SAND2005-7588C

Physical Security and Vulnerability Modeling for Infrastructure Facilities

Dean A. Jones
Chad E. Davis
Sandia National Laboratories
Albuquerque, NM

Mark A. Turnquist
Linda K. Nozick
Civil & Environmental Engineering
Cornell University
Ithaca, NY

HICSS-39 January, 2006

Critical Infrastructures

- Telecommunications
- Electric power
- Natural gas and oil
- Banking and finance
- Transportation
- Water supply
- Government services
- Emergency services

List created by Presidential Commission on Critical Infrastructure Protection, 1997

- Critical Infrastructure Assurance Office (CIAO) established by Presidential Directive in 1998
- CIAO broadened the definition, adding:
  - Food production, storage and distribution
  - Health care
  - Educational system
  - Some specific industries (aluminum, steel, etc.)
- Responsibility now in DHS

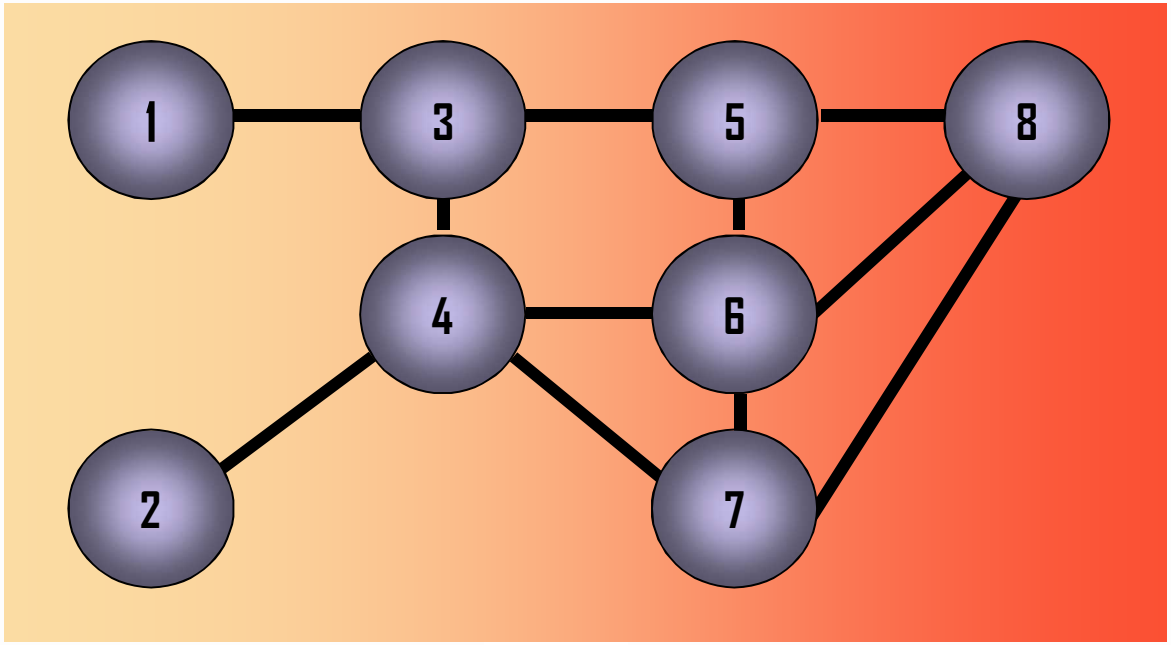
Motivation

- Infrastructure facilities are potential terrorist targets
- “Malicious intrusions” may be focused on either a physical facility or supporting information systems
- An intrusion may be viewed as negotiating a network of barriers and paths in an attempt to reach a goal state
- This viewpoint can highlight vulnerabilities
- Provides a basis to analyze the benefits of various “hardening” measures

Modeling an Attempted Intrusion

Markov Decision Model **to understand path(s) of greatest vulnerability**

System Entry → Undetected Exit



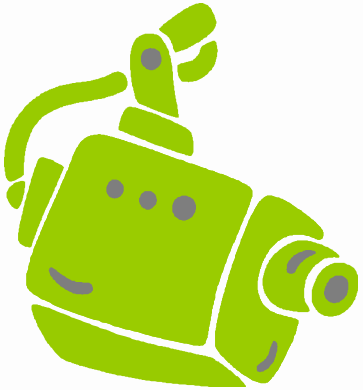
Nodes represent barriers

Arcs represent movements

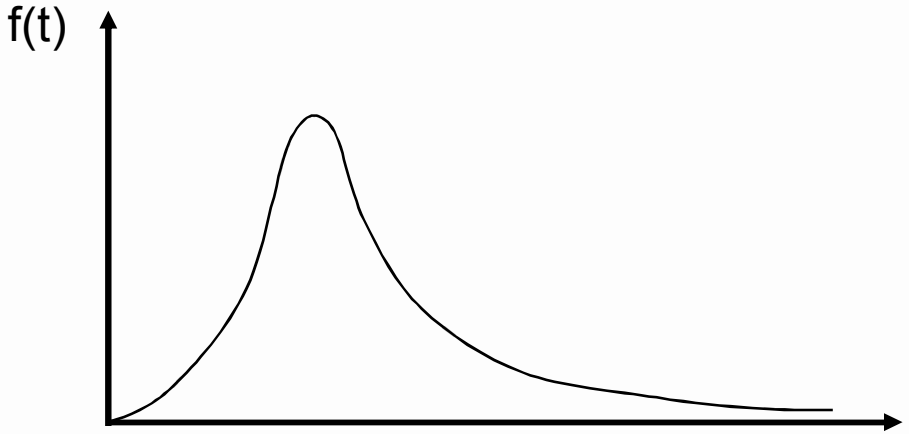
Improving System Security

- Assume that the intruder is “smart”
  - Has knowledge of the structure of the system
  - Knows the probabilities of success and detection
  - Follows an “optimal” strategy (i.e., maximizing the probability of successful intrusion)
- Against such an adversary, where are the places to make the largest potential improvements in security (i.e., greatest reduction in the probability of successful intrusion)

Attempting Penetration of a Barrier

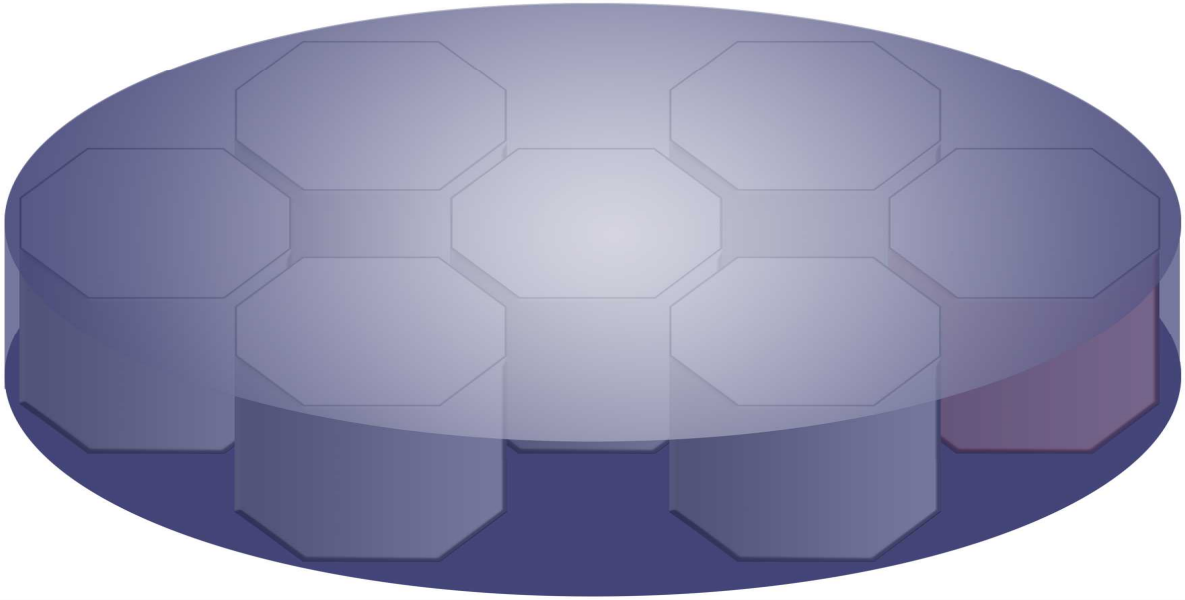


- Requires uncertain amount of time
- Risks detection
- May fail without being detected



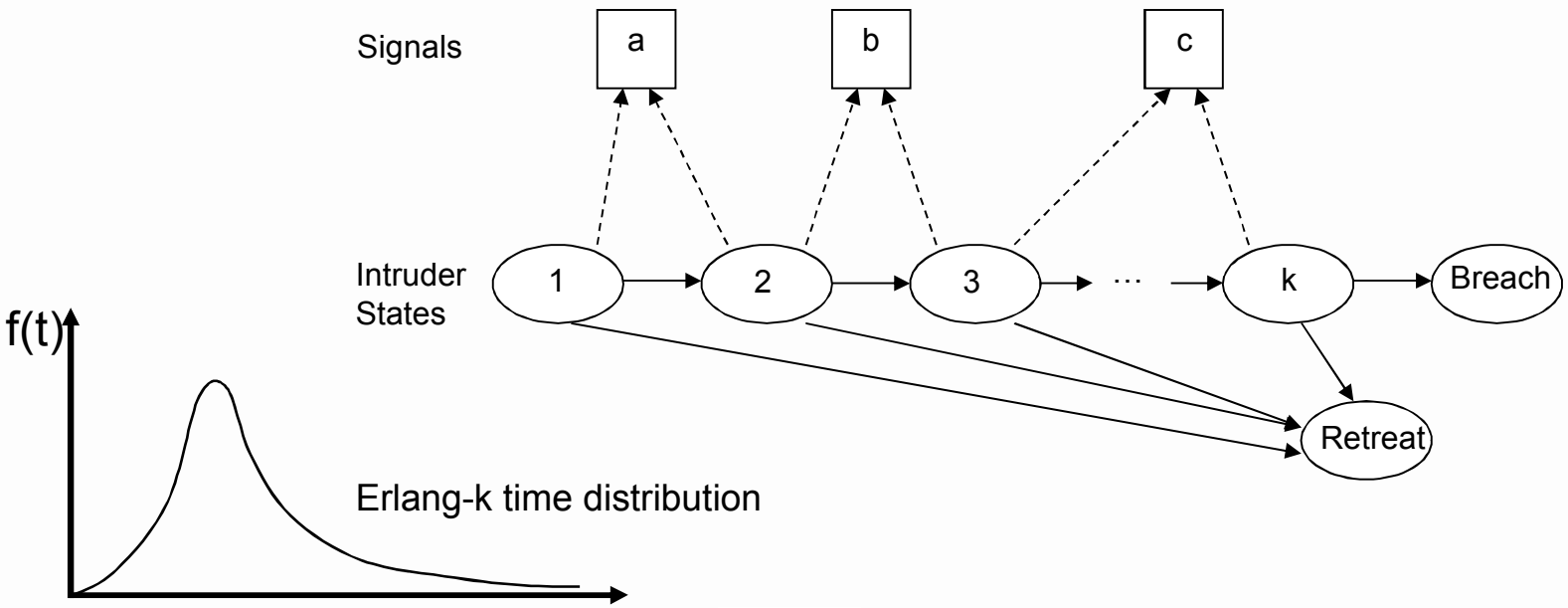
Modeling Attempted Penetration

Collection of states “inside” a node in the system network



Modeling Attempted Penetration

Hidden Markov Model to model interaction between intruder and the intrusion detection system.



Hidden Markov Model

- Transition dynamics

$$X_{n+1} = A^T X_n$$

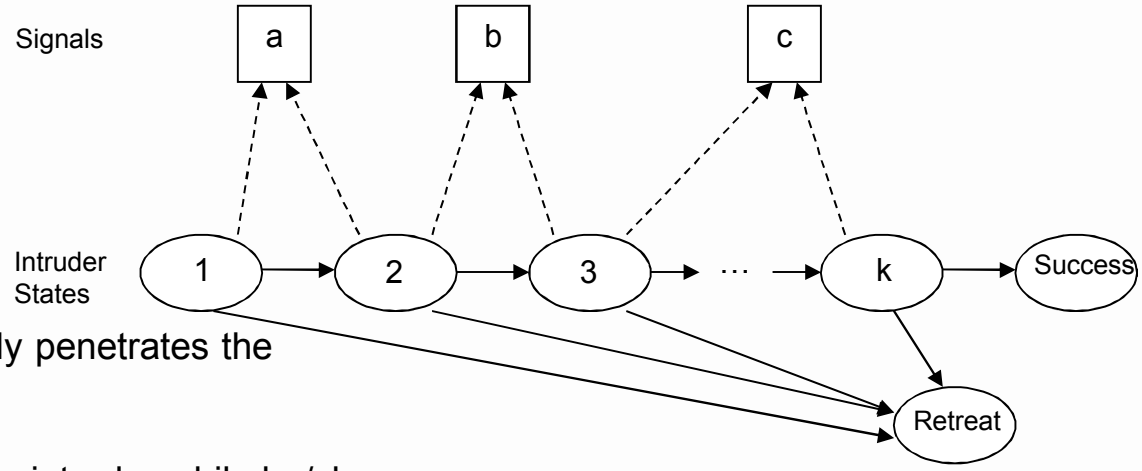
- "Signals" from state occupancy

$$Y_n = BX_n$$

- Matrix *B* is conditional probability of a signal, given state occupancy
- Definition of detection as a subset of possible signals

Key Steps: Summarizing a Node (Barrier) in the Model

Summary Characteristics



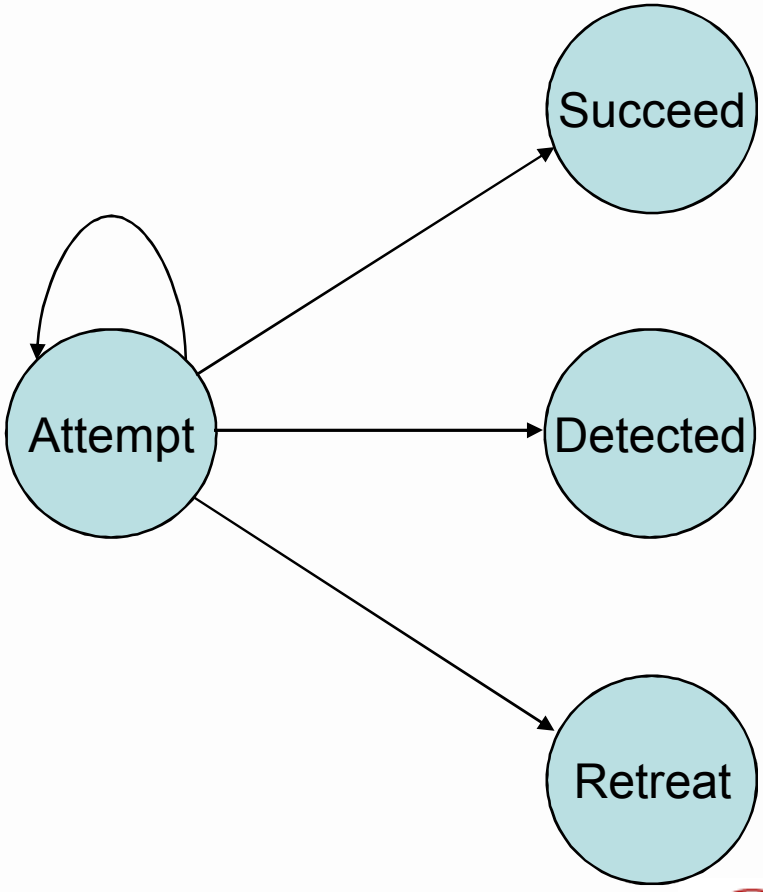
Prob(Success): Intruder successfully penetrates the barrier without being detected

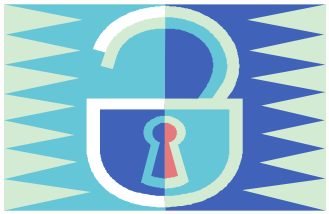
Prob(Detection): System detects the intruder while he/she is attempting to penetrate the barrier

Prob(Retreat): Intruder fails to penetrate the barrier, but is not detected, and leaves

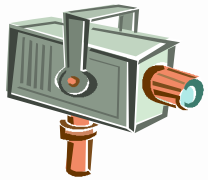
Expected Duration: Expected length of time the intruder spends trying to penetrate barrier before one of the "absorbing states" (detection, success, or retreat) is entered

Aggregate Node Representation





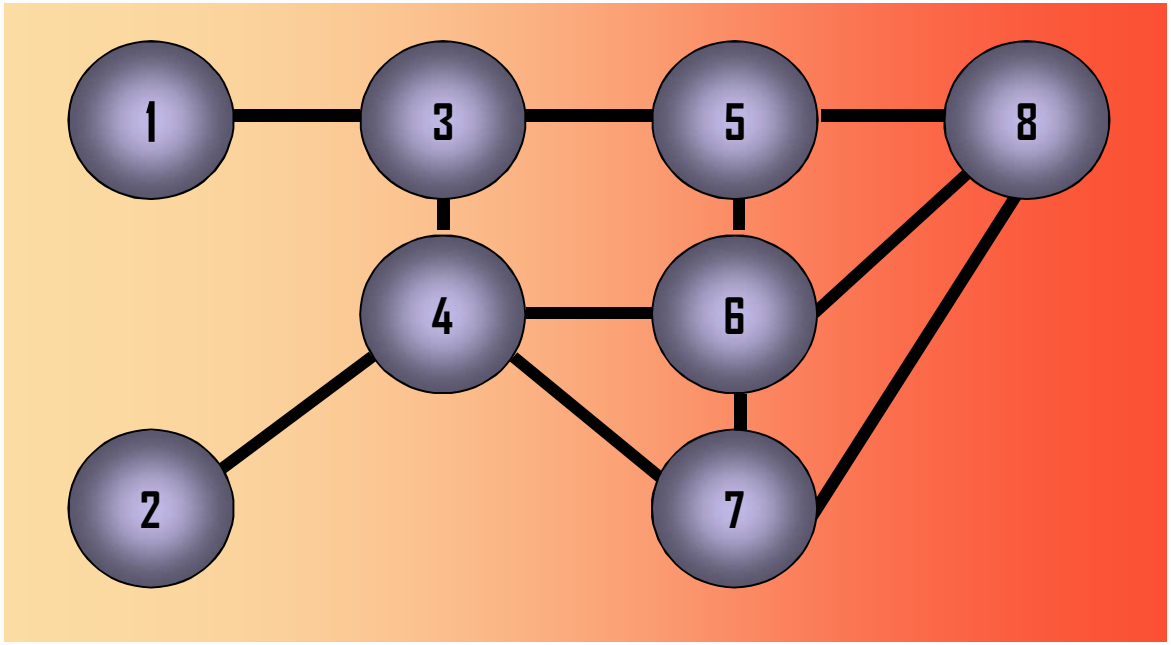
Make decision about where to go next



Modeling an Attempted Intrusion

Markov Decision Model **to understand path(s) of greatest vulnerability**

System Entry → Undetected Exit



Nodes represent barriers

Arcs represent movements

Markov Decision Model

- $R_i(a_i)$: the immediate reward from being in state *i* and choosing action a_i (1 for "goal" state, and 0 everywhere else)
- $P_{ij}(a_i)$: transition matrix associated with choosing action a_i in state *i*
- $w(i, a_i)$: expected value of future stream of rewards (probability of reaching "goal" state)
- $w^*(i)$: optimal value of $w(i,a_i)$ for best policy

$w^*(i)$ is the smallest set of values for which:

$$w(i) \geq R_i(a_i) + \sum_j P_{ij}(a_i) w(j) \qquad \forall\, i, a_i$$

Solving for Optimal Policies

$$\min \quad \sum_i \beta_i w(i)$$

Subject to: $$w(i) - \sum P_{ij}(a_i) w(j) \geq R_i(a_i) \qquad \forall\ i, a_i$$

$$w(i) \geq 0 \qquad \forall\ i$$

β_i is a set of positive scalars with $\sum_i \beta_i = 1$

Many more constraints than variables, so use dual formulation

Dual LP

$$\max \quad \sum_i \sum_{a_i} R_i(a_i) x_i(a_i)$$

Subject to:

$$\sum_{a_j} x_j(a_j) - \sum_i \sum_{a_i} P_{ij}(a_i) x_i(a_i) \le \beta_j \qquad \forall\ j$$

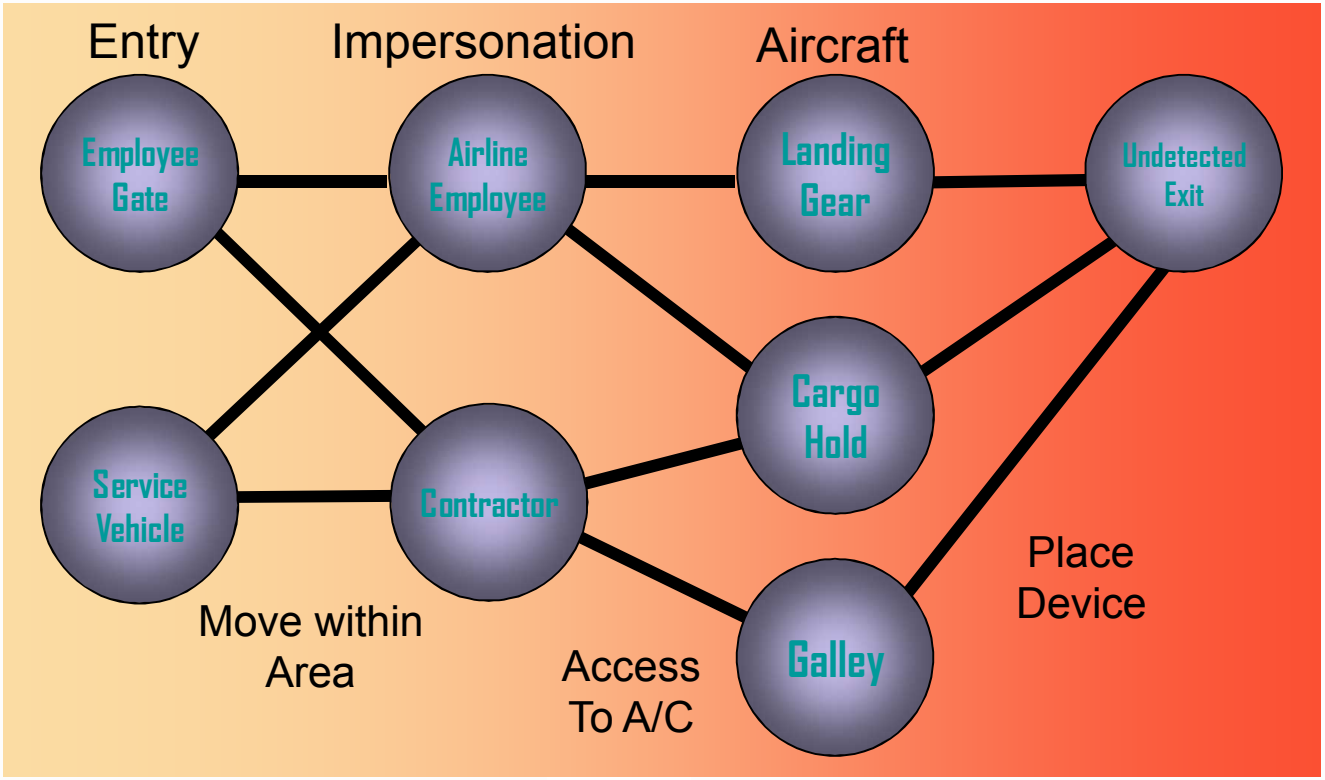
$$x_i(a_i) \ge 0 \qquad \forall\ i, a_i$$

For each state, *i*, no more than one $x_i(a_i)$ will be positive. This indicates the optimal action a_i^* for state *i*

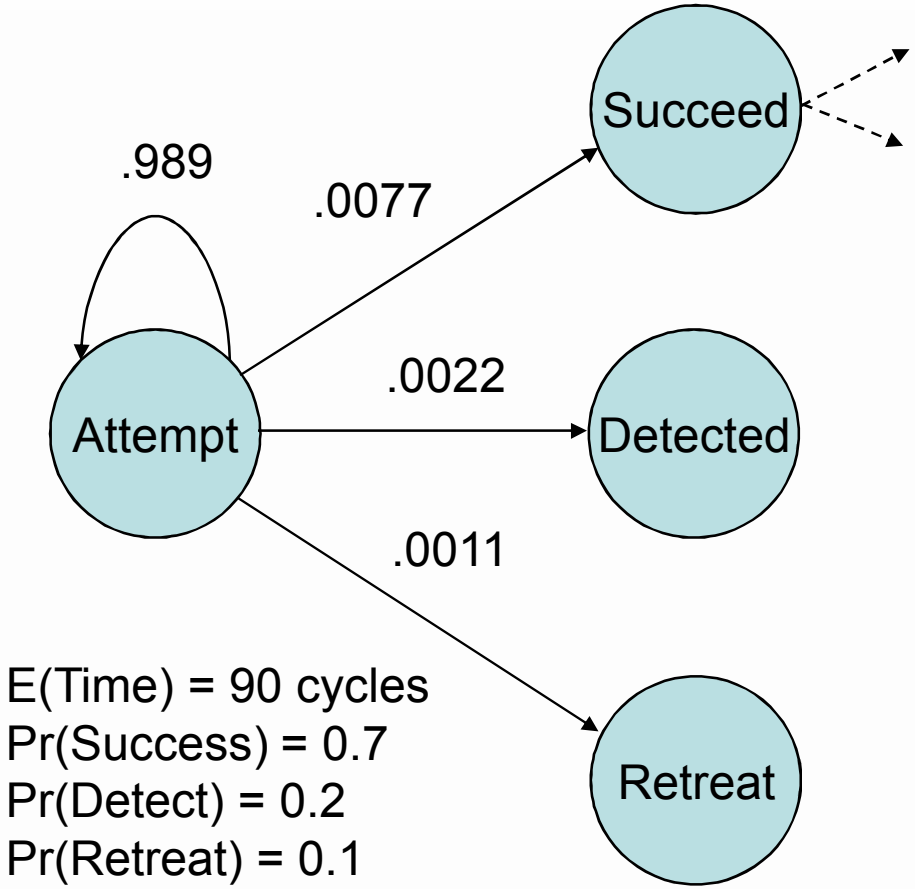
We get the probabilities of successful intrusion, $w^*(j)$, given the intruder has reached state *j*, as the shadow prices from the dual problem (i.e., the primal variables).

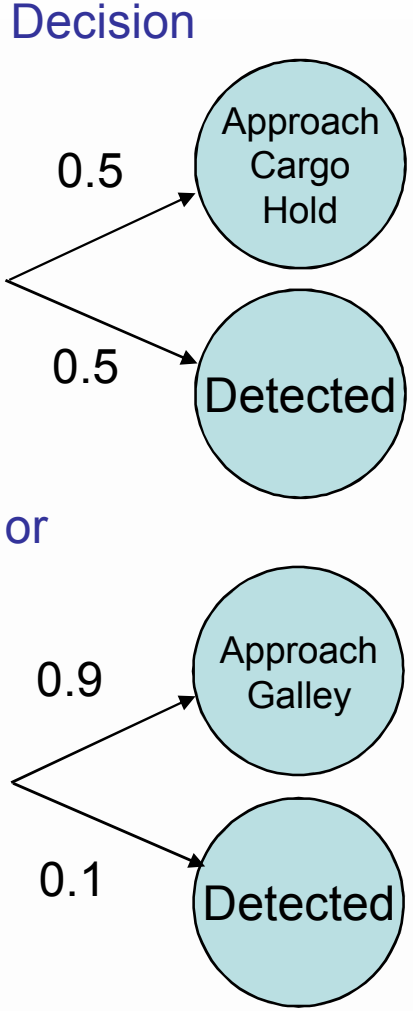
A Simple Example

Intruder attempting to place an explosive device on an aircraft while it is at the gate.



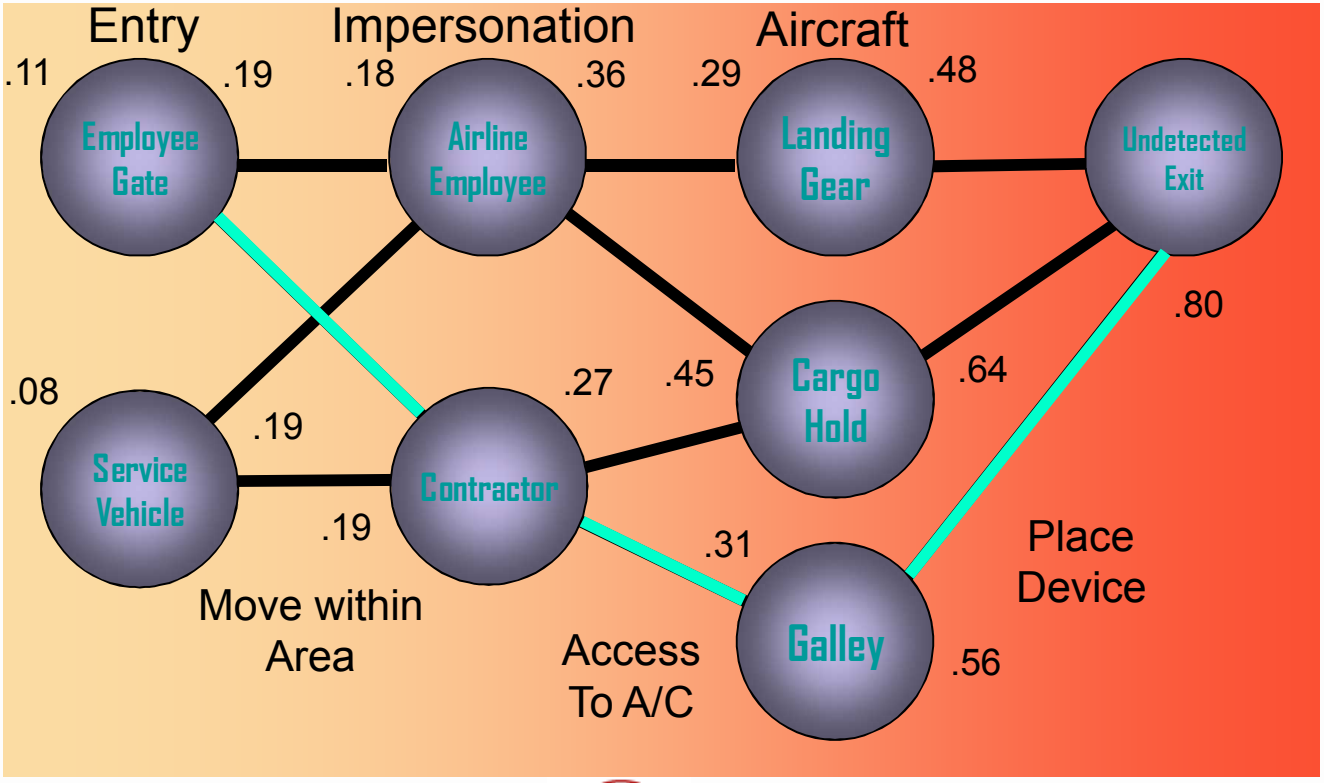
Hypothetical Node Data (Impersonate Contractor)





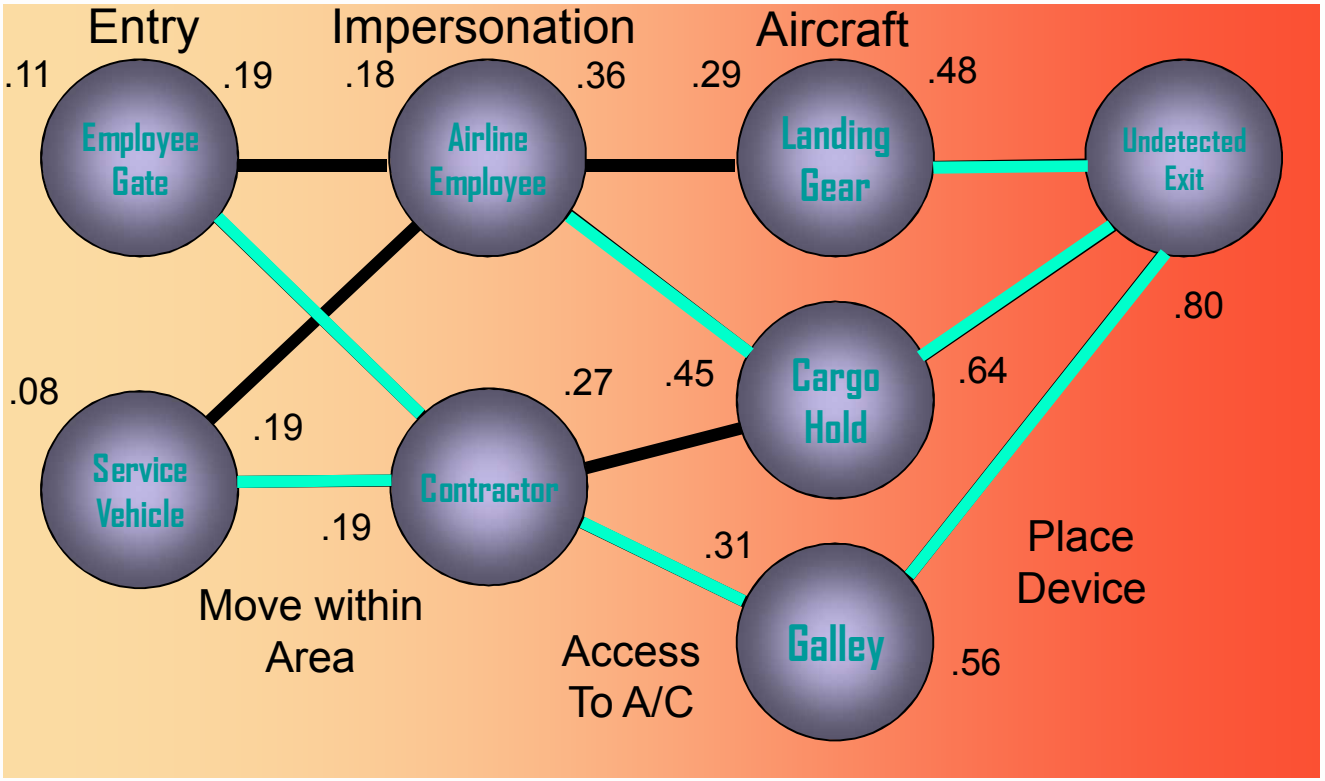
Solution to Hypothetical Problem

Intruder attempting to place an explosive device on an aircraft while it is at the gate.

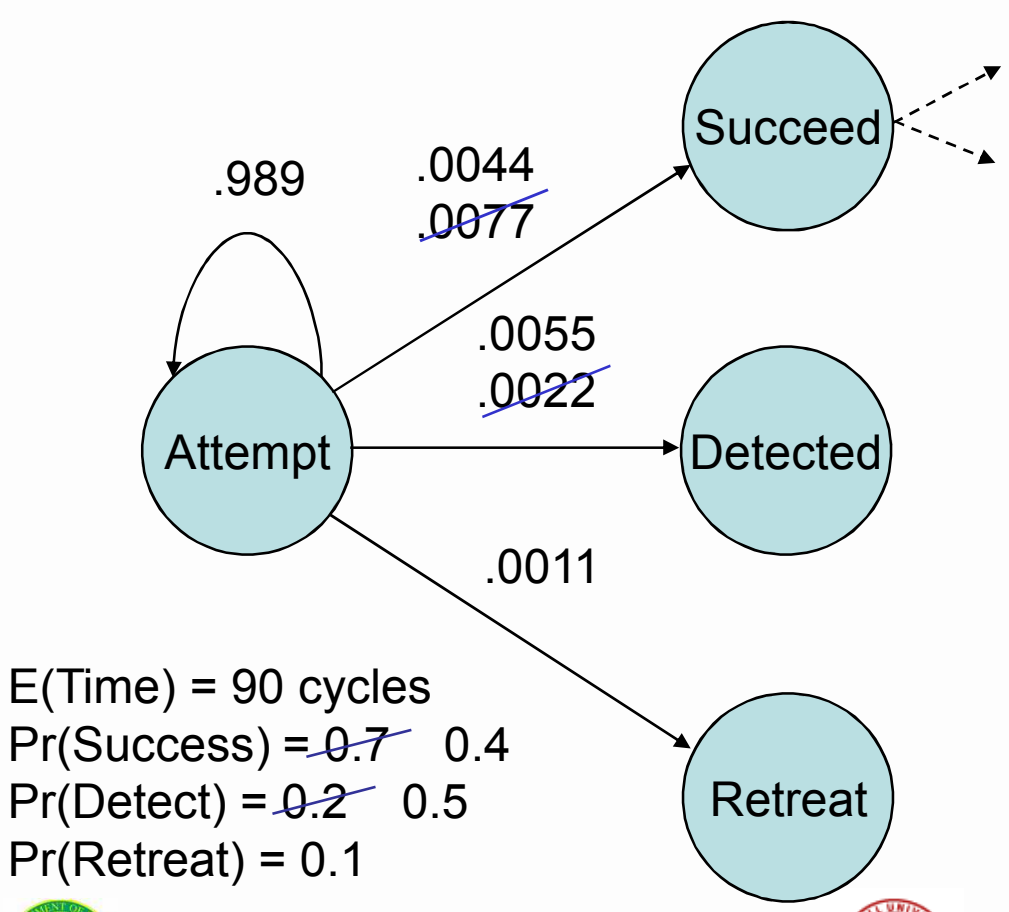


Vulnerability "Tree"

Given an intruder's location, what is the optimal strategy from there?

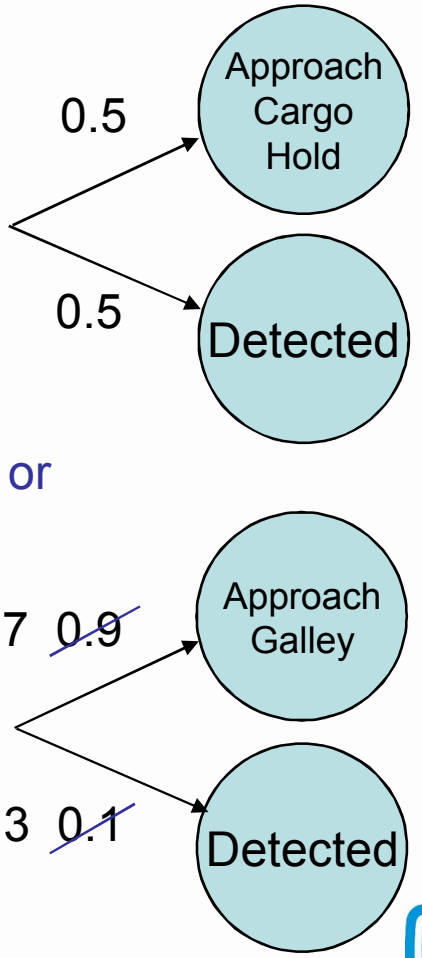


Illustrative Change (Checking Contractors More Closely)



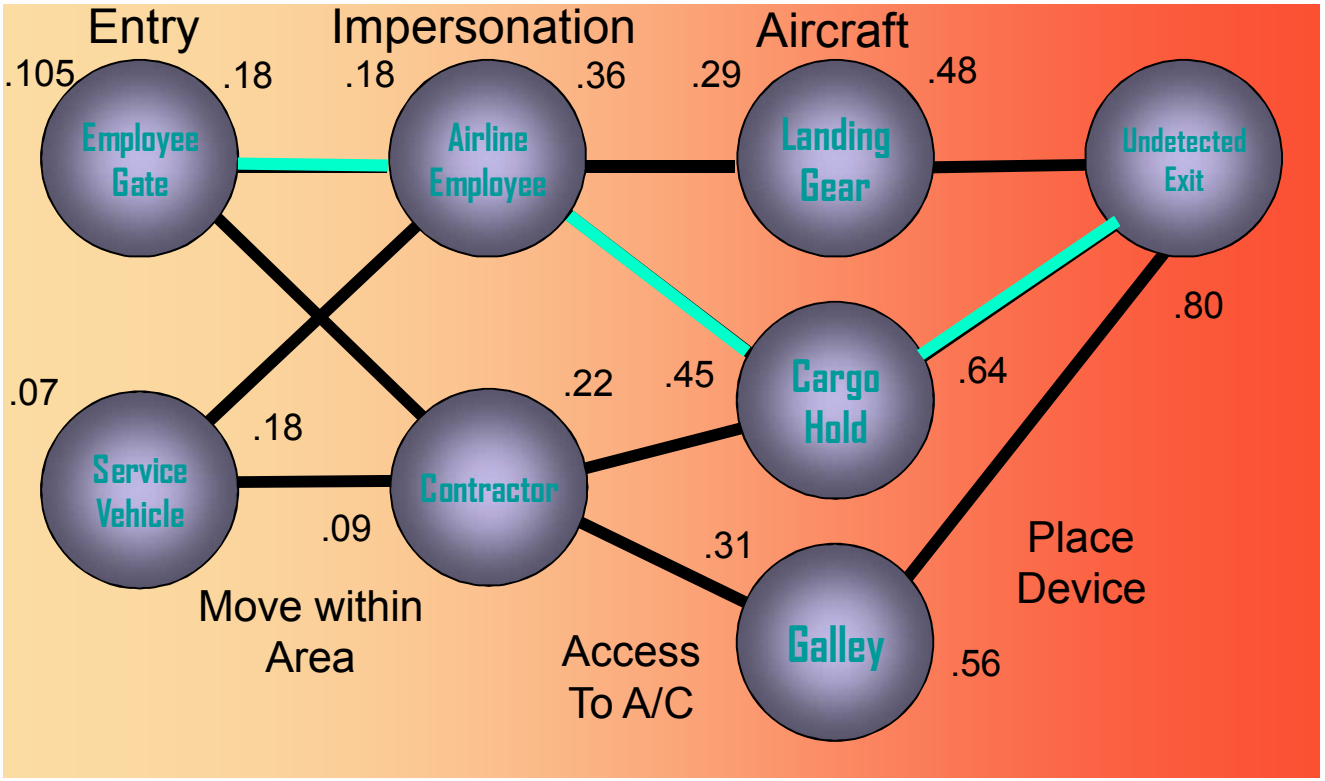
E(Time) = 90 cycles
Pr(Success) = ~~0.7~~ 0.4
Pr(Detect) = ~~0.2~~ 0.5
Pr(Retreat) = 0.1

Decision



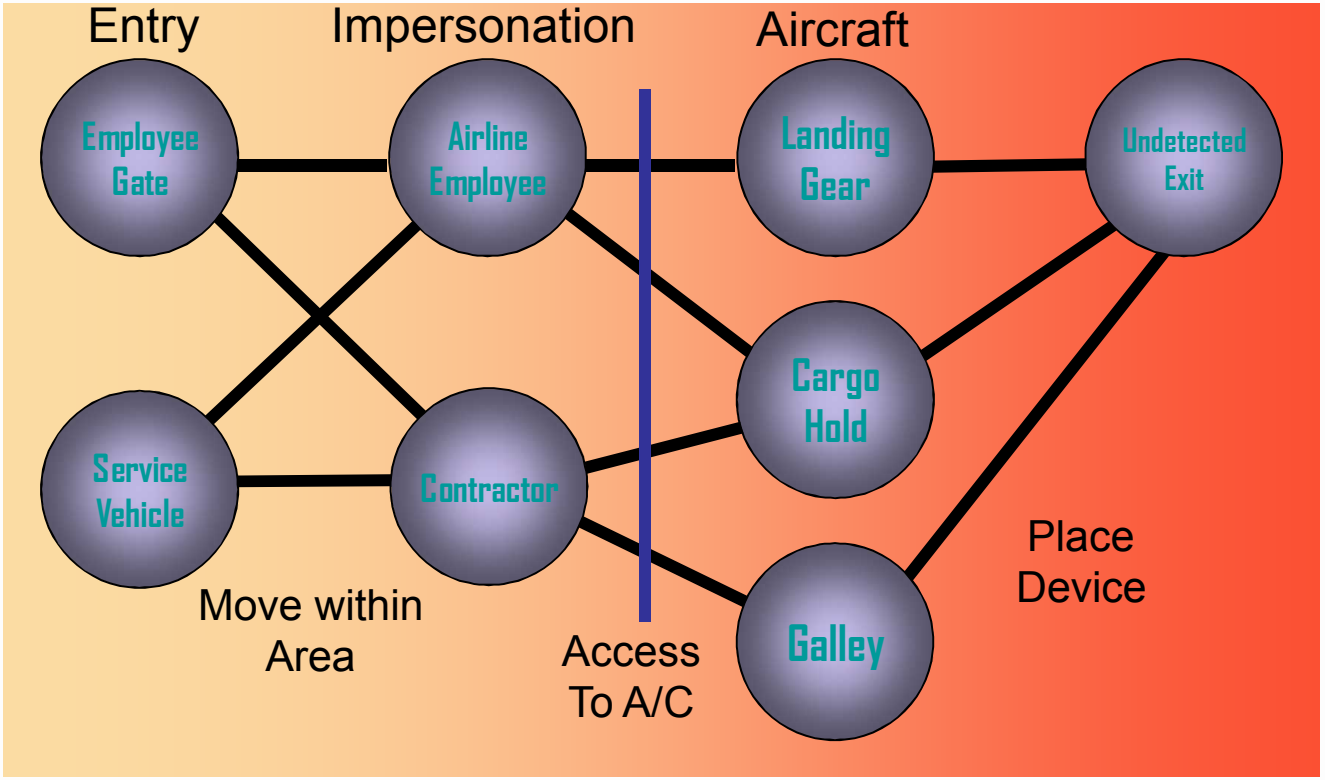
Revised Solution to Hypothetical Problem

"Smart" intruder adapts by changing strategy



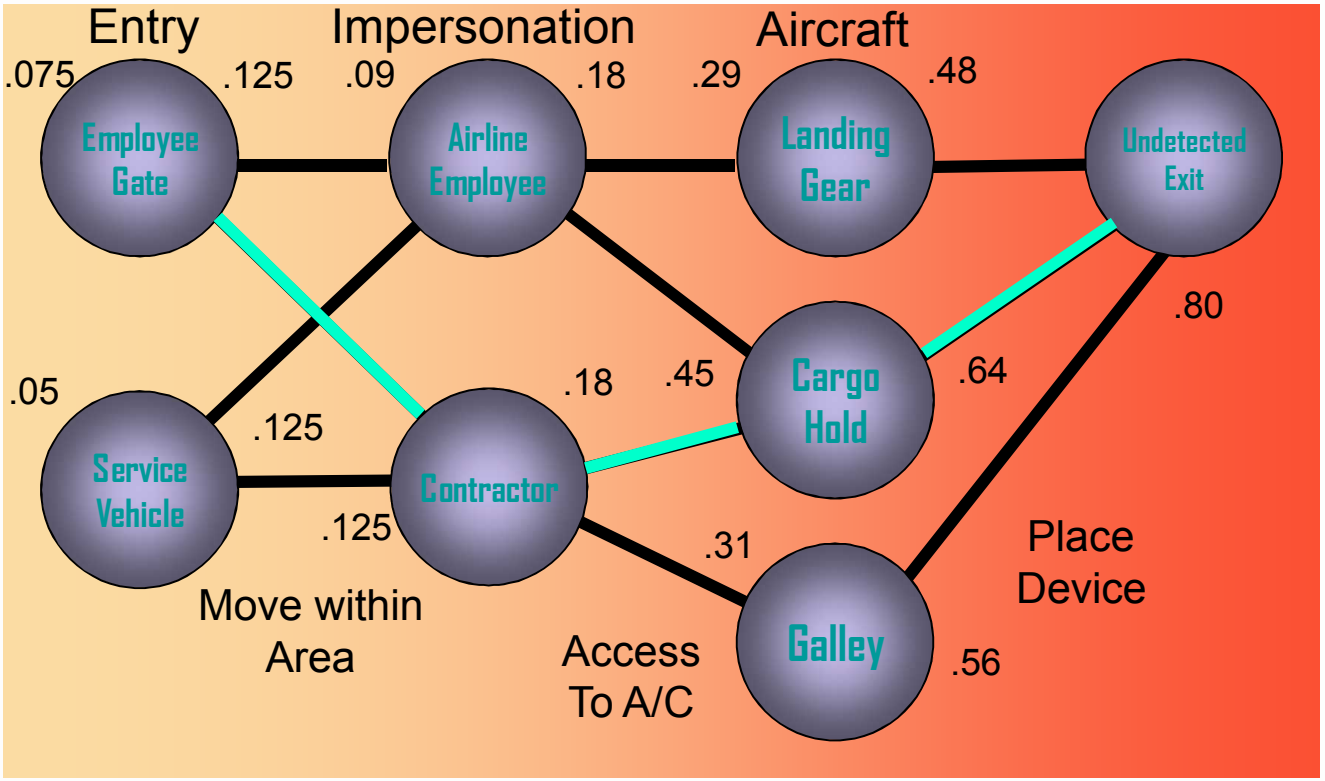
Identifying Cutsets

Increase detection probabilities across the cutset



Focusing on Cutsets

Make prob(detection) = 0.6 on all access to aircraft arcs



Examples of Other Questions

- If we were to focus on detection of intruders as they attempt to access the aircraft, how good would we have to be in order to reduce the probability of success to .01? (Answer: 97% detection probability)
- If we could achieve a 90% detection probability on the access arcs, how much would we have to improve the detection of impersonations to reach .01 success probability on intrusion? (Answer: to 68%)

Optimizing Resource Allocation

- Where should we put resources to "optimally" reduce the likelihood of a successful intrusion?
- Need to estimate marginal costs of changing various probabilities (difficult)
- Result is a bi-level optimization:
  - Outer level: Allocate resources to change individual probabilities (detection, etc.) $\Rightarrow$ changes in transition matrix
  - Inner level: Given new transition probabilities, intruder optimizes strategy

Extensions (In Progress)

- Intruders with imperfect information
  - Uncertain, but unbiased
  - Biased estimates of probabilities
- Semi-Markov models for individual barriers to represent elapsed time (and time-dependent detection rates) more accurately
- Develop bi-level optimization model to optimize investments in reducing vulnerability

Conclusions

- Integration of Hidden Markov Models and Markov Decision Processes provides a useful modeling framework for investigating infrastructure system vulnerabilities to physical or cyber intrusions
- Analysis also leads naturally to optimization of investments in "system hardening"
- Can take advantage of work in CS community on intrusion detection
- Modeling perspective offers the "system-level view" that is missing in component and individual threat analyses