Offre n°2024-07773

Doctorant F/H Detection d'attaques et d'anomalies dans l'Internet des Objets

Type de contrat : CDD

Niveau de diplôme exigé : Bac + 5 ou équivalent

Fonction : Doctorant

A propos du centre ou de la direction fonctionnelle

Le centre Inria Université de Lille, créé en 2008, emploie 360 personnes dont 305 scientifiques répartis dans 15 équipes de recherche. Reconnu pour sa forte implication dans le développement socio-économique de la région Hauts-De-France, le centre Inria de l'Université de Lille poursuit une relation étroite avec les grandes entreprises et les PME. En favorisant les synergies entre chercheurs et industriels, Inria participe au transfert de compétences et d'expertises dans le domaine des technologies numériques et donne accès au meilleur de la recherche européenne et internationale au profit de l'innovation et des entreprises, notamment dans la région.Depuis plus de 10 ans, le centre Inria de l'Université de Lille est situé au cœur de l'écosystème universitaire et scientifique de Lille, ainsi qu'au cœur de la Frenchtech, avec un showroom technologique basé avenue de Bretagne à Lille, sur le site d'excellence économique d'EuraTechnologies dédié aux technologies de l'information et de la communication (TIC).

Contexte et atouts du poste

The PhD student will be co-supervised by Valeria Loscri (FUN Team) and Kevin Jiokeng (École Polytechnique).

The Inria FUN research group investigates solutions to enhance programmability, adaptability and reachability of FUN (Future Ubiquitous Networks) composed of RFID, wireless sensor and robot networks. Limited resources, and high mobility evolving in distrusted environments characterize the objects that compose FUN. They communicate in a wireless way. To be operational and efficient, such networks have to follow some self-organizing rules. Indeed, components of FUN have to be able in a distributed and energy-efficient way to discover the network, self-deploy, communicate, self- structure in spite of their hardware constraints while adapting the environment in which adapting the environment in which they evolve. For additional information on the FUN research group, please see http://team.inria.fr/fun/

Mission confiée

The ubiquitous deployment of Internet of Things (IoT) devices, make this technology a key actor of our daily activities, by enabling advanced services and applications that could not be imagined few years ago. This PhD wiil be in the context of a National project, NEMIoT (NEtwork Methods for IoT). This project aims at developing new methods to increase trust in IoT devices before and after their deployment on existing network infrastructures. Although many efforts have been made in securing IoT devices with regards to hardware, software, trustworthiness, data leaking, interoperability, or privacy, relatively little has been made on the issue of the availability of existing and expected services following the introduction of a (fleet of) new IoT device(s) (e.g., massive access problem) [1, 2]. After deployment, IoT devices may remain vulnerable and prone to abnormal behavior that needs to be quickly identified and mitigated. The characterization of the IoT devices and their traffic, to identify if it is normal/anomalous or under attack, will revolve on Machine Learning approaches [3].

The primary objective is developing original cross-layer solutions to finely and quickly detect and/or mitigate potential anomalies resulting from the introduction of IoT devices.

Expected outcomes

The specific outcomes will be new methods and tools resorting to a cross-layer approach, to finely characterize the activity of IoT nodes, to detect eventual anomaly behaviors, and ultimately to identify the root cause of these anomalies.

Main Activities

- Study of the State of Art of anomaly/attack detection in IoT systems
- Characterization of IoT devices behavior through Machine Learning approaches
- Design of new cross-layer detection approaches in IoT architectures
- Validation of the solutions via simulation and experiments

Additional activities :

- Writing reports
- Participation to the deliverables writing

References:

[1] Emilie Bout, Valentin Bout, Alessandro Brighente, Mauro Conti, Valeria Loscri. Evaluation of Channel Hopping Strategies Against Smart Jamming Attacks. IEEE ICC 2023 - IEEE International Conference on Communications, IEEE, May 2023, Rome, Italy.

[2] E. Bout, V. Loscri and A. Gallais, "HARPAGON: An Energy Management Framework for Attacks in IoT Networks," in IEEE Internet of Things Journal, vol. 9, no. 20, pp. 19959-19970, 15 Oct.15, 2022, doi: 10.1109/JIOT.2022.3172849.

[3] E. Bout, V. Loscri and A. Gallais, "How Machine Learning Changes the Nature of Cyberattacks on IoT Networks: A Survey," in IEEE Communications Surveys & Tutorials, vol. 24, no. 1, pp. 248-279, Firstquarter 2022, doi: 10.1109/COMST.2021.3127267.

Compétences

Compétences techniques et niveau requis :

Langues :

Compétences relationnelles :

Compétences additionnelles appréciées :

Avantages

- Restauration subventionnée
- Transports publics remboursés partiellement
- Congés: 7 semaines de congés annuels + 10 jours de RTT (base temps plein) + possibilité d'autorisations d'absence exceptionnelle (ex : enfants malades, déménagement)
- Possibilité de télétravail et aménagement du temps de travail
- Équipements professionnels à disposition (visioconférence, prêts de matériels informatiques, etc.)
- Prestations sociales, culturelles et sportives (Association de gestion des œuvres sociales d'Inria)
- Accès à la formation professionnelle
- Sécurité sociale

Rémunération

Les deux premières années : 2100€ brut par mois.

La 3ème année : 2190€ brut par mois

Informations générales

- **Thème/Domaine :** Réseaux et télécommunications
  Système & réseaux (BAP E)
- **Ville :** Villeneuve d'Ascq
- **Centre Inria :** Centre Inria de l'Université de Lille
- **Date de prise de fonction souhaitée :**2024-10-01
- **Durée de contrat :**3 ans

- **Date limite pour postuler :** 2024-07-14

Contacts

- **Équipe Inria :** FUN
- **Directeur de thèse :**
  Loscri Valeria / Valeria.Loscri@inria.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.

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

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.