Ben-Gurion University of the Negev

Faculty of Engineering Science

Department of Software and Information Systems Engineering

Project in Offensive Artificial Intelligence Course

OAI Final Project - Robustness of Real Time Deepfakes

Author:
Amit Kama

Author:
Oren Shvartzman

June 11, 2022

Contents

1 Introduction

2 Methods

Given the growing need for IDS and IPS for securing ICS, there is a growing need to create quality datasets for training and evaluating anomaly detection models. This includes setting up testbeds, collecting data from them, and usually simulating data to provide anomalies. In this section we present the main datasets developed for the purpose of training and evaluating such models in the ICS domain.

3 Experiment and Results

Below is a comparison table between the abovementioned ICS datasets. The purpose of the table is to be a decision support tool in selecting a suitable dataset for conducting anomalies detection studies in the ICS field. Note that only BATADAL dataset does not cointain the class labels for the test set.

4 Discussion

Today, ICS are an integral part of the day-to-day operations of many industries and critical infrastructures, from power generation, through water treatment, and to oil and gas processing. Cyber attacks against ICS would lead to disruption to controlling those critical infrastructures and result in harmful physical damage to plants, environment and humans. According to ICS-CERT, the ICS-targeted attacks are continuously increasing from year to year [1].

References

[1] Cheng Feng, Tingting Li, and Deeph Chana. Multi-level anomaly detection in industrial control systems via package signatures and LSTM networks. In *47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2017, Denver, CO, USA, June 26-29, 2017*, pages 261–272. IEEE Computer Society, 2017.