Proposition de sujet de thèse

Diagnostic distribué et explicable de cyber-malveillance dans les systèmes multi-énergies via des jumeaux numériques interopérables et l'apprentissage fédéré pour la cyber-résilience

Proposition de sujet de thèse de doctorat – ED EEA

Diagnostic distribué et explicable de cyber-malveillance dans les systèmes multi-énergies via des jumeaux numériques interopérables et l'apprentissage fédéré pour la cyber-résilience

Laboratoire d'accueil

Laboratoire Ampère (UMR CNRS 5005), INSA Lyon – Université Claude Bernard Lyon 1

École Doctorale

ED EEA – Électronique, Électrotechnique, Automatique – Université de Lyon

Encadrement

Pr. Eric Zamaï, Dr. Emil Dumitrescu, Dr. Mohammed Farouk Bouaziz

Abstract

The increasing digitalization of multi-energy systems (electricity, heat, gas and hydrogen) has significantly expanded the cyber-attack surface of critical infrastructures. This PhD aims to develop a distributed cyber-malicious behavior diagnosis framework relying on interoperable Digital Twins and Federated Learning to enable collaborative intrusion detection while preserving data confidentiality. The proposed approach will combine model-based diagnosis, discrete-event systems theory and AI techniques to detect, explain and mitigate cyberattacks across interconnected energy infrastructures. The research will be validated on realistic multi-energy demonstrators within the PEPR FutuRE project and is expected to contribute to the development of trustworthy and cyber-resilient energy management systems.

Mots-clés

Cyber-résilience, Diagnostic distribué, *Federated Learning, Digital Twins*, Systèmes multi-énergies, *Discrete Event Systems,* Cybersécurité industrielle, *Explainable AI (XAI)*

Contexte scientifique

La transformation numérique des systèmes énergétiques s'accompagne d'une interconnexion croissante des infrastructures électriques, thermiques, gazières et hydrogène. Ces systèmes cyber-physiques multi-énergies reposent sur des échanges de données continus et des fonctions de supervision distribuées. Cette évolution accroît la surface d'attaque cyber et crée de nouveaux risques de propagation entre infrastructures interconnectées.

Dans le cadre du PEPR FutuRE et du projet FutuRE.Net, il devient nécessaire de développer des méthodes de détection et de diagnostic distribués capables d'opérer sur plusieurs plateformes tout en préservant la confidentialité des données et l'autonomie locale des opérateurs.

Verrous scientifiques

• Modélisation événementielle distribuée de systèmes multi-énergies évoluant à différentes échelles temporelles.
• Conception de jumeaux numériques interopérables pour la cybersurveillance.
• Combinaison de modèles physiques et de méthodes d'apprentissage fédéré.
• Détection robuste malgré la rareté des données d'attaques réelles.
• Partage sécurisé d'informations de détection entre plateformes hétérogènes.
• Développement de méthodes d'IA explicable permettant de justifier les décisions de diagnostic et d'améliorer la confiance des opérateurs.

Objectifs de la thèse

1. Concevoir une architecture de diagnostic distribué de cyber-malveillance.
2. Développer des jumeaux numériques événementiels dédiés à la supervision.
3. Concevoir des algorithmes hybrides combinant supervision discrète et apprentissage fédéré.
4. Développer des mécanismes sécurisés d'échange et d'agrégation d'indicateurs.
5. Valider les solutions sur des scénarios réalistes de cyberattaques multi-vecteurs.
6. Développer des mécanismes d'explicabilité des diagnostics afin de fournir aux opérateurs des justifications interprétables, compatibles avec les exigences de certification et de confiance des systèmes critiques.

Programme de travail

- Année 1 :
  - Analyse bibliographique approfondie.
  - Modélisation des systèmes multi-énergies.
  - Définition de l'architecture distribuée.
  - Premiers prototypes de jumeaux numériques.

- Année 2 :
  - Développement des méthodes de diagnostic basées modèles.
  - Développement des algorithmes d'apprentissage fédéré.
  - Développement de méthodes d'IA explicable (XAI) pour l'interprétation des résultats issus de l'apprentissage fédéré.
  - Fusion des approches modèle/données.
  - Premières validations sur cas d'étude.

- Année 3 :
  - Mise en œuvre des mécanismes sécurisés de partage d'informations.
  - Validation expérimentale sur plateformes du PEPR FutuRE.
  - Évaluation de l'interprétabilité, de la confiance et de l'acceptabilité des diagnostics auprès des experts métier.
  - Évaluation des performances et rédaction des publications et du manuscrit.

Résultats attendus

• Architecture distribuée de détection cyber pour FutuRE.Net.
• Jumeaux numériques interopérables.
• Algorithmes hybrides de détection d'anomalies.
• Mécanismes d'agrégation sécurisée d'indicateurs.
• Contributions logicielles open source.
• Publications internationales en automatique, cybersécurité et systèmes énergétiques.

Profil recherché

Master 2 ou diplôme d'ingénieur en automatique, informatique industrielle, cybersécurité, intelligence artificielle ou systèmes cyber-physiques. Des compétences en modélisation, systèmes à événements discrets, Python, et apprentissage automatique seront appréciées.

Bibliographie indicative

Sampath M. et al. (1995). Diagnosability of Discrete-Event Systems. IEEE Transactions on Automatic Control, 40(9), 1555–1575.

Cassandras C.G., Lafortune S. (2021). Introduction to Discrete Event Systems (3rd ed.). Springer.

Zaytoon J., Lafortune S. (2013). Overview of Fault Diagnosis Methods for Discrete Event Systems. Annual Reviews in Control, 37(2), 308–320.

Fuller A. et al. (2020). Digital Twin: Enabling Technologies, Challenges and Open Research. IEEE Access, 8, 108952–108971.

Tao F. et al. (2019). Digital Twin in Industry: State-of-the-Art. IEEE Transactions on Industrial Informatics, 15(4), 2405–2415.

Humayed A. et al. (2017). Cyber-Physical Systems Security—A Survey. IEEE Internet of Things Journal, 4(6), 1802–1831.

Ahmed C.M. et al. (2020). Challenges and Opportunities in CPS Security. IEEE Security & Privacy, 18(6), 16–26.

McMahan B. et al. (2017). Communication-Efficient Learning of Deep Networks from Decentralized Data. AISTATS.

Kairouz P. et al. (2021). Advances and Open Problems in Federated Learning. Foundations and Trends in Machine Learning, 14(1–2), 1–210.

Li T. et al. (2020). Federated Learning: Challenges, Methods, and Future Directions. IEEE Signal Processing Magazine, 37(3), 50–60.

Nguyen T.D. et al. (2022). DÏoT: Federated Self-learning Anomaly Detection System for IoT. IEEE Transactions on Dependable and Secure Computing.

Ferrag M.A. et al. (2020). Deep Learning for Cyber Security Intrusion Detection in Smart Grids. IEEE Access, 8.

Moosavi S. et al. (2024). Explainable AI in Manufacturing and Industrial Cyber–Physical Systems: A Survey. Electronics, 13(17), 3497.