AI-Enabled Slice Protection Exploiting Moving Target Defense in 6G Networks

Maria Christopoulou[1], Wissem Soussi[2,3], George Xilouris[1], Gürkan Gür[2],
Edgardo Montes de Oca[4], Harilaos Koumaras[1], Burkhard Stiller[3]
[1]National Center for Scientific Research Demokritos (NCSRD), Greece
[2]Zurich University of Applied Sciences (ZHAW), Switzerland
[3]University of Zurich, Switzerland
[4]Montimage, France
Emails: [1] [maria.christopoulou, xilouris, koumaras]@iit.demokritos.gr, [2] [sous, gueu]@zhaw.ch,
[3] stiller@ifi.uzh.ch, [4] edgardo.montesdeoca@montimage.com

***Abstract*—As commercial 5G roll-outs continue progressing, research efforts are shifting toward requirements, challenges, and critical enablers for prospective 6G networks. The introduction of Artificial Intelligence (AI) support in 5G will be further exploited, rendering AI a key enabler for providing automated network management and orchestration, while improving the network resilience against potential threat actors. Therefore, it is crucial to investigate smart security schemes in "Beyond 5G" networks. This paper presents a use case for the proactive and reactive defense of end-to-end network slices that relies on AI-based attack detection to apply Moving Target Defense (MTD) policies based on an innovative framework.**

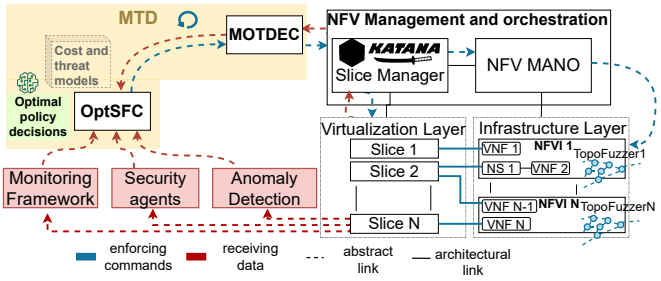

Fig. 1: Network Slices' Security Framework

I. Introduction

The advent of 5G commercial rollouts launched discussions on potential 6G use cases, requirements, challenges, and critical enablers [1]. In this context, AI is considered a potential 6G enabling technology for the design and optimization of intelligent networks with self-organizing capabilities [2]. 5G and beyond networks include extensive capabilities, such as multi-tenant service paradigms, multi-tier architectures, and software-defined infrastructures, introducing several challenges regarding network security, as each one leads to potential vulnerabilities. Thus, this paper presents a security use case that leverages AI to provide end-to-end network slice protection. Security mechanisms include the Moving Target Defense (MTD) and Anomaly Detection paradigms that ingest diverse data from multiple points across a cellular network. Their analysis can provide per-slice proactive and reactive defense policies from potential threat actors.

II. Use Case Description

The objective of this paper's use case is the demonstration of MTD as an effective mechanism in improving the network's resilience against attacks, providing the means for validation of the MTD's framework AI-inferred security enhancements. The demonstration of the use case will take place on actual 5G infrastructure and its operation will be validated by related Key Performance Indicators (KPI), while the network is under emulated attacks.

A. Overview

The security use case describes the operation of the proposed MTD framework that exploits AI and network softwarisation in order to assess an autonomous security system (*cf.* Fig. 1) for protecting Network Slices (NSi), Network Services (NS), and Virtual Network Functions (VNF) as instantiated in part of the Athens 5GENESIS Facility [3]. The Katana Slice Manager [4] is responsible for configuring, orchestrating and monitoring all sub-components of NSis. The MTD Framework is responsible for the MTD mechanism, assisted by the Anomaly Detection Framework, the Security Agents and Monitoring Framework, which are further described below.

The MTD framework deploys two components: *(i)* the MTD controller MOTDEC, responsible for enforcing MTD actions, and *(ii)* OptSFC, a Machine Learning (ML) optimizer of security functions, providing MTD strategies to maximize attack prevention and mitigation and to minimize computational costs according to requirements of Security Service Level Agreements (SSLAs) [5]. For this purpose, OptSFC models the state of the network using an incomplete information Markov game, since the defender does not know directly what the attacker is doing, but can perceive it through network changes and alerts. To this end, OptSFC will be fed with real-time monitoring data provided from *(a)* infrastructure monitoring and Management elements, *(a)* Anomaly Detection initiated alerts, and *(c)* Security Agents' monitoring feed. The Markov Decision Process (MDP) trains a Reinforcement Learning agent, integrated into OptSFC, to provide an MTD policy to MOTDEC.

The overall solution will be evaluated as a proactive and reactive defense mechanism through a set of KPIs. An important consideration is the security effectiveness of MTD

and the cost of reconfiguring the network. As a result, the KPIs include Protection Gain of MTD Policy, MTD Action Cost, QoS (Quality-of-Service) Loss/Gain of the protected resources when defense prevails over efficiency and vice-versa, and the Mean Time to Detect a security incident.

B. Moving Target Defense

MOTDEC will perform MTD shuffle actions on network interfaces, traffic flow, or on the resources themselves, in order to annul the network data gathered by the attacker, forcing him to perform more reconnaissance scans, which leads to higher probability of attack detection. Such operations can be performed on both the internal interfaces of the network and on the external/public ones. In the former case, MOTDEC prevents an attacker inside the network from easily exploring and further penetrating it. In the latter case, the resource is meant to be always accessible by external devices with a public interface, and it provides a different public IP address to suspicious end-users or User Equipments (UE), allowing further targeted analysis of their generated traffic. MOTDEC will decide on the appropriate policies to be applied, by communicating with the proper management and control elements.

So as a universal and scalable method, MOTDEC integrates an SDN controller (i.e., ONOS) and creates a middle virtual network, called *Topology Fuzzer*, used to change the node links and network data flow, increasing the difficulty of identifying the network topology. Similarly to the work presented by Islam et. Al [6], we assign dynamic ephemeral IP addresses to the virtual nodes, and redirect the packets to the protected resources with a softwarized address translation (NAT). MOTDEC will also perform MTD diversity actions, making it possible to move a protected resource from an NFVI cloud infrastructure to a different one, e.g., from an OpenStack VIM to an Azure VIM. This changes the environment of the running resource and reduces the threats due to specific system's vulnerabilities.

C. Anomaly Detection

The Anomaly Detection Framework is responsible for tracking suspicious activities and alerting the OptSFC. The Framework forms an end-to-end ML pipeline, comprising three distinct modules: the Data Ingestion, the ML, and the Analytics modules. The Data Ingestion module collects and pre-processes data from various underlying networks (i.e., the Radio Access, Core, Transport, and Cloud). The pre-processing function includes data translation to appropriate formats and storage to central databases. In turn, the ML module retrieves the prepared data and proceeds with training and inference in an unsupervised manner in order to remove the additional cost of labeling the available datasets, suitable for production environments. Anomaly Detection has been extensively studied in the literature, so the underlying algorithms will follow recent graph-based efforts that have shown promising results compared to traditional ML techniques for various types of attacks [7]. Finally, the Analytics module enriches the ML module's results with additional context, such as geolocation information, provides a graphical user interface (GUI) highlighting potential threats, and acts as the communication endpoint with external entities, e.g., OptSFC.

D. Security Agents and Monitoring Framework

To achieve automated network management and orchestration, security functions require precise information on the status of the network and functions. This is provided by the INSPIRE-5Gplus MMT Monitoring Framework (MF) being composed of distributed probes and a centralized function for the management and analysis. In the context of SDN/NFV and network slicing, monitoring probes (i.e., Security Agents) need to be easily deployed and adapted to changing requirements and topology. These monitoring probes extract data (from packets, flows, but also system and application logs) needed to detect anomalies, assess SSLAs, but also to obtain training data for supervised or semi-supervised ML algorithms. The data extracted needs to be analyzed by MF that implements several features including managing the deployment and dynamic configuration of distributed probes, analyzing data to detect anomalies using different techniques (such as rule and behaviour-based analysis, ML, Change Point Detection), generating alarms, providing dashboards to provide users with the information and control needed, and interacting with orchestrators, controllers, and security functions to automate remediation actions.

III. Conclusions

The objective of this security use case is the protection of network slices in heterogeneous cellular environments. MTD is considered a promising method for increasing the network's resilience against attacks leveraging AI, a potentially enabling technology in 6G. Anomaly Detection can act as a complementary source of information providing additional context to optimize policy decisions.

Acknowledgments

The work described in this paper has received partially funding from *(a)* the European Union's Horizon 2020 research and innovation programme under grant agreement no. 871808, the 5G-PPP project INSPIRE-5Gplus, and *(b)* University of Zürich UZH, Switzerland.

References

[1] J. Ortiz *et al.*, "INSPIRE-5Gplus: Intelligent security and pervasive trust for 5G and beyond networks," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, ser. ARES '20. New York, NY, USA: Association for Computing Machinery, 2020.

[2] W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, "The road towards 6G: A comprehensive survey," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 334–366, 2021.

[3] H. Koumaras *et al.*, "5GENESIS: The genesis of a flexible 5G facility," in *2018 IEEE 23rd Int. Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2018, pp. 1–6.

[4] M. Kourtis *et al.*, "5g network slicing enabling edge services," in *2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, 2020.

[5] INSPIRE-5Gplus Project, "INSPIRE-5Gplus-D5.1 security test cases," https://doi.org/10.5281/zenodo.4569524, Accessed on 10.03.2021.

[6] M. M. Islam and E. Al-Shaer, "Active deception framework: An extensible development environment for adaptive cyber deception," in *2020 IEEE Secure Development (SecDev)*, 2020, pp. 41–48.

[7] L. Leichtnam, E. Totel, N. Prigent, and L. Mé, "Sec2graph: Network attack detection based on novelty detection on graph structured data," in *2020 Detection of Intrusions and Malware, and Vulnerability Assessment, Springer International Publishing*, 2020, pp. 238–258.