Contemporary Network Slicing Security

ZORAN MILICEVIC[1], ZORAN BOJKOVIC[2]
[1]Telecommunications and Information Technology,
Directorate GS of SAF,
11000 Belgrade,
REPUBLIC OF SERBIA

[2]University of Belgrade,
Studentski trg 1, 11000 Belgrade,
REPUBLIC OF SERBIA

Abstract: - Security slicing in contemporary networks is a powerful tool that can serve operators to deliver a more secure, reliable, and efficient network extension. In order to ensure secure deployment and implementation, it is necessary to build a corresponding security framework that contains security threats, requirements, and recommendations. On the other hand, by segmenting the network, operators can allocate resources more effectively and provide a more customized and optimal experience for users. This work illustrates contemporary network slicing security. After an introductory presentation, an illustration of security considerations in contemporary network slicing security is provided. The next two sessions addressed for the influence of artificial intelligence and security closed-loop automation. Further, the role of future research consideration together with operated achievements are demonstrated. The final session referred to concluding remarks.

Key-Words: - Network slicing, Security threats, Artificial Intelligence, Network Slice Instance, Interaction.

Received: May 19, 2024. Revised: November 11, 2024. Accepted: March 4, 2025. Published: April 14, 2025.

1 Introduction

Wireless networks are vulnerable to a wide range of security threats and attacks that can compromise the confidentiality, integrity, and availability of data, [1], [2], [3]. The complexity of these threats increases exponentially as the current wireless network infrastructure evolves so that security attacks target network resources, confidential data, and user privacy. Overcoming the threats as well as providing a secure environment is highly needed. Of course, it is assumed that all users, devices, applications, and their internal and external traffic are untrusted and should be continuously verified and validated at every stage of digital interaction before admission to network resources.

Contemporary mobile systems have changed the architecture communications. For example, fifth-generation (5G) mobile systems have drastically changed not only the architecture but also the nature of communications in terms of data rate, latency, connection density, reliability, spectrum as well as energy efficiency. For the use cases mobile broadband (eMBB), ultra-reliable low latency communications (uRLLC), and massive machine-type communications (mMTC), together with the new additions for 5G and beyond including virtual reality, machine vision for automatic inspection security, and so on, are required, [4].

Network slicing (NS) technology is one of the foundations for contemporary mobile networks. This technology is promptly evolving with 5G advanced and is expected due to its flexibility and cost-effectiveness to be included in six generation (6G) networks, providing ways for mobile network operators (MNOs) to leverage physical infrastructure across the different domains for supporting many applications. NS divides the network into slices each with unique features with requirements for individual users (Figure 1). Network slices are defined as end-to-end logical networks, mutually isolated within independent control and management, which can be created on demands. The main idea is to select the optimal control/user plane split, compose, and allocate a virtualized network function (VNF). In fact, NS represents a solution for logical networks as mutually isolated according to the service requirements for different use cases. On the other hand, a network slice is a bundle of service functions, applications, and resources, together with belonging equipment characterized by independent

control and management, [5]. As the NS market is projected to grow by over 50% annually from 2023 to 2030, contemporary network slicing security has become one of the key technologies.

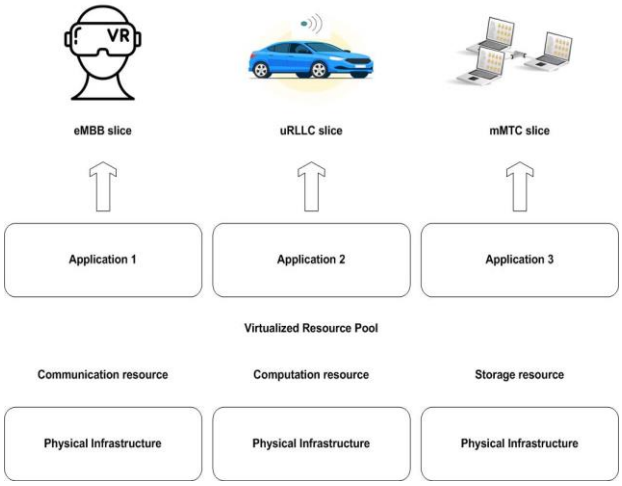

Fig. 1: An example scenario of network slicing

This paper is organized as follows. First of all, security considerations in network slicing are presented. Secondly, the influence of artificial intelligence is demonstrated together with security closed-loop automation. Finally, the role of future research considerations is emphasized.

2 Security Consideration in Network Slicing

Network slicing has appeared as one of the key technologies enabling efficient resources allocation, as well as providing different applications such as Virtual Reality (VR), Augmented Reality (AR), Connected Autonomous Vehicles (CAV), Internet of Everything (IoE). In this case, these applications were enabled owing to diverse features using realization not feasible through fixed, inflexible network infrastructure (eMBB, uRLLC, mMTC), [6].

Key security considerations in network slicing include different phases of the network slice instance (NSI) life cycle such as preparation, commissioning, operation, and decommissioning as shown in Table 1. The roles of each phase are presented, too [7].

To provide the security for contemporary network slicing, various security concerns have to be taken into consideration such as isolation, authentication, and authorization.

The security concerns related to contemporary networks have to be addressed in such a way as to assure the safe and secure operation. One of the key requirements to ensure security is strong isolation between slice instances. It should be added that strong encryption, access control, and physical protection technologies can be also applied where ensuring in the case of NS security. As for the life cycle, they are required to be managed carefully, as these security and privacy vulnerabilities are at the point of being explored.

Table 1. Key security considerations related to different NSI life-cycle

No.	Phase	Characteristics and roles
1.	**Preparation**	Planning the composition of a slice with security by design principles
2.	**Commissioning**	a) Creation of an NSI b) Ensure access control and proper authentication are integrated together with NSI policy management
3.	**Operation**	Include activation, supervision, performance reporting, resource capacity planning, modification, and deactivation of NSI.
4.	**Decommissioning**	The slice manager demolishes the NSI-specific configuration from the shared constituents.

3 Influence of Artificial Intelligence

For achieving security in network slicing, artificial intelligence (AI) has got a great interest from researchers all over the world because of the possibility to analyze data in real-time. In that way, AI improves security, but unfortunately at the same time, its opens a door to many different threats. Thus, it is of great interest to take into consideration the different risks. Also, AI allows contemporary security measures to be implemented in order to protect data including network integrity from vulnerabilities. In one of the solutions for network slicing architecture, each slice can be approved for specific service requirements. The application of AI seems to be in this case tailored for network slicing, together with software-defined networking (SDN), network function virtualization (NFV), and cloud computing, [8].

Three main characteristics are identified for contemporary networks: a massive number of connected devices, high traffic volume, and diverse technologies and services. This leads to complex and dynamic threats. The adoption of AI is one of the ways to deal with these threats, thanks to its potential to make possible intelligent, adaptive, and autonomous security management. Potential problems concerning its identification enable reaction on reliability and availability requirements. It understands timely detection and prediction of malicious/demands service degradation as well as

financial loss. Today, AI has proven its force to recognize security threats, [9].

4 Security in Closed Loop Automation

In order to ensure potency against possible threats, security closed-loop automation architecture (SCLA) is applied. While monitoring adaptability and scalability, SCLA integrates three main goals: monitoring, decision-making, and automated responses. Taking advantage of AI technology, SCLA adjusts defenses in real-time based on predictive analysis. Here, there are some objectives such as proactive security, threat response in real-time, adaptive learning, and operational efficiency.

To implement this kind of objective and to be the first line of defense the components interact with each other as shown in Figure 2.

The security data collection serves to collect packets of data network traffic which are later retrieved by components. The security data analysis component is responsible for analyzing the collected data and detecting any possible threats in the network through the use of AI models, [10]. The security decision model is used to ensure that appropriate action is taken to solve the issue in the case of an attack or non-compliance with the required policies.

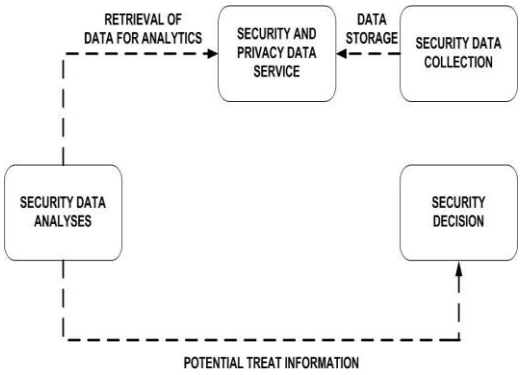

Fig. 2: Interaction between components of SCLA

Security and privacy data service is the specialized model responsible for safety management and storing security data with the closed loop. In other words, it represents the SCLA's database.

5 Role of Future Research Consideration

Taking into consideration that NS is one of the key factors in future architecture, it will be of great importance to note security future directions. The role of some future research considerations is presented in Table 2.

Table 2. Some future research considerations and operated achievements

No.	Future considerations	Note
1.	**Artificial Intelligence with new algorithms and security models**	• A tool to design intelligent security solutions by network slicing (NS) • To facilitate identification and predictions of attacks and threats reducing at the same time human intervention
2.	**One slice available for security**	• To achieve coordination between security mechanisms and their impact allocation of an independent network slice is welcome • To promote the operation of the network monitoring and security systems to be run on the top of this security slice • Resources allocated for security services to be changed
3.	**Content-aware security**	• This mechanism requires intelligent and control systems by the network operators and stockholders • Security issues to be scaled in and out according to the network concept playing an important role in enabling content-aware slices
4.	**Security orchestration**	• To control both the virtual and physical network segments • Responsibility for deployment, configuration, maintenance, monitoring and management • The research should be carried out together with the new interfaces to communicate with 5G, 5G and beyond, and 6G elements
5.	**Security-by-Design**	• To offer benefits such as the establishment of reliable operation of controls • To enable continuous and real-time auditing • To reduce the impact of new attacks of the system
6.	**Security as a service**	• Research consideration where service providers can offer security services for customers • Concept where it is possible to offer an easy integration for operators

6 Conclusion

Network slicing is one of the solution for network architecture. It has evolved from a simple fixed network overlay concept to a fundamental feature of

the emerging multi-provider 5G systems, enabling new business opportunities by facilitating flexible support for multi-service. Future mobile networks will be subject to technical service requirements, such as energy efficiency and cost. It is important that challenges are addressed through continuous consultations by regulators, industry, applications, network operators, service/technology providers, and public-private partnership organizations. For achieving more robust security solutions, artificial intelligence technology is provided. The main reason was its ability to analyze vast amounts of data and detect errors in real-time, making it necessary for improving network slicing security. However, it should be noted that AI exposes systems to a new range of threats. Thus, prioritizing efforts for reducing the changes is one of the primary goals to ensure artificial intelligence secure implementation, while enhancing the corresponding resilience.

References:

[1] C. De Alwis, P. Porambage, K. Dev, T. R. Gadekallu, M. Liyanage, A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions, *IEEE Communications Surveys & Tutorials*, vol. 26, is. 1, 2024, pp. 534-570. https://doi.org/10.1109/COMST.2023.3312349.

[2] Z. Bojkovic, Z. Milicevic, D. Milovanovic, Next Generation of Cellular Networks, in *Proceedings of the 15th WSEAS International Conference on Communications (Part of the 15th WSEAS CSCC Multiconference) and the 5th International Conference on Communications and Information Technology (CIT '11)*, pp. 233-239, Corfu Island, Greece, July 14-17, 2011.

[3] L. U. Khan, I. Yaqoob, N. H. Tran, Z. Han, C. S. Hong, Network Slicing: Recent Advances, Taxonomy, Requirements, and Open Research Challenges, *IEEE Access*, vol. 8, 2020, pp. 36009-36028. Available at: https://doi.org/10.1109/ACCESS.2020.2975072.

[4] W. Saad, M. Bennis, M. Chen, A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems, *IEEE Networks*, vol. 34, no. 3, 2020, pp.134-142. https://doi.org/10.1109/MNET.001.1900287.

[5] H. Chergui, L. Blanco, L. A. Garrido, K. Ramantas, S. Kukliński, A. Ksentini, Zero-Touch AI-Driven Distributed Management for Energy-Efficient 6G Massive Network Slicing, *IEEE Network*, vo. 35, is. 6, 2021, pp. 43-49. https://doi.org/10.1109/MNET.111.2100322.

[6] R. Khan, P. Kumar, D.N.K. Jayakody, M. Liyanage, A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions, *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1, 2020, pp.196-248. https://doi.org/10.1109/COMST.2019.2933899.

[7] 3GPP, Study on management and orchestration of network slicing for next generation network, Technical Specification, 2017, [Online]. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3091 (February 15, 2025).

[8] S. Wang, Y. Hu, N. Zhang, Y. Liu, A Survey on Service Migration in Mobile Edge Computing, *IEEE Access*, vol. 6, 2018, pp.23511-23528. https://doi.org/10.1109/ACCESS.2018.2828102.

[9] Ch. Benzaid, T. Taleb, AI for Beyond 5G Networks: A Cyber-Security Defense of Offense Enabler, *IEEE Networks*, vol. 34, no. 6, 2020, pp.140-147. https://doi.org/10.1109/MNET.011.2000088.

[10] V. Chandola, A. Banerjee, V. Kumar, Anomaly Detection: A Survey, *ACM Computing Surveys (CSUR)*, vol. 41, no. 3, 2009, pp.1-58. https://doi.org/10.1145/1541880.1541882.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare.