Sujet de thèse : Analyse de la vulnérabilité des systèmes logistiques et de transport (CYBERLOG)

Directeurs de thèse : Dimitri Lefebvre en co-direction avec Edouard Leclercq

Laboratoire d'accueil : GREAH
Etablissement : Normandie Université – Université Le Havre
Ecole doctorale : PSIME
Financement : allocation Région Normandie RIN CTM 50% et LHSM 50%
Date de début : 01/10/2022

Profil recherché : candidat.e avec un profil informatique ou automatique - systèmes à événements discrets. Une connaissance de la théorie des automates et des systèmes stochastiques sera appréciée ainsi qu'une bonne pratique de la programmation.

Les candidat.e.s sont invité.e.s à envoyer CV, lettre de motivation et résultats académiques du Master ou de la formation d'ingénieur à
dimitri.lefebvre@univ-lehavre.fr

Contexte et objectif

La liste des sociétés de transport et de logistique victimes de cyberattaques ne cesse de s'allonger. Pour mémoire, en 2017, une cyberattaque mondiale avait ciblé plusieurs grandes entreprises : le ransomware NotPetya avait notamment frappé Maersk et FedEx. Fin septembre 2020, le secteur du transport et de la logistique a de nouveau été frappé : le groupe Gefco a été la victime d'une attaque, suivie quelques jours plus tard par CMA CGM. Au même moment, l'Organisation maritime internationale a également annoncé avoir été concernée. Dans son rapport annuel de la sécurité maritime 2020, publié en juillet dernier, l'assureur Allianz faisait état d'une augmentation de 400% des tentatives de cyberattaques dans le secteur maritime depuis début 2020. Le phénomène ne cesse donc de prendre de l'ampleur et est désormais considéré comme une menace majeure par les entreprises du secteur mais aussi les pouvoirs publics. Le secteur de la logistique et du transport est en quelque sorte victime de ses avancées technologiques les plus récentes, notamment en matière d'automatisation et de traitement de l'information. L'utilisation accrue de réseaux de communication ouverts et de moyens de transport et manutention autonomes fragilise ces systèmes. De nombreuses études font désormais états des cyber-menaces dans les moyens de transport autonomes et connectés terrestres [19], [20], [21] ou maritimes [22].

Si, face à la cyber menace, les plus grandes entreprises améliorent leur protection, les fournisseurs et prestataires de services ont moins de facilité à se protéger. Pour ces entreprises, généralement de taille plus modeste, la question de la cyber-sécurité ne fait malheureusement pas partie des priorités et les transforme donc en cibles de choix pour les cyberattaques. En milieu industriel, les lignes de production de conditionnement, le stockage ou encore le passage dans les réseaux de distribution sont autant de points de vulnérabilité propices à une contamination malveillante. De façon générale, les cyber-criminels reproduisent dans les systèmes logistiques les schémas d'attaque qu'ils utilisent pour nuire aux systèmes informatiques [15] [18] [11]. Dans ce contexte, **l'objectif du projet CYBERLOG est de proposer une méthodologie d'analyse de la vulnérabilité des systèmes permettant de quantifier le risque d'attaque pour un environnement donné.** Afin d'impacter le plus grand nombre de bénéficiaires, CYBERLOG se propose de travailler sur des modèles d'échange de données et de cyber-attaques standards.

Position

Le développement d'algorithmes et d'architectures efficaces pour l'analyse des cyberattaques est un domaine de recherche très actif et en rapide expansion [17]. L'hétérogénéité des composants des systèmes logistiques et l'émergence continue de nouvelles menaces rendent cette question à la fois difficile à résoudre pour les opérateurs du secteur et captivante pour les chercheurs. De nombreux travaux existent liés aux enjeux de sécurité [16] et plus particulièrement à la détection des cyber-attaques. Les approches proposées peuvent être classées par domaine ou selon les supports utilisés pour échanger des informations [12]. Les axes « Fondements du numérique : informatique, automatique, traitement du signal (E1) » et « Sécurité globale, résilience et gestion de crise, cybersécurité (H17) » de l'aap générique ANR en 2021 en ont notamment fait une de leur priorité. Récemment, le problème a également été abordé en utilisant les systèmes à événements discrets (SED) [14]. Pour la modélisation et l'analyse des systèmes dynamiques, la théorie des SED fournit des abstractions et des formalismes mathématiques, notamment les automates et les réseaux de Petri [5]. L'un des avantages de l'approche proposée par les SED est de fournir une abstraction des mécanismes d'échange et de manipulation de la donnée qui s'affranchie de la technologie mise en œuvre. Plusieurs équipes en France s'intéressent à certains aspects des questions liées à la cyber-sécurité sous l'angle des SED (Pôle d'excellence Cyber, Université de Paris Saclay, Université de Lorraine, Université de Renne…). Malgré les avancées récentes dans ces domaines, des améliorations des formalismes existants et des développements théoriques sont encore nécessaires pour faire face efficacement aux cyber-menaces. Le GREAH contribue lui aussi depuis 2019 à une étude (avec l'Université Aix Marseille et l'Université de Paris Saclay) soutenue par l'INSII (CNRS) au travers du projet CPSécurité.

Dans le cadre de cette thèse, nous supposons que l'attaquant a réussi à accéder au réseau du système logistique et a la capacité d'altérer les données échangées. Cela signifie que toutes les mesures de protection adoptées pour empêcher de telles attaques ont échoué et que l'attaquant peut agir sur les commandes envoyées au système et/ou interférer avec les informations renvoyées par le système. Plus précisément, l'attaquant peut modifier, supprimer ou ajouter des symboles de commande ou des informations de sortie dans le but d'altérer le fonctionnement du processus ou de tromper ses utilisateurs. Sur la base de ces hypothèses, le GREAH, avec ses partenaires de CPSécurité, a récemment proposé un nouveau formalisme à base de réseaux de Petri synchronisés sur des événements d'entrées et délivrant des sorties et d'une classe d'automates avec des entrées [1] pour modéliser ce type d'échanges. Ce formalisme étend celui des PN synchronisés [18], des PN étiquetés et aussi des PN interprétés [5] en prenant en compte les symboles d'entrée des contrôleurs et les étiquettes de sortie générées par les capteurs. Des travaux ont démarré sur les observateurs dédiés à ces modèles [1] et sur l'analyse de la vulnérabilité [3], [4].

Méthodologie, programme de travail et perspectives

La question centrale qui sera abordée au cours de cette thèse est d'étudier les informations temporelles associées aux symboles d'entrée et aux informations de sortie afin de proposer une analyse plus fine de la vulnérabilité. De tels aspects ont été rarement considérés jusqu'à présent et les approches existantes sont principalement basées sur le comportement logique des systèmes étudiés [8]. Une des difficultés qui devra être résolue [14] est l'extension de la composition de modèles logiques (automates) dans le domaine temporel. Le projet CYBERLOG vise à étudier en particulier les aspects temporels et probabilistes : la modélisation du temps, dans un cadre événementiel, la manipulation et la composition de modèles temporisés probabilistes, l'analyse d'observations temporisées, l'utilisation d'horloges asynchrones dans des structures distribuées, les délais de communication dans les systèmes critiques. Les schémas de détection reposeront sur la discrimination non seulement des écarts logiques du comportement du système, mais également de toute incohérence temporelle causée par l'attaque.

L'étude sera décomposée en deux tâches principales accompagnées d'une étape préliminaire d'état de l'art.

Analyse de vulnérabilité du système : elle sera envisagée à partir de modèles formels par automates finis et réseaux de Petri. L'analyse s'appuiera sur une spécification des états du système : états interdits, dangereux ou normaux. L'objectif sera d'évaluer la détectabilité moyenne d'une attaque visant à mettre le système dans un état dangereux. Pour se faire, nous proposons d'adapter certains indicateurs probabilistes déjà utilisés pour évaluer l'opacité (la confidentialité de l'information) avec des modèles stochastiques [2], [6] ainsi que quelques résultats disponibles proposés originellement pour évaluer une détectabilité moyenne d'attaque [7]. De tels indicateurs pourraient inclure (mais ne seront pas limités à) des délais de détection moyens, des temps et des fréquences d'exposition (qui mesurent combien de temps et à quelle fréquence, en moyenne, le système est vulnérable aux attaques), et des temps de révélation (qui mesurent combien de temps, sur moyenne, le système reste résilient aux attaques). L'utilisation de modèles de Markov sera privilégiée. Une analyse moyenne de la vulnérabilité sera ainsi proposée.

Détection : pour les systèmes vulnérable cette tâche vise à développer des méthodes exploitant les aspects temporels pour améliorer la détection des cyberattaques. Ici par détection, nous entendons apporter une décision (oui, non ou ambigüe) à la question « Le système est-il actuellement attaqué ?». Le.la doctorant.e se concentrera sur la conception de certaines structures de détection particulières – vérificateurs - qui seront intégrés dans les schémas de détection des cyber-attaques [10]. Une première étape consistera à composer des modèles temporisés avec des vérificateurs logiques [1]. Dans ce cas, les aspects temporels seront limités aux comportements du système. Une deuxième étape plus difficile devra inclure également les aspects temporels dans les vérificateurs. Cette étude pourra tirer profit de quelques travaux préliminaires sur les observateurs temporisés pour des délais constants [13] et des délais par intervalle [9] ainsi que sur les travaux développés dans le cadre du projet CPSécurité.

Cette thèse est menée en partenariat avec LHSM et des applications à l'analyse de vulnérabilité des systèmes logistiques et de transport – en particulier maritimes – seront privilégiées.

Bibliographie

[1] Ammour, R., Amari, S., Brenner, L., Demongodin, I., and **Lefebvre**, D. (2021). Observer design for output synchronized Petri nets. *European Control Conference (ECC)*.

[2] **Lefebvre** D., Hadjicostis C., Privacy and safety analysis of timed stochastic discrete event systems using Markovian trajectory-observers, *Journal of Discrete Event Systems*, 30(3), pp. 413-440, 2020.

[3] Ammour, R., Amari, S., Brenner, L., Demongodin, I., and **Lefebvre**, D. (2021). Costs analysis of stealthy attacks with bounded output synchronized Petri nets. *IEEE Int. Conference on Automation Science and Engineering (CASE)*, 799-804.

[4] Ammour, R., Leclercq, E., Sanlaville, E., and **Lefebvre**, D. (2017). Fault prognosis of timed stochastic discrete event systems with bounded estimation error. *Automatica*, *82*, 35-41.

[5] David, R., and Alla, H. (2010). *Discrete, continuous, and hybrid Petri nets*. Berlin: Springer.

[6] **Lefebvre** D., Hadjicostis C., Exposure and revelation times as a measure of opacity in timed stochastic discrete event systems, *IEEE Trans. On Automatic* Control, December 2021.

[7] **Lefebvre** D., Seatzu C., Hadjicostis C.N., Giua A., Probabilistic state estimation for labeled continuous time Markov models with applications to attack detection, to appear in *Journal of Discrete Event Systems*, 2021.

[8] Fritz, R., Schwarz, P., and Zhang, P. (2019). Modeling of cyber-attacks and a time guard detection for ICS based on discrete event systems. *European Control Conference (ECC)*.

[9] Gao, C., **Lefebvre**, D., Seatzu, C., Li, Z., and Giua, A. (2020). A region-based approach for state estimation of timed automata under no event observation. *IEEE Int. Conference on Emerging Technologies and Factory Automation (ETFA), 1*, 799-804.

[10] Hadjicostis, C. N. (2020). *Estimation and Inference in Discrete Event Systems*. Springer International Publishing.

[11]Zhang, M., Tao, F., Huang, B., Liu, A., Wang, L., Anwer, N., and Nee, A. Y. C. (2021). Digital twin data: methods and key technologies. *Digital Twin*, *1*(2), 2.Koucham, O., 2018, *Intrusion detection for industrial control systems* (Doctoral dissertation).

[12]Li J., **Lefebvre** D., Hadjicostis C.N., and Li Z. (2022). Observers for a class of timed automata based on elapsed time graphs, IEEE *Transactions on Automatic Control*.

[13]Li, Y., Tong, Y., and Giua, A. (2020). Detection and Prevention of Cyber-Attacks in NCSs. *IFAC-PapersOnLine*, *53*(4), 7-13.

[14]Tao, F., Anwer, N., Liu, A., Wang, L., Nee, A. Y., Li, L., and Zhang, M. (2021). Digital twin towards smart manufacturing and industry 4.0. *Journal of manufacturing systems*, *58*, 1-2.

[15]Lun, Y. Z., D'Innocenzo, A., Smarra, F., Malavolta, I., and Di Benedetto, M. D. (2019). State of the art of cyber-physical systems security: An automatic control perspective. *Journal of Systems and Software*, *149*, 174-216.

[16]Mao, Y., Jafarnejadsani, H., Zhao, P., Akyol, E., and Hovakimyan, N. (2020). Novel stealthy attack and defense strategies for networked control systems. *IEEE Transactions on Automatic Control*, *65*(9), 3847-3862.

[17]Pocci, M., Demongodin, I., Giambiasi, N., and Giua, A. (2016). Synchronizing sequences on a class of unbounded systems using synchronized Petri nets. *Discrete Event Dynamic Systems*, *26*(1), 85-108.

[18]Sandberg, H., Amin, S., and Johansson, K. H. (2015). Cyberphysical security in networked control systems: An introduction to the issue. *IEEE Control Systems Magazine*, *35*(1), 20-23.

[19]Dibaei M., Zheng X., Jiang, K., Abbas R., Liu S., Zhang Y., Xiang Y., Yu S., Attacks and defenses on intelligent connected vehicles: a survey, *Digital Communications and Networks*, Volume 6, Issue 4, pp. 399-421, 2020.

[20]Kim K., Seok J. Kim, Jeong S., Park J-H., Kim H.K., Cybersecurity for autonomous vehicles: Review of attacks and defense, *Computers & Security*, vol. 103, 2021.

[21]Pham M., Xiong K., A survey on security attacks and defense techniques for connected and autonomous vehicles, *Computers & Security*, vol. 109, 2021.

[22]Alcaide J.I., Llave R.G., Critical infrastructures cybersecurity and the maritime sector, *Transportation Research Procedia*, vol 45, pp. 547-554, 2020.