# DDOS attack identification via a silicon photonic Deep Neural Network with 50 GHz input and weight update

**Apostolos Tsakyridis[(1)], George Giamougiannis[(1)], Miltiadis Moralis-Pegios[(1)], George Mourgias-Alexandris[(1)], Angelina R. Totovic[(1)], George Dabos[(1)], Manos Kirtas[(1)], Nikolaos Passalis[(1)], Anastasios Tefas[(1)], Dimitrios Kalavrouziotis[(2)], Dimitris Syrivelis[(2)], P. Bakopoulos[(2)], E. Mentovich[(3)], Nikos Pleros[(1)]**

*[(1)]Department of Informatics, Center for Interdisciplinary Research & Innovation, Aristotle University of Thessaloniki, Thessaloniki, Greece*

*[(2)]NVIDIA, Ermou 65, 105 63 Athens, Greece*

*[(3)]NVIDIA, Hakidma 26, 2069200 Yokneam, Israel*

*e-mail address: atsakyrid@csd.auth.grAuthor*

**Abstract:** We experimentally demonstrate distributed denial of service (DDOS) attack identification using Deep Learning over a photonic neuromorphic engine that supports both input signal and weight update at 50 GHz, reporting a Cohen's κ-score of 0.636.

## 1. Introduction

Cybersecurity in Data Centers (DCs) is faced with a challenging operational framework as the explosive growth of intra-DC traffic brings an increased appeal in various types of malicious attacks [1]. The massive amount of data flowing through a high number of servers and switches within today's hyperscale DCs is forcing threat detection mechanisms to comply with a new set of requirements: i) real-time threat detection, implying that packet inspection has to be processed at ultra-high speeds, ii) threat detection as early as possible within the route of the malicious packets, implying that every DC node has to be equipped with a powerful cybersecurity toolkit [2]. This new operational framework has forced major DC equipment vendors to migrate from traditional threat detection mechanisms [3] into Artificial Intelligence (AI) and Deep Neural Network (DNN)-based methods for the identification of malicious attacks [4]. This paradigm shift, aims to utilize the proven credentials of AI and DNNs in generalizing and classifying patterns beyond static rule sets, allowing them to detect and react to multiple threats immediately [5]. As such, industry is steering its efforts towards the development of Deep Learning (DL)-assisted converged look-aside accelerators [4] that can perform real-time inference across vast amounts of cybersecurity data, mainly relying on state-of-the-art powerful GPUs and/or TPUs for realizing tiled matrix multiplication (TMM) and implement DNNs with dimensions significantly higher than the available hardware [6]. However, modern digital AI engines can hardly perform at clock-frequencies higher than ~2 GHz [7],[8]; with processing speed being one of the decisive factors for real-time detection, neuromorphic photonic accelerator technologies [9]-[13] emerge as ideal candidates for penetrating the DC cybersecurity domain, provided, however, that they can i) demarcate from their current static into a dynamic and high-speed weighting technology in order to support TMM and DNNs with a large number of NN parameters, ii) successfully adapt to threat detection AI algorithms and yield high-accuracy operation.

In this paper, we present, for the first time to the best of our knowledge, the successful silicon photonic DNN-based detection of distributed denial of service (DDoS) attacks within DC traffic at an ultra-fast operational rate of 50 GHz. We utilize a neuromorphic silicon photonic (SiPho) engine with TMM capabilities [13] and increase its speed credentials to 50 GHz towards demonstrating the execution of a DDOS-detecting DNN with 64 trainable parameters over a single SiPho neuron hardware, highlighting this way the technology credentials to perform over complex and large cybersecurity-oriented neural networks (NNs) and datasets. The TMM-based inference of a DC traffic dataset was realized experimentally with an accuracy, expressed with the Cohen's κ-score metric [14], equal to 0.636, reduced by only 0.064 compared to the software acquired κ-score value.

## 2. DDoS attack identification and experimental testbed

DDoS attacks comprise a pressing threat to the security and integrity of computer networks and DC infrastructures, provoking unavailability of resources for a considerable amount of time. A DDoS attack is created by a malicious user via the transmission of a great abundance of packets into a target DC server, as visualized in Fig. 1(a). With the current industrial roadmap for DC cybersecurity extending along the use of state-of-the-art electronic converged accelerators [4] within a smart network interface card (SmartNIC), DDOS attacks are expected to be detected at real-time through AI-based methods [15], [16] executed over digital electronic DL accelerators. Here we propose to upgrade the speed capabilities of this cybersecurity hardware by investing in a photonic NN (PNN) accelerator that can communicate with an electronic data processing unit (DPU), as illustrated in Fig. 1(b). The DPU receives and pre-processes telemetry data and after a tensor transformation, feeds them into the PNN to perform the inspection of the ingress traffic at high clock frequencies.

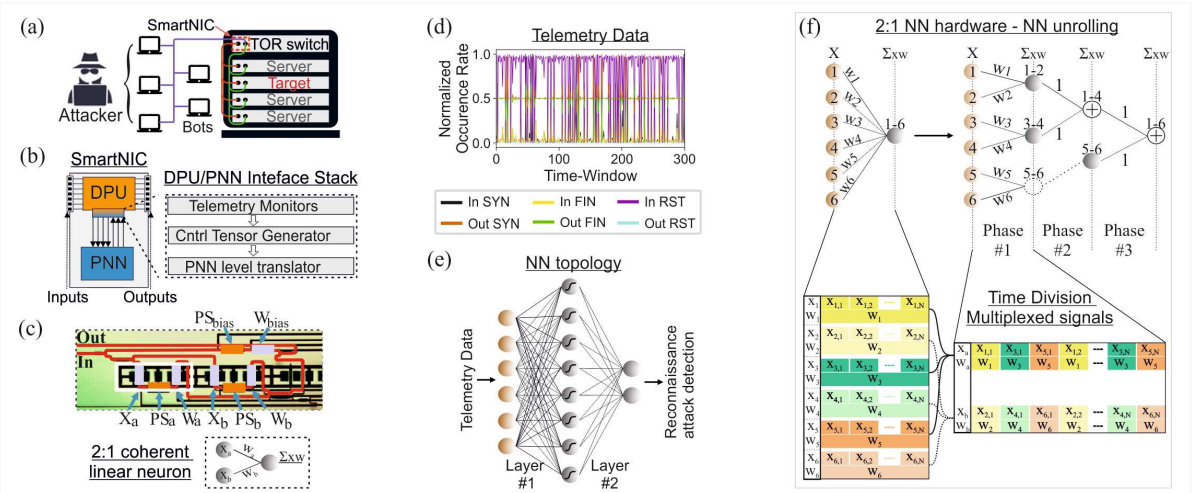


Fig. 1. (a) Pictorial representation of a DDoS attack in a DC rack. (b) Proposed SmartNIC architecture composing of a data processing unit (DPU) and a photonic NN (PNN) accelerator. (c) PNN accelerator employing high-bandwidth EAMs for NN input and weight data encoding. (d) Port-scanned telemetry data time-trace (e) NN topology for the DDoS attacks identification. (f) Methodology employed for the implementation of a neuron of the 1st neural layer via TDM.

In view of evaluating the PNN accelerator classification performance, we employed the SiPho processor depicted in Fig. 1(c) and propose to prevent DDoS attacks during the reconnaissance attack (RA) phase, when the attacker tries to determine critical information about the target's configuration. The fabricated chip deploys high-speed 50 um long SiGe EAMs both for the input and the weight amplitude imprinting. We simulated RAs using the publicly available software tool ddosflowgen [17] and created a dataset with six features that correspond to the statistics of the port scanning telemetry data (TCP flags SYN, FIN and RST) retrieved within 3 ms, with a slice of the resulting time-series being shown in Fig. 1(d). Thereafter, we trained the NN, illustrated in Fig. 1(e), to classify these data into benign and malicious. Specifically, the 6 features of the telemetry data comprise the input of the fully connected 6-8-2 NN, that uses the softmax function to make the RA detection. The NN inference was realized via time division multiplexing (TDM) and optical TMM, following the procedure described in [13]. Fig. 1(f) presents an indicative visualization of the employed methodology in one of the 8 fully-connected, 6-input neurons of Layer #1, when utilizing the integrated 2:1 neuron and TDM at both the input and weight signal sequences. In this specific neural layer, $\lceil \log_{No,axons}(No, inputs) \rceil = \lceil \log_2(6) \rceil = 3$ distinct phases are required for the calculation of the weighted summations, where $No, axons$ and $No, inputs$ correspond to the number of axons the hardware deploys and the number of inputs of each neuron, respectively. In the first phase, the 6 inputs $x_1$-$x_6$, comprising N samples each, along with their respective weights, $w_1$-$w_6$, were time multiplexed to generate the $x_a$,$w_a$ and $x_b$,$w_b$ data streams [13]. A pictorial representation of the multiplexed signals of the 1st phase is illustrated in the bottom of Fig. 1(f). The resulting partial sums are added in the remaining phases in the photonic hardware by tuning the weight values into 1. The experimental setup employed for the validation of the proposed NN is illustrated in Fig. 2(a). A light beam at 1560 nm was injected to the SiPho chip via a grating coupler. An arbitrary waveform generator was employed to generate the multiplexed $x_a$, $w_a$ and $x_b$, $w_b$ sequences at 16 and 50 GHz clock frequencies, with each constituent $x_1$-$x_6$ input signal comprising 500 samples. The multiplexed signals, after RF amplification, were injected into the respective EAMs with a Vpp of approximately 3 Volts. The resulting multiplexed weighted summation signals obtained at the chip output were converted to the electronic domain via a 70 GHz photodiode and captured via a 160 Gsa/s real time oscilloscope. Followingly, the received signal was demultiplexed to realize the individual

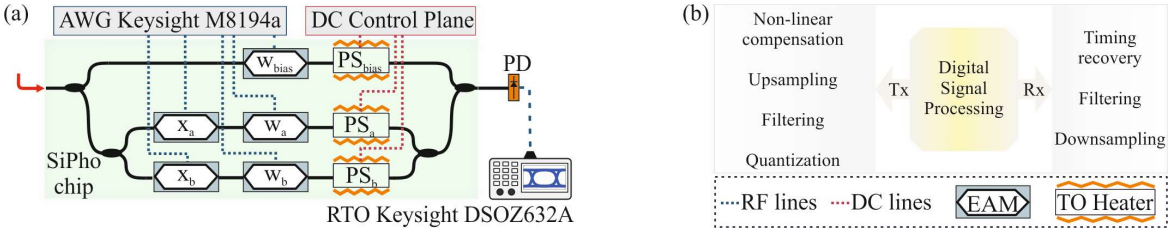


Fig. 2. (a) Experimental setup (b) Digital signal processing stack utilized for interfacing the DNN with the photonic hardware.

weighted summations and got forwarded to the next phase or layer of the NN after electronic application of the non-linear activation function. Finally, the digital signal processing stack, depicted in Fig. 2(b), was employed during the experimental process.

## 3. Experimental Results

Figure 3(a)-(c) depict the experimentally derived weighted summation traces of the first neural layer, denoted with blue lines, along with the respective traces obtained when executed over software, denoted with orange lines. As expected, the mean squared error (MSE) of the weighted sum increases with the phase rank within a single layer, due to noise accumulation. A detailed overview of the MSE along all 54 (40 at Layer #1 and 14 at Layer #2) weighted sums and its evolution through different phases and layers is shown in Fig. 3(d). The MSE increases with the phase rank within a single layer but drops from ~3% to ~0.8% when entering Layer #2, being the result of the non-linear sigmoid activation function following Phase 3 of Layer #1. Figure 3(e),(f) illustrate the experimentally derived confusion matrices when the PNN was operated at 16 and 50 GHz, respectively, while Fig. 3(g) depicts the software acquired confusion matrix. Taking into account the imbalanced dataset where only 20 out of 500 samples correspond to malicious packets, the κ-score metric was employed to quantify the classification accuracy. As shown in Fig. 3(h), the classification of the malicious traffic at 16 and 50 GHz revealed a κ-score of 0.688 and 0.636, respectively with minor degradations of only 0.012 and 0.064 with respect to the software-derived performance. Finally, the SNR values of the linear summations emerging from the PNN were measured equal to 14.1 dB and 11.2 dB, respectively.

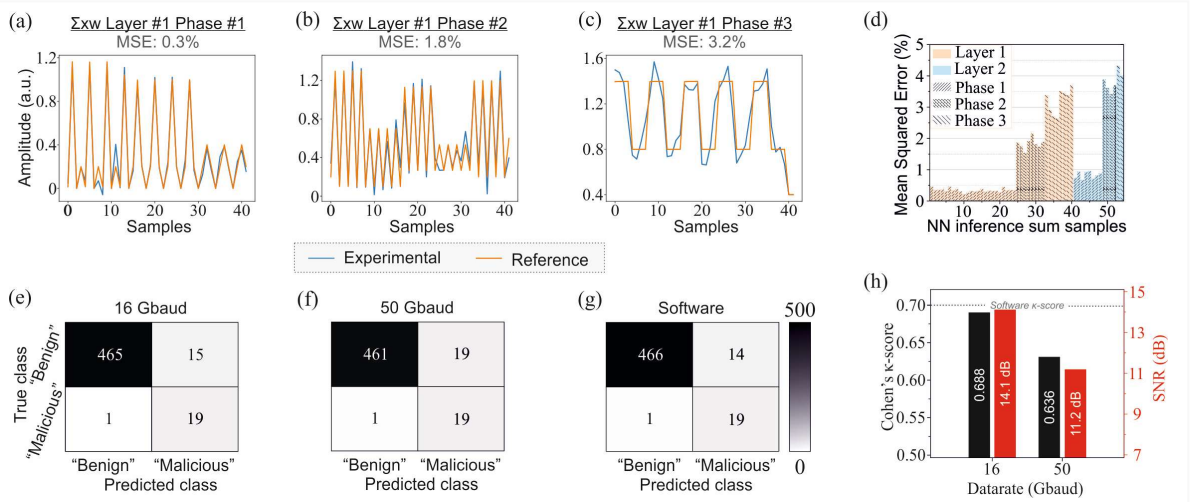


Fig. 3. (a)-(c) Time traces of the experimental (blue) and reference (orange) signals of the weighted summations of the 3 phases of Layer #1. (d) MSE distribution along Layer #1, Layer #2 for all 3 TDM Phases. (e),(f) Experimentally obtained confusion matrices when the PNN was operating at 16 and 50 GHz, respectively. (g) The respective software acquired confusion matrix, (h) Cohen's κ-score and SNR performance calculated for the operating data rates.

## 4. Acknowledgements

This work was supported by the EC via H2020 Projects PLASMONIAC (871391), SIPHO-G (101017194).

## 5. References

[1] F. Cremer, et. al.,"Cyber risk and cybersecurity: a systematic review of data availability," Gen. Pap Risk Insur. Issues Pract. 47, (2022).
[2] N.Z. Bawany, et. al. "DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions," Ar. J. Sc. Eng. 42. (2017).
[3] G. Carl, G. Kesidis, R. R. Brooks and Suresh Rai, "Denial-of-service attack-detection techniques," in IEEE Int. Comp., vol. 10, no. 1, 2006.
[4] NVIDIA app. Note [Online]. Available: https://www.nvidia.com/en-us/data-center/products/converged-accelerator/.
[5] Mittal, K. Kumar and S. Behal, "Deep learning approaches for detecting DDoS attacks: a systematic review." Soft Comput (2022).
[6] NVIDIA app. Note [Online]. Available: https://docs.nvidia.com/deeplearning/performance/dl-performance-matrix-multiplication/index.html
[7] NVIDIA app. Note [Online]. Available: https://developer.nvidia.com/blog/nvidia-ampere-architecture-in-depth/
[8] https://cloud.google.com/blog/products/ai-machine-learning/google-breaks-ai-performance-records-in-mlperf-with-worlds-fastest-training-supercomputer.
[9] A. Tait. et. al., "Neuromorphic photonic networks using silicon photonic weight banks", Sci. Rep., 7 (1), 2017.
[10] S. Xu, et. al. "Optical coherent dot-product chip for sophisticated deep learning regression". Light Sci Appl 10, 221 (2021).
[11] Y. Shen, et. al., "Deep learning with coherent nanophotonic circuits." Nature Photon 11, 441–446 (2017).
[12] G. Giamougiannis, et. al. "Silicon-integrated coherent neurons with 32GMAC/sec/axon compute line-rates using EAM-based input and weighting cells", ECOC 2021.
[13] A. Tsakyridis, et. al., "Silicon Photonic Neuromorphic Computing with 16 GHz Input Data and Weight Update Line Rates," CLEO 2022.
[14] Mary L. McHugh, "Interrater reliability: the kappa statistic." Biochemia medica 22.3 (2012).
[15] A. Saied, et. al., "Detection of known and unknown ddos attacks using artificial neural networks," Neurocomp.vol. 172, pp. 385–393, 2016.
[16] M. Kirtas, et. al., "Early Detection of DDoS Attacks using Photonic Neural Networks," IEEE IVMSP pp. 1-5, 2022.
[17] DDOS flowgen simulator, [Online]. Available: https://github.com/GaloisInc/ddosflowgen.