Programme de cotutelles U. Libanaise - UT INSA

Description du sujet (merci de vous conformer aux recommandations indiquées sur le site web)

Nom :	Lounis	Prénom :	Ahmed
Fonction (prof., MdC) :	Enseignant Chercheur		
Laboratoire :	Heudiasyc	Adresse web :	https://www.hds.utc.fr/
Etabliss[t] :	UTC	Adresse web :	https://www.utc.fr/

Compétence scientifique:

Sécurité et sûreté de fonctionnement des architectures réseau : cela inclut la protection des réseaux IoT (réseaux de capteurs, Cloud, edge/fog computing), mobiles contre les menaces et la garantie de leur fonctionnement fiable et continu.
Communication et optimisation des réseaux : cela concerne l'amélioration de l'efficacité et des performances des réseaux (enérgie, qualité de service, gestion des collisions, ...).

2 publications importantes en relation avec le sujet proposé :

- Beyrouti, M., Lounis, A., Lussier, B., Bouabdallah, A., & Samhat, A. E., Vulnerability-oriented risk identification framework for IoT risk assessment, Internet of Things, 27, 2024.

- Beyrouti, M., Lounis, A., Lussier, B., Bouabdallah, A., & Samhat, A. E., Security-Bag: A Specification-based Intrusion Detection System Applied to Star Topology BLE Networks, In IEEE IOTSMS, 2024.

Adresse web de votre page personnelle : https://www.hds.utc.fr/~lounisah/dokuwiki/doku.php

Adresse mail : ahmed.lounis@hds.utc.fr

Description du sujet de thèse proposé ***n° du thème :*** 2

Titre : Cybersécurité et sécurité-innocuité des systèmes IoT pour les transports intelligents

Sujet :

L'Internet des objets (IoT) joue un rôle clé dans les systèmes de transport intelligents et les infrastructures sensibles, permettant la collecte et l'analyse de données via des objets connectés (capteurs, boutons d'urgence, etc.). Ces technologies offrent des applications variées, telles que la détection d'incidents, l'optimisation des itinéraires et la gestion des urgences. Cependant, leur adoption dans des environnements critiques est freinée par des défis liés à la cybersécurité (security) des données et des services, ainsi qu'à la sécurité-innocuité (safety). Ce projet de thèse vise à développer un composant Security-Safety Bag, intégrant ces deux aspects pour les systèmes IoT. Ce composant assurera la détection rapide des menaces et des erreurs, tout en garantissant la continuité des services critiques. Il traitera les risques liés aux attaques, aux erreurs de composants IoT, et aux pannes dans les contrôles d'accès. Le projet étendra cette solution à une large gamme de protocoles IoT utilisés dans le système critique choisi et tiendra compte des contraintes de temps réel, notamment pour les environnements IoT décentralisés comme la 5G et l'Edge computing. L'objectif est de garantir la sécurité et la sûreté des systèmes tout en maintenant une faible latence et une haute performance, dans des applications critiques telles que les transports intelligents, notamment les systèmes ferroviaires.

mots clés :

IoT, cybersécurité, sécurité-innocuité, cyberattaques, injection de fautes

Collaborations attendues :

Collaboration intra-équipe Heudiasyc : cette thèse se déroulera dans l'axe de recherche 1 de l'équipe SCOP du laboratoire Heudiasyc (systèmes sûrs et sécuriés) à travers la collaboration d'Ahmed Lounis et Benjamin Lussier ;
Collaboration UTC / UL : cette thèse se déroulera en co-tutelle avec l'Université Libanaise à travers la collaboration d'Ebed Ellatif Samhat.

Compétences nécessaires du candidat :

cybersécurité, réseaux informatiques

Existence d'un fichier pdf détaillant le sujet (oui-non) : oui

(respecter les indications données sur le site web)