Folie 1:

Guten Tag, ich bin Yorick LALY. Ich bin Masterstudent am KIT. Der Titel meiner Masterarbeit lautet „**Analyse der elektrischen Signale zur Angriffserkennung in industriellen Systemen basierend auf maschinellem Lernen**“. In dieser Masterarbeit beschreibe ich einen neuen Ansatz zur Anomalie Detektion. Ich detektiere Anomalien auf Basis der elektrischen Signale zwischen der SPS und den Sensoren und Aktoren eines industriellen Prozesses.

Folie 2:

Zuerst werde ich das System und das Schaltungsdesign vorstellen. Danach Stelle ich die Analyse der elektrischen Signale vor, die ich abgegriffen habe. Danach beschreibe ich die Lernmodelle die ich für meinen anomaliebasierten Ansatz ausgewählt habe. Zum Schluss stelle ich die Evaluation und Bewertung vor.

Folie 3:

Heutzutage sind industrielle System immer mehr vernetzt darum ist es einfacher für externe Menschen um die Kommunikation zu beobachten und um das System zu verstören. Internen Angriffe sind möglich. Z.B. ein Mitarbeiter kann das System verstören mit einem USB-Stick der ein Angriff Code enthalt.

Beispielsweise, der Stuxnet Angriff in Iran der, nach Analyse des Systems, die Kontrolle des PLC hat und vielen Maschinen zerstören. In jüngerer Zeit gab es einen Angriff auf eine Abwasserentgiftungsanlagen. Während des Angriffs übernahm jemand die Kontrolle über einen Computer und änderte den Gehalt bestimmter Grundstoff.

Folie 4:

In einem industriellen System werden die Prozessdaten an den Buskoppler gesendet, der sie an die speicherprogrammierbare Steuerung (SPS) übermittelt. Die SPS sendet die Daten an den Switch, der sie an einen Computer zur Verwaltung industrieller Systeme sendet.

Der klassische Ansatz um Cyber-Angriffe in einem industriellen System zu detektieren basiert auf dem Einsatz eines NIDS. Das NIDS detektiert Anomalien und Cyber-Angriffe anhand der übertragenen Netzwerkpakete am Switch. Cyber-Angriffe, wie Stuxnet oder Irongate, können mit einem NIDS **nicht** erkannt werden. Diese Angriffe verändern den SPS-Code ohne dass wir eine Änderung in den Netzwerkpaketen sehen.

Folie 5:

Mit meinem System SAAD, abgreife und analysiere ich die Signale der Sensoren und Aktoren direkt aus den Prozess um eine Veränderung des Normalverhalten zu detektieren. Somit können auch die Angriffe, wie bei Stuxnet und Irongate erkannt werden.

Folie 6:

Wir testen SAAD an einen Prozess des Fraunhofer IOSBs in Karlsruhe der Objekte nach ihrer Beschaffenheit sortiert. SAAD soll leicht zu integrieren sein. Es soll auch nicht das ganze System stören. Die Lernmodellen lernen das Normalverhalten des Prozesses.

Folie 7:

In diesem Bild sehen wir das gesamte System, das einen Bildschirm zum Lesen von Informationen über den Prozess (Anzahl der Anwendungen, ...), eine Notaus Taster, eine SPS und einen Buskoppler enthält. Das System ist über ein DB15-Kabel mit dem Prozess verbunden, das den Prozess mit dem Buskoppler verbindet.

Folie 8:

Der Betrieb des Prozesses ist einfach. Ein Topf geht unter das Lichtschranke das das Objekt erkennt und das Laufband an macht. Die Beschaffenheit wird von dem induktiven Sensor erkannt. Wenn der Topf silbern ist dann die Schranke geht runter sonst es bleib hoch. Die Lampe blinkt, wenn der Prozess an ist und bleibt an, wenn der Prozess in Betrieb ist. Durch drücken des Tasters bewegt sich das Band nach links.

Folie 9:

Ich habe das alte Kabel mit ein Y-Splitter ausgetauscht. Dank des Y-Splitter können der Prozess und der Buskoppler weiterhin miteinander kommunizieren. Während dieser Zeit kann das SAAD-System die vom Prozess und vom Buskoppler gesendeten Signale lesen, ohne die Kommunikation zwischen beiden zu stören. SAAD wird nur als Empfänger verwendet und sendet kein Signal an den Buskoppler oder Prozess.

Folie 10:

Die Signale gehen an das rechte elektrische Board und im elektrische Spannung Reduktion Montage. Danach gehen sie an das linke Board in dem AD Converter. Am Ende:

Um die Signale abzugreifen benutzen wir die Raspberry Pi 3. Es ist ein kleines Computer mit dem wir die Daten abgreifen und auf ein externe HDD speichern. Es kann Strom liefern und mehrere digitale Signale gleichzeitig lesen. Die Abtastfrequenz ist 33 Hz. Ich benutze ein Generator für den OP.

Folie 11:

Die Raspberry lese nur digitalen Signale darum brauchen wir ein AD Converter. Ich habe den MCP3008 ausgewählt. Es hat 8 analogen Channels. Die elektrische Spannung ist zu hoch für die Raspberry. Man benutze Kirchhoffsche Regeln um die Spannung zu reduziert. Der OP isoliert die Montage von der Y-Splitter.

Folie 12:

Das System benutzt 8 verschiedenen Signale zu funktionieren. Das Signal der Schranke zeigt, wenn die Schranke runter geht. Und der induktive Sensor zeigt, wenn ein silberner Topf vor ihr befindet.

Folie 13:

In diesem Bild können wir sehen, welche Signale mit welchem ​​Sensor oder Aktuator im Prozess entsprechen. Es gibt ein Signal, wenn das Laufband an ist, eins für den Taster, eines wann das Laufband nach links geht. Wir haben jeweils ein Signal für die Licht, den Schalter und die Lichtschranke.

Folie 14: Die Erkennung von Anomalien erfolgt dabei durch Erkenntnis die Abweichungen vom erlernten Normalverhalten durch maschinelles Lernen. Es gibt zwei Arten der Erkennung von Anomalien: Clustering, bei dem das normale Verhalten in einem einzigen Cluster zusammengefasst wird, und die Daten außerhalb sind Anomalien und Vorhersage, die auf der Grundlage der vorherigen Werte der Signale die nächsten Werte vorhersagen.

Folie 15:

Nach Litteraturrecherche, habe ich 5 Methode ausgewählt, eine für die Vorhersage und vier für das Clustering. Unter diesen Methoden verwenden zwei neuronale Netze.

Folie 16:

Jeden Lernmodellen lernen das Normalverhalten des Prozesses. Es gibt 4 Normalverhalten, eins für den silbernen Topf und eins für den schwarzen Topf, eins für den Taster und eins für den Notaus Taster. Jeden Neuronen Netzwerk lernen über 10 Epochen.

Folie 17:

Wenn der Taster gedrückt wird, bewegt sich das Laufband nach links. Es erscheint also drei Signale, eines zeigt an, dass das Laufband gedrückt ist, ein zweites zeigt an, dass sich das Laufband bewegt, und ein drittes zeigt an, dass sich das Laufband nach links bewegt.

Folie 18:

Zehn Scalers werden verwendet, um zu bestimmen, welcher Scalers am besten geeignet ist, und für jede Methode die besten Ergebnisse erzielt wurden. Mit Scalers können Daten basierend auf ihren statistischen Parametern (Mittelwert, Minimal- / Maximalwerte, Varianz usw.) auf unterschiedliche Weise dargestellt werden.

Folie 19:

Es gibt verschiedene Arten von Angriffen. Einige sollen das ursprüngliche Verhalten des Prozesses ändern wie PLCinject und Profinet-Replay Angriff. Per PLCinjekt wird Schadcode auf die primäre SPS eingespielt. Durch einen Profinet-Replay-Angriff auf den Profinet-Buskoppler werden die Anweisungen der SPS ignoriert. Andere Angriffe ändern nichts daran. Unseren Lernmodellen sollen eine Anomalie detektieren wann es ein PLCinject oder Profinet-Replay Angriff gibt.

Folie 20:

Um die Lernmodellen zu evaluieren, gibt es vier Angriffen, drei Angriffen die das Verhalten verändert und ein Angriff die das Verhalten nicht verändert. Zwei Angriffe, die das Verhalten des Prozesses ändern, sind Rename Angriff und Replay Angriff. Durch den Rename Angriff wird die Kommunikation von der SPS zum Prozess blockiert.

Folie 21:

Replay Angriff stoppt alle Aktivitäten im Prozess und bewegt das Laufband nach links.

Folie 22:

Der letzte Angriff, der das Verhalten des Systems ändert, ist an sich kein wirklicher Angriff, da er nicht durch Injizieren eines Computerwurms oder durch Ändern eines Teils des Systems ausgeführt wurde. Es wurde ein Simulated Angriff genannt. Ich habe einen Lauf mit einem silbernen Topf und dann einen mit dem schwarzen Topf aufgenommen. Ich habe dann die Schranke-Signale zwischen den beiden Läufen ausgetauscht.

Folie 23:

Dieser Angriff ist der Safety Angriff. Damit soll verhindert werden, dass die Stromversorgung des Systems unterbrochen wird, wenn der Not-Aus-Taster gedrückt wird. Daher stoppt der Prozess nicht mehr, wenn die Not-Aus-Taste gedrückt wird, und läuft weiter, wenn ein Topf in den Prozess eingefügt wurde.

Folie 24:

Folie 25:

Für jede Methode wurden unterschiedliche Scalers verwendet, aber auch unterschiedliche Parameter. Für 1DCNN habe ich die Fenstergröße in Eingabe und den Schwellenwert geändert. Für Autoencoder habe ich die Schwellenwert und die Klassifizierungsmethode geändert. Der Punktklassifikator klassifiziert jeden Punktdaten. Fenster Classifier klassifiziert Fenster.

Für das SVM hat diese Arbeit den Parameter "nu" geändert, der eine Obergrenze für den Anteil der Trainingsfehler und eine Untergrenze für den Anteil der Unterstützungsvektoren darstellt.

Folie 26:

Für 1DCNN werden die besten Ergebnisse für den StandardScaler für ein Fenster der Größe 20 erzielt. Für die Autoencoder werden die besten Ergebnisse für MinMaxScaler und BooleanScaler erzielt.

Folie 27:

Für die clusterbasierten Methoden werden die besten Ergebnisse mit MinMaxScaler, Normalizer und No Scaler erzielt.

Folie 28:

Diese Tabelle zeig das beste Ergebnis für jede Methode zusammen. Wir stellen fest, dass DBSCAN uns den besten Wert für die Erkennung von Anomalien bietet.

Folie 29:

In dieser Masterarbeit konnte ich die Signale eines Prozesses erfassen, mit dem Objekte nach ihrer Beschaffenheit sortiert wurden. Mit diesen Signalen habe ich sie in zwei Datensätze unterteilt, einen Trainingsdatensatz und einen Testdatensatz. Die Datensätze wurden mit Scalern erstellt, um die Abhängigkeit von Lernmodellen von Scalern zu beobachten. 5 Methoden wurden verwendet: CNN, Autoencoder, SVM, LOF, DBSCAN. DBSCAN liefert uns die besten Ergebnisse.

Diese Ergebnisse könnten verbessert werden, indem die Anomalie auf jedem einzelnen Sensor erkannt wird oder indem bessere Methoden zur Schwellenwertauswahl angewendet werden. Zur Vorbereitung der Daten können andere Methoden als Scalern verwendet werden, z. B. PCA oder maschinelles Lernen.