SAND2015-10299C

Exceptional service in the national interest

Sandia National Laboratories

Multi-Layered Security Investment Optimization Using a Simulation Embedded within a Genetic Algorithm

A Complex Systems Approach to More Resilient Multi-Layered Security Systems

Nathanael Brown, Katherine Jones, Linda Nozick, and Ningxiong Xu
Sandia National Laboratories and Cornell University

U.S. DEPARTMENT OF ENERGY
NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2015-10299 C

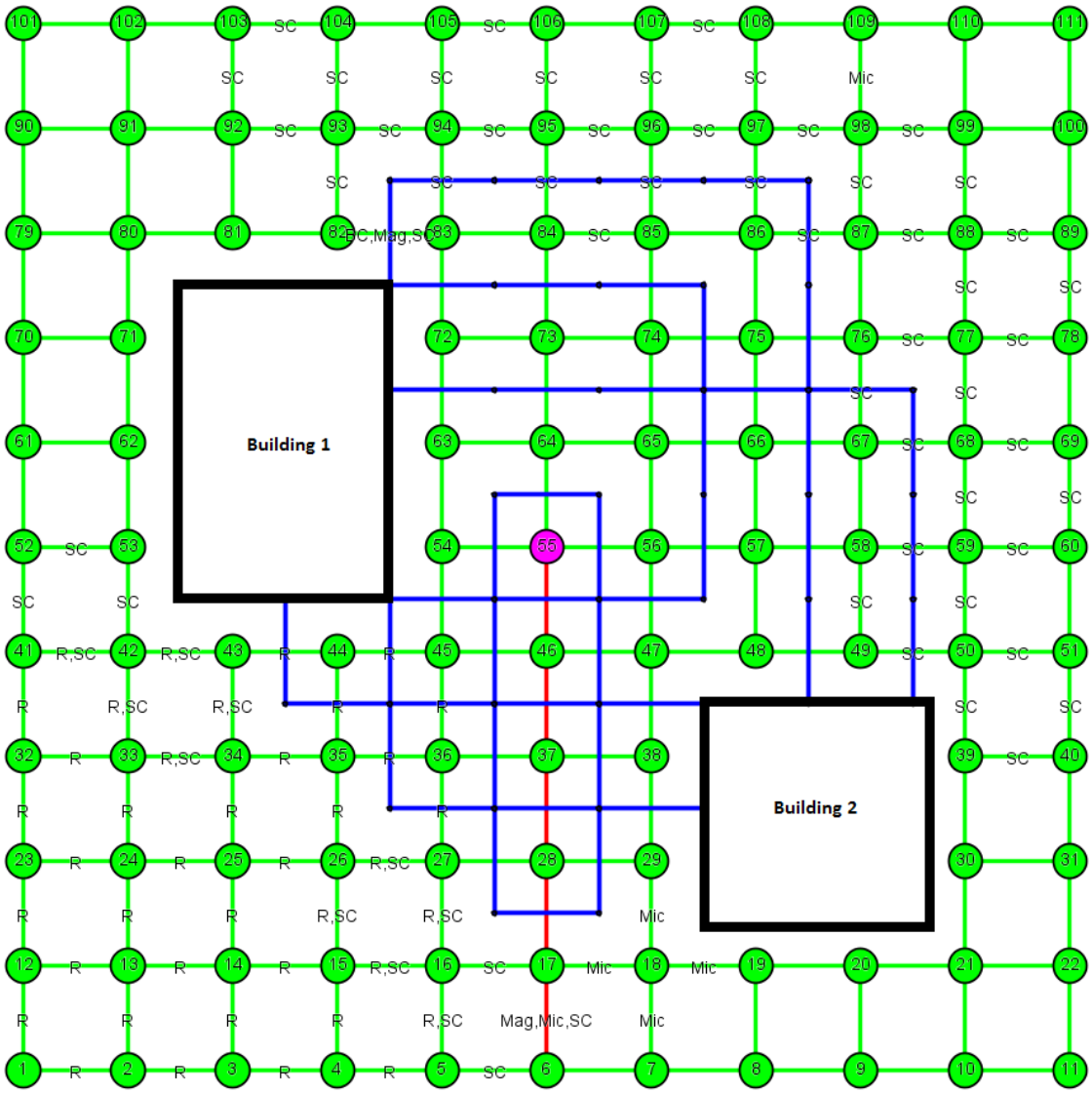
Research Goal

- 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

http://www.cleveland.com/business/index.ssf/2011/08/nuclear_security_911_firstener.html

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

0.96 Probability of Interruption Solution



notional data

Investment Optimization

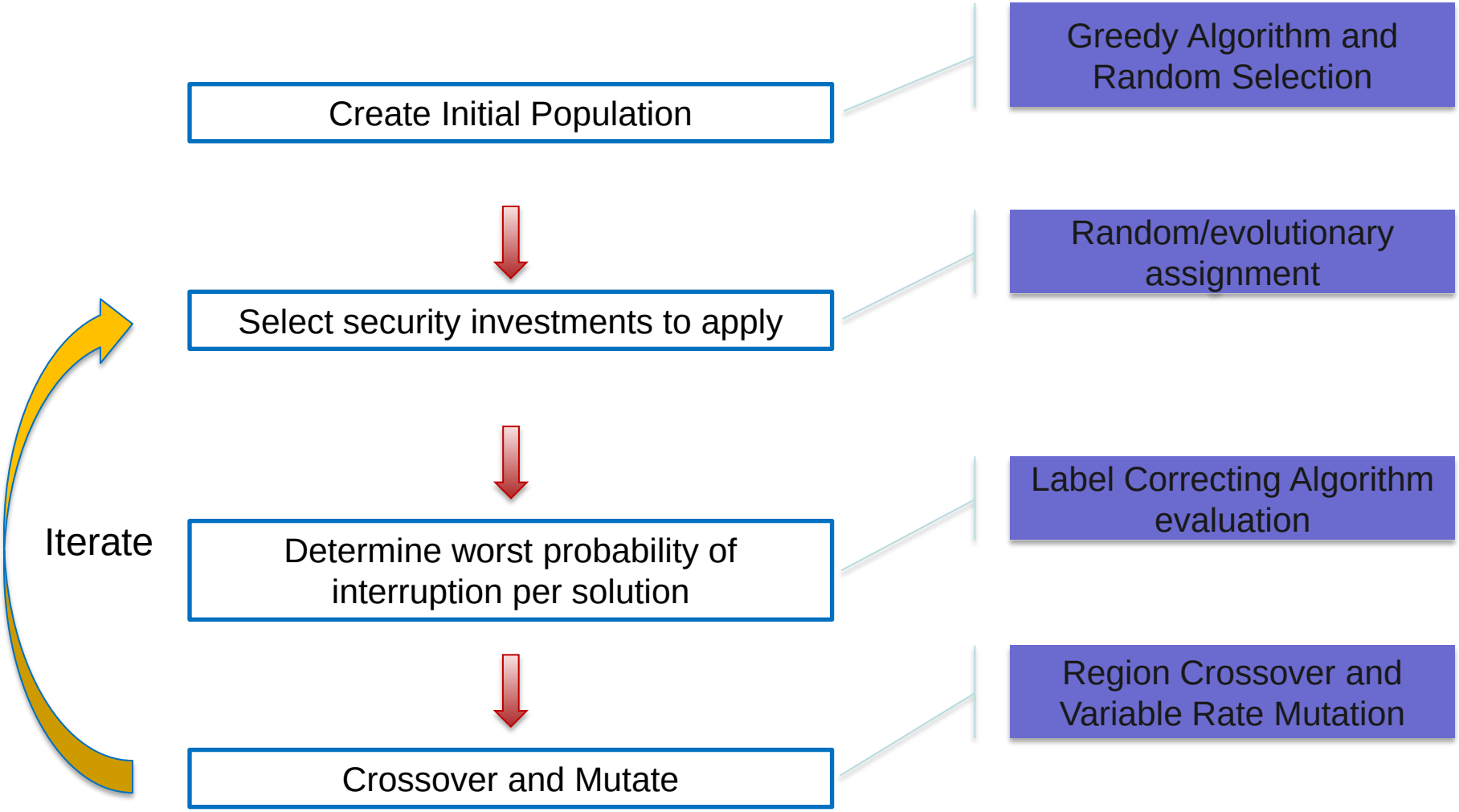
- **Intruder goal**: Minimize the probability that the time remaining after detection will exceed the response time of the protective force (probability of interruption)
- **System owner goal**: Maximize the probability that the intruder will be interrupted given that the intruder can adapt to different 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/

Genetic Algorithm (GA) – Overview

- Utilize 3 objectives: 10-year cost (minimize), NAR/FAR (minimize) and probability of being interrupted (maximize)
- Individuals are a sequence of possible investment IDs
- Each Investment is composed of:
  - Upgrade type (e.g., fence, magnetic sensor, etc.)
  - Location (node ID)
  - Affected network links
  - Can increase delay and/or probability of detection on each affected link
- Solution scenario is composed of:
  - A collection of Investment IDs where each investment is a security technology at a specific location
  - Overall cost, NAR/FAR and probability of being interrupted
  - Lowest probability of interruption path for the given package of investments
    - This is the “best” path for the intruder

Defender Investment Optimization



Initial Population Creation using Greedy Algorithm

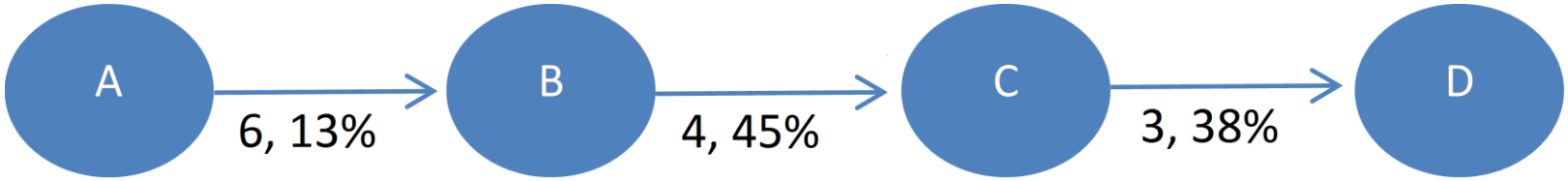
- Initial security network with no investments
- Identify the most desirable path for the intruder which has the lowest probability of interruption (P_{int}) assuming constant Response Force Time (RFT)
- Add investments to this path in order of largest incremental benefit until the minimum path characteristics are achieved
  - Min Path has delay time > RFT and $P_{int} \geq 0.9999$
  - Delay incremental benefit = [Delay(new) – Delay(init)]/cost
  - P_{int} incremental benefit = [P_{int}(new) – P_{int}(init)]/cost
- Iterate until all paths meet minimum path characteristics
  - results in symmetric investment structure
- "Clean" final solution by removing all investments that do not degrade solution below minimum P_{int}
- Randomly decimate final solution to create Pareto Frontier (PF) of derived solutions where $P_{int} > 0$

Security Investment Selection

- Fitness function is smallest Euclidean distance from any of the Pareto points using the three objective values as the solution space coordinates
- Utilize a biased random selection where points on the PF are 3 times as likely to be selected as points furthest from the PF
  - Likelihood for intermediate points varies linearly between the extremes
- Since objective values have large differences in magnitude, the initial PF is used to create normalization factors to avoid objective biasing
- Taxicab/Manhattan distance is utilized for the distance calculation in order to decrease computation time
  - Taxicab distance = 3 absolute differences and 2 additions
  - Euclidean distance = 3 multiplies, 2 additions and a square root

Intruder path selection – Constant Time

- Intruder's objective is to minimize the probability that delay time after detection exceeds the protective force response time (assumed to be constant)
- Modified Dijkstra's algorithm (Label-Correcting Algorithm) used to select the path

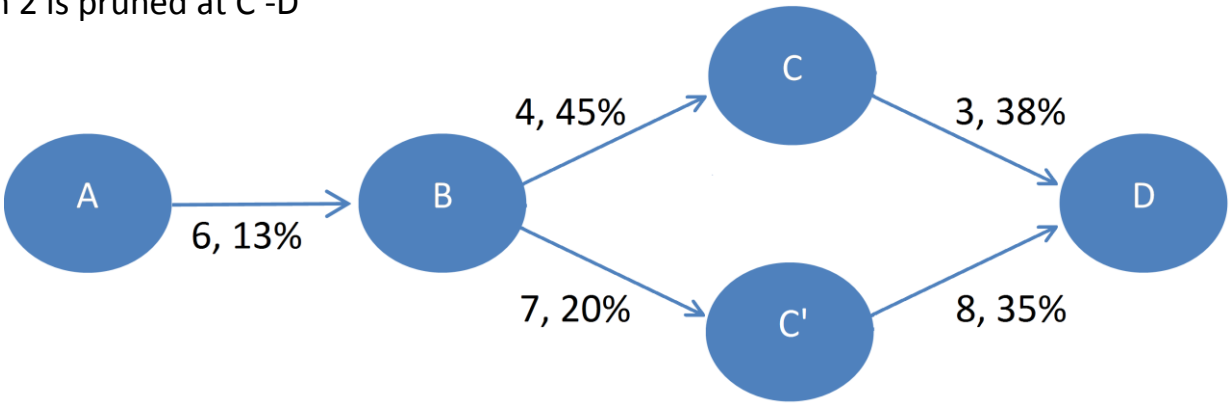


If response force time is 6 minutes, detection on the third link leaves insufficient time to respond (and hence is irrelevant)

Probability for this route is 0.13 + (1-0.13)*0.45 = 0.5215

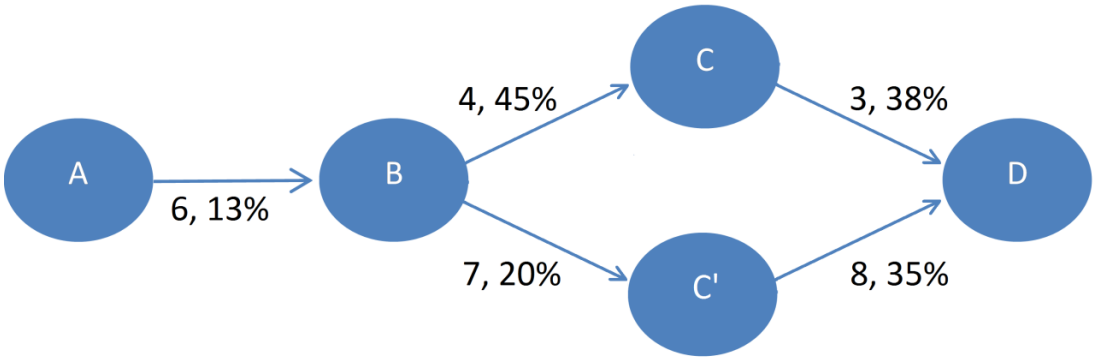
Intruder path selection – Variable Time

- Response force time (RFT) is exponentially distributed with a mean of 6
  - Probability that response time will not exceed a given path travel time *x* is 1 – exp(-x/6)
  - Probability of Interruption (P_{int}) calculation is dependent on link probability of detection (P_{det}) and probability that response time is less than path time ($P_{RFT<p}$)
- Simple network with two possible paths from A to D
  - Path 1 (A-B-C-D) or Path 2 (A-B-C'-D)
  - In each case, intruder can be detected on 1st, 2nd or 3rd link or not at all
- Probability of interruption assuming constant RFT
  - P_{int} for Path 1 = $P_{\det(A-B)} + \overline{P_{\det(A-B)}} * P_{det(B-C)}$ = 0.13 + (1-0.13)*0.45=0.5215
  - P_{int} for Path 2 = $P_{\det(A-B)} + \overline{P_{\det(A-B)}} * P_{det(B-D)}$ = 0.13 + (1-0.13)*(0.2 + (1-0.2)*0.35))=0.5476
  - Path 2 is pruned at C'-D



Intruder path selection – Variable Time (2)

- Path 1 (A-B-C-D) probability of interruption
  - P_{int} on C-D = P_{det} * $P_{RFT<3}$ = (0.38)*0.3935 = 0.15
  - P_{int} on B-D =$P_{\det(B-C)} * P_{RFT<7} + \overline{P_{\det(B-C)}} * P_{int(C-D)}$= 0.45*0.6866 + (1-0.45)*0.38*0.3935=0.3921
  - P_{int} on A-D =$P_{\det(A-B)} * P_{RFT<13} + \overline{P_{\det(A-B)}} * P_{int(B-D)}$= 0.13*0.8854 + (1-0.13)*0.3921=0.4562
- Path 2 (A-B-C'-D) probability of interruption
  - P_{int} on C'-D = P_{det} * $P_{RFT<8}$ = (0.35)*0.7364 = 0.2577
  - P_{int} on B-D =$P_{\det(B-C')} * P_{RFT<15} + \overline{P_{\det(B-C')}} * P_{int(C'-D)}$= 0.2*0.9179 + (1-0.2)*0.2577=0.3898
  - P_{int} on A-D =$P_{\det(A-B)} * P_{RFT<21} + \overline{P_{\det(A-B)}} * P_{int(B-D)}$= 0.13*0.9698 + (1-0.13)*0.3921=0.4652
- Pruning would have selected path B-C'-D which is incorrect!



Region Crossover Procedure

P1

F	F,SC	--	F
F,SC	--	F	--
--	F	--	SC

P2

F,SC	--	SC	F
F,SC	F	--	SC
--	--	F	--

C1

F	F,SC	--	F
F,SC	--	--	SC
--	F	F	--

C2

F,SC	--	SC	F
F,SC	F	F	--
--	--	--	SC

- Given 2 parent solutions (P1, P2) create 2 new child solutions (C1, C2)
- From one to four random two-dimensional regions within the network are selected, each ranging in size from 5% to 25% of the total network area
- Investments from each parent are collected within the random regions.
- Each parent has a primary child (e.g., P1 to C1) which receives all of the parent's investments *outside* of the region but *none* of the investments *within* the region.
- The investments *within* the region are then assigned such that each child receives those from its non-primary parent.

Results

Initial Pareto frontier

Greedy Initialization		
10-Year Cost (Thousands)	NAR/FAR	Probability of Interruption
1110	172	0.189
1338	186	0.192
1370	188	0.256
1382	188	0.301
1644	196	0.304
2146	240	0.336
2149	240	0.36
2337	262	0.684
2346	262	0.738
2349	262	0.81
2402	266	0.864
2438	268	0.9408
2441	268	0.96
2471	270	0.99

Random Initialization		
10-Year Cost (Thousands)	NAR/FAR	Probability of Interruption
27911	1804	0.4137
29064	1670	0.4513
26128	1806	0.4986
25782	1902	0.5765
26285	1956	0.5889
28327	1800	0.8304
27231	1810	0.8305
29132	1758	0.8368
27051	1822	0.8383
29079	1788	0.839
27573	1904	0.8391
27107	1990	0.8392
27272	1966	0.8394
27826	1866	0.8398
27830	1888	0.84
28998	1820	0.9278
27596	1940	0.9304
29186	2060	0.9336
29782	1940	0.937
29627	1986	0.9394
31075	2032	0.9528
31357	2030	0.9542
29450	2096	0.9567
36229	2480	0.9574

notional data

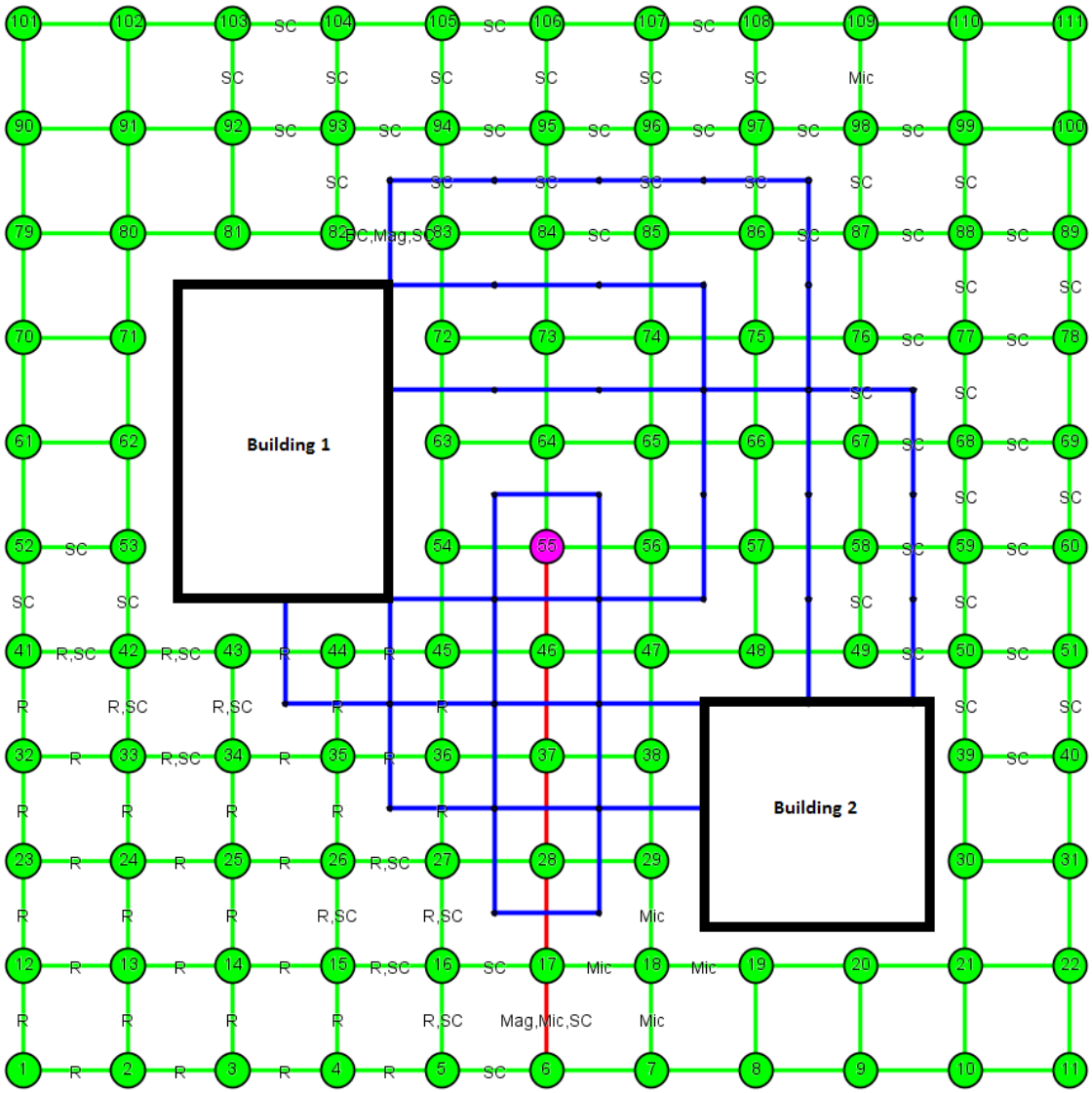
Final Pareto frontier

Greedy Initialization		
10-Year Cost (Thousands)	NAR/FAR	Probability of Interruption
1050	148	0.18
1040	156	0.18
1073	158	0.189
1106	172	0.192
1115	172	0.256
1121	172	0.304
1411	180	0.336
1426	178	0.36
1432	178	0.384
1435	178	0.464
1438	178	0.54
1462	180	0.684
1489	180	0.81
1581	224	0.83
1646	212	0.864
1781	228	0.96
2471	270	0.99

Random Initialization		
10-Year Cost (Thousands)	NAR/FAR	Probability of Interruption
90	16	0.064
630	82	0.16
510	102	0.192
750	100	0.192
820	114	0.272
1481	158	0.7232
1681	162	0.7291
2218	262	0.8292
4156	386	0.838
3297	406	0.8392
4383	356	0.8392
3417	424	0.9244
4800	410	0.9278
4003	512	0.9321
4713	476	0.9334
4950	482	0.9444
5757	488	0.9527
5670	534	0.954
5828	484	0.9565
7178	630	0.9573
35737	2464	0.9574

notional data

0.96 Probability of Interruption Solution



notional data

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	Improve system resiliency to multiple environmental scenarios
Effect of NAR/FAR on CAS operators	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 or be “stealthy”	Improve system resiliency to multiple intruder types

Backup

Simplified Investment Set (Notional)

Investment	Cost ($K)	NAR/FAR (events/day)	Detection Probability	Delay Time (minutes)
Fence	3	0	0	10
Ditch	10	0	0	5
Fence + Ditch	13	0	0	20
Fence w/Sensor	6	15	0.65	10
Fence w/Sensor + Ditch	16	15	0.65	20
Magnetic	20	2	0.80	0
Microwave	30	2	0.90	0
Radar	500	2	0.75	0
Security Camera	90	2	0.80	0
Buried Cable	200	2	0.90	0
Guard	700	0	0.50	0