An intelligent agent views it’s world through percepts and affects it through it’s choice of actions. “The agent function maps given percept sequence to an action” (Norvig, 2022) and is an abstract mathematical model of the agents behaviors. The actions are decided by the agent program.

It would be possible to produce attack data through a deep learning, neural network but this would not be able to choose the most appropriate attack for the current system condition.

The aim of the agent is to learn the system passively, refine this knowledge by probing it ( information gathering via packet injection) then use it’s inbuilt knowledge of attack types to choose how to manipulate the system.

Industrial systems share common components and common failure modes, this knowledge will be incorporated as heuristics. The agent will try to map observed behavior to a known component type then prepare an attack against it.

An example would be identifying a water level sensor and the switch, pump and valve responsible for maintaining it’s level. An attack could try to manipulate the associated devices in order move the level beyond it’s highest known value. Reaction to this attack should also be recorded and incorporated into the model.

The agent will make rational decisions based on it’s knowledge of the system, if the consequence of this decision supports it understanding then this is a positive performance measure.

To make the agent more appropriate a penalty is given for the amount of noise on the system- the number of packets required to attain the effect. A noisy attack is more likely to be spotted by anomaly detectors.

The aim is that the agent is not reliant on it’s prior knowledge and has some degree of autonomy. This may be altering relationship gradients etc.

**Does gradient based attacks dictate the step size?**

**Pseudo Code…** Chapter 15 on decisions

The task environment is defined by the Performance, Environment, Actuators and Sensors description (PEAS).

|  |  |  |  |
| --- | --- | --- | --- |
| **Performance** | **Environment** | **Actuators** | **Sensors** |
| Attack Types for real world effects: | Intrusion detection | Find out which have effect directly | Findout which can be spoofed to cause effect |
| False alarms  Accelerated wear  Over level/ pressure/ temp etc. | Scada counteracting actions |  |  |

It is assumed that the task environment is partially observable due to the insider level of access but demands on the system ( clean water output) are unknown(?).

unknown in regards to the behaviour and relationship of component. Physical laws will be included. As such the system is deterministic, sequential and dynamic.

It is continuous-state both and continuous time,

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.