Early Anomaly Detection for Securing IoT in Industrial Automation (ELLIOTT)

Shreevanth K. Gopalakrishnan
Dr. Nilufer Tuptuk
Prof. Stephen Hailes
University College London

INTRODUCTION

The ELLIOTT project investigates the detection of abnormal changes in IoT-based industrial control and automation systems (ICS). Attacks on these systems, often masked by natural disturbances and faults, could cause physical impact on vital industrial systems and even harm humans. Therefore, early anomaly detection can help detect attacks and enable countermeasures before serious consequences.

AIM

This research seeks to develop and/or identify the most effective and efficient methods from amongst "off-the-shelf" outlier detection tools, classical machine learning, and deep learning for anomaly detection in ICS. Building Management Systems (BMS), which were found to be the most targeted and highly susceptible to cyber-attacks, were selected as the use case for exploration.

WHY

IoT, Edge computing and wireless technology have resulted in networked ICS with increased sensing capacity, remote access, and ease of reconfiguration. The downside is that there are new, highly potent cyber-attack vectors attracting capable adversaries. This work is of importance as modern BMS systems are deployed within environment-sensitive infrastructures such as hospitals, data centres, etc., and there is a general lack of practical cyber-security expertise here.

METHODOLOGY

The ELLIOTT project is being carried out using a four-step methodology:

1. Selection of relevant ICS scenarios with industry partners.
2. Design and assembly of testbed and co-simulation environment.
3. Testing of "off-the-shelf" anomaly detection models against manual attacks.
4. Development of novel anomaly detection models and testing with adversarial AI-generated attacks.

EXPECTED IMPACT

Firstly, this research seeks to build models and a testbed which can generate reproducible results allowing benchmarking within the BMS community. Secondly, it seeks to construct more ICS-specific anomaly detection metrics which account for the latency and accuracy of detection.

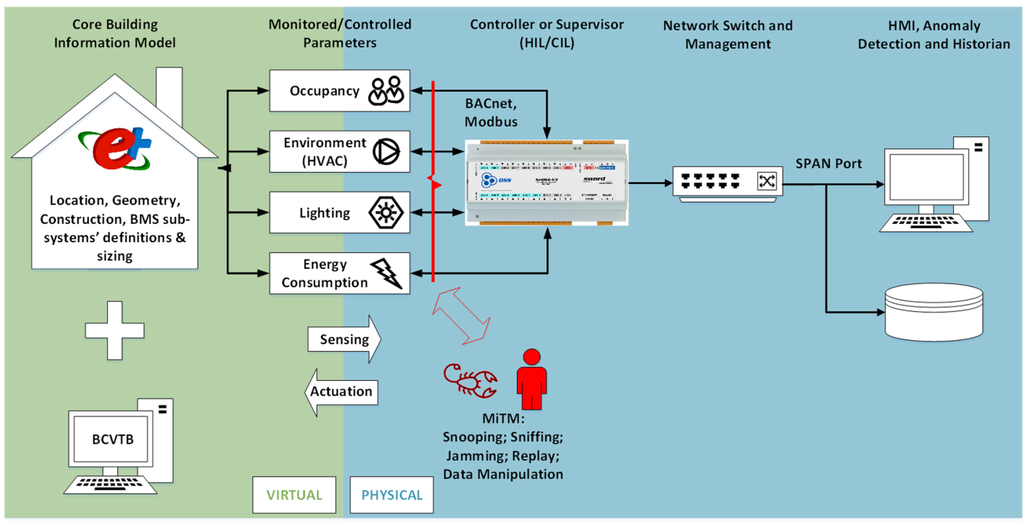

Figure 1: Hardware-in-the-loop simulation environment

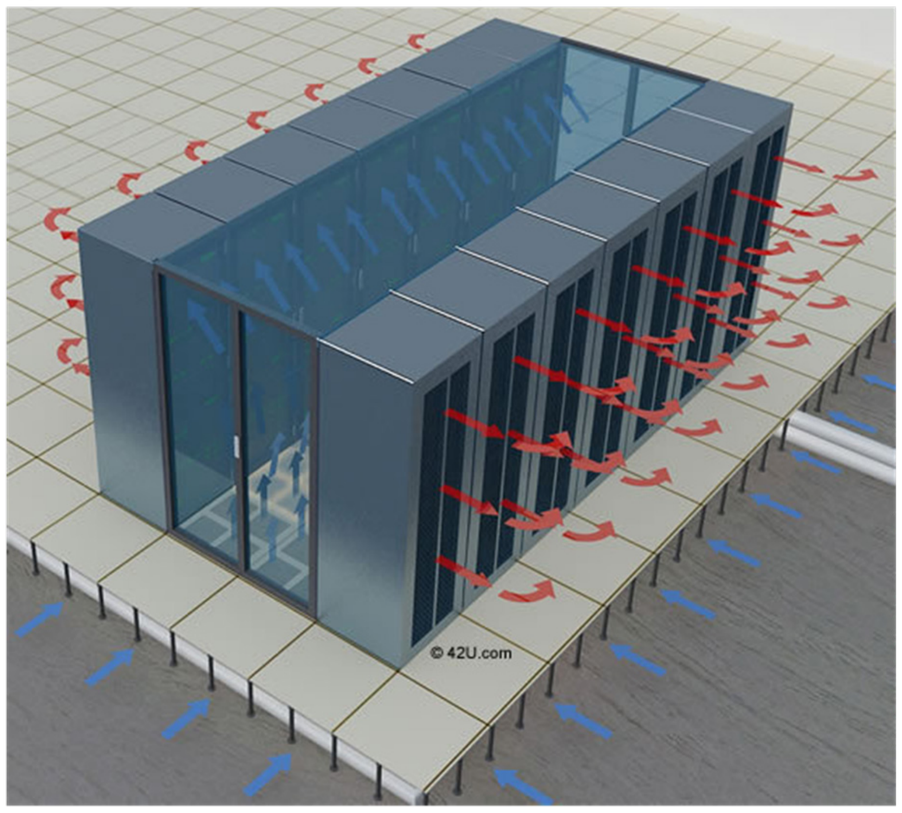

Figure 2: Computer Room Air Conditioning (CRAC) unit

KEY OUTCOMES

The project aims to develop an industry standard hybrid testbed and accompanying datasets to enable modelling and experimentation with a BMS's core sub-systems from a cyber-security perspective. Further, any new anomaly detection models and attack generation techniques developed will also be made open source.

MAJOR FINDINGS

Our co-simulation environment and updated defence metrics are allowing us to build and evaluate anomaly detection models for a variety of BMS scenarios. With increasing sophistication of preventative defence measures (asset management, end-to-end encryption, etc.) and attack techniques, behavioural anomaly detection will be the last line of defence for the ICS.

USER PARTNERS

Cube Controls, Rockwell Automation.

ACKNOWLEDGEMENTS

This work has been supported by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which has been funded by the UK EPSRC under grant number EP/S035362/1.

PROJECT TIMELINE

Start date: 01/02/2020
Finish date: 31/01/2023

PETRAS
UK Research and Innovation
UCL