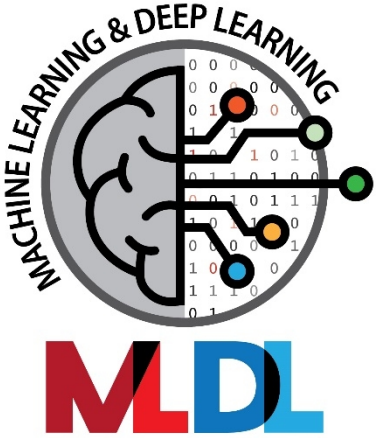
SAND2021-8256C



MLDL

Machine Learning and Deep Learning Conference 2021

Cyber Decision Support System for Industrial Control Systems

Robert Cole/SNL-NM, Dept. 05682

Team: Tyson Bailey, Logan Carpenter, Robert Cole, Jerry Cruz, Scottie-Beth Fleming, Trevor Hutchins, Deepu Jose, Ahmad Jrad, Nicole Murchison, Megan Nyre-Yu, Sasha Outkin, Meghan Sahakian and Tu-Thach Quach

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

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.

Abstract

The majority of Industrial Control Systems (ICS) lack experienced Cyber-staff to provide the necessary level of protection to defend against today's Cyber-threat. The development of effective Cyber-Decision Support Systems (CDSSs) would help in closing this gap.

We are investigating the development of CDSSs for protection of critical ICS environments. We are entering the third phase of our investigations. Our studies explore the application of Partial Observable Markov Decision Processes (POMDPs) as the Artificial Intelligence – Engine (AI-Engine) within our CDSS. We are in the process of experimenting within a SCEPTRE Emulytics™ model of a representative electrical grid facility. We have an initial prototype of the CDSS deployed within the SCEPTRE ICS model.

Active areas of investigation include:

- Improved/simplified Cyber-ICS model development with automation and operator inputs, covering attack, system, actions and reward models,
- Resilience of the CDSS against modeling and state estimation errors,
- Incorporation of dynamic learning capabilities,
- Additional Use Case studies in different ICS environments and
- (LDRD proposal) Human Factors Studies of functional allocation in a joint human/machine Centaur system for guidance in future CDSS capabilities development.

We are in the initial and early application and development of this technology. It is an exciting adventure and we look forward to improving the security posture of our Nation's critical ICS infrastructure in the process.

Abstract

The majority of Industrial Control Systems (ICS) **lack experienced Cyber-staff** to provide the necessary level of protection to defend against today's Cyber-threat. The development of effective Cyber-Decision Support Systems (CDSSs) would help in closing this gap.

We are investigating the development of CDSSs for protection of critical ICS environments. We are entering the third phase of our investigations. Our studies explore the application of Partial Observable Markov Decision Processes (POMDPs) as the Artificial Intelligence – Engine (AI-Engine) within our CDSS. We are in the process of experimenting within a SCEPTRE Emulytics™ model of a representative electrical grid facility. We have an initial prototype of the CDSS deployed within the SCEPTRE ICS model.

Active areas of investigation include:

- Improved/simplified Cyber-ICS model development with automation and operator inputs, covering attack, system, actions and reward models,
- Resilience of the CDSS against modeling and state estimation errors,
- Incorporation of dynamic learning capabilities,
- Additional Use Case studies in different ICS environments and
- (LDRD proposal) Human Factors Studies of functional allocation in a joint human/machine Centaur system for guidance in future CDSS capabilities development.

We are in the initial and early application and development of this technology. It is an exciting adventure and we look forward to improving the security posture of our Nation's critical ICS infrastructure in the process.

Abstract

The majority of Industrial Control Systems (ICS) lack experienced Cyber-staff to provide the necessary level of protection to defend against today's Cyber-threat. The development of effective **Cyber-Decision Support Systems** (CDSSs) would help in closing this gap.

We are investigating the development of CDSSs for protection of critical ICS environments. We are entering the third phase of our investigations. Our studies explore the application of Partial Observable Markov Decision Processes (POMDPs) as the Artificial Intelligence – Engine (AI-Engine) within our CDSS. We are in the process of experimenting within a SCEPTRE Emulytics™ model of a representative electrical grid facility. We have an initial prototype of the CDSS deployed within the SCEPTRE ICS model.

Active areas of investigation include:

- Improved/simplified Cyber-ICS model development with automation and operator inputs, covering attack, system, actions and reward models,
- Resilience of the CDSS against modeling and state estimation errors,
- Incorporation of dynamic learning capabilities,
- Additional Use Case studies in different ICS environments and
- (LDRD proposal) Human Factors Studies of functional allocation in a joint human/machine Centaur system for guidance in future CDSS capabilities development.

We are in the initial and early application and development of this technology. It is an exciting adventure and we look forward to improving the security posture of our Nation's critical ICS infrastructure in the process.

Abstract

The majority of Industrial Control Systems (ICS) lack experienced Cyber-staff to provide the necessary level of protection to defend against today's Cyber-threat. The development of effective Cyber-Decision Support Systems (CDSSs) would help in closing this gap.

We are investigating the development of CDSSs for protection of critical ICS environments. We are entering the third phase of our investigations. Our studies explore the **application of Partial Observable Markov Decision Processes** (POMDPs) as the Artificial Intelligence – Engine (AI-Engine) within our CDSS. We are in the process of experimenting within a SCEPTRE Emulytics™ model of a representative electrical grid facility. We have an initial prototype of the CDSS deployed within the SCEPTRE ICS model.

Active areas of investigation include:

- Improved/simplified Cyber-ICS model development with automation and operator inputs, covering attack, system, actions and reward models,
- Resilience of the CDSS against modeling and state estimation errors,
- Incorporation of dynamic learning capabilities,
- Additional Use Case studies in different ICS environments and
- (LDRD proposal) Human Factors Studies of functional allocation in a joint human/machine Centaur system for guidance in future CDSS capabilities development.

We are in the initial and early application and development of this technology. It is an exciting adventure and we look forward to improving the security posture of our Nation's critical ICS infrastructure in the process.

Abstract

The majority of Industrial Control Systems (ICS) lack experienced Cyber-staff to provide the necessary level of protection to defend against today's Cyber-threat. The development of effective Cyber-Decision Support Systems (CDSSs) would help in closing this gap.

We are investigating the development of CDSSs for protection of critical ICS environments. We are entering the third phase of our investigations. Our studies explore the application of Partial Observable Markov Decision Processes (POMDPs) as the Artificial Intelligence – Engine (AI-Engine) within our CDSS. We are in the process of experimenting within a SCEPTRE Emulytics™ model of a representative electrical grid facility. We have an initial prototype of the CDSS deployed within the SCEPTRE ICS model.

Active areas of investigation include:

- Improved/simplified Cyber-ICS model development with automation and operator inputs, covering attack, system, actions and reward models,
- Resilience of the CDSS against modeling and state estimation errors,
- Incorporation of dynamic learning capabilities,
- Additional Use Case studies in different ICS environments and
- (LDRD proposal) Human Factors Studies of functional allocation in a joint human/machine Centaur system for guidance in future CDSS capabilities development.

We are in the initial and early application and development of this technology. It is an exciting adventure and we look forward to improving the security posture of our Nation's critical ICS infrastructure in the process.

Abstract

The majority of Industrial Control Systems (ICS) lack experienced Cyber-staff to provide the necessary level of protection to defend against today's Cyber-threat. The development of effective Cyber-Decision Support Systems (CDSSs) would help in closing this gap.

We are investigating the development of CDSSs for protection of critical ICS environments. We are entering the third phase of our investigations. Our studies explore the application of Partial Observable Markov Decision Processes (POMDPs) as the Artificial Intelligence – Engine (AI-Engine) within our CDSS. We are in the process of experimenting within a SCEPTRE Emulytics™ model of a representative electrical grid facility. We have an initial prototype of the CDSS deployed within the SCEPTRE ICS model.

Active areas of investigation include:

- **Improved/simplified Cyber-ICS model development** with automation and operator inputs, covering attack, system, actions and reward models,
- Resilience of the CDSS against modeling and state estimation errors,
- Incorporation of dynamic learning capabilities,
- Additional Use Case studies in different ICS environments and
- (LDRD proposal) Human Factors Studies of functional allocation in a joint human/machine Centaur system for guidance in future CDSS capabilities development.

We are in the initial and early application and development of this technology. It is an exciting adventure and we look forward to improving the security posture of our Nation's critical ICS infrastructure in the process.

Abstract

The majority of Industrial Control Systems (ICS) lack experienced Cyber-staff to provide the necessary level of protection to defend against today's Cyber-threat. The development of effective Cyber-Decision Support Systems (CDSSs) would help in closing this gap.

We are investigating the development of CDSSs for protection of critical ICS environments. We are entering the third phase of our investigations. Our studies explore the application of Partial Observable Markov Decision Processes (POMDPs) as the Artificial Intelligence – Engine (AI-Engine) within our CDSS. We are in the process of experimenting within a SCEPTRE Emulytics™ model of a representative electrical grid facility. We have an initial prototype of the CDSS deployed within the SCEPTRE ICS model.

Active areas of investigation include:

- Improved/simplified Cyber-ICS model development with automation and operator inputs, covering attack, system, actions and reward models,
- **Resilience of the CDSS against modeling and state estimation errors**,
- Incorporation of dynamic learning capabilities,
- Additional Use Case studies in different ICS environments and
- (LDRD proposal) Human Factors Studies of functional allocation in a joint human/machine Centaur system for guidance in future CDSS capabilities development.

We are in the initial and early application and development of this technology. It is an exciting adventure and we look forward to improving the security posture of our Nation's critical ICS infrastructure in the process.

Abstract

The majority of Industrial Control Systems (ICS) lack experienced Cyber-staff to provide the necessary level of protection to defend against today's Cyber-threat. The development of effective Cyber-Decision Support Systems (CDSSs) would help in closing this gap.

We are investigating the development of CDSSs for protection of critical ICS environments. We are entering the third phase of our investigations. Our studies explore the application of Partial Observable Markov Decision Processes (POMDPs) as the Artificial Intelligence – Engine (AI-Engine) within our CDSS. We are in the process of experimenting within a SCEPTRE Emulytics™ model of a representative electrical grid facility. We have an initial prototype of the CDSS deployed within the SCEPTRE ICS model.

Active areas of investigation include:

- Improved/simplified Cyber-ICS model development with automation and operator inputs, covering attack, system, actions and reward models,
- Resilience of the CDSS against modeling and state estimation errors,
- **Incorporation of dynamic learning capabilities**,
- Additional Use Case studies in different ICS environments and
- (LDRD proposal) Human Factors Studies of functional allocation in a joint human/machine Centaur system for guidance in future CDSS capabilities development.

We are in the initial and early application and development of this technology. It is an exciting adventure and we look forward to improving the security posture of our Nation's critical ICS infrastructure in the process.

Abstract

The majority of Industrial Control Systems (ICS) lack experienced Cyber-staff to provide the necessary level of protection to defend against today's Cyber-threat. The development of effective Cyber-Decision Support Systems (CDSSs) would help in closing this gap.

We are investigating the development of CDSSs for protection of critical ICS environments. We are entering the third phase of our investigations. Our studies explore the application of Partial Observable Markov Decision Processes (POMDPs) as the Artificial Intelligence – Engine (AI-Engine) within our CDSS. We are in the process of experimenting within a SCEPTRE Emulytics™ model of a representative electrical grid facility. We have an initial prototype of the CDSS deployed within the SCEPTRE ICS model.

Active areas of investigation include:

- Improved/simplified Cyber-ICS model development with automation and operator inputs, covering attack, system, actions and reward models,
- Resilience of the CDSS against modeling and state estimation errors,
- Incorporation of dynamic learning capabilities,
- **Additional Use Case studies in different ICS environments** and
- (LDRD proposal) Human Factors Studies of functional allocation in a joint human/machine Centaur system for guidance in future CDSS capabilities development.

We are in the initial and early application and development of this technology. It is an exciting adventure and we look forward to improving the security posture of our Nation's critical ICS infrastructure in the process.

Abstract

The majority of Industrial Control Systems (ICS) lack experienced Cyber-staff to provide the necessary level of protection to defend against today's Cyber-threat. The development of effective Cyber-Decision Support Systems (CDSSs) would help in closing this gap.

We are investigating the development of CDSSs for protection of critical ICS environments. We are entering the third phase of our investigations. Our studies explore the application of Partial Observable Markov Decision Processes (POMDPs) as the Artificial Intelligence – Engine (AI-Engine) within our CDSS. We are in the process of experimenting within a SCEPTRE Emulytics™ model of a representative electrical grid facility. We have an initial prototype of the CDSS deployed within the SCEPTRE ICS model.

Active areas of investigation include:

- Improved/simplified Cyber-ICS model development with automation and operator inputs, covering attack, system, actions and reward models,
- Resilience of the CDSS against modeling and state estimation errors,
- Incorporation of dynamic learning capabilities,
- Additional Use Case studies in different ICS environments and
- (LDRD proposal) **Human Factors Studies of functional allocation in a joint human/machine Centaur system** for guidance in future CDSS capabilities development.

We are in the initial and early application and development of this technology. It is an exciting adventure and we look forward to improving the security posture of our Nation's critical ICS infrastructure in the process.

Abstract

The majority of Industrial Control Systems (ICS) lack experienced Cyber-staff to provide the necessary level of protection to defend against today's Cyber-threat. The development of effective Cyber-Decision Support Systems (CDSSs) would help in closing this gap.

We are investigating the development of CDSSs for protection of critical ICS environments. We are entering the third phase of our investigations. Our studies explore the application of Partial Observable Markov Decision Processes (POMDPs) as the Artificial Intelligence – Engine (AI-Engine) within our CDSS. We are in the process of experimenting within a SCEPTRE Emulytics™ model of a representative electrical grid facility. We have an initial prototype of the CDSS deployed within the SCEPTRE ICS model.

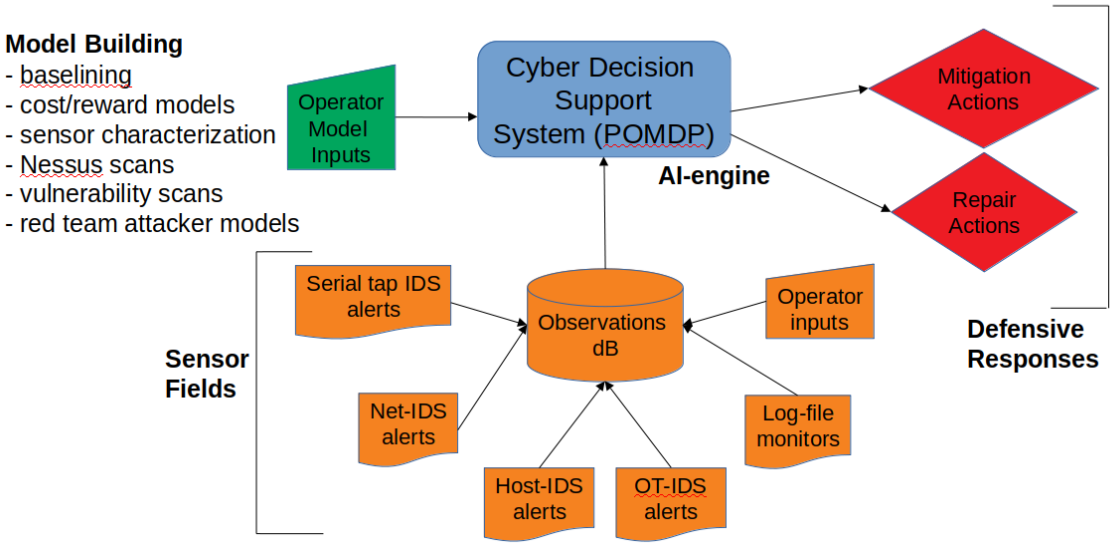
Active areas of investigation include:

- Improved/simplified Cyber-ICS model development with automation and operator inputs, covering attack, system, actions and reward models,
- Resilience of the CDSS against modeling and state estimation errors,
- Incorporation of dynamic learning capabilities,
- Additional Use Case studies in different ICS environments and
- (LDRD proposal) Human Factors Studies of functional allocation in a joint human/machine Centaur system for guidance in future CDSS capabilities development.

We are in **the initial and early application and development of this technology**. It is an exciting adventure and we look forward to improving the security posture of our Nation's critical ICS infrastructure in the process.

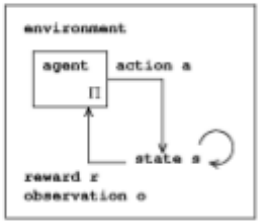
The Problem

- We are developing a Cyber Decision Support System to aid in the cyber defense of Industrial Control Systems (ICSs).
- Trained and experienced Cyber Defenders are hard to find.
- We want to improve this situation with the development of decision support systems.



Algorithmic approach

POMDP Formal Definitions

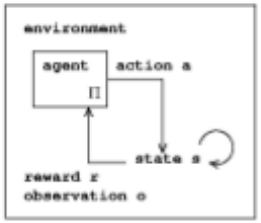


So we can more formally define a POMDP as follows:

Definition: a Partially Observable Markov Decision Process (MDP) is defined by the tuple $\langle S, A, \Omega, T, O, R \rangle$ where S is a finite set of states, A is a finite set of actions, Ω is a finite set of observations, T is a transition function defined as $T : S \times A \times S \to [0, 1]$, O is an observation function defined as $O : S \times A \times \Omega \to [0, 1]$, and R is a rewards function defined as $R : S \times A \times S \to \mathbb{R}$.

Algorithmic approach

POMDP Formal Definitions



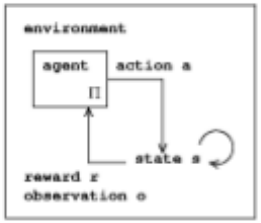
So we can more formally define a POMDP as follows:

Definition: a Partially Observable Markov Decision Process (MDP) is defined by the tuple $\langle S, A, \Omega, T, O, R \rangle$ where S is a finite set of states, A is a finite set of actions, Ω is a finite set of observations, T is a transition function defined as $T : S \times A \times S \rightarrow [0, 1]$, O is an observation function defined as $O : S \times A \times \Omega \rightarrow [0, 1]$, and R is a rewards function defined as $R : S \times A \times S \rightarrow \mathbb{R}$.

System Security State

Algorithmic approach

POMDP Formal Definitions



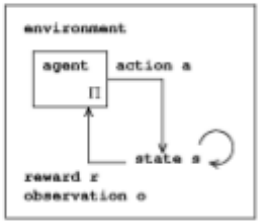
So we can more formally define a POMDP as follows:

Mitigation and Repair

Definition: a Partially Observable Markov Decision Process (MDP) is defined by the tuple $\langle S, A, \Omega, T, O, R \rangle$ where S is a finite set of states, A is a finite set of actions, Ω is a finite set of observations, T is a transition function defined as $T : S \times A \times S \rightarrow [0, 1]$, O is an observation function defined as $O : S \times A \times \Omega \rightarrow [0, 1]$, and R is a rewards function defined as $R : S \times A \times S \rightarrow \mathbb{R}$.

Algorithmic approach

POMDP Formal Definitions



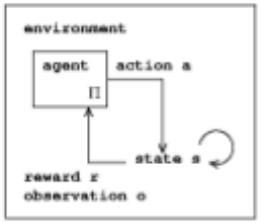
So we can more formally define a POMDP as follows:

Definition: a Partially Observable Markov Decision Process (MDP) is defined by the tuple $\langle S, A, \Omega, T, O, R \rangle$ where S is a finite set of states, A is a finite set of actions, Ω is a finite set of observations, T is a transition function defined as $T : S \times A \times S \rightarrow [0, 1]$, O is an observation function defined as $O : S \times A \times \Omega \rightarrow [0, 1]$, and R is a rewards function defined as $R : S \times A \times S \rightarrow \mathbb{R}$.

Alerts and Logs

Algorithmic approach

POMDP Formal Definitions



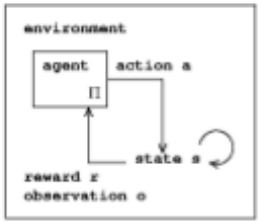
So we can more formally define a POMDP as follows:

Definition: a Partially Observable Markov Decision Process (MDP) is defined by the tuple $\langle S, A, \Omega, T, O, R \rangle$ where S is a finite set of states, A is a finite set of actions, Ω is a finite set of observations, T is a transition function defined as $T : S \times A \times S \rightarrow [0, 1]$, O is an observation function defined as $O : S \times A \times \Omega \rightarrow [0, 1]$, and R is a rewards function defined as $R : S \times A \times S \rightarrow \mathbb{R}$.

Attacker modeling and Action effects

Algorithmic approach

POMDP Formal Definitions



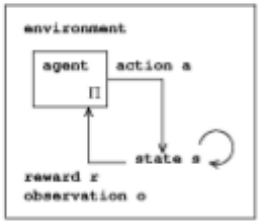
So we can more formally define a POMDP as follows:

Definition: a Partially Observable Markov Decision Process (MDP) is defined by the tuple $\langle S, A, \Omega, T, O, R \rangle$ where S is a finite set of states, A is a finite set of actions, Ω is a finite set of observations, T is a transition function defined as $T : S \times A \times S \rightarrow [0, 1]$, O is an observation function defined as $O : S \times A \times \Omega \rightarrow [0, 1]$, and R is a rewards function defined as $R : S \times A \times S \rightarrow \mathbb{R}$.

Alert likelihood based on Actions

Algorithmic approach

POMDP Formal Definitions



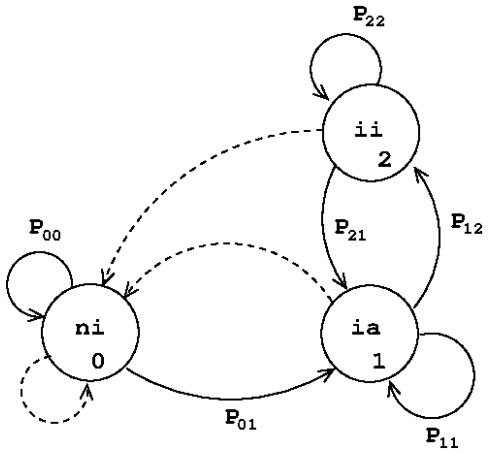
So we can more formally define a POMDP as follows:

Definition: a Partially Observable Markov Decision Process (MDP) is defined by the tuple $\langle S, A, \Omega, T, O, R \rangle$ where S is a finite set of states, A is a finite set of actions, Ω is a finite set of observations, T is a transition function defined as $T : S \times A \times S \rightarrow [0, 1]$, O is an observation function defined as $O : S \times A \times \Omega \rightarrow [0, 1]$, and R is a rewards function defined as $R : S \times A \times S \rightarrow \mathbb{R}$.

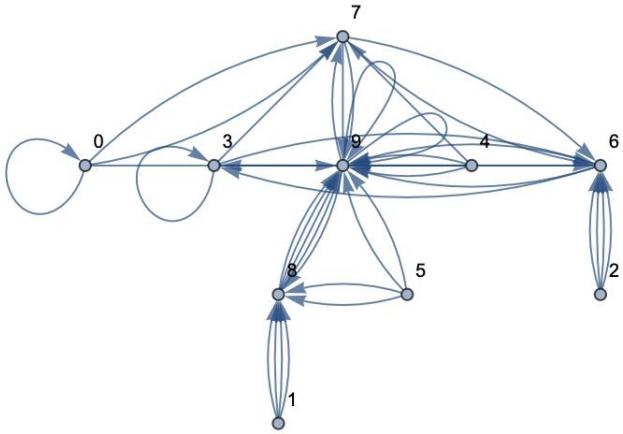
Rewards and costs for Actions

Algorithmic approach

- The Artificial Intelligence being designed within the Cyber Decision Support System is based upon Partial Observable Markov Decision Process (POMDP) modeling.
- We have developed POMDP models for the cyber defense of Enterprise Technology (ET) and Supervisory Control And Data Aquisition (SCADA) and ICS systems.
- We have developed the AI-Engine based upon POMDP forming the basis of the Decision Support System.



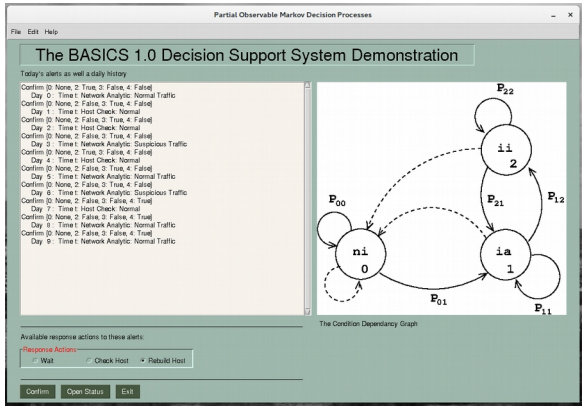
POMDP Modeling



Policy Graph Solutions

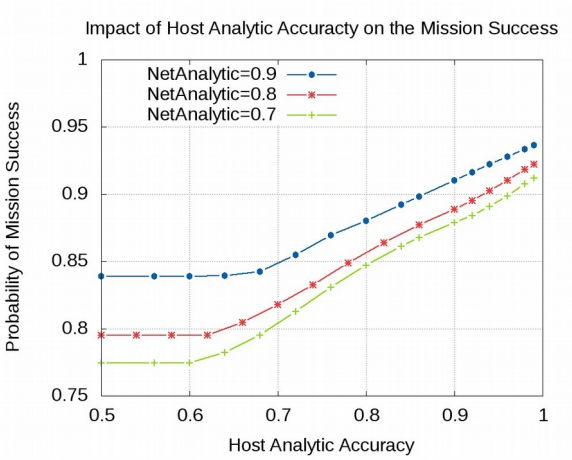
Early Results

- On an early prototype system we have explored the POMDP modeling and results.

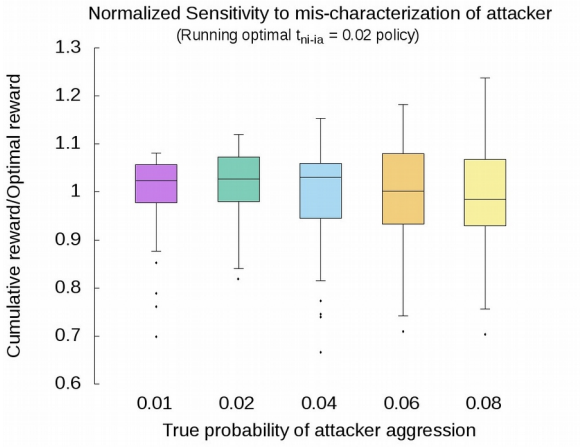


POMDP Simulation and Operator Interface for gaming.

Analytics Assessments

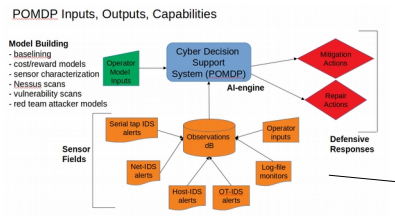


Sensitivity Analysis

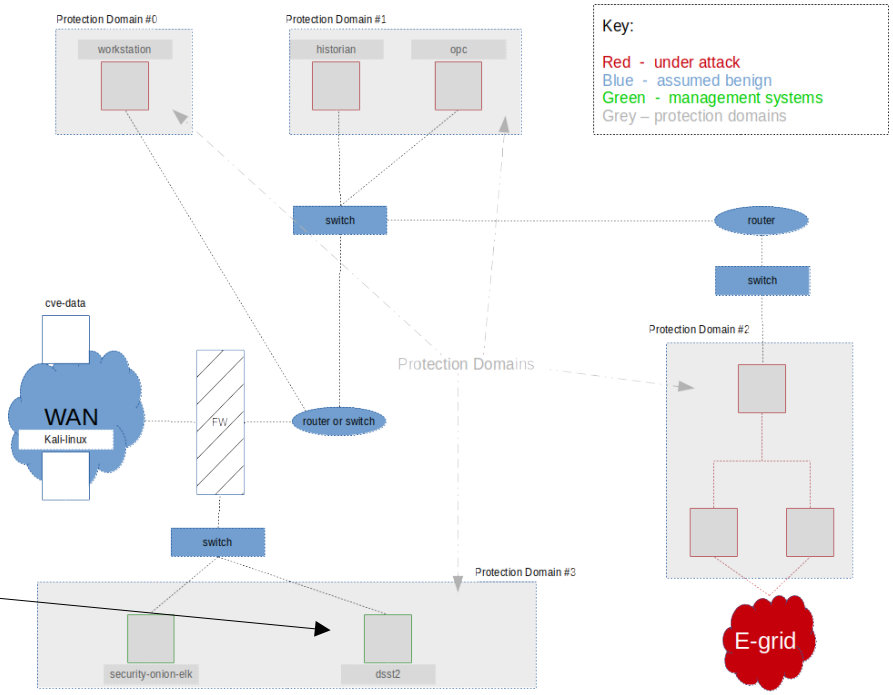


Description of More Data

- We have developed a SCEPTRE emulation model of a slimmed down version of a Department of Defense (DoD) ICS system.
- We have embedded the AI-Engine into our SCEPTRE model for test and demonstration.



Embedded AI-Engine



SCEPTRE ICS Model

Conclusions

- Developing POMDP models for cyber defense is a way to incorporate domain expertise into the AI.
- Need to perform more varied performance studies of the POMDP models in the protection of other ICS domains (electrical, water, pipeline).
- Need to figure out how to incorporate learning into these systems.
- Need to simplify POMDP model building.
- Need to perform human factors studies to determine optimal functional allocation between human and machine.