Providing Anomalous Behaviour Profiling by extending SmartNIC Transceiver support in Packet-Optical Networks

R. Vilalta[1], F. J. Vílchez[1], Ll. Gifre[1], C. Manso[1], J.L. Carcel-Cervera[2], R. Leira[3], J. Aracil-Rico[3], J.P. Fernández-Palacios[4], R. Martínez[1], R. Casellas[1], R. Muñoz[1]

[1] *Centre Tecnològic de Telecomunicacions de Catalunya (CTTC/CERCA), Castelldefels (Barcelona), Spain*
[2] *Eviden, Madrid, Spain;* [3] *Naudit, Madrid, Spain;* [4] *Telefónica Innovación Digital, Madrid, Spain*
e-mail: ricard.vilalta@cttc.es

Abstract: This paper presents the architectural and data model extensions necessary to provide support for SmartNICs from SDN controller perspective. It later presents a use case for providing anomalous behaviour profiling support using the proposed extensions. ©2024 The Authors.

1. Introduction

The escalating sophistication of cyber threats demands a paradigm shift in defense mechanisms. Software-Defined Networking (SDN) has provided flexibility and control over network resources, enabling dynamic adaptation to changing traffic patterns and service demands. However, this increased agility comes hand-in-hand with heightened vulnerability, as the traditional static security approaches struggle to keep pace with the evolving threat landscape. As the attack surface expands in this dynamic architecture, there arises a critical need for an adaptive and responsive security framework that can seamlessly integrate with the programmability of SDN [1], [2].

Anomaly detection stands at the forefront of proactive defense strategies, offering the potential to identify subtle deviations from normal network behavior indicative of malicious activities. Anomaly detection begins with the establishment of a baseline behavior profile, encapsulating the anticipated patterns and behaviors of data during normal operation [3]. Anomalous Behavior Profiling (ABP) involves creating a detailed understanding of deviations from the established normal behavior. It identifies and characterizes patterns that deviate from the expected, contributing to a comprehensive analysis of anomalies within the incoming data. Then, incoming data undergoes scrutiny. Data points are carefully evaluated to assess their conformity with the expected characteristics outlined in the normal behavior profile. Any data points that significantly deviate from it are flagged as anomalies. The distributed and programmable nature of packet-optical network elements require an orchestrated approach to anomaly detection. For this reason, the SDN controller needs to orchestrate the subsequent mitigation actions across the network infrastructure.

Many works addressed the detection of physical attacks in optical fibers, for instance, authors in [4] use Machine Learning (ML)–based techniques to detect fiber tapping conditions and fiber cuts. However, it remains a challenge to detect cyber threats on the packet layer at line speed. Smart Network Interface Cards (SmartNICs) have introduced enhanced Data Processing Units (DPU) enhancing the capabilities and programmability at the network's edge. The introduction explores the unique features embedded in SmartNICs, ranging from their advanced hardware components to their ability to offload network functions, subsequently paving the way for a more intelligent and agile network infrastructure. SmartNICs can be combined with Graphics Processing Units (GPU) that can be used to accelerate the ML inference. SDN needs to play a significant role in orchestrating these SmartNICs, presenting a comprehensive examination of how logically centralized control facilitates dynamic network management, optimization, and security.

This paper proposes a novel architecture that addresses the intricacies of anomaly detection and mitigation within SDN [5] by introducing the usage of SmartNICs. By leveraging the collaboration between the SDN controller, and the control of SmartNICs introduced at the borders of transport network, our architecture aims to enhance the overall security mechanisms of SDN-controlled networks.

2. Extending SmartNIC Transceiver support in Packet-Optical Networks

Fig. 1 presents the proposed architecture for SDN-based control of SmartNIC and deployment of Anomalous Behaviour Detection using ETSI TeraFlowSDN SDN controller [6]. The connectivity service workflows have been previously described, so this paper only focuses on the necessary architectural extensions. The threat detection is backed by the NVIDIA Morpheus [7] open application framework that enables cybersecurity developers to create optimized AI pipelines for filtering, processing, and classifying large volumes of real-time data.

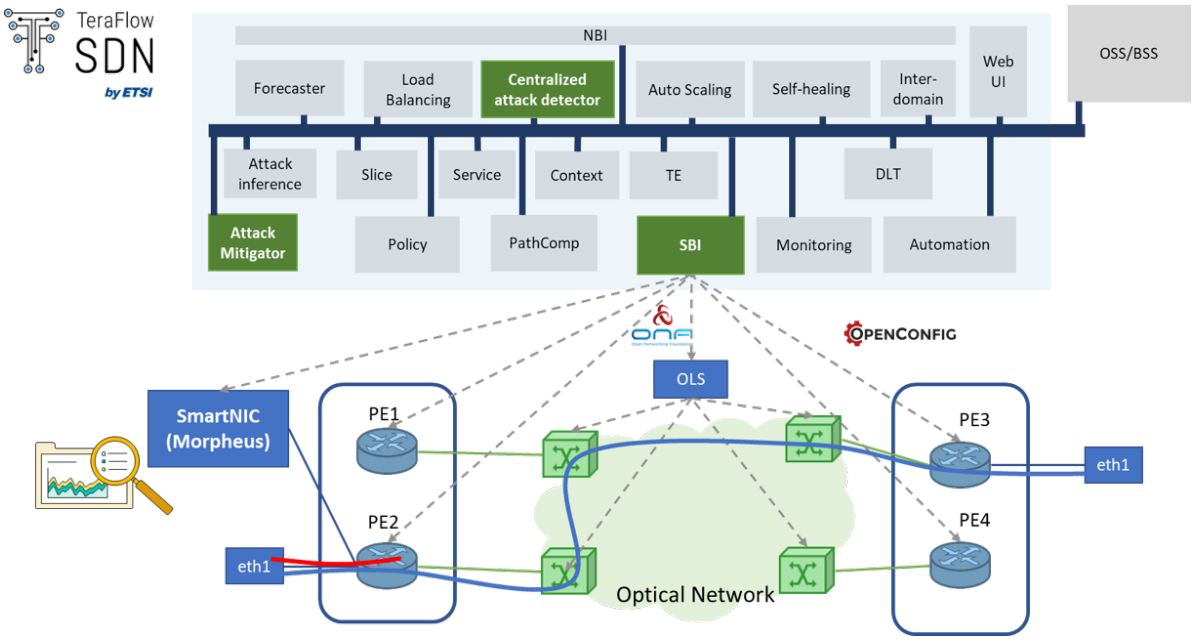

Fig. 1. Proposed architecture for providing Anomalous Behaviour Profiling by extending SmartNIC Transceiver support in Packet-Optical Networks

Firstly, the extension of the context for SmartNICs incorporates a series of functionalities in ProtocolBuffer format, including information about the manufacturer, model, and serial number, as well as details about their transceivers, DPUs, and GPUs. For transceivers, their port types and speeds are modeled for each. DPUs include information about their cores, RAM, and eMMC memory. Lastly, GPUs are modeled for their architecture, memory, cores, etc. This extended model enables the discovery of the characteristics of each SmartNIC node. After defining the context extension for SmartNICs, an extension of the OpenConfig-Probes data model has been carried out to support the configuration of SmartNICs through the Morpheus agent and Python API. This data model, specified in YANG format, defines a Morpheus pipeline providing various information such as its name, number of threads, pipeline size, input and output files, model name, server URL, and the configuration of various stages within the modeling phase, including deserialization, monitoring, inference, and serialization. This data model has been introduced in SBI component in order to directly interact with each SmartNIC. Centralized Attack Detector has been extended to support the necessary closed loop for monitoring the anomalous traffic behaviour and react accordingly as described.

Fig. 2(left) shows the proposed workflow. The workflow involves 3 main components, the SDN controller, the SmartNIC, and the IP routers that are part of the network. The relevant SDN controller components are the Centralized Attack Detector (CAD), the Attack Mitigator (AM) and the South Bound Interface (SBI). On the SmartNIC, the two main software components are the Operating System (SmartNIC_OS) managing the SmartNIC and the Morpheus agent carrying on the detection (SmartNIC_M). The workflow starts when the CAD, after a new connection has been detected, triggers the configuration of the anomaly detection capacities of the SmartNIC through the SBI component. The SBI component, upon activation, communicates with the SmartNIC_OS to configure traffic capture and subsequently initiates the activation of traffic analysis using the Morpheus module. This involves the creation of the SmartNIC_M and starting the analysis of raw network traffic. Later, the detection of anomalous raw traffic is symbolized by the red-colored arrows. The SmartNIC_M, detecting an anomaly, raises a notification to the SmartNIC_OS, which, in turn, firwards it to the SBI module. The SBI module promptly notifies the CAD of the detected anomaly, initiating a chain reaction for mitigation. The CAD, triggers the Attack Mitigator, which interfaces with the SBI module to block traffic. The SBI module configures new Access Control List (ACL) rules in the IP routers through NETCONF and the IETF ACL [8] data model to fortify the network against the identified threat.

3. Deployment of Anomalous Behaviour Profiling using SmartNICs

The proposed proof-of-concept has been implemented in ADRENALINE Testbed. To this end, NVIDIA SmartNIC BlueField-2 has been incorporated in COTS server, with prove traffic between interconnected whiteboxes Cell-Site Gateways (GSW) from EdgeCore using IP Infusion Network Operating System (NOS), namely PE in Fig. 1. The CSG were interconnected using a photonic network of 4 ROADMs, controlled using an Optical Line System. TeraFlowSDN

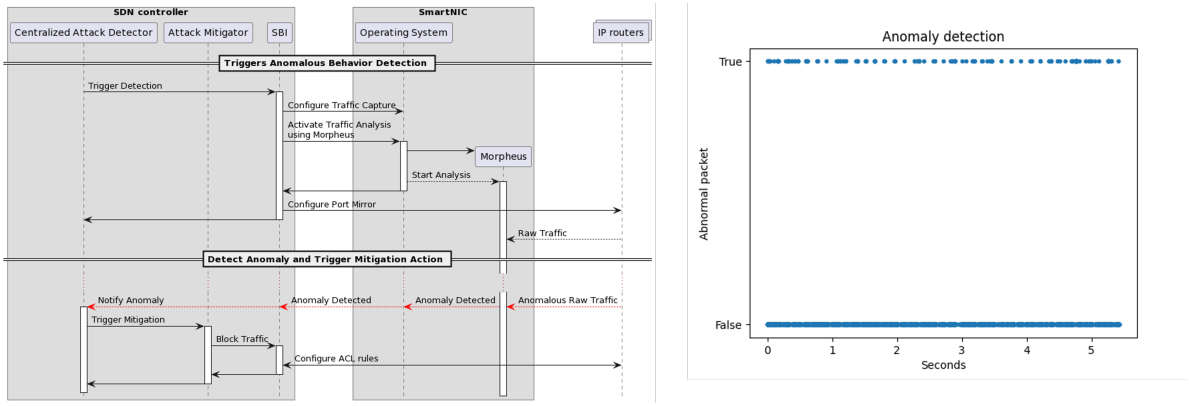

Fig. 2. (left) proposed ABP workflow; (right) detected abnormal packets in SmartNIC

[6] has been deployed on top, using the necessary extensions for the previously presented architecture.

The generated pipeline for the SmartNIC has been deployed using Morpheus and configured to use the XGBoost model. The proposed model is an example of a binary classifier to differentiate between anomalous crypto mining / malware, and normal workflows.

The defined API for activating traffic analysis in the SmartNIC includes a JSON-based configuration outlining the parameters and stages of a data processing pipeline. The pipeline operates with two threads, processes data in batches of 2048, and utilizes a model with an expected feature length of 8. The pipeline follows a series of stages, including pre-processing, metric monitoring, interaction with Triton Inference Server, classification, addition, and serialization. The Triton Inference Server stage involves connecting to a server for model retrieval and data processing.

Fig. 2(right) shows the obtained results from the SmartNIC ABP, when using a sequence of pre-trained traffic behaviour and using a dataset which includes several of the proposed attacks.

4. Conclusions

An architecture to control and manage SmartNIC descriptions and threat detection pipelines has been proposed in this paper. Later, a validation of the proposed architecture in an end-to-end packet-optical scenario has been provided.

Acknowledgements

This work is partially funded by the EC through the Hexa-X-II (101095759) project, and the Spanish RELAMPAGO grant PID2021-127916OB-I00 and UNICO-5G programm 6GMICROSDN (TSI-063000-2021-19/20/21) both funded by MCIN/AEI/10.13039/501100011033/FEDER,UE.

References

1. R. Vilalta et al. Experimental evaluation of control and monitoring protocols for optical sdn networks and equipment [invited tutorial]. *Journal of Optical Communications and Networking*, 13(8):D1–D12, 2021.
2. R. Casellas et al. Advances in sdn control and telemetry for beyond 100g disaggregated optical networks. *Journal of Optical Communications and Networking*, 14(6):C23–C37, 2022.
3. M. S. Gill et al. Profiling network traffic behavior for the purpose of anomaly-based intrusion detection. In *IEEE TrustCom / IEEE BigDataSE)*, pages 885–890, 2018.
4. K. Abdelli et al. Machine-learning-based anomaly detection in optical fiber monitoring. *Journal of Optical Communications and Networking*, 14(5):365–375, 2022.
5. C. Natalino et al. Scalable and efficient pipeline for ml-based optical network monitoring. In *OFC*, 2023.
6. R. Vilalta et al. Teraflow: Secured autonomic traffic management for a Tera of SDN flows. In *EuCNC/6G Summit*, pages 377–382. IEEE, 2021.
7. NVIDIA Morpheus Cybersecurity and AI framework. https://developer.nvidia.com/morpheus-cybersecurity, October 2023.
8. M. Jethanandani, S. Agarwal, L. Huang, D. Blair. YANG Data Model for Network Access Control Lists (ACLs). IETF RFC 8519, March 2019.