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

Zakariya Ghalmane[1,*], Amine Brahmia[1,*], Mourad Zghal[1,*], Ahmad Fadlallah[2,**], Ali Jaber[2,**]
[1] LINEACT, CESI Strasbourg, France
[2] Université Libanaise, Beyrouth, Liban
[*] zghalmane@cesi.fr, abrahmia@cesi.fr, mzghal@cesi.fr
[**] ahmad.fadlallah@ul.edu.lb, ali.jaber@ul.edu.lb

Mots clés : IoT, Sécurité, Détection, Smart Cities, Réseaux Complexes, Apprentissage automatique.

L'Internet des objets (IoT) joue un rôle important dans la transformation numérique dans plusieurs domaines. En connectant des capteurs, des instruments et autres dispositifs, l'IoT facilite la collecte et l'analyse des données ainsi que le contrôle automatisé. 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. Cependant, avec le développement et le déploiement à grande échelle de dispositifs loT, la capacité de ces appareils à communiquer de manière sécurisée sans compromettre les performances représente un grand défi. Ainsi, mettre en place une approche globale pour la détection d'intrusion devient la solution de sécurité de premier plan dans divers domaines (transports, énergie, usines intelligentes, etc.), qui protégera les réseaux contre différentes activités malveillantes. 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.

L'objectif de ce projet est d'appliquer l'outil d'analyse de réseaux complexes ainsi que différents algorithmes d'apprentissage automatique pour détecter et prédire avec efficacité les anomalies sur tout type d'intrusions dans les réseaux IoT. Ces dernières années, le développement de réseaux complexes a suscité un grand intérêt pour l'étude des principes et des mécanismes caractérisant l'Internet des objets (IoT). Effectivement, les analyses basées sur les réseaux complexes sont en plein essor dans de nombreuses disciplines scientifiques, telles que le numérique, la santé, l'écologie, etc.[2–8] Ces méthodes suscitent un intérêt croissant en raison du nombre d'informations et de données différentes qu'elles peuvent traiter ainsi que de leur capacité à décrire et à révéler des modèles et des dynamiques complexes[9,10]. Ces analyses font intervenir des algorithmes de modélisation, des indices mathématiques et des approches graphiques qui complètent les outils traditionnels de ces disciplines[11–14]. Cependant, malgré son importance en tant qu'outil adapté à l'analyse des réseaux IoT, les réseaux complexes semble peu appliquée à leur sécurité contre les intrusions malveillantes. Il reste encore beaucoup à faire pour que cette technique soit pleinement intégrée afin de faire face aux défis liés à cette problématique.

Dans des travaux précédents[15–21], certaines propriétés des réseaux IoT ont déjà été exploitées pour alimenter des classificateurs d'apprentissage automatique supervisé pour la détection d'anomalies. Dans ce contexte, 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

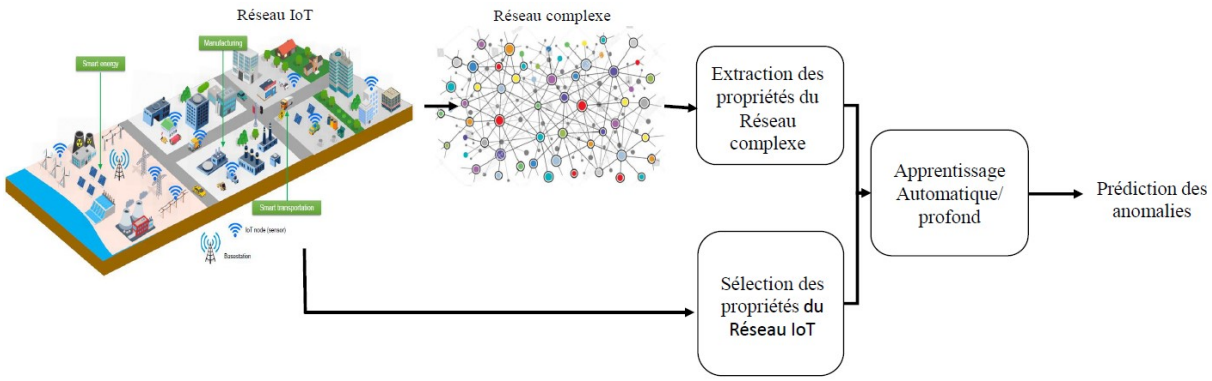

Figure 1. Figure représentant les étapes de l'approche proposée par ce projet.

automatique. Ce projet de recherche fournirait donc une nouvelle approche basée sur la modélisation en réseau complexe combinée avec des algorithmes d'apprentissage automatique et/ou profond, visant à détecter avec une grande précision les anomalies liées à la sécurité des réseaux IoT (Figure 1). L'approche visée est donc originale dans le sens où elle intègre des mécanismes permettant de prendre en compte le fonctionnement macroscopique du réseau ainsi que les spécificités des noeuds le composant.

References

1. Bourdon, M. *Détection d'intrusion basée sur l'analyse de compteurs matérielspour des objets connectés. (Intrusion detection based on the analysis of hardware countersfor connected objects)*. Ph.D. thesis, INSA Toulouse, France (2021).
2. Sporns, O. Graph theory methods: applications in brain networks. *Dialogues clinical neuroscience* (2022).
3. Herrera, M., Pérez-Hernández, M., Kumar Parlikad, A. & Izquierdo, J. Multi-agent systems and complex networks: Review and applications in systems engineering. *Processes* **8**, 312 (2020).
4. Xie, P. & Xu, Z. Formation feature analysis with heterogeneous unmanned vehicles for ocean monitoring based on complex network. *CONVERTER* **2021**, 503–520 (2021).
5. Wang, Z. *et al.* Controllability robustness of heat exchanger network based on complex network theory. *Asia-Pacific J. Chem. Eng.* **16**, e2711 (2021).
6. Ma, X., Zhou, H. & Li, Z. On the resilience of modern power systems: A complex network perspective. *Renew. Sustain. Energy Rev.* **152**, 111646 (2021).
7. Soloviev, V., Solovieva, V., Tuliakova, A., Hostryk, A. & Pichl, L. Complex networks theory and precursors of financial crashes (CEUR Workshop Proceedings, 2020).
8. Zhao, Z., Wang, Z., Zou, L. & Guo, J. Set-membership filtering for time-varying complex networks with uniform quantisations over randomly delayed redundant channels. *Int. J. Syst. Sci.* **51**, 3364–3377 (2020).
9. Estrada, E. Introduction to complex networks: structure and dynamics. In *Evolutionary equations with applications in natural sciences*, 93–131 (Springer, 2015).
10. Battiston, F. *et al.* Networks beyond pairwise interactions: structure and dynamics. *Phys. Reports* **874**, 1–92 (2020).
11. Mata, A. S. d. Complex networks: a mini-review. *Braz. J. Phys.* **50**, 658–672 (2020).
12. Scabini, L. F. *et al.* Social interaction layers in complex networks for the dynamical epidemic modeling of covid-19 in brazil. *Phys. A: Stat. Mech. its Appl.* **564**, 125498 (2021).
13. Berahmand, K., Nasiri, E., Forouzandeh, S. & Li, Y. A preference random walk algorithm for link prediction through mutual influence nodes in complex networks. *J. King Saud Univ. Inf. Sci.* (2021).
14. Ghalmane, Z., Cherifi, C., Cherifi, H. & Hassouni, M. E. Centrality in complex networks with overlapping community structure. *Sci. reports* **9**, 1–29 (2019).
15. Buczak, A. L. & Guven, E. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Commun. surveys & tutorials* **18**, 1153–1176 (2015).
16. Kilincer, I. F., Ertam, F. & Sengur, A. Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Comput. Networks* **188**, 107840 (2021).
17. Stoian, N.-A. *Machine Learning for anomaly detection in IoT networks: Malware analysis on the IoT-23 data set*. B.S. thesis, University of Twente (2020).

18. Hasan, M., Islam, M. M., Zarif, M. I. I. & Hashem, M. Attack and anomaly detection in iot sensors in iot sites using machine learning approaches. *Internet Things* **7**, 100059 (2019).

19. Alrashdi, I. *et al.* 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)*, 0305–0310 (IEEE, 2019).

20. Garg, S. *et al.* A hybrid deep learning-based model for anomaly detection in cloud datacenter networks. *IEEE Transactions on Netw. Serv. Manag.* **16**, 924–935 (2019).

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