Improving Cyber Resiliency Through Microsegmentation Policy Optimization

Steven Noel, PhD

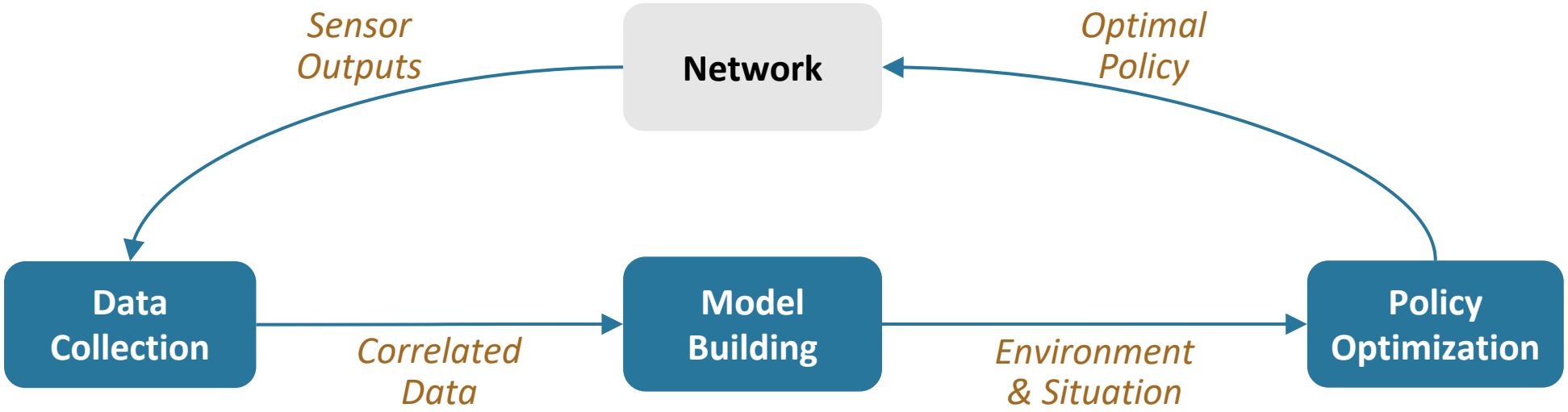
January 11, 2022

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD

Introduction

- Optimal microsegmentation access policy rules <*source IP*, *destination IP*, *source port*, *destination port*, *protocol*> enforced via AWS Group Policy
- Optimization objective function that balances cyberattack risks against accessibility to critical network resources
- Genetic algorithm finds policy rules that optimize the objective function
- MITRE *Adaptive Resiliency Experimentation System* (ARES)
  - Off-the-shelf security tools and AI/ML components for optimizing cyber resilience
  - Includes microsegmentation, authentication, policy generalization, redundancy, deception, zero-trust architecture
- Reference: Steven Noel, Vipin Swarup, Karin Johnsgard, “Optimizing Network Microsegmentation Policy for Cyber Resilience,” *Journal of Defense Modeling and Simulation*, Special Issue on Impact Analysis for Cyber Defense Optimization, 2021.

Overview of Approach

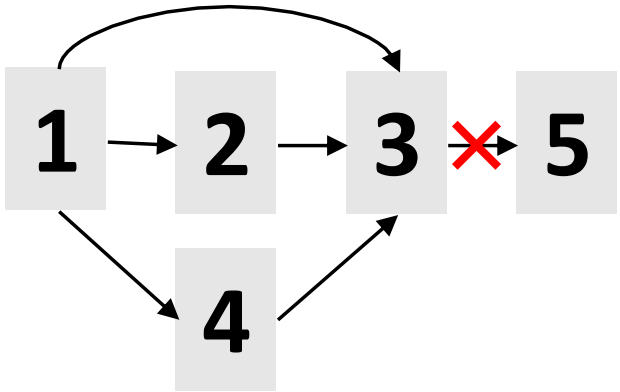


- Host and network sensors forward data to repository
- Data elements correlated across the sensor types

- Network data mapped to model for threat and mission
  - Adversary reachability via multi-step exploitation
  - Mission criticality for access to network resources

- Policy rules that provide optimal network resiliency
- Optimization objectives: maximize adversary effort and mission availability

Optimization Framework



$$A = \begin{bmatrix} 01110 \\ 00100 \\ 00001 \\ 00100 \\ 00000 \end{bmatrix} \quad P = \begin{bmatrix} 01110 \\ 00100 \\ 00000 \\ 00100 \\ 00000 \end{bmatrix}$$

Genetic Algorithm Fitness Function

Optimization Objectives $\vec{f}(\acute{A}, \acute{M})$

Score

$$\acute{A} = \begin{bmatrix} a'_{1,1} & \cdots & a'_{1,n} \\ \vdots & \ddots & \vdots \\ a'_{n,1} & \cdots & a'_{n,n} \end{bmatrix} \quad \acute{M} = \begin{bmatrix} m'_{1,1} & \cdots & m'_{1,n} \\ \vdots & \ddots & \vdots \\ m'_{n,1} & \cdots & m'_{n,n} \end{bmatrix}$$

Attacks Hardened — Mission Hardened

Hardened

$$A = \begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{bmatrix} \quad M = \begin{bmatrix} m_{1,1} & \cdots & m_{1,n} \\ \vdots & \ddots & \vdots \\ m_{n,1} & \cdots & m_{n,n} \end{bmatrix}$$

Attack Vectors — Mission Needs

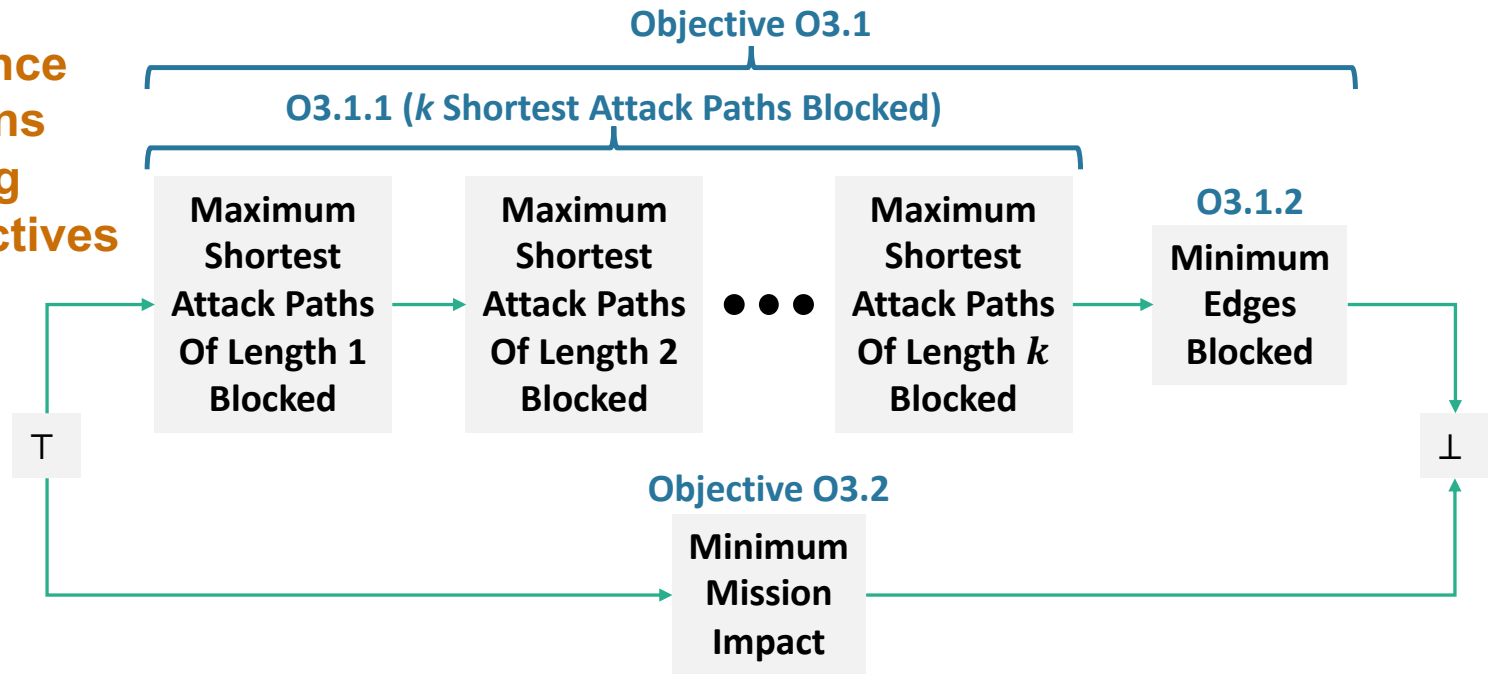
Apply

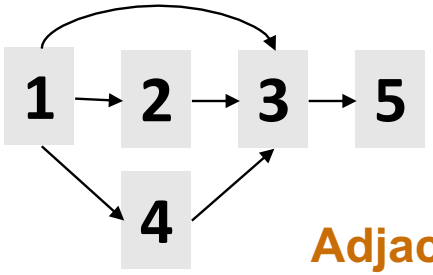
Policy Rules $P = \begin{bmatrix} p_{1,1} & \cdots & p_{1,n} \\ \vdots & \ddots & \vdots \\ p_{n,1} & \cdots & p_{n,n} \end{bmatrix}$

Genetic Algorithm Individual (Chromosome)

Optimization Objective Function

Dominance Relations Among Sub-Objectives



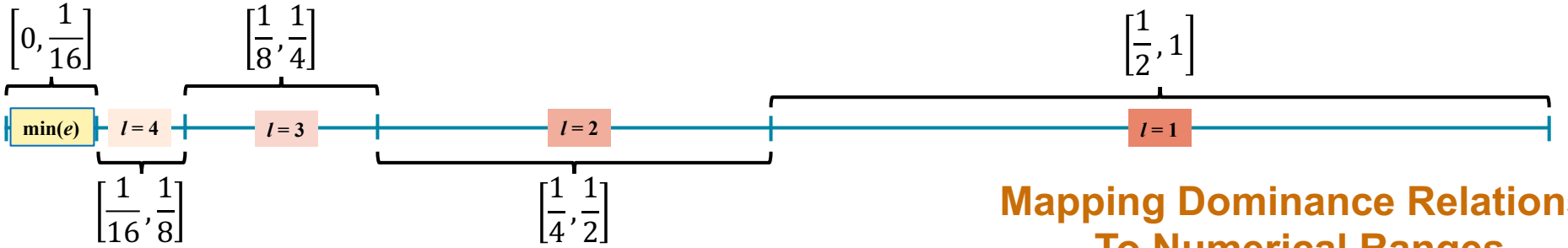


Graph Adjacency Matrix And Powers

$$A = \begin{bmatrix} 01110 \\ 00100 \\ 00001 \\ 00100 \\ 00000 \end{bmatrix}$$

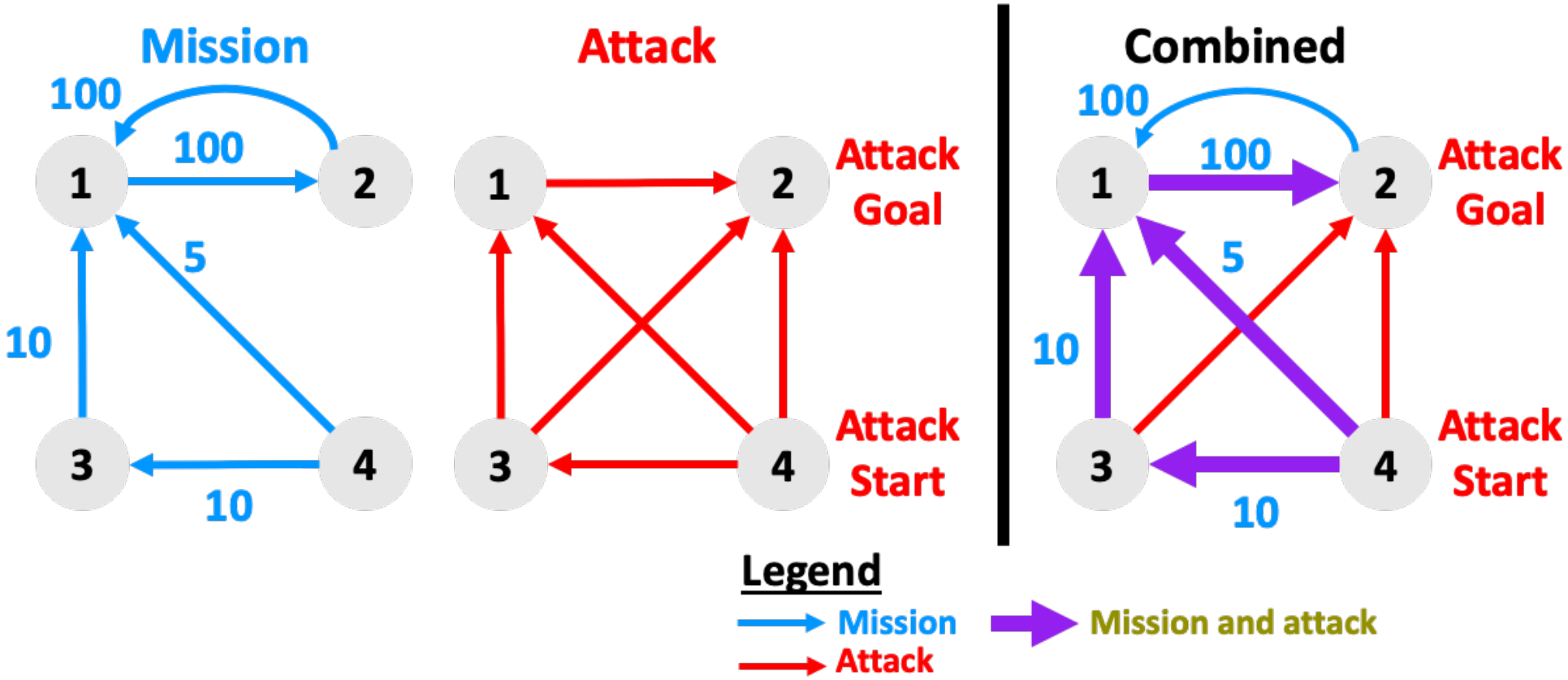
$$A^2 = \begin{bmatrix} 01110 \\ 00100 \\ 00001 \\ 00100 \\ 00000 \end{bmatrix} \times \begin{bmatrix} 01110 \\ 00100 \\ 00001 \\ 00100 \\ 00000 \end{bmatrix} = \begin{bmatrix} 00201 \\ 00001 \\ 00000 \\ 00001 \\ 00000 \end{bmatrix}$$

$$A^3 = A \times A^2 = \begin{bmatrix} 01110 \\ 00100 \\ 00001 \\ 00100 \\ 00000 \end{bmatrix} \times \begin{bmatrix} 00201 \\ 00001 \\ 00000 \\ 00001 \\ 00000 \end{bmatrix} = \begin{bmatrix} 00002 \\ 00000 \\ 00000 \\ 00000 \\ 00000 \end{bmatrix}$$



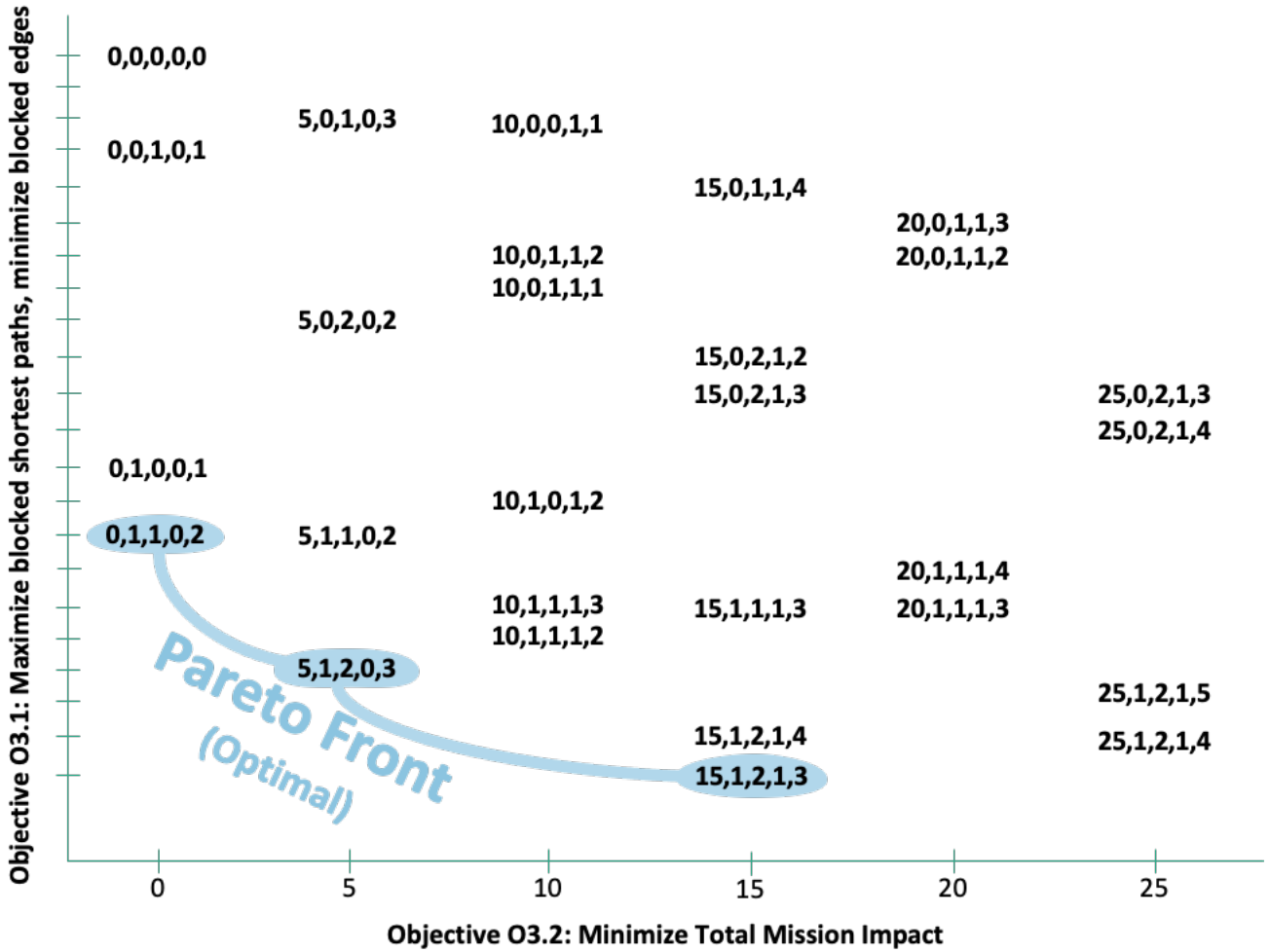
Mapping Dominance Relations To Numerical Ranges

Illustrative Example



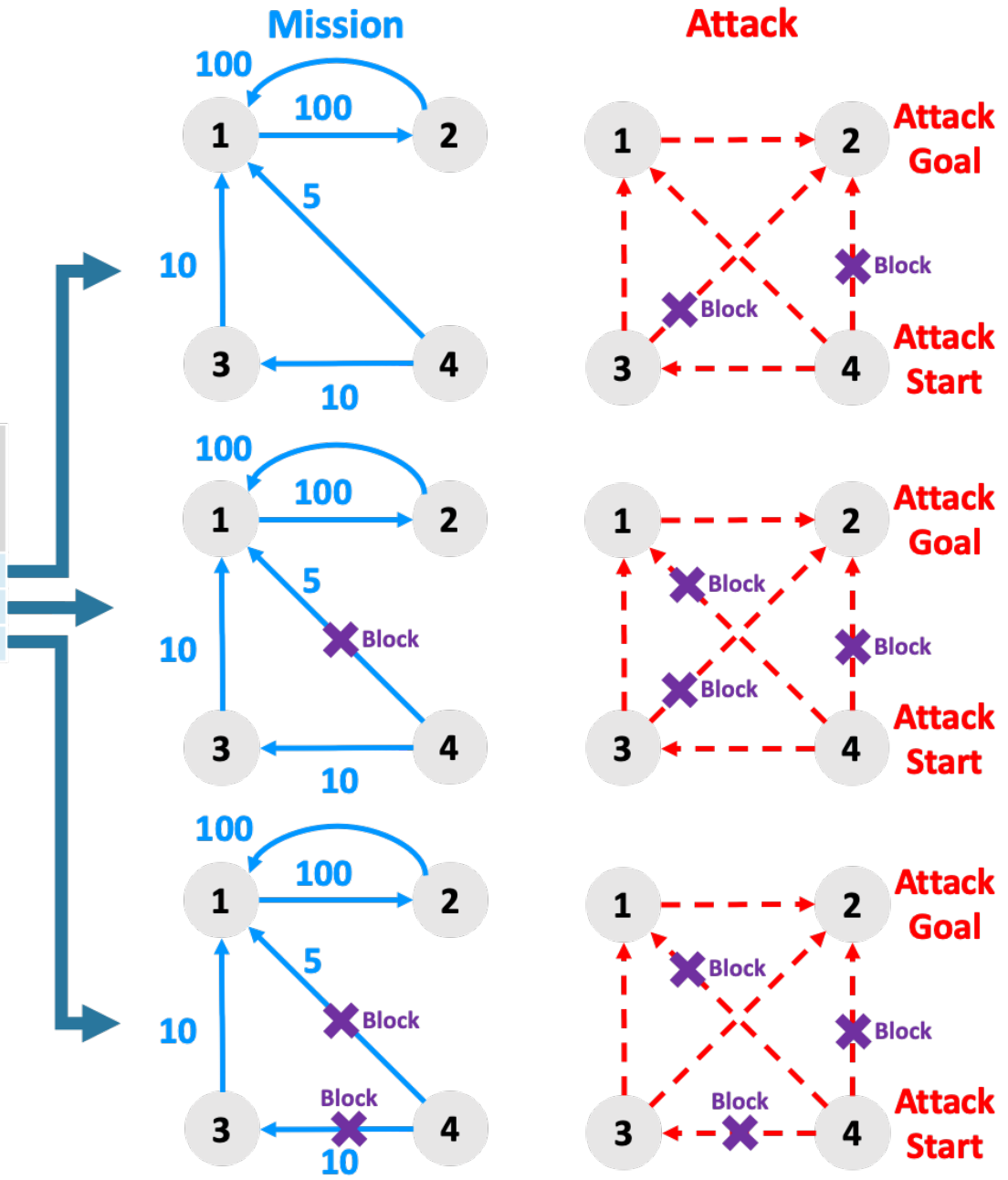
Scoring Candidate Solutions

Policy (With Host-to-Host Impact)					Total Mission Impact	Blocked Shortest Paths			Blocked Edges	
$p_{3,1}$ (10)	$p_{3,2}$	$p_{4,1}$ (5)	$p_{4,2}$	$p_{4,3}$ (10)		Length 1	Length 2	Length 3		
0	0	0	0	0	25	1	2	1	5	
0	0	0	0	1	15	1	2	1	4	
0	0	0	1	0	25	0	2	1	4	
0	0	0	1	1	15	0	2	1	3	
0	0	1	0	0	20	1	1	1	4	
0	0	1	0	1	10	1	1	1	3	
0	0	1	1	0	20	0	1	1	3	
0	0	1	1	1	10	0	1	1	2	
0	1	0	0	0	25	1	2	1	4	
0	1	0	0	1	15	1	1	1	3	
0	1	0	1	0	25	0	2	1	3	
0	1	0	1	1	15	0	1	1	4	
0	1	1	0	0	20	1	1	1	3	
0	1	1	0	1	10	1	0	1	2	
0	1	1	1	0	20	0	1	1	2	
0	1	1	1	1	10	0	0	1	1	
1	0	0	0	0	15	1	2	1	4	
1	0	0	0	1	5	1	2	0	3	Pareto Front
1	0	0	1	0	15	0	2	1	3	
1	0	0	1	1	5	0	2	0	2	
1	0	1	0	0	10	1	1	1	3	
1	0	1	0	1	0	1	1	0	2	Pareto Front
1	0	1	1	0	10	0	1	1	2	
1	0	1	1	1	0	0	1	0	1	
1	1	0	0	0	15	1	2	1	3	Pareto Front
1	1	0	0	1	5	1	1	0	2	
1	1	0	1	0	15	0	2	1	2	
1	1	0	1	1	5	0	1	0	3	
1	1	1	0	0	10	1	1	1	2	
1	1	1	0	1	0	1	0	0	1	
1	1	1	1	0	10	0	1	1	1	
1	1	1	1	1	0	0	0	0	0	



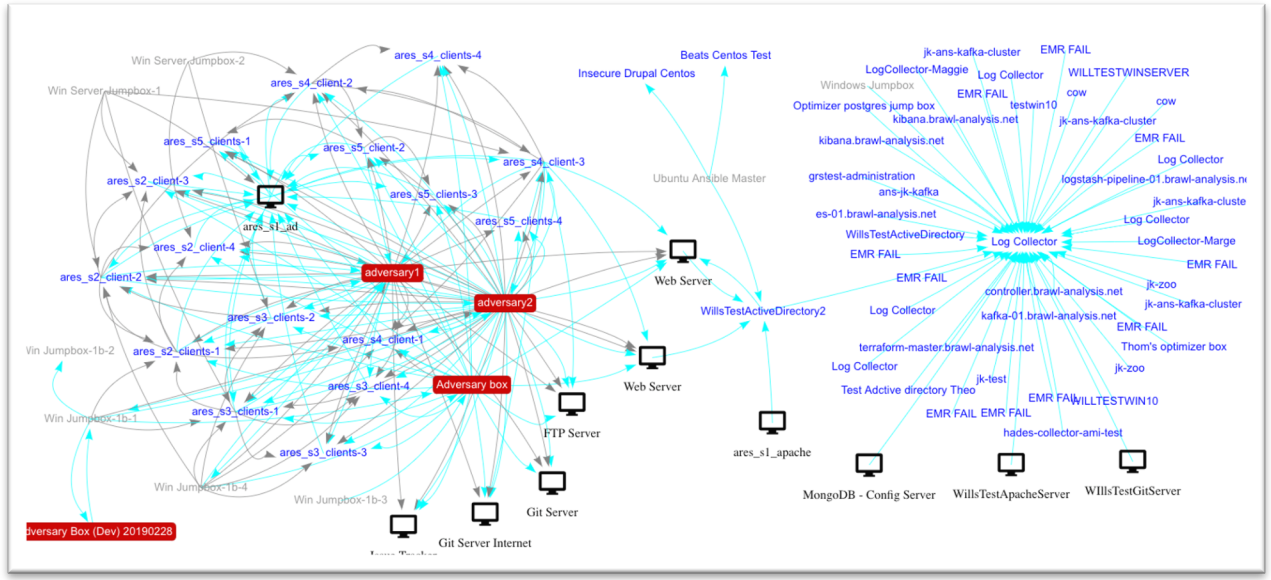
Pareto Optimal Solutions

Policy (With Host-to-Host Impact)					Total Mission Impact	Blocked Shortest Paths			Blocked Edges
$p_{3,1}$ (10)	$p_{3,2}$	$p_{4,1}$ (5)	$p_{4,2}$	$p_{4,3}$ (10)		Length 1	Length 2	Length 3	
1	0	1	0	1	0	1	1	0	2
1	0	0	0	1	5	1	2	0	3
1	1	0	0	0	15	1	2	1	3

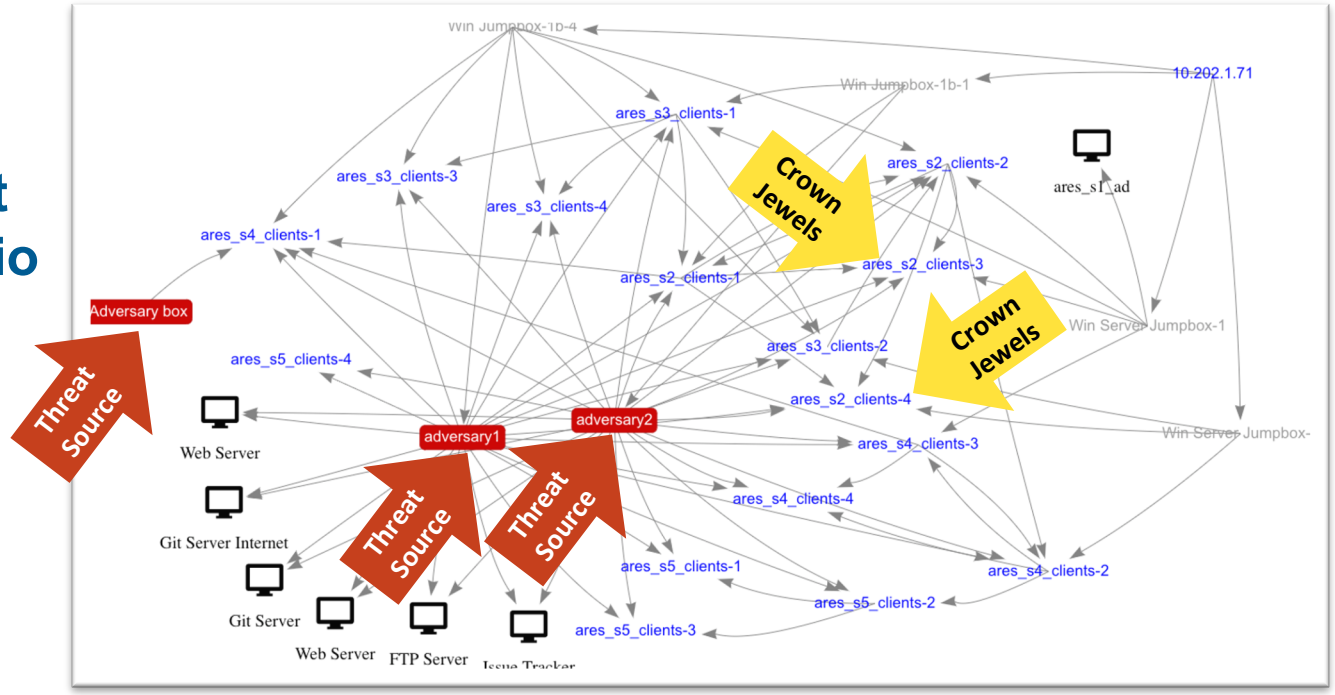


Baseline Policy For Testbed Network

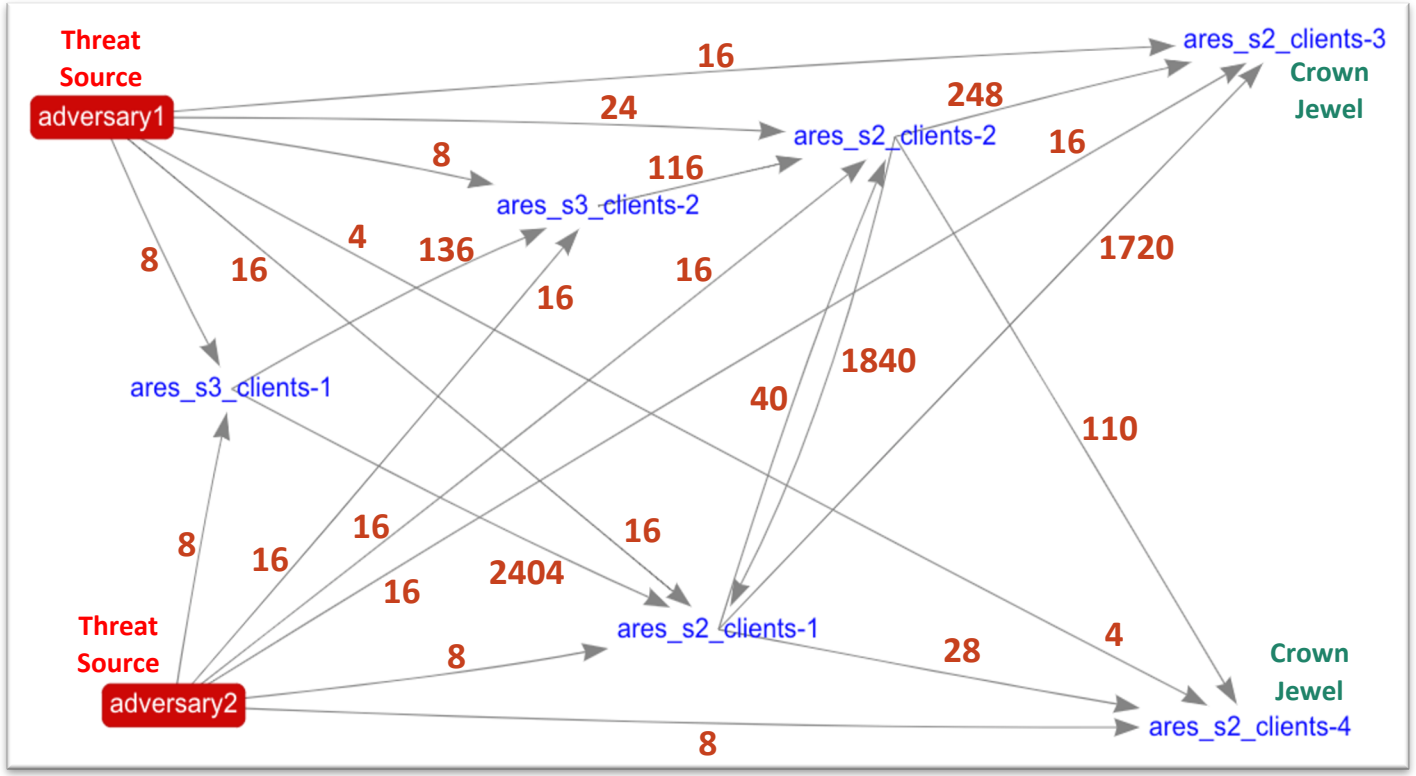
Observed Network Flows



Threat Scenario

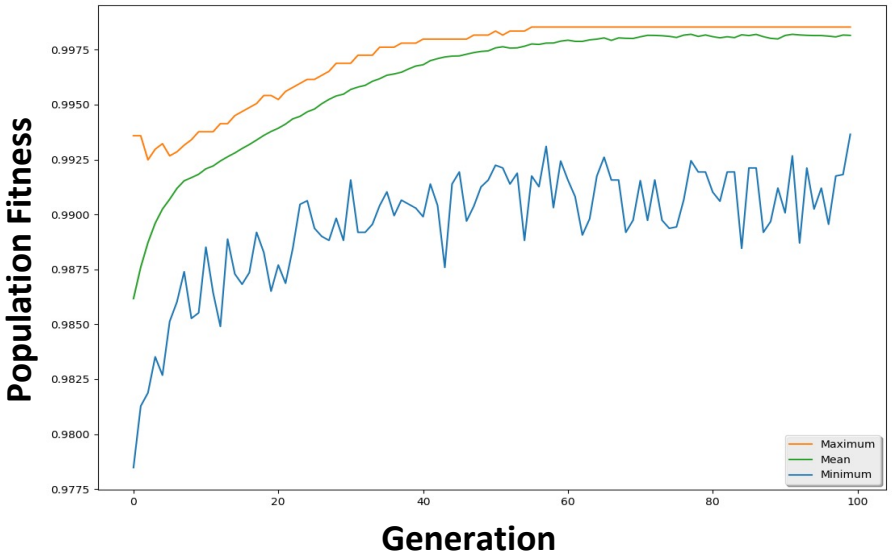


Optimizing Policy Over a Threat Scenario

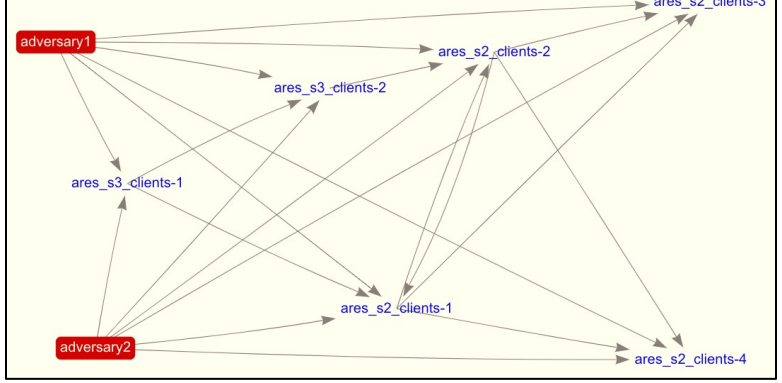


Threat Scenario

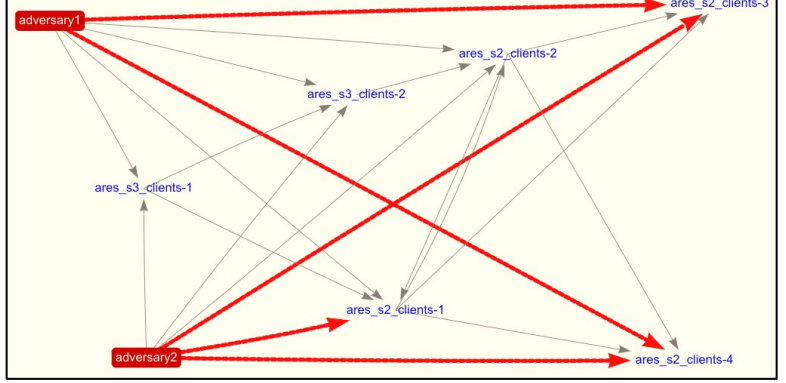
Genetic Algorithm Evolution



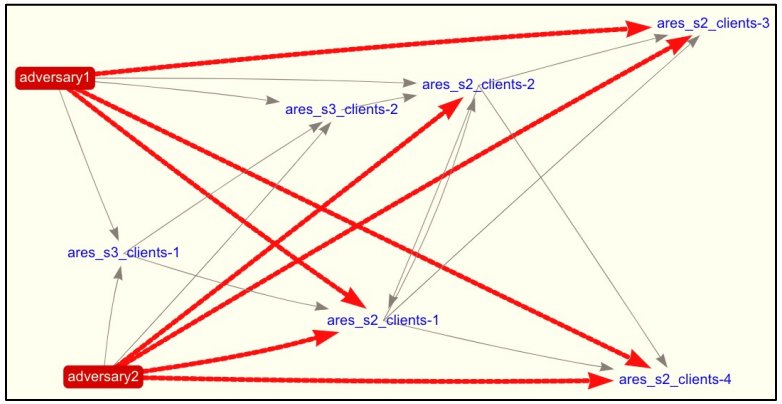
Optimal Solutions For Different Mission vs Threat Tradeoff



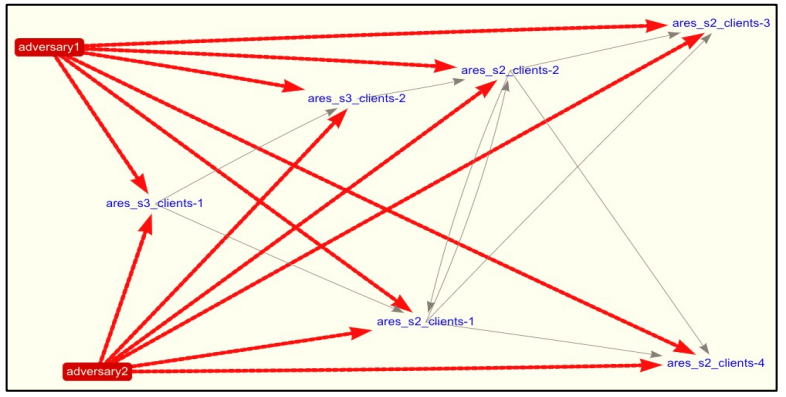
Mission Accessibility: 100%



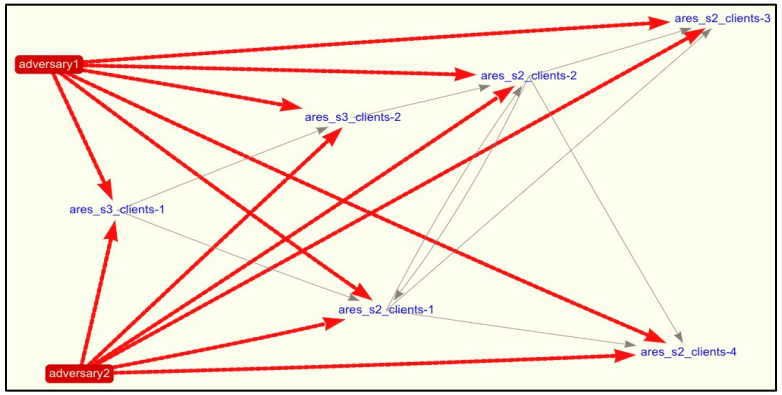
75%



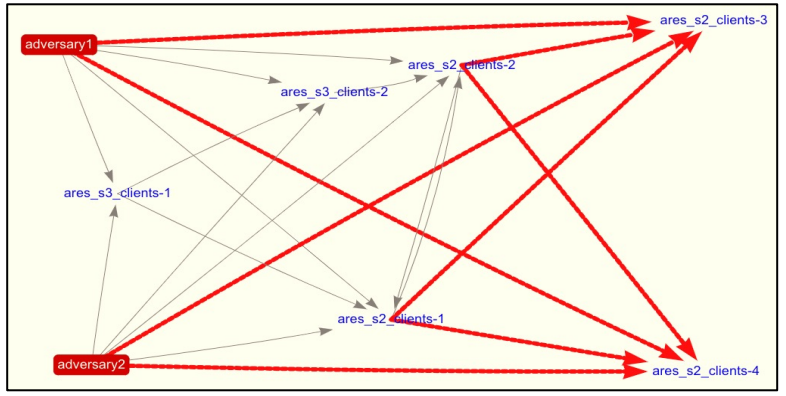
62.5%



50%

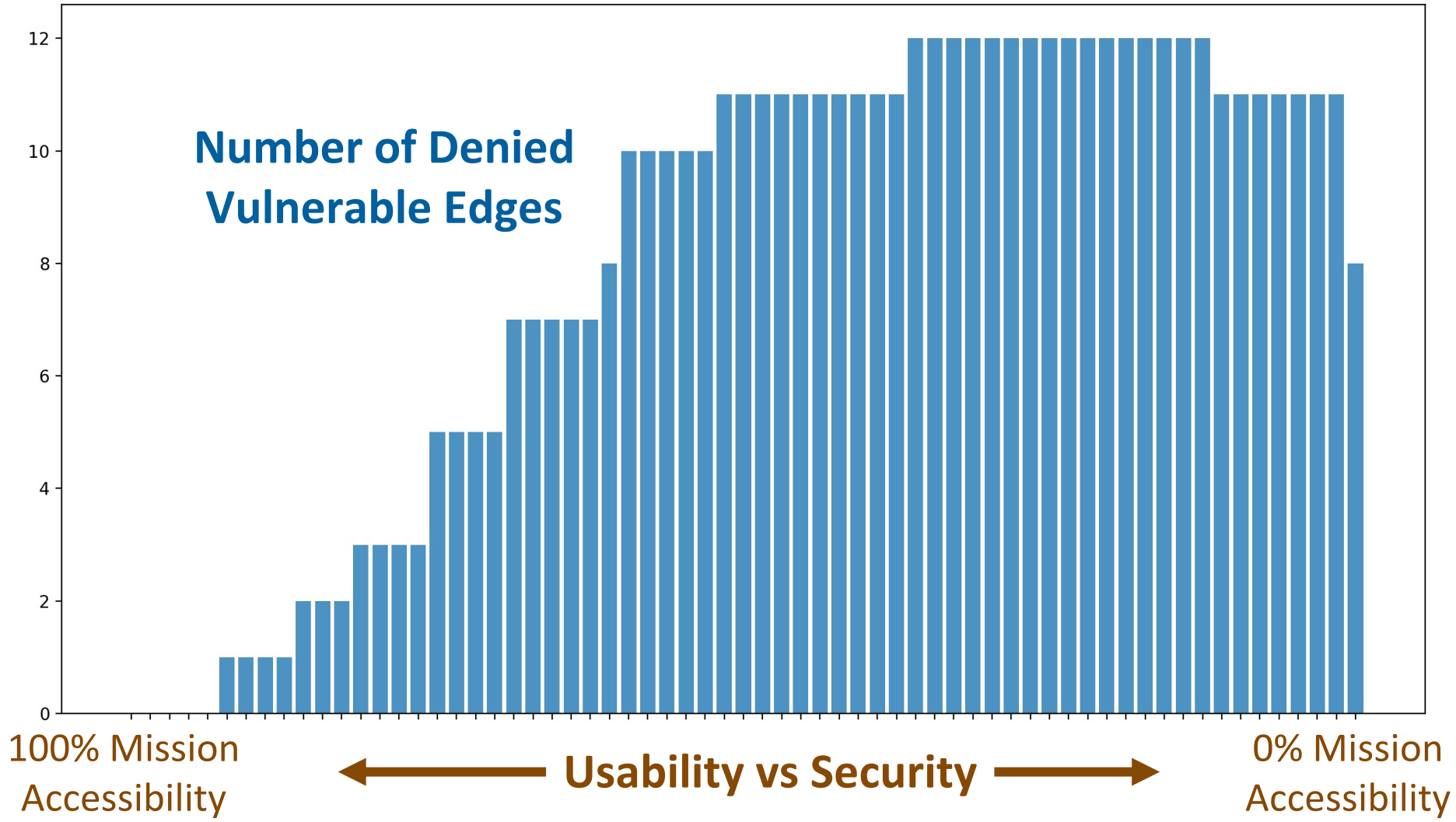


25%



0%

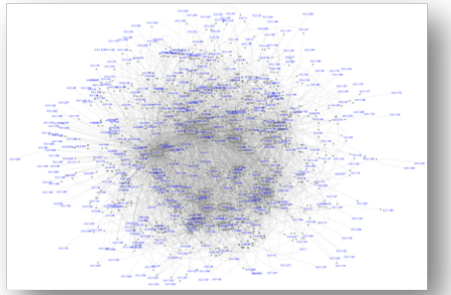
Full Range of Tradeoff between Mission and Threat



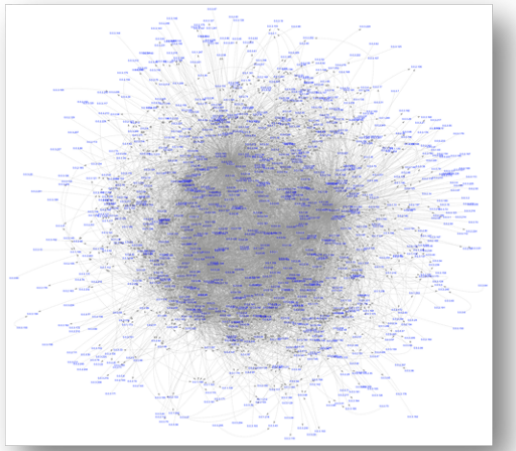
Scalability

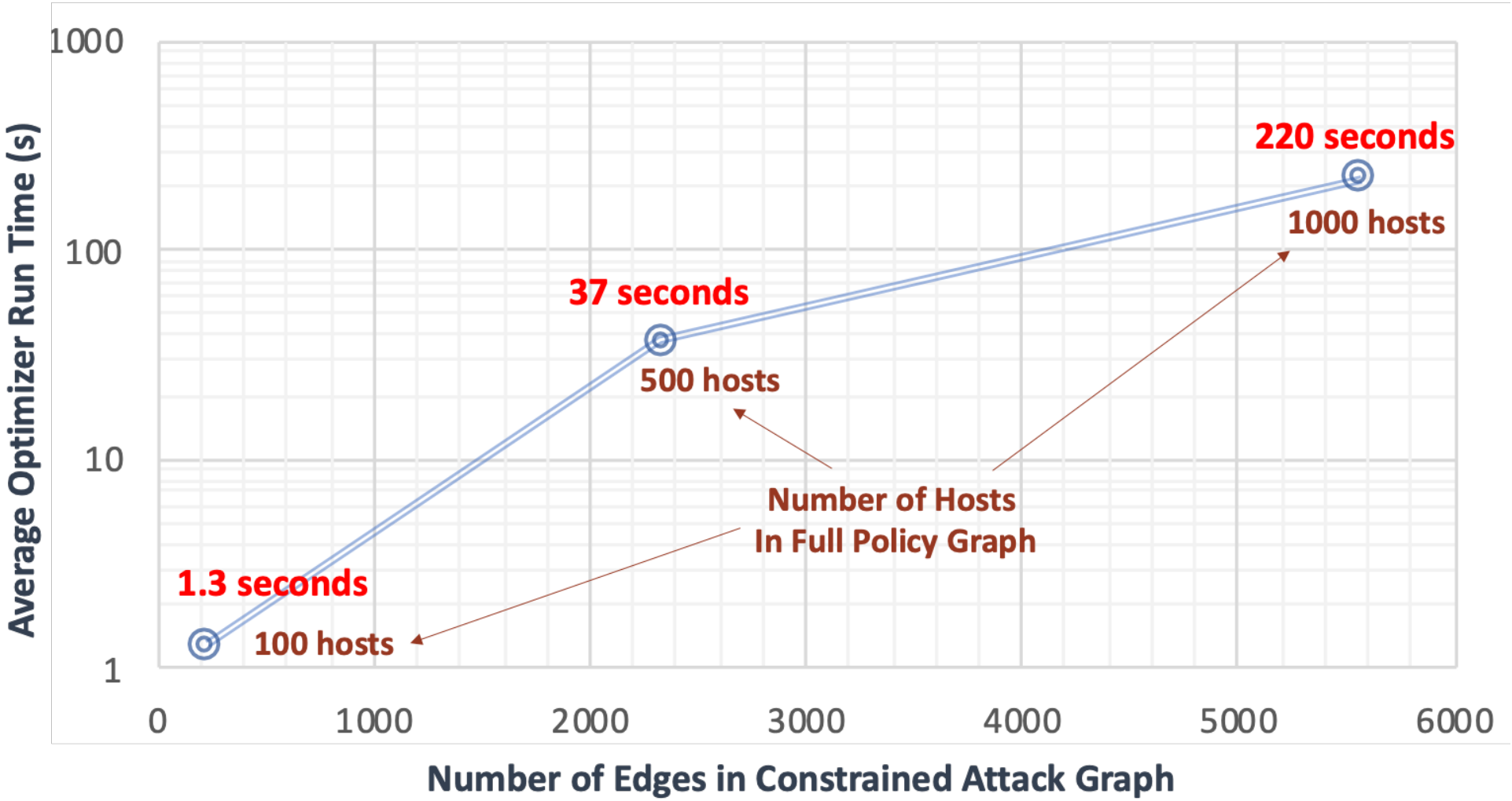
100 hosts

500 hosts



1000 hosts





Synthesized based on data distributions
from testbed network (74 hosts)

Summary

- Optimization of microsegmentation policy for a network, with tunable tradeoffs between security and mission
  - Maximize adversary effort in exploitation steps (block shorter paths)
  - Maximize accessibility to critical network resources
- Genetic algorithm to find optimal policy
  - Candidate solutions as individuals in evolving population
  - Fitness function for security/mission tradeoff
- Baseline for MITRE Adaptive Resiliency Experimentation System (ARES), which jointly optimizes microsegmentation, authentication, policy generalization, redundancy, deception, and zero-trust architecture for adaptive intelligent cyber resiliency

Steven Noel, PhD

snoel@mitre.org

https://www.linkedin.com/in/snoel1/

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD