Bilan Activité Scientifique 2022-2024

Les activités scientifiques menées au laboratoire IRIT portent sur les thématiques de la sécurité et des performances, en particulier en ce qui concerne la fiabilité, la disponibilité et la maintenabilité des systèmes. Deux projets locaux financés par le CNRS et l'ICO sur les périodes 2022-2023 et 2024-2025 ont abouti à des résultats scientifiques majeurs.

### **Projet CNRS Jeune Chercheur :** Période allant de novembre 2022 à décembre 2023.

Cette projet se concentre sur le développement d'un framework robuste pour la spécification et la vérification des systèmes IoT.

#### **Aspects clés:**

* Faire face aux défis architecturaux: Le projet s'attaque aux complexités de la spécification des systèmes IoT, notamment en définissant les parties logiciel, les éléments physiques et les exigences fonctionnelles/non fonctionnelles pertinents.
* Intégration des considérations de sécurité: Les aspects de sécurité, notamment le spoofing et tampering, sont intégrés tout au long du processus de modélisation.
* Prise en compte des facteurs environnementaux: Le modèle tient compte des facteurs environnementaux (température, humidité) et de la fiabilité des appareils, qui peuvent avoir un impact significatif sur le comportement du système.
* Utilisation d'une approche hybride: Le projet combine la simulation (à l'aide d'OMNeT++) avec la vérification formelle et les techniques d'apprentissage pour relever les défis de la modélisation des systèmes IoT complexes.
* Concentration sur la sécurité et les performances: La recherche étudie l'impact des menaces de sécurité (par exemple, STRIDE) sur les performances du système, en particulier la consommation d'énergie et l'intégrité des données.

Cette approche vise à fournir un cadre complet pour la spécification, la vérification et l'analyse des systèmes IoT, garantissant leur sécurité, leur sûreté et leur fiabilité dans un environnement dynamique et en évolution.

#### Réalisations

Les activités de recherche ont donné lieu à la production de trois publications, à savoir trois articles de revues. Les détails de ces publications sont présentés ci-dessous. :

* Abdelhakim Baouya, Brahim Hamid, Levent Gürgen, and Saddek Bensalem. Security Risk Assessment of the RabbitMQ Protocol through Concurrent Stochastic Games. In Internet of Things, Elsevier, 2024.

Résumé : *Cette étude propose une approche basée sur le modèle de jeu stochastique concurrent (CSG) pour spécifier le comportement du courtier RabbitMQ dans les systèmes IoT, en tenant compte des attaques potentielles de corruption de données (Tampering and spoofing). Ces attaques et leurs fréquences sont apprises pour une évaluation paramétrable. Le modèle CSG est implémenté dans PRISM games pour une analyse automatisée, utilisant la logique temporelle alternée probabiliste (rPATL) pour modéliser les exigences de sécurité comme des objectifs de jeu. Une étude de cas industrielle sur l'impact des attaques de corruption de données sur les données captées dans une infrastructure de barrage hydraulique valide empiriquement le travail et fournit des informations précieuses sur le déploiement de RabbitMQ en périphérie.*

* Abdelhakim Baouya, Brahim Hamid, Levent Gürgen, and Saddek Bensalem Formal Modeling and Analysis of Tampering Attacks and Energy Consumption Effects on Edge Servers using Concurrent Stochastic Games. In Soft Computing, Springer, 2024 (In press).

Résumé : *Cette approche utilise le formalisme des Jeux Stochastiques Concurrents (CSG) pour modéliser le comportement des entités de communication IoT, en tenant compte des attaques en périphérie et de leur impact sur la consommation énergétique. L'analyse automatisée, réalisée avec PRISM-games, utilise la logique temporelle alternée probabiliste avec récompense (rPATL) pour exprimer les exigences fonctionnelles et de sécurité. Une étude de cas sur une attaque de corruption de données affectant le contrôle du débit d'un barrage valide l'approche et analyse son impact énergétique. L'innovation majeure réside dans l'utilisation de modèles formels au niveau architectural pour explorer les attaques potentielles et leur consommation énergétique, en considérant les styles de communication synchrones et asynchrones. Les résultats numériques montrent que les styles asynchrones subissent une augmentation significative des tampons infectés et de la consommation d'énergie due aux attaques (de 66% à 91%) par rapport à la communication synchrone.*

* Abdelhakim Baouya, Brahim Hamid, Otmane Ait Mohamed, and Saddek Bensalem. Detection and Mitigation of Clock Deviation in the Verification & Validation of Drone-aided Lifting Operations, Elsevier Ad Hoc Networks.(In press). 2025.

Résumé : *Cette étude modélise les effets des dérives d'horloge dans les systèmes cyber-physiques, en considérant les conditions physiques et environnementales, pour la vérification et la validation, notamment dans le domaine des drones (UAV). Une simulation OMNeT++ est utilisée pour définir le comportement du système, puis traduite en un modèle basé sur des arbres de décision probabilistes interprété par PRISM pour la vérification formelle. L'approche est validée par l'étude de l'influence des dérives d'horloge sur des opérations de levage par drone, en examinant diverses sources de dérives (normes, fabrication, défaillances, humidité, température). L'efficacité de la validation par simulation et model checking est étudiée, et l'approche est généralisée à l'orchestration robotique et aux infrastructures de barrage hydraulique, démontrant son applicabilité, y compris avec des facteurs de dégradation.*

### **Projet ICO :** Période allant de décembre 2023 à décembre 2025.

Ce projet vise à améliorer la prise de décision dans le développement de systèmes en abordant l'interdépendance entre le système cyber-physique, l'expertise humaine et les incertitudes liées au logiciel.

#### **Aspects clés:**

* Déterminer l'influence des facteurs humains: La projet reconnaît le rôle crucial des facteurs humains, notamment l'expertise individuelle, les connaissances dans la prise de décision.
* Utiliser des méthodes formelles: La recherche vise à utiliser des méthodes formelles pour modéliser l'humain en tant qu’opérateur, représenter la connaissance du système (logiciel et matérielle) et analyser l'impact des décisions humaines sur les performances du système (fiabilité, disponibilité et maintenabilité ).
* **Utilisation des techniques d'IA** : les approches des méthodes formelles et de la théorie des jeux intègrent des modèles pour répondre au défi de la prise de décision mutuelle entre l'humain et les mondes physique et logiciel, en tenant compte des interactions et des rétroactions entre ces différents domaines, et où l'expertise humaine joue un rôle crucial.

#### Réalisations

Les travaux de recherche ont conduit à la publication d'une communication acceptée en conférence et laissent entrevoir la publication d'articles de revues actuellement en cours de rédaction.

* Abdelhakim Baouya, Brahim Hamid, Otmane Ait Mohamed, and Saddek Bensalem. “Model-Based Reliability, Availability, and Maintainability Analysis for Satellite Systems with Collaborative Maneuvers via Stochastic Games”. In: The 50th EUROMICRO Conference on Software Engineering and Advanced Applications (SEAA). 2024. August 2024.

Résumé : *Cet article propose une nouvelle approche utilisant les jeux stochastiques concurrents (CSG) pour modéliser un satellite et ses propriétés de Fiabilité, Disponibilité et Maintenabilité (RAM) avec des spécifications formelles en rPATL. L'analyse quantitative est réalisée avec le model checker PRISM-games, en considérant les comportements collaboratifs entre les acteurs en orbite et au sol. Cette approche CSG offre un espace de conception riche où les acteurs impliqués dans la maintenance du satellite peuvent collaborer et apprendre des stratégies optimales. L'objectif est d'optimiser la durée de vie des satellites, dont la durée de vie est de 10 ans ou plus, en maximisant leur temps moyen entre les pannes (MTBF).*