IMMI: an architecture integrated for management of modern internet service providers

Matheus Monteiro Silveira* and Rafael Lopes Gomes

Center of Science and Technology,
State University of Ceará (UECE),
Av. Silas Munguba 1700, ZIP 60714903,
Fortaleza, CE, Brazil
Email: matheus.monteiro@aluno.uece.br
Email: matheus.monteiro@larces.uece.br
Email: rafaellgom@larces.uece.br
*Corresponding author

Abstract: Nowadays, the human society claims for modern computational services based on internet access through an internet service provider (ISP). Similarly, ISPs expanded their service delivery, giving different alternatives of access networks and interconnected by a edge network. This new reality creates the idea of modern internet service providers (MISPs), applying network virtualisation (NV), software-defined network (SDN) and network function virtualisation (NFV) technologies. However, the MISPs need a solution to perform an integrated management of these network environments. Within this context, this article proposes an architecture, called integrated management of modern internet service providers (IMMI), to perform the management of both edge and access networks, allowing information exchange, the deployment of slices and resources based on the profile of the access network. Additionally, this article analyses the current status of the ISPs (and their limitations), as well as it discusses the key technical trends and challenges for the management of MISPs. Finally, a case study is presented to show the suitability of the proposed architecture to enhance the management capacity of MISPs.

Keywords: edge network; access network; network management; internet service provider; ISP; network virtualization; software-defined network; SDN; network function virtualisation; NFV; resource allocation; strategic planning; future internet.

Reference to this paper should be made as follows: Silveira, M.M. and Gomes, R.L. (xxxx) 'IMMI: an architecture integrated for management of modern internet service providers', *Int. J. Security and Networks*, Vol. x, No. x, pp.xxx–xxx.

Biographical notes: Matheus Monteiro Silveira is an undergraduate student in Computer Science at the State University of Ceara (UECE). He received Honorable Mention by the International Collegiate Programming Contest (ICPC). He has the following research interests: network management, experimentation and mobility.

Rafael Lopes Gomes is an Associate Professor at the State University of Ceara (UECE), being coordinator of Laboratory of Computer Networks and Security (LARCES). He received his PhD in Computer Science from the University of Campinas (UNICAMP) at Brazil. He was a research visitor at Network Research Lab from the University of California Los Angeles (UCLA) in 2014. He is part of technical program committees of several international conferences, such as International Symposium on Integrated Network Management (IM), IEEE/IFIP Network Operations and Management Symposium (NOMS), IEEE Latin-American Conference on Communications (LATINCOM), and others. He has experience and researches on the following topics: network management, cybersecurity, software defined networks, resilience planning, wireless networks and internet of things.

This paper is a revised and expanded version of a paper entitled 'Management framework for future internet service providers' presented at 2018 IEEE Symposium on Computers and Communications (ISCC).

1 Introduction

Nowadays, the human society claims for modern computational services, most of them based on internet access through an internet service provider (ISP). ISP provides to its clients the service of access to the internet, firming a service level agreement (SLA) to specify the parameters of this service (Doverspike et al., 2010). In the last few years, the internet emerged as the main medium for content sharing, playing a vital role in our modern private and institutional lives.

In the same way, ISPs expanded their service delivery, giving different alternatives to access internet (Liang and Yu, 2015). The traditional broadband access networks (BANs), to companies and residences, have now the companion of radio access networks (RANs), for example 3G, 4G and 5G (in next years), close to the final users. These distinct access networks pass through an edge network before reaching the core of the internet (Doverspike et al., 2010).

Each type of access network (BANs and RANs) has distinct requirements, since, besides the environment characteristics, the kind of user's application present in each access network has an specific network demand. In RANs, it is necessary to deal with unpredictable mobility, signalling, interference and the new paradigm to access content anytime, anywhere, and with best effort quality level. Also, the users utilise low traffic application for content sharing in social medias, text message exchange, and voice calls (Granelli et al., 2015). On the other hand, the network traffic arising from BANs is composed of both data and multimedia applications, for example web pages, social network (like Instagram and Facebook), IPTV, Youtube, Netflix, online games, among others. Therefore, BANs need to deal with the traffic profile present in RANs plus real-time/multimedia applications, that have high bandwidth demand and are sensitive to delay and packet losses (Ferrús et al., 2018).

Regardless the type of access network, all of them need to address key features, such as: low delay, flexibility, resilience, compatible capital expenditure (CAPEX) and operational expenditure (OPEX). These features influence the quality of service (QoS) and quality of experience (QoE) of the final users. Thus, problems of slowness, service interruption and constant disconnections in the internet access frustrate users. In addition, the dynamic traffic demand through the day (due to the human mobility within cities), resulting in an elastic demand of networking resources affect the internet delivery service (Galdino et al., 2020).

Recently, researchers in the scientific community and global enterprises are investigating possible approaches to address the points of this new scenario of the internet, where the network virtualisation (NV), software-defined network (SDN) and network function virtualisation (NFV) are expected to be the key technologies (Leconte et al., 2018) to be part of the modern internet service providers (MISPs). These technologies arise as a possible solution to evolve the resource management, as well as to flexibilise and to customise the behaviour of the networks.

The junction of NV, SDN, and NFV approaches allows the split of the network infrastructure in customised slice of network, including resources and a particular set of virtual network functions (VNFs) inside the SDN controller (Ma et al., 2018; Ordonez-Lucena et al., 2017; Ferrús et al., 2018). Therefore, the MISPs tend to apply NV, SDN, and NFV technologies to optimise the service delivery, as well as to reduce the financial investment (mainly CAPEX and OPEX) (Han et al., 2018; Afolabi et al., 2018; Alvizu et al., 2017).

Therefore, the MISPs need a solution to perform an integrated management of distinct network types (BANs and RANs) and the edge network that interconnects them to each other and to the core of the internet, considering the deployment of NV, SDN, and NFV as technological tools. Nevertheless, the existing approaches deal with only specific issues regarding the management of this kind of environments with NV, SDN, and NFV (Mohan and Gurusamy, 2019).

Within this context, this article introduces an architecture, called integrated management of modern internet service providers (IMMI), to allow the management of MISPs, evolving the usage of the technologies cited in both access and edge networks. The goal of IMMI is to perform an integrated management approach, relating the management of both edge and access networks. This approach allows the information exchange among the edge and the access networks, the deployment of slices and VNFs based on the profile of the access network, and the dynamic adjustment of the parameters according to the current state of the MISP infrastructure (edge and access).

Additionally, this article analyses the current status of the ISPs (and their limitations), as well as it discusses the key technical trends and challenges for the management of MISPs, considering the requirements of user's applications and the current technologies. All these points discussed were applied during the designed of the proposed IMMI architecture.

This article is organised as follows. Section 2 presents related work, encompassing topics related to management of NV, NFV and/or SDN. Section 3 details the trends and challenges for the management of MISPs. Section 4 describes the proposed architecture for management of MISPs, while in Section 5 presents a case study. Finally, Section 6 summarises the article and presents some future work.

2 Related work

This section describes key related work about resource management strategies of SDN, NFV, and NV. Table 1 summarises these existing work in the literature, highlighting the differences to our proposal.

Table 1 Related work

Reference	*SDN*	*NV*	*NFV*	*Focus*
Ma et al. (2018)	Yes	No	No	Routing paths and bandwidth guarantee in VTN
Son and Buyya (2019)	No	No	Yes	Latency-aware distribution of VNFs in edge
Manzalini and Crespi (2016)	Yes	No	Yes	Integration of SDN and NFV in edge networks
Leconte et al. (2018)	Yes	Yes	No	Optimisation framework for clouds
Caballero et al. (2018)	Yes	Yes	No	Framework for Nash equilibrium
Han et al. (2018)	Yes	No	Yes	On-demand application-aware end-to-end slices
This work	Yes	Yes	Yes	Architecture for integration of edge and access networks

Ma et al. (2018) propose a dynamic resource adjustment architecture that includes a routing planning mechanism and a bandwidth resource planning mechanism for a virtual tenant network (VTN) with SDN. The proposed architecture helps not only to plan routing paths in a physical network to satisfy a VTN user request but also to guarantee bandwidth usage based on overall network conditions. However, this architecture does not consider the integration of edge and access networks.

Son and Buyya (2019) present a dynamic resource provisioning approach for VNFs, adapting to dynamically changing network volumes and automatically allocating resources for VNFs. The proposal considers the latency requirement of different applications in the service function chain, which allows the latency-sensitive applications to reduce the end-to-end network delay. Nevertheless, this proposal is limited to resource provision for VNFs in edge network, disregarding access networks and their integration with the edge network.

Manzalini and Crespi (2016) describe the edge operating system (EOS), an architecture to provide among others, the following features for the edge network: abstractions, low-level element control, message-passing between processes, management of packets of processes. The authors suggest that EOS can be seen as an expression of the integration of the SDN and the NFV, enabling anything-as-a-service in the edge network. The main limitation of EOS is its exclusivity for edge network (ignoring the access networks and their characteristics). Additionally, EOS does not consider the existence of virtualisation and slicing. These two aspects prevent EOS to be applied in the MISPs.

Leconte et al. (2018) propose an optimisation framework for massively distributed cloud infrastructure interconnected with SDNs. It allows the resource allocation for slices both in terms of network bandwidth and cloud processing. Additionally, the authors present an iterative algorithm to converge to the optimal resource allocation. However, this proposal does not consider the integration of edge and access networks.

Caballero et al. (2018) present a network slicing (NES) framework, which applies an admission control policy, resource allocation scheme and a user dropping method to maintain the system in a Nash equilibrium. The NEs framework uses the admission control to guarantee that slices can satisfy the rate requirements of all their users. Nevertheless, the NEs framework does not consider the integration of edge and access networks, as well as the adaptations necessary on them.

Han et al. (2018) apply a network system to guarantee bandwidth resources in an application-aware end-to-end (E2E) slices on-demand scenario. Additionally, the authors use the idea of software-defined wireless and NFV as basis for the system. However, this paper does not concern about integration issues between the networks.

To the best of our knowledge, none of the works found in the literature focuses on the development of an architecture to deal with the MISPs main issues, as well as the management of multiple access networks through the integration of SDN, NV, and NFV. These trends and challenges are considered in the IMMI described in this article.

3 Trends and challenges for MISPs

Despite the financial investments over the last years, the current internet structure and its network characteristics have inherent constraints from the reality of decades ago, that could not glimpse the new requirements of the internet for the society and businesses, emerging the need of MISPs.

The rise of these new characteristics, such as user mobile devices, real time multimedia applications, traffic for cloud computing and data centres, and others, changed the context of internet, highlighted issues related to mobility, multiple network interfaces, resilience, delay constraints and traffic engineering in a network that is not designed to this new reality. As consequence, the internet aggregated to the existing fixed network, several heterogeneous wireless networks accessed from mobile devices, using Wi-Fi or cellular networks.

This scenario makes the internet an essential part of human life, where the users access contents and services through different technologies according to day time. In general, at home or work, the users access internet through a BAN (which has a wireless/cabled router). In contrast, on the way between home and work, users access internet through a RAN (usually, 3G or 4G technology, and 5G in future). Each situation has distinct requirements, since the kind of user's application has a specific network demand. The MISPs need to manage these access networks accordingly, as well the edge network which interconnects them to the core of the internet.

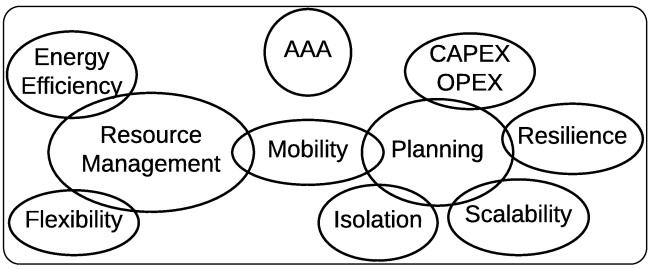
Within this context, in the next few years, MISPs have several challenges to be considered during the delivery

of internet access service: resource management; energy efficiency; authentication, authorisation and accounting (AAA); CAPEX and OPEX; flexibility; planning; scalability; resilience; isolation; and mobility.

- *Resource management:* MISPs need to share the network resources among the clients accordingly, since it must comply with the SLAs and keep the services isolated. In addition, a MISP aims to have as many clients as its infrastructure can bear, as the more clients the MISP has, the higher its profits are. Thus, the resource management must avoid the wastage of resource, which directly impacts the resource availability and, consequently, the provider's profit.
- *Energy efficiency:* In order to reduce costs and consequently increase profit, MISPs have to use the network device only when it is necessary, minimising energy consumption. Underutilisation of networking devices reduces energy efficiency of the MISP, as their power consumption does not scale with utilisation.
- *Authentication, authorisation and accounting (AAA):* Currently, users want to dynamically change the characteristics of their service delivery (consequently, the SLA). The MISPs must provide a suitable interface to its clients to adapt the service (for example, add more bytes to the data plane, increase the bandwidth assigned, among others) whenever they want. This interface must control access, as well as provide the information necessary to bill for services.
- *CAPEX and OPEX:* Companies want to reduce business expenses, where CAPEX and OPEX represent two categories that are influenced by the management and structure of provider. Therefore, the decoupling between software and hardware tends to minimise these financial issues.
- *Flexibility:* MISPs must use this quick adaptation of resource allocation and network functions to mould the service delivery according to the current state of network infrastructure and the users traffic characteristics. It is possible to change the behaviour and configuration of the network when the separation between hardware and software is deployed.
- *Planning:* The management of MISPs includes the task of glimpse possible situations, such as hardware failure, unpredictably high injection of traffic, emergency maintenance of network device, among others. The monitoring of client's behaviour (generating a kind of profile) can help the MISP to anticipate and to adapt the service to predicted situations.
- *Scalability:* The number of users is increasing every year, and the applications demand more features from the network. Therefore, the MISPs need to maintain its performance when the demand increases and to identify when it is necessary to expand the physical resources to assure QoS/QoE for the users. MISPs must apply high levels of abstraction to ease its expansion, as well as handle the control communication to avoid extra overhead.
- *Resilience:* MISPs need to keep a minimum specified level of service, even when failures occur in the network infrastructure, being a key requirement to assure QoS/QoE to the users. Resilience encompasses not only reactive actions to manage post-failure impact, but also pre-failure strategic planning.
- *Isolation:* The user's applications have distinct requirements, thus different network behaviours can optimally address these requirements. In this way, when MISPs isolate distinct type of traffic (either by user or type) it can customise the network for the ongoing traffic. Additionally, this isolation guarantees no negative effect between them, for example a greedy application sharing the same resource of a constant bitrate application.
- *Mobility:* Traditionally, the mobility of users is related to wireless base stations. However, the mobility of users tends to evolve, including the transition between the BANs and RANs. Therefore, the MISPs need to concern about the handover of RAN-to-RAN and BAN-to-RAN (or vice versa). The BAN-to-RAN is presented when the user has the mobile and home internet access service from the same MISP. This business model is becoming popular due to convenience and/or financial savings for the user.

The presented challenges are correlated when a MISP is considered. This correlation is illustrated in Figure 1. The existing flexibility in the MISP will be the basis of resource management and energy efficiency, since dynamic resource allocation and selectively turned on and off of the network devices come from flexibility, both resource management and energy efficiency can be achieved. In the same way, the planning of situations must encompass issues related to scalability and reduction of CAPEX/OPEX, since both challenges need medium/long time perspectives to be addressed.

Figure 1 Relations among challenges



Resilience relies on planning and isolation. The failure of physical network equipments should not affect the service delivery due to the efficient planning of the network to maintain a minimum level of quality. Similarly, a problem in one client can not affect other clients. For example, if a

client is victim of a denial of service attack, it should not influence the QoS/QoE of other clients that are connected to the MISP.

Mobility from BAN to RAN and vice versa is still an open issue, which depicts the social behaviour of existing cities around the world, moving the network resource demand from RAN to the BAN (or the reverse). Thus, the MISPs should be aware of this social behaviour during the resource management and planning tasks.

In front of these challenges, MISPs tend to apply NV, SDN, and NFV. NV is a technology that allows the deployment, over a single physical infrastructure, of multiple network slices with customised, dynamically adjusted properties corresponding to the required behaviour (Gomes et al., 2016). The usage of slices is viewed as a mean to cope with both the varying demand for high-bandwidth and the lack of flexibility in current networks. Similarly, at a lower layer, SDN is exploited to reduce the load on networks and to enable a more effective usage of elastic resources through the separation of control and data planes (Ma et al., 2018). NFV is an architecture to decompose the functions of the network from the hardware, allowing the running of these functions in remote devices (Son and Buyya, 2019). NFV introduces the following advantages:

1 the software can evolve independently from the hardware, since they are separated

2 the deployment of VNFs is flexible and adaptable

3 dynamic provisioning services, enabling scalable growth performance according to current network conditions.

The combination of NV, SDN, and NFV enables the sharing of the network infrastructure by several VNs. Each VN has a specific behaviour (that can be configured dynamically inside the SDN controller tied to the VN) and network resources isolated from the other VNs. However, the deployment of this combination of technologies for MISPs to address these challenges is not trivial and it is still an open issue. Thus, in the next section, an architecture to be applied by MISPs is proposed.

4 IMMI architecture

In the last few years, the society diversified its internet usage, aggregating new applications and services in its behaviour. As consequence, the demand for network resources has increased, claiming for a suitable integration between edge and access networks. Additionally, ISPs modernised their type of access network, deploying both wired and wireless networks (3G, 4G and 5G in next years). Usually, the former provides internet to residences, buildings, companies, etc, while the later supports mobile users and long-range services. Each case has singular particularities and requirements, turning the management of MISPs very complex. Thus, MISPs tend to apply NV, SDN, and NFV approaches to improve the service delivery and their network infrastructure capabilities.

However, the management of several access networks interconnected by an edge network applying the NV, SDN and NFV technologies is still an open issue, since the challenges described in Section 3 need to be overcome. Therefore, to fill this gap of management of MISPs, this article presents the architecture for integrated management of modern internet service providers (IMMI). IMMI aims to evolve the service delivery of MISPs, performing an integrated management of edge and access networks (RANs and BANs), focusing on the existing challenges.

IMMI architecture supports the information exchange and carrying out actions between the edge and the set of access networks, i.e., it attaches management capabilities for the MISP, without severe changes in the applied technologies (NV, SDN and NFV) and devices. For MISPs, this fact represents a management improvement with low financial investment, as well as an interoperability with the existing technologies.

An overview of the IMMI architecture is shown in Figure 2, where the structure of designed modules and their interaction with the existing technologies is highlighted. All the MISPs environment is presented as follows:

a access network (green boxes): it represents the devices and functions expected in the RANs/BANs

b edge network (orange box): it includes the existing SDN and virtualisation approaches (in grey boxes) and the network functions to be deployed through NFV (in purple boxes)

c IMMI (blue boxes): each module designed has a specific role at the edge and access network to address the challenges for MISPs.

The following modules were designed: resource allocator, SLA analyser, billing counter, health monitor, NFV manager, slice deployer, infrastructure handler, interaction broker, profile descriptor and access controller. Next, the designed modules are detailed, highlight how them can suppress the existing challenges.

A crucial feature for MISPs is the adaptation of resources when necessary, which is performed by *resource allocator*. It dynamically assigns the network resources for each slice in the edge network. Similarly, *infrastructure handler* is a communication interface between IMMI and the SDN infrastructure, providing the essential information to perform the tasks (such as load, flow table, energy consumption, etc). These two modules have a crucial role to allow resource management and energy efficiency in the MISP.

SLA analyser controls the SLA firmed, working together with *billing counter*, which measures the financial values of MISP, including current SLAs and the estimated CAPEX and OPEX. Thus, the AAA challenge is addressed by *SLA analyser* and *billing counter*.

Figure 2 Modules of IMMI (see online version for colours)

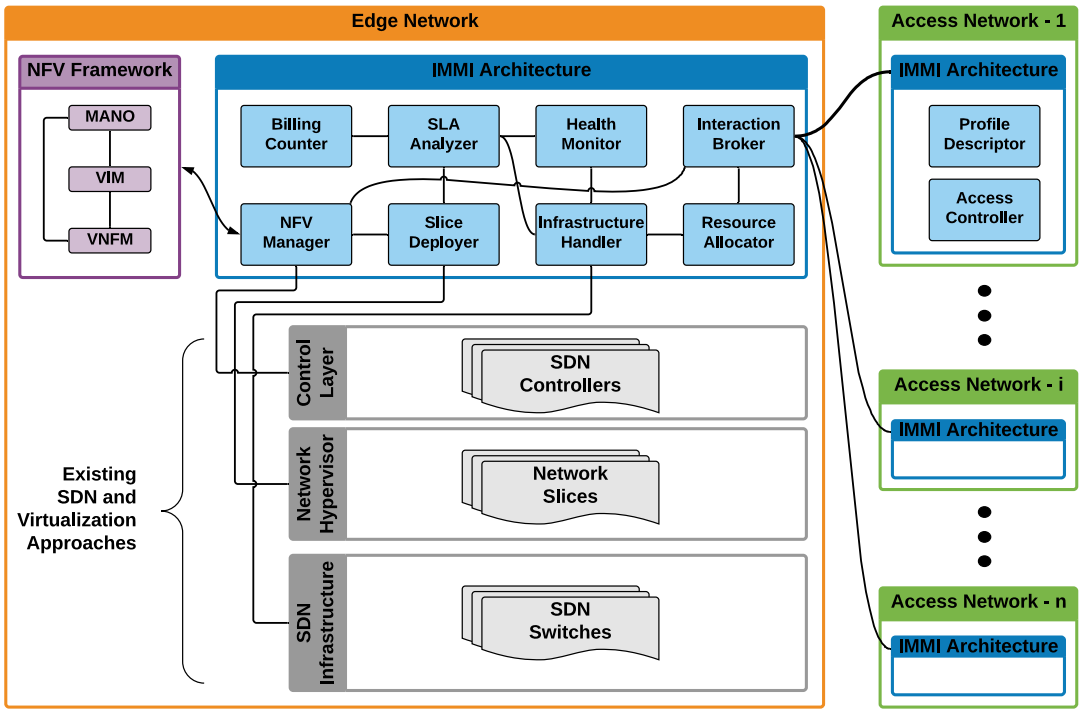


Figure 3 Relation between modules and challenges (see online version for colours)

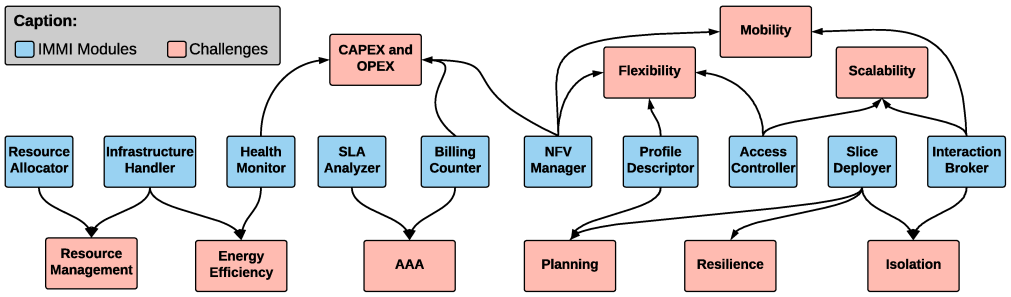
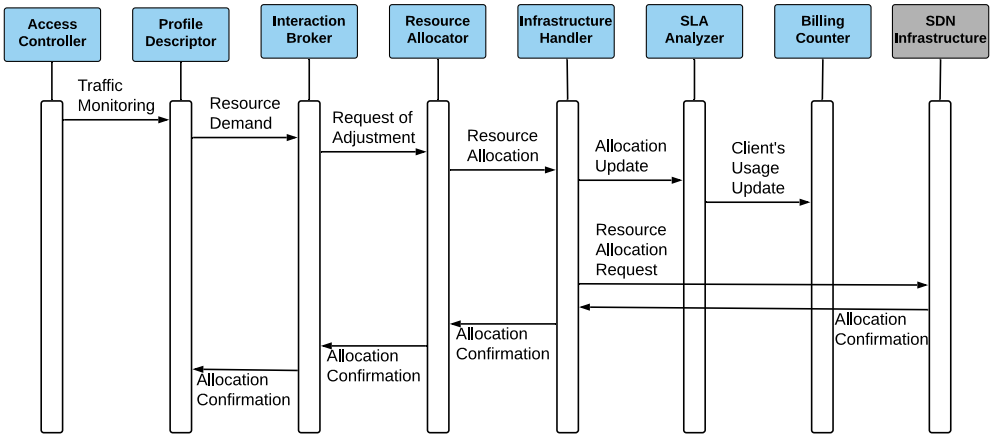


Figure 4 Sequence diagram for dynamic resource allocation (see online version for colours)



Besides the *billing counter*, *health monitor* and *NFV manager* modules also address the CAPEX and OPEX challenges. *Health monitor* collects information for analysis of the network infrastructure, such as congestion points, link failures, etc. On the other hand, *NFV manager* interacts with the existing NFV framework to deploy the VNFs.

Slice deployer controls the deployment of slices (in the network hypervisor) in the edge network following the specification of SLA as well as adjustment requested by

the *NFV manager*. Additionally, *slice deployer* defines the structure of the slice (i.e., the links and switches that will be used), that affects directly the resilience of the slice. This slicing approach enables isolation between the clients (one client per slice) and the strategic planning of the MISP.

Each access network has two modules: *profile descriptor* and *access controller*. *Profile descriptor* identifies the traffic profile of the client during the day, allowing the improvement of service delivery through the inference and the planning of resource allocation of the MISP. *Access controller* is placed in each access network, interacting directly with the physical device, adding flexibility and scalability to the access network. It monitors the access network and alerts the *profile descriptor* when events that could affect the service delivery occurs.

A crucial module in the IMMI architecture is the *interaction broker*. It intermediates the communication between the modules in the edge and access networks, allowing the synchronisation actions of an *access controller* and the edge network. The inclusion of this feature allows the MISP to handle the mobility of clients through the access networks, while keeping the isolation and scalability of the MISP, since access networks would not directly influence each other.

Thus, the split of modules between MISP edge and access networks aims to enhance the deployment of slices and VNFs, since the split smooths the delay in the deployment process and it eases the management of specific VNFs for each access network. This same benefits exist in the definition of two types of controller: an access controller in each access network and a set of SDN controllers (one for each slice) in the edge network.

Figure 3 summarises how the designed modules address each challenge for MISPs described in Section 3. It is possible to note that one module (individually or in junction with others) is responsible to deal with the requirements of each challenge. This strategy allows the adaptation of the functionalities of each module to encompass new requirements that may arise throughout the years.

To illustrate a practical usage of the IMMI architecture in a realistic scenario, Figure 4 shows a sequence diagram of a dynamic resource adjustment case (later the same scenario is applied in experiments of Section 5).

Initially, the *access controller* informs to the *profile descriptor* the current traffic volume of the physical devices. The *profile descriptor* identifies that the traffic volume is higher than the current resource allocation in the slice of the edge network. Next, the *profile descriptor* notifies to the *interaction broker* the current situation, which repasses it to the *resource allocator*. The *resource allocator* evaluates if it is possible to adjust the resource allocation, if it is possible it requests the resource allocation to the *infrastructure handler*.

The *infrastructure handler* performs two tasks:

1 it informs the information about the new resource allocation to the *SLA analyser*, which updates the situation to the *billing counter*

2 it performs the resource allocation update in the SDN infrastructure.

After these steps, the modules confirm the action performed, finishing the process.

Through the steps described, it is possible to adapt the resource allocation and service delivery according to the behaviour of the access network, increasing the QoS/QoE of the users in the access network, as well as avoiding the wastage of resource in the edge network of the MISP.

5 Case study

In this section a case study is presented to evaluate the suitability of IMMI based on a prototype. The experiment consists of monitoring the client's traffic volume (in the access network) and adjusts the resource reservation in the slice deployed over SDN infrastructure when necessary (in the edge network). The usage of IMMI allows these functions to cooperate, aiming to avoid packet loss (lower quality of service delivery) and waste of resources in the MISP (reducing the efficiency of resource allocation, generating lower profits).

In the experiment, the Mininet (http://mininet.org) represents the MISP infrastructure, Ryu (http://osrg.github.io/ryu) was used as controller, while a wireless router acted as access network. The prototype of IMMI was compared against the existing static resource allocation approach (25 Mbps fixed). The experiments were performed 50 times for each case, and are presented with a 95% confidence interval.

Usually, network traffic models apply a exponential distribution to the inter-arrival time and duration of flows, which results in traffic demand. Hence, a set of random UDP flows were injected in the network during 30 seconds, and the following mean values for the exponential distribution were used: 200 Kbps of transmission rate, 100 ms of interval between flows, and 30 seconds of duration per flow.

Figure 5 presents the waste of resources in the experiment. The positive values represent the wastage situation (the allocation of resources is higher than the traffic volume coming from the client), while the negative values depict the QoS degradation situation (the opposite case, allocation is lower than the traffic volume). It can be seen that IMMI keeps the waste of resources very low, avoiding both situations. This occurs due to the capacity of IMMI to interact the functions of access and edge, enabling the edge network being aware what is happening in the access network.

Figure 6 shows the average percentage of loss of all flows that started at each second in the experiment. For example, the loss of the tenth second refers to loss of the flows started at time 10 s regardless its configuration. Thus, Figure 6 illustrates the QoS degradation caused by the difference between the traffic demand and the resource allocation. According to the loss information, IMMI has low loss percentage. This fact happens because

it keeps the allocation higher than the traffic demand (since the management of both edge and access networks are integrated), while the 25 Mbps case experienced higher losses.

Figure 5 Difference between allocation and demand (see online version for colours)

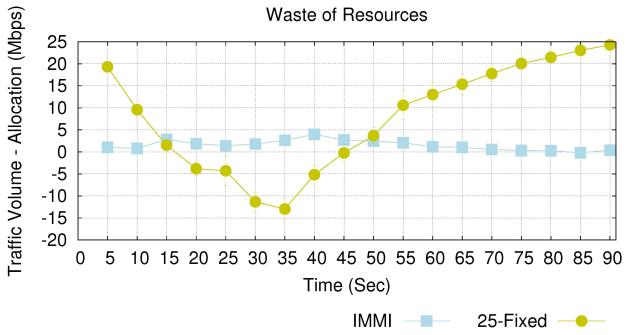
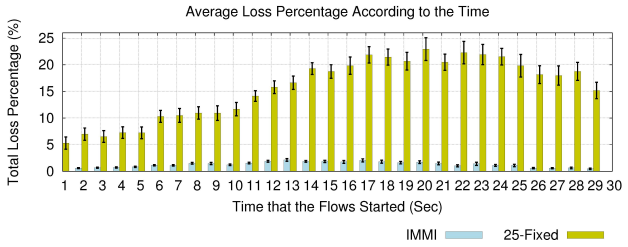


Figure 6 Average loss (see online version for colours)



Based on the experiments, IMMI has showed suitable for managing the MISP infrastructure, achieving the lowest wastage of resources and avoiding the degradation of the QoS experienced by the client. Thus, applying the proposed architecture, the client can keep the QoS level high, while avoiding unnecessary expenses. This better performance of IMMI came from its nature to allow the integration of edge and access networks. Thus, applying IMMI a MISP enables the cooperation between the function deployed in the access and edge networks.

6 Conclusions

Recently, the human society changed the traditional behaviour, starting to use applications that have features like real time communication, multimedia content, and others. As consequence, the internet needs to extend its service delivery. Therefore, this article analysed the current status of the ISPs and the key trends and challenges to be utilised by the MISPs to deal with these new requirements: SDN, NV, and NFV.

In addition, we proposed the architecture for integrated management of modern internet service providers (IMMI) to evolve the management capacity of MISPs, enabling the management of both access and edge networks in an integrated way. The IMMI allows information exchange among edge and access networks, the deployment of slices based on the usage profile of the access network, and the adaptation of the characteristics considering the current state of the MISP infrastructure (edge and access). As future work, we plan to include an end-to-end approach in the architecture.

References

Afolabi, I., Taleb, T., Samdanis, K., Ksentini, A. and Flinck, H. (2018) 'Network slicing and softwarization: a survey on principles, enabling technologies, and solutions', *IEEE Communications Surveys Tutorials*, Vol. 20, No. 3, pp.2429–2453.

Alvizu, R., Maier, G., Kukreja, N., Pattavina, A., Morro, R., Capello, A. and Cavazzoni, C. (2017) 'Comprehensive survey on T-SDN: software-defined networking for transport networks', *IEEE Communications Surveys Tutorials*, Vol. 19, No. 4, pp.2232–2283.

Caballero, P., Banchs, A., de Veciana, G., Costa-Pérez, X. and Azcorra, A. (2018) 'Network slicing for guaranteed rate services: admission control and resource allocation games', *IEEE Transactions on Wireless Communications*, Vol. 17, No. 10, pp.6419–6432.

Doverspike, R.D., Ramakrishnan, K.K. and Chase, C. (2010) 'Structural overview of ISP networks', *Guide to Reliable Internet Services and Applications*, Chapter, pp.19–93, Springer London, London.

Ferrús, R., Sallent, O., Pérez-Romero, J. and Agustí, R. (2018) 'Management of network slicing in 5G radio access networks: functional framework and information models', *CoRR*, abs/1803.01142.

Galdino, G., Gomes, R.L., Bittencourt, L.F. and Madeira, E.R.M. (2020) 'Reliable network slices based on elastic network resource demand', *IEEE/IFIP Network Operations and Management Symposium (NOMS 2020)*.

Gomes, R.L., Bittencourt, L.F., Madeira, E.R.M., Cerqueira, E.C. and Gerla, M. (2016) 'Software defined management of edge as a service networks', *IEEE Transactions on Network and Service Management*, Vol. 13, No. 2, pp.226–239.

Granelli, F., Gebremariam, A.A., Usman, M., Cugini, F., Stamati, V., Alitska, M. and Chatzimisios, P. (2015) 'Software defined and virtualized wireless access in future wireless networks: scenarios and standards', *IEEE Communications Magazine*, Vol. 53, No. 6, pp.26–34.

Han, K., Li, S., Tang, S., Huang, H., Zhao, S., Fu, G. and Zhu, Z. (2018) 'Application-driven end-to-end slicing: when wireless network virtualization orchestrates with NFV-based mobile edge computing', *IEEE Access*, May.

Leconte, M., Paschos, G.S., Mertikopoulos, P. and Kozat, U.C. (2018) 'A resource allocation framework for network slicing', *IEEE INFOCOM 2018 – IEEE Conference on Computer Communications*, pp.2177–2185.

Liang, C. and Yu, F.R. (2015) 'Wireless virtualization for next generation mobile cellular networks', *IEEE Wireless Communications*, Vol. 22, No. 1, pp.61–69.

Ma, Y-W., Chen, J-L., Chang, C-C., Nakao, A. and Yamamoto, S. (2018) 'A novel dynamic resource adjustment architecture for virtual tenant networks in SDN', *Journal of Systems and Software*, Vol. 143, pp.100–115.

Manzalini, A. and Crespi, N. (2016) 'An edge operating system enabling anything-as-a-service', *IEEE Communications Magazine*, Vol. 54, No. 3, pp.62–67.

Mohan, P.M. and Gurusamy, M. (2019) 'Resilient VNF placement for service chain embedding in diversified 5G network slices', *2019 IEEE Global Communications Conference (GLOBECOM)*, pp.1–6.

Ordonez-Lucena, J., Ameigeiras, P., Lopez, D., Ramos-Muñoz, J.J., Lorca, J. and Folgueira, J. (2017) 'Network slicing for 5G with SDN/NFV: concepts, architectures and challenges', *CoRR*, abs/1703.04676.

Son, J. and Buyya, R. (2019) 'Latency-aware virtualized network function provisioning for distributed edge clouds', *Journal of Systems and Software*, Vol. 152, pp.24–31.