Fishy Cyber Attack Detection in Industrial Control Systems

Zone-Based PCA and A new approach based on LSTM

Manikanta Reddy D.

IIT Kanpur

Table of contents

1. Introduction
2. Water Plant
3. Zone Division[1]
4. Principal Component Analysis Based Detection[3]
5. Install a Brain in the Plant.
6. Summary

Introduction

Industrial Control Systems

Industrial Control Systems (ICS) are connected to Internet for information exchange and control transfer.

This potentially exposes the critical system to various side channel attacks.

The Problem with ICS

Security Patches are rarely applied, as they could cause other critical failures.

Detect and Shutdown

In ICS the norm is to cure rather than to prevent the disease.

Detect the attack and *shutdown* the systems to prevent any damage.

Later fix the problem.

It is important to build a reliable manipulation detection system.

Water Plant

Hot Water Plant

We’ll emulate a simple hot water plant, to test our systems.

The plant consists of hot water circulating between two tanks.

One tank heats and the other lets it cool down.

A pump circulates the water

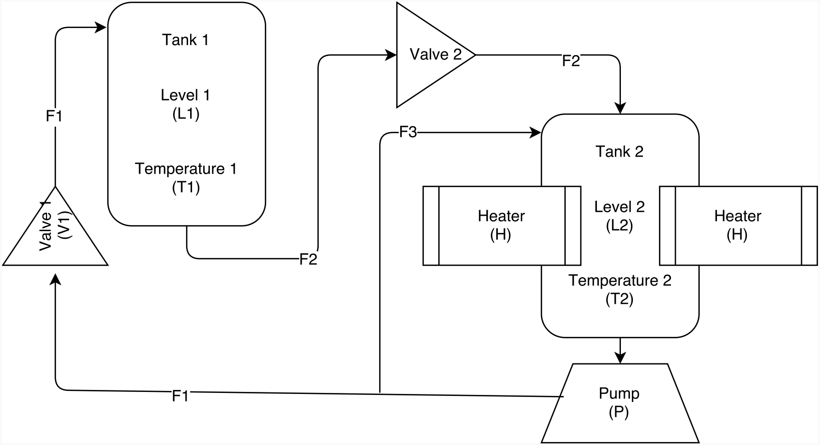


Figure 1: Hot Water Plant

Attack Detection

There are 11 process variables in the system.

Control Variables: V1, V2, P, H

Process Variables: L1, L2, T1, T2, F1, F2, F3

In reality there could be many more.

Impossible to monitor all of them concurrently for any manipulation.

Zone Division[1]

An attempt to minimize risk

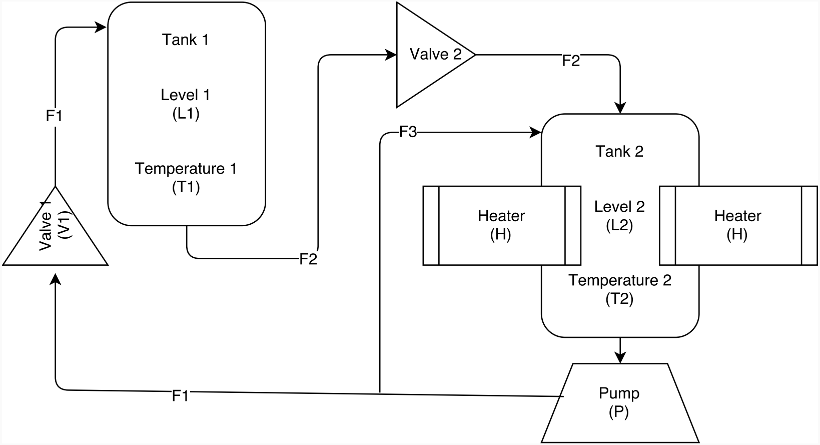
Divide the entire system into zones.

One zone is compromised, try to detect it in other zones.

Allow for cross control and prevent control of variables in the same zone.

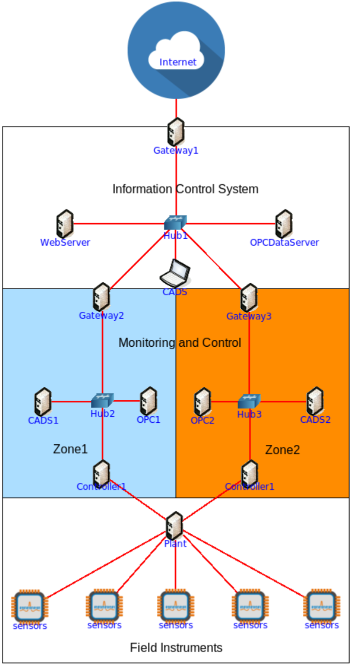
A controller in a zone is not allowed to manipulate the variables that change the variables it measures.

Zone Division



Zone1: L1, T1, V2, F2, H

Zone2: L2, T2, V1, F1, F3, P


Internet
Gateway1
Information Control System
WebServer
Hub1
OPCDataServer
CADS
Gateway2
Gateway3
Monitoring and Control
CADS1
Hub2
OPC1
OPC2
Hub3
CADS2
Zone1
Zone2
Controller1
Controller1
Plant
sensors
sensors
sensors
sensors
sensors
Field Instruments

Principal Component Analysis Based Detection[3]

The Problem

It is very difficult to monitor all process variables concurrently.

Attacker can also mask the incorrect readings from the compromised zone.

Good Luck with that.

Detect the Change

Instead detect only the change.

Device a method to extract the ones that change the most.

Monitor it and you are done.

This is exactly what PCA based method does.

PCA

Prinicipal component analysis reprojects the data into a new space along maximum variance.

Monitor values along these components and any change should be visible. (That too in a magnified fashion).

We have considered 3 PCA components to monitor.

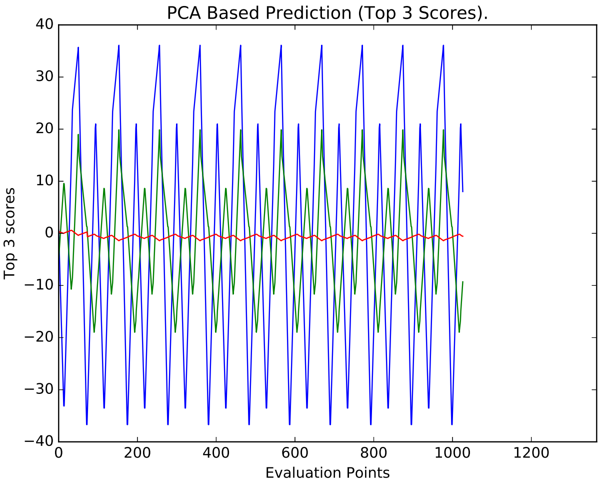


Figure 2: Normal Functioning of Plant (PCA Top 3 scores (Blue, Green, Red))

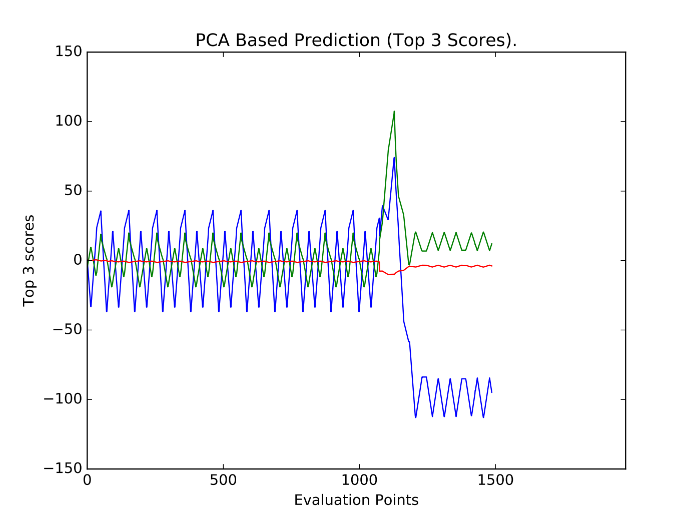


Figure 3: PCA Top 3 Scores, plant compromised around evaluation point 1000

Notice how humorously the values in blue change.

Any on-site observer can notice it and shutdown the system.

Install a Brain in the Plant.

Revisiting the Problem

What makes *an attack*, **an attack**?

Anomaly!

Any anomalous behavior is bad for us.

Anything bad ⇒ Shutdown the system

Can we *LEARN* what the normal working is?

Neural Networks

Neural networks are extremely good at learning things, after-all they are modeled after neurons!

They can *learn* anything from recognizing objects to repetitive patterns.

We'll be using a specific kind of an architecture, which currently excels at memorizing behaviors.

Long Short Term Memory (LSTM)[2]

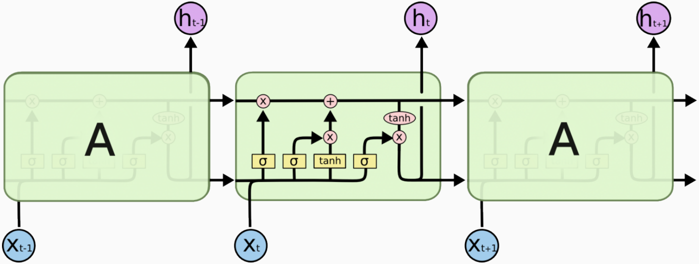


Figure 4: Long Short Term Memory (LSTM) Units in action. Img: colah

LSTM is form of Recurrent Neural Network, it remembers what’s important and forgets the trivial things.

LSTM is capable of learning patterns in data and rejecting those that don’t match.

Anomaly rejection!

LSTM Training

Before we use the brains, we need to teach them how our system works.

We log the data (Process Variables) for sufficiently long period of normal working and *train* the LSTM block accordingly.

The output of the LSTM block is a confidence score evaluating to how close the current pattern is to regular working conditions.

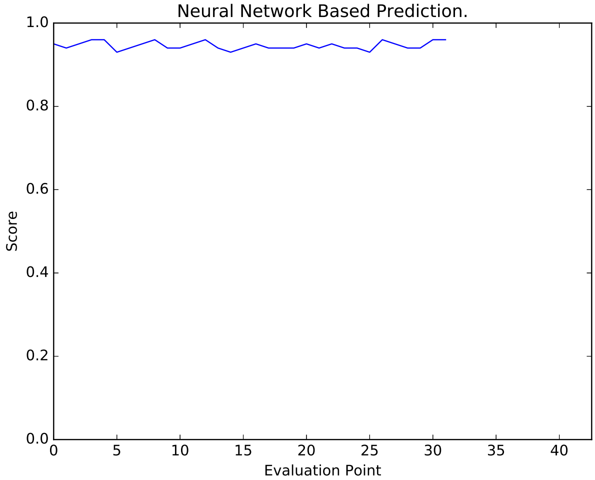


Figure 5: Normal Functioning of Plant (LSTM Confidence)

Notice the high levels of confidence (~1)

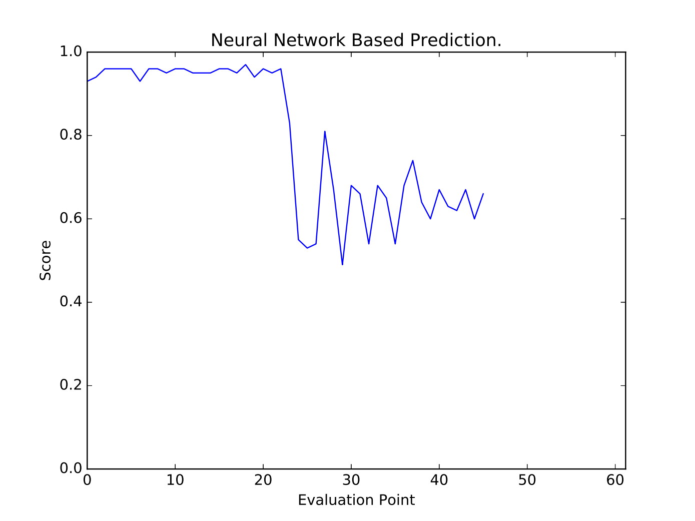


Figure 6: LSTM Confidence Scores, plant compromised around evaluation point 20

Notice how significantly the confidence drops (~40% reduction!)

Automation

LSTM based prediction paves way for an automated protocol in the event of an attack. (Difficult with PCA based method)

As the regular working confidence is close to 1 any confidence value less than, say 0.8, might be considered as an attack.

Further cases could be split on what action should be taken based on the confidence.

Summary

Summary

We discussed how security aspects are handled in ICS.

Zone division helps in minimizing damage, but yet needs to piggy back on a detection system.

PCA based method is great in monitoring highly variable values when attacked.

LSTM can learn to detect any anomaly and empower us with an automated damage control system.

References

Y. Hashimoto, T. Toyoshima, S. Yogo, M. Koike, T. Hamaguchi, S. Jing, and I. Koshijima.
Safety securing approach against cyber-attacks for process control system.
Computers & Chemical Engineering, 57:181–186, 2013.

S. Hochreiter and J. Schmidhuber.
Long short-term memory.
Neural computation, 9(8):1735–1780, 1997.

T. Morita, S. Yogo, M. Koike, T. Hamaguchi, S. Jung, I. Koshijima, and Y. Hashimoto.
Detection of cyber-attacks with zone dividing and pca.
Procedia Computer Science, 22:727–736, 2013.

Code Repository for the project

Thank You