UNIVERSITÉ DE RENNES 1

Direction de la Recherche et de l'Innovation

Appel à projets - Année 2022

Contrats doctoraux «Ordinaires»

ECOLE DOCTORALE : MathSTICC **POLE DE RECHERCHE : Mathématiques – Numérique**

Unité de recherche d'accueil

Unité de Recherche : IRISA

Equipe : Taran

Encadrement

Directeur de thèse : D.Chillet **Unité de recherche** : IRISA

Employeur/Établissement d'origine : Université de Rennes 1 / ENSSAT

HDR : ♦ oui □ non **Nb de thèses en cours** : 2

Mail : daniel.chillet@univ-rennes1.fr **Tél**. : 02 96 46 90 69

Co-directeur de thèse : E.Casseau **Unité de recherche** : IRISA

Employeur/Établissement d'origine : Université de Rennes 1 / ENSSAT

HDR : ♦ oui □ non **Nb de thèses en cours** : 3

Mail : emmanuel.casseau@univ-rennes1.fr **Tél.** : 02 96 46 91 76

Co-encadrant de thèse : C.Killian **Unité de recherche** : IRISA

Employeur/Établissement d'origine : Université de Rennes 1 / IUT Lannion

HDR : □ oui ♦ non **Nb de thèses en cours** : 2

Mail : cedric.killian@univ-rennes1.fr **Tél.** : 02 96 46 94 85

Sujet : PAMIA

Titre : Protection d'Architectures Multi-coeurs hétérogènes par Intelligence Artificielle embarquée sur la puce

Mots clés : Protection d'Architectures Multi-coeurs hétérogènes par Intelligence Artificielle embarquée sur la puce

Cotutelle internationale (~~oui~~/non) : **Si oui, préciser l'établissement et le pays de rattachement** :

Descriptif (15-30 lignes) :
Contexte socioéconomique et scientifique ; Les hypothèses et questions posées ; Les grandes étapes de la thèse et démarche ; Approches méthodologiques et techniques envisagées

Pour répondre aux exigences de nombreux domaines applicatifs (véhicules autonomes/intelligents, santé, domotique, industrie, télécommunication, etc.), les systèmes numériques qui embarquent l'exécution des applications doivent proposer de plus en plus de capacité de calcul. Depuis une vingtaine d'années, l'augmentation de cette capacité de calcul est principalement soutenue par l'accroissement du nombre ressources d'exécution au sein de ces systèmes. La conséquence directe de cette évolution a été le développement de systèmes sur puce complexes (SoC pour System on Chip) reposant sur des architectures multi-cœurs organisées sur la puce autour d'un médium d'interconnexion, classiquement un réseau sur puce (NoC pour Network on Chip). Par ailleurs, la grande majorité de ces domaines applicatifs nécessite une connectivité aux infrastructures afin de répondre à des besoins de mobilité et d'ubiquité. Cette fonctionnalité de connexion à des réseaux externes constitue un point de vulnérabilité important pour les systèmes, les exposant alors à des événements externes pouvant provoquer des fautes et/ou erreurs. Des travaux importants ont été menés au niveau logiciel pour accroître la robustesse de ces systèmes, toutefois, pour être tout à fait fiable, le niveau matériel doit également être abordé, et la plateforme d'exécution doit donc être adaptée afin de compléter l'arsenal de protections de ces systèmes critiques.

Concernant ces plateformes matérielles d'exécution, le médium de communication est un élément central puisqu'il supporte les échanges entre les tâches des applications. Dans ce contexte, un évènement malveillant induisant l'augmentation du trafic sur le NoC peut rapidement conduire à un déni de service par saturation de tout ou partie du réseau (DoS – Denial of Service). L'apparition de ce scénario est fortement liée à la connectivité du système, ce dernier pouvant par exemple subir une perturbation au travers de

l'arrivée/l'exécution d'une tâche corrompue dont l'exécution générerait un trafic sur le NoC conduisant soit à un dépassement des échéances de tâches critiques soit à un blocage complet du trafic de données sur le réseau. Dans ce dernier cas, le système est en situation de déni de service puisque certaines fonctionnalités du système seraient rendues inopérantes.

Ce scénario constitue un cas de disfonctionnement important qu'il faut pouvoir contrer. Un certain nombre de travaux ont abordé la problématique du déni de service au sein d'architectures MPSoC s'appuyant sur un NoC [1]. Lorsqu'il est volontairement déclenché, ce disfonctionnement peut consister à surcharger le réseau pour analyser les évolutions du trafic des tâches pour en déduire une information cachée, ou pour bloquer totalement le service [2,3,4]. La détection de ce disfonctionnement peut par exemple reposer sur une analyse de la violation des temps de communication [3] ou sur l'analyse de l'évolution des temps de communication d'une tâche afin d'en déduire le trafic généré par une autre tâche sur le même chemin [4]. Des solutions de monitoring à base d'intelligence artificielle ont été récemment proposées [5]. En cas de détection d'un disfonctionnement, les méthodes de protection qui sont généralement développées reposent sur des techniques d'isolation de la tâche générant le trafic réseaux ou sur de l'adaptation du routage au sein du réseau [1,2,4]. Cependant, ces solutions ont généralement un coût énergétique élevé et des solutions moins énergivores doivent être proposées pour être déployées dans un plus grand nombre de domaines applicatifs.

Les travaux que nous proposons dans cette thèse ont pour objectif d'anticiper l'apparition de déni de service au sein du NoC d'un système sur puce afin d'enclencher des contre-mesures permettant de maintenir le système dans un état de fonctionnement acceptable, le tout en veillant à développer des solutions efficientes en énergie.

- [1] R. F. Faccenda, L. L. Caimi and F. G. Moraes, "Detection and Countermeasures of Security Attacks and Faults on NoC-Based Many-Cores," in IEEE Access, vol. 9, pp. 153142-153152, 2021, doi: 10.1109/ACCESS.2021.3127468
- [2] T. Boraten and A. K. Kodi, "Mitigation of Denial of Service Attack with Hardware Trojans in NoC Architectures," 2016 IEEE International Parallel and Distributed Processing Symposium (IPDPS), 2016, pp. 1091-1100, doi: 10.1109/IPDPS.2016.59
- [3] S. Charles, Y. Lyu and P. Mishra, "Real-time Detection and Localization of DoS Attacks in NoC based SoCs," 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE), 2019, pp. 1160-1165, doi: 10.23919/DATE.2019.8715009.
- [4] M. J. Sepúlveda, J. Diguet, M. Strum and G. Gogniat, "NoC-Based Protection for SoC Time-Driven Attacks," in IEEE Embedded Systems Letters, vol. 7, no. 1, pp. 7-10, March 2015, doi: 10.1109/LES.2014.2384744.
- [5] J. Yao, Y. Zhang, Z. Mao, S. Li, M. Ge and X. Chen, "On-line Detection and Localization of DoS Attacks in NoC," 2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), 2020, pp. 173-178, doi: 10.1109/ITAIC49862.2020.9338861.