**Control Logic Based Cyber Attacks in Industrial Control Systems**

**Laurence Browne**

**Supervised by: Dr. Sridhar Adepu**

**Abstract:**

Cyber Physical Systems (CPS) use a cyber supervisory system to monitor sensors and control actuators in order to interact with the physical world. Smart devices and the Internet of Things (IoT) mean CPS are common in everyday life, from home automation to Critical National Infrastructure (CNI). As such, understanding the threats posed to these system by emerging technologies is a key area of research for both the public, private and defence sectors.

This paper illustrates the application of machine learning techniques to passively model the dependencies and relationships within a typical CPS and use these to form the beliefs of an intelligent agent. The intelligent agent probes the system to verify these beliefs then pushes the system beyond it’s normal operational parameters- a cyber-attack.

Data from the Secure Water Treatment Testbed (SWaT) was used as these are present in the majority of industrial process.

A physics-informed intelligent agent was used which could identify components by their characteristics. A Classification Neural Network was trained on normal and attack data, this anomaly detector is a common Intrusion Detection System (IDS) and used to provide feedback to the intelligent agent.

The agent was tested against simulations of the SWaT using traditional and deep learning models.

It can be seen that even basic statistical tools give a reasonable approximation of an unknown systems and would be sufficient to draft simple attacks.

More advanced methods which model temporal relationships were combined to produce a tool which was highly effective in generating simple cyber-attacks and facilitating more complex, human in the loop attacks. This tool is system agnostic so applicable to other CPS system without a need to modify its parameters.

ABSTRACT SHOULD BE AROUND HALF A PAGE IN LENGTH OR MORE

>

**Ethics statement:**

This project does not require ethics approval, as reviewed by my supervisorDr. Sridhar Adepu.

I have completed the ethics test on Blackboard. My score is 12/12.

**Project plan:**

The iTrust Centre for Cyber Security operates a Secure Water Treatment Testbed (SWaT) which is used to “support research into the design of secure, public infrastructure” [1]. SWaT is a Cyber Physical System (CPS) so consists of the physical side which implements a process and a cyber side which performs control, monitoring and security [2].

The testbed produces clean water by using both Ultra Filtration and Reverse Osmosis which is implemented through a six stage, distributed control system.

Each stage is managed by a Programmable Logic Controller (PLC) which applies pre-programmed logic to switches and actuators based on the input signals ( sensor readings) or control messages from other PLCs. This logic is in the form of ‘Ladder’ diagrams which are a graphical programming language derived from electrical switch schematics [3].

The effect is that the PLC is a standalone micro-controller which is able to control one stage of an industrial process autonomously.

A CPS will consist of multiple stages, each performing a distinct process and controlled by it’s own PLC. These PLC’s communicate with each other in order to pass or request data pertinent to their own stage of the process e.g. request a faster flow of water or indicate a batch is ready to move to the next stage.

The internal logic (rules) of the PLCs are designed to account for all possible system states and includes parameters such as maximum temperatures, pressures and flow rates [1]. Should a stage of the system move outside of these parameters the PLC will take appropriate action and raise an alert.

A cyber vulnerability methodology was used to identify vulnerabilities suitable for machine learning techniques to be applied to [4]. Here we don’t assume full ‘insider’ level of access- where the attacker can manipulate the rules and logic programmed into the PLC’s.

It is assumed instead that only access to the signals between PLCs are available. The TCP/IP packets which carry the control and monitoring messages are first analysed in order to passively model normal system function- identifying the rules within the PLCs as these are the parameters which dictate normal operation.

The modelling is accomplished using the normal operation data from the SWaT dataset as a proxy for the live sampling of the system. Applying unsupervised techniques such as clustering, correlation coefficients and mutual information will suggest similar or interrelated components/ stages.

The SWaT is a deterministic system as all system states are entirely predicted by the state of the other components, though it is possible to use a probabilistic approach to the interaction of components, temporal analysis is more appropriate to model the causality.

The data may exhibit seasonality due to demand patterns in output stage which could identify distinct modes of operation such as high demand/ refill stage. Auto correlation of features, the correlation of a random variable with a lagged version of itself, is a common approach- methods such as “Autoregressive Integrated Moving Average (ARIMA) and Exponential Smoothing (ES) … are widely used due to their simplicity and interpretability” [4].

Extending this auto-correlation to the multivariate dataset and recording if a time lag produces stronger correlations will be used to illustrate dependencies between components- such as a water level lagging the flow in its feed pipe.

Fourier analysis, “… a decomposition of the series into a sum of sinusoidal components” [5] will be used to achieve the same aim. By considering the whole data set as complex waveforms, the fundamental frequencies and harmonics can be found for each component. Components which exhibit similar fundamentals with a consistent phase difference are likely to be functionally dependent.

The model of the system which results from this passive analysis will be used as the initial beliefs of an intelligent agent which will test and update its beliefs by probing models of the SWaT which will be implemented using traditional and deep learning methods.

In a real-world application the agent will interact with the system by ‘spoofing’ the control packets sent between PLCs. Using the Man-On-The-Side (MOTS) attack methodology it seeks to inject a packet into the communication channel just before the real value is sent. The control system accepts this first packet and rejects the subsequent, real packet as a duplicate. For the purpose of validating the methods the agent will craft values to act as input to the ML model and compare the models output to it’s own predictions.

The SWaT is a competitive, multi-agent environment because the control system is trying to maintain a system state the attack agent is trying to disrupt [7]. It is assumed that the agent is able to spoof multiple packets in a single system cycle in order to suppress the effect of PLCs in other stages counteracting the attack (and so control all input values in the case of the simulation models).

To constrain the agent from choosing values which would be impossible/ unusual in the real-world system, classifier based on a Recurrent Neural Network (RNN) will be trained on the normal and attack datasets. This acts as an anomaly detector and provides feedback to the agent, improving its ability to choose the rate at which it affects system values and so avoid detection. Anomaly detectors, often Support Vector Machine or Deep Neural Networks, are common in CPS as they act as Intrusion Detection Systems [2]. These anomaly detectors may reside on the SCADA system or possibly on a stand-alone processor at PLC level [2]- an example of edge computing.

The intelligent agent is a simple physics-informed model whereby it includes heuristics for common industrial components, for example a swich is likely to have two discrete states whereas a sensor is likely to have a fixed range of values and, due to the need for digitized data, a fixed step size. The heuristic will also include temporal relationships- a switch event is likely to precede a change in another components state.

The agent will be able to create a network diagram of all components, their interactions and normal operating parameters which it has found by testing system limits. Simply passing these limits or increasing the duty cycle of components ( rapid switching etc.) constitute common cyber attack methods. The explainable, in depth knowledge of a previously unknown system would facilitate complex attack when there is a human in the loop.

MAX TWO PAGES >

**References:**

< A list of all the literature sources cited in your literature survey, **consistently**formatted in a commonly-used style (such as APA or IEEE), and with each item in the References being **complete**, i.e. as you would format it in your final submitted thesis, with author names, publication year, publication venue (conference or journal name), page numbers, DOI, etc.

References do not count towards your total page count

>

**Appendix: Project Timeline**

**<** one-page time-plan for your project, which you may choose to format as a week-by-week bullet-list, or possibly as a Gantt Chart

MAX ONE PAGE

>

**Appendix: Risk Assessment**

< one-page risk assessment for your project, talking about the major risks you can foresee that might plausibly occur and interfere with your plans. For each risk, state clearly what it is, what its likelihood is, what its effects/impact would be on the project, and what your intended mitigation or risk-reduction involves.

MAX ONE PAGE

>