS's reduced timer/interrupt coalescing, triggered by the raise in computational load. Performance optimizations of the developed source, realtime kernels and higher thread-count CPUs should address this for deployment in highly-sliced networks.

A stress test of scalability is given by Figure 8. In normal operation (left side) 21 coexisting slices fully utilize their allocated data rate, achieving stable end-to-end delays with a median of $1ms$. Delays are higher than in the previous case as more slices share a slower PN ($100Mbps$). During partial overload (right side) seven slices try to exceed their allocated data rate. Accordingly their delays rise to $3.5s$, while slices without overloads remain unaffected. Thus network isolation remains robust even under high loads in several slices. Data rate remains stable across all presented scalability tests.

C. *Critical Infrastructure Communication Scenario*

For the CI communication scenario Figure 9 shows the measured data rate of the traffic flows given by Table I. At first only best effort traffic is present, fully utilizing the PN. This use case continues to transmit with $950Mbps$, regardless of available data rate, but has no guaranteed minimum data rate and can thus be displaced by other slices. Hence, once passenger internet, respectively FCD traffic of the ITS slice enters the network, nearly instantaneously best effort throughput reduces accordingly. The same applies when Protection and Smart Metering traffic of the SG slice are introduced. A simultaneous $50Mbps$ increase of Protection and FCD traffic at $90s$ into the measurement, serves as an especially critical test case. Both use cases can see a spontaneous rise in their demands, e.g. due to faults in the electrical grid forcing increased monitoring and control activity. While fast reactions with precise data rate levels are shown, Figure 10 confirms that hard service guarantees are provided during transitions. Here best effort traffic typically stays below the desired $100ms$ boundary. Yet, outliers to $350ms$ occur, resulting from slice overloads, i.e. after $10s$ in Figure 9. Smart Metering and passenger internet delays are below $3ms$ with $\sim 1.3ms$ medians, meeting service level guarantees. Outliers result from the starting phase, with stable delays throughout runs. The violins of protection as well

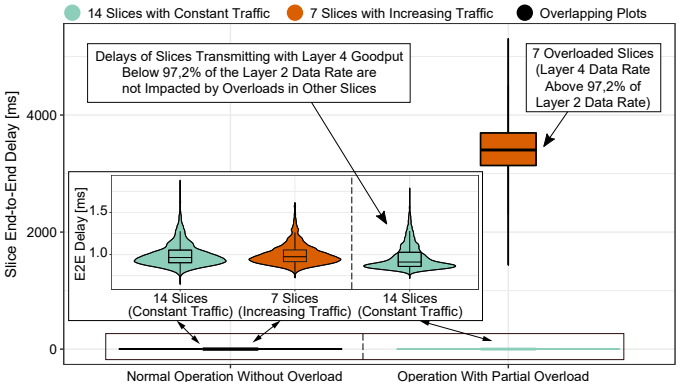

Figure 8: Stress Testing Scalability with Partial Overload Showcasing Isolation of Resources (21 Slices Total)

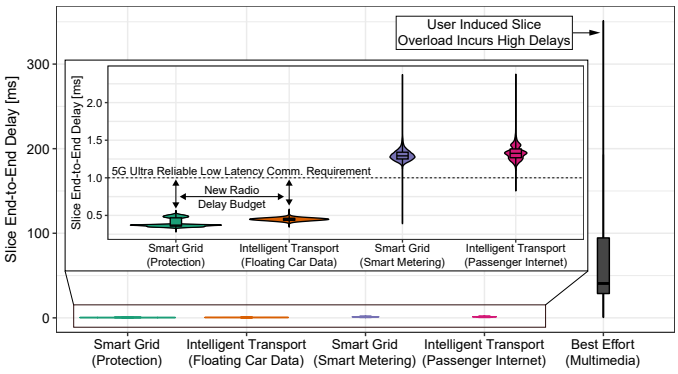

Figure 10: Critical Infrastructure Communication Scenario - End-to-End Slice Delays

as FCD traffic show a slight delay variance during slice re-configuration. However, requirements are fulfilled with delays mostly below $0.5ms$. Thus a delay budget, which is sufficient for 5G new radio air interfaces, is obtained.

VI. Conclusion and Outlook

In this work we present an NFV and SDN based approach to network slicing for CI communications in shared 5G infrastructures. Building on nested bridges and HTB queueing, an ETSI NFV compatible solution is implemented and thoroughly analyzed. Performance is validated by way of a physical testing setup, showcasing slice isolation even during partial overloads. Scalability is highlighted as well, with no performance reduction aside from cases with highly sliced networks. Here, virtual hops between bridges increase computational loads, yet optimizations are identified for further improvements. A real-world scenario with SG and ITS traffic flows covering 5G's service classes is discussed. Dynamic data rate allocation, slice re-configuration and the ability to provide hard service guarantees under realistic conditions with enough headroom for 5G new radio air interfaces are demonstrated. Future work will concentrate on the integration of the here described solution with a mmWave radio interface. Thereby a comprehensive 5G end-to-end slicing architecture will be created, capable of transparently hosting multiple tenants while meeting challenging requirements imposed by e.g. Smart Grids. Furthermore, network orchestration will be studied to achieve policy-based automated deployment, configuration and management of VNFs and slices (as required by individual services). An evaluation in field trials is targeted to provide an in-depth performance validation in realistic CI deployments.

Acknowledgement

This work has been carried out in the course of research unit 1511 *'Protection and control systems for reliable and secure operations of electrical transmission systems'*, funded by the German Research Foundation (DFG) and the Franco-German Project *BERCOM* (FKZ: 13N13741) co-funded by the German Federal Ministry of Education and Research (BMBF).

References

[1] Y. Yan, Y. Qian, H. Sharif and D. Tipper, 'A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges', *IEEE Communications Surveys and Tutorials*, vol. 15, no. 1, pp. 5–20, 2013.

[2] J. Ordonez-Lucena *et al.*, 'Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges', *IEEE Communications Magazine*, vol. 55, no. 5, pp. 80–87, May 2017.

[3] R. El Hattachi and J. Erfanian, 'NGMN 5G Initiative White Paper', NGMN (Next Generation Mobile Network) Alliance, White Paper, 2015. [Online]. Available: https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf.

[4] K. Mallinson, 'The path to 5G: as much evolution as revolution', *3GPP - The Mobile Broadband Standard*, May 2016. [Online]. Available: http://www.3gpp.org/news-events/3gpp-news/1774-5g_wiseharbour.

[5] G. Karagiannis *et al.*, 'Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions', *IEEE Comm. Surveys Tutorials*, vol. 13, no. 4, pp. 584–616, 2011.

[6] *IEC 61850: Communication Networks and Systems for Power Utility Automation*, International Electrotechnical Commission TC57.

[7] T. Soenen *et al.*, 'Demystifying network slicing: From theory to practice', in *IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, May 2017, pp. 1115–1120.

[8] H. Zhang *et al.*, 'Network Slicing Based 5G and Future Mobile Networks: Mobility, Resource Management, and Challenges', *IEEE Communications Magazine*, vol. 55, no. 8, pp. 138–145, 2017.

[9] X. Foukas, G. Patounas, A. Elmokashfi and M. K. Marina, 'Network Slicing in 5G: Survey and Challenges', *IEEE Communications Magazine*, vol. 55, no. 5, pp. 94–100, May 2017.

[10] P. Rost *et al.*, 'Network Slicing to Enable Scalability and Flexibility in 5G Mobile Networks', *IEEE Communications Magazine*, vol. 55, no. 5, pp. 72–79, May 2017.

[11] B. Chatras, U. S. T. Kwong and N. Bihannic, 'NFV enabling network slicing for 5G', in *2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN)*, Mar. 2017, pp. 219–225.

[12] V. K. Choyi *et al.*, 'Network slice selection, assignment and routing within 5g networks', in *IEEE Conference on Standards for Communications and Networking (CSCN)*, Oct. 2016, pp. 1–7.

[13] A. Mayoral *et al.*, 'Cascading of tenant SDN and cloud controllers for 5G network slicing using transport API and openstack API', in *Optical Fiber Comm. Conference and Exhibition (OFC)*, Mar. 2017, pp. 1–3.

[14] S. Vassilaras *et al.*, 'The Algorithmic Aspects of Network Slicing', *IEEE Communications Magazine*, vol. 55, no. 8, pp. 112–119, 2017.

[15] R. Trivisonno, R. Guerzoni, I. Vaishnavi and A. Frimpong, 'Network Resource Management and QoS in SDN-Enabled 5G Systems', in *IEEE Global Comm. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–7.

[16] M. Jiang, M. Condoluci and T. Mahmoodi, 'Network slicing in 5G: An auction-based model', in *IEEE International Conference on Communications (ICC)*, May 2017, pp. 1–6.

[17] R. Sherwood *et al.*, 'FlowVisor: A Network Virtualization Layer', Tech. Rep., Oct. 2009.

[18] J. L. Chen, Y. W. Ma, H. Y. Kuo and W. C. Hung, 'Enterprise visor: A Software-Defined enterprise network resource management engine', in *IEEE/SICE International Symposium on System Integration*, Dec. 2014, pp. 381–384.

[19] C.-H. Chen, C. Chen, S.-H. Lu and C.-C. Tseng, 'Role-based campus network slicing', in *International Conference on Network Protocols (ICNP)*, Nov. 2016, pp. 1–6.

[20] C. W. Tseng *et al.*, 'A network traffic shunt system in SDN network', in *International Conference on Computer, Information and Telecommunication Systems (CITS)*, Jul. 2017, pp. 195–199.

[21] S. Sharma, R. Miller and A. Francini, 'A Cloud-Native Approach to 5G Network Slicing', *IEEE Communications Magazine*, vol. 55, no. 8, pp. 120–127, 2017.

[22] X. Li *et al.*, '5G-Crosshaul Network Slicing: Enabling Multi-Tenancy in Mobile Transport Networks', *IEEE Communications Magazine*, vol. 55, no. 8, pp. 128–137, 2017.

[23] P. K. Chartsias *et al.*, 'SDN/NFV-based end to end network slicing for 5G multi-tenant networks', in *European Conference on Networks and Communications (EuCNC)*, Jun. 2017, pp. 1–5.

[24] *OpenDaylight*, 2018. [Online]. Available: www.opendaylight.org.

[25] D. Giatsios *et al.*, 'SDN implementation of slicing and fast failover in 5G transport networks', in *European Conference on Networks and Communications (EuCNC)*, Jun. 2017, pp. 1–6.

[26] M. Richart, J. Baliosian, J. Serrat and J. L. Gorricho, 'Resource Slicing in Virtual Wireless Networks: A Survey', *IEEE Trans. on Network and Service Management*, vol. 13, no. 3, pp. 462–476, Sep. 2016.

[27] C. Johnson, *Long Term Evolution in Bullets, 2nd Edition*. CreateSpace Independent Publishing Platform, Jul. 2012.

[28] *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, The Institute of Electrical and Electronics Engineers, Inc.

[29] *IEEE Std 802.3-2015 (Revision of IEEE Std 802.3-2012)*, The Institute of Electrical and Electronics Engineers, Inc.

[30] *OpenFlow Switch Specification Version 1.3.0*, Open Networking Foundation, 2018. [Online]. Available: www.opennetworking.org.

[31] *Open vSwitch Virtual Network Switch*, 2018. [Online]. Available: http://openvswitch.org/.

[32] *Docker Software*, 2018. [Online]. Available: www.docker.com.

[33] *Floodlight Controller Version 1.2*, Project Floodlight, 2018. [Online]. Available: www.projectfloodlight.org/floodlight/.

[34] *Ryu Software-Defined Networking Framework*, 2018. [Online]. Available: https://osrg.github.io/ryu/.

[35] *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems 1588–2008*, The Institute of Electrical and Electronics Engineers, Inc.

[36] *Iperf Community Edition*, Feb. 2018. [Online]. Available: https://sourceforge.net/projects/iperf2/.