International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 13, Issue 4 (Jul.-Aug. 2024), PP. 05-09

End-To-End Slice Security Management in AI-Driven Network Slicing

Dr. Alex Mathew
Department of Cybersecurity, Bethany College, USA

Abstract
The dawn of software-based networks has enhanced the capacity of network slicing to effectively allocate end-to-end logical networks that facilitate the dynamic requirements of emerging applications in the backdrop of the fifth generation (5G) networks. Integrating Artificial intelligence (AI) was vital in easing and automating the management of slices. For instance, by automating the network slices across slice commissioning, activation, operation, and decommissioning. Besides enabling automated and efficient resource relocation within individual network slices and across the entire network, it has also enabled proactive end-to-end slice security management approaches such as comprehensive threat detection, lifecycle management, dynamic policy enforcement, ensuring secure communication channels, Identity and Access Management (IAM) and automated response to threats, among others. It has also enabled real-time analysis, reporting, and integration of security threats before actualizing automated incident response.

Keywords: *End-to-End Slice Security Management, Network Slicing, Artificial intelligence (AI), Identity and Access Management (IAM), dynamic policy enforcement and automated response to threats*

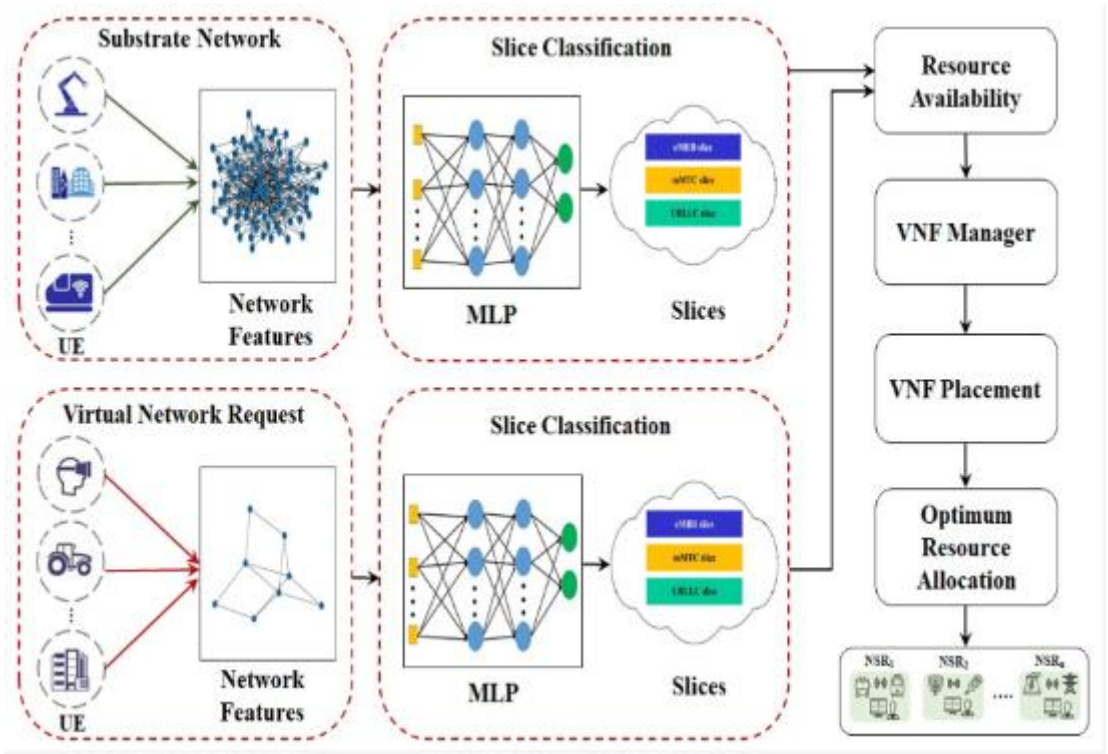
Date of Submission: 14-07-2024 Date of acceptance: 31-07-2024

I. INTRODUCTION

End-to-end slice security management refers to the holistic approach adopted in securing network slices across their Lifecycle. This holistic approach is meant to ensure that network slices are protected across lifecycle stages such as commissioning, activation, operation, and decommissioning (Martins et al., 69149). On the other hand, Thantharate et al. (0855) assert that network slicing is an emerging paradigm that utilizes network function virtualization to support the instantiation of numerous virtual networks referred to as slices on a single physical network infrastructure. Before the integration of AI, the network management process was complex, especially due to the need for dynamic management of network resources in real-time. Nevertheless, this challenge was addressed through automation using AI. Subsequently, the integration of AI in network slicing has also uniquely influenced End-to-end-slice security management. The objective of the current research paper is to demonstrate the dynamics of end-to-end slice security management in AI-based network slicing. This objective will be attained by discussing some of the key aspects and recent advancements supporting the argument using a flow chart, algorithm, and methodology block diagram.

II. PROPOSED METHODOLOGY BLOCK DIAGRAM

The proposed methodology block diagram of AI based Network slicing.



ALGORITHM

Notably, the machine learning algorithm will be trained using labelled data.

i. Set up *eMBB*, *mMTC*, *uRLLC* to be a blank *k*-length vector.
ii. Set node i=0i=0
iii. Get KPI for $NsNs$
iv. Perform classification: **MLP Classifier ()**
v. **while** i<=ni<=n **do**
vi. $XPredXPred$ of node *i*
vii. Y$PredPred$ = Predict the class of X$PredPred$
viii. **if** Y$PredPred$ = "eMBB Class" **then**
ix. *eMBB = i*
x. **else if** Y$Pred$Y$Pred$ = "mMTC Class" **then**
xi. *mMTC = i*
xii. **else**
xiii. *uRLLC = i*
xiv. **end if**
xv. *i = i + 1*
xvi. **end while**
xvii. *eMBB, mMTC, uRLLC* node

Additionally, the process of establishing the performance metrics like accuracy and precision of End-to-End security management in AI based network slicing is as follows;

$Accuracy$=TP+TN/TP+FP+FN+TN

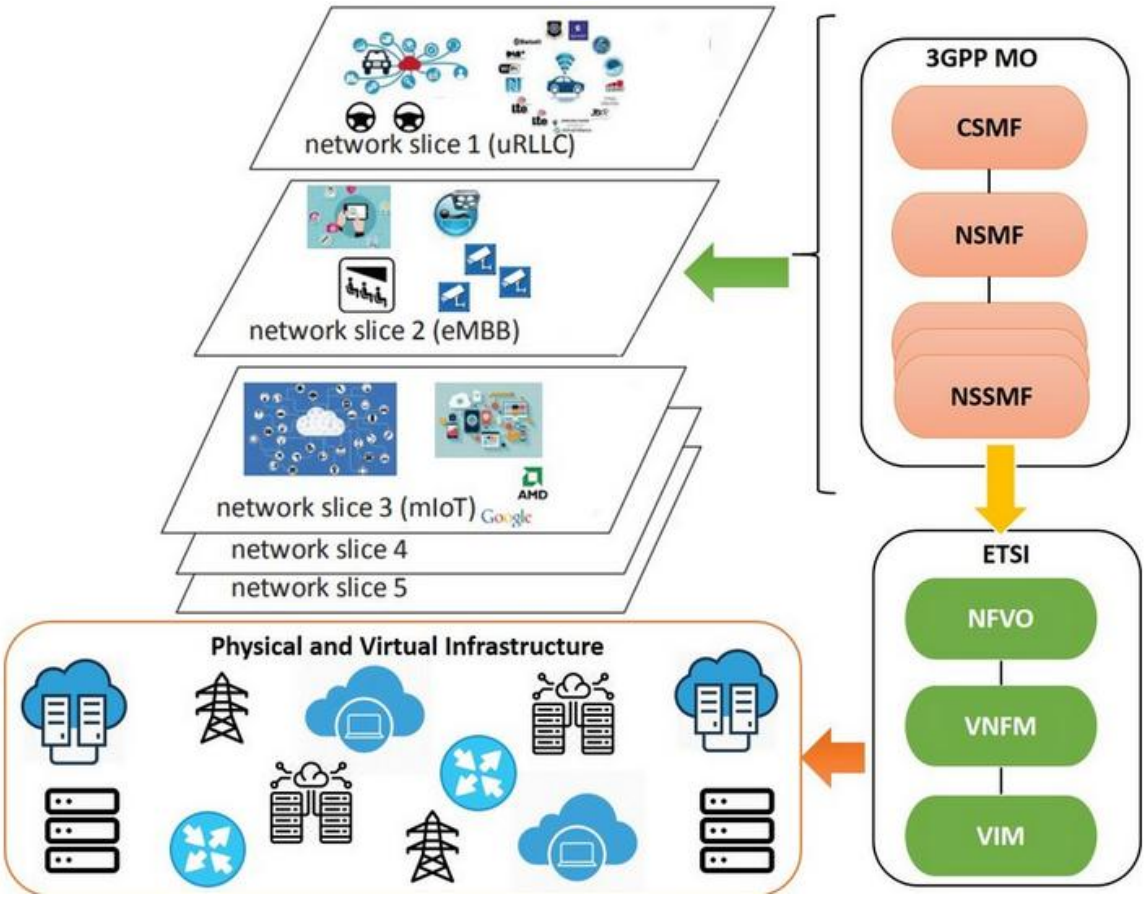
$Precision$=TP/TP+FP

$Recall$=TP/TP+FN

$F1Score$=2∗$Precision$∗$Recall$/$Precision$+$Recall$

III. FLOW CHART

The flowchart below shows the network slice configuration in a 5G network with either shared or dedicated resources over the same network.



IV. RESULT ANALYSIS

Notably, AI-driven network slicing is also beneficial for operators in multiple ways. According to Bega et al. (34), the introduction of AI in networks has benefits like increasing the expected performance gains by between 25% and 85%. These expected performance gains are realized due to the automatic management of slices and network resources enabled by AI. However, the impact and role of AI extends beyond managing slices and network resources to supporting end-to-end slice security management through approaches like comprehensive threat detection, lifecycle security management, dynamic policy enforcement, ensuring secure communication channels, Identity and Access Management (IAM), automated response to threats, integrating User and Entity Behavior Analytics (UEBA) and Multi-Domain Security Orchestration among others

Artificial intelligence has improved network slice lifecycle security management during network slicing by enabling real-time monitoring and configuration of security policies depending on the lifecycle stage (Suárez et al.,28). Abbas et al. show that the network slicing lifecycle involves four major steps, including the preparation or creation, commissioning, operation, and decommissioning phases (39). During creation, AI is responsible for safely structuring and provisioning network slices before administrating the appropriate security configurations and policies (Cunha et al., 226). In the operational phase of the slices, Abbas et al. postulate that AI proceeds to monitor and manage security configurations to ensure consistent End-to-End Slice Security Management (80128). In the final decommissioning step, AI safely decommissions slices, constantly monitoring residual data and configurations to avert potential security risks (Abbas et al., 80128). Therefore, as shown in the case of Lifecycle security management, AI features are vital in network slicing as they enable the deployment of a robust, real-time, and holistic protection of slices across different phases.

Another vital key aspect of End-to-End Slice Security Management in AI-Driven Network Slicing is dynamic policy enforcement. According to Guan et al., policy enforcement is essential in outlining and guiding the implementation of network security management protocols and procedures (267). Artificial intelligence leads to proactive and dynamic policy enforcement. Salahdine et al. also assert that the primary objective of dynamic

policy enforcement is to identify and adopt anomalous conduct that tends to be in direct contrast to the existing static security protocols (27). Additionally, dynamic policy enforcement leads to the development of a security policy that is adaptive to the existing and emerging landscape and security landscape using the learning capabilities of Artificial intelligence. Subsequently, AI supports dynamic policy enforcement by availing real-time and accurate data on existing and emerging security threats, as well as performing a fast and reliable evaluation of the impact and effectiveness of policies in ensuring robust End-to-End Slice Security Management.

Importantly, the aspects of lifecycle security management and dynamic policy enforcement are supported by AI-enabled comprehensive threat detection. Comprehensive threat detection in network slicing is essential and justified by the dynamic and constantly changing threat landscape. Due to this justification, Abood & Abdul-Majeed (109) also agree with the need to deploy cutting-edge systems not only for threat detection but also for incident response. Hence, the multifaced and robust capabilities of AI technologies, including machine learning, natural learning processes, and software-designed networking (SDN), are vital in designing and implementing robust security solutions that enhance AI-based network slicing (Cunha et al.226). Subsequently, implementing AI-driven tools is essential and effective for detecting threats across all network slice layers, such as application, transport, and physical layers.

AI is also essential in monitoring different users and identities on the network and enforcing network security protocols. For instance, ensuring security during Identity and Access Management (IAM) is essential since unauthorized users can easily exploit it to launch network attacks (Wichary et al., 222). Additionally, Wichary et al. (222) opined that implementing insufficient IAM guidelines incentivizes malicious insider and external attackers to exploit weak guidelines. Moreover, some of the security risks affiliated with IAM range from the risk associated with managing user access manually, inadequate visibility into user access data risk, granting excessive permission, and irregular access review (Sharavanan 1). Such malicious attacks compromise network slicing to security threats like injection of malicious code and data theft.

On the other hand, AI ensures strict compliance with security protocols during IAM by actively assessing security threats and potential gaps in IAM security protocols that might increase network susceptibility to external and internal attacks (Olimid et al., 100007). AI also manages user behavior by constantly ascertaining and verifying users' identities. According to Olimid et al. (100007), It also alleviates the dynamic sources of risk associated with IAM, such as automating the user access management, providing holistic comprehension and visibility into user access data risk, and performing credible and reliable user access reviews to identify and address anomalies.

De Alwis et al. also agree that End-to-End Slice Security Management in AI-driven network Slicing is also susceptible to multiple security risks due to the structural complexity of AI-driven network slicing (12). Depending on the scope of features, a network might be complicated to suit advanced applications and services. This complexity increases the likelihood of mistakes in the design, implementation, and configuration of network slices which also exacerbates security risks. For example, with the dawn of 5G networks, network complexity has been amplified, as illustrated by the increase in inter-operator commands by 4.7 times, whereas inter-operator information attributes and elements have increased by 3.4 times (De Alwis et al., 12).

Ultimately, AI alleviates security risks and supports end-to-end security management in such complex networks through approaches like automated incidence response, self-learning security algorithms, and AI-driven threat Intelligence Integration. Firstly, automated incident response is essential in such complex network configurations as it deploys AI mechanisms like data analytics and machine learning to asses and derive real-time threat intelligence feeds that enable the identification and real-time intervention against emerging threats that are either specific to each network slice or entire network configurations. Additionally, with the reported increment in inter-operator commands and information attributes, especially on 5G networks, manually inspecting each element and command to ascertain security compliance is slow and inaccurate (Khan et al. 198). Therefore, the use of AI would be effective in accurately inspecting voluminous network data traffic and generating real-time insights on security threats before enabling automated incidence response.

V. CONCLUSION

The integration of AI in network slicing has influenced not only the network slice Lifecycle but also end-to-end security management. As discussed in the previous section, AI is responsible for introducing robust security mechanisms such as comprehensive threat detection, lifecycle management, and dynamic policy enforcement, and automating incident response which have collectively enhanced end-to-end security management in AI-driven Network slicing. Regarding IAM in AI-based Network slicing, the existing findings showed that AI has enabled such user access management and providing holistic comprehension, and visibility into user access data risk.

REFERENCES

[1]. Abood, Mohammad J., and Ghassan H. Abdul-Majeed. "Classification of network slicing threats based on slicing enablers: A survey." International Journal of Intelligent Networks, vol. 4, 2023, pp. 103-112.

[2]. Abbas, Khizar, et al. "Network Data Analytics Function for IBN-based Network Slice Lifecycle Management." 2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS), 2021.

[3]. Abbas, Khizar, et al. "Network Slice Lifecycle Management for 5G Mobile Networks: An Intent-Based Networking Approach." IEEE Access, vol. 9, 2021, pp. 80128-80146.

[4]. Bega, Dario, et al. "Network slicing meets artificial intelligence: An AI-based framework for slice management." IEEE Communications Magazine 58.6 (2020): 32-38.

[5]. Cunha, José, et al. "Enhancing Network Slicing Security: Machine Learning, Software-Defined Networking, and Network Functions Virtualization-Driven Strategies." Future Internet, vol. 16, no. 7, 2024, p. 226.

[6]. De Alwis, Chamitha, et al. "A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions." IEEE Communications Surveys & Tutorials (2023).

[7]. Guan, Wanqing, Haijun Zhang, and Victor CM Leung. "Customized slicing for 6G: Enforcing artificial intelligence on resource management." IEEE network 35.5 (2021): 264-271.

[8]. Khan, Rabia, et al. "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions." IEEE Communications Surveys & Tutorials, vol. 22, no. 1, 2020, pp. 196-248.

[9]. Martins, Joberto SB, et al. "Enhancing network slicing architectures with machine learning, security, sustainability and experimental networks integration." IEEE Access 11 (2023): 69144-69163.

[10]. Olimid, Ruxandra F., and Gianfranco Nencioni. "5G network slicing: A security overview." Ieee Access 8 (2020): 99999-100009.

[11]. Salahdine, Fatima, Qiang Liu, and Tao Han. "Towards secure and intelligent network slicing for 5g networks." IEEE Open Journal of the Computer Society 3 (2022): 23-38

[12]. Sharavanan. "7 Identity & Access Management Risks." Zluri | Unified SaaS Management Platform. www.zluri.com/blog/identity-and-access-management-risks/.

[13]. Suárez, Luis, et al. "Enhancing network slice security via Artificial Intelligence: Challenges and solutions." Conférence C&ESAR 2018. 2018.

[14]. Thantharate, Anurag, et al. "Secure5G: A deep learning framework towards a secure network slicing in 5G and beyond." 2020 10th annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2020.

[15]. Wichary, Tomasz, et al. "Network Slicing Security Controls and Assurance for Verticals." Electronics, vol. 11, no. 2, 2022, p. 222.