RESUME DU PROJET

Nom et prénom des porteurs du projet :

- Lounis Ahmed, UTC (co-directeur)
- Lussier Benjamin, UTC (co-encadrant)
- Samhat Abed Ellatif, Université Libanaise (co-directeur)

Intitulé du sujet de thèse : Cybersécurité et sécurité-innocuité des systèmes IoT pour les transports intelligents

Financement demandé (support entier ou demi-support) : demi-support

Résumé en français :

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.

Résumé en anglais :

Internet of Things (IoT) Systems can play a key role in intelligent transport systems and sensitive infrastructure, enabling the collection and analysis of data via connected objects (sensors, emergency buttons, etc.). These technologies offer a variety of applications, such as incident detection, route optimization and emergency management. However, their adoption in critical environments is hampered by challenges related to the cybersecurity and safety of data and services. This thesis aims to develop a Security-Safety Bag component, integrating these two aspects for IoT systems. This component will ensure the rapid detection of threats and errors, while ensuring the continuity of critical services. It will address the risks related to both attacks and failures on IoT components. This thesis will extend a previously developed Security Bag to a wide range of IoT protocols used in IoT systems and take into account real-time constraints, especially for decentralized IoT environments like 5G and edge computing. It will also incorporate safety rules into this component. The aim is to ensure the safety and security of critical IoT applications such as intelligent transport, while maintaining low latency and high performance.

DESCRIPTIF DU PROJET

1) *Motivation et contexte du sujet de recherche*

Cette thèse sera menée au sein de l'équipe de recherche SCOP (Sûreté, Communication, Optimisation) du Laboratoire Heudiasyc de l'UTC et du CNRS, en co-tutelle avec l'Université Libanaise (UL). Le sujet porte sur une problématique qui concerne l'axe 1 de l'équipe SCOP : système sûrs et sécurisés. Les encadrants, Dr Ahmed Lounis et Dr Benjamin Lussier, sont membres de l'équipe SCOP et travaillent actuellement sur des solutions innovantes en s'appuyant sur des approches globales de cybersécurité et sécurité-innocuité pour concevoir des systèmes résilients à la fois à des cyberattaques et à des fautes de développement matérielles et logicielles. Ces approches, reposant sur des composants indépendants de sécurité, s'appliquent à des systèmes IoT réels, tels que les systèmes intelligents et autonomes, les systèmes de gestion des crises et des urgences, et cela dans des domaines variés, notamment la santé, le ferroviaire, et la défense. Une attention particulière est portée au transport intelligent, en raison des compétences reconnues de notre laboratoire dans ce secteur. Il convient de souligner qu'une thèse, dont la soutenance est prévue prochainement, a déjà apporté des résultats significatifs sur des problématiques connexes, avec plusieurs publications de rang A. Cette nouvelle thèse représente une opportunité de renforcer ces travaux et de consolider nos activités et expertises sur ce domaine, ainsi que notre collaboration avec le professeur Abed Ellatif Samhat de l'Université Libanaise. Nous souhaitons également valoriser les solutions innovantes proposées par le biais d'un transfert technologique vers l'industrie.

2) *Description du sujet (2 pages minimum) : questions, état de l'art, pistes de résolution et méthodologie envisagée, objectifs visés et résultats escomptés, évaluation*

2.1. Contexte

L'Internet des objets (IoT) connaît un succès grandissant grâce à son intégration dans divers domaines, qu'il s'agisse de la vie quotidienne ou de l'industrie. Les objets connectés jouent un rôle clé en facilitant la collecte de données utilisées pour surveiller, détecter des situations d'urgence et piloter des actions, notamment dans les systèmes de transport intelligents. Dans ce contexte [4], l'IoT offre une multitude d'applications, telles que l'optimisation des itinéraires, le stationnement intelligent, la prévention et la détection des accidents, la surveillance des infrastructures, ainsi que le développement de véhicules autonomes et connectés (trains, voitures). Ces applications contribuent à améliorer le flux de circulation, à réduire les congestions, à accroître l'efficacité globale et à optimiser l'empreinte énergétique des infrastructures.

Cependant, plusieurs défis freinent encore le développement de ces solutions, en particulier la sécurité des infrastructures IoT. Tout d'abord, la complexité de l'IoT, caractérisée par une multitude de protocoles de communication et de types d'objets connectés, ainsi que l'introduction des nouvelles technologies telles que la 5G/6G et du Edge computing [9] qui renforcent la décentralisation de l'architecture pour garantir des traitements en temps réel, cependant, expose ces systèmes à divers risques. Ces menaces incluent les fuites de données sensibles, l'indisponibilité des services, la perte de données, et les accès non autorisés. En outre, ces vulnérabilités peuvent avoir un impact significatif sur la sécurité-innocuité (safety) du système ou de ses utilisateurs, notamment parce que les applications concernées sont souvent critiques. Par conséquent, assurer leur cybersécurité et leur sécurité-innocuité est une condition essentielle pour garantir leur adoption à grande échelle. Cela demande ainsi d'adopter des approches intégrant ces deux aspects.

2.2. Etat de l'art

Concernant l'aspect sécurité-innocuité, Klein et al. ont proposé dans [10] l'utilisation d'un composant de sécurité indépendant appelé Safety-Bag dans le système ferré ELEKTRA (Electronic Interlocking System) qui vérifie les commandes d'aiguillage automatique selon des règles de sécurité-innocuité. Par la suite, d'autres solutions ont intégré un composant Safety-Bag dans des applications critiques [10], comme des centrales nucléaires (système SPIN) ou des véhicules autonomes [7]. Le Safety-Bag est un système de sécurité logiciel et matériel indépendant qui doit être capable de détecter et éventuellement traiter toute évolution du système vers un état à risque. Pour cela, il est chargé de vérifier en ligne un ensemble de règles de sécurité-innocuité. Si une condition de sécurité-innocuité est violée, le Safety-Bag intervient en inhibant une action potentiellement dangereuse ou en forçant une action de sécurité afin de maintenir ou ramener le système dans un état sûr, évitant ainsi des défaillances catastrophiques. Pour réduire les pannes de cause commune, il doit être spécifié et développé séparément du système fonctionnel, et disposer de moyens d'action et de détection indépendants des erreurs à tolérer. À notre connaissance, il n'existe actuellement aucune solution qui intègre le composant Safety-Bag pour traiter conjointement les problématiques de cybersécurité et de sécurité-innocuité. Jusqu'à présent, le

composant Safety-Bag a été utilisé pour aborder soit l'un soit l'autre, l'aspect cybersécurité ayant été proposé dans nos précédents travaux. De plus, les chercheurs et les experts impliqués dans ces domaines proviennent de communautés distinctes, avec des approches et des outils souvent très différents, ce qui complique le développement de solutions intégrées et cohérentes.

Concernant l'aspect cybersécurité, [1] présente les limitations des approches existantes aux systèmes IoT, que ces approches soient traditionnelles ou spécifiquement développées pour l'IoT. En particulier, ces limitations reposent sur :

- les fortes contraintes de ressources sur les composants IoT, qui empêchent le déploiement d'approches coûteuses en espace ou temps de calcul, comme la cryptographie lourde,
- les politiques de publication (*advertising*) et de couplage (*coupling*) des protocoles de communication IoT, qui sont souvent ignorées par les approches traditionnelles et souffrent de nombreuses vulnérabilités,
- la dynamique des réseaux IoT, dans lesquels des composants peuvent se connecter ou se déconnecter régulièrement dans les sous-réseaux sans-fil, alors que les approches traditionnelles se concentrent sur des systèmes plus statiques,
- la possibilité qu'un composant IoT victime d'une attaque soit utilisé par l'attaquant comme nouveau vecteur d'attaque, ce qui est souvent ignoré dans des approches traditionnelles, cherchant à sécuriser tous les composants du réseau,
- le manque de considération des aspects sécurité-innocuité, cruciaux pour des applications critiques.

Dans [1, 3], nous avons proposé une approche d'identification et d'estimation des risques de cybersécurité dans l'IoT. Cette approche est centrée sur l'identification des vulnérabilités et consiste à concevoir des scénarios d'attaques réalistes ciblant les systèmes IoT. La motivation de cette proposition réside dans l'absence d'une approche prenant en compte les spécificités de l'IoT dans l'état de l'art, où la majorité des solutions se concentrent sur des systèmes informatiques classiques, ou ne traitent qu'incomplètement les limitations posées par ces systèmes. Dans l'article [2], nous avons présenté le premier *Security-Bag*, un composant indépendant conçu pour jouer un rôle clé dans la détection des attaques de sécurité. Ce composant utilise des règles de cybersécurité développées à partir des scénarios d'attaques identifiés dans notre analyse de risque. Il permet de mettre en œuvre un ensemble de mécanismes visant à identifier des attaques, tout en exécutant des actions correctives une fois un problème détecté pour garantir la cybersécurité des systèmes IoT. En tant que couche de protection supplémentaire, il assure une détection rapide des menaces potentielles et facilite une réponse appropriée pour sécuriser les dispositifs ainsi que les données sensibles.

2.3. Pistes de résolution et méthodologie proposée

Le composant indépendant *Security Bag* n'a encore été validée que sur quelques protocoles (BLE (Bluetooth Low Energy), MQTT, …). Il est essentiel de la généraliser à d'autres piles protocolaires des architectures IoT afin de couvrir une plus large surface d'attaques exploitables par des attaquants. En outre, la coopération possible entre la cybersécurité et la sécurité-innocuité n'a pas encore été exploité. Pour cela, il rst nécessaire de développer un Security-Safety Bag, intégrant à la fois les erreurs liées à la sécurité et celles affectant la sûreté de fonctionnement. Plusieurs défis sont ainsi soulevés :

- *Généralisation des protocoles et amélioration des aspects cybersécurité* : étendre le support du composant à des protocoles IoT variés pour accroître la couverture des menaces (Zigbee, Wifi, 4/5G…). Il est également essentiel de prendre en compte le fait que certaines vulnérabilités, telles que les attaques de type zero-day, peuvent survenir. Cela impose d'adapter l'approche d'analyse des risques pour les inclure correctement. Il conviendrait également de proposer des règles au sein du Security Bag pour détecter les conséquences des attaques, et ainsi prendre en charge la reprise des services de manière efficace. Enfin, il est crucial de développer des mécanismes d'alerte intelligente, capables de réagir rapidement et de minimiser l'impact sur les systèmes critiques.

- Couplage sécurité/sûreté : développer une approche globale complémentaire intégrant à la fois les aspects cybersécurité (protection contre les attaques) et sécurité-innocuité (non-occurrence de défaillances catastrophiques). Il sera crucial de valider que les deux types de règles peuvent coexistent sans impacts négatifs.

Interopérabilité, performance et temps réel : l'intégration de solutions de sécurité dans des architectures IoT hétérogènes, telles que celles reposant sur la 5G et l'Edge / Fog computing, représente un défi majeur en raison de la décentralisation des processus de traitement des données sur des nœuds éloignés. Cette distribution complique l'implémentation de mécanismes de sécurité uniformes et cohérents à travers l'ensemble du réseau. Pour garantir la sécurité et la sûreté des systèmes IoT tout en répondant aux exigences de performance, il est crucial d'intégrer efficacement les principes de cybersécurité et de sécurité-innocuité au niveau de l'Edge

computing. Notre solution a pour cela des avantages, avec l'existence de composants locaux et globaux dans le système IoT, communiquant entre eux : les composants locaux peuvent être situés au plus près des objets IoT, tandis que les composants globaux peuvent se trouver proches des nœuds effectuant les traitements. De plus, dans un environnement IoT dynamique et évolutif, où la détection des menaces et des erreurs doit être rapide, il est nécessaire de maintenir une performance optimale sans compromettre la latence et la réactivité du système. La détection des erreurs et des fautes, tout en minimisant les faux positifs et faux négatifs, devient d'autant plus importante pour ne pas compromettre la sûreté des systèmes critiques. L'utilisation de l'intelligence artificielle pour identifier ces anomalies peut étendre la couverture de détection, mais la fiabilité des résultats doit être garantie, afin de concilier la cybersécurité, la sécurité-innocuité et la performance dans des environnements de traitement en temps réel.

2.4. Objectifs visés

Nous visons dans ce projet les objectifs suivants :

1. Proposer un Security-Safety Bag qui intègre conjointement des règles de cybersécurité et de sécurité-innocuité, en gérant efficacement leurs interactions, au sein d'une architecture IoT ayant des ressources réduites.

2. Proposer des exemples de règles pour un composant Security-Safety-Bag, adaptées aux cas d'utilisation des systèmes de transport intelligents. Ces règles de sécurité seront définies à partir d'études de sécurité du système, en tenant compte de la complexité de l'architecture (5G, edge computing), ainsi que des exigences en termes de temps réel et de performance.

3. Valider le composant et les règles développés en simulation face à des injections de fautes et des attaques en étudiant la réponse du système avec et sans Security-Safety-Bag.

4. Expérimenter les solutions proposées en les intégrant dans des environnements existants (ou les créer) et les évaluer face à des situations réelles.

2.5. Evaluation

L'évaluation des travaux sera réalisé d'après le calendrier suivant :

- Première année : étude bibliographique et proposition des cas d'utilisation liés aux transports intelligents.

  Livrable : Bibliographie et spécification des cas d'utilisation (objectif 2).

- Deuxième année : réalisation d'analyses de sécurité sur le cas d'utilisation, proposition des règles du composant Security-Safety-Bag (objectif 2) et développement d'un composant PoC implémentant ces règles (objectif 1)

  Livrable : PoC du composant Security-Safety-Bag

- Troisième année : validation expérimentale du PoC développé face à des injections de fautes et des attaques, en simulation (objectif 3) et en opération réelle (objectif 4), et rédaction du manuscrit de thèse

  Livrable : campagne de validation du composant Security-Safety-Bag face à des attaques réalistes et des injections de fautes, publication internationale et manuscrit de thèse

3) Bibliographie

[1] Beyrouti, M., Lounis, A., Lussier, B., Bouabdallah, A., & Samhat, A. E. (2024). Vulnerability-oriented risk identification framework for IoT risk assessment. Internet of Things, 27, 101333.

[2] Beyrouti, M., Lounis, A., Lussier, B., Bouabdallah, A., & Samhat, A. E. (2024). Security-Bag: A Specification-based Intrusion Detection System Applied to Star Topology BLE Networks. In 2024 11th

International Conference on Internet of Things: Systems, Management and Security (IOTSMS) (pp. 169-176). IEEE.

[3] Beyrouti, M., Lounis, A., Lussier, B., Bouadallah, A., & Samhat, A. E. (2023). Vulnerability and Threat Assessment Framework for Internet of Things Systems. In 2023 6th Conference on Cloud and Internet of Things (CIoT) (pp. 62-69). IEEE.

[4] Oladimeji, D., Gupta, K., Kose, N. A., Gundogan, K., Ge, L., & Liang, F. (2023). Smart transportation: an overview of technologies and applications. Sensors, 23(8), 3880.

[5] He, Y., Kong, M., Du, C., Yao, D., & Yu, M. (2022). Communication security analysis of intelligent transportation system using 5G Internet of Things from the perspective of big data. *IEEE Transactions on Intelligent Transportation Systems*, *24*(2), 2199-2207.

[6] Wang, W., Harrou, F., Bouyeddou, B., Senouci, S. M., & Sun, Y. (2022). Cyber-attacks detection in industrial systems using artificial intelligence-driven methods. *International journal of critical infrastructure protection*, *38*, 100542.

[7] Paul, C., Benjamin, L., Walter, S., & Brini, M. (2018). Validation of safety necessities for a Safety-Bag component in experimental autonomous vehicles. In *2018 14th European Dependable Computing Conference (EDCC)* (pp. 33-40). IEEE.

[8] Mohy-Eddine, M., Guezzaz, A., Benkirane, S., & Azrour, M. (2023). An effective intrusion detection approach based on ensemble learning for IIoT edge computing. Journal of Computer Virology and Hacking Techniques, 19(4), 469-481.

[9] Bendaouia, S., Lounis, A.,& Bouabdallah, A. (2024). Green, scalable and efficient IoT architecture. In *2024 9th International Conference on Fog and Mobile Edge Computing* (FMEC) (pp. 237-244). IEEE.

[10] Klein, P. et al. “The safety-bag expert system in the electronic railway interlocking system elektra,” Expert Systems with Applications, vol. 3, no. 4, pp. 499–506, 1991

4) Collaborations prévues

Collaboration intra-équipe : ce projet se déroulera dans l’axe de recherche 1 de l’équipe SCOP du laboratoire Heudiasyc (système sûrs et sécurisés) à travers la collaboration d’Ahmed Lounis et Benjamin Lussier.

Collaboration internationale : ce projet se déroulera en co-tutelle avec l’Université Libanaise, à travers la co-direction du professeur Abed Ellatif Samhat.

Collaborations passées : les mêmes collaborations intra-équipe SCOP et internationales UTC-UL avaient été réalisées pour la thèse de Mohammad Beyrouti. Ce projet est une occasion de continuer et approfondir ces travaux et ces collaborations.