SECURE SERVICE FUNCTION CHAIN DEPLOYMENT VIA MOVING TARGET DEFENSE

Author's: P. Deepa [1], R. Surendiran[2], K. Sujith[3], N. Vanjulavalli[4]

Abstract

The rapid evolution of Network Function Virtualization (NFV) and Software-Defined Networking (SDN) has enabled flexible and dynamic deployment of Service Function Chains (SFCs) to meet diverse Quality of Service (QoS) requirements. However, the programmable and shared nature of virtualized network infrastructures also expands the attack surface, making SFC deployments vulnerable to targeted cyber threats, lateral movement, and persistent exploitation. This work, titled "Towards Security Enhanced Service Function Chain Deployment by Moving Target Defense," proposes a security-aware SFC deployment framework that integrates Moving Target Defense (MTD) strategies into the orchestration process to enhance resilience against evolving threats.The proposed framework models the substrate network as a set of interconnected nodes characterized by resource capacities, link delays, and vulnerability scores. Each SFC request consists of ordered Virtual Network Functions (VNFs) with specific CPU, bandwidth, and latency constraints. A risk-aware placement mechanism is developed to allocate VNFs by jointly optimizing resource feasibility, latency requirements, and security risk. The security model incorporates node vulnerability and exposure time to compute a dynamic risk score for each deployed VNF. Unlike static deployment strategies, the framework continuously monitors exposure levels and triggers adaptive reconfiguration when predefined risk thresholds are exceeded.