Proposition de Thèse LUE au CRAN (2019-2022)
Directeurs de thèse : Benoît Marx et Jean-Christophe Ponsart

–

Titre : Détection, localisation et identification d'attaques de systèmes cyber-physiques
Mots-clefs : : Sécurité, systèmes cyber-physique, diagnostic.

Contexte

Les systèmes cyber-physiques (SCP) se caractérisent par l'intégration de processus physiques et de capacités de calcul et de communication (par exemple un réseau instrumenté et supervisé de transport et de distribution d'eau potable). Ces systèmes sont dits cyber-physiques car ils sont constitués d'une partie physique (canalisations, réservoirs, stations de pompage, etc.) mais comportent également des organes de mesure de grandeurs physiques (capteurs de débits de pressions et de qualité de l'eau), des réseaux de transmission d'information ainsi que des organes de commandes qui vont agir sur la partie physique. Ces systèmes, outre leurs propres défaillances éventuelles (usure de composants), doivent faire face à des attaques externes malveillantes qui peuvent dégrader fortement leurs fonctionnements. La surveillance des SCP est donc un enjeux majeur [7, 9, 11, 17] : il est essentiel d'être en mesure de détecter, localiser et identifier ces attaques extérieures et de les distinguer des dysfonctionnements propres aux SCP.

Différentes approches existent dans la littérature : certains auteurs utilisent la supervision de systèmes à événements discrets [6, 13], d'autres le traitement statistique de données [5] ou un mélange de théorie des graphes et du contrôle [17]. Enfin, une majorité utilise des outils de la théorie du contrôle [1, 3, 4, 9, 10, 11, 12, 15, 16, 19]. Dans ces travaux, les SCP sont représentés par différentes classes de modèles : linéaires [3, 8, 10, 12, 15, 16, 18, 21], linéaires descripteurs [11, 17] ou non linéaires [1, 4, 19]. Dans le cas de modèles linéaires, des outils de la théorie des graphes et de l'automatique permettent respectivement une analyse structurelle des attaques (détectabilité, distinguabilité, etc.) et leur estimation [10, 17].

Les attaques prises en compte dans les travaux existants sont de différentes natures. Les attaques de type *denial of service (DoS)* consistent à submerger le contrôleur de requêtes ou d'informations, ce qui - à cause des files d'attente - se traduit par des retards dans les transmissions vers ou depuis la partie commande. Les attaques DoS peuvent aussi être des pertes et des interceptions de données et sont alors modélisées par des mesures manquantes ou irrégulièrement échantillonnées [4, 12, 18]. La modification ou l'insertion de fausses données sont appelées *deception attacks* et sont généralement prises en compte sous forme de signaux additifs en entrée ou sortie de la partie physique du SCP [3, 8, 10, 15]. L'attaquant peut également remplacer un signal par un signal passé, il s'agit alors de *replay attacks*, prise en compte par des délais variables sur les transmissions [17].

Détail des recherches attendues

Comme cité précédemment, certains travaux utilisent des modèles descripteurs linéaires comportant des relations dynamiques et statiques pour tenir compte des contraintes de conservation de matière ou d'information dans les réseaux physiques ou de communication [14, 22]. D'autres travaux utilisent des modèles dynamiques non linéaires. Logiquement, l'objet des travaux de thèse serait l'extension de l'étude de la détection d'attaques de SCP représentés par des modèles descripteur non linéaires. Ceci permettrait la généralisation des résultats existant à une classe plus large de SCP. Cette extension n'a pas été faite jusqu'ici car les outils utilisés ne sont pas généralisables au cas non linéaire générique. Parmi les nombreuses approches non linéaires possibles, on privilégiera l'approche polytopique ou LPV permettant de modéliser efficacement des phénomènes non linéaires tout en bénéficiant de certains avantages des structures linéaires [20].

Les attaques à envisager dans le cadre de cette thèse sont les suivantes :
- les attaques extérieures prennant la forme de corruptions des mesures faites sur le SCP : entrées inconnues se substituant ou corrompant les données transmises [17] ;
- les attaques sous forme de défauts de transmission depuis ou vers la partie physique : données manquantes, saturations [2], ou zones mortes.

Après une étude bibliographique, les solutions que le candidat pourrait envisager dans le cadre de cette thèse sont les suivantes :
- diagnostic à base d'observateurs pour les SCP basés sur une représentation par des modèles descripteurs polytopiques / LPV ;
- diagnostic de SCP représentés par des modèles descripteurs polytopiques / LPV par factorisation copremière, cette technique a été utilisée dans le cadre linéaire pour le diagnostic et le contrôle tolérant aux fautes [23], mais son extension au cas LPV reste ouverte ;
- synthèse de filtres de diagnostic pour modèles descripteurs polytopiques / LPV ;

- modélisation polytopique des phénomènes de saturations et / ou de zones mortes permettant leur prise en compte dans le modèle du système, voire leur estimation [2].

Références

[1] G. Bernieri, E.E. Miciolino, F. Pascucci, R. Setola, Monitoring system reaction in cyber-physical testbed under cyber-attacks , Computer and Electrical Engineering, 59 : 86-98, 2017.

[2] S. Bezzaoucha, B. Marx, D. Maquin, J. Ragot, State and output feedback control for Takagi-Sugeno systems with saturated actuators, International Journal of Adaptive Control and Signal Processing, 30 : 888-905, 2016.

[3] S. Bezzaoucha Rebai, H. Voos and S.A. Sajadi Alamdari, A Contribution to Cyber-Physical Systems Security : an Event-based Attack-tolerant Control Approach, IFAC Safeprocess, 2018.

[4] F. Boem, R.M.G. Ferrari, C. Keliris, T. Parisini, M.M. Polycarpou, A Distributed Networked Approach for Fault Detection of Large-Scale Systems, IEEE Transactions on Automatic Control, 62(1) : 18-33, 2017.

[5] E. Bou-Harb, N. Ghani, A. Erradi, K. Shaban, Passive inference of attacks on CPS communication protocols, Journal of Information Security and Applications, 43 : 110-122, 2018.

[6] L.K. Carvalho,Y.C. Wu, R. Kwong, S. Lafortune, Detection and mitigation of classes of attacks in supervisory control systems, Automatica, 97 : 121-133, 2018.

[7] I. Colak, S. Sagiroglu, G. Fulli, M. Yesilbudak, C.F. Covrig, A survey on the critical issues in smart grid technologies, Renewable and Sustainable Energy Reviews, 54 : 396-405, 2016.

[8] M.L. Corradini, A. Cristofaro, A sliding-mode scheme for monitoring malicious attacks in cyber-physical systems, IFAC World Congress, 2017.

[9] D. Ding, Q.L. Han, Y. Xiang, X Ge, X.M. Zhang, , A survey on security control and attack detection for industrial cyber-physical systems, Neurocomputing, 275 : 1674-1683.

[10] F. Fu, D. Wang, P. Liu, W. Li, Evaluation of fault diagnosability for networked control systems subject to missing measurements, Journal of the Franklin Institute, 355 : 8766-8779, 2018.

[11] F. Hu, Y. Lu, A.V. Vasilakos, Q. Hao, R. Ma, Y. Patil, T. Zhang, J. Lu, X. Li, N.N. Xiong, Robust Cyber-Physical Systems : Concept, models, and implementation, Future Generation Computer Systems, 56 : 449-475, 2016.

[12] Z.M. Li, X.H. Chang, Robust H_∞ control for networked control systems with randomly occurring uncertainties : Observer-based case. ISA Transactions (2018).

[13] P.M. Lima, M.V.S.Alves, L.K. Carvalho, M.V. Moreira, Security Against Network Attacks in Supervisory Control Systems, IFAC World Congress, 2017.

[14] R. Lopez Estrada, Contribution au diagnostic de défauts à base de modèles : Synthèse d'observateurs pour les systèmes singuliers linéaires à paramètres variants aux fonctions d'ordonnancement non mesurables, Thèse de doctorat de l'Université de Lorraine, 2014.

[15] Y. Mo, R. Chabukswar, B. Sinopoli, Detecting Integrity Attacks on SCADA Systems, IEEE Transactions on Control Systems Technology, 22(4) : 1396-1407, 2014.

[16] M. Pajic, S. Sundaram, G.J. Pappas,R. Mangharam, The Wireless Control Network : A New Approach for Control Over Networks, IEEE Transactions on Automatic Control, 56(10) : 2305-2318, 2011.

[17] F. Pasqualetti, F. Dorfler, F. Bullo, Attack Detection and Identification in Cyber-Physical Systems, IEEE Transactions on Automatic Control, 58(11) :2715-2729, 2013.

[18] K. Schenk, B. Gulbitti, J. Lunze, Cooperative Fault-Tolerant Control of Networked Control Systems, IFAC Safeprocess, 2018.

[19] H. Shahnazari, P. Mhaskar, Distributed fault diagnosis for networked nonlinear uncertain systems, Computers and Chemical Engineering, 115 : 22-33, 2018.

[20] K. Tanaka and H.O. Wang. Fuzzy Control Systems Design and Analysis : A Linear Matrix Inequality Approach. Wiley, 2001.

[21] G. Xiao, F. Liu, System Reconfiguration and Fault-Tolerant for Distributed Model Predictive Control Using Parameterized Network Topology, IFAC ADCHEM, 2018.

[22] S. Xu and J. Lam. Robust Control and Filtering of Singular Systems. Lecture Notes in Control and Information Sciences. Springer, 2006.

[23] K. Zhou and Z. Ren. A new controller architecture for high performance, robust, and fault-tolerant control. IEEE Transactions on Automatic Control, 46(10) :1613-1618, 2001.