Using GRID for Centralized Synthesis of FPGA-based Information Security Systems

Viktor Evdokimov
Dept. of Mathematical and Computer Modelling
Pukhov Institute for Modelling in Energy Engineering of NAS of Ukraine
Kyiv, Ukraine
evdokimov@ipme.kiev.ua

Anatoly Davydenko
Dept. of Mathematical and Econometric Modelling
Pukhov Institute for Modelling in Energy Engineering of NAS of Ukraine
Kyiv, Ukraine
davydenko@ipme.kiev.ua

Serhii Hilgurt
Dept. of Mathematical and Econometric Modelling
Pukhov Institute for Modelling in Energy Engineering of NAS of Ukraine
Kyiv, Ukraine
hilgurt@ipme.kiev.ua

Abstract. **The functioning of such signature-based information security tools as network intrusion detection system, antivirus, anti-worms and others are based on solving in real time resource-intensive task of multi-pattern string matching. Due to rising traffic rates, increasing number and sophistication of attacks and the collapse of Moore's law, traditional software solutions can no longer keep up. Therefore, hardware approaches are frequently being used by developers to accelerate pattern matching. Reconfigurable FPGA-based devices, providing the flexibility of software and the near-ASIC performance, have become increasingly popular for this purpose. Signature databases of the current information security systems contain hundreds of thousands and even millions of rules. Every signature database update or change in network parameters forces the digital circuit of such system to be resynthesized, and the FPGA – to be reconfigured. To facilitate such reconfigurations we propose a centralized service for information security reconfigurable tools synthesis, which uses free high-performance resources of GRID infrastructure.**

Keywords: **security, signature, FPGA, GRID, centralization**

I. INTRODUCTION

The propagation of Internet and network technologies in both industrial and civil enterprises together with the widespread availability of system hacks and viruses have made the importance of network security more significant. The increase in number and sophistication of attacks against the network infrastructure and computer systems requires more robust security solutions. Unfortunately, despite the great progress made in deep neural networking (DNN), security tools based on such methods still suffer from nonzero recognition error probability.

This work was supported in part by the Informatization program of the NAS of Ukraine in 2020-2024.

Even as low false positive rate as 0.01% is able to disrupt the correct operation of the information system [1]. Using such systems in critical infrastructure can have disastrous consequences. Therefore, signature-based recognition methods with their theoretically exact match are still relevant when creating information security systems.

The main disadvantage of the signature-based principle is its computational complexity. Checking every byte of every packet to see if it matches one of set of hundred thousand strings becomes a major performance bottleneck in traditional software solutions which have to scan the incoming data in real time [2]. To keep up with these speeds a specialized device is required.

Different types of available hardware solutions are result in higher efficiency. Among them the Field Programmable Gate Array (FPGA) devices have commonly been proposed because they feature both the flexibility of software and the high performance of specialized hardware at a reasonable cost [3]. The reconfigurable accelerators based on FPGAs became a suitable and popular hardware platform for many security applications, including network intrusion detection/prevention systems (NIDS/NIPS) [4], antivirus, anti-worms and other signature-based information security tools. The main difficulty when using programmable logic is to synthesize the digital circuit and generate the appropriate configuration file (bitstream) for the FPGA device to give it required functionality. This process is quite complicated and requires the efforts of a highly qualified developer. Not every firm or enterprise can afford such an asset.

As a solution we propose a centralized service for security tasks hardware accelerators synthesis. Such service can use computation power of GRID or other high performance equipment to process requests

Pattern Recognition and Information Processing (PRIP'2021) : Proceedings of the 15th International Conference, 21–24 Sept. 2021, Minsk, Belarus. – Minsk : UIIP NASB, 2021. – 246 p. – ISBN 978-985-7198-07-8.

from users to obtain desired FPGA configuration files.

II. FPGA-BASED NETWORK INTRUSION DETECTION/PREVENTION SYSTEMS

Historically the first and therefore the most studied FPGA-based tools of information security were network intrusion detection systems [5]. Without losing the generality of reasoning, consider the typical functions of reconfigurable security systems on the example of NIDS/NIPS.

The generalized structure and the content of a NIDS/NIPS based on FPGA can be compiled on the basis of a number of well-known works [5, 6] (Fig. 1).

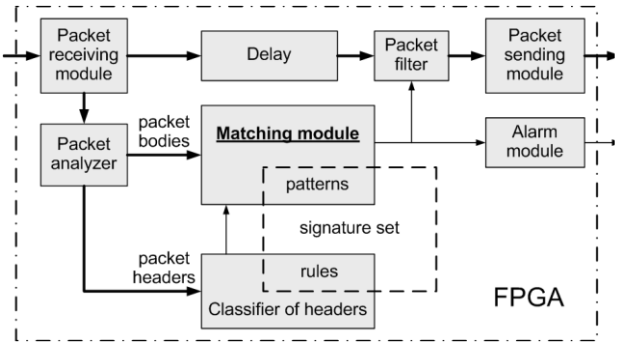

Fig. 1. The generalized structure of the FPGA-based network intrusion detection/prevention system

The Matching module is the most important component of NIDS/NIPS. It solves a computationally complex task of multi-pattern string matching, i.e. checks the content of network packets against certain sequences of symbols, so-called *patterns*, which are parts of the signatures – the descriptions of the known attacks.

Components Delay, Packet filter and Packet sending module are present only in NIPS option of the system.

III. UPDATING THE STRUCTURE OF RECONFIGURABLE SECURITY SYSTEM

As we can see when analyzing the structure shown above, the signature set is "wired" into the circuitry of the device at hardware level. This feature ensures the highest performance rate due to the maximally possible parallelism has been reached. On the other hand, any change in the circumstances of NIDS/NIPS functioning leads to the need to update the digital circuit. There are two possible reasons of such update. Firstly, new unknown attacks can emerge; consequently, new signatures have to be added into the signature set. Secondly, the operating conditions of the protected system can be changed (modification of the local network, change of its content or structure, modification of the software, etc.), resulting in necessity to add or remove whole classes of signatures, so the content of signature set is also to be changed. That is the digital circuit of the security tool needs to be re-synthesized, new bitstream to be obtained and loaded into the FPGA.

Analyzing of this structure shows that some components are independent from signature set, let's call them *constant modules*, whereas another parts have to be reconstructed obligatorily, we name them *variable modules*. The Packet receiving module, the Packet analyzer and the Alarm module belong to the first group. The Matching module and the Classifier of headers constitute the second one.

Thus, the key feature of reconfigurable information security system is the necessity occasionally to perform a so called *operational update procedure*, i.e. – to re-synthesize the variable modules and reconfigure the FPGA chip.

IV. ORGANIZING THE SYNTHESIS OF RECONFIGURABLE SECURITY TOOLS

Constructing reconfigurable devices is a complex and resource-intensive task. This task, firstly, requires high performance computer hardware. Generation of a bitstream, to be loaded into the FPGA chip, is usually fulfilled by a proprietary CAD software tool from the FPGA manufacturer and includes a number of computationally-intensive procedures such as Synthesize, Translation, Map, Place & Route and the Bitstream Generating. Depending on the complexity of the circuit and the type of FPGA, this process can take from tens of minutes to several hours. Secondly, the developers must have a high qualification and knowledge of digital device design specifics.

There are many approaches to build an FPGA-based scheme able to fulfill multi-pattern string matching [7]. Each of them has its own strengths and weaknesses. None of them demonstrates key advantages over others. The lack of the best solution, which exceeds the competitive ones by all technical parameters, makes the developers modify and elaborate the known approaches thoroughly.

That is why owners of information security systems do not have possibilities to solve this task on their own.

In this work, we propose to organize synthesizing reconfigurable tools so that complex and resource-intensive procedures are performed not locally on each individual system, but centrally, using free high-performance computer resources of GRID. Fig. 2 shows the principle of operation of a service that implements this approach.

Pattern Recognition and Information Processing (PRIP'2021) : Proceedings of the 15th International Conference, 21–24 Sept. 2021, Minsk, Belarus. – Minsk : UIIP NASB, 2021. – 246 p. – ISBN 978-985-7198-07-8.

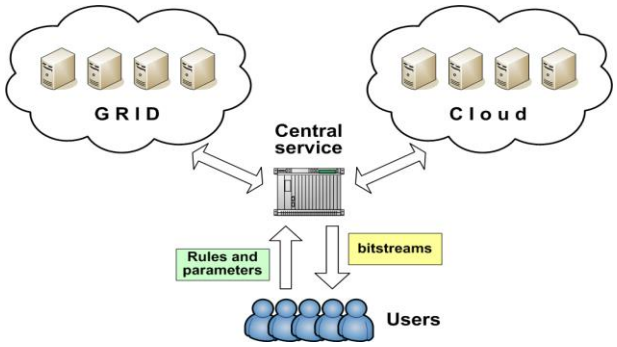

Fig. 2. Service for centralized synthesis of FPGA-based information security systems

Users send requests containing signature set (NIDS rules) and FPGA parameters to the central service. Central service using computation power of GRID infrastructure processes these requests, synthesizes digital circuits in automatic mode, compiles projects, generates bitstreams and returns them to users. To avoid a hypothetical situation when there are no free GRID resources, the service is able to use the cloud infrastructure as well.

V. GRID-Service

To verify the concept provided above the service was realized as a model sample on the base of computing cluster of Pukhov Institute for Modelling in Energy Engineering of NAS of Ukraine using the resources of Ukrainian National GRID (UNG). This project was named as Security Tasks Reconfigurable Accelerators GRID-Service (STRAGS).

In order to facilitate the solution of the problem the Rainbow framework, recently developed by Ukrainian scientists, was chosen as the functional base of the service [8]. This technology, in fact, implements a cloud service at the PaaS level over the GRID infrastructure by running virtual machines (VMs) equipped with all necessary software as GRID-jobs. To provide real-time interaction between the user and VM that run at remote GRID-node, special techniques was invented and applied by the developers of Rainbow. Initially, this technology was created to run specialized software "Moldyngrid" for the virtual organization "Medgrid" in the UNG environment. However, the work turned up successful and soon found wider use.

When functioning, the STRAGS service initiates the work of several agents on remote GRID-sites, which support Rainbow platform (Fig. 3). Wherein, every agent is a VM with all the necessary instrumental software preinstalled and configured for the synthesis of reconfigurable devices and generation of the bitstreams.

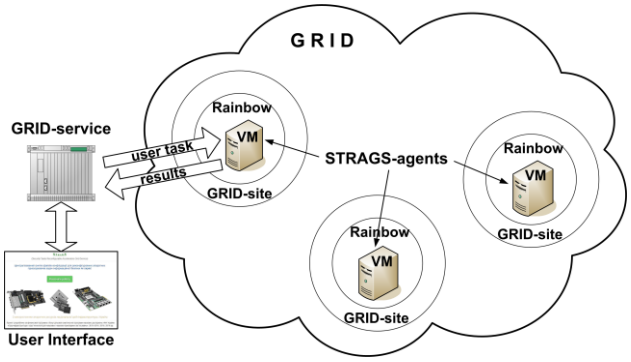

Fig. 3. STRAGS service functioning

As requests from clients are received, the service distributes tasks among active agents, maintaining their number sufficient to ensure required availability. Having received the task as a GRID-job, the agent starts the processes of automatic synthesis of the required digital circuit and synthesis of the corresponding configuration for the FPGA, and then returns the results of the work to the service.

Comparing to the traditional GRID-jobs batch submission, running an agent as a VM has several benefits:

- VMs already have FPGA synthesis software installed that simplifies the operational update procedure;
- pulling VMs from GRID-site allows to minimize latencies in synthesis task lifecycle;
- Rainbow framework interactive access feature allows extending service with debug capabilities and provides direct access to the platform with pre-installed synthesis software eliminating the need of local software copy;
- users have the ability to track the synthesis progress with a high granularity.

Fig. 4 presents one of STRAGS service user interface windows, which depicts a current security tool synthesis process progress (the substep "Placer" of the step "Place & Root" is fulfilling).

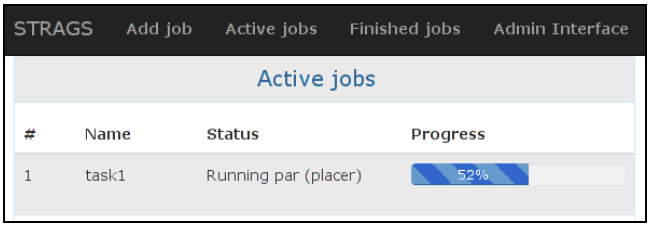

Fig. 4. User's job "task1" synthesis progress in the "Active jobs" window of the STRAGS service

The proposed architecture of GRID-service addresses issues of user's authorization, agent's

Pattern Recognition and Information Processing (PRIP'2021) : Proceedings of the 15th International Conference, 21–24 Sept. 2021, Minsk, Belarus. – Minsk : UIIP NASB, 2021. – 246 p. – ISBN 978-985-7198-07-8.

authorization and availability of a sufficient number of agents. It also implements centralized updating of VMs to ensure their relevance when distribution across the GRID infrastructure.

VI. Experimental Results

Verifying the service on a lot of test tasks did not allow us to obtain numerical estimates. Instead, significant quality benefits were identified:

1. Increasing of system performance in general due to the use of GRID and cloud which quickly synthesize the parallel matching circuits for modern FPGAs.
2. Improving the technical characteristics of local information security systems through the division of labor. Centralization allows the use of highly qualified specialists, whose work results are used on each of the local systems.
3. Lower total cost of ownership due to reducing staffing requirements for local systems.
4. Reducing overall computational costs by grouping similar requests.

As a minor disadvantage, the complexity of the whole system and some decrease in the speed of reconfiguring hardware components can be noted, which however is fully compensated by the listed advantages.

VII. Conclusion

In this work, the principle of centralized creation of FPGA-based information security systems is proposed. A GRID-service that implements this principle has confirmed the viability of the idea of transferring resource-intensive procedures from a local FPGA-based security system to a remote HPC environment.

It is worth noting that such a centralized service is applicable to the synthesis of any FPGA-based digital schemes, regardless of which recognition method it uses. It can be successfully used to build systems based on the mentioned above DNN approaches, when they become robust enough. In recent years, adversarial attacks detecting have become topical issue. Hardware solutions, including FPGA-based ones, are already used when corresponding systems constructing [9, 10].

References

[1] G. E. Dahl, J. W. Stokes, L. Deng, and D. Yu "Large-scale malware classification using random projections and neural networks," in IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), Vancouver, Canada, May 26-31 2013, New York: IEEE.

[2] B. Smyth, Computing Patterns in Strings. Essex: Pearson Addison Wesley, 2003.

[3] V. Paxson et al., "Rethinking hardware support for network analysis and intrusion prevention," presented at the USENIX First Workshop on Hot Topics in Security (HotSec), Vancouver, July 31, 2006.

[4] С. В. Казмірчук, А. О. Корченко, і Т. І. Паращук, "Аналіз систем виявлення вторгнень," Захист інформації, Т. 20, № 4, С. 259–276, 2018, doi: 10.18372/2410-7840.20.13425.

[5] T. Katashita, Y. Yamaguchi, A. Maeda, and K. Toda, "FPGA-based intrusion detection system for 10 Gigabit Ethernet," IEICE Transactions on Information and Systems, Article vol. E90D, no. 12, pp. 1923–1931, Dec 2007, doi: 10.1093/ietisy/e90-d.12.1923.

[6] Ю. М. Коростиль и С. Я. Гильгурт, "Принципы построения сетевых систем обнаружения вторжений на базе ПЛИС," Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ ім. Г.Є. Пухова НАН України, № 57, С. 87-94, 2010.

[7] W. Jiang, Y. H. E. Yang, and V. K. Prasanna, "Scalable multi-pipeline architecture for high performance multi-pattern string matching," in 24th IEEE International Parallel and Distributed Processing Symposium, IPDPS 2010, Atlanta, GA, 2010, doi: 10.1109/IPDPS.2010.5470374.

[8] А. А. Сальников, В. В. Вишневский, и А. Ф. Борецкий, "«Платформа как сервис» в грид для интерактивного анализа медицинских данных," Математичні машини і системи, № 1, С. 53-64, 2015.

[9] C. Song et al., "MAT: A Multi-strength Adversarial Training Method to Mitigate Adversarial Attacks," 2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Proceedings Paper, pp. 476–481, 2018, doi: 10.1109/isvlsi.2018.00092.

[10] M. Capra, B. Bussolino, A. Marchisio, G. Masera, M. Martina, and M. Shafique, "Hardware and Software Optimizations for Accelerating Deep Neural Networks: Survey of Current Trends, Challenges, and the Road Ahead," IEEE Access, Article vol. 8, pp. 225134–225180, 2020, doi: 10.1109/access.2020.3039858.

Pattern Recognition and Information Processing (PRIP'2021) : Proceedings of the 15th International Conference, 21–24 Sept. 2021, Minsk, Belarus. – Minsk : UIIP NASB, 2021. – 246 p. – ISBN 978-985-7198-07-8.