Offre n°2022-04643

Doctorant F/H Protection d'Architectures Multi-coeurs hétérogènes basée sur une Intelligence Artificielle embarquée sur puce

Type de contrat : CDD

Niveau de diplôme exigé : Bac + 5 ou équivalent

Autre diplôme apprécié : Master recherche

Fonction : Doctorant

A propos du centre ou de la direction fonctionnelle

Le centre Inria Rennes - Bretagne Atlantique est un des huit centres d'Inria et compte plus d'une trentaine d'équipes de recherche. Le centre Inria est un acteur majeur et reconnu dans le domaine des sciences numériques. Il est au cœur d'un riche écosystème de R&D et d'innovation : PME fortement innovantes, grands groupes industriels, pôles de compétitivité, acteurs de la recherche et de l'enseignement supérieur, laboratoires d'excellence, institut de recherche technologique

Contexte et atouts du poste

Pour répondre aux exigences de nombreux domaines applicatifs (véhicules autonomes/intelligents, sante, 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 medium 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 a des besoins de mobilité et d'ubiquité. Cette fonctionnalité de connexion a des réseaux externes constitue un point de vulnérabilité important pour les systèmes, les exposant alors a des évènements pouvant provoquer des fautes et/ou erreurs. Des travaux importants ont été menés au niveau logiciel pour accroitre la robustesse de ces systèmes, toutefois, pour être tout a fait fiable, le niveau matériel doit également être aborde, 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 medium 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 a un déni de service par saturation de tout ou partie du réseau (DoS – Denial of Service). L'apparition de ce scénario est fortement liée a 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 génèrerait un trafic sur le NoC conduisant soit a un dépassement des échéances de tâches critiques soit a 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 a 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 a 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 génère par une autre tâche sur le même chemin [4]. Des solutions de monitoring a 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.

1. 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. 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. 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. J. Sepu□lveda, 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. 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.

Mission confiée

La première mission qui devra être prise en charge par la personne recrutée sera de réaliser un état de l'art des méthodes développées pour protéger les réseaux sur puce, en particulier pour protéger l'apparition de déni de service lié à une forte augmentation du trafic en un point donné du réseau.

Sur la base de cet état de l'art, la seconde mission consistera à proposer une contribution permettant de surveiller le trafic réseau et de l'analyser pour détecter des dérives anormales. Les méthodes développées pourront s'appuyer sur la connaissance d'un trafic nominal de chaque tâche (connaissance acquise par apprentissage depuis une exécution sans défaut), sur une analyse temporelle du trafic et sur une comparaision des trafics prédit et observé.

Des expérimentations seront menées pour démontrer la pertinence des contributions. Ces expérimentations seront principalement menéés par simulation sur la base d'un simulateur de réseaux sur puce qui reste à sélectionner.

Principales activités

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.

Le principe reposera sur l'observation du trafic sur le réseau à la manière d'une série temporelle et en se basant sur un ensemble de moniteurs matériels, afin de détecter l'apparition d'augmentations intempestives ou inappropriées du trafic, signe d'une possible dérive de fonctionnement d'une ou plusieurs tâches du système. En effet, le trafic réseau généré par une tâche n'est pas aléatoire et une analyse temporelle permettra de capturer le profil de ce trafic (par exemple au travers d'algorithmes de type LSTM - Long Short-Term Memory). Sur la base de la caractérisation de ce profil, un contrôleur basé sur un algorithme d'intelligence artificielle pourra agir sur plusieurs leviers pour maintenir un fonctionnement sûr du système.

- Le premier levier consistera à réguler dynamiquement l'attribution des bandes passantes pour chaque tâche du système. L'attribution des bandes passantes reposera sur un mécanisme de type bonus/malus qui récompensera les tâches utilisant le média de communication de façon « raisonnable/appropriée » et pénalisera les tâches au comportement suspicieux. La dynamicité du contrôle permettra de tenir compte du comportement irrégulier d'une tâche générant un trafic sporadique important puis revenant à un fonctionnement normal. Dans ce cas de figure, le mécanisme de bonus/malus permettra de maintenir la tâche en activité tout en contrôlant son impact sur l'exécution des autres tâches.
- Le second levier consistera à allouer des canaux de communication spécifiques pour toute nouvelle tâche arrivant dans le système (ou toute nouvelle application). Les canaux attribués seront observés pour « apprendre » le comportement des échanges générés. Une fois la caractérisation de la tâche effectuée par l'algorithme d'IA, les communications de la tâche seront alors basculées sur les autres canaux du NoC. Cette caractérisation de la tâche servira à vérifier que son comportement reste dans une enveloppe de fonctionnement acceptable par rapport au profil nominal.
- Le dernier levier envisagé concernera la gestion de la ré-allocation des tâches au sein du système en cas de perturbations constatées dans les échanges d'un sous ensemble du système. En effet, par une ré-allocation intelligente de tout ou partie d'une application, et donc implicitement du trafic entre ses tâches, il est possible de rendre l'attaque inoffensive pour le système tout en accordant du temps pour contrer l'attaque.

Le niveau de granularité des différentes actions proposées a pour objectif de réduire la complexité des mécanismes de détection et ainsi limiter le surcoût énergétique de la contre mesure.

Compétences

Compétences techniques et niveau requis :

Les candidats doivent disposer de compétences dans le domaine des architectures matérielles de calcul et en particulier concernant les réseaux sur puce. Des connaissances en intelligence artificielle ainsi qu'en tolérance aux fautes seront un atout important pour appréhender rapidement le sujet et proposer

des contributions scientifiques pertinentes.

Langues :

La langue de travail pourra être le fraçais ou l'anglais.

Les candidats doivent disposer d'un bon niveau d'anglais, notamment à l'écrit afin que la valorisation des travaux puisse être assurée aussi bien au niveau national qu'international.

Compétences relationnelles :

Le travail se déroulera au sein d'une équipe de 4 personnes.

Des réunions régulières seront mises en place, et la personne devra être en mesure de présenter l'avancée de ses travaux de façon claire et détaillée.

Avantages

- Prise en charge à 50 % des frais de transport en commun sur le trajet domicile-travail ou FMD.
- Restauration subventionnée
- Prise en charge partielle des frais de mutuelle
- Possibilité de télétravail (à hauteur de 90 jours annuels) et d'aménagement du temps de travail

Rémunération

Rémunération mensuelle brute de 1982 euros les deux premières années et 2085 euros la troisième année

Informations générales

- **Thème/Domaine :** Systèmes embarqués et temps réel
- **Ville :** Lannion
- **Centre Inria :** Centre Inria de l'Université de Rennes
- **Date de prise de fonction souhaitée :** 2022-10-01
- **Durée de contrat :** 3 ans
- **Date limite pour postuler :** 2022-06-25

Contacts

- **Équipe Inria :** TARAN
- **Directeur de thèse :**
  Chillet Daniel / Daniel.Chillet@irisa.fr

A propos d'Inria

Inria est l'institut national de recherche dédié aux sciences et technologies du numérique. Il emploie 2600 personnes. Ses 215 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3900 scientifiques pour relever les défis du numérique, souvent à l'interface d'autres disciplines. L'institut fait appel à de nombreux talents dans plus d'une quarantaine de métiers différents. 900 personnels d'appui à la recherche et à l'innovation contribuent à faire émerger et grandir des projets scientifiques ou entrepreneuriaux qui impactent le monde. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 200 start-up. L'institut s'efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l'économie.

L'essentiel pour réussir

Les candidats doivent pouvoir faire preuve d'automonie, de curiosité dans la conduite de leur travaux. Ils devront également disposer d'un sens critique pour parvenir à positionner leurx ttavaux au regard de l'état de l'art.

Attention: Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.

Consignes pour postuler

Merci de déposer en ligne CV, lettre de motivation et éventuelles recommandations

Pour plus d'information, contactez daniel.chillet@irisa.fr ou cedric.killian@irisa.fr

Sécurité défense :
Ce poste est susceptible d'être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L'autorisation d'accès à une zone est délivrée par le chef d'établissement, après avis ministériel favorable, tel que défini dans l'arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l'annulation du recrutement.

Politique de recrutement :
Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.