SAND2022-9058C

MLDL

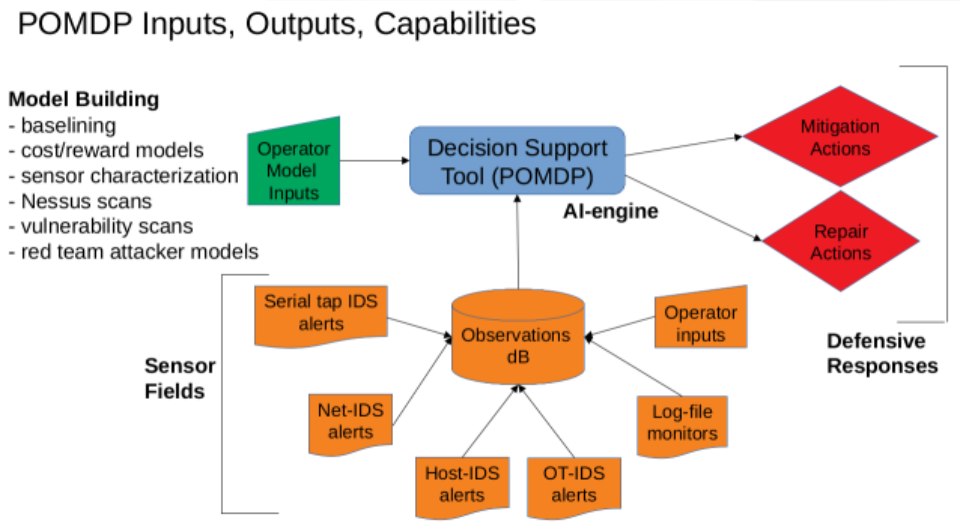
Machine Learning and Deep Learning Conference 2022

POMDP Modeling for Cyber-Defense of Industrial Control Systems

Robert G. Cole (x05823)

T. Bailey, D. Cardona, A. Fahey, A. Gonzales, D. Jose, A. Outkin, J. Robinson, C. Sturgill and S. Walsh

Funding Source (SPP)



Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Unclassified Unlimited Release

Abstract

The DoD's mission success depends critically upon the performance of numerous Supervisory Control and Data Acquisition (SCADA) / Industrial Control Systems (ICS). SCADA/ICS systems are known to be under constant malicious cyber attack by nation state actors. It is absolutely critical that we provide effective and extensive protection. However, the nation suffers from a lack of trained and experienced cyber defenders. One mitigation is the development of Decision Support Systems (DSS) to advise novice cyber defenders as to the optimal actions to perform to maximize the protection of the SCADA/ICS systems for which they are responsible.

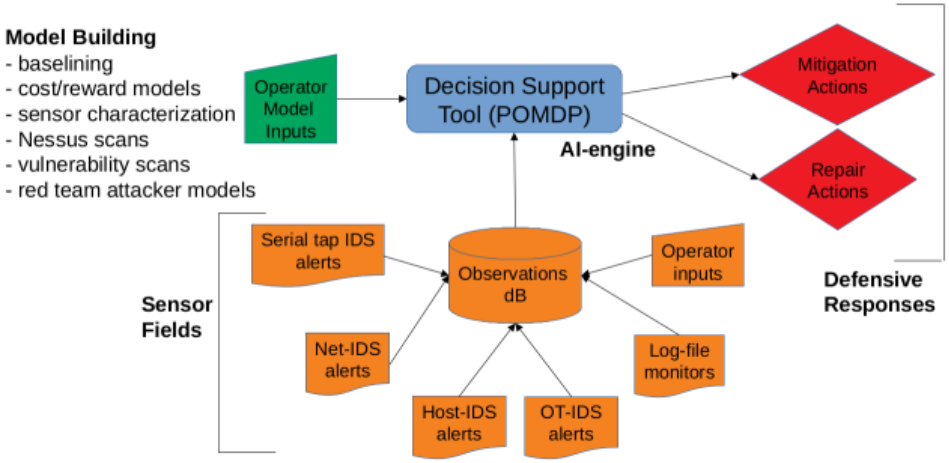
We are developing a DSS for cyber defenders of SCADA/ICS systems. The core of our DSS development is a Partial Observable Markov Decision Process (POMDP) model of the SCADA/ICS. The POMDP model is comprised of threat actor attack models, system security states, cyber activity sensor observations, operator actions and a utility based reward structure. We are developing an extensive emulation model of an exemplar DoD-based SCADA/ICS environment. The emulation modeling is based upon the SCEPTRE emulation environment. The sensor environment is provided by Security Onion and Elasticsearch. Our attack execution is provided by attack scripts using the Cobalt Strike commercial platform. This platform is providing the test framework for the effectiveness of our DSS development.

In addition, we describe the complexity of the POMDP model development, our work on developing an AI Expert System Shell which hides the AI parts of the DSS and collects only local domain expertise from the operators, our efforts on designing a hybrid Human/Machine 'Centaur' system and the capabilities of our emulation SCADA/ICS test bed and associated attack scripting.

Problem you are trying to solve

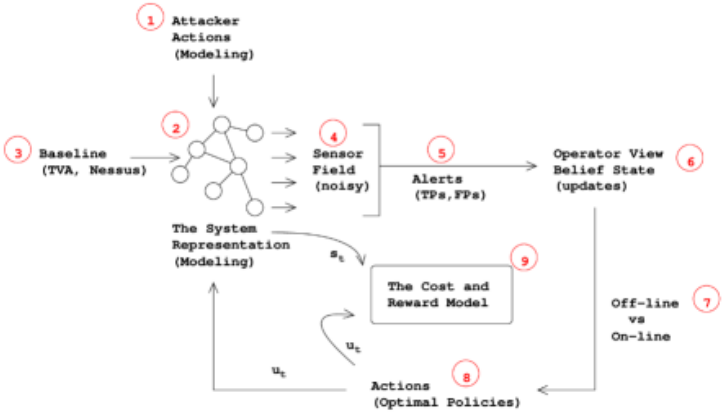
To Design, Develop and Test a Decision Support System (DSS) to support novice cyber defenders of the nation's critical SCADA/ICS infrastructure. The DSS must be:

- Effective in the defense of SCADA/ICS environments,
- Contain an AI Expert System Shell, which hides the AI parts and collects only the useful domain expertise,
- Intuitive and easily described,
- Scalable and
- Well tested and validated.

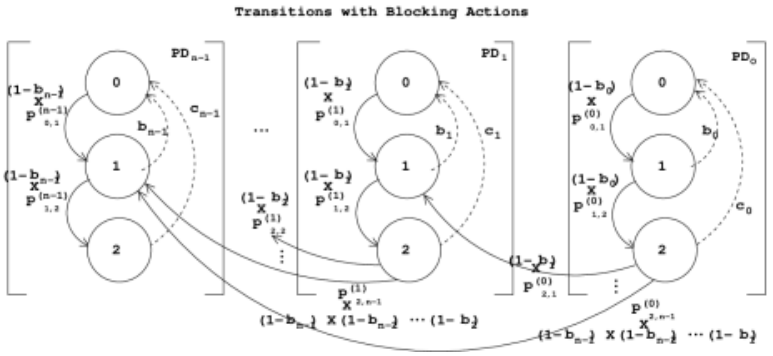


Algorithmic approach of your solution

- We have chosen to implement our DSS based upon a Partially Observable Markov Decision Process (POMDP) models.
- The models comprising the brains of the DSS will be based upon Domain Expertise and will 'hit the ground running'.
- The POMDP models comprising the DSS will not require vast data sets for Deep Machine Learning.
  - Large data sets from SCADA/ICS and malicious attacks are extremely hard to obtain.
- The POMDP models comprising the DSS will not require learning optimal policies through extensive trial and error.
  - In these environments trials cannot be performed on actual systems.
  - On emulation models trials are extremely time consuming.



POMDP Components

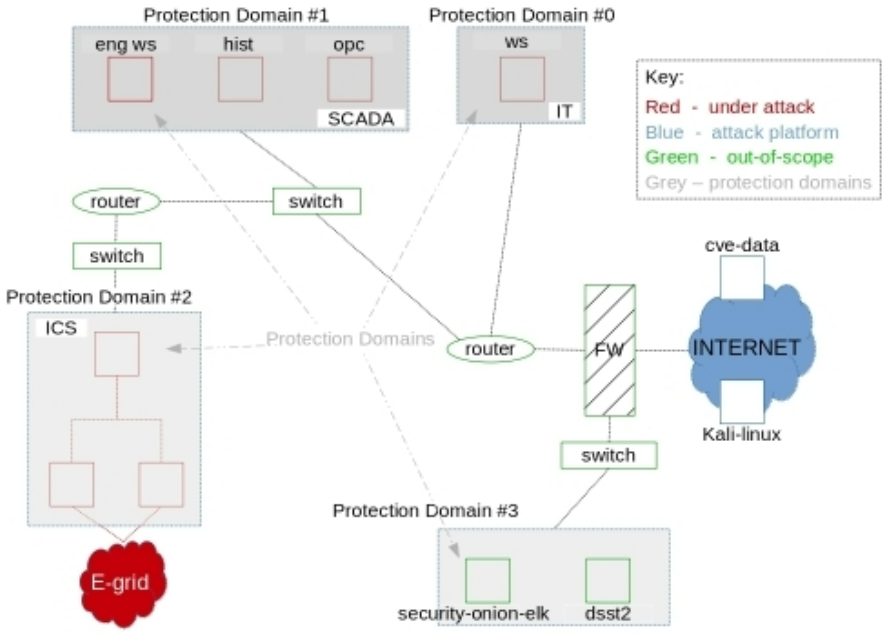


The BASICS POMDP Logic Model

Description of the data used

No data. Just Experimentation, Test and Evaluation.

- Our approach does not require the extensive data sets for training as with Machine Learning and Deep Learning.
- Our approach does not require the extensive trial and error (exploration and exploitation) learning as with Reinforcement Learning.
- Instead, we use domain expertise to develop our POMDP models and then extensively test them out on high fidelity emulation models of SCADA/ICS systems.
- We are using SCEPTRE to emulate SCADA/ICS environments and CobaltStrike for cyber attack scripting and we plan on running live Red Team attacks against our systems in the future.
- We are looking towards on-site testing on live ICS facilities (at first, decision support only) in the near future.



SCEPTRE Emulation Modeling of Industrial Control Systems.

Results

We are extending the operational domains of Partial Observable Markov Decision Processes (an Artificial Intelligence) to cyber defense of Industrial Control Systems and experimenting, testing and evaluating their performance in high fidelity emulated systems which we have developed.

We are developing a Decision Support System for cyber defenders of Industrial Control Systems based upon the highest level (i.e. Type 4) of Artificial Intelligence.

Conclusions

All Artificial Intelligence (AI) is not covered within ML, DL, and RL; we believe there is a role for Partial Observable Markov Decision Processes (POMDPs) in application to cyber defense of ICS.

We believe that POMDPs offer a attractive alternative to develop Decision Support Systems for the cyber defense of critical ICS which do not require large data sets and which offer a path to explain-ability of its actions.