IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 7, Issue 6 - V7I6-1305)
Available online at: https://www.ijariit.com

Study of 5G network slicing

Juhi Singh
juhisi.94@gmail.com
GLA University, Mathura, Uttar Pradesh

ABSTRACT

Network operators deploys currently 5th generation (5G) of cellular network and many manufacturers commercialized new 5G end-user devices. It is the first step in the development of 5G still the 5G potential is far from being reached. Network slicing is the one of the main 5G technologies for the researcher's community. Many heterogeneous services like voice communication, video streaming, e-health, vehicular communication are provided and flexibly by exploiting the 5G infrastructure. Security is the critical aspect like a every new technology. In this paper, security in 5G network slicing is highlighted life-cycle security, intra-slice security and inter-slice security along with threats and recommendations are highlighted in this paper.

***Keywords**— 5G, Network slicing, security*

1. INTRODUCTION

As compared to 4G, 5G is the evolution in terms of performance parameter which is already released in the market. But 5G is under investigation for the researcher and work is in progress by standard organization [1], [2]. Services like voice communication, video streaming, e-health, vehicular communication all these are differentiated services are coming under infrastructure of 5G. Network slicing is the challenging target for 5G network to be accomplished [3]. Currently, network slicing is one of the topics targeted in the 3rd Generation Partnership Project (3GPP) release 14[1] and further addressed in 3GPP release 15[2] still they are in progress and soon to be completed may be in 2021.This time motivates the investigation in respect of network slicing.

Under virtualization networking, network slicing is one of the category, together with Software Defined Networking (SDN) and Network Function Virtualization (NFV). Network slicing is one of the independent technology which takes the advantages of SDN and NFV. It allows the flexible and efficient creation of specialized end-to-end logical networks on top of shared network infrastructure. Specific type of services is accommodated by each of these logical networks with different and heterogeneous requirements through which vertical industries are being facilitated. In [4], three main 5G use cases are being specified by International Telecommunication (ITU) and 3GPP and these are:

- Enhanced mobile broadband (eMBB)
- Ultra-reliable low latency communication (URLLC)
- Massive machine type communication(mMTC)

There is an advantage of infrastructural and functional sharing in terms of cost and resource consumption, but at same time, it raises issues that have to be addressed. Clarification in terms of multi-tenancy context is to be needed for security and privacy aspects of network slicing. Consequences might to be served otherwise.

5G network slicing is being elaborated in this paper focusing on network security. Concept of isolation is not directly addressed which implies operation without any direct or indirect influence between slices or even between entities within the same slice like resources, operation, man-agreement. To achieve security, we refer an isolation technique to mention it whenever needed. At various levels, slice isolation can be implemented according to requirements and in various forms.

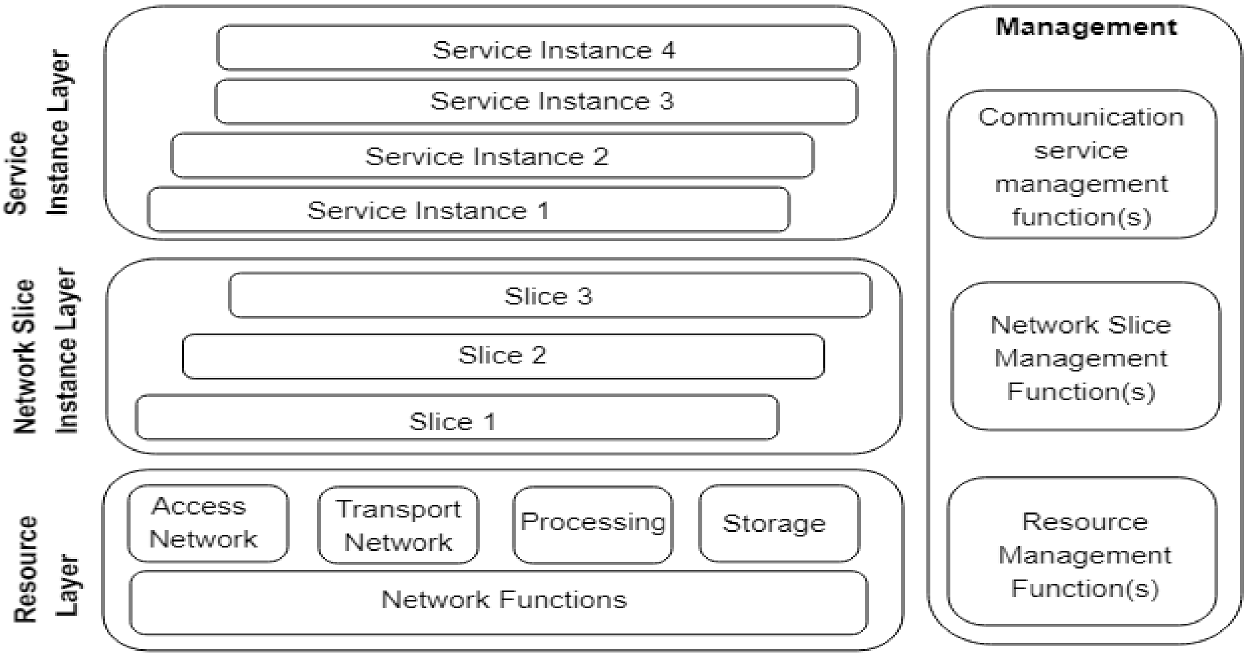

Figure 1Network Slicing Architecture

The aim of this article is to indicate possible points of attack and investigate security requirements and recommendations. There are four perspectives:

- Security aspects in different stages of the life cycle of a network slice.
- Intra- slice security: means security aspects of a network slice by itself
- Intra-slice security: security aspects in relation to other network slices.
- E2E slicing with intent-based networking

While using network slicing within this classification, we present and examine the security challenges. There is need to be clarification and discussion as network slicing is a new field with still open new aspects. Some of these are referred and indicate further research directions.

2. LITERATURE REVIEW

For the current status of 5G network slicing 3GPP standards establishes the fundamentals [1] ,[2]. TR33.811[5] and TR33.813[6] are the specifications related to security of network slicing and TS33.501 are the specification related to security architecture and procedures for 5G[7].

In [8], security requirements and network capabilities exposure are investigated by Next Generation Mobile Networks(NGMN) , use of network slicing might be emerged through identify flaws and make recommendations[9].For network slicing[10], a threat for network is given by European Union Agency for cybersecurity [ENISA]. From three perspectives which were mentioned previously, security for network slicing is looking. In [11], it is mentioned that for end-to-end slice isolation ZTE is referred to slice security on the industry side. With references to network slices [12]. Huawei gives an overview of architecture for 5G security.5G infrastructure Public Private Partnership (PPP) security white paper is adopted because to indicate weak isolation as a security risk and network slicing security is dedicated by a subsection [13].

Author in [14] mentioned for 5G as security and privacy, network slicing as a key technology is discussed for 5G along with SDN, NFV and Multi-access Edge Computing(MEC). In [15], architecture for 5G is introduced with possible security threats. Objectives of a 5G security architecture and concept of network slicing is in focus [16],[17]. Author in[18], introduce a term Network Slice Manager which is a element used by telco on top of NFV orchestration and confidentiality, integrity, authentication, authorization and availability are the principles which is considered for security threats. For IoT, 5G!Pagoda[19] and ANASTACIA [20] are the network slicing . 5G-MoNArch, 5G-ENSURE are some 5G-PPP projects[21]

The following abbreviations are used in this manuscript:

API	Application Program Interface
CN	Core Network
DoS	Denial of Service
DDoS	Distributed Denial of Service
E2E	End-to-End slicing

eMMB	Enhanced Mobile Broadband
MME	Mobile Management Entity
ENISA	European Union Agency for Cybersecurity
EPC	Evolved Packet Core
FGN	Future Generation Network
HSS	Home Subscriber Server
ITU	International Telecommunication
MANO	Management and Orchestration
MEC	Multi-Access Edge Computing
mMTC	Massive Machine Type Communication
MNO	Mobile Network Operator
NGMN	Next Generation Mobile Network
PPP	Public Private Partnership
RAN	Radio Access Network
SDN	Software Defined Network
URLLC	Ultra-reliable Low Latency Communication
3GPP	Third Generation Partnership Project
5GPPP	Fifth Generation Partnership Project

3. 5G NETWORK SLICING

In this section, main concepts and terminology in 5G network slicing are presented [22]. Differentiated 5G services are provided by network slicing. In respect of functionality; differentiation can be seen as mobility, security, control. In respect of performance, latency, throughput, error rate, reliability, availability is differentiation [23]. Small set of requirements containing specific services is served to the particular use-case. As compare to large set, small set of requirements is more feasible and efficient [24].To satisfy required networking characteristics, network slice instance is an end-to-end logical network which provide services to serve particular use cases like voice communication, video streaming , e-health, vehicular communication[17],[22],[25],[26]. On top of physical and virtual resources like storage, network, processing and access nodes is a set of network function instances called logical network. There is another local logical network i.e., Network slice subnet instance. A network slice instance can be constituted by one or more network slice subnet instance and network slice instance and network slice subnet instance will be referred. Core Network (CN) and Radio Access Network(RAN) are the network domains which is the part of 5G architecture. An example for sub-slice chaining is RAN sub-slice and CN sub-slice chained together. Isolation should be proper for slices and can be created on demand which are self-contained and have independent control and management [17],[27].Different perspectives like performance, dependability, management can be regarded from isolation[33].

A. Architecture

Three layers with each its own management functions comprises can form a overall network slicing architecture.

1. <u>Resource Layer:</u> Based on end-user request, services are provided by network resources and network functions together form a lower layer in architecture. Both may be logical/virtual or physical. Storage, processing and transmission nodes are the examples of resources. Switching and routing, slice selection and authentication are the examples of network slice instances can have served a resource or a network function.
2. <u>Network Slice Instance Layer:</u> Service instances requires network capabilities which is provided by a slice. And middle layer consists of slices. A slice can serve one or multiple service instances which can run directly over the network resources or over another slice. On the same physical architecture, it may or may not be possible to run two distinct slices and hence share or not resources and network functions.
3. <u>Service Instance Layer:</u> This is the upper layer that consists of service instances that are consuming the slices and are offered to customers. Here we refer a service instance as simply ‘service’.

From figure ‘1’ resources and network functions are related to resource management functions and different administrative domain is associated with each function. Network slice management function(s) are simply refer as ‘slice manager’. Life cycle of slices are managed by slice manager and interacts with other management functions. There is also management function for the sub-slices which together forms a slice. Life cycle is managed by communication service management functions(s) and interacts with slice manager [22].

It is described in [22],[29] that roles are defined within a business model and different operational responsibilities are characterized by roles in the 3GPP specification. 5G offers an opportunity of new business roles for 3rd parties, allowing them more control and system capabilities [29]. Other than the Mobile Network Operator (MNO), there are entities like 3rd parties which is referred as tenants that is considered to manage some of the resources, functions, slices and services. Hence, among the MNO and the 3rd parties, ownership and management can be split at each layer [30].

B. Slice Life Cycle

There are four phases in slice life cycle that are:

1. Preparation: For the preparation of the network environment, designing, creation and modification of network slices templates the first phase is dedicated for above. To describe the components, structure and configuration of a slice a network slice template is used. In this phase, slice doesn't exist and in the second phase it will be built from the template.
2. Installation, configuration and activation: Resources and network functions are created, installed and configured during the second phase. To installed, configured and activated, slice is built from the template.
3. Run Time: Upgrades, change of configuration, associations or disassociations of resources and network functions are modifications. Supervision and reporting take place in this phase.
4. Decommissioning: Resources and network functions are liberating and after this phase, slice is no more. Slice manager handles the life-cycle management and also responsible for creating and destroying the slices. Application Program Interface(API) access the slice manager [31]. Creation or deletion of slices, different levels of configuration, report and monitoring as depending on the scenario, operator might allow different actions in the API

4. SECURITY THREATS AND RECOMMENDATIONS

Threats and probable points of attack are identifying in slice network. In terms of life-cycle security, intra-slice security and inter-slice security are described as:

A. Slice Life-cycle security

1. Preparation Phase: Network slice template is the main point of attack in this phase. All the slices are offered from a poorly designed, tampered with or improperly implemented network slice template (e.g. with design flaws, without up-to-date security patches or injected malware) [12] [25]. To provide confidentiality, integrity and authenticity of network slice templates, crypto graphical protocols are used.
2. Installation, configuration and activation phase:Before or during activation, the main threats are creating fake slices or changing the configuration of slices. Secure APIs, such as access and operational rights are the specific mitigation techniques. API should permit auditing, monitoring and reporting securely [31].
3. Run-time Phase: Denial of Service(DoS), performance attacks, data exposure and privacy breaks are the variety of threats in this phase. Slice isolation have been considered through Distributed DoS(DDoS) [32]. On-demand security mechanisms are enabled by Dynamic NFV
4. Decommissioning Phase: Explosion of sensitive data that had been improperly handled during decommissioning is the main threat during and after deactivation of slices [25]. If resources are improperly liberating to mount a DoS attack, then it is also a threat. So, destruction of sensitive data and de-allocation of network functions and resources are the specific mitigation techniques so that they don't remain busy [22].

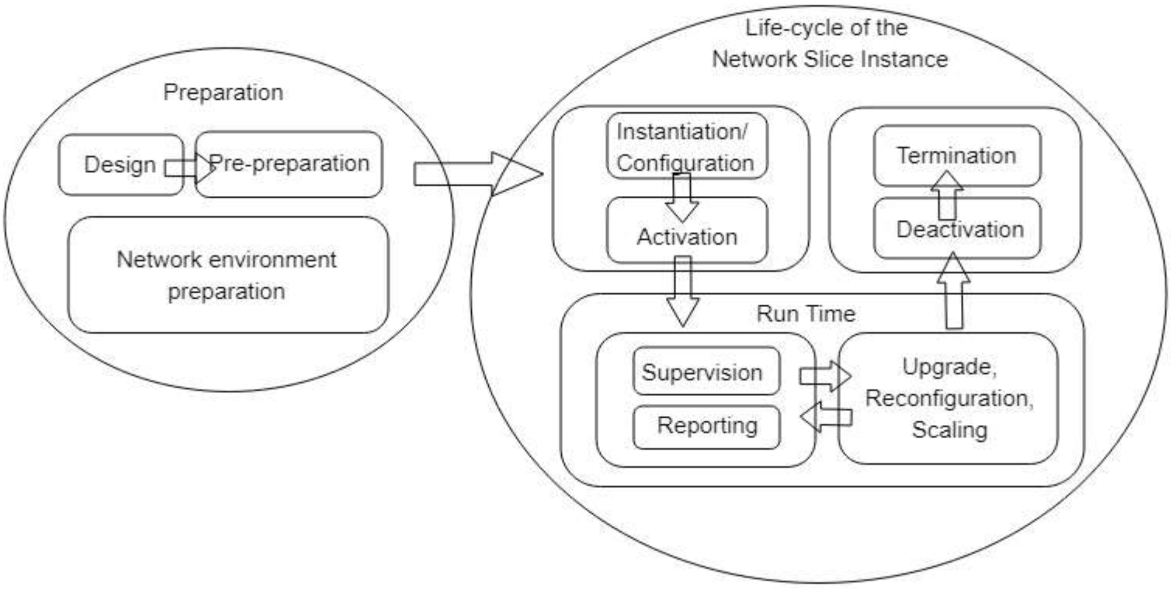
Preparation
Design
Pre-preparation
Network environment preparation
Life-cycle of the Network Slice Instance
Instantiation/ Configuration
Activation
Termination
Deactivation
Run Time
Supervision
Reporting
Upgrade, Reconfiguration, Scaling

Figure 2Network Slice Instance Management

B. ***Intra-Slice Security***

1. 5G Customer Devices

Customer devices are an accessible point of attack which are mostly used by non-technical users. For DoS attacks, there are several possibilities like confidentiality problem unauthorized access impacts the consumption of resources [6]. Via non-3GPP networks, risk related to 5G customer devices increase while accessing the network.

There is recommendation for authentication i.e. at primary authentication, devices are allowed to access the network at secondary authentication. Slice level is recommended [6] [26] [34]. Primary authentication standardized for allowing roaming and different technologies interconnection. And for decrease the costs and facilitate integration, secondary authentication is standardized. To mitigate risks associated with DoS, limited number of customer devices can access a network slice simultaneously, number of simultaneous active sessions, data rate per device, performed at different levels in the network are some suggestions.

2. Slice- Services Interface: The interface between the slice and the services that consume the slice is a possible point of attack. A correct level of isolation is the specific mitigation technique that might be implemented among the services and between slice and consuming services.
3. Sub-slices: Attack points are presented in the interconnection between the sub-slices and weakest sub-slice is the prone for attack. If the access network is non-3GPP then securing sub slices and implemented, decrease the risks at interconnection is the specific mitigation technique.
4. Slice Manager: Tenants may increase the risk as are responsible for the slice management as they might try to access functionalities that our outside of the legal agreement [9], [31]. For the mutual authentication, more slice managers co-exist[14] tenants capabilities should be restricted because they are responsible for slice management. This is done for conformity to legal agreements between the parties.
5. Resources and network functions: To damage the slices, resources and network functions might be attacked. Physical attacks, software attacks and cyber-attacks are the possible attacks can take place. Mutual authentication, secure boot, credential access, physical security and integrity verification are the specific mitigation techniques.

C. Inter-Slice Security

1. 5G Customer Devices: Most vulnerable points of attack are 5G customer devices. When authorized slice of a customer device might try to gain access to unauthorized one that invites the security threat. In intra-slice device is not complete outsider that is the advantage. Performance of a slice or DoS attack might be damage the through adversarial device. Several slices simultaneously attach if device needs diversified access to services [33]. Proper isolation between slices is the specific mitigation technique in terms of integrity, authenticity access control, confidentiality and resource consumption.
2. Service-service Communication: Interface between the services that consume different slices is the possible point of attack. This is a low-security risk because usually services running on different slices are independent and hence no need of communication. Within or between the slices and different components [37], [38], traffic and behavioral analysis and anomaly detection are the techniques to investigate disallowed communication.
3. Intra-Slices and Intra-Sub-Slices Communication: As compare to a more-secured slice, an adversary might try to attack a less-secured [8], [25] threats like unauthorized access, leakage of shared parameters sensitive data may be transmitted between the slices if the comm. between slices is allowed [10]. Again proper isolation between the slices are the specific mitigation techniques. Controlled and secured communication between slices is another technique [14]. Between slices it is avoid to share cryptographic parameters to avoid leakage [25]
4. Management Systems: It is also a point of attack. Chances for attack increases when a tenant might try to access other tenant's slices or change parameters.

Proper isolation between different slices in the slice manager is the specific mitigation technique and restrict the tenants to change the parameter of other tenants [9].

5. Resource Infrastructure: Exhaustive consumption or DoS or software attacks are the resource layer attack point. Code isolation and code protection techniques are the specific mitigation techniques.

5. DISCUSSION

There is impossible for complete analysis of security in respect to network slicing. As because of on-going security specifications for 5G are prone to changes and lack of implementation of slicing. Analysis of network slicing is quite difficult and there is much to be learned about slicing concept and regarding its risks. Based on threats and recommendations challenges and problems are further discuss.

D. End-to-end Security: End-to-end security is needed as network slices are end-to-end logical networks. Authors suggested in [15] that network slicing as one of the 5G enabling technologies and their possible security threats in 5G architecture. For end-to-end security, end-to-end isolation is a prerequisite [11]. In [7], end-to-end security is referred. In 5G, end-to-end security remains a challenge and topic for further research.

E.

A.(a) End-to-end (E2E) slicing: E2E slicing is very important from5G requirements point of view. 3GPP, 5GPPP, ITU and NGMN are bodies related to network communication. Here, E2E mechanism can perform for both core and access network. These standard bodies give outline for E2E network slicing for FGN. Many researchers suggested E2E slicing architectures. In [39], Author suggested the architecture for E2E slicing with intent-based networking that consists of four major modules IBN tool, OSM network orchestrator, FlexRAN controller, and deep learning model. To deploy the higher configuration networks first module is IBN tool which is automated in deploy and execution mode. Network service providers are enabled by IBN tool just to configure the network resources for both in core and access networks. To continuously monitors the statistics of network resources hybrid deep learning model GAN is used which also stores the IBN database. Core network slicing is supported by OSM framework. Since JSON strings for slice configuration are accepted by OSM orchestrator so for this higher-level configurations are converted by OSM policy configurator IBN tool.

Information is provided to the OSM orchestrator through core NFVs that are deployed. After deployment, slices configurations are dispatched by OSM NFVO to OpenStack for the deployment of network functions(NFs). MME, HSS and SPGW are the core network functions of EPC which are deployed for each slice. For managing and creating the access network slicing SDN-Based controller FlexRAN controller is used. To convert the high-level slice configuration provided at the IBN tool to JSON slice template format a specific RAN slicing policy configurator is developed and send it under FlexRAN controller. Further these configurations are deploys at eNodeB for creation of slice.

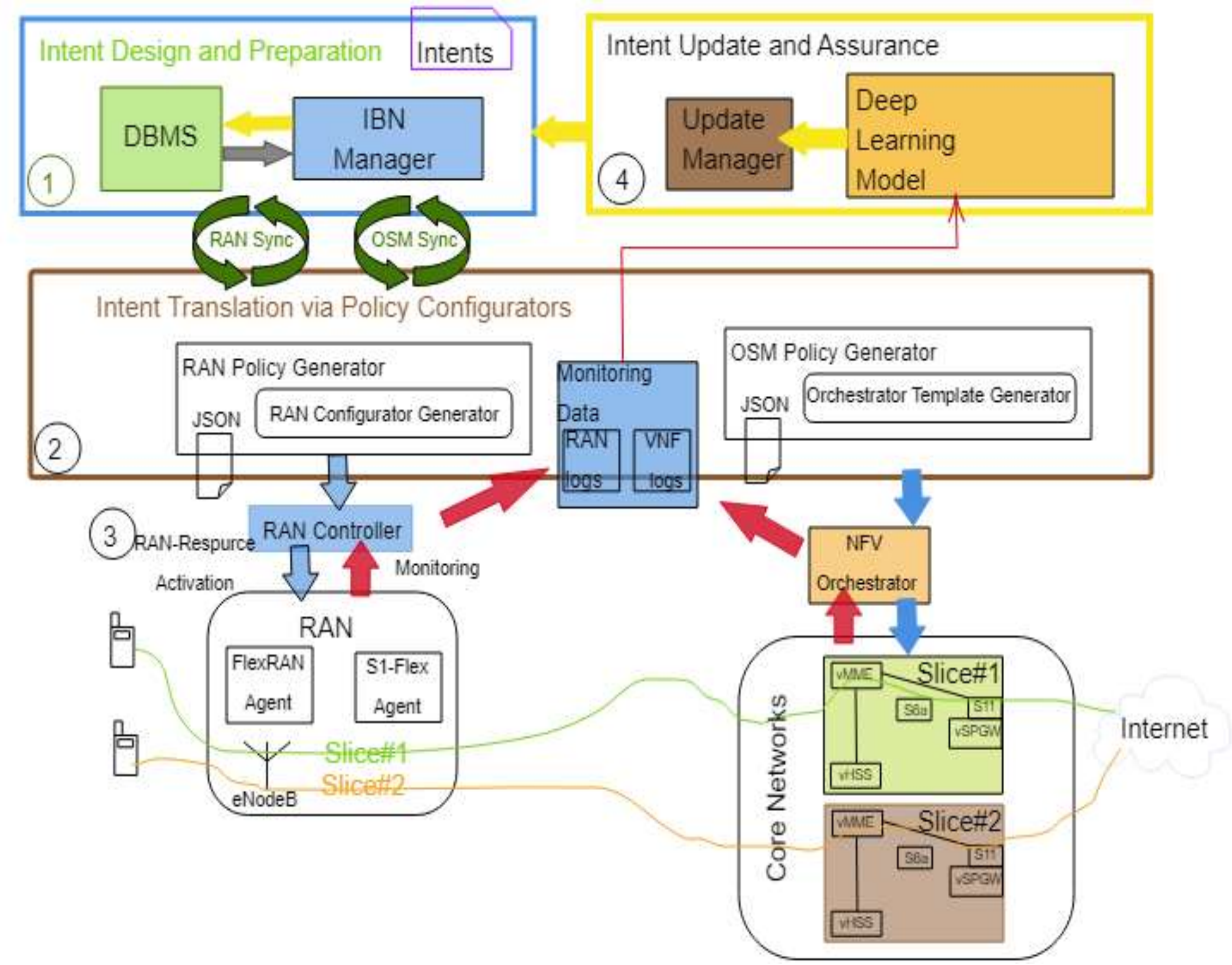

Figure 3 Complete Architecture of E2E slicing with Intent-based network

F. Isolation

From different perspectives isolation may be considered as: isolation between network slices, isolation between network functions and isolation between users etc. [11]. Isolation can be performed by both physical and logical means [11], [28] and can be either full or partially [24]. Isolation is achieved by technologies like firewalls, gateways, hypervisors. At all levels starting from physical isolation hardware, operating systems, virtual machines, sandbox based isolation or at the network programming language level [24], [35].

G. Secure Management and Orchestration

3GPP introduces Management and Orchestration(MANO) of network slicing. NFV and network slice orchestration are directly connected to each other. From a business model perspective architecture of network slice MANO is challenging with multi-domain environments, several layers of tenants. To assure a minimum security level standardization of inter-connection interfaces.

H. Trust Model: For network slicing security, trust plays an important role. Between MNOs and tenants, trust can be considered at different layers which is directly related to business model and overall architecture [25], [29]. By legal agreements, parties assume a level of trust. There are 3 architectural layers: resource, slice and service layers which applies in the relation to tenants. In [36], author described about overall trust model of the network slice.

I. 5G Customer Devices: The main attack points are identified 5G customer devices. If one in device is associated with several devices, then there is need of attention. There is need for discussion that emergency services are highly vulnerable so to handle this at slice level is tedious.

6. CONCLUSION

As concern for network slicing security, threats and their recommendations are presented in this paper. There is future direction of research in network slicing as it has many issues to resolve it. Also mention end-to-end security, isolation concept and security models. This paper focuses on the end-to-end security based network because end to end communication needs end to end encryption so that information not get deteriorated. Architecture of slicing system and E2E slicing with intent-based network is described which facilitates the network operators to deploy network services in a flexible and customizable manner.

7. REFERENCES

[1] 3GPP. (2019). *Release 16*. [Online]. Available: https://www.3gpp.org/release-16

[2] 3GPP. (2020). *Release 17*. [Online]. Available: https://www.3gpp.org/release-17

[3] G. Nencioni, R. G. Garroppo, A. J. Gonzalez, B. E. Helvik, and G. Procissi, ''Orchestration and control in software-de_ned 5G networks: Research challenges,'' *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1_18,Aug. 2018.

[4] IMT Vision Framework and Overall Objectives of the Future Development *of IMT for 2020 and Beyond*, document Recommendation ITU-R M.2083-0, 2015.

[5] Study on Security Aspects of 5G Network Slicing Management (Release *15) V15.0.0*, document 3GPP TR33.811, 2018.

[6] Study on Security Aspects of Enhanced Network Slicing (Release 16) *V0.8.0*, document 3GPP TR33.813, 2019.

[7] Security Architecture and Procedures for 5G System (Release 16) V16.2.0,document 3GPP TS33.501, 2020.

[8] NMNG Alliance: 5G Security Recommendations, Package #2: Network *Slicing*, NMGN, Frankfurt, Germany, 2016. [Online]. Available:https://www.ngmn.org/wp-content /uploads /Publications /2016/160429_NGMN_5G_Security_Network_Slicing_v1_0.pdf

[9] NMNG Alliance: Security Aspects of Network Capabilities Exposure in *5G*, NMGN, Frankfurt, Germany, 2018. [Online]. Available: https://www.ngmn.org/wp-content /uploads /Publications /2018 /180921_NGMNNCEsec_white_paper_v1.0.pdf

[10] ENISA Threat Landscape for 5G Networks-Threat Assessment for the Fifth Generation of Mobile Telecommunications Networks (5G), ENISA,Heraklion, Greece, Nov. 2019.

[11] 5G Security White Paper-Security Makes 5G Go Further, ZTE, Shenzhen,China, May 2019.

[12] Huawei: Huawei: 5G Security Architecture White Paper, Huawei, Shenzhen, China, 2017.

[13] 5G-PPP. 5G PPP Phase1 Security Landscape. Accessed: Apr. 2020.[Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5GPPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf

[14] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, ``A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions,'' IEEE Commun. Surveys Tuts., vol. 22, no. 1, pp. 196248, 1st Quart., 2020.

[15] T.-H. Ting, T.-N. Lin, S.-H. Shen, and Y.-W. Chang, ``Guidelines for 5G end to end architecture and security issues,'' 2019, arXiv:1912.10318.[Online]. Available: http://arxiv.org/abs/1912.10318

[16] G. Arfaoui, P. Bisson, R. Blom, R. Borgaonkar, H. Englund, E. Félix, F. Klaedtke, P. K. Nakarmi, M. Näslund, P. O'Hanlon, J. Papay,J. Suomalainen, M. Surridge, J.-P. Wary, and A. Zahariev, ``A security architecture for 5G networks,'' IEEE Access, vol. 6, pp. 22466-22479,
2018.

[17] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Folgueira, ``Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges,'' IEEE Commun. Mag., vol. 55, no. 5,pp. 80-87, May 2017.

[18] V. A. Cunha, E. da Silva, M. B. de Carvalho, D. Corujo, J. P. Barraca, D. Gomes, L. Z. Granville, and R. L. Aguiar, ‘’Network slicing security: Challenges and directions,'' Internet Technol. Lett., vol. 2, no. 5, p. e125, Sep. 2019. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/itl2.125

[19] 5G!Pagoda. Accessed: Apr. 2020. [Online]. Available: https://5g-pagoda.aalto.fi/

[20] ANASTACIA. Accessed: Apr. 2020. [Online]. Available: http://www.anastacia-h2020.eu/

[21] 5G-PPP. Accessed: Apr. 2020. [Online]. Available: https://5g-ppp.eu/

[22] Study on Management and Orchestration of Network Slicing for Next Generation Network (Release 15) v15.1.0, document 3GPP TR28.801, 2018.

[23] P. Rost, C. Mannweiler, D. S. Michalopoulos, C. Sartori, V. Sciancalepore, N. Sastry, O. Holland, S. Tayade, B. Han, D. Bega, D. Aziz, and H. Bakker, ``Network slicing to enable scalability and flexibility in 5G mobile networks,'' IEEE Commun. Mag., vol. 55,no. 5, pp. 72-79, May 2017.

[24] Z. Kotulski, T. Nowak, M. Sepczuk, M. Tunia, R. Artych, K. Bocianiak,T. Osko, and J.-P.Wary, ``On end-to-end approach for slice isolation in 5G networks. Fundamental challenges,'' in Proc. Federated Conf. Comput. Sci. Inf. Syst., Prague, Czech Republic, Sep. 2017, pp. 783792.

[25] Study on the Security Aspects of the Next Generation System (Release 14) V1.3.0 (Withdraw), document 3GPP TR33.899, 2017.

[26] System Architecture for the 5G System; Stage 2 (Release 16) v16.4.0, document 3GPP TS23.501, 2020.

[27] Feasibility Study on New Services and Markets Technology Enablers; Stage 1; Stage 1 (Release 14) V14.2.0, document 3GPP TR22.891, 2016.

[28] A. J. Gonzalez, J. Ordonez-Lucena, B. E. Helvik, G. Nencioni, M. Xie, D. R. Lopez, and P. Grønsund, ``The isolation concept in the 5G network slicing,'' in Proc. Eur. Conf. Netw. Commun. (EuCNC), Dubrovnik,Croatia, Jun. 2020.

[29] Feasibility Study on Business Role Models for Network Slicing (Release 16) V16.1.0, document 3GPP TR22.830, 2018.

[30] Study on Tenancy Concept in 5G Networks and Network Slicing Management (Release 16) V16.0.1, document 3GPP TR28.804, 2019.

[31] Study on Common API Framework for 3GPP Northbound APIs (Release15) V15.1.0, document 3GPP TR23.722, 2018.

[32] D. Sattar and A. Matrawy, ``Towards secure slicing: Using slice isolation to mitigate DDoS attacks on 5G core network slices,'' in Proc. IEEE Conf. Commun. Netw. Secur. (CNS), Jun. 2019, pp. 82-90.

[33] Feasibility Study on New Services and Markets Technology Enablers-Network Operation; Stage 1 (Release 15) V15.0.0, document 3GPP TR22.864, 2016.

[34] Study on Enhancement of Network Slicing (Release 16) V16.0.0, document 3GPP TR23.740, 2018.

[35] S. Gutz, A. Story, C. Schlesinger, and N. Foster, ``Splendid isolation: A slice abstraction for software-dened networks,'' in Proc. 1st Workshop Hot Topics Softw. Dened Netw. (HotSDN), 2012, pp. 79-84.

[36] B. Niu, W. You, H. Tang, and X. Wang, ``5G network slice security trust degree calculation model,'' in Proc. 3rd IEEE Int. Conf. Comput. Commun. (ICCC), Dec. 2017, pp. 1150-1157.

[37] The Evolution of Security in 5G: A, `Slice' of Mobile Threats, 5G Americas, Bellevue, WA, USA, 2019.

[38] D. Schinianakis, R. Trapero, D. S. Michalopoulos, and B. G.-N. Crespo, ``Security considerations in 5G networks: A sliceaware trust zone approach,'' in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Apr. 2019, pp. 18.

[39] Khizar Abbas , Muhammad Afaq, Talha Ahmed Khan, Adeel Rafiq and Wang-Cheol Song “Slicing the Core Network and Radio Access Network Domains through Intent-Based Networking for 5G Networks”, Received: 9 September 2020; Accepted: 14 October 2020; Published: 18 October 2020