sciendo

Műszaki Tudományos Közlemények vol. 13. (2020) 101–104.
DOI: Hungarian: https://doi.org/10.33895/mtk-2020.13.17
English: https://doi.org/10.33894/mtk-2020.13.17

EME MTSZ MTK

SDMN ARCHITECTURE IN 5G

Márk KOVÁCS,[1] Péter András AGG,[2] Zsolt Csaba JOHANYÁK[3]

John von Neumann University, GAMF Faculty of Engineering and Computer Science, Kecskemét, Hungary

[1] *kovacs.mark@gamf.uni-neumann.hu*

[2] *agg.peter@gamf.uni-neumann.hu*

[3] *johanyak.csaba@gamf.uni-neumann.hu*

Abstract

Due to the exponentially growing number of mobile devices connected to the Internet, the current 4G LTE-A mobile network will no longer be able to serve the nearly 5 billion mobile devices. With the advent of the fifth generation, however, the number of cybercrimes may increase. This requires building an architecture that can adequately protect against these attacks. For wired networks, the SDN-type architecture has been introduced for some time. As a result, a similar design concept has emerged, which is called Software Defined Mobile Networks (SDMN). This article describes this technology and how it helps prevents DoS, DDoS at-tacks, and IP source spoofing.

Keywords*: SDN, 5G, NFV, SDMN, security.*

1. Software Defined Networks (SDN)

One of the most widespread and effective networking solutions today is Software Defined Networks (SDN) [1]. The major innovation of SDN over conventional networks is that it separates the control plane from the data plane. With this approach, centralized control plays an important role. For SDN networks, three major layers are distinguished: the data plane, the control plane, and the application plane.

In the data plane, there are switches and routers (also known as SDN switches) which are responsible only for delivering packets to the destination address on the basis of a higher command received from the control plane. Instructions are received through the so-called Southbound Interface, which requires the devices to be OpenFlow [2] compatible.

The control plane provides automatic configuration of the network, dynamic access and control according to needs, with the help of the programs used here. One of the most important layers of this plane is virtualization, but this is not to be confused with network function virtualization (NFV [3], Network Function virtualization). (The relationship between SDN and NFV is discussed below.) In this plane, there is a Network Operating System, which provides solutions to any network management problems that may arise. The control plane is in direct contact with the third plane of the SDN, the so-called application plane. The North-bound Interface is responsible for communication between them.

The third plane of the SDN is the application plane, which has three sub-layers: Language-based virtualization, Programming languages, and Network Applications. Their task is to issue the appropriate instructions to the controller to ensure fast and reliable communication under central supervision.

2. SDN and NFV

Network function virtualization is often referred together with SDN, but actually they are not interdependent. There is a relationship between the two solutions, but we could say that they are complementary.

SDN virtualizes network devices (switches, routers), uses cheaper, faster, centrally controlled hardware instead of traditional transmission de-

vices and of course, one or more control controllers to provide appropriate centralized protection and responsiveness to user needs.

NFV prioritizes the virtualization of network functions. It provides virtualization with quick deployment, cost savings and flexibility. It allows us to run software services that were previously implemented in hardware. (e.g. Network Address Translation (NAT), Firewall Services, DHCP). It is important to note that in order to implement NFV services, any IP network can be used, not necessarily an SDN network.

3. Shortcomings of current cellular networks

Mobile communication began in the 1980s, and at that time it was used exclusively for voice calls at a data rate of only 56 kbps. Nowadays, however, this rudimentary service has evolved into a separate large network that is capable of connecting to the Internet and, as a result, is used, in addition to voice calls, for video calls, high definition online video streaming, and online games [5].

There are several disadvantages to today's mobile networks, such as:

- *Lack of appropriate scalability*: rapid traffic growth is expected due to mobile services requiring new bandwidth, which is too inflexible for current static networks, and will be too costly to operate in the future.
- *Complex Network Management*: Physical network devices do not have a common control interface, so even a small task requires great expertise.
- *Manual Network Configuration:* One needs to configure everything manually. This requires a lot of expert knowledge and work from operators, and is the cause of most system crashes.
- *Complex and expensive network devices*: Some devices have to perform too many tasks, such as traffic monitoring, billing, QoS, or parental controls, which increase the complexity and cost of the device.
- *High costs:* Operators are unable to reconcile assets from different cheaper manufacturers, which increases costs and, due to manual setup and inflexibility, high operational costs.
- *Rigidity*: Due to the long process of standardization, the introduction of a new service takes a long time

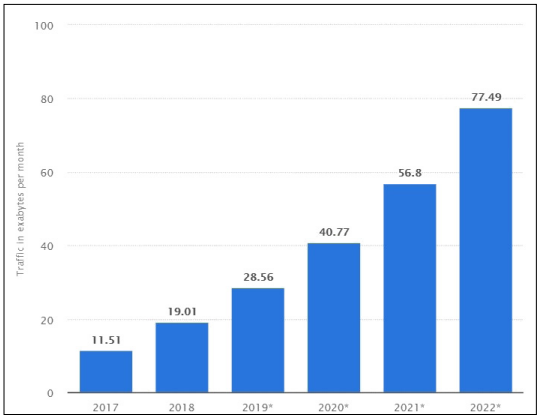

Figure 1. *Global mobile data traffic between 2017 and 2022.* [4]

4. Software defined mobile networks (SDMN)

SDN was originally designed for wired networks; however, system developers have noticed the possibility that this solution may work in a wireless environment as well.

SDMN is a programmable, flexible, and traffic-centric network construction consisting of a combination of SDN, NFV, and cloud computing. It differs from existing mobile networks in that it integrates expensive hardware devices with a traffic-based model and places a centralized logic controller for optimal operation.

Similar to SDN SDMN also has three parts, which are the data plane, the control plane, and the application plane.

Unfortunately, the SDN concept does not solve all the problems mentioned in the previous chapter, but it does increase flexibility, scalability and thus performance. It directs the current mobile network towards a traffic-centric model that utilizes cheap hardware and logically centralized control.

SDN-compatible switches, routers, and gateways can be controlled via the SDN controller and the network operating system (NOS). The controller can be deployed as a plane virtual component in an operator cloud. **Figure 2.** illustrates the structure of the SDMN [7].

4.1. DP layer

It is also commonly referred to as the infrastructure layer, where network devices such as switches and routers are located. The base stations are connected to limit switch data plane switches.

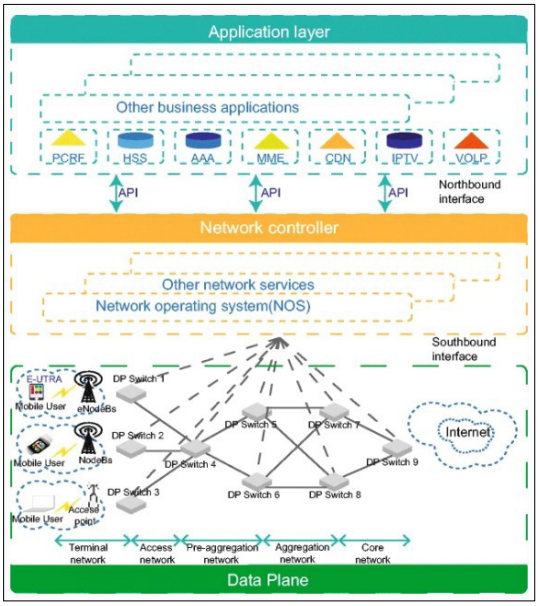

Figure 2. *SDMN architecture.* [6]

The other side's interfaces are connected to the Internet,

4.2. Network controller

The logically centralized controller is used to configure and control the DP devices. It uses a control protocol, such as OpenFlow, to access DP elements and install traffic controls. Like the SDN architecture, the network controller and the DP layer are interconnected by so-called southward APIs. The controller runs NOS to support the control services.

4.3. Application layer

All the control and business applications such as policy, subscriber server, authentication, authorization and accounting can be found here. The node-bound API provides the connection between the application layer and the network controller.

5. Security flaws

Vulnerabilities originating from SDN can also be found in SDMN:

– Centralized management integrates network configuration, network service access control and service deployment on the control layer. If an attacker successfully obtains control of SDN, the network service will be paralyzed, and the entire network will be affected [8].
– The main problem with SDN's programmability is trust based on third-party applications and controls. Because of the risk of malicious applications, the authentication process between the application and the control layers must be strengthened to protect the controller.
– The combination of NFV and SDN can represent a series of security problems. Examples include OpenFlow, NFV, software-defined fronthaul network security issues and terminal issues, etc. In the case of a software-defined fronthaul, virtualized attack poses a threat.
– For software-defined Front-haul (SDF) wireless programs, SDMN security threats include launching wireless media and recognizing the attack surface. Some radio frequency interference, MAC counterfeiting, and malicious RF interference can adapt. [10]

Of course, researchers are already working on these issues to develop a more secure architecture

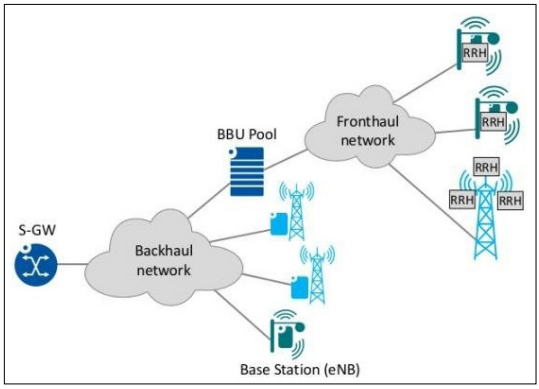

Figure 3. *Connection between Backhaul and Fronthaul networks.* [9]

Conclusion

With increasing traffic, there is a growing need for a well-designed network architecture to include mobile networks. As a result, much research is underway to develop well-designed yet secure technologies for next-generation technology

Acknowledgement

This research is supported by EFOP-3.6.1-16-2016-00006 "The development and enhancement of the research potential at John von Neumann University" project. The Project is supported by the Hungarian Government and co-financed by the European Social Fund.

References

[1] Ramos F. M. V., Kreutz D., Verissimo P.: *Software-defined networks: On the road to the softwarization of networking*. Agile Product Management & Software Engineering Excellence, Business Technology & Digital Transformation Strategies Cutter Business Technology Journal, 28. (2015) 6–13.

[2] Lara A., Kolasani A., Ramamurthy B.: *Network innovation using OpenFlow: A survey*. IEEE Communications Surveys & Tutorials, 16/1 (2014), 493–512.

[3] Bo Han, Vijay Gopalakrishnan, Lusheng Ji, Seungjoon Lee: *Network function virtualization: Challenges and opportunities for innovations.* IEEE Communications Magazine 53/2. (2015) 90–97. DOI: 10.1109/MCOM.2015.7045396

[4] Statista: *Global mobile data traffic from 2017 to 2022*. (letöltve: 2020. február 20). https://www.statista.com/statistics/271405/global-mobile-data-traffic-forecast/

[5] Militano L., Araniti G., Condoluci M., Farris I., Iera A.: *Device-to-Device Communications for 5G Internet of Things*. EAI Endorsed Transactions on Internet of Things 1/1. (2015) 150598. https://doi.org/10.4108/eai.26-10-2015.150598

[6] Chen, M., Qian, Y., Mao, S. et al. Software-Defined Mobile Networks Security. Mobile Netw Appl 21, 729–743 (2016). https://doi.org/10.1007/s11036-015-0665-5

[7] Liyanage M., Gurtov A., Ylianttila M.: *Software Defined Mobile networks (SDMN) Beyond LTE network architecture*. Wiley, 2015.

[8] Ji, X., Huang, K., Jin, L. et al.: *Overview of 5G security technology.* Sci. China Inf. Sci. 61, 081301 (2018). https://doi.org/10.1007/s11432-017-9426-4

[9] Hailu D. H., lema G. G., Bjørnstad S.: *Performance Evaluation of Ethernet Network for Mobile Fronthual Networks*. IJEESC 7/1. (2017) 287–298.

[10] Liyanage M. et al.: *Enhancing Security of Software Defined Mobile Networks.* IEEE Access, 5 (2017) 9422–9438.