SAND2017-8828PE

A Stochastic Programming Approach to the Design Optimization of Layered Physical Protection Systems

Nathanael Brown, Katherine Jones, Alisa Bandlow, Lucas Waddell, and Linda Nozick

Sandia National Laboratories and Cornell University

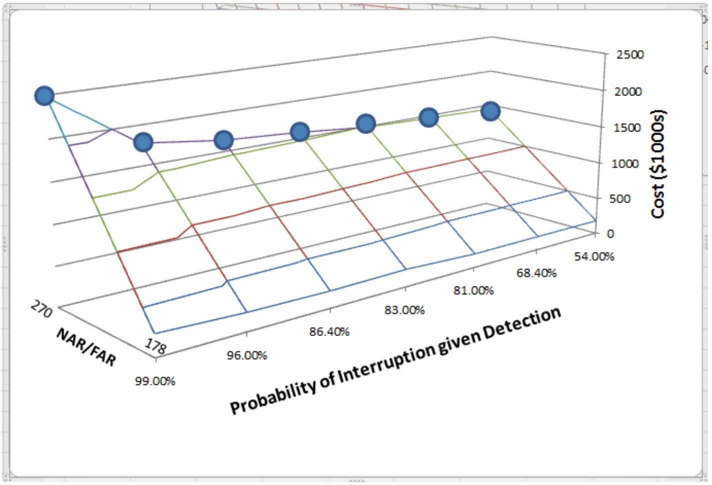
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND NO. 2017-XXXX C

Optimization for Risk Analysis

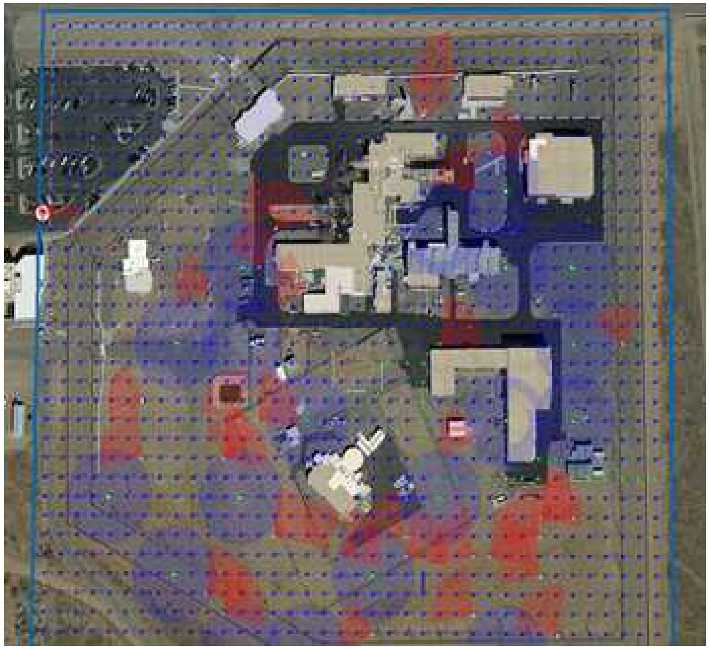
- Research project was focused on likelihood of adversary success given an attack, not analyzing the likelihood of attack or consequence evaluation.
- Optimization model helps compare different risk mitigation strategies and includes representation of attacker strategy given those mitigations.
- Instead of an event tree or fault tree, represent all possible paths the attacker could take and use 1) probability of detection and 2) uncertain travel time at points along the paths to determine likelihood that the attacker reaches their target before interception, and trade off that likelihood against other metrics (cost, nuisance/false alarms)
- For integrated 3S analysis, useful to think about PRA extensions which:
  - Incorporate attacker capability and strategy in different environments
  - Use optimization or simulation optimization to recommend mitigation strategies that best represent the risk preferences of stakeholders (for example, balancing security and safety risk)

Research Goals

- Create a mathematical framework to represent a multi-layered security system as a complex system
- Provide insight into the trade-off between performance and cost



- Requires:
  - Model of security architecture of a Physical Protection System (PPS)
  - Representation of intruder behavior
  - Consideration of Nuisance Alarm/False Alarm Rates (NAR/FAR) and impact on Alarm Station Operators (ASOs)
  - Optimization to estimate triple objective trade-off frontier



Previous Work Referenced

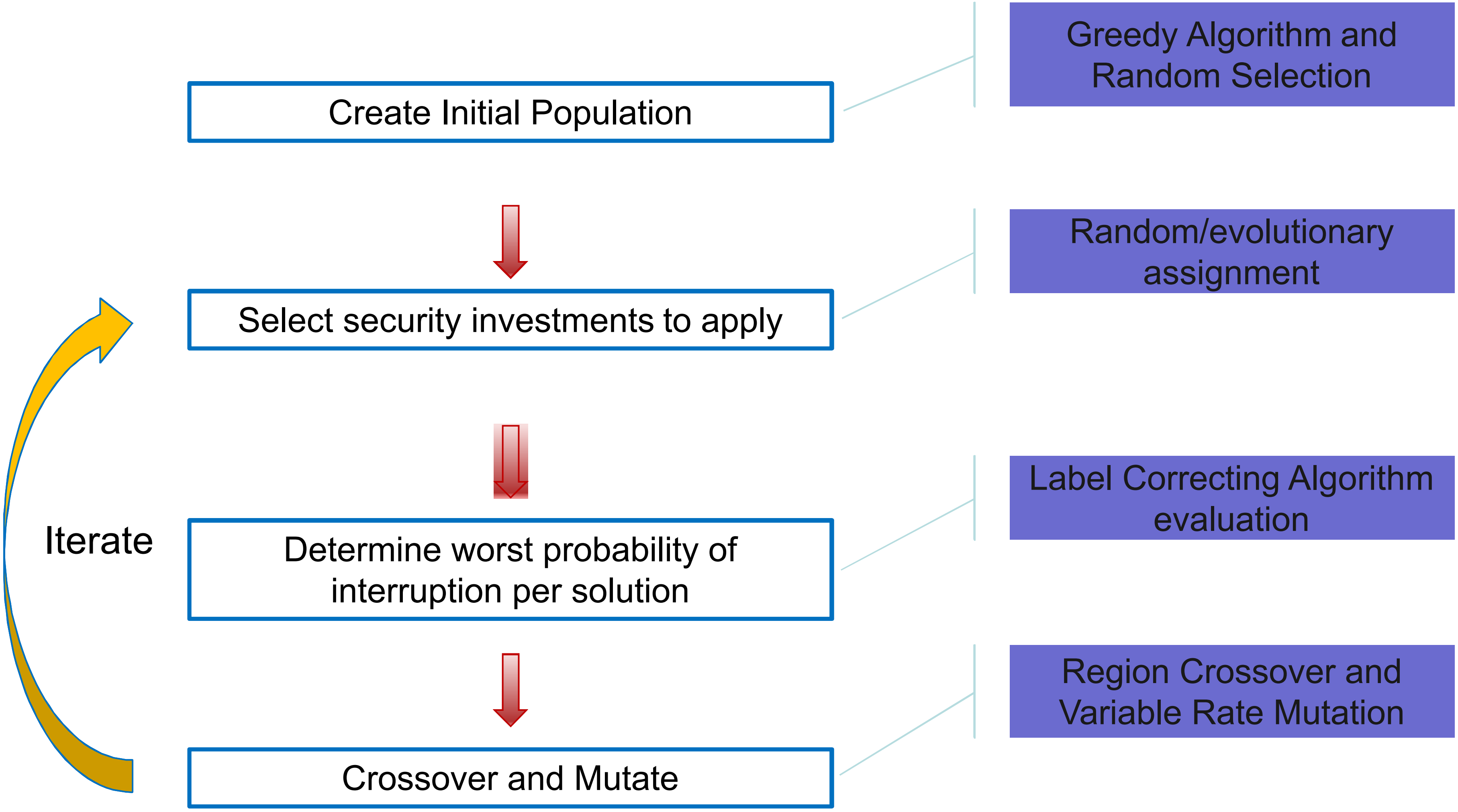
- Bennett, H.A., The "EASI" Approach to Physical Security Evaluation (NUREG-760145), U.S. Nuclear Regulatory Commission, Washington, D.C., 1977.
  - Seminal work which defines calculation for probability of interruption (P_I)
- Garcia, M., The Design and Evaluation of Physical Protection Systems, Butterworth-Heinemann, Oxford, 2007.
  - Describes established approach to evaluating a PPS (Physical Protection System) using adversary sequence diagrams (ASDs) which describe the layers of protection that the attacker must pass through in order to reach a target
- Jang, S., S. Kwak, H. Yoo, J. Kim, and W. Yoon, Development of a Vulnerability Assessment Code for a Physical Protection System: Systematic Analysis of Physical Protection Effectiveness (SAPE), *Nuclear Engineering and Technology*, 41(5), 2009.
  - Develops a shortest path algorithm to determine the MVP (Most Vulnerable Path) in a security system

Investment Optimization

- **Intruder goal**: Minimize the probability that the time remaining after detection will exceed the response time of the protective force (probability of interruption)
- **System owner goal**: Maximize the probability that the intruder will be interrupted given that the intruder can adapt to different investment strategies
- **System owner decision**: What technologies and physical barriers to invest in and where to place them subject to budget and false alarm rate limits

http://levgrossman.com/tag/spy-vs-spy/

Defender Investment Optimization



Create Initial Population

Select security investments to apply

Determine worst probability of interruption per solution

Crossover and Mutate

Iterate

Greedy Algorithm and Random Selection

Random/evolutionary assignment

Label Correcting Algorithm evaluation

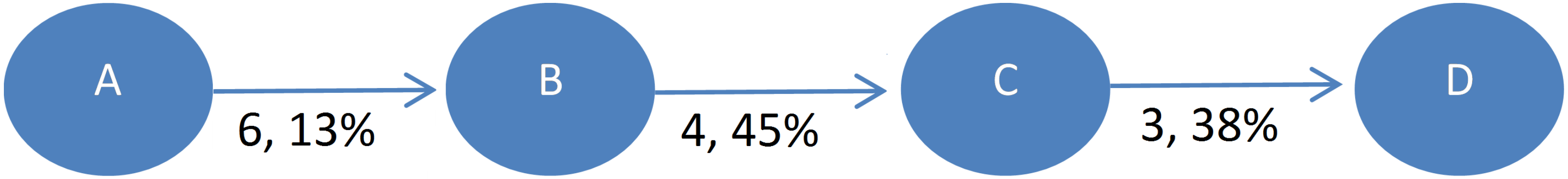
Region Crossover and Variable Rate Mutation

Creating a (more) Realistic Model

Characteristic	Simplified Model	Realistic Model	Impact
Response force/ intruder travel times	Constant	Variable (Gaussian)	Addresses uncertainty; Gaussian improves computational efficiency
Lighting/weather effects	None	Decreases sensor detection probability	Improves system resiliency to multiple environmental scenarios
Effect of NAR/FAR on ASOs	None	Longer assessment time (increased response force time)	Realistic NAR/FAR degradation with mitigation strategy
Variable Intruder Capabilities	None	Intruders can degrade certain sensors/barriers	Improves system resiliency to multiple intruder types

Intruder path selection – Constant vs. Variable Time

- Intruder's objective is to minimize the probability of interruption (P_I) which is the probability that the delay time after detection exceeds the response force time (RFT)



- If RFT is 6 minutes and *constant*, detection on link C-D leaves insufficient time to respond (and hence is irrelevant)

$$P_I = P_{D(AB)} + \overline{P}_{D(AB)} {}^{*} P_{D(BC)} = 0.13 + (1-0.13)*0.45 = 0.52$$

- If RFT is 6 minutes and *Gaussian* with link travel times that are also *Gaussian*, must consider all links

$$P_I = P_{D(AB)} {}^{*} P(RFT<T_{AD}) + \overline{P}_{D(AB)} {}^{*} P_{D(BC)} {}^{*} P(RFT<T_{BD}) + \overline{P}_{D(AB)} {}^{*} \overline{P}_{D(BC)} {}^{*} P_{D(CD)} {}^{*} P(RFT<T_{CD})$$

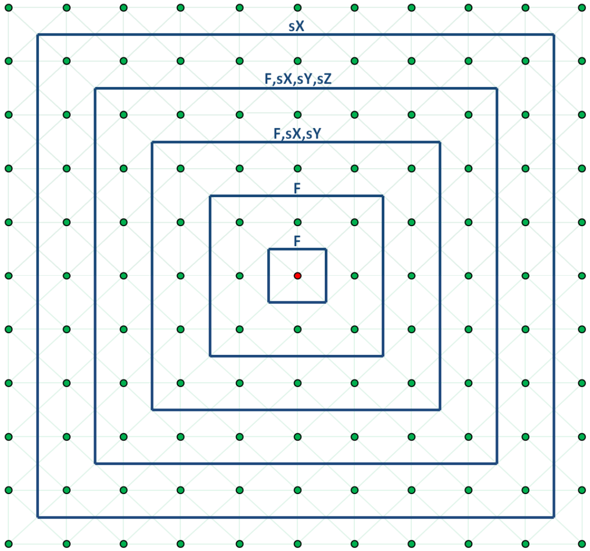
$$P_I = 0.44 \text{ (15\% standard deviation)}$$

Accounting for Alarm Queueing

- If NAR/FAR is high enough, ASOs (Alarm Station Operators) won’t be able to process alarms “immediately”
  - ASOs will also likely not respond as quickly to alarms that are perceived as unreliable (trust lag time)
  - The *effective* RFT is increased by alarm queue time plus assessment time
- Probability of Interruption becomes:
  - $P_{\mathrm{I}} = D_1 P(T_1) + \sum_{i=2}^{n} D_i P(T_i) \prod_{j=1}^{i-1} (1 - D_j)$
- Where
  - $P(T_i) = P(T_{R+AS} < T_{AT}) = \varphi \left[\frac{\sum_{j \geq i} \mu_j - (\mu_R + \mu_{AS})}{\sum_{j \geq i} \sigma_j^2 + (\sigma_R^2 + \sigma_{AS}^2)} \right]$
  - D_i = probability of detection on link i
  - R = Response Force Time (RFT)
  - AS = ASO assessment time plus queue time
  - AT = Attacker travel time

Accounting for Multiple Scenarios

- Create multiple environmental effects (e.g., day, night, precipitation) which lowers the P_D (probability of detection) of certain sensors
- Allow "smart" intruders to degrade certain sensors (decrease the P_D) and/or barriers (decrease travel time)
- Optimization evaluates a candidate architecture against all scenarios to determine the worst case P_I and best complementary investments
- A naïve designer might choose to create an "average" architecture which uses the average sensor/barrier values (across all scenarios) to conduct a single scenario optimization

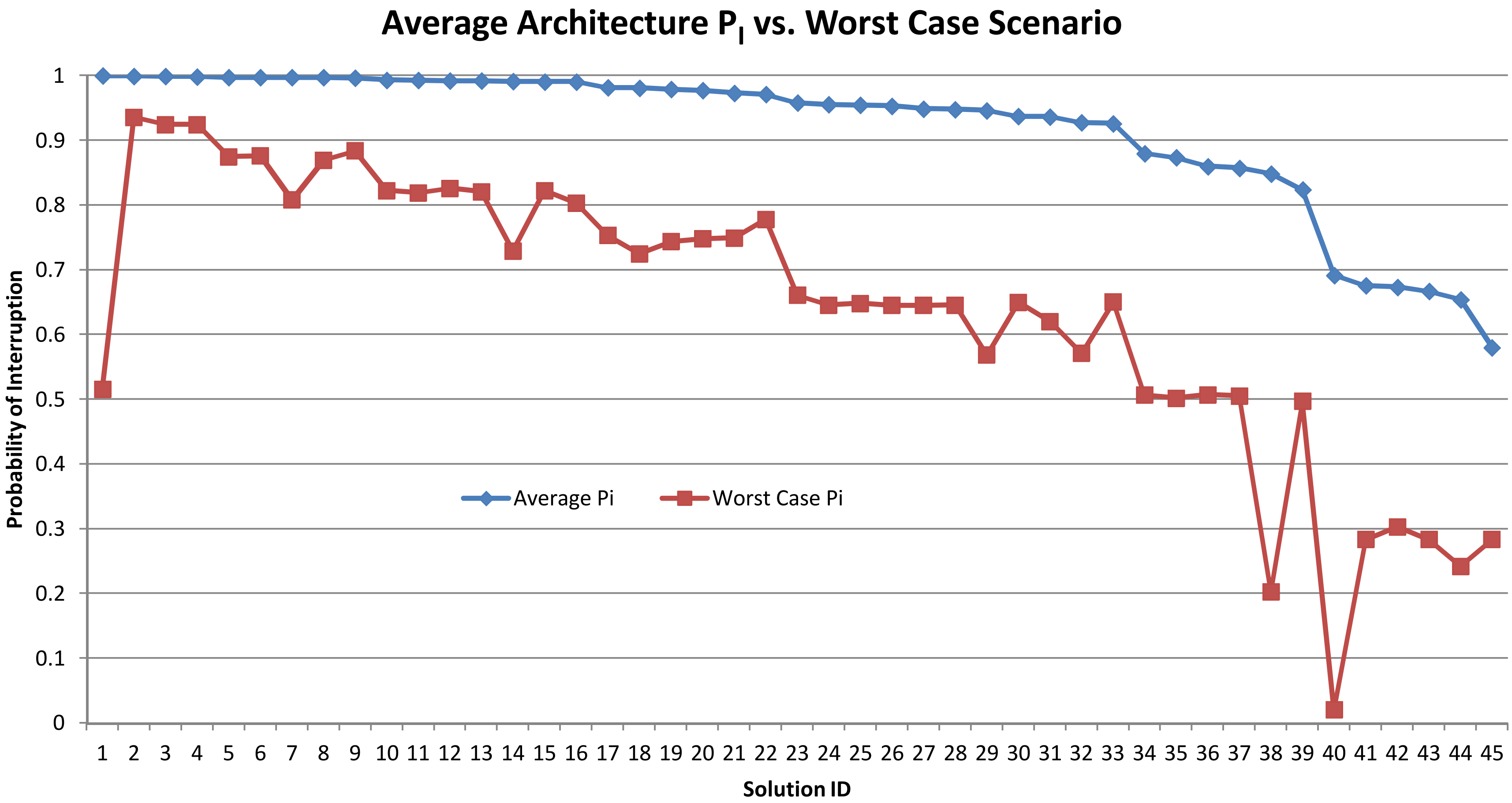


Notional Security Architecture

Results

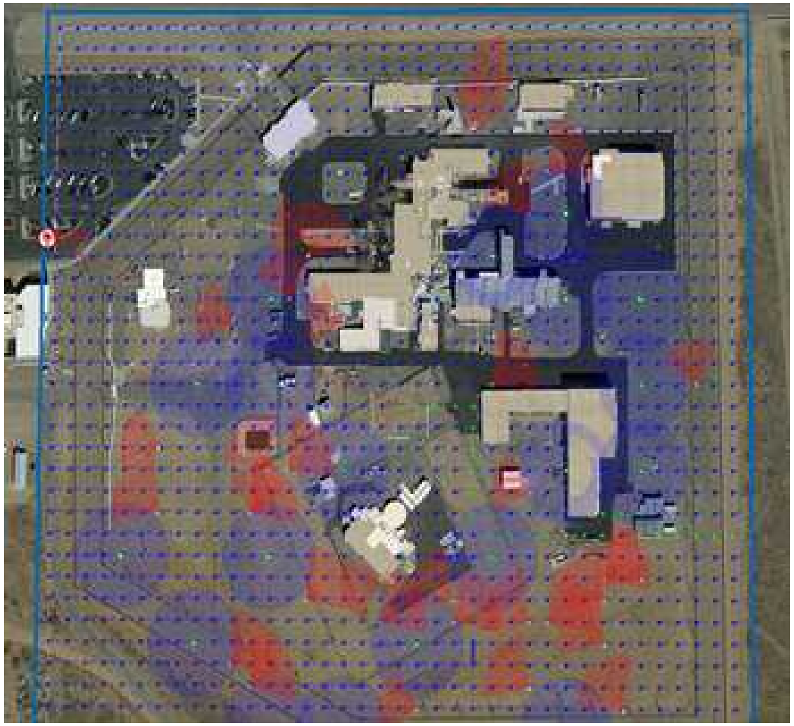
Average Architecture Optimization

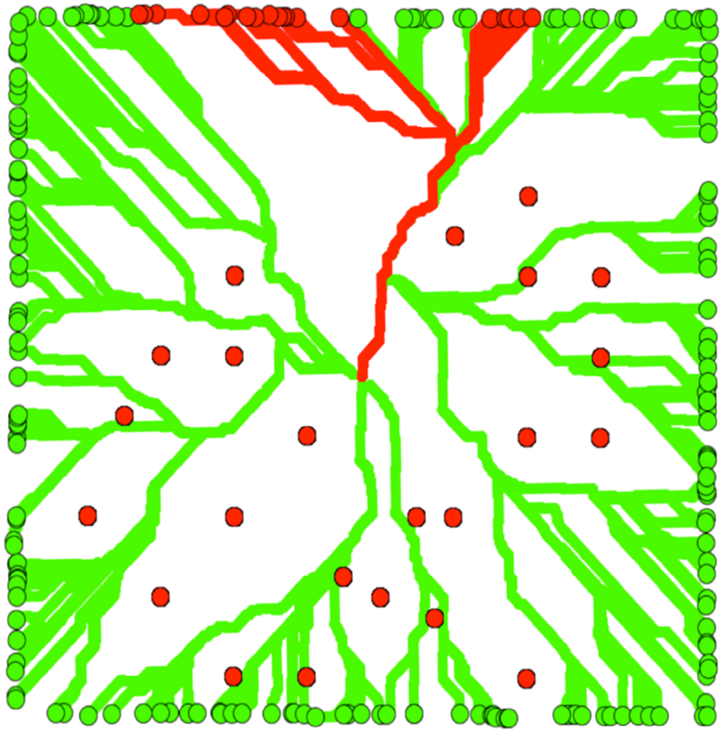
- Run single-scenario optimization against “average” architecture
  - Technology parameters have average value across all scenarios
- Average architecture performs poorly against worst case scenario



Validation: Dante Simulation from MLS Input

- Use solutions from MLS engine to seed Dante scenarios
  - Perform batch analyses on solutions with random start positions for attacker
  - Allow human-in-the-loop to adjust scenarios for further examination
  - Comparison of P_I simulated value is within 1-2% of MLS calculation





Summary

- Use an adaptive game-theoretic approach combined with stochastic optimization, so that the PPS design changes based on varying conditions and available options
- Create designs that are symmetric with respect to P_I even when the physical layout is asymmetric
- Provides greater resiliency to variable:
  - Travel/response times
  - Environmental effects
  - Intruder behavior and/or abilities
  - ASO (Alarm Station Operator) behavior
- Allows a decision maker to choose architectures that trade off performance versus cost

Backup

Case Study – Multi-Scenario vs. Average

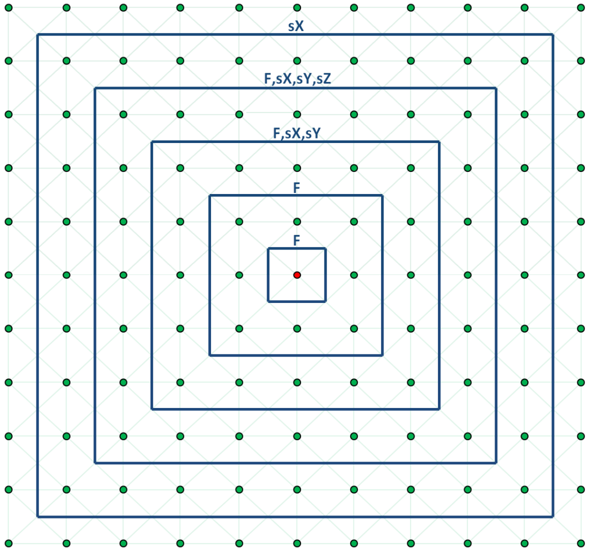
- Scenarios consist of four different environmental scenarios in combination with an intruder which is either uninformed or “smart”
- The smart intruder is able to degrade all site technologies
- Designer can choose from 3 different types of sensor (sX, sY and sZ) and 1 type of barrier (Fence) to be placed throughout the facility

Environmental Conditions	Abbreviation	Probability of Occurrence
Daytime No Precipitation	DNP	0.5
Daytime With Precipitation	DWP	0.1
Nighttime No Precipitation	NNP	0.3
Nighttime With Precipitation	NWP	0.1

Notional Environmental Scenarios

Tech.	10-year Cost ($1000s)	NAR /FAR	Average	Worst Case
sX	$100	3	0.58	0.3
sY	$200	6	0.64	0.3
sZ	$300	12	0.61	0.47
F	$3	0	51.5	30
ASO	$10,000	N/A	N/A	N/A

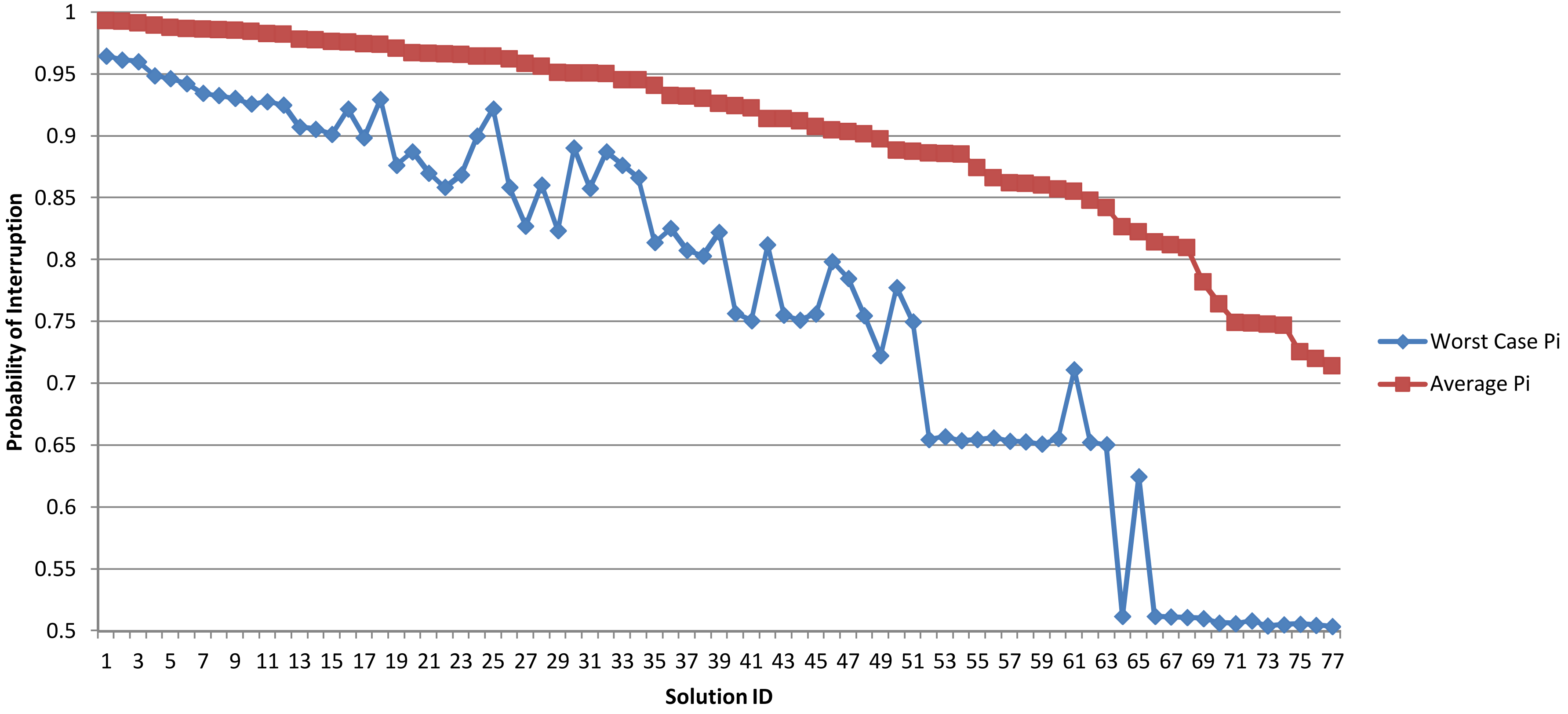
Notional Technology Investments



Notional Security Architecture

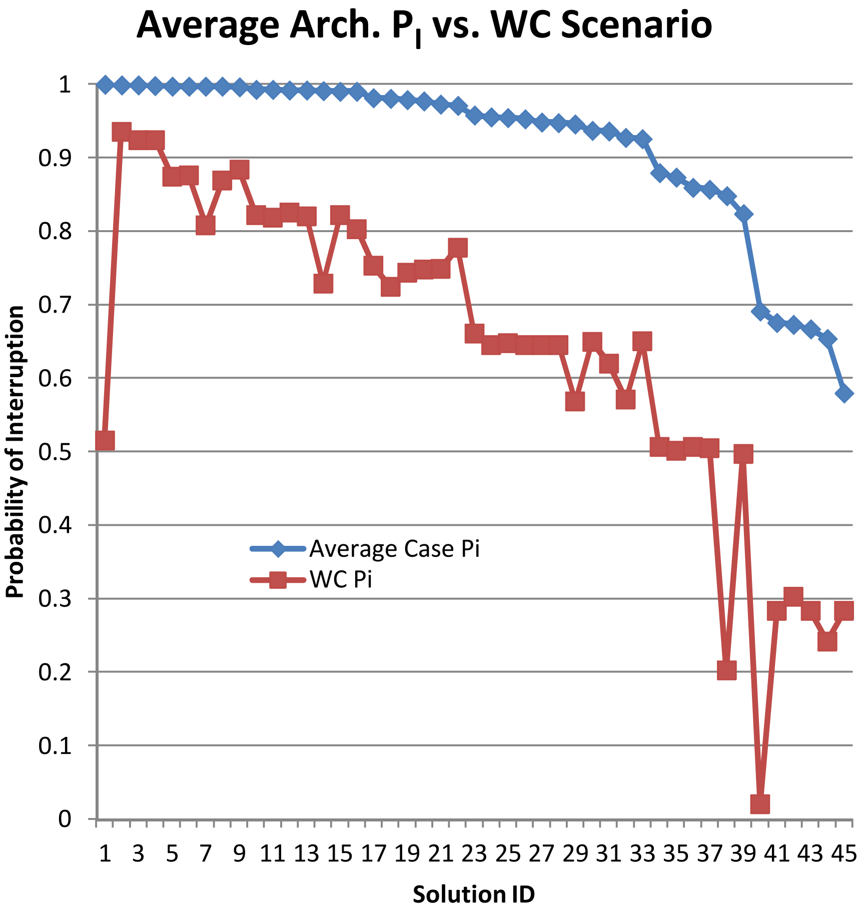
Case Study – Worst Case vs. Average

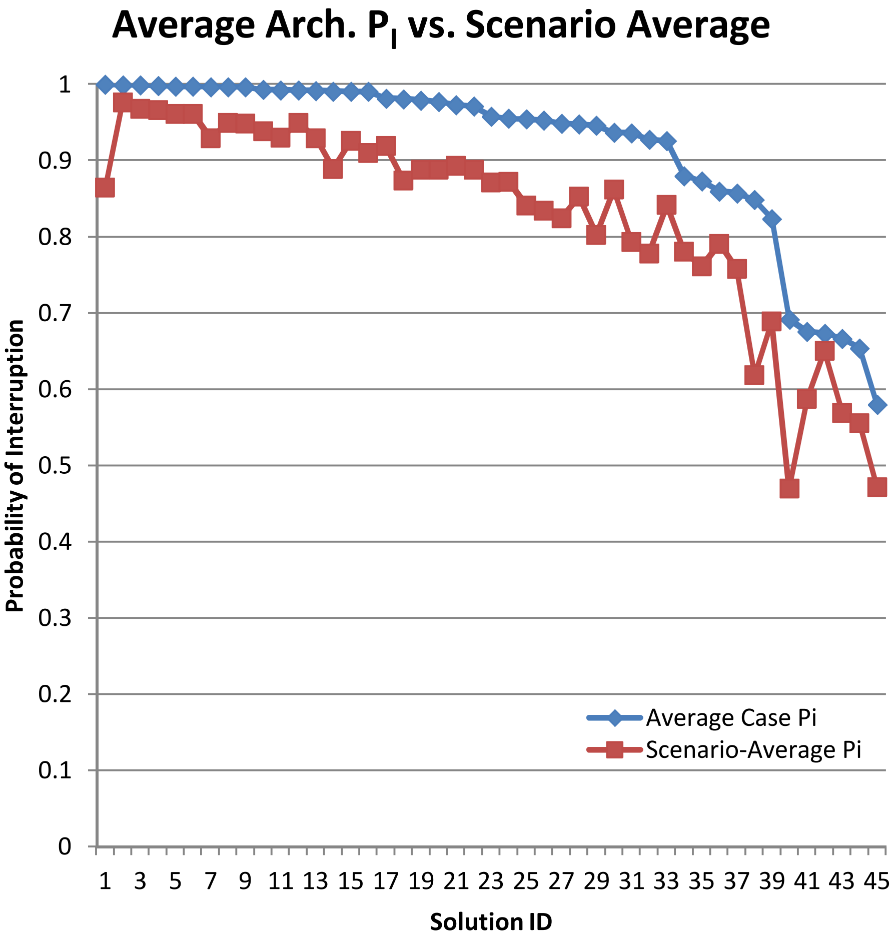
- Run multi-scenario optimization where technology parameters vary according to the scenario
- Optimize against worst case P_I (Probability of Interruption)
- Average P_I across all scenarios is higher (often substantially)



Average Architecture Optimization

- Run single-scenario optimization against "average" architecture
  - Technology parameters have average value across all scenarios
- Average architecture performs poorly against worst case scenario





Technology Attributes by Scenario

- Eight different scenarios with different sensor and barrier performance characteristics
- The “average” value is weighted by the probability of each scenario
  - Probability of each type of intruder is equally likely (50%)
  - For example, NNP with no degradation has probability 0.3*0.5 = 0.15

Notional intruder sensor/barrier degrade capabilities under different environmental conditions

	DNP		DWP		NNP		NWP		Average	Worst Case
Tech.	N	D	N	D	N	D	N	D		
sX	0.80	0.70	0.70	0.60	0.4	0.30	0.35	0. 30	0. 58	0. 30
sY	0.85	0.75	0.82	0.75	0.45	0.30	0.50	0.47	0. 64	0. 30
sZ	0.60	0.55	0.95	0.8	0.53	0.47	0.85	0.75	0. 61	0. 47
Fence	60	30	70	40	70	40	80	60	51.5	30

*Technology Impact: N = Normal, D = Degraded by Intruder