The title (Hidden —— No title)

Author: A code to be assigned to you (for blind review by peers)

Abstract:

5G introduced network slicing, enabling the existence of several independent logical networks on top of a physical infrastructure. These logical networks are specially dedicated to meet the performance requirements of heterogeneous 5G use cases. This contradicts the premise of net neutrality, which dictates that all traffic should be treated equally, without discrimination. So, the question arises: How to detect traffic differentiation in a 5G network? To answer this question, this dissertation analyzes the architecture of the 5G network and develops a new approach to the "Network data analytics function" (NWDAF). To develop and test this NWDAF, the 5G core network and its components are emulated, and a new use case is defined.

1 Introduction

5G uses a concept known as network slicing to virtualize the network with dedicated radio and computational resources. These slices are designed to customize certain Quality of Service (QoS) requirements such as throughput, latency, reliability, or connection density to account for the diversity of traffic. The customization of performance parameters in logical networks creates a set of virtual domains that give a different treatment to internet traffic. This creates a potential conflict with the net neutrality principle, which states that all internet traffic should be treated equally. The net neutrality concept is still a polemic subject. More conservative opinions indulge the idea that there should be no exceptions and traffic differentiation should not be allowed, while others support the segmentation of internet traffic into classes, for example. Both points of view seem to agree that net neutrality imposes a non-discriminatory treatment of internet traffic.

Therefore, the research question addressed in this dissertation is the following: How can you identify traffic differentiation in a 5G network in the context of net neutrality? Taking this into consideration, the following objectives were established: a) Define the concept of net neutrality; b) Characterize the 5G network architecture; c) Analyze the "Network data analytics function" (NWDAF); d) simulate the 5G Core Network and its components; e) Define and implement a use case for testing; f) Test and validate the developed function.

To accomplish these objectives, it was developed a "network Data Analytics Function" (NWDAF) specifically aimed at monitoring traffic differentiation that could impact the net neutrality principle. It's important to notice that, as NWDAF is part of the network functions of the 5G network architecture, the data is collected from the inside of the network. As such, the data could be accessible to the telecom regulator. The most critical metrics for detecting traffic differentiation (TD) are packet delay and packet loss. These two indicators allow us to determine whether the ISP has deliberately tampered with the packets in the UPF packet queue. The ISP can purposefully delay packets from a specific content and applications provider (CAP) by using Quality of Service (QoS) techniques such as traffic shaping. They can go even further and discard the packets entirely. The purpose is to detect these activities using the measurements provided by the Operations, Administration and Maintenance (OAM) service.

As a use case, two flows from two separate CAPs will be monitored. A YouTube and a Netflix traffic flow will be created, with one of them facing throttling. Throttling is an

intentional degradation in network performance for a given service, application, or class of applications. Everything will be done remotely, in simulations, on top of a virtual 5G Core Network. Then, by comparing the two flows, the NWDAF should be able to detect the TD and report back to the telecom regulator.

If done successfully, this will represent an innovative way to use the NWDAF, and, most importantly, it will enable the detection of traffic differentiation (TD) practices inside the network. This is a game changer, as ISPs will not be able to justify allegedly discriminative traffic practices as being unknown network behavior.

In section 2, a brief introduction of three of the major themes of this dissertation is done. First, the definition of net neutrality and Traffic differentiation (TD) is presented. Then, the next subsection is about 5G, with special focus on network slices, Network Functions (NFs) and the 5G network architecture. Lastly it's briefly explained what is NWDAF, what it does and how it can obtain analytics from the network.

Section 3 talks about what is being implemented and what is possibly going to be implemented in the future.

2 Network neutrality,5G and Network Data Analytics Function overview

2.1 Network Neutrality

Net Neutrality states that all internet traffic, regardless of origin, destination, or content, should be treated equally. ISPs feel compelled to apply discriminatory traffic management practices to obtain a competitive advantage over the competitors, increase the number of customers, or charge higher fees. Discriminatory traffic management practices are often called Traffic Differentiation (TD). In some cases, TD can be considered reasonable and allowed, as long as it is transparent, such as i) Addressing illegal content (piracy, spam, or viruses); ii) Prioritizing DNS queries; and iii) Prioritizing special services, e.g., real-time health services. In general, TD can be seen as reasonable if it is beneficial to the network and its users as a whole. However, TD is detrimental to innovation, fair competition, and consumers' freedom of choice, three important factors deemed essential for the success of the Internet.

The issue with TD emerges while attempting to detect it. Three major factors offer a problem: 1) Detect TD as an external observer with no access to the network configurations; 2) Detect TD with only features of the network (source address, destination address, port); 3) Identify which features trigger TD and where it's happening.

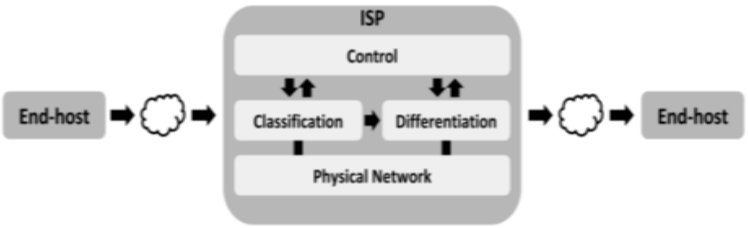

Figure 1: High-level description of TD on an ISP network [1]

Figure 1 exemplifies how an ISP can affect traffic between two end-hosts. Any traffic traversing through the ISP is classified and handled accordingly to the assigned class.The classification of the internet traffic can be based on several criteria, such as: 1) TCP/UDP port, which may contain information about the traffic type; 2) Source address; 3) Destination address; 4) Application protocol.

Just like the Internet, the TD mechanisms used by ISPs are continuously evolving. Traffic characteristics, such as payload and port, can be used by commercial traffic shapers to determine many applications. Still, newer technologies like software defined networking (SDN), will increase the flexibility and will enable various types of discriminatory behaviors to be easily implemented in the network. TD detection mechanisms will have to be ale to adapt to the evolution of networks.

Overall, network neutrality is a topic that is getting a lot of notoriety, as all around the world, regulations are implemented and withdraw.[1]

2.2 5G

5G network slices are designed with the goal of optimizing the priorities of traffic. As such, they aim at providing low latency, high data rates, reliability and a huge number of connected devices. The three main 5G network slices are: enhanced Mobile Broadband (eMBB), massive Machine-Type Communications (mMTC), and Ultra-Reliable and Low-Latency Communications (URLLC). eMBB corresponds to services that enable the transfer of large amounts of data for an improved user experience. mMTC corresponds to services designed to server a massive number of connected devices (IoT), which have low cost and consume very little energy. URLLC was projected for services that require ultra reliability and low latency. *Figure 2* showcases some use cases for each of the three mentioned network slices.

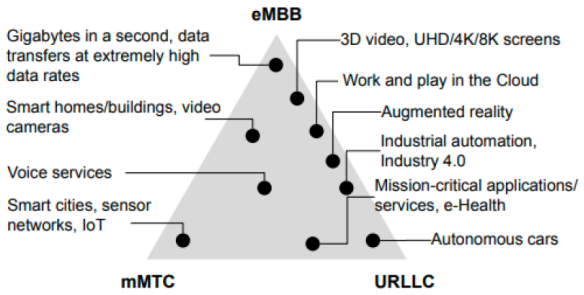

Figure 2: 5G eMBB, URLLC, and mMTC network slices use cases [2]

When it comes to its architecture, the 5G network can be decomposed into two planes: control plane and data plane. These two planes are independent, and they are connected by numerous interfaces. To provide scalability, evolution and flexible deployments, their functions are divided. Software-Defined Networking (SDN) makes this possible, by logically separating the two planes. The data plane, also known as user plane, has three main components: User Equipment (UE), Radio Access Network (RAN), and UPF. The UE connects to the UPF through the RAN. The UPF acts as a router to the Internet. The data plane is the part of the 5G network responsible for the transportation of packets. The two planes, their main functions and the dissociation between the access network and Core network is shown in *Figure 3*.

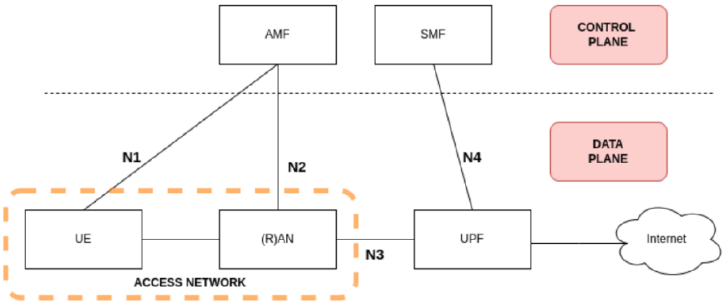

Figure 3: 5G network architecture [2]

The UPF acts as a gateway between the RAN and the internet. As stated above, the UPF acts like a router, so it also has the functions of routing and forwarding packets. Quality of service (QoS) is also handled by the UPF. All the radio networking is ensured by the RAN. The RAN is primarily composed of a node, called gnB. The gnB is responsible for establishing connection between the UE and the core Network.

The main functions of the control plane are the Access and Mobility Management Function (AMF) and the Session Management Function (SMF). The AMF is responsible for access control and UE location management, while the SMF is in charge of managing sessions between the UE and the UPF. The control plane functions are all virtualized, and they behave like web services. They are called Network Functions (NFs) and they are all independent of each other.

Essentially, the 5G Core network can be seen as a set of independent Web services that communicate with each other using HTTP, over the standard TCP/IP protocol stack. The HTTP protocol includes a set of methods that perform various tasks. The six main HTTP methods are: 1) GET, which is used to read a resource; 2) POST, which is used to create a resource; 3) PATCH, used to alter a portion of a resource; 4) DELETE, used to delete a resource; 5) PUT, used to update the full resource; 6) OPTIONS, used to obtain information about a resource.[2]

2.3 NWDAF

The Network Data Analytics function (NWDAF) is one of the Network Functions (NFs) of the 5G network and is able to provide analytics information to an NF consumer. Usually, an NF consumer is another NF of the 5G Network. The NWDAF is capable of getting analytics information about the network such as: 1) Slice load level analytics; 2) Observed Service Experience analytics; 3) NF load analytics; 4) Network Performance analytics; 5) UE related analytics; 6) User Data Congestion analytics; 7) QoS Sustainability analytics.

The NWDAF, just like other NFs of the Core Network, uses a subscribe/unsubscribe methodology. It can subscribe to specific events and receive notifications about them. As stated earlier, the NFs are basically web servers that interact with each other via HTTP (HTPP/2 more specifically). As such, the NWDAF uses an HTTP/2 based API to communicate with other NFs. It's important to note that the NWDAF can also subscribe to other NFs, and act as a consumer. That is how NWDAF is able to get analytics information from the network.

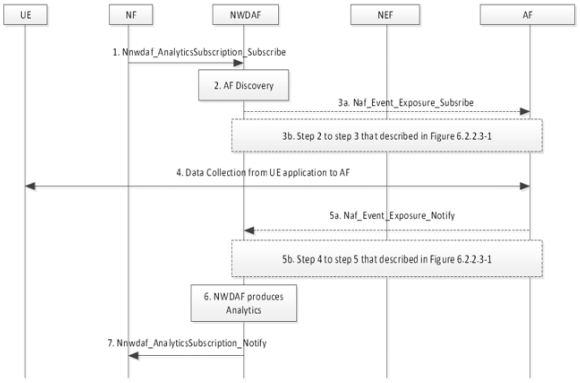

Figure 4: Data collection procedure from UE [3]

Figure 4 shows how a NF can obtain analytic data about a User equipment (UE) from the NWDAF. It can be observed that the NWDAF can obtain information from other NFs (acting like a NF consumer), but it can also provide information for other NFs.

1) An NF subscribes to analytics from the NWDAF; 2) NWDAF discovers the Application Function (AF) that provides data collection; 3) NWDAF subscribes to the AF for UE data collection; 4) The AF collects the UE data; 5) The AF receives the input data from the UE, and processes the data. The AF then notifies the NWDAF on the processed data; 6) The NWDAF produces analytics using the UE data received from the AF; 7) The NWDAF provides analytics to the consumer NF.

The NWDAF also has Machine Learning (ML) services. It follows the same subscribe/unsubscribe paradigm. A consumer can be notified when an ML model matching the subscription parameters becomes available, and it can also provide information about the ML model.[3]

3 Conclusion

The main objective of this research is to get to a point where the NWDAF is able to detect traffic differentiation for a specific eMBB scenario. However, that alone is already a good breakthrough, taking into account that NWDAF being used to check for net neutrality compliance is unheard of.

For future work, the virtualization of the network will be implemented using the most suitable software for the task. Once that is done, other types of traffic might be tested (the NWDAF might have to be re-adjusted). Also, the ML capabilities of the NWDAF can be explored to help improve the automation of the network.

4 References

[1] T. Garrett, L. Setenareski, L. Peres, L. Bona, and E. Duarte, "Monitoring network neutrality: A survey on traffic differentiation detection," *IEEE Communications Surveys and Tutorials*, vol. 20, pp. 2486–2517, 3 2018. DOI: 10.1109/COMST.2018.2812641.

[2] D. M. de Almeida Coimbra Maia, "Control and positioning of a 5g radio access node deployed in a mobile robotic platform," Portuguese, Ph.D. dissertation, 2022.

[3] 3GPP, "5G;Architecture enhancements for 5G System (5GS) to support network data analytics services," no. 23.288, Mar. 2022, Version 17.4.0. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3579.