

TP de sécurité des systèmes embarqués

Hugues de Valon

Paul Luperini

Lucas Mahieu

23 janvier 2017

Table des matières

1	Introduction	3
2	TP 1	3
2.1	Quelle protections sont mises en place contre les attaques par fautes?	3
2.2	Quelles sont les faiblesses de cette sécurité?	3
2.3	Implémentation de l'attaque par faute	3
2.4	Embarcation du code	3
3	TP 2	3
4	Conclusion	3

1 Introduction

De nos jours, les réseaux de neurones artificiels reprennent de plus en plus d'importance car la puissance de calculs disponible permet d'obtenir des résultats satisfaisant en temps raisonnable. Le traitement d'images, la reconnaissance vocale ou le traitements lexicaux sont des applications qui pourraient être intégrées dans des systèmes embarqués. Pour ce type d'application, il est possible d'implémenter sur des CPU ou GPU des algorithmes neuronales, mais la consommation et la vitesse de traitement deviendraient vite limitant.

Créer un composant électronique (ASIC ou une IP FPGA dans un premier temps) implémentant un réseau de neurones réduirait drastiquement sa consommation et améliorerait la vitesse du réseau par rapport à un CPU. De plus, étant donnée que l'IP serait spécialisé à cette application permettrait de rendre paramétrable dynamiquement le composant lui permettrait de s'adapter à de multiples applications.

Le projet "Réseau de neurones sur FPGA" s'inscrit dans ce cadre. Sous le tutorat de Frédéric Pétrot et Adrien Prost-Boucle, nous devons créer un tel composant, et tester ses performances en vue de le comparer à des systèmes existants tels que la puce Spinnaker ou TrueNorth d'IBM ou encore de systèmes en développement tel que les réseaux de neurones ternaires du laboratoire TIMA. Une fois implémenté et validé, nous utiliserons une carte FPGA Zedboard pour tester notre composant sur une application classique de reconnaissance de chiffres manuscrits, en utilisant la base de données MNIST.

2 TP 1

2.1 Quelle protections sont mises en place contre les attaques par fautes ?

2.2 Quelles sont les faiblesses de cette sécurité ?

2.3 Implémentation de l'attaque par faute

2.4 Embarcation du code

3 TP 2

4 Conclusion

Merci à nos chers professeurs de nous avoir fait découvrir cette délicieuse matière. Merci beaucoup, du fond du coeur.

Guillaume Anoufa