Yu-jun Xiao, Wen-yuan Xu, Zhen-hua Jia, Zhuo-ran Ma, Dong-lian Qi, 2017. NIPAD: a non-invasive power-based anomaly detection scheme for programmable logic controllers. *Frontiers of Information Technology & Electronic Engineering*, **18**(4): 519-534. http://dx.doi.org/10.1631/FITEE.1601540

NIPAD: a non-invasive power-based anomaly detection scheme for programmable logic controllers

Key words: Industrial control system; Programmable logic controller; Side-channel; Anomaly detection; Long short-term memory neural networks

Corresponding author: Wen-yuan XU
E-mail: xuwenyuan@gmail.com
ORCID: http:// orcid.org/0000-0002-2428-973X

Motivation

- Industrial control systems (ICSs) are widely used in critical infrastructures, which make them popular targets for attacks causing catastrophic physical damage.
- The programmable logic controller (PLC) controls the actuators directly, thus plays a vital role in ICSs. A PLC executing a malicious program can cause significant property loss or even casualties.
- PLCs cannot be protected by traditional intrusion detection systems or antivirus software.
- An effective method for PLC protection which is non-invasive to ICSs is yet to be designed.

Main idea

- PLCs execute a program in a cycle-scanning manner. The CPU power consumption of a PLC varies and is determined by the executing programs.
- PLCs tend to execute a predefined sequence of instructions within a period of time, and the sequence will not be modified frequently.
- Most PLCs have a separate AC-DC converter, and thus we can measure the power consumption at the DC power supply without modifying the hardware or software.
- We can detect malicious software execution in a PLC through analyzing its power consumption.

Method

1. We insert a current shunt resistor between CPU module and power supply (PS) module of a PLC to measure its power consumption.
2. We first choose the statistical histogram, basic time-domain features, and frequency- domain features of a power trace as our original features. And then use sparse coding algorithm to select a set of discriminative features.
3. We train a long short-term memory (LSTM) neural network with the features of normal samples to predict the next time step of a normal sample, and an abnormal sample is identified through comparing the predicted sample and the actual sample.

Major results

- As the monitoring time goes on, the FRR of LSTM increases slightly, but is always less than 0.95%.

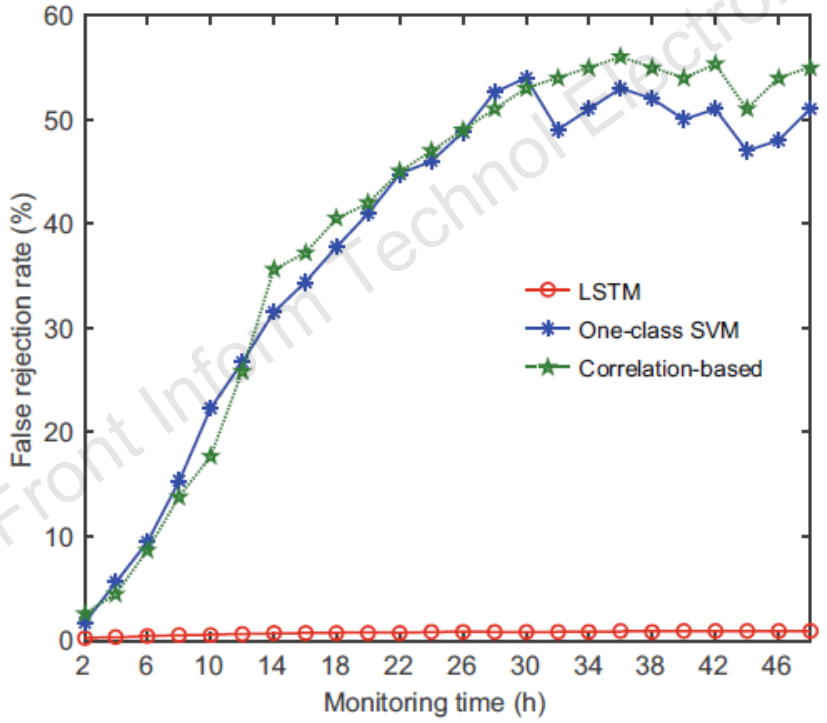

Fig. 7 Performance of continuous monitoring with time. It illustrates the change of the false rejection rate (FRR)

Major results

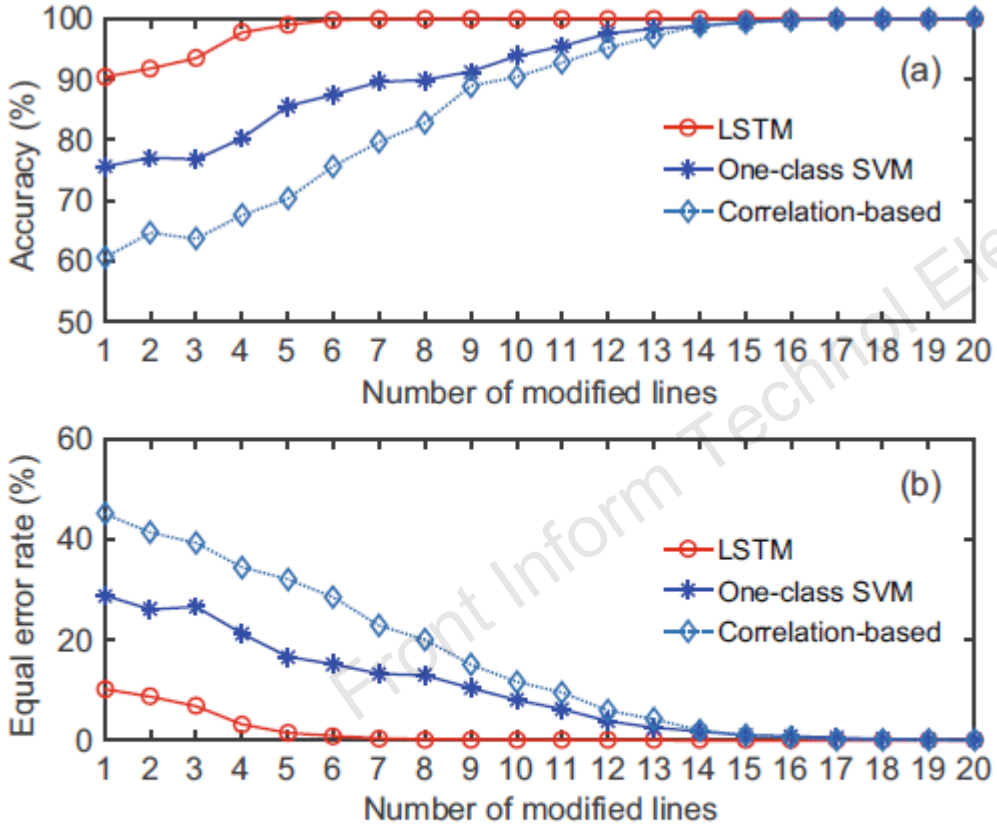

Fig. 9 Detection sensitivity of different anomaly detection algorithms: (a) detection accuracy at different numbers of modified lines; (b) equal error rate (EER) at different numbers of modified lines

- As we increase the number of modified lines, the detection performance improves.
- When the change of program size reaches 0.44%, LSTM is able to detect an abnormality with an accuracy of above 97.56%.

Major results

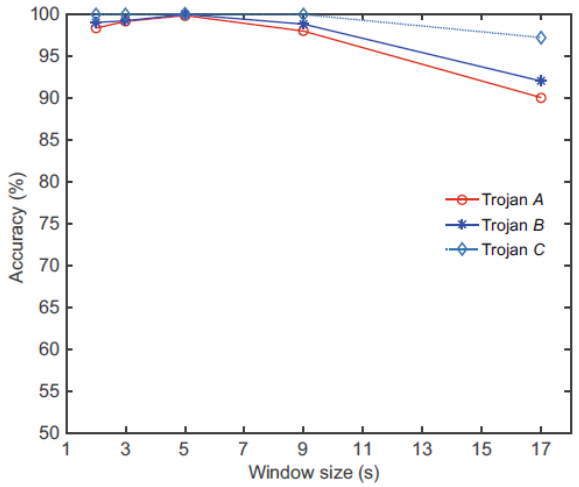

Fig. 10 Detection accuracy under different window sizes. The trojan programs are the three attacks mentioned in the text

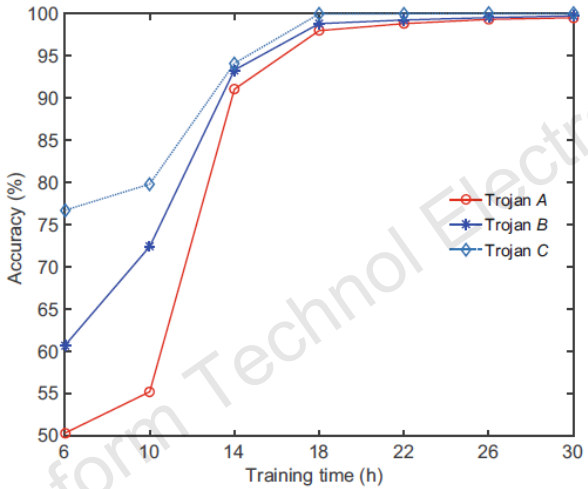

Fig. 11 Detection accuracy with different training times. The trojan programs are the three attacks mentioned in the text

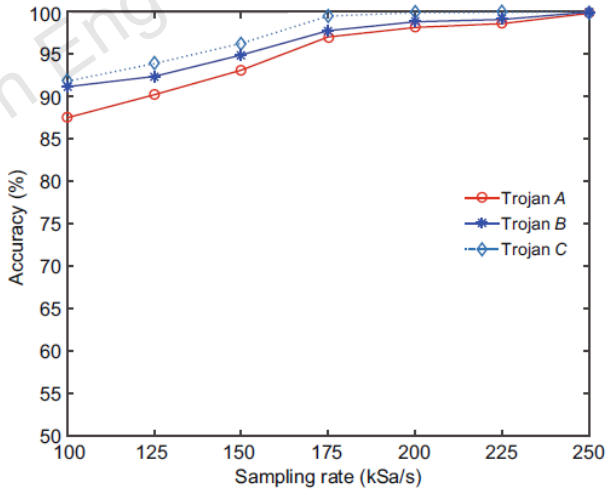

Fig. 12 Detection accuracy under different sampling rates. The trojan programs are the three attacks mentioned in the text

- The performance of LSTM depends greatly on the window size, training time, and sampling rate.

Conclusions

- we have proposed a non-invasive power-based anomaly detection scheme for detecting attacks on PLCs.
- We have detected the attacks which we implement with an accuracy as high as 99.83% in our lab experiments.
- We discussed the detection sensitivity of our method. Even when the modification of the original program is as little as 0.07%, we are able to detect the change with an accuracy of 90.33%.
- We are able to detect unknown attacks without abnormal samples.