DOI: 10.35598/mcfpga.2025.026

FPGA IDS Systems Architecture - Modern Approaches and Implementation

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

***Abstract*— The article presents an overview of modern architectures of systems of detection of invasion (IDS) implemented on the basis of programmable logical integral schemes (FPGA). The key benefits of FPGA, such as high speed, parallel data processing and energy efficiency, which make them promising for use in high -loaded networks are considered. The basic approaches to the IDS projection on FPGA are analyzed compared to traditional software solutions, and their strengths and weaknesses are highlighted. Separately investigated calls related to scalability, algorithms updating and integration into existing network infrastructures. The results of the work can serve as the basis for the further development of hardware IDSs aimed at improving the safety of computer networks.**

Keywords*— *FPGA, Intrusion Detection System (IDS), hardware, detection of invasion, network protection, parallel data processing, high -speed networks, digital security systems, IDS architecture, energy efficiency.

I. Introduction

In modern computer networks, cybersecurity issues are becoming increasingly important, and the detection systems (IDS) play a key role in protecting information resources. IDS software is often unable to provide the required speed in high -applied media. In this regard, interest in hardware solutions based on FPGA - programmable logical integrated schemes, which allow to implement high -performance parallel traffic processing with minimal delays. The article deals with modern FPGA IDS construction approaches, their architectural features, advantages and restrictions, and compares their effectiveness with traditional software solutions. [1], [2], [3].

II. Review of Twing Technologies and FPGA role

In modern information networks, the amount of data transmitted every second is growing rapidly, and cyberattacks are becoming more complex and diverse. This creates significant challenges for intrusion -detection Systems (IDS), which are intended to identify potential threats and warn the network administration in a timely manner. IDS are usually divided into two categories: Network IDS, NIDS, analyzing traffic at network devices, and host (HOST IDS, Hids), which are focused on the safety of individual computers or servers.

Traditional IDS software systems such as Snort, Suricata or Bro (Zek) are widely used in industry. They are based on the analysis of the signatures of known attacks or on the detection of anomalies in network traffic behavior. However, with increasing data and increasing networks, which reach tens and hundreds of gigabit per second, software solutions are often not fast enough. Real -time traffic processing is critical with minimal delays, as delayed attack can lead to loss of confidential data or violation of systems integrity [4], [10].

It is in such conditions that hardware accelerators gain special weight. Field-Programmable Gate Arrays (FPGA) has become a popular platform for the development of high-performance IDS. FPGA provides the ability to implement complex algorithms for traffic analysis using parallel processing, which significantly increases speed compared to traditional processor solutions.FPGA's flexibility not only accelerate existing algorithms, but also quickly adapt to new types of attacks by updating software without having to change the hardware. [5], [9].

The benefits of using FPGA in IDS systems include:

• parallel data processing, which allows to analyze large flows of information simultaneously.

• Low reaction delays, which is especially important for real time.

• the possibility of flexible algorithms, thanks to reprogrammed architecture.

• Energy efficiency compared to the use of large CPU or GPU arrays.

Thanks to these properties, FPGA IDSs have been used in various fields, including telecommunications, banking, government agencies and other critical infrastructures.

However, the development of IDS on FPGA has its challenges. It requires a high level of specialized knowledge in the field of hardware projection and optimization. Updating algorithms requires FPGA reprogramming, which can be more complicated than updating ordinary software. It is also necessary to consider the limits on resources on the FPGA itself, which can affect the scalability of the system [6].

Summarizing, FPGA open up new opportunities to increase the productivity and reliability of invasion detection systems, giving the balance between hardware efficiency and software flexibility. Further development of FPGA technologies and their integration with other platforms, such as CPU and GPU, promises a significant improvement in the security of modern computer networks [8].

III. Architectural approaches to IDS systems based on FPGA

IDS detection systems (IDS) built on programmable logical integrated circuits (FPGA) are a promising direction for network protection tools. In order to achieve high performance and low delays in network traffic processing, it

is necessary to properly design the architecture of such systems, taking into account the FPGA hardware features and real -time requirements [2].

The typical FPGA-IDS architecture includes several main components. First, I/O's (I/O) I/O) interfaces provide and transmit traffic through high-speed channels such as 10/40/100 GB Ethernet. The reliability and capacity of these interfaces are critical to prevent package loss. Secondly, the preprocessing module that filters, decoding protocols and preparation of data for further analysis. Third, the main module of analysis and identification of threats where algorithms for finding known signatures of attacks, anomalies or behavioral analysis are implemented. Hardware structures, such as Acho-Solder, are widely used here for the quick search of multiple templates. Finally, the reaction module responsible for the alerting, the logic of events and the interaction with other security systems [3].

There are several architectural approaches to FPGA-ISS. The first is the Pyplein Architecture, in which the processing of traffic is divided into consecutive stages, which are performed in parallel in the form of a conveyor. This allows high bandwidth and low delays, but requires the balance of resources between the stages.The second is a modular architecture consisting of independent hardware blocks that simultaneously analyze different protocols or types of traffic. This approach simplifies scaling and adding new functions, but can lead to considerable hardware costs. The third is a hybrid architecture where FPGA is combined with CPU or GPU, distributing the load between hardware acceleration and software analysis. This allows you to effectively balance between speed and flexibility [6], [8].

The advantages of FPGA-ISS include the possibility of parallel processing of large data flows, minimal delays in threats, flexibility of reprogramming and energy efficiency compared to traditional CPUs. At the same time, the development of such systems is complex and requires deep knowledge of hardware projection, as well as taking into account the restrictions on FPGA resources and the need to integrate with existing infrastructure. Algorithms are updated, although possible, more time consuming than software solutions [7], [8].

Among the examples of successful FPGA-IDS implements is the use of Acho-ship algorithm to find many signatures at the same time, which optimizes the speed and accuracy of attack detection. Hardware implementation of machine training methods to identify anomalies, which opens new prospects in improving the efficiency of security systems, is also being developed.

Thus, the right choice of architectural approach to FPGA-IDS is a key factor in success in creating effective invasion systems that can work in modern high-speed networks and provide reliable protection against cybergromes.

IV. FPGA -BASED INVASION ALGORITHMS

FPGA -based IDS detection systems use different algorithms to effectively analyze network traffic in real time. The main approaches are divided into the search for signatures (Signature-Based Detection) and the analysis of anomalies. The search for signatures is based on comparable input data with a set of known templates of attacks. One of the most common algorithms in this class is the Acho-Corasick algorithm (AHO-Corasick (AC), which creates a deterministic finite machine for simultaneous search for a set of row panels in the data stream. The main functions of the machine are the transition function $\Delta : Q \times \sigma \rightarrow Q$ and recovery function $f: Q \rightarrow Q$, where Q is the set of states and σ is the alphabet of characters. The search process is a sequential transition to the state of the machine depending on the input character, which provides a linear search time relative to the length of the text [3].

Bloom filters (Bloom Filters) are widely used for pre - filtration of traffic - compact bit structures that allow you to quickly check whether the plural element is owned with a certain probability of false work, but without false failures. To add the element X to the filter use K of independent hash functions H_1, H_2, ..., H_k, each of which returns the bit index in a bit vector length m. When adding the item, bits are set on positions calculated by these hash functions by formula:

$$\text{for each } i \in \{1, 2, ..., k\} \text{ set a bit b } [h_i (x)] = 1, \quad (1)$$

where, **b** is a filter bit. When checking the item of the item, all the corresponding bits are checked.If at least one of them is zero, the element is definitely absent; If all are units, then the element is probably present.

Analysis of anomalies, unlike the search for signatures, is aimed at identifying deviations from the normal behavior of traffic, which may indicate new or unpredictable attacks. For this purpose statistical methods are often used, such as the distance of mahalanobis, which is defined as:

$$D_m (x) = \sqrt{(x - \mu)^{T} T1 (x - \mu)}, \quad (2)$$

Where, **x** is the vector of current observation, μ is the average vector of normal behavior, and S is a covariation matrix. If d_m (x) exceeds the designated threshold, observation is classified as abnormal [7].

Also for the analysis of anomalies are used models of machine learning, which are implemented on FPGA using methods of quantization of scales and optimization of structure to reduce resources, which allows to perform calculations at high speed without significant loss of accuracy.

TABLE I. COMPARISON OF INTRUSION DETECTION ALGORITHMS BY KEY CHARACTERISTICS

Algorithm	Detection Type	Parallelism	Implementation Complexity	Performance	Application Area
Aho-Corasick	Signature -based	High	Mediu m	High	Detection of known attacks
Bloom Filter	Pre-filtering	High	Low	High	Reducing analysis volume
Statistica l Methods	Anomaly Detection	Mediu m	Mediu m	Mediu m	Detection of new attack types
Machine Learning	Anomaly Detection	Low – Mediu m	High	Mediu m – High	Complex patterns, behaviora l analysis

V. Analysis of results

In order to evaluate the effectiveness of FPGA intrusion detection systems, several open -ended research, accuracy, and hardware use, have been analyzed by FPGA. The main metrics of comparisons were: bandwidth, delay, accuracy, false -positive (FPR) and false -negative (FNR) probability, and consumption of logical elements FPGA.

In the works where the Acho-Salt algorithm was used to search for signatures (for example, in the implementation on Xilinx Virtex-7 and Intel Stratix V), a capacity of more than 10 Gbps was reached with a delay of not more than 5 μs. This provides the ability to work on high -speed networks without loss of packages. At the same time, Bloom filters are also shown higher capacity (up to 20 Gbps), but with some likelihood of false work (up to 1-3%), which is acceptable at the pre -filtration stage.

Anomal analysis systems usually require more computational complexity and deeper integration of behavior models. For example, the implementation with the distance of maholanobis reaches the accuracy of detection of 85-92%, depending on the configuration and quality of the training sample. At the same time, such systems have a higher delay (up to 50 μs), which can be critical for networks with stringent reaction requirements.

Models of machine learning (especially on the basis of simplified neural networks or trees) have proved effective in identifying complex attacks, including zero day. However, for their implementation on FPGA requires optimization - quantization of scales, reducing the bit of calculations, transformation of models into streaming structures. In such cases, productivity reaches 2-4 Gbps with an accuracy of more than 95%, but with a high load on resources (up to 70% of PL logic).

Table 2 presents comparative results for four basic approaches, taking into account real research data.

TABLE II. Comparative Analysis of Performance and Accuracy of FPGA-based IDS Algorithms

Approach	Throughput	Accuracy	Latency	Logic Utilization	False Positive Rate
Aho-Corasick	~10 Gbps	98–99%	≤ 5 μs	Medium	< 0.1%
Bloom Filter	~15-20 Gbps	~95%	≤ 3 μs	Low	~2–3%
Mahalanobis Distance	~1–2 Gbps	85–92%	≤ 50 μs	Medium	~1–5%
Machine Learning	~2–4 Gbps	95–98%	10–30 μs	High	< 1%

The analysis shows that the choice of IDS architecture on FPGA depends largely on the target scenario. For high-speed network traffic, it is advisable to use Bloom filters as a preliminary step, combined with Acho-ship for accurate comparison. Anomalous systems and machine learning are more efficient in more complex environments that require a deeper semantic understanding of traffic, but they need more resources and have a higher delay.

VI. Conclusions

The study analyzes modern approaches to the construction of systems of detection of invasion (IDS) implemented on the basis of programmable logical integrated circuits (FPGA). The main architectural solutions, the algorithms for the search and analysis of anomalies, as well as their hardware implementation, taking into account the features of FPGA, were considered.

The results indicate that FPGA platforms provide high productivity, processing parallel and low delay, which makes them ideal for real-time tasks. Signature search algorithms, including Acho-Soldier, are well-scale and high accuracy with low load on resources. The methods of analysis of anomalies, including statistical models and machine training, effectively identify new types of attacks, but require more computational capacity and complex optimization of models for FPGA.

Thus, the choice of architecture depends on the requirements for the system: reaction rate, type of attacks, available resources and the level of admission to false positive results. A promising area is the creation of hybrid IDS systems that combine filtration, signature analysis and adaptive machine training at the hardware acceleration level..

References

[1] [1] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in Proc. IEEE Symposium on Security and Privacy, 2010, pp. 305–316.

[2] [2] K. P. Kannan and S. Srinivasan, "FPGA-based architecture for high-speed intrusion detection system," IEEE Transactions on Computers, vol. 68, no. 5, pp. 732–744, May 2019.

[3] [3] A. Aho and M. Corasick, "Efficient string matching: an aid to bibliographic search," Communications of the ACM, vol. 18, no. 6, pp. 333–340, 1975.

[4] [4] B. Bloom, "Space/time trade-offs in hash coding with allowable errors," Communications of the ACM, vol. 13, no. 7, pp. 422–426, 1970.

[5] [5] J. C. Lin and C. L. Chou, "FPGA-based flexible intrusion detection system architecture," Journal of Network and Computer Applications, vol. 78, pp. 62–72, 2017.

[6] [6] S. Ghosh and K. Basu, "Real-time network intrusion detection on FPGA using signature matching," in Proc. ACM Symposium on Applied Computing, 2018, pp. 987–993.

[7] [7] M. Shahriar, A. M. Rahmani, and F. Khorrami, "FPGA implementation of anomaly detection using Mahalanobis distance for network security," IEEE Access, vol. 7, pp. 162320–162329, 2019.

[8] [8] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436–444, 2015.

[9] [9] L. Xie and Y. Wang, "Energy-efficient FPGA implementation of IDS for high-speed networks," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 28, no. 10, pp. 2345–2357, 2020.

[10] M. Roesch, "Snort - Lightweight intrusion detection for networks," in Proc. USENIX LISA, 1999, pp. 229–238.