A CANVAS OF 5G NETWORK SLICING: ARCHITECTURE AND SECURITY CONCERN

Chandini
School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India

Sahil Verma
School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India

Kavita
School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India

M N Talib
Papua New Guinea University of Technology, Lae, PNG

Gagandeep Kaur
School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India

NZ. Jhanji
School of Computer Science and Engineering, Taylor’s University, Malaysia

Corresponding author: sahilverma@ieee.org

Abstract— Multi-services with different configurations are contemplated in the fifth generation abbreviated as 5G and even beyond networks. Network slicing is described as a key infrastructure that facilitates integrated service in associations with 5G networks. Network slice makes the transition to a NaaS from a network-as-infrastructure structure to support several smart 5G networks with different specifications. Via network slicing, service providers could perhaps flexibly and easily deliver their software and services to meet unique demands of a variety of services, including virtual and augmented reality, video gaming, e-health, and several others. Security is one of the main factors that must be taken into account, like all emerging innovations. The protection of 5G network slicing is illustrated in this paper.

Keywords—5G network slicing, Software- Defined Network, Network Function Virtualization, security, MANO

I. INTRODUCTION

Mobile networks of the fifth generation (5G) push the network paradigm into the automated function network. The network infrastructure is very dynamic and incorporates heterogeneous interaction and networking technology [1]. In addition, 5G provides capacity, efficiency as well as spectrum access in the segments of radio network, combined with native versatility including conversion of programming in all branches of the non-radio network [2]. Three key areas such as the most persuasive 5G cases are established are massive IOT (Internet of Things), mobile broadband and the last one is critical communication in which every segment has various levels of latency requirements, robustness, capacity, and versatility[3]. For example, smart city framework need large connection and voluminous capacity. The "one-fits-all" kind’s architectural design is not, under certain conditions, adequate and effective to meet the various needs of 5G networks that have very diverse demands.

Thus a new framework for the mobile grid, network slicing (NS), is envisaged in implementation of 5G, that is critically based on Cloud Computing(CC), Software- Defined Network(SDN) as well as Network Function Virtualization (NFV). The word “Slice” by theory, a slice is a logical structure, which has certain network functionalities and features, offering versatile solutions to different business situations that have various functional, efficiency and resource allocation criteria[4](International Telecommunications Union 2017). In essence, NS offers differentiated services for various network traffic groups running on the same networks at the same time. Network slicing is perhaps a philosophy for the delivery of distinct 5G networks in the very same structure. The functionality (for example mobility, protection, control) and efficiency (for example, delay, performance, error rates, robustness and availability) can be differentiated. A network slice aspect is a logical network end-to - end instance customized to meet the required networking features and provide specialized services for special use cases such as speech communication, streaming media, e-health, and communication between vehicles.
Fig. 1. Network slicing in 5G (where each slice contribute to different functionality)

The devoted resources will adjust as needs alter. The slicing of network allows the construction of slices for functional, self-contained, and segmented network operations utilizing available resources, like storage and processors. Essentially, network slicing enables several virtual networks to be incorporated into a common network hardware. Physical resources are tertiary under this virtualized network situation, whereas logical (software-based) modules are the main component, and dynamically devote resources to certain applications as required.

II. LITERATURE REVIEW

Latif U.Khan et.al [6] have presented and identified important recent network slicing advancements in making smart applications for the IOT. A taxonomy is built with various parameters in mind: main creation concepts, enablers, resource slicing stages, chaining schemes for service operations, physical systems and security. In addition, the author talked about precise specifications in order to allow smart services in network slicing. Finally, the author have address some active research challenges and including potential network slicing guidance.

Pawani Porambage and Madhusanka Liyanage [7] have deeply discussed that 5G would enable attackers to enforce ultra-low latency feature of the identical high-speed safety risks. Thus, NS would also need proactive safety measures as a main drivers of 5G because the reaction would be too late. The security flaws that are implicit in NS architecture's multiple logical functions can also put NSI life span at pressure. Taking into account the implications and the pertinence of NS security attacks, strong separation of slices is the safest way to minimize much of the risks.

Michel Bonfim et.al [8] advocated FrameRTP4, A framework to provide mechanisms for detecting and mitigating attacks in 5G NS environments in real-time. To do this, it implements the SDN infrastructure by dividing the problem solutions into data plane as well as control planes. FrameRTP4 Transfer includes a personalizable P4 programme for the data plane to enforce the SFC protocol interface to handle the lifecycle of NS instances.

Ruxandra F.Olimid and Gianfranco Nencioni [9] proposed a clear overview of security aspect of 5G network slicing. Network slicing will indeed allow the 5G networks to deliver a heterogeneous service in
a scalable and productive manner. The author has focused on 5G network slicing protection and have emphasized risks and guidelines in terms of protection during the life-cycle, intra and inter-slice security.

Vitor A. Cunha et.al [10] addressed the primary safety issues in the use of packet core network slices, the strategies offered by the academia and practitioners, and illuminate several directions to follow. The problems that have been established can be classic and nontrivial. There are already some common problems, such as shared authentication protocols, security frameworks and data security / verification steps.

III. NS ARCHITECTURE AND FUNDAMENTAL NOMUNCLATURE

A. NS Architecture

The all-inclusive framework of network slice consist of major three modules [9], each module have their own working and management in the network as presented in Fig. 2.

- **RESOURCE LAYER:** The bottom layer is made up of network infrastructure and network roles to support a target audience on request. The network services and services can be either physical or logical / virtual. Resource examples require nodes for computing, transformation and transmission. Network features include switching, filtering, slice selection and verification features. One or even more network slice variants may be used by a service or even a network function [11].

- **NS INSTANCE SLICE:** The intermediate layer is composed of slice where the network bandwidth for the services instances can be given by a slice. A slice can operate either on or over the network services, and it can support one or more instances of operation. Two different slice could or could not operate in the same hardware design, and either share or otherwise network support functions and resources.
• SERVICE INSTANCE LAYER: - The top layer includes instances of service which consume the slices and which are provided to customers. Often, referred as a service instance simply by service for the ease of visibility.

B. Software defined networking (SDN)

Software-defined networking (SDN) is very much the differentiation from its forwarding features of its control functions to allow for increased network automation and network programming. The network function virtualization which is abbreviated as NFV also blends network functions with hardware as virtualized network functions. SDN supports network-like cloud computing. This helps system administrators and management to easily reflect changes in business needs via a standardized control console that has been obfuscated from the network's actual hardware. In a nutshell, SDN produces a core network brain that is able to connect and monitor the parts of the system.

Fig. 3. SDN Layered Framework

SDN three layer architecture involve [12]:

• Infrastructure Layer: Involve all the assisting physical hardware such as switches and routers. This is the physical category that will allow network virtualization across the control layer (in which SDN controllers are located and handle the physical network underneath).

• Control Layer: Is a control planes in which intelligent reasoning will exist in the charge of network connectivity within the SDN controllers. That's an environment in which each network provider works to create its own SDN controller as well as framework products. A number of industrial logic is written in this layer to locate and manage various forms of network information, data about the environment, topology, statistical information and more in the controller. Control layer is categorize in two variation of interfaces:
  ▪ Northbound interface: is intended for topmost, application layer communication which can in general be performed via controller REST APIs.
  ▪ Southbound interface: The communication is structured to be performed in general via south bound standards-Openflow, Netconf, Ovsdb, and many more-with the lower, network aspect connectivity layer.
• Application Layer: The field to create as creative framework as possible is open to the use of any network topology, network status, network statistics etc, and network details. Applications such as Network integration, setup and maintenance of the network, network control, network troubleshooting, network policy and security can be built in many different forms. These SDN applications will offer multiple end-to - end applications to networks in real-world enterprises and centers.

C. Network Functions Virtualization (NFV)

Virtualization Network Functions (NFV) disconnects network functions from hardware machine and runs on virtual machines (VMs) as applications. NFVs are named for various functionality including the firewalls, traffic management and virtual routing [13].

The purpose of NFV should be to revolutionize the structure of networks and services. With NFV, any organization can automate a broad range of network functions and optimize performance and provide new revenue generation applications more efficiently and conveniently than ever before. NFV is a crucial activated device to virtualize all the different devices in a network in the forthcoming 5 G networks. NFV allows network slicing in 5 G – an element of the virtual network architecture which enables many virtual networks to just be built with a single physical infrastructure.

D. MANO

MANO is an abbreviation for slicing management and orchestration is a essential component of network slicing layout. It implements and arranges NFV-MANO in a manner that combines hardware components, virtual resources, including network slices. Slicing MANO may have sub-tasks like server management, VNF management and orchestrator slices. The MANO scale tasks include: (1) the development and management with the help of infrastructure tools for VM instances. (2) Mapping virtual resource network functions and building network access chains by linking network functions. (3) Management of the development process of network slices through communicating with the device and process layer, i.e. through automating service-oriented diagram development and complex maintenance by process and virtual resource monitoring criteria.
IV. SECURITY ASPECT OF NETWORK SLICE

Infrastructural and operational sharing provides cost and resource management benefits but also poses problems that must be overcome. In particular as in multi-tenancy sense, security and privacy dimensions of network slice need to be explained. If not, the impacts Perhaps hard. Taking this into account we have presented a table of security threats along with the alleviation techniques for the network slicing [9][20]. Besides of that security issues generally in 5G are highly considered [21-23]. In addition, 5G dependent IoT based applications such as E-health, and community applications, 5G plays an important role [24-25], will have higher boost using 5G. Security and privacy issues [26] will also increase with this growth.

| Broad-class       | Sub-Class                             | Elucidation                                                                 | Alleviation Technique                                                                 |
|-------------------|---------------------------------------|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Slice longevity   | Preparation stage                     | • The principal attack point during the preparation is the slice prototype for the network. All the built-in slices of the network are influenced by an incorrectly constructed, abused, or poorly deployed blueprint (e.g., a hardware error, no up-to-date maintenance activities, or malware injected). • Besides the critical information may also be exposed through intense aggressive assaults, which may harm the reliability of a design, content disclosure. | • Includes methods to restrain examining templates. • Network slice models are generated using cryptographic protocols for confidentiality (for both transmission as well as storage). It must also be checked that the network slice prototype is correct. • At the period of template implementation, real-time protection monitoring can be used as a good practice [14]. |
| SLICE SECURITY    | Induction, configuration and activation stage | • The key threats during the second step are to build fake slices or to alter slice settings before or after or sometime during the activation. • A normal attack point in this step is the API, which will undermine the installation, setup, or triggering of a slice by an enemy. | Includes access and operating rights frameworks for API secure. The use of TLS (collaborative authentication) either O-Auth (authorization of requests for service) are sound strategies. In addition, the API must facilitate reliable checks, logging and monitoring (e.g. traffic reports, invocation of the APIs). During the first stage, general cryptography and security research are also effective throughout the second phase, also. |
|                   | Run-Time stage                        | • The most significant risks, including Denial of Service (DOS), productivity attacks, data leakage and privacy breaches are revealed during this process. • In comparison, risks relating to administration, such as unwanted configuration modifications, occur in time and new risks including discontinuation of the slice emerge. • In this step, the API and the services that process the slice remain a big attack point. | In order for a network slice to avoid false or changed instances [15], the validity and integrity checking is needed here. For Distributed DOS (DDoS), slice isolation is considered to have basic mitigation methods [16]. Dynamic NFV that allow for on-demand protection frameworks has yet to be investigated but is a reasonable candidate for run-time safety mitigation. |
|                   | Decommissioning stage                 | • Throughout so after the slices have been deactivated, the principal hazard is to reveal confidential data stored illegally during decommissioning. • A second possibility is the illegal use of resources to initiate a DOS attack. | Require the removal of confidential information and de-allocation of network and resource functions, to prevent them from being active. During the entire life cycle of a slice, security, integrity and replay must be secured (for instance TLS) as the interaction interface being used slice management. |
| Broad-class          | Sub-Class          | Elucidation                                                                                                                                                                                                 | Alleviation Technique                                                                                                                                                                                                                     |
|---------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Intra-slice         | 5G user devices    | • Customer devices are an open point of attack, aside from the corporate security used mainly by non-technical consumers.                                                                             | • This must ensure that only approved parties can build, alter, and erase instances of network slice [17].                                                                                                                                  |
|                     |                    | • Illegal activity to slices or facilities requires direct risks.                                                                                                                                     | • In addition, it is incredibly necessary to monitor and audit.                                                                                                                                                                           |
|                     |                    | • Besides economic and privacy concerns and secrecy, unauthorized disclosure affects resource usage and thus therefore makes DOS attacks possible.                                                         | • Includes solid 5G customer machine authentication and access protection.                                                                                                                                                                  |
|                     |                    | • Furthermore, it could itself contribute to Consumer privacy issues merely by adding to a slice.                                                                                                        | • A secondary identification (or slice-specific identification) only at slice level would be recommended as well as primary authentication which enables users to connect the network.  |
| Slice services       |                    | • The communication in both the slice as well as the resources receiving the slice is one potential point of attack.                                                                                  | • Appropriate security standards deployment and proper application setup (e.g. limits on privileges and resources).                                                                                                                        |
| interface            |                    | • More specifically, by targeting a service, an opponent could impact the division. This could lead to other facilities on the same slice being impaired.                                                 | • An accurate degree of isolation between providers and between slice and consuming services is important.                                                                                                                           |
| Sub-Slices           |                    | • The sub-slice itself and the interrelationships among the sub-slice constitute an attack point when the slice is identified as a multiple sub-slice chain.                                                  |                                                                                                                                                                                                                                         |
|                     |                    | • The overall security standard is determined by the poorest sub-slice in the sub-slice series.                                                                                                         |                                                                                                                                                                                                                                         |
| Slice manager        |                    | • Problems of security related to network slice templates, plugins, access privileges, authentication mechanisms, trust, etc.                                                                         | • Protecting sub-slices and frameworks for enforcing to reduce risks at interoperability, notably if a non-3GPP access network.                                                                                                            |
| Resources and        |                    | • Slices that absorb (resources and network) can be threatened by resources and network operations.                                                                                                       | • Future work is also under way to explore security problems for the interconnection of various technology and further research must be conducted on RAN sub-slice [18].                                                                 |
| network operations   |                    | • A wide range of threats, including physical, technological and general cyber-attacks, may take place.                                                                                            |                                                                                                                                                                                                                                         |
| Inter-slice          | Service-service     | • The interface among services which consume numerous slices is a potential line of focus.                                                                                                             | • Integrity verification                                                                                                                                                                                                                 |
| security             | interaction         | • More specifically, an opponent might disrupt other services running on top of many other slices by disrupting those services.                                                                       | • Credential access                                                                                                                                                                                                                        |
|                     |                    |                                                                                                                                                                                                  | • Mutual authentication                                                                                                                                                                                                                   |
|                     |                    |                                                                                                                                                                                                  | • Physical security                                                                                                                                                                                                                     |
|                     |                    |                                                                                                                                                                                                  | • Secure boot                                                                                                                                                                                                                           |

7
Resource infrastructure | A resource layer is not only an attachment point for exhaustive use or DOS, as well as for device attacks. • An enemy, for example, can enter and manipulate code over one slice, triggering execution changes in all other slices with the same code. | code security methodology, code isolation
Management systems | A line of contact is the management system. A tenant may try accessing slices of other tenants, or adjust the parameters of various tenants’s slices. | Slice isolation
[24] Alshammari, M. O., Almulhem, A. A., & Zaman, N. (2017). Internet of Things (IoT): Charity Automation. International Journal of Advanced Computer Science and Applications (IJACSA), 8(2).

[25] Hussain, S. J., Irfan, M., Jhanjhi, N. Z., Hussain, K., & Humayun, M. (2020). Performance Enhancement in Wireless Body Area Networks with Secure Communication. Wireless Personal Communications, 1-22.

[26] Fong, Teoh joo, Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). The Coin Passcode: A Shoulder-Surfing Proof Graphical Password Authentication Model for Mobile Devices The Next Generation Swift and Secured Mobile Passcode Authenticator. INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 10(1), 302-308.