Analyse der elektrischen Signale zur Angriffserkennung in industriellen Systemen basierend auf maschinellem Lernen

Kurzfassung

Industrielle Systeme werden zunehmend vernetzt, um die Verwaltung eines gesamten Industriekomplexes, der eine große Anzahl von Maschinen enthalten kann, mithilfe von Computern zu erleichtern. Dies macht sie jedoch angesichts von Computerangriffen, die die im industriellen System vorhandenen Geräte beschädigen können, umso schwächer. Diese Angriffe können erkannt werden, indem die Signale untersucht werden, die direkt von den Prozesssensoren und -aktoren kommen. Da diese Angriffe darauf abzielen, Geräte zu zerstören, indem ihr ursprüngliches Verhalten drastisch geändert wird, können wir diese Verhaltensänderungen erkennen, indem wir die Signale des Prozesses mithilfe der Methode des maschinellen Lernens untersuchen.

In dieser Masterarbeit wurde ein Prozess untersucht, um Signale von einer Maschine wiederherzustellen, die Objekte nach ihren Materialien sortiert. Damit habe ich einen Datensatz von über 130 Läufen mit normalem Verhalten aufgezeichnet. Dieser Datensatz wurde halbiert, ein Teil für das Methodentraining und der andere Teil für das Testen. Mit der wiederhergestellten Signalen könnte eine Anomalieerkennung unter Verwendung verschiedener maschineller Lernmethoden durchgeführt werden. Die folgenden Methoden werden vergleichen: Convolutionnal Neural Network, Autoencoder, Support Vector Machine, Local Outlier Factor und Density-Based Spatial Clustering of Applications with Noise (DBSCAN). Unter den verschiedenen Methoden, ist DBSCAN die Methode mit der wir die besten Ergebnisse für die Erkennung von Anomalien erzielen.