UNIKASSEL VERSITÄT

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

Seminararbeit

Zur Erkennung von Cyber-Attacken auf Anlagen: Lineare Zustandsraumodellbasierte Methoden und Anwendungskonzept für Modellfabrik µPlant

Janik Rabe

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. So ist Cybercrime mittlerweile eine große Bedrohung für die Industrie mit großer wirtschaftlicher Bedeutung [4]. Verschiedene Cyber-Attacken haben gezeigt, dass konventionelle Schutzmaßnahmen wie Firewalls oder Virenscanner zur Bedrohungsabwehr nicht ausreichen. Vielmehr sind maschinennahe Maßnahmen erforderlich, die Kenntnisse der Maschinendynamik wie auch der Automatisierungs- und Regelungssysteme erfordern. Ein bekanntes Beispiel ist der Stuxnet-Angriff auf die Siemens-Steuerung einer Uran-Anreicherungsanlage, der unentdeckt blieb und so etwa 1000 Zentrifugen zerstören konnte [8].

Seit wenigen Jahren erfolgt eine wissenschaftliche Auseinandersetzung mit dem Problemfeld [5,6]. So werden auch regelungstechnische Methoden eingesetzt, die den Maschinenzustand prädizieren und mit dem beobachteten vergleichen, um einen Cyber-Angriff zu detektieren.

Im Rahmen dieser Arbeit soll eine in der Literatur [1-3] vorgestellte zustands-modellbasierte Methodik zur Detektion von Cyberattacken auf Maschinen untersucht, bewertet und am Beispiel der Modellfabrik µPlant [7] ein Umsetzungskonzept entworfen werden. Ziel von Angriffen in der Modellfabrik kann bspw. das Überlaufen von Tanks oder das Trockenlaufen von Pumpen sein. Folgende Teilaufgaben sollen bearbeitet werden:

- Einarbeitung in Entwurf und Erkennung maschinennaher Cyberangriffe
- Aufarbeitung, Einordnung und kritische Bewertung des Zustandsraum-modell-basierten Cyberangriffs-Detektionskonzepts aus [1-3] inklusive methodischer Grundlagen (Subspace-Identifikation, Kalmanfilter, CUSUM-Detektor)
- Auswahl und Konzeption von Angriffsszenarien auf die Prozessinseln I und II der Modellfabrik µPlant und Bewertung alternativer Orte für die Integration des Angriffsdetektors in die IT-Architektur der Modellfabrik
- Dokumentation und Kolloquiumsvortrag.

Betreuer: Prof. Dr.-Ing. A. Kroll

Beginn: 28.10.2021

Geplantes Ende: 31.01.2022

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

[3] 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.

[4] Bitkom, Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt, Studienbericht 2020.

[5] J. Giraldo et al. A survey of physics-based attack detection in cyber-physical systems, ACM Computing Surveys 51 (4) 76:1 – 76:36, 2018.

[6] E. Bou-Harb. A brief survey of security approaches for cyber-physical systems. 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Larnaca, Cyprus, 2016.

[7] 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.

[8] R. Langner, Stuxnet und die Folgen, Langner Communications, 2017.