DOI: 10.35598/mcfpga.2025.008

FPGA Efficiency in Intrusion Detection Systems (IDS): A Formalized Assessment

Oleksandr Vorgul
ORCID 0000-0002-7659-8796
dept.Microprocessor Technologies and System
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
oleksandr.vorgul@nure.ua

Anton Sierikov
ORCID 0000-0002-3917-2008
dept.Microprocessor Technologies and System
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
anton.sierikov1@nure.ua

Oleksii Bilotserkivets
ORCID 0000-0002-8514-9650
dept.Microprocessor Technologies and System
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
oleksii.bilotserkivets@nure.ua

***Abstract*— This study examines the use of Field-Programmable Gate Arrays (FPGA) in the field of cybersecurity, with a particular focus on Intrusion Detection Systems (IDS). A formal analysis of key efficiency indicators is conducted, including energy efficiency, performance-to-cost ratio, and processing latency. A methodology for the quantitative assessment of these parameters is proposed, using comparative calculations for CPU, GPU, and FPGA platforms. Relevant scientific sources and practical data are included to support the analysis.**

Keywords*— PGA, IDS, energy efficiency, hardware acceleration, performance, latency.

I. Introduction

Now the networks are growing very quickly, and the attacks are becoming more tricky. Ordinary processors simply cannot cope with such a load. Video cards are fast, but they eat a lot of electricity, and it is not always convenient. Therefore, FPGA is increasingly used - these are such "smart" chips that can be customized to a specific task. They process a lot of data very quickly and do not consume so much energy. It is because of this that they are often taken for systems that should quickly catch attacks on the network [1], [2], [3].

II. FPGA in Cybersecurity

Programmed logical integrated circuits (FPGA) are flexible hardware platforms that allow you to reprogram hardware logic even after the device is manufactured. This possibility provides a significant advantage in the prompt renewal of protection algorithms without the need for physical replacement of equipment, which is especially important for modern cybersecurity systems, where the speed of response to new threats is critical.

FPGA architecture is characterized by a high degree of parallelism, which allows to process a large number of network packages simultaneously. This increases the capacity and reduces delays compared to classic CPU or GPU processor solutions. For the detection systems (IDS), which must function in real time, this feature is key, since even minor delays can lead to loss of important information or inability to detect the attack on time.

Another significant factor is the energy efficiency of FPGA. Due to the hardware implementation of computing algorithms directly at the level of logical elements, these devices use more efficiently electricity more efficiently than the software solutions on CPU and GPU. This reduces the total cost of operation and allows you to use FPGA in built-in systems or dates with limited power resources.

In addition, FPGA support the integration of cryptographic modules and traffic filtration mechanisms, which expands their functionality and increases the overall level of security of network systems.This allows you to implement a comprehensive approach to identifying and preventing cyberattacks, combining deep inspection of packages with confidential information protection.

Recent studies show that FPGA is successfully used for hardware acceleration of deep packages (DPI), network traffic processing, anomalies and adaptive real -time threats [4], [5]. In this case, the possibility of reprogramming FPGA allows you to quickly update algorithms according to changes in attackers' tactics, which significantly increases the efficiency of the IDS and extends the life of the system without significant investments.

Summarizing, it can be noted that the use of FPGA in the detection systems opens new horizons to build high - performance, energy efficient and adaptive solutions in the field of cybersecurity. Given the growing complexity and scale of network threats, the use of FPGA is one of the key areas for the development of modern information protection systems.

III. Methodology for Efficiency Evaluation

To assess platform efficiency, the following three indicators are used:

- Performance per Watt (energy efficiency):

$$\eta_p = R / P \quad (1)$$

where, R is the throughput and P is power consumption.

- Performance per Dollar (cost efficiency):

$$\eta c = R / C \quad (2)$$

where, C is the cost of the hardware.

- Latency per Gbit:

$$\delta^{R} = D / R \quad (3)$$

where, D is the absolute latency in milliseconds.

IV. Output and calculations

The following characteristics were used to compare the efficiency of different hardware platforms:

- CPU: Intel Xeon Silver [1];
- GPU: nvidia tesla t4 [2];
- FPGA: Xilinx Zynq-7000 [3].

The data are taken from the official technical specifications of manufacturers and projects that ensure the accuracy of performance estimates.

TABLE I. Baseline Hardware Characteristics for IDS Platforms

Platform	Throughput (R), Gbit/s	Latency (D), ms	Power (P), W	Cost (C), USD
CPU	1.2	4.0	95	500
GPU	3.8	2.0	250	800
FPGA	10.5	0.3	45	650

TABLE II. Calculated Efficiency Metrics for IDS Hardware Platforms

Platform	η_p (Gbit/s $\cdot W^{-1}$)	ηc (Gbit/s $\cdot USD^{-1}$)	δ^R (ms$\cdot$ Gbit^{-1})
CPU	0.0126	0.0024	3.33
GPU	0.0152	0.00475	0.526
FPGA	0.2333	0.0162	0.0286

V. Analysis of results

The data obtained clearly demonstrates the significant advantages of FPGA in three main performance indicators.

First, FPGA energy efficiency is significantly higher than the traditional CPU and GPU. In particular, FPGA is almost 19 times more than CPU and 15 times - GPU by performance indicator for OJSC. This is of particular importance in the context of the date centers and built-in systems, where limited energy consumption is a critical factor. The use of FPGA can significantly reduce electricity costs, as well as reduce thermal load, which has a positive effect on the reliability and duration of the equipment.

Second, the economic efficiency of FPGA is also a significant advantage. According to calculations, productivity per unit of value in FPGA exceeds CPU 6.75 times and GPU - more than 3.4 times. This means that investments in FPGA provide a higher return, which is a significant argument when choosing a hardware platform for cybersecurity systems.

The third key indicator is the delay of traffic processing. FPGA shows minimal delays that are 116 times smaller than the corresponding CPU rates and almost 18 times smaller than GPU. This difference is especially important for invasion (IDS) detection systems where the efficiency of potential threats determines the effectiveness of protection. Low delay makes it possible to detect and block attacks almost in real time, which significantly increases the level of network safety.

In addition to the advantages, FPGA has another important quality - the ability to reprogramming to support new algorithms for detecting attacks without the need to replace hardware. This significantly prolongs the life cycle of the system, allowing you to respond quickly to the evolution of cyber threats and reducing the total cost of modernization [6].

Thus, the set of these factors confirms the feasibility of using FPGA in modern cybersecurity systems, especially where high productivity, energy efficiency and rapid adaptation to new challenges are required.

VI. Conclusions

The study confirmed that FPGA is the most effective among the three hardware platforms under key criteria - energy efficiency, economic feasibility and delayed data processing. The proposed evaluation technique allows you to objectively and quantify different architectures, which is important for making informed decisions when choosing equipment for invasion detection systems (IDS).

Due to its low energy, high bandwidth and minimal delays, FPGA meets the requirements of modern cyber threats, where the rapid reaction to attacks and efficient processing of large traffic flows is critical. The use of FPGA provides an optimal balance between productivity and cost, which makes them an attractive option to build reliable and scaled IDS.

Prospects for further research include the development of more detailed modeling of FPGA platform behavior under different load conditions and types of network traffic. This will help to predict productivity more accurately and determine the optimal configurations for specific applications.

It is also important to develop hybrid architectures that combine the benefits of FPGA with CPU and GPU computing capabilities, which opens up new opportunities to create IDS adaptive systems with high efficiency and flexibility.

In addition, automation of the process of transmitting signatures of popular threat detection systems, such as Snort and Suricata, in the HDL code for FPGA will greatly simplify the development of hardware solutions and respond faster to the emergence of new threats.

In general, the integration of FPGA into modern cybersecurity systems is a promising area that requires further study and development, taking into account the fast -variable conditions of network attacks [8].

References

[1] Intel Corporation, *Intel Xeon Silver Specifications*. [Online]. Available: https://ark.intel.com

[2] NVIDIA Corporation, *Tesla T4 Datasheet*. [Online]. Available: https://developer.nvidia.com/tesla-t4

[3] Xilinx Inc., *Zynq-7000 Overview*. [Online]. Available: https://xilinx.com

[4] NetFPGA Project. [Online]. Available: https://netfpga.org

[5] S. Dharmapurikar, P. Krishnamurthy, and D. Taylor, "Deep Packet Inspection Using Parallel Bloom Filters," *IEEE Micro*, vol. 26, no. 1, pp. 52–61, Jan.–Feb. 2006, doi: 10.1109/MM.2006.6.

[6] R. Sivaraman, O. Spatscheck, J. Van der Merwe, and L. Peterson, "Packet Processing with Reconfigurable Hardware," in *Proc. ACM SIGCOMM*, 2016, pp. 99–112, doi: 10.1145/2934872.2934885.

[7] [7] A. Shabtai, Y. Elovici, and L. Rokach, "FPGA for IDS Acceleration," *arXiv preprint arXiv:2203.07544*, 2022. [Online]. Available: https://arxiv.org/abs/2203.07544

[8] Cisco Systems, *Snort vs Suricata*. Cisco Whitepaper, 2021. [Online]. Available: https://www.cisco.com/c/en/us/products/security/snort/index.html