AI-POMDP Modeling for the Cyber-Defense of Joint Ground Station and Satellite Systems

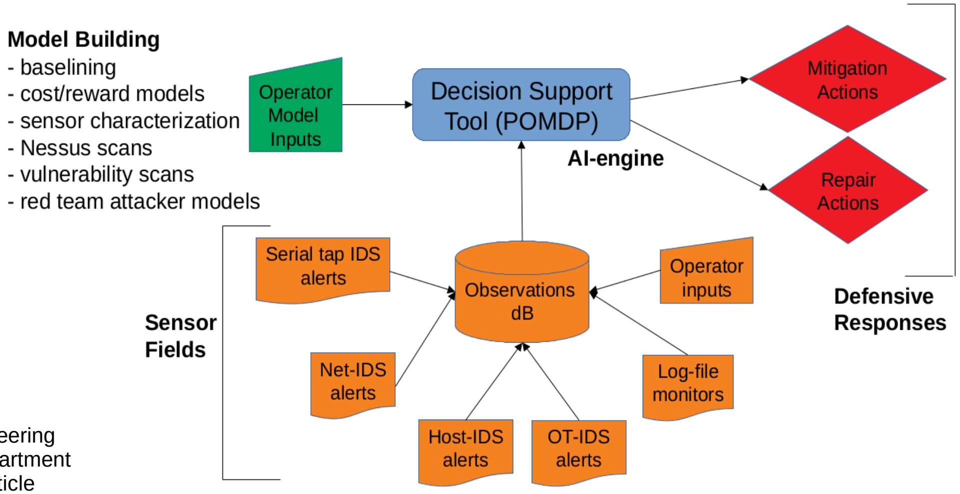
Robert G. Cole and Alexander Outkin

The Sandia BASICS Team

Sandia National Laboratories

Albuquerque, New Mexico USA

POMDP Inputs, Outputs, Capabilities

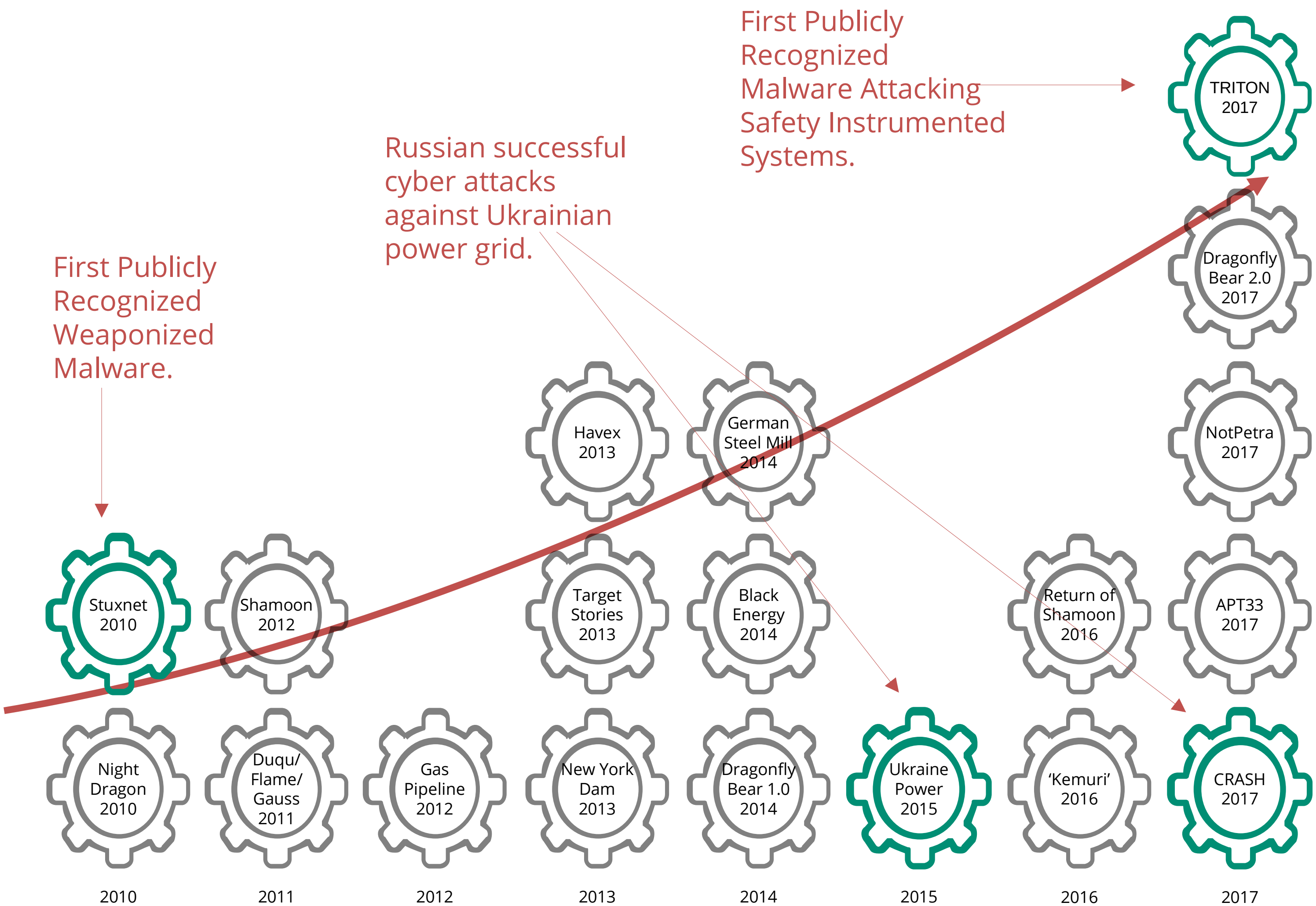


This article has been authored by an employee of National Technology & Engineering Solutions of Sandia, LLC under Contract No. DE-NA0003525 with the U.S. Department of Energy (DOE). The employee owns all right, title and interest in and to the article and is solely responsible for its contents. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this article or allow others to do so, for United States Government purposes. The DOE will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan "https://www.energy.gov/downloads/doe-public-access-plan."

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.

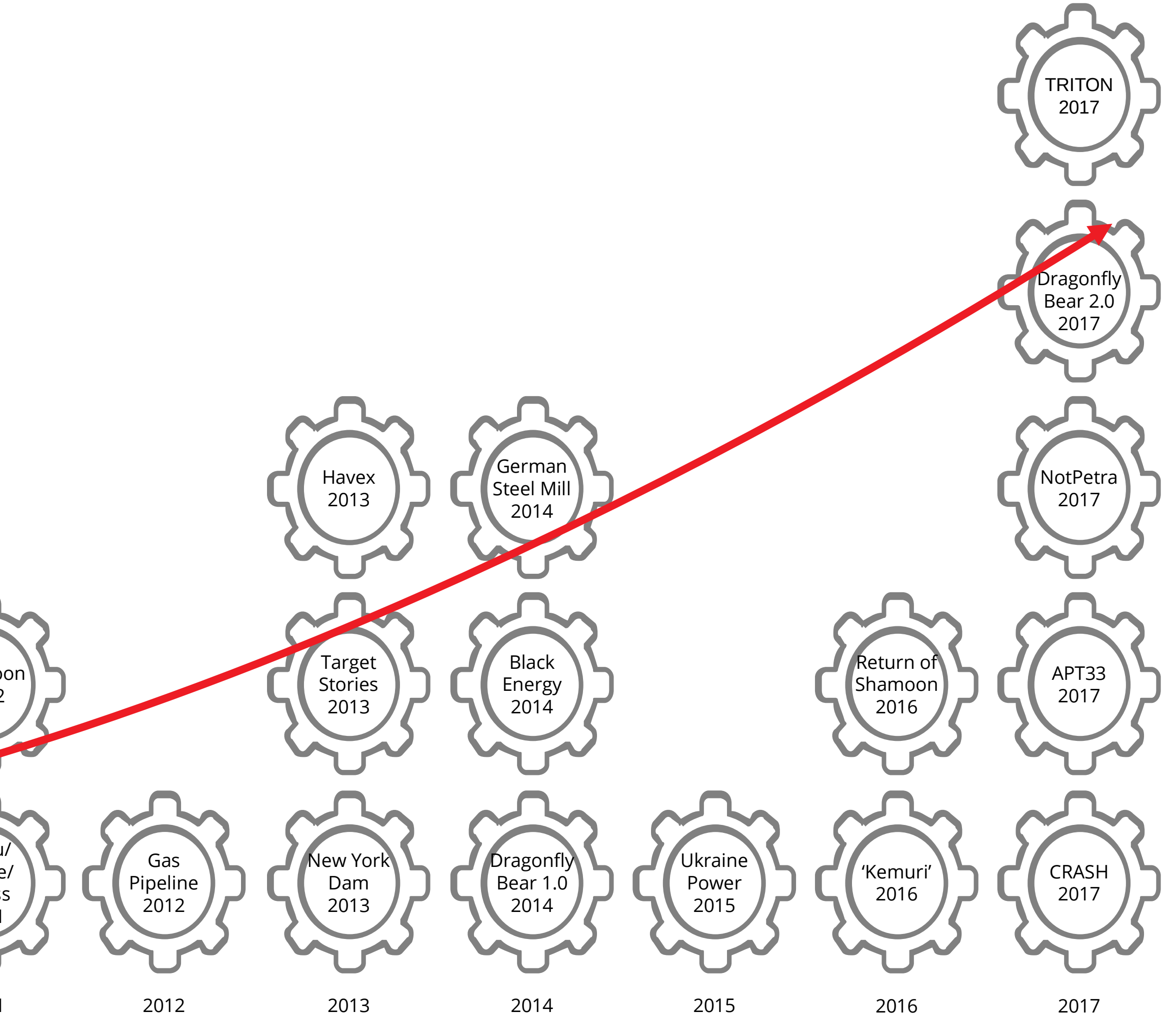
Motivated by Escalating Threats Against ICS

Sandia National Laboratories



Reference: Hemsley, K.E. and R.E.Fisher, "History of Industrial Control Systems Cyber Incidence", INL Technical Report, DOE/ID-Number-1505628 December (2018).

Motivated by Escalating Threats Against ICS

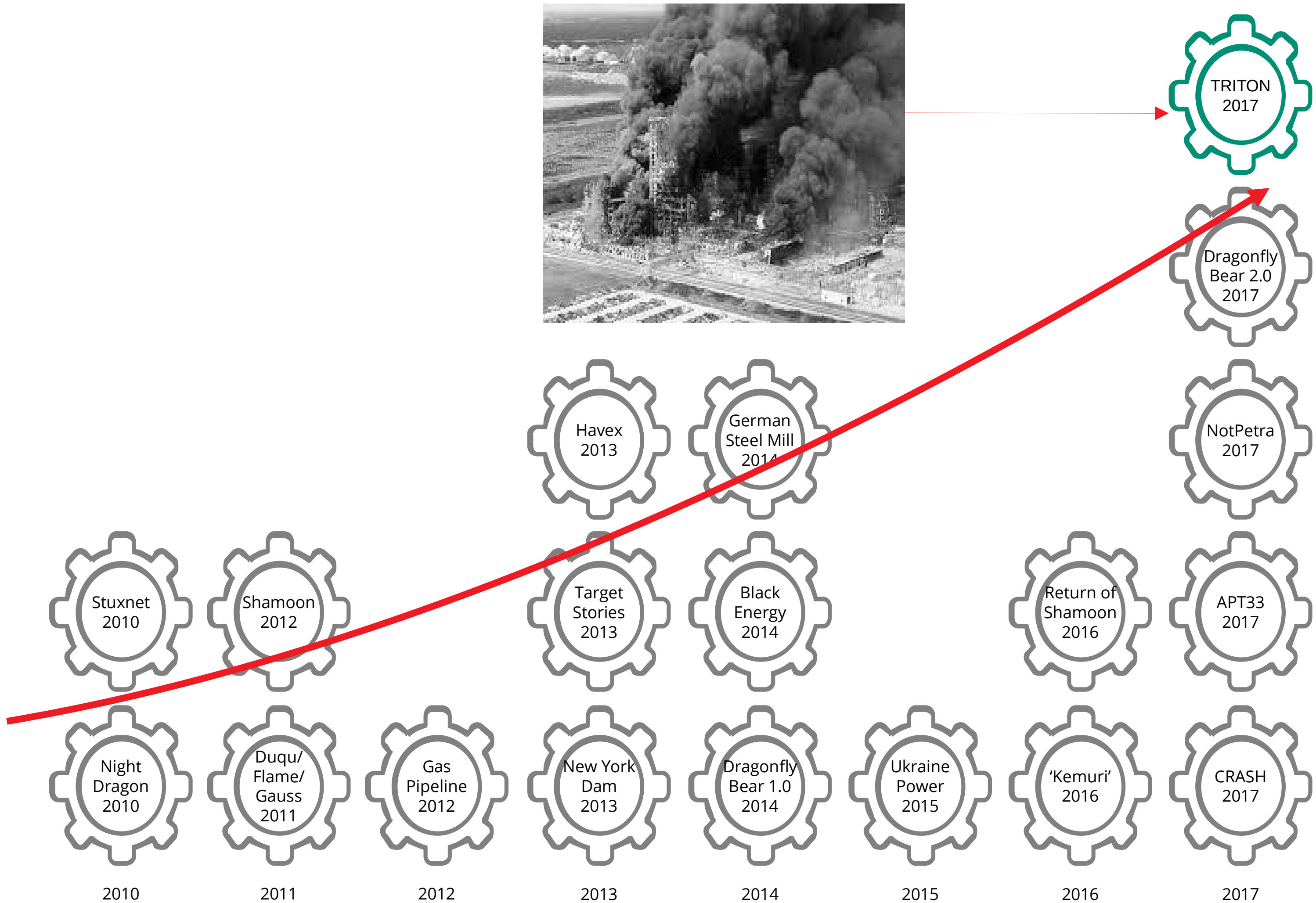


Reference: Hemsley, K.E. and R.E.Fisher, "History of Industrial Control Systems Cyber Incidence", INL Technical Report, DOE/ID-Number-1505628 December (2018).

Motivated by Escalating Threats Against ICS

Reference: Hemsley, K.E. and R.E.Fisher, "History of Industrial Control Systems Cyber Incidence", INL Technical Report, DOE/ID-Number-1505628 December (2018).

Motivated by Escalating Threats Against ICS

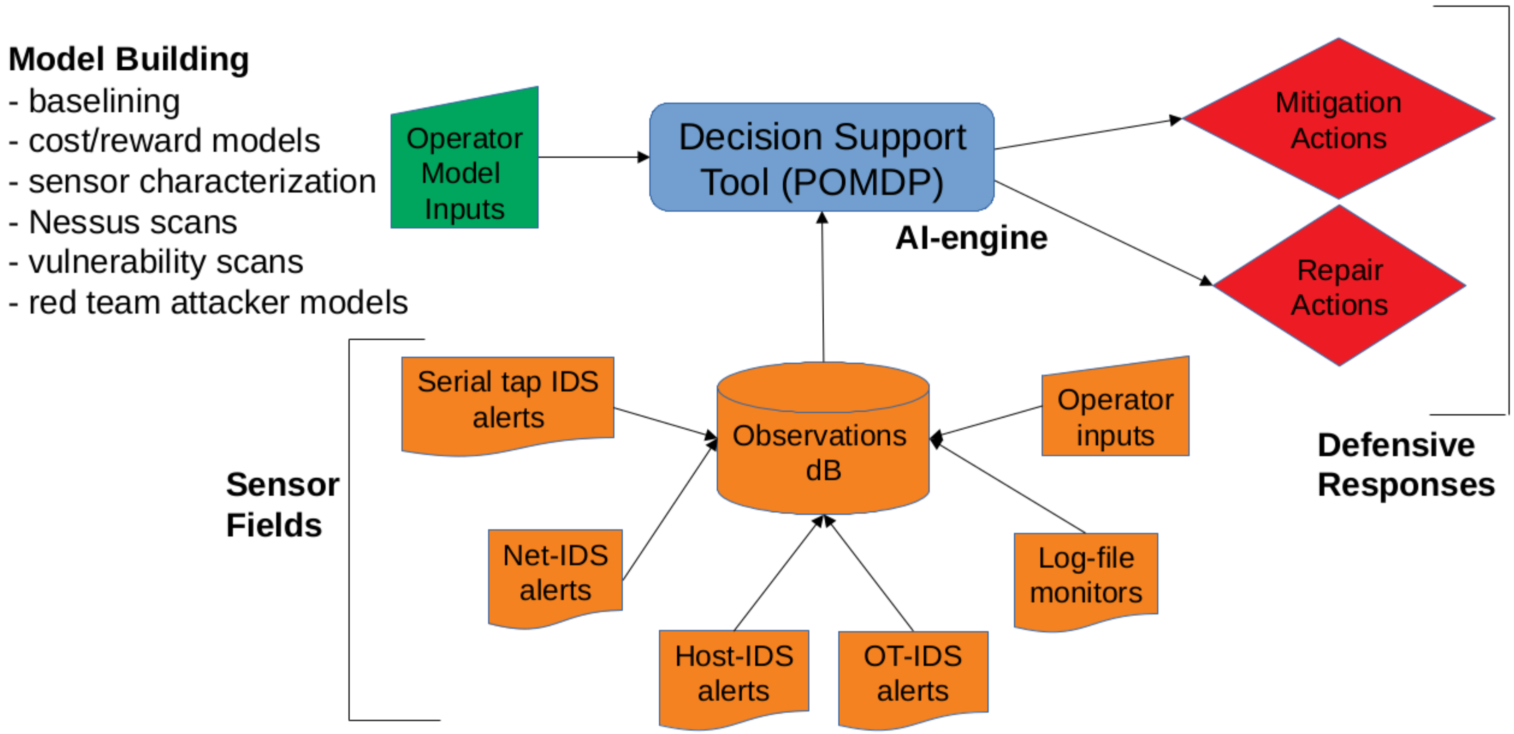


Reference: Hemsley, K.E. and R.E.Fisher, "History of Industrial Control Systems Cyber Incidence", INL Technical Report, DOE/ID-Number-1505628 December (2018).

Bottom Line Up Front

- We have developed a Decision Support prototype based upon an POMDP Artificial Intelligence (AI) agent (see diagram below).
- This currently acts as a Security Orchestration and Automated Response (SOAR) system for Industrial Control Systems.
- Initial testing in protection against cyber-attacks on an emulated ICS have been favorable.
- Working on the development of multiple Operator Interfaces for deployment.

★ Exploring applications of this technology to defense of joint Ground Station/Satellite systems.



Technical Details

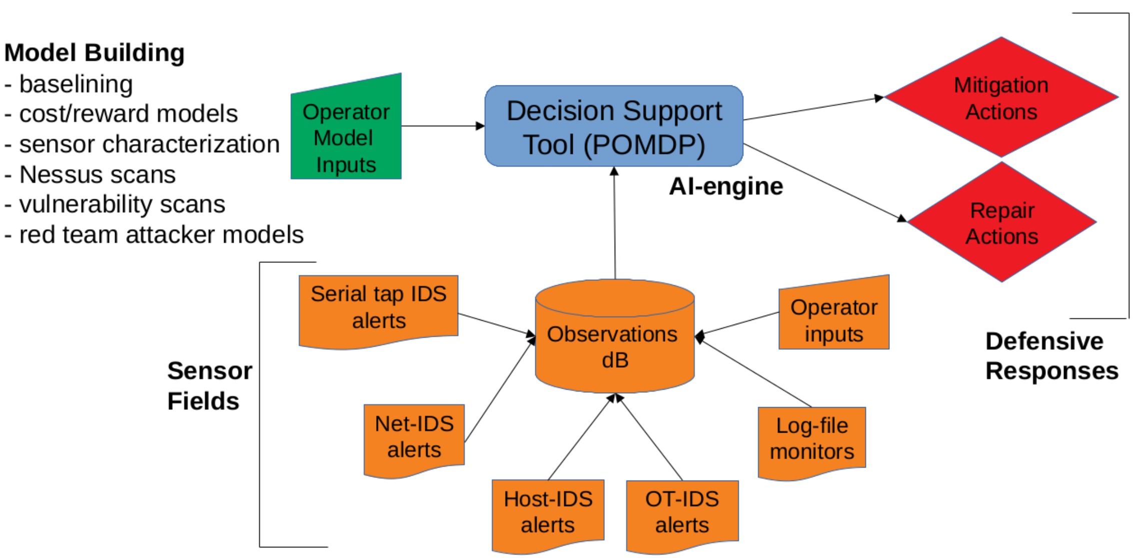
Unclassified Unlimited Release

Requirements and Design

Design, Develop and Test a Decision Support System (DSS) to support novice cyber defenders of the nation's critical GS/Satellite systems.

The DSS must be:

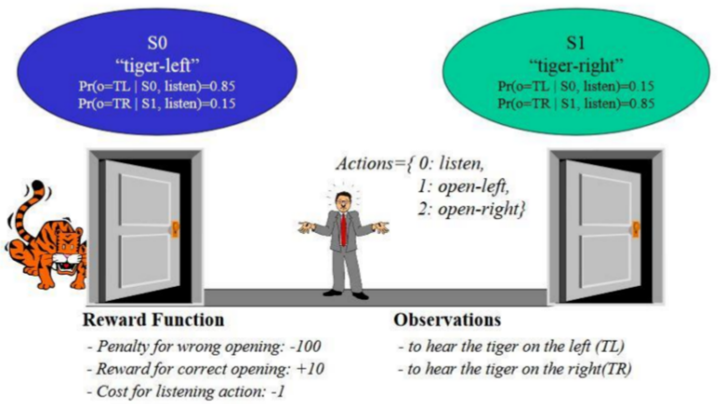
- Effective in the defense of GS/Satellite environments,
- Does not require vast, labeled datasets to train,
- Does not require running thousands to millions of trials to learn,
- Contain an AI Expert System Shell to simplify configuration and deployment,
- Intuitive and easily described,
- Scalable and
- Well tested and validated.



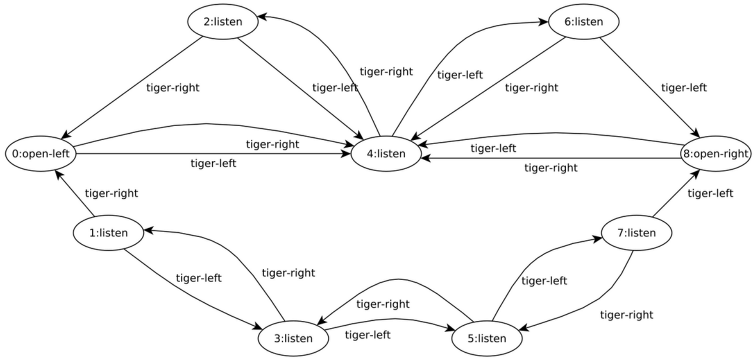
We chose POMDP AI !

What is a POMDP - the Tiger Problem

A POMDP Example: The Tiger Problem



The Tiger Problem Policy Graph (solved)



The POMDP Configuration: The Tiger Problem

This example is from the Examples section of 'pomdp.org'

discount: 0.75
values: reward
states: tiger-left tiger-right
actions: listen open-left open-right
observations: tiger-left tiger-right

T:listen
identity

T:open-left
uniform

T:open-right
uniform

O:listen
0.85 0.15
0.15 0.85

O:open-left
uniform

O:open-right
uniform

R:listen : * : * : * -1
R:open-left : tiger-left : * : * -100
R:open-left : tiger-right : * : * 10
R:open-right : tiger-left : * : * 10
R:open-right : tiger-right : * : * -100

Why an AI based upon POMDP

+ Russell, S. and P. Norvig, “Artificial Intelligence”, define four levels of artificial intelligence agents. These are:

a) Simple Reflex Agents, ← least sophisticated

b) Model Based Reflex Agents,

c) Goal Based Agents and

d) Utility Based Agents. ← most sophisticated

+ State of the Art in cyber-defense deployments is Simple Reflex Agents, i.e., think ‘Table Lookup’, ‘Playbooks’, etc.

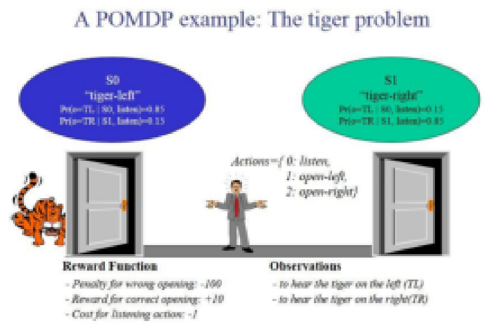
+ If we ran Simple Reflex Agent for the Tiger Problem, its long term reward would be

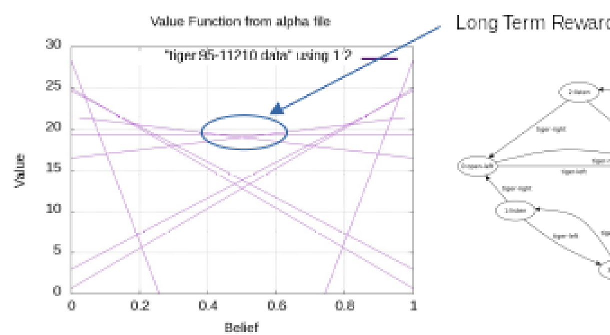
0.85x10 – 0.15x100 = - 6.5

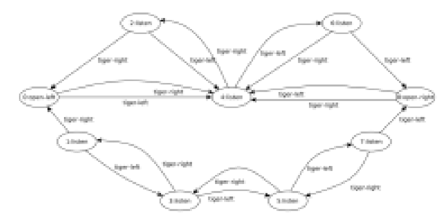
+ If we ran a Utility Based Agent, e.g., a POMDP, for the Tiger Problem, its long term reward would be (see diagram to the right)

+19.5 !

What do you want in your wallet ?

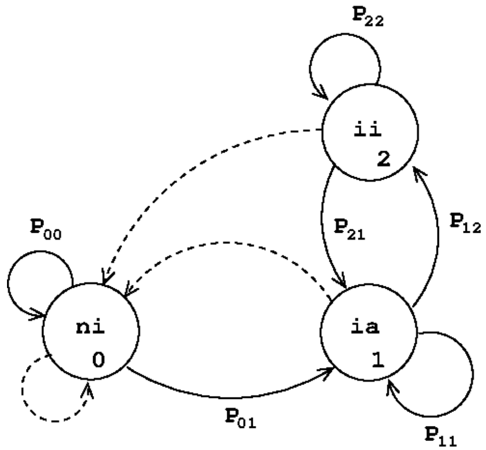




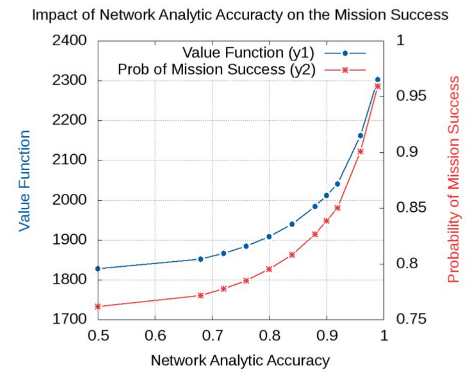


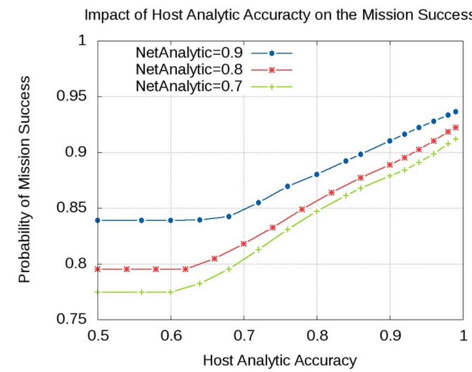
A POMDP Cyber Example

A POMDP Example: Day in the Life of a Host

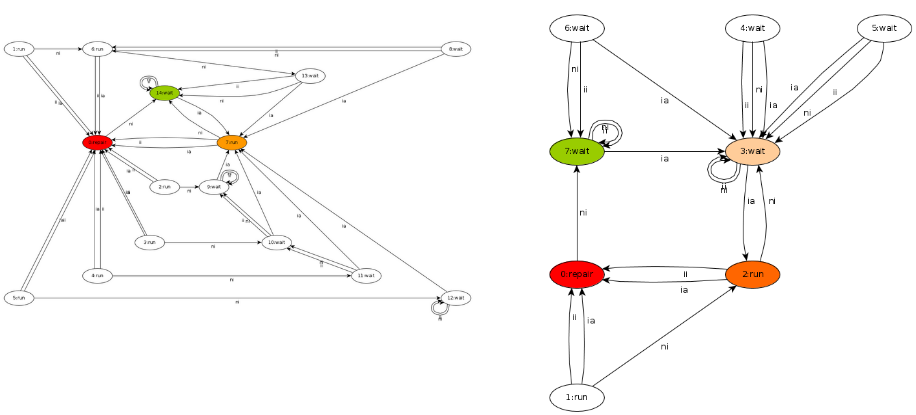


The Host POMDP Studies

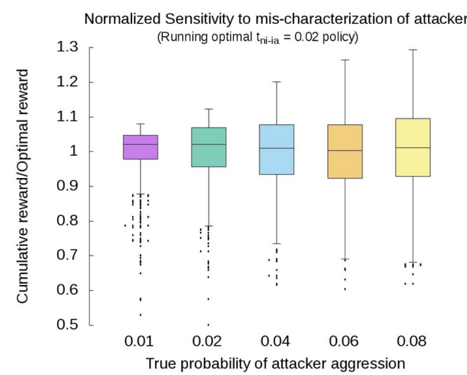




The Host Problem Policy Graph (solved)

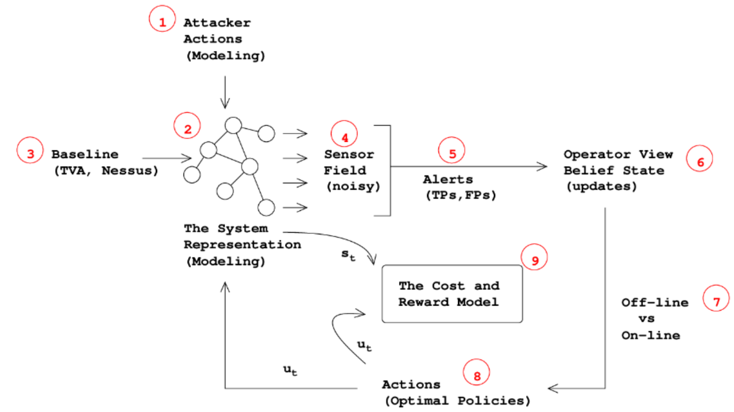


Sensitivity Studies or errors in POMDP modeling

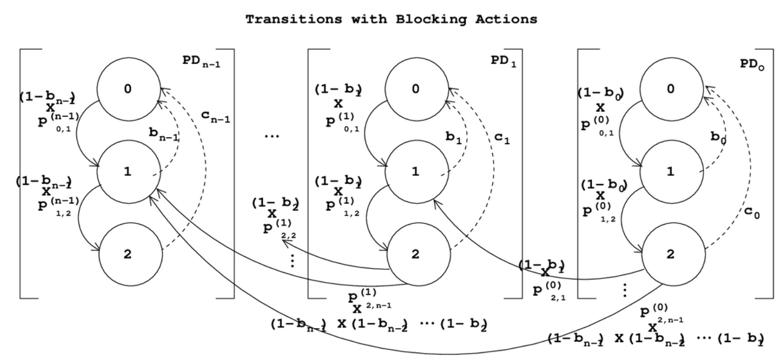


Algorithmic Approach and its Advantages

- 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



An ICS POMDP Logic Model

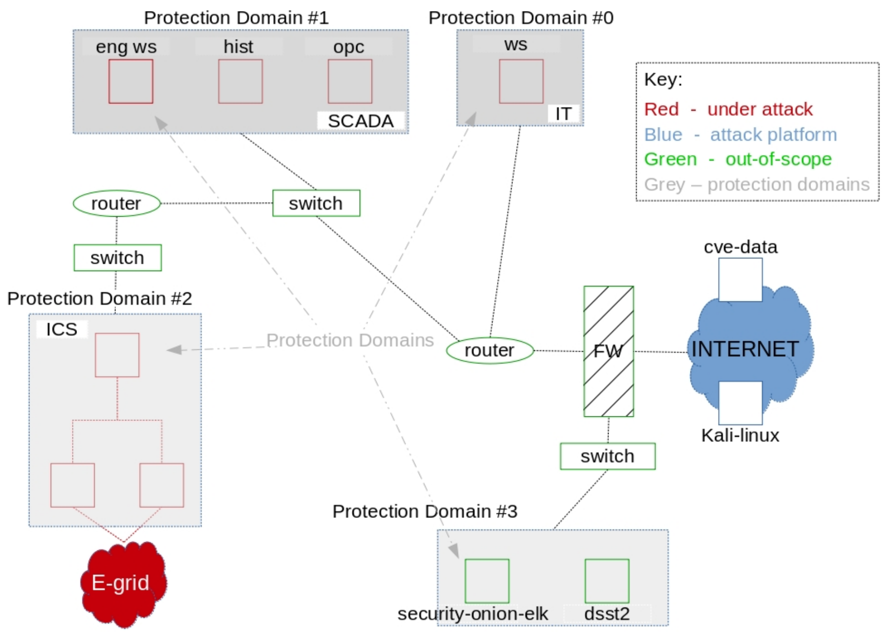
Unclassified Unlimited Release

Test and Evaluation Methods

Sandia National Laboratories

No data! Just Experimentation, Test and Evaluation ...

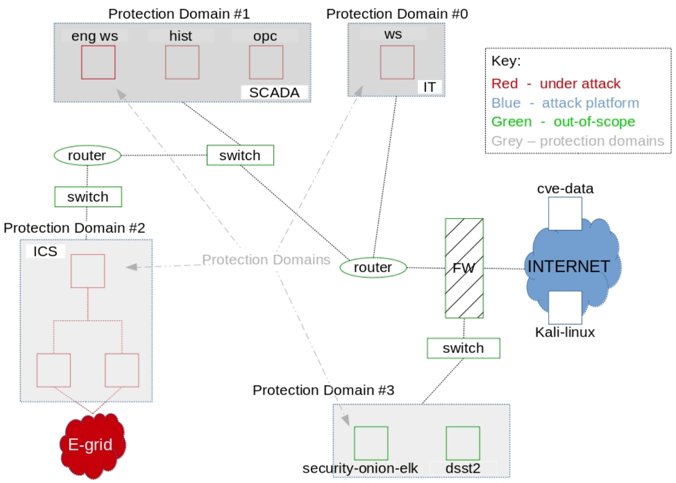
- We will use domain expertise to develop our POMDP models and then extensively test them out on high fidelity emulation models of SCADA/ICS systems.
- We are using SCEPTRE to emulate SCADA/ICS environments and CobaltStrike for cyber attack scripting and we plan on running live Red Team attacks against our systems in the future. Derived from the previous programs.
- Red Teaming capabilities taken from previous programs and expanded.



SCEPTRE Emulation Modeling of Industrial Control Systems.

Simulating an attacker

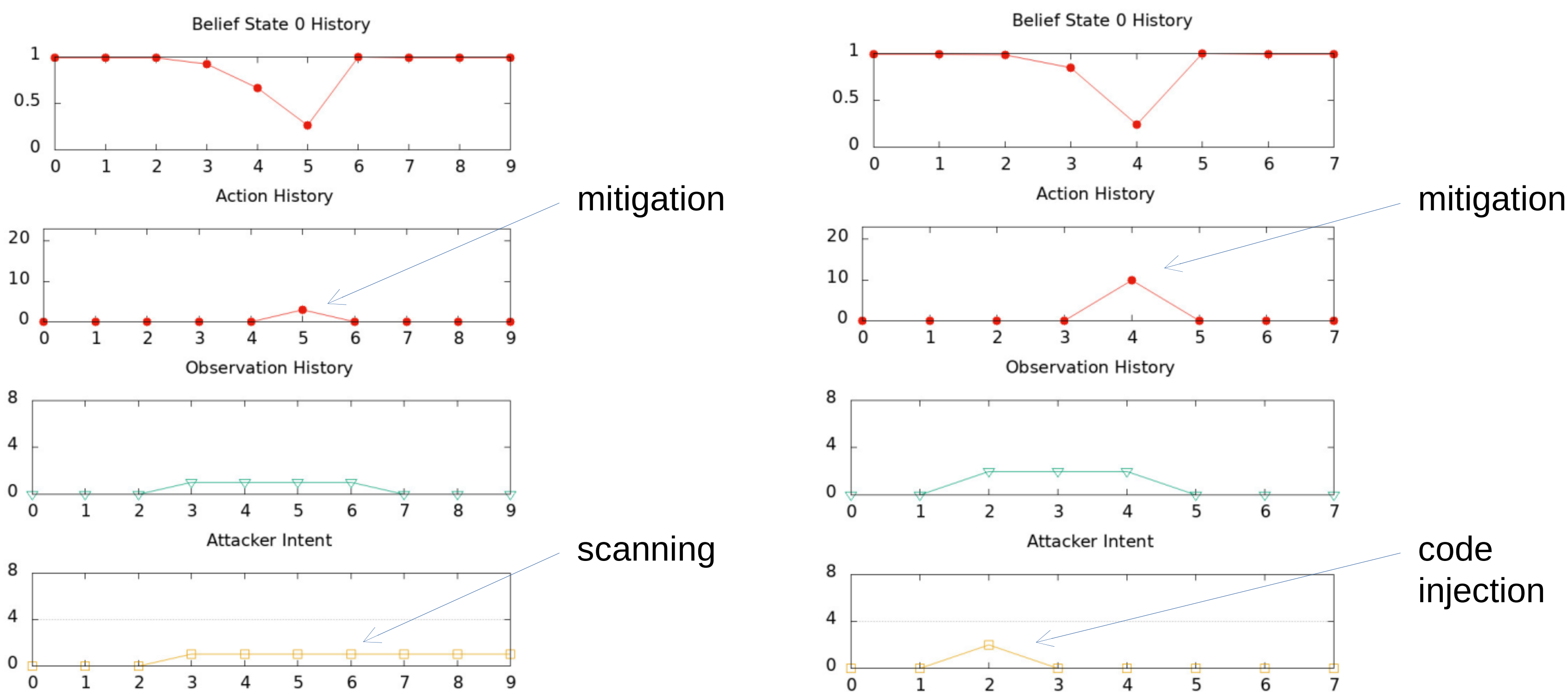
- **Role**
  - Conduct simulated attacks on systems within the network.
- **Intent**
  - Simulate actions an attacker might take to gain access to target systems and compromise certain components.
  - Test how existing NIDS and HIDS systems respond and how the POMDP model responds.
  - Help conceptualize how a real-world attack might affect the system.
- **Process**
  - Simulate IT/OT environment using SCEPTRE.
  - Create an attacker system sitting outside Network (Kali-linux, Cobalt Strike).
  - Use Cobalt Strike to plant/communicate with beacons on compromised machines.
  - Establish foothold in network by using known vulnerabilities to compromise an IT system.
  - Use this foothold to launch attacks on other systems in the OT network.



Results – Representative, Simple Attacks

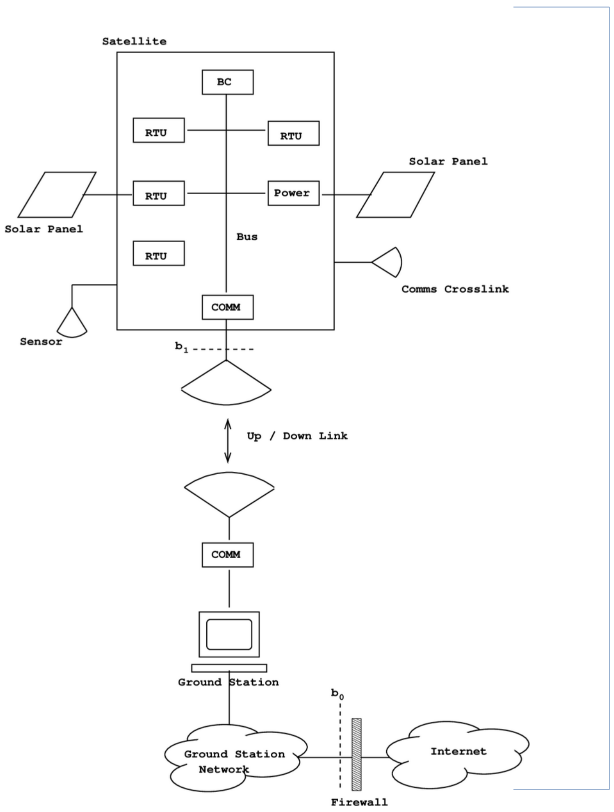
Sandia National Laboratories

- Our system reacts to the attacks thrown at it with a reasonable and explainable response.
- We are testing with more attack types and are constrained only in the quality of the sensors.
- The response is reasonable even when the attacker is deviating from our attack modeling.

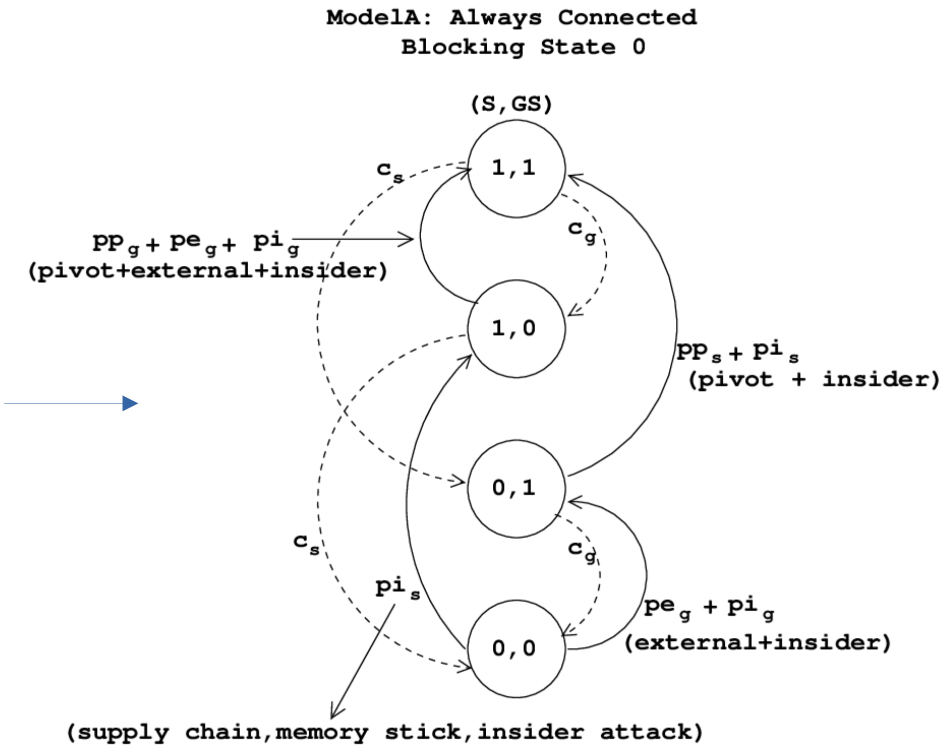


Simplified POMDP model of GS/Satellites

- POMDP cyber modeling of permanently connected GS/Satellite system.
- Solid arrows represent attack vectors. Dashed arrows represent 'Actions'.
- Firewall actions represented through topology changes to POMDP model.



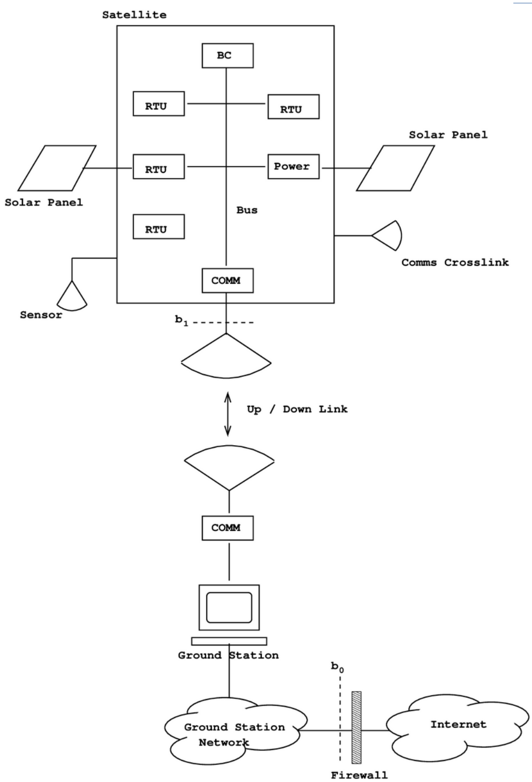
Abstract GS/Satellite system diagram



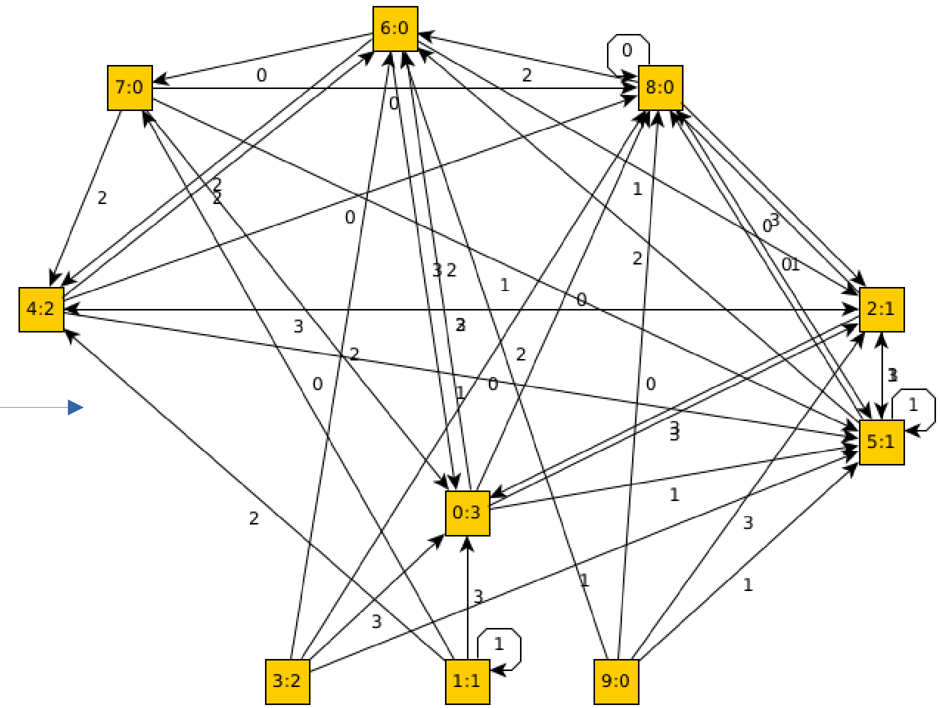
Associated POMDP of GS/Satellite

Policy Graph of Simplified GS/Satellite Model

- A policy graph for permanently connected ground stations and satellite system.



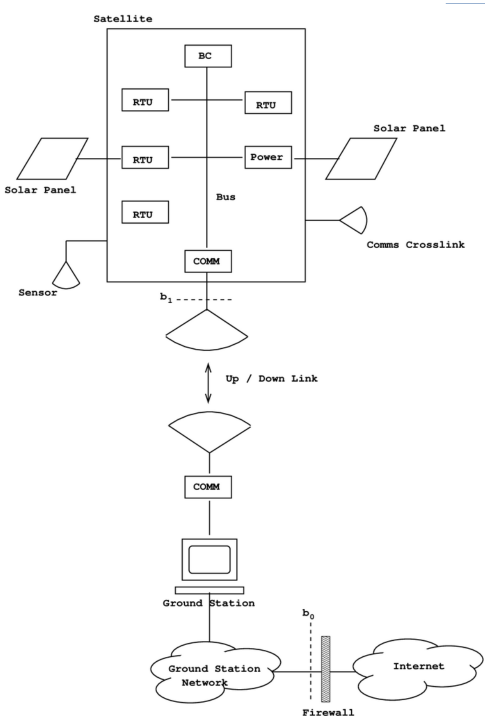
An abstracted Ground Station and Satellite system diagram



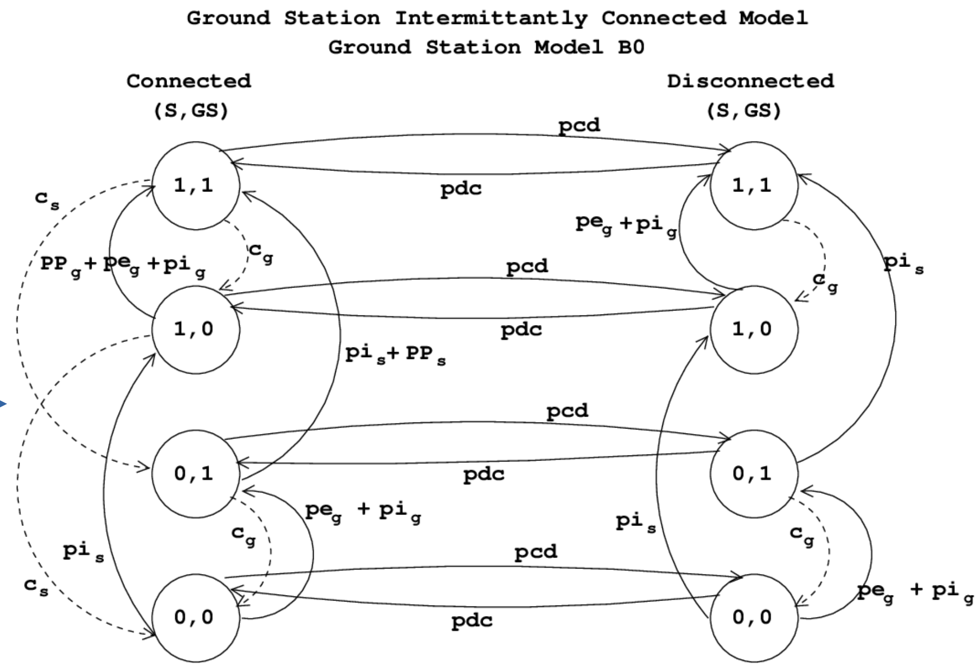
- Nodes represent different Belief States.
- Node labels contain arbitrary label followed by optimal action.
- Arrows labeled by Observations indicate transitions to next Belief State.

Modeling intermittent connectivity

- One approach to model distributed, interacting multiple agents under intermittent connectivity situations, one for the GS and one for the Satellite.
- Seems overly complicated; tracking unnecessary components.
- Still requires a split/rejoin procedure.



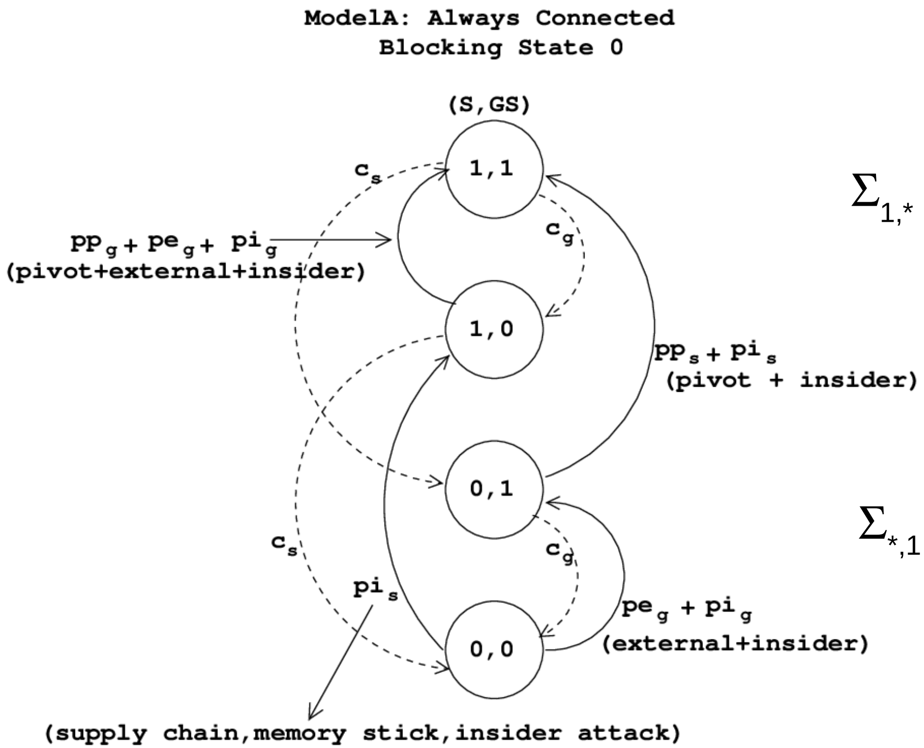
An abstracted Ground Station and Satellite system diagram



Ground Station directed agent model

Reduction modeling intermittent connectivity

- So, ...another approach is to maintain reduced models when disconnected.
- Then reconstruct full model upon re-connection.



An abstracted Ground Station and Satellite system diagram

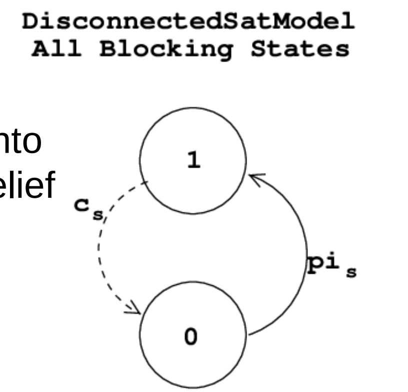
$\Sigma_{1,*}$

$\Sigma_{*,1}$

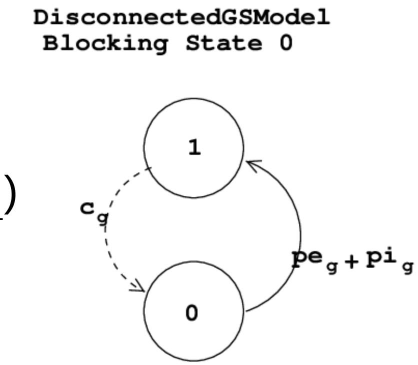
Disconnect

Reduce belief state into separate b_s and b_g belief states.

$b_s = (b_{s,0}\ ,\ b_{s,1})$



$b_g = (b_{g,0}\ ,\ b_{g,1})$



Rejoin

Merge Belief State probabilities of b_s and b_g into a connected model Belief State for connected model on right.

Potential Future Work

- Develop and experiment with higher fidelity models of the Ground Stations and Satellite systems.
- Perform simulation studies of the performance of the high fidelity GS/Satellite models under attack.
- Explore potential emulation platforms for more realistic studies, attack scenarios, etc. in order to better assess the capabilities of POMDP models defending GS/Satellite systems against cyber attacks.

Questions ?

Robert G. Cole
rcole@sandia.gov