RISC-V Embedded AI for IDS Applications

Pierre Garreau, Pascal Cotret, Julien Francq, Jean-Christophe Cexus, Loïc Lagadec

RISC-V Embedded AI for IDS Applications

Pierre Garreau*†, Pascal Cotret†, Julien Francq‡, Jean-Christophe Cexus†, Loïc Lagadec†
* Chair of Naval Cyber Defense, École Navale (CC 600, 29240 Brest Cedex 9, France)
pierre.garreau@ecole-navale.fr
† Lab-STICC, UMR CNRS 6285, ENSTA-Bretagne (29806 Brest Cedex 9, France)
‡ Naval Group, Naval Cyber Laboratory (83190 Ollioules, France)

***Abstract*—IDSs (*Intrusion Detection Systems*) include more and more AI (*Artificial Intelligence*) engines to detect several attack types. However, in order to be efficient in both learning and inference phases, such systems must include hardware coprocessors to improve AI-related computations. In this PhD thesis, we would like to explore the capabilities of RISC-V based processors in this context. RISC-V is an open-source ISA (*Instruction Set Architecture*) than can be easily extended. The main goal of this thesis is to propose RISC-V extensions for an IDS embedded into collaborative and heterogeneous unmanned vehicles (submarine, marine, or aerial): it must detect abnormal behaviors and must be efficient in terms of power consumption, area and runtime overheads. Furthermore, coprocessors developed in this thesis should not introduce security breaches into the system. Finally, a proof-of-concept should be developed to demonstrate the efficiency of algorithms and hardware implementations compared to software solutions.**

I. Introduction

Nowadays, unmanned vehicles become more and more important for military forces. Whether aerial, marine, or submarine, whether they are on their own, or in a swarm, drones play a pivotal role in military mission strategies. Moreover, with the exponential growth of cyberattack methods, it becomes of paramount importance to figure out a way to ensure security of the communications between unmanned vehicles and their mothership, so that our systems remain impervious to novel attacks. For that matter, Machine Learning (ML) models have recently been highlighted as powerful paradigms for detecting intrusions. However, these models often coincide with substantial computational power and large memory needs.

As embedded devices on drones comes with power, battery life and memory constraints, traditional hardware architectures and ML models are unsuitable. To address the challenge of fitting ML algorithms to our use case, we would like to explore the capabilities of RISC-V based processors and to propose extensions that speed up AI-related computations. Hence, we discuss, in this work, several optimized ML models and techniques that could be embedded on unmanned vehicles. Then, we explore RISC-V based processor architectures that could speed up any AI-related computation, so that models execution times fit our applications context.

Section II presents related works: first, on ML techniques that are commonly brought up when dealing with IDSs based on ML; then, on ML algorithms hardware acceleration. Section III describes the goals of our work.

II. Related Work

A. AI for IDS

For a couple of years, researchers have put a lot of effort into applying ML to IDSs. Ferrag et al. [1] presents several deep learning techniques for intrusion detection, dividing 7 different models into 2 categories: deep discriminatives models and generative/unsupervised models.

The first category includes DNN (*Deep Neural Network*), RNN (*Recurrent Neural Network*) and CNN (*Convolutional Neural Network*). These models are commonly used in ML and tend to output decent results on IDS applications, according to [1].

The second category considers RBM (*Restricted Boltzmann Machine*), DBN (*Deep Belief Network*), DBM (*Deep Boltzmann Machine*) and DA (*Deep Autoencoder*).

Various other ML techniques have been investigated as well. For example, Bouazzati et al. [2] implement a Reinforcement Learning (RL) based IDS using a periodic offline training, as online learning would increase significantly the resources consumption of the IDS. Farnaaz et Jabbar [3] introduce an IDS based on another ML model: RF (*Random Forest*). According to the authors, these techniques allow obtaining commendable results and outperform traditional IDSs that are not based on AI. Indeed, as depicted by Choudhary et al. [4], these traditional techniques are mostly based on signatures and specifications, and get gradually surpassed by anomaly-based techniques that include AI.

Furthermore, considering the IDS is supposed to be embedded in a drone or a swarm of drones leverages the need for more specific ML models, such as Federated Learning or Multi-Agent based IDS for example [5].

B. Machine learning hardware acceleration

As previously mentioned, constraints arising from the utilization of drones may prevent from using ML for intrusion detection. This is where RISC-V based architectures can possibly prove themselves advantageous. Thanks to its extendability, RISC-V allows to build hardware dedicated to computation acceleration, and therefore, enables the utilization of heavy and powerful algorithms such as ML models.

The main deep learning models that have been hardware accelerated are CNNs. Computations behind CNN are known to be heavy and costly, particularly the convolution operation. To address this challenge, Kovacevic et al. [6] developed a RISC-V processor that includes a traditional scalar processor and a

vector processor. Both cores work together and optimize the workload so that any vector or matrix-based operation, such as convolution operations, are performed by the vector core. This optimization becomes achievable through the creation of new instructions added to RISC-V basic instruction set. Wu et al. [7] added their own instructions to RISC-V instruction set as well, in order to link a coprocessor to the main processor and use it to speed up AI-related computations.

DNNs can be hardware accelerated as well. For example, Askarihemmat et al. [8] designed a DNN accelerator called BARVINN that includes Matrix Vector Units (MVUs), which are hardware processing elements that speed up computations such as GEMV (General Matrix-Vector) and GEMM (General Matrix Multiply) operations, convolutions, batch normalization and so on. Vermat et al. [9] also developed an accelerator, using new instructions as well, but, on top of that, they described a complete co-design method to optimize the energy efficiency of their solution.

The acceleration of ML algorithm can also be achieved by quantization. This technique aims to reduce the computation time and cost by optimizing data precision. Sanchez-Flores et al. [10] represent the weights of their CNN with multi-precision to optimize the memory usage of their CNN and its runtime. By finding a fair trade-off between accuracy of the model and resource consumption efficiency, some large models can easily fit on embedded devices and meet our application's requirements.

III. Our Goals

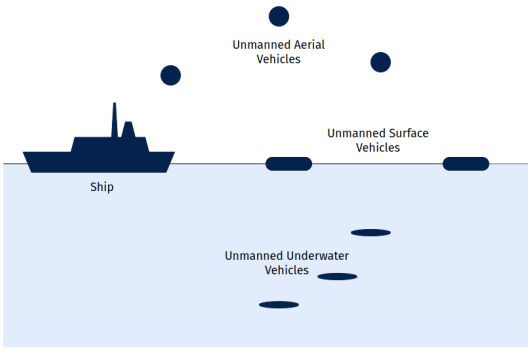

Fig. 1. Global situation.

The purpose of our work is to secure communications in a swarm of drones by designing an IDS. Explicitly, by improving and combining state-of-art methods discussed in Section II, we want to build a RISC-V extension for a custom coprocessor. This coprocessor should implement traditional ML classification algorithms such as DNN, CNN or RFs, but should also enhance the utilization of other various ML algorithm such as RL, trained for intrusion detection in a swarm of unmanned aerial, surface and underwater vehicles.

There are several challenges to address because of the situation described on Figure 1. First, the differences between considered devices may be challenging during the training of the ML algorithm. These differences trigger the utilization of various communication protocols, that can rely on highly different peripherals, depending on the drone's type and brand, for example. Hence, a dataset that would include state-of-art attacks on enough different drones so that our model is able to detect attacks of any kind, on any of the drone in the swarm, is, as of writing, unavailable. Then, gathering all types of attacks will be challenging as well, but will determine the robustness of our IDS. Eventually, our hardware solution must not introduce any security breach in the system. Therefore, resisting any kind of hardware attack such as fault injection or side-channel analysis would be a nice feature to have.

IV. Conclusion

In this PhD thesis, we focus on securing communications of unmanned vehicles in a swarm of drones in a military situation. To achieve this, we would like to benefit from RISC-V capabilities and propose an extension to the basic instruction set to build an hardware architecture that will enhance the acceleration of as many ML models as possible, to extend the utilization of our accelerator beyond intrusion detection.

Acknowledgement

Funded and supported by Ecole navale, ENSM, ENSTA Bretagne, IMT Atlantique, Naval Group and Thales.

References

[1] M. A. Ferrag, L. Maglaras, H. Janicke, and R. Smith, "Deep Learning Techniques for Cyber Security Intrusion Detection : A Detailed Analysis," in *6th International Symposium for ICS & SCADA Cyber Security Research 2019*, 2019.

[2] M. E. Bouazzati, R. Tessier, P. Tanguy, and G. Gogniat, "A Lightweight Intrusion Detection System against IoT Memory Corruption Attacks," in *2023 26th International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS)*. IEEE, 2023, pp. 118–123.

[3] N. Farnaaz and M. Jabbar, "Random forest modeling for network intrusion detection system," *Procedia Computer Science*, vol. 89, pp. 213–217, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050916311127

[4] G. Choudhary, V. Sharma, I. You, K. Yim, I.-R. Chen, and J.-H. Cho, "Intrusion detection systems for networked unmanned aerial vehicles: A survey," in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, 2018, pp. 560–565.

[5] S. Ouiazzane, F. Barramou, and M. Addou, "Towards a Multi-Agent based Network Intrusion Detection System for a Fleet of Drones," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 10, 2020.

[6] N. Kovacevic, D. Miseljic, and A. Stojkovic, "Risc-v vector processor for acceleration of machine learning algorithms," in *2022 30th Telecommunications Forum (TELFOR)*, 2022, pp. 1–4.

[7] N. Wu, T. Jiang, L. Zhang, F. Zhou, and F. Ge, "A reconfigurable convolutional neural network-accelerated coprocessor based on risc-v instruction set," *Electronics*, vol. 9, no. 6, 2020. [Online]. Available: https://www.mdpi.com/2079-9292/9/6/1005

[8] M. Askarihemmat, S. Wagner, O. Bilaniuk, Y. Hariri, Y. Savaria, and J.-P. David, "Barvinn: Arbitrary precision dnn accelerator controlled by a risc-v cpu," in *Proceedings of the 28th Asia and South Pacific Design Automation Conference*, ser. ASPDAC '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 483–489. [Online]. Available: https://doi.org/10.1145/3566097.3567872

[9] V. Verma, T. Tracy II, and M. R. Stan, "Extrem-edge—extensions to RISC-V for energy-efficient ml inference at the edge of IoT," *Sustainable Computing: Informatics and Systems*, vol. 35, p. 100742, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2210537922000749

[10] A. Sanchez-Flores, L. Alvarez, and B. Alorda-Ladaria, "A review of cnn accelerators for embedded systems based on risc-v," in *2022 IEEE International Conference on Omni-layer Intelligent Systems (COINS)*, 2022, pp. 1–6.