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


Zusammenfassung

In dieser Masterarbeit wird die Erkennung von Anomalien in einem industriellen System untersucht, indem analoge Signale von Sensoren und Aktoren eines industriellen Prozesses mithilfe maschineller Lernmethoden direkt analysiert werden.

Da industrielle Systeme zunehmend miteinander verbunden sind, sind sie umso anfälliger für Computerangriffe. Obwohl Verteidigungssysteme existieren, können nicht alle Cyber-Angriffe erkennen. Mit der Analyse der Signale von den Sensoren und Aktoren eines Prozesses können wir dieses normalen Verhalten dank maschinellem Lernen lernen und Abweichungen von diesem Verhalten erkennen, indem wir in Echtzeit die vom Prozess kommenden Signale mit dem normalen Verhalten vergleichen, das bekannt sein soll die Methoden des maschinellen Lernens.

Dies erfordert zuerst das Erfassen der Signale aus dem Prozess. Ich habe an einem Prozess von Fraunhofer IOSBs gearbeitet, der Objekte nach ihrer Beschaffenheit sortiert. Acht Signale müssen erkannt werden: die Lichtschranke, die die Objekte erkennt, das Laufband, das das Objekt nach links oder rechts bewegt, der induktive Sensor, der die Beschaffenheit des Objekts erkennt, die Schranke, die die Objekte sortiert, der Taster, um das Laufband herzustellen Bewegen Sie sich nach links, ein Signal, wenn sich das Laufband nach links bewegt, das Licht, das die Basis blinkt und eingeschaltet bleibt, wenn der Prozess verwendet wird, und der Schalter, der den Prozess ein- oder ausschaltet. Zum Lesen dieser Signale habe ich einen Raspberry Pi 3 mit einer Spannung Reduktion Montage verwendet, da die Spannung innerhalb des Prozesses 24 V beträgt, und einen AD-Wandler, da der Raspberry nur digitale Signale liest.

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. Ich habe auch verschiedene Angriffe aufgezeichnet, die das normale Verhalten des Prozesses ändern können oder nicht, z. B. indem ich das Laufband jederzeit nach links bewege, ohne den Taster zu drücken. Ich habe verschiedene Methoden verwendet, die entweder auf der Erkennung von Anomalien oder auf der Vorhersage basieren und entweder neuronale Netze oder Cluster verwenden, um die Methoden zu vergleichen, um die herauszufinden, die uns die beste Erkennung von Anomalien bietet. Unter den verwendeten Methoden, One Dimension Convolutionnal Neural Network (1D-CNN), Autoencoder, Support Vector Machine (SVM), Local Outlier Factor (LOF) und Density Based Spatial Clustering of Applications with Noise (DBSCAN), ist DBSCAN die Methode, die die Beste Ergebnisse von bis zu 65 Prozent Accuracy bei der Erkennung von Anomalien und 87 Prozent Accuracy bei der Erkennung von normalem Verhalten.