UNIKASSEL VERSITÄT

Mess- und Regelungstechnik
Univ.-Prof. Dr.-Ing. Andreas Kroll

Masterarbeit

Erkennung von Cyber-Angriffen auf die Modellfabrik µPlant mittels linearer regelungstechnischer Methoden

Felix Lattmann

Die Vernetzung von Maschinen mittels Internettechnologien ist die Grundlage für die digitale Transformation der Industrie sowie für die 4. Industrielle Revolution (Industrie 4.0). Der so ermöglichte Datenaustausch und Datenzugriff ermöglicht einerseits Funktionen angefangen von zustandsorientierter Wartung über Energieeinsparungen durch vorausschauende Betriebsführung bis hin zu selbstoptimierenden und resilienten Produktionsanlagen. Andererseits vereinfacht der Einzug von Internet-technologien in den maschinennahen Bereich Angriffe auf Produktionsanlagen über Automatisierungs- und (Feld-)Kommunikationssysteme.

Im Rahmen dieser Masterarbeit soll untersucht werden, wie die Prozessinsel II der Modellfabrik µPlant angegriffen und wie die Angriffe mittels regelungstechnischer Methoden detektiert werden können. Dazu ist insbesondere vorgesehen, für die Detektion den Prozesszustand mittels Kalman-Filter zu schätzen und die geschätzten Sensorwerte mit den tatsächlichen Messwerten zu vergleichen. Startpunkt für die Residuumsbewertung sind Schwellenwert-, χ^2- und CUSUM-Methode. Beispiel-szenarien sind über- oder leerlaufende Tanks, wobei letzteres zum Trockenlauf und zur Beschädigung von Pumpen führt.

Folgende Teilaufgaben sollen bearbeitet werden:

- Einarbeitung in die Modellfabrik µPlant sowie Einarbeitung in und Recherche zu Entwurf und Erkennung maschinennaher Cyberangriffe
- Experimentelle Rauschanalyse in der µPlant involvierter Sensorsignale
- Konzipierung und Auslegung von Fallstudien (Betriebssituationen, Angriffe)
- Experimentelle Gewinnung von Daten, Subspace-Identifikation eines dynami-schen Modells, Bewertung der Modellgüte bei Closed-loop-Identifikation
- Kalman-Filter-Realisierung und Verbesserung seiner Zuverlässigkeit
- Entwurf und Auslegung verschiedener Angriffe und Detektoren (univariate Schwellenwerte, χ^2, CUSUM, multivariate Bewertung, modellbasiert)
- Experimentelle Demonstration und Evaluation der entwickelten Verfahren in der µPlant: Parameterstudien, Detektionsgrenzen, Empfindlichkeits- und Robustheitsanalysen (Rauschen, Nichtlinearitäten), Unterscheidung Angriff von Komponentendegeneration und -fehlern
- Analyse, Bewertung und Einordnung der Ergebnisse, Ableitung verbesserter Angriffs- sowie Detektionsvorgehensweisen
- Dokumentation und Kolloquiumsvortrag

Es ist vorgesehen, die Arbeiten mittels Matlab durchzuführen.

Betreuer: Prof. Dr.-Ing. A. Kroll, Dr.-Ing. Robert Schmoll

Beginn: 01.06.2024

Geplantes Ende: 31.03.2025

Literaturhinweise:

[1] A. Athalye, C. M. Ahmed, J. Zhou. Model-based CPS attack detection techniques: strengths and limitations. In: A.I. Awad et al. (eds.) Security in cyber-physical systems, Springer, 155-187, 2021.

[2] C. M. Ahmed, S. Adepu, A. Mathur. Limitations of state estimation based cyber attack detection schemes in industrial control systems, 2016 Smart City Security and Privacy Workshop (SCSP-W), Wien, 2016.

[3] C. M. Ahmed, C. Murguia, J. Ruths. Model-based attack detection scheme for smart water distribution networks, ASIA CCS '17, Abu Dhabi, 101-113, 2017.

[4] D. Arengas. On the Detection and Selection of Informative Subsequences from Large Historical Data Records for Linear System Identification. Dissertation. FG Mess- und Regelungstechnik, Universität Kassel, 2021.

[5] M.H. Basiri, J.G. Thistle, J.W. Simpson-Porco, S. Fischmeister. Kalman filter based secure state estimation and individual attacked sensor detection in cyber-physical systems, 2019 American Control Conference (ACC), Philadelphia, USA, 2019.

[6] C. Bohn, H. Unbehauen. Identifikation dynamischer Systeme: Methoden zur experimentellen Modellbildung aus Messdaten, Abschnitt 5.5.3, Springer Vieweg, 2016.

[7] D. Ding, Q.-L. Han, X. Ge, J. Wang. Secure state estimation and control of cyber-physical systems: a survey, IEEE Transactions on Systems, Man, and Cybernetcs; Systems, Vol. 51., No. 1, 176-190, 2021.

[8] J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N.O. Tippenhauer, H. Sandberg, R. Candell. A survey of physics-based attack detection in cyber-physical systems, ACM Computing Surveys 51, No. 4, Article 76, 2018.

[9] A. Kroll, A. Dürrbaum, D. Arengas, H. Al Mawla, L. Kistner, A. Rehmer. µPlant: Eine automatisierungstechnisch-orientierte Modellfabrik für vernetzte heterogene Systeme, atp edition 59 (9) 40-53, 2017.

[10] Y. Mo, S. Weerakkody, B. Sinopoli. Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs. IEEE Control Systems Magazine, Feb 2015, 93-109, 2015.

[11] J. Rabe. Zur Erkennung von Cyber-Attacken auf Anlagen: Lineare Zustandsraum-modellbasierte Methoden und Anwendungskonzept für Modellfabrik µPlant, Seminar-arbeit, FG Mess- und Regelungstechnik, Universität Kassel, 2022.

[12] G. Raman, C.M. Ahmed, A. Mathur. Machine learning for intrusion detection in industrial control systems: challenges and lessons from experimental evaluation. Cybersecurity 4:27, 2021.

[13] J.B. Rawlings, F. Lima. State estimation of linear and nonlinear dynamic systems, Part IV: Nonlinear systems: Moving horizon estimation (MHE) and particle filtering (PF), Presentation, AICES Regional School, RWTH Aachen, 2008.

[14] M. Verhaegen, V. Verdult. Filtering and system identification for linear systems: A least squares approach, Cambridge University Press, 2007.