Network Intrusion Detection Using Neural Networks on FPGA SoCs

Lenos Ioannou and Suhaib A. Fahmy

School of Engineering, University of Warwick, UK

WARWICK
THE UNIVERSITY OF WARWICK

Introduction

WARWICK
THE UNIVERSITY OF WARWICK

- Mainstream approaches in intrusion detection do not scale well to the embedded domain, mainly due to computational complexity
- Limited computing power at the nodes, not intended for significant security mechanisms
- More lightweight security mechanisms required, adaptable to updates
- Explore the use Neural Networks as a more lightweight Network Intrusion Detection approach

Intrusion Detection Neural Network

WARWICK
THE UNIVERSITY OF WARWICK

- NSL-KDD dataset:
  - Used 29 of the 41 features of each record (3 in categorical form)
  - 110 inputs after one-hot encoding
- Trained a NN with 110-21-2, similar to that in [1], with Tensorflow [2]
- Obtaining at best:
  - **96.02%** accuracy on the train set
  - **80.52%** accuracy on the test set

Test set classification results

Predicted Class	Actual Class	
	Normal	Malicious
Normal	9257	3937
Malicious	454	8896

HLS Implementation

WARWICK
THE UNIVERSITY OF WARWICK

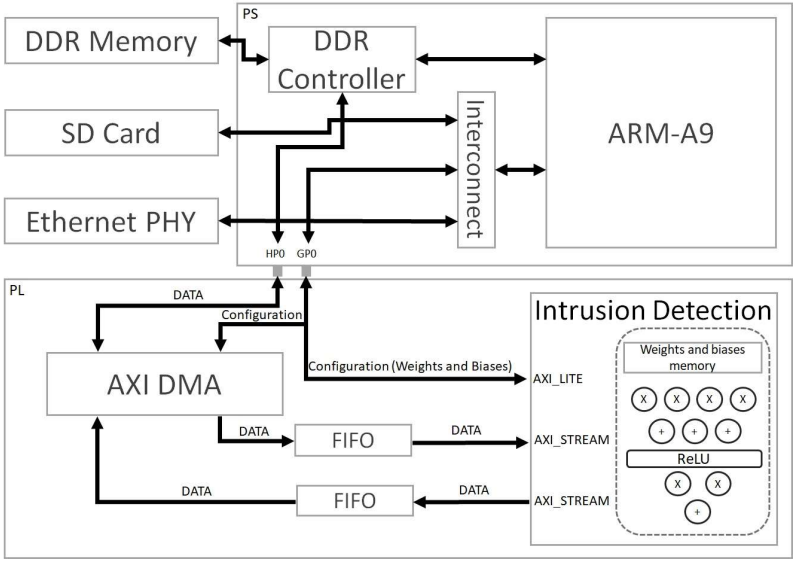
- Vivado High Level Synthesis 2016.4, targeting a Xilinx Zynq Z-7020
  - Use of memories as Look-Up-Tables, inputs restored to 29
  - Use of floating point IEEE-754 to support coefficient updates
  - Configurable weights and biases through AXI-Lite (2375) : **2.3ms**
  - Resource utilization:

	LUTs	FFs	DSPs	BRAM
Utilized	26463	56478	111	88
Available	53200	106400	220	280
% Utilization	50	53	50	31

  - Timing results:

Frequency (MHz)	Latency (Clock Cycles)	Initiation Interval (Clock Cycles)
76	237	29

FPGA System-Implemented System



- Execution time-Test set:

Arm-A9 [a] @667MHz	Arm-A9 [b] @667MHz	Accelerator [b] @76MHz	Idhammad et al. [3] (normalized)
4751.440ms	1458.1ms	9.018ms	240.136ms

[a] Unoptimised, 110 inputs.
[b] Optimised, Look-Up-Table.

- Detection rate (IPv4 min-576B):

Transfer Rate (Packets/Second)	Platform	Latency (µs)	Detection Rate (Packets/Classification)
1Gbps (217,014)	Arm-A9	64.678	14.036
	Accel	0.4	0.0868
10Gbps (2,170,139)	Arm-A9	64.678	140.360
	Accel	0.4	0.8680

Conclusion

WARWICK
THE UNIVERSITY OF WARWICK

- Network Intrusion Detection NN with moderate complexity
- Flexible accelerator that adapts to newly trained weights dynamically
- Offers fast detection rate, within a single packet

Future work

- Explore different and alternative network topologies
- Extend our approach to other datasets
- Explore approaches that reduce latency

WARWICK
THE UNIVERSITY OF WARWICK

References

[1] B. Ingre and A. Yadav. Performance analysis of NSL-KDD dataset using ANN. In Proc. International Conference on Signal Processing and Communication Engineering Systems, pages 92–96, 2015.

[2] Martin Abadi et al. TensorFlow: Large-scale machine learning on heterogeneous systems, 2015.

[3] M. Idhammad, K. Afdel, and M. Belouch, “DoS detection method based on artificial neural networks,” International Journal of Advanced Computer Science and Applications, vol. 8, no. 4, 2017.

[4] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani. A detailed analysis of the KDD CUP 99 data set. In Proc. IEEE International Conference on Computational Intelligence for Security and Defense Applications, pages 53–58, 2009.