

**Proposition d’un sujet de thèse en cotutelle**

**Université Libanaise**

**Nom : Prénom :**

JABER

Ali

**Titre (Prof, HDR, ….) :**

Prof

**Laboratoire : Adresse Web :**

PRASE

www.ul.edu.lb

**Etablissement : Adresse Web :**

Lebanese University

www.ul.edu.lb

 **Nom : Prénom :**

Fadlallah

Ahmad

**Titre (Prof, HDR, …) :**

Maître de conference

**Laboratoire :Adresse Web :**

PRASE

www.ul.edu.lb

**Etablissement :Adresse Web :**

Lebanese University

www.ul.edu.lb

**Domaines d’expertise :**

Computer and network security, Computer Networks, Open and Distance Learning

**Publications importantes en relation avec le sujet proposé :**

Fadlallah, Y., Sbeiti, M., Hammoud, M., Nehme, M., & Fadlallah, A. (2020, June). On the Cyber Security of Lebanon: A Large Scale Empirical Study of Critical Vulnerabilities. In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-6). IEEE.

El-Hajj, M., Fadlallah, A., Chamoun, M., & Serhrouchni, A. (2020, January). Secure PUF: Physically unclonable function based on arbiter with enhanced resistance against machine learning (ML) attacks. In *Proc. 5th Int. Conf. Sensors Electron. Instrum. Adv.(SEIA)* (pp. 216-220).

El-Hajj, M., Fadlallah, A., Chamoun, M., & Serhrouchni, A. (2019). A survey of internet of things (IoT) authentication schemes. *Sensors*, *19*(5), 1141.

**Adresse Web de votre page personnelle :**

www.researchgate.net/profile/Ali-Jaber-5

www.scholar.google.com/citations?&user=1l9dgVEAAAAJ

ali.jaber@ul.edu.lb, ahmad.fadlallah@ul.edu.lb

**Adresse mail :**

**Partenaire à l’étranger :**

**Nom : Prénom :**

ZGHAL

Mourad

**Titre (Prof, HDR, …) :**

HDR

**Laboratoire : Adresse Web :**

LINEACT

www.lineact.cesi.fr

**Etablissement : Adresse Web :**

CESI

www.cesi.fr

**Nom : Prénom :**

BRAHMIA

Mohamed-El-Amine

**Titre (Prof, HDR, …) :**

Prof

**Laboratoire : Adresse Web :**

LINEACT

www.lineact.cesi.fr

**Etablissement : Adresse Web :**

CESI

www.cesi.fr

**Nom : Prénom :**

GHALMANE

Zakariya

**Titre (Prof, HDR, …) :**

Prof

**Laboratoire : Adresse Web :**

LINEACT

www.lineact.cesi.fr

**Etablissement : Adresse Web :**

CESI

www.cesi.fr

**Domaines d’expertise :**

IoT, WSN, Routing, Protocols, Optimization problems, Smart Buildings

Data analysis, Complex networks, Machine learning

**Publications importantes en relation avec le sujet proposé :**

Syarif, A., Brahmia, M. E. A., Dollinger, J. F., Abouaissa, A., & Idoumghar, L. (2022). RPL-OC: Extension of RPL Protocol for LLN Networks based on the Operator Calculus approach. In *Proceedings of Sixth International Congress on Information and Communication Technology* (pp. 47-58). Springer, Singapore.

Brahmia, M. E. A., Babouche, S., Ouchani, S., & Zghal, M. An Adaptive Attack Prediction Framework in Cyber-Physical Systems. Sumitted to Globecom conference 2022.

Ghalmane, Z., Cherifi, C., Cherifi, H., & El Hassouni, M. (2021). Extracting modular-based backbones in weighted networks. Information Sciences, 576, 454-474.

Ghalmane, Z., Cherifi, C., Cherifi, H., & Hassouni, M. E. (2019). Centrality in complex networks with overlapping community structure. *Scientific reports*, *9*(1), 1-29.

**Adresse Web de votre page personnelle :**

<https://scholar.google.fr/citations?user=7UbBSZ0AAAAJ>

<https://scholar.google.fr/citations?user=9M3L2ZUAAAAJ>

<https://scholar.google.fr/citations?user=U1p40c4AAAAJ>

**Adresse mail :**

mzghal@cesi.fr, abrahmia@cesi.fr, zghalmane@cesi.fr

**Description du sujet de thèse proposé : Discipline :**

Informatique

**Titre et Résumé :**

Détection d'anomalies de sécurité dans les réseaux IoT par réseaux complexes et techniques d'IA

**Sujet :**

**Description du sujet (contexte scientifique, description du problème, Objectifs, …..) :**

L'Internet des objets (IoT) joue un rôle important dans la transformation numérique dans plusieurs domaines. Le renforcement de la sécurité des réseaux loT est en passe de devenir l'un des problèmes les plus cruciaux auxquels doit faire face la communauté des technologies de l'information. En effet les mécanismes de surveillance sont souvent compliqués à mettre en œuvre notamment dans des environnements hétérogènes comportant des nœuds avec des caractéristiques différentes **[1]**. La ville intelligente ainsi que l’industrie du futur sont fortement concernées par cette transition inévitable où l’intégration de nouveaux capteurs et actionneurs doit se faire en toute harmonisation avec les équipements déjà existants. Cette contrainte ne devrait pas tout de même exposer le réseau IoT aux multiples attaques dont il est régulièrement la cible. En plus d’empêcher les intrusions, notre but dans le cadre de ce projet est de détecter les anomalies en temps réel, voire les prédire tout en prenant en compte les spécificités des objets connectés.

**Approche méthodologique :**

Dans des travaux précédents **[2-8]**, certaines propriétés des réseaux IoT ont déjà été exploitées pour alimenter des classificateurs d'apprentissage automatique supervisé pour la détection d'anomalies. Dans ce projet, notre but est aussi d'utiliser les propriétés de réseaux complexes pour détecter avec précision toute anomalie/intrusion potentielle dans les réseaux IoT. À notre connaissance, il s'agit de la première tentative où des mesures de réseaux complexes ainsi que des caractéristiques de réseaux IoT sont extraites de chaque dispositif IoT et utilisées comme propriétés d'entrée pour les classificateurs d'apprentissage automatique.

**Résultats attendus :**

- Définir un cadre générale basé sur les réseaux complexes et les techniques IA

- Détection des anomalie dans les réseaux IoT

- Amélioration de la sécurité des réseaux IoT

**Bibliographie :**

**[1]** Bourdon, M. (2021). *Détection d'intrusion basée sur l'analyse de compteurs matériels pour des objets connectés* (Doctoral dissertation, Toulouse, INSA).

**[2]** Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications surveys & tutorials, 18(2), 1153-1176.

**[3]** Kilincer, I. F., Ertam, F., & Sengur, A. (2021). Machine learning methods for cyber security intrusion detection: Datasets and comparative study. Computer Networks, 188, 107840.

**[4]** Stoian, N. A. (2020). Machine Learning for anomaly detection in IoT networks: Malware analysis on the IoT-23 data set (Bachelor's thesis, University of Twente).

**[5]** Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. M. A. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet of Things, 7, 100059.

**Bibliographie :**

**[6]** Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., & Ming, H. (2019, January). Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0305-0310). IEEE.

**[7]** Garg, S., Kaur, K., Kumar, N., Kaddoum, G., Zomaya, A. Y., & Ranjan, R. (2019). A hybrid deep learning-based model for anomaly detection in cloud datacenter networks. IEEE Transactions on Network and Service Management, 16(3), 924-935.

**[8]** Eltanbouly, S., Bashendy, M., AlNaimi, N., Chkirbene, Z., & Erbad, A. (2020, February). Machine learning techniques for network anomaly detection: A survey. In 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT) (pp. 156-162). IEEE.

**Mots clés :**

IoT, Sécurité, Détection, Smart Cities, Réseaux Complexes, Apprentissage automatique.

**Possibilité de financement (Justificatif éventuel) :**

Candidature pour une bourse UL-EDST

**Profil Scientifique du candidat :**

Titulaire d'un master recherche en informatiques.

* À joindre un fichier PDF détaillant le sujet.