Topological Game-Semantic Methods for Understanding Cyber Security

Peter Chin at JHU
Samson Abramsky at Oxford
John Harer at Duke

AFOSR Complex Networks Annual Review
December 21, 2012

The Johns Hopkins University
APPLIED PHYSICS LABORATORY

Outline

- Brief history & applications of game theory
- Game theory meets cyber defense
- Game theory meets topology
- Future ideas towards measurement

Outline

- ***Brief history & applications of game theory***
- Game theory meets cyber defense
- Game theory meets topology
- Future ideas towards measurement

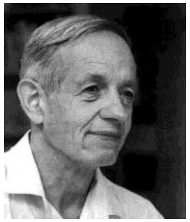
From Princeton Office to Starship Enterprise

history

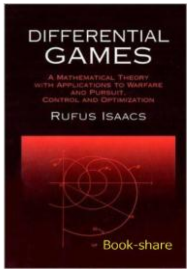
1st generation

Von Neumann, 1924
2-person game

2nd generation

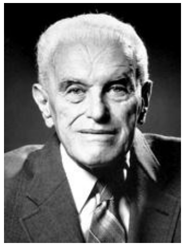


John Nash, 1951
N-person game

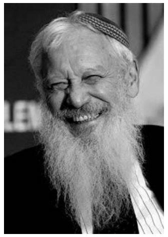


DIFFERENTIAL GAMES
A MATHEMATICAL THEORY WITH APPLICATIONS TO WARFARE AND PURSUIT, CONTROL AND OPTIMIZATION
RUFUS ISAACS
Book-share

Rufus Isaacs,1951
differential games

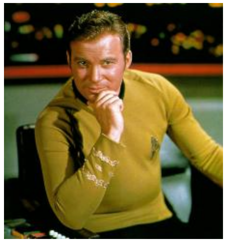


John Harsanyi,
uncertain games



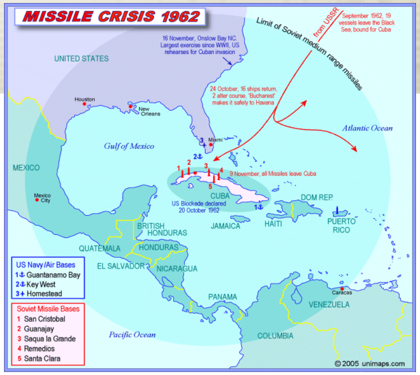
Bob Aumann, 1951
dynamic game

3rd generation

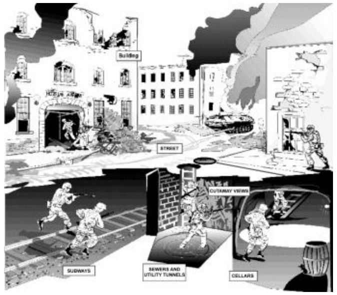


David Meyers, et.al
quantum games

applications



Cold War, Cuban
Missile Crisis, 1962



Urban Warfare, GWOT

Cyber Warfare

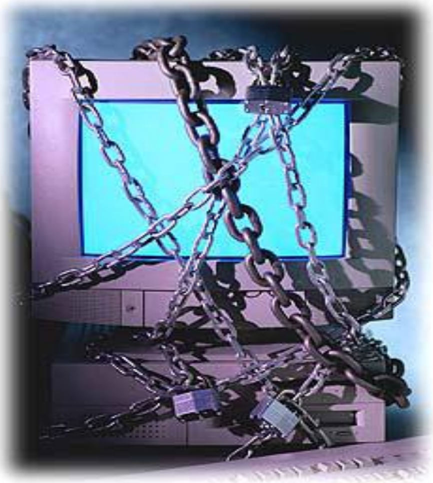
21st Century

Outline

- Brief history & applications of game theory
- ***Game theory meets cyber defense***
- Game theory meets topology
- Future ideas towards measurement

Sophistication of Network Warfare (from *tactics* to *strategies*)

- No longer cyber attack is just about different hacking tactics
- Attacking a part/whole of network is becoming increasingly sophisticated and now involves a *set of strategies*. Therefore, defending the network does, too!



- This can be viewed as a *contest or game* between the attacker trying to gain access to a network and the defender attempting to thwart such efforts

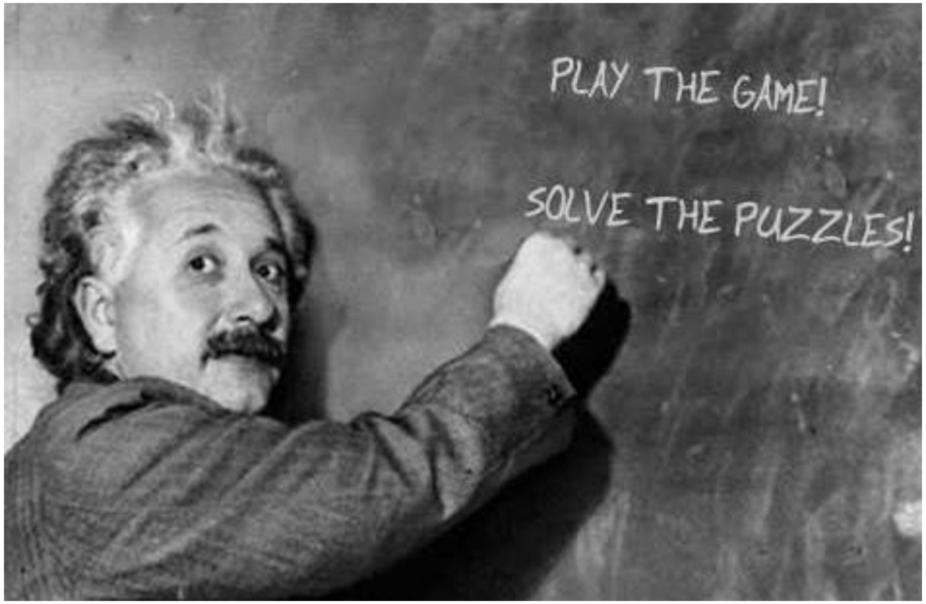
Game Theory is well suited for Cyber Warfare, *Because…*

- Can be seen as a classical two-person game, between cyber attacker and cyber-defender (even as a zero-sum 2 person game as the initial model.)
- Different attack/depend cyber moves can be seen as strategies of this game, and the potential harm & benefit can be formulated into payoff matrix.

Game theory affords rigorous yet computational ways to comb thru strategy space and reason about adversary's moves.

Benefits of applying Game Theory

- Gives an approach to analyze *different types of cyber interactions* (2-person, N-person, etc.)
- Gives an approach to compare *different cyber strategies* as well as finding *likely* adversarial & *optimal* defensive strategies
- Gives an approach to detect *anomalous* behavior by measuring *distance from Nash equilibrium.*



7-layer Map between *Cyber Warfare* & *Game Theory*

- **2-person vs. N-person**
- **Static vs. Dynamic**
- **Simultaneous vs. Stackberg**
- **Deterministic vs. Stochastic**
- **Perfect vs. Imperfect Information**
- **Cooperative vs. Non-Cooperative**
- **Classical vs. Quantum**

2-person at global level, N-person to account multiple adversaries attacking multiple defense sites that are working together

Static for initial model, becoming increasingly dynamic, as cyber attacks morph quickly

Ideally simultaneous, but many interactions are leader/follower

Many cyber attacks have stochastic elements

Realistically Imperfect information

Depends on communication ability between players

Got Quantum Computer? More on this later…

Strategy Space, *example*

ATTACK STRATEGIES

- WEB DEFACEMENTS AND SEMANTIC ATTACKS
- DOMAIN NAME SERVICE (DNS) ATTACKS
- DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS
- WORMS
- ROUTING VULNERABILITIES
- INFRASTRUCTURE ATTACKS
- COMPOUND ATTACKS
- WHEN TO ATTACK
- WHERE TO ATTACK

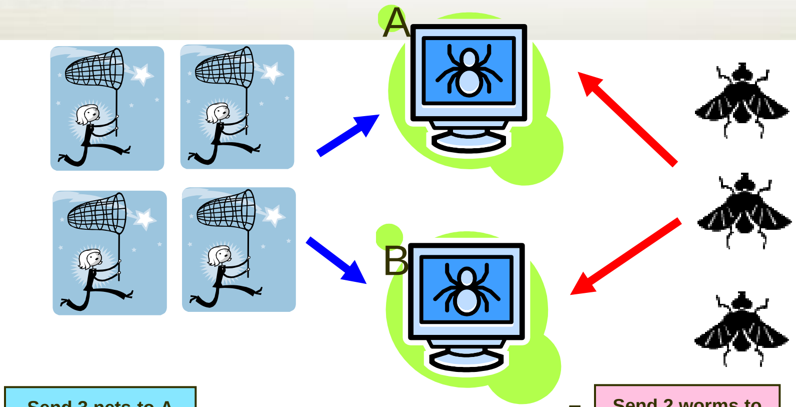
Counter ACTIONS STRATEGIES

- Shut down the network
- Reconfiguration of Hosts
- Renumbering of IP addresses
- Moving critical data between different hosts
- Revealing part of the system

	R1	R2	R3	R4	R5	R5
B1	0	-1	2	2	2	2
B2	1	0	-1	2	2	2
B3	-2	1	0	-1	2	2
B4	-2	-2	1	0	-1	2
B5	-2	-2	-2	1	0	-1
B6	-2	-2	-2	-2	1	0

Blue = (¼, ½, ¼,0, 0, 0) vs. Red = (¼, ½, ¼,0, 0, 0)

Simple Example: Divide and Conquer or *NOT*?



Send 3 nets to A and 1 net to B

payoff matrix

Send 2 worms to A and 1 to B

	(3,0)	(2,1)	(1,2)	(0,3)
(4,0)	4	2	1	0
(3,1)	1	3	0	-1
(2,2)	-2	2	2	-2
(1,3)	-1	0	3	1
(0,4)	0	1	2	4

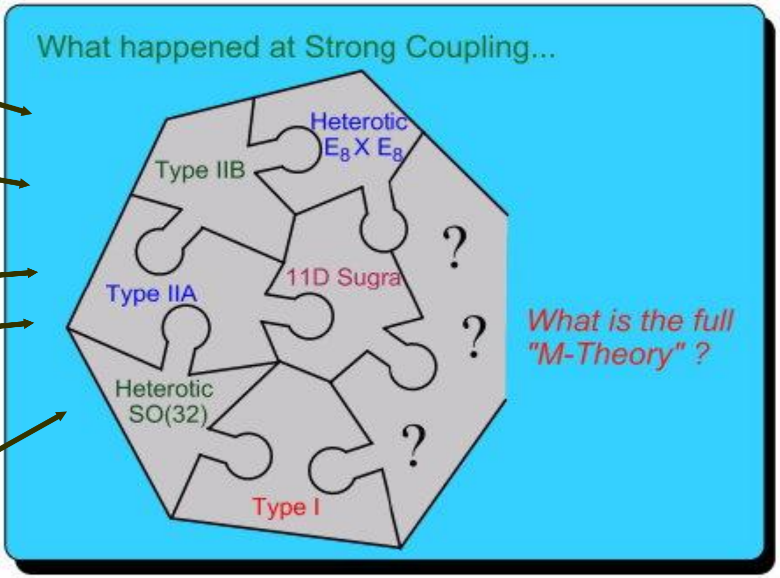
- **Problem**: A network of 2 computers needed to be defended.
- Offense Strategies: Distribute 3 worms to 2 computers (A & B)
- Defense Strategies: Distribute 4 nets to 2 computers (to catch the worms).
- **Rules**: The side that has more captures all of the other side and wins 1 pt and gains another additional point for each of the other side that's captured or thwarted.
- **(3,1) vs. (1,2):** Blue wins 1pt & gains 1 pt for capturing 1 bug at A. Red wins 1pt and gains 1 pt for thwarting 1 net at B. Payoff for blue = 2 – 2 = 0.
- **Solution from game**:

  (4,0) (3,1) (2,2) (1,3) (0,4)
  - Blue = (4/9, 0, 1/9, 0, 4/9)

  (3,0) (2,1) (1,2) (0,3)
  - Red = (1/18, 4/9, 4/9, 1/18)
- Lesson for Blue: Don't send 1 net to either A or B

Go Game Theory! But *what's stopping us?*

- 2-person vs. *N-person*
- Static vs. *Dynamic*
- Simultaneous vs. Stacklberg
- Deterministic vs. *Stochastic*
- Perfect vs. *Imperfect*
- Cooperative vs. Non-Cooperative
- Classical vs. *Quantum*


What happened at Strong Coupling...
Heterotic $E_8 \times E_8$
Type IIB
11D Sugra
Type IIA
Heterotic SO(32)
Type I
?
?
?
What is the full "M-Theory" ?

Lack of theory, *Lack* of usable theory!!

A novel/Nobel Moment…..

- Can new approaches such as:
  - Fixed-point approach for N-person Game
  - Techniques for Dynamic Game

HELP in game theoretic understanding of cyber security?

A New Approach To Solving Dynamic Games

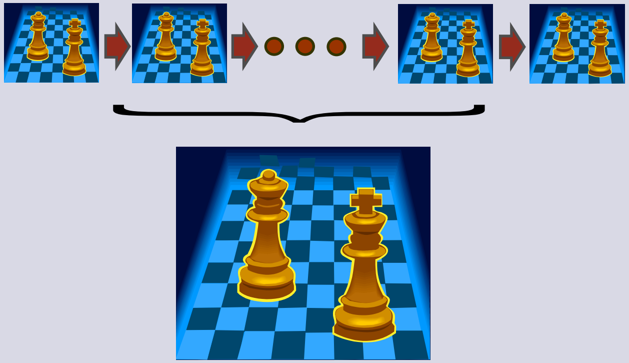
(Theoretical Foundation #1)

Old Approach by FOLK Theorem:

Every finite horizon two-person game has a solution.

HOW IT WORKS:

Build up one big game consisting of a game at each stage, and then apply von Neumann’ s theorem to the big game:

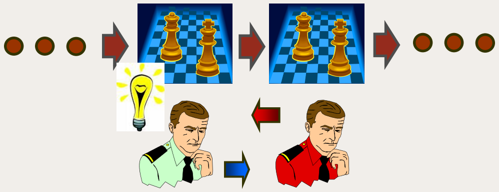


DRAWBACKS:

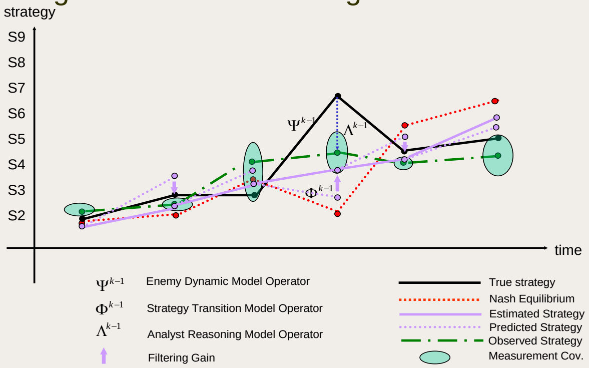
- No insight for what strategy to implement next.
- Too much emphasis on Nash Equilibrium

NEW INSIGHT:

Exploit perceived adversarial strategy each time a measurement of adversarial move (e.g. sensor measurement) is made.



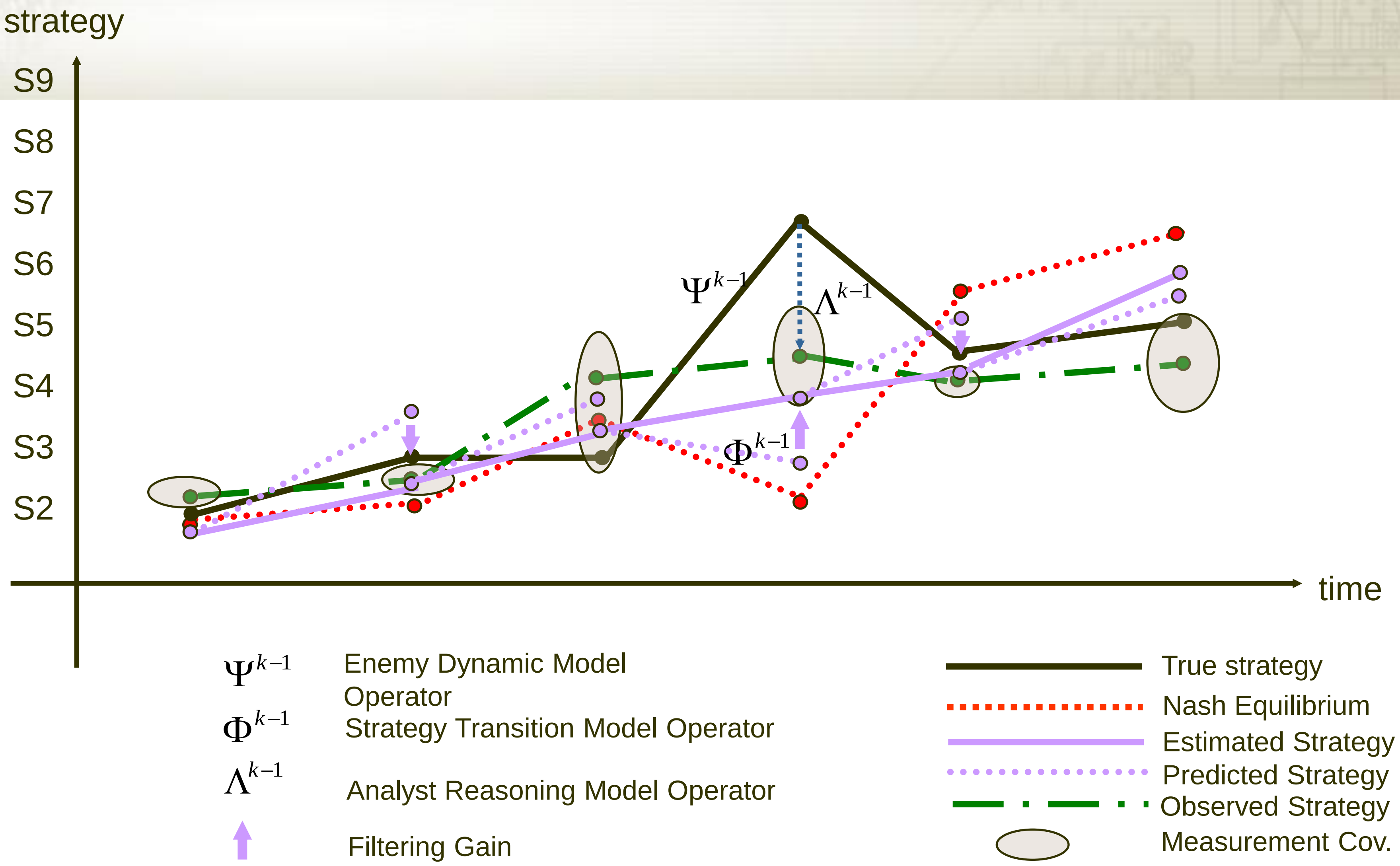
Apply Kalman filtering techniques for moving targets to estimate moving adversarial strategies



HOW IT WORKS:

Exploit the current observed enemy strategy by combining Bayesian response with Nash equilibria

Filtering Techniques for Dynamic Games (in picture)



Filtering Techniques for Dynamic Games (in equations)

Kalman Filter Equations

$$\hat{y}_t^t = \hat{y}_t^{t-1} + K_t(x_t - B\hat{y}_t^{t-1})$$

$$P_t^t = (I - K_t B)P_t^{t-1}$$

$$K_t = P_t^{t-1}B^T(R + BP_t^{t-1}B^T)^{-1}$$

$$\hat{s}_t^t = \mathrm{F}^{t-1}\hat{s}_{t-1}^{t-1} + K_t(\mathrm{L}^t s_t - \mathrm{L}^{t-1}\mathrm{F}^{t-1}\hat{s}_{t-1}^{t-1}) +$$

$$c_t(P_t^{t-1})N(G_t)$$

$$P_t^t = (I - K_t\mathrm{L}^t)P_t^{t-1}$$

$$K_t = P_t^{t-1}(\mathrm{L}^t)^T(R + \mathrm{L}^t P_t^{t-1}(\mathrm{L}^t)^T)^{-1}$$

$\hat{s}_t^t$ = estimated strategy at time t

s_t = true strategy at time t

F^t Î $\mathrm{HOM}(\mathrm{S}^t, \mathrm{S}^{t+1}; \mathrm{Â})$, models strategy transition

S^t = set of strategies at time t

L^t Î $\mathrm{HOM}(\mathrm{S}^t, \mathrm{S}^t; \mathrm{Â})$, models IA's understanding of enemy strategy

G_t = Game at time t

$N(G_t)$ = a Nash equil. solution for the game G_t at time t

c_t = a Nash equil. solution discount factor for the game G_t at time t and measures how much analyst's reasoning should be trusted

Initial Architecture

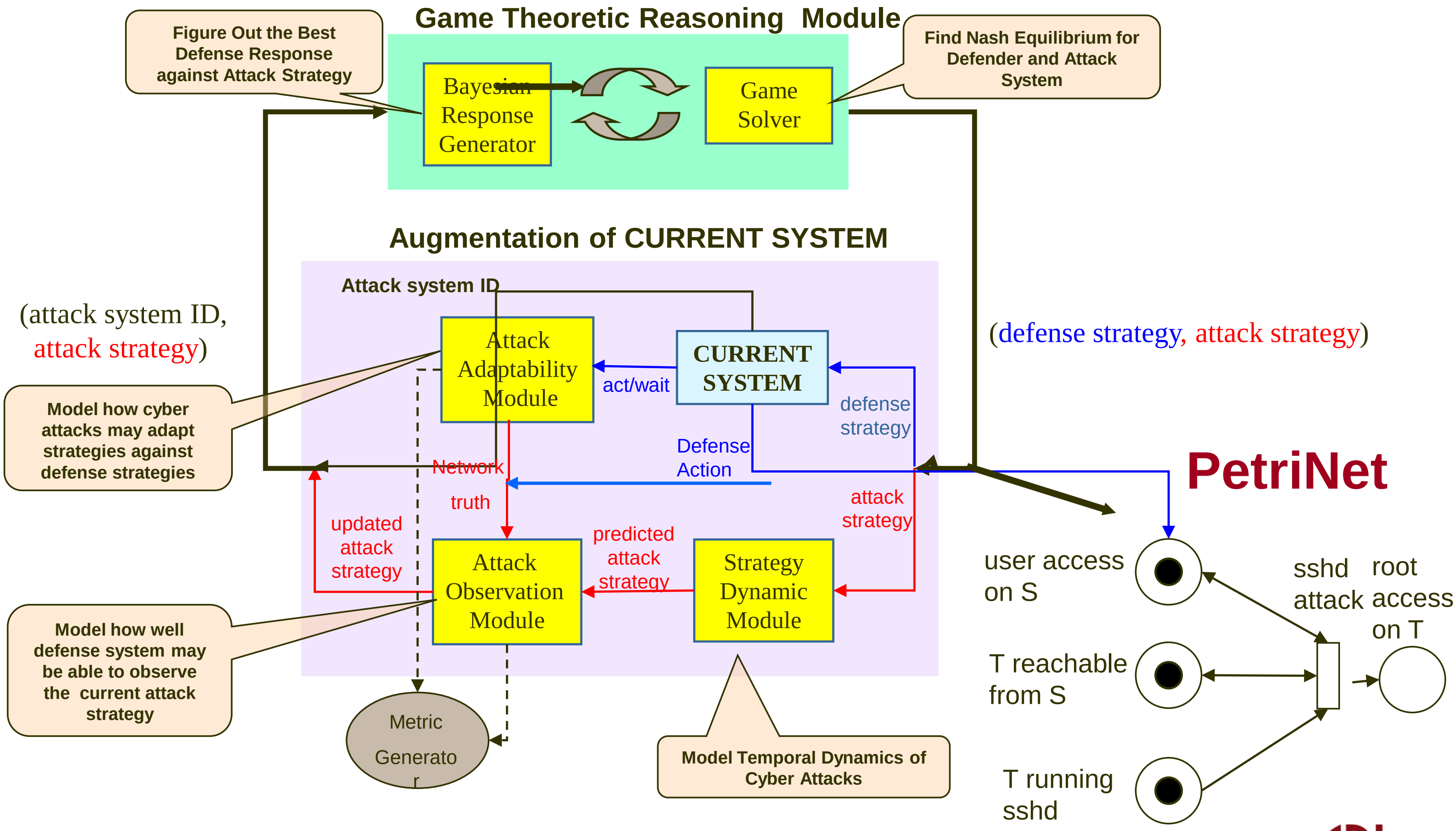


Figure Out the Best Defense Response against Attack Strategy

Find Nash Equilibrium for Defender and Attack System

Model how cyber attacks may adapt strategies against defense strategies

Model how well defense system may be able to observe the current attack strategy

Model Temporal Dynamics of Cyber Attacks

Game Definitions

- **Defender's strategies = {act, wait}**
- **Attacker's types = (offensive infiltrator, defensive infiltrator, deceptive infiltrator) where**
  - **Offensive infiltrator consists of 2 of malware type A.**
  - **Defensive infiltrator consists of 2 of malware type B.**
  - **Deceptive infiltrator consists of 1 of malware type A and 1 of malware type B.**
- **Red strategies = {attack, defend, deceive}**
- **Payoff Matrix::**

$$A(offensive)=\begin{bmatrix} 5 & -2 & 1 \\ -5 & 3 & 2 \end{bmatrix}$$

$$A(defensive)=\begin{bmatrix} -1 & 2 & 2 \\ 1 & -1 & 1 \end{bmatrix}$$

$$A(deceptive)=\begin{bmatrix} 2 & -1 & 3 \\ -2 & 1 & -2 \end{bmatrix}$$

Bayesian Response

- ***Bayes_p(offensive) = argmax(p)*** $_{p \in X^*} \, p^T A(offensive) q$

- ***Bayes_p(defensive) = argmax(p)*** $_{p \in X^*} \, p^T A(defensive) q$

- ***Bayes_p(deceptive) = argmax(p)*** $_{p \in X^*} \, p^T A(deceptive) q$

- ***Bayes_p = prob(offensive)*Bayes_p(offensive) + prob(defensive)*Bayes_p(defensive) + prob(deceptive)*Bayes_p(deceptive)***

Game Solutions

$$A(offensive) = \begin{bmatrix} 5 & -2 & 1 \\ -5 & 3 & 2 \end{bmatrix} : \quad p(offensive) = \begin{bmatrix} \frac{8}{15} & \frac{7}{15} \end{bmatrix} \quad q(offensive) = \begin{bmatrix} \frac{1}{3} & \frac{2}{3} & 0 \end{bmatrix}$$

$$A(defensive) = \begin{bmatrix} -1 & 2 & 2 \\ 1 & -1 & 1 \end{bmatrix} : \quad p(defensive) = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \end{bmatrix} \quad q(defensive) = \begin{bmatrix} \frac{1}{3} & \frac{2}{3} & 0 \end{bmatrix}$$

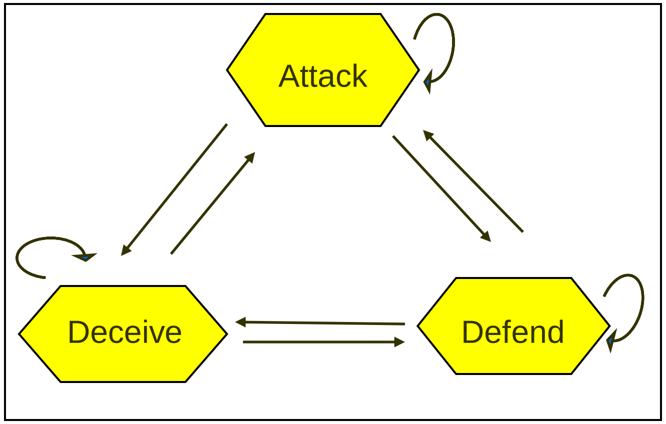
$$A(deceptive) = \begin{bmatrix} 2 & -1 & 3 \\ -2 & 1 & -2 \end{bmatrix} : \quad p(deceptive) = \begin{bmatrix} \frac{2}{5} & \frac{3}{5} \end{bmatrix} \quad q(deceptive) = \begin{bmatrix} \frac{3}{5} & \frac{2}{5} & 0 \end{bmatrix}$$

*Game_p = prob(offensive)*p(offensive) + prob(defensive)*p(defensive) + prob(deceptive)*p(deceptive)*

*Game_q = prob(offensive)*q(offensive) + prob(defensive)*q(defensive) + prob(deceptive)*q(deceptive)*

Strategy Dynamics Simulator

- Modeled by a Markov model



$$\text{Enemy strategy transition matrix} = \begin{pmatrix} .95 & .025 & .025 \\ .025 & .95 & .025 \\ .025 & .025 & .95 \end{pmatrix}$$

Analyst Reasoning Simulator

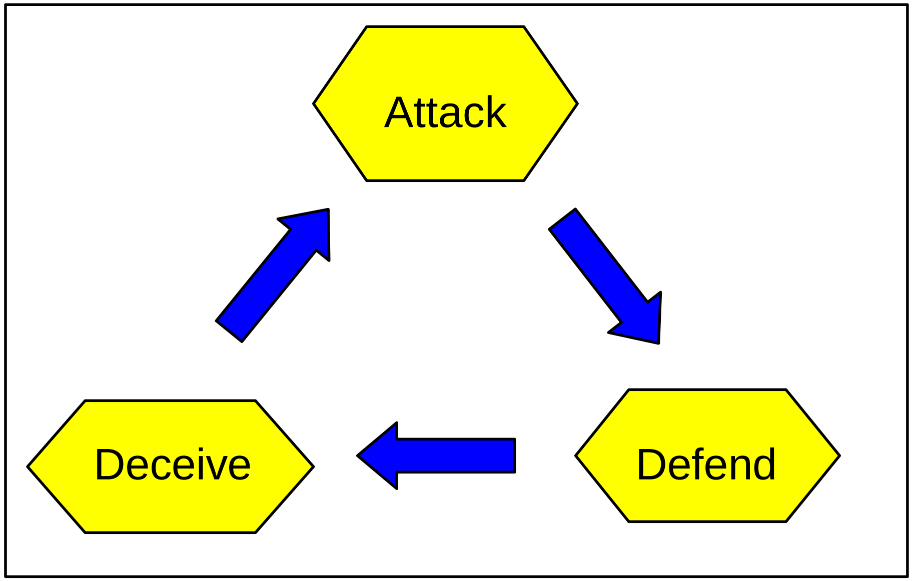
- Modeled by the following confusion matrix

Cyber Sensor 1_confusion matrix = $\begin{pmatrix} .7 & .1 & .2 \\ .2 & .4 & .4 \\ .4 & .2 & .4 \end{pmatrix}$

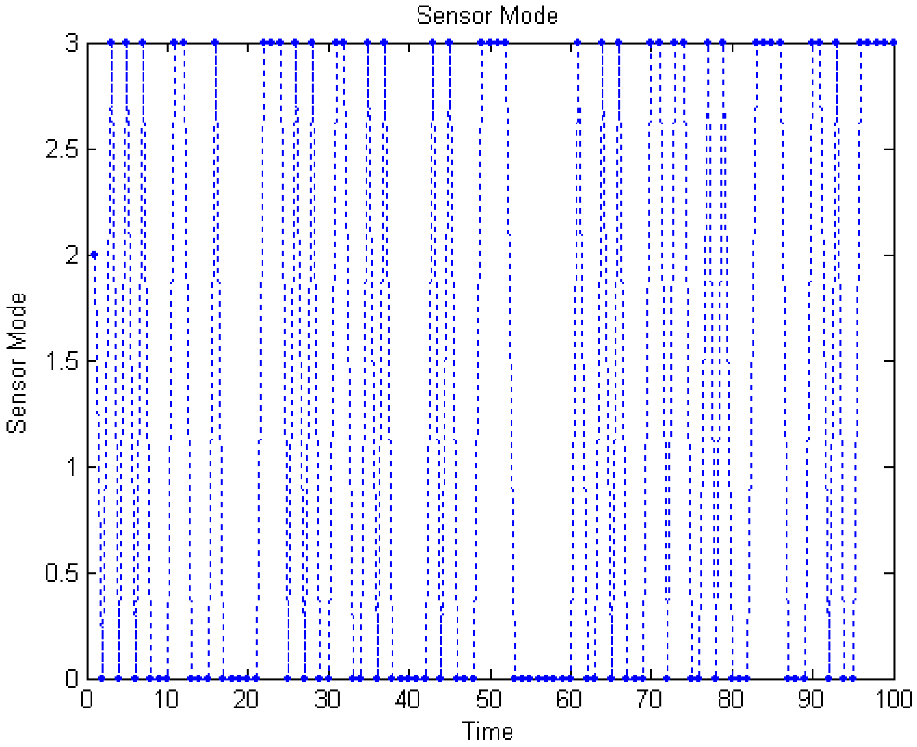
Cyber Sensor 2_confusion matrix = $\begin{pmatrix} .5 & .2 & .3 \\ .2 & .6 & .2 \\ .4 & .1 & .5 \end{pmatrix}$

Enemy Dynamics Simulator

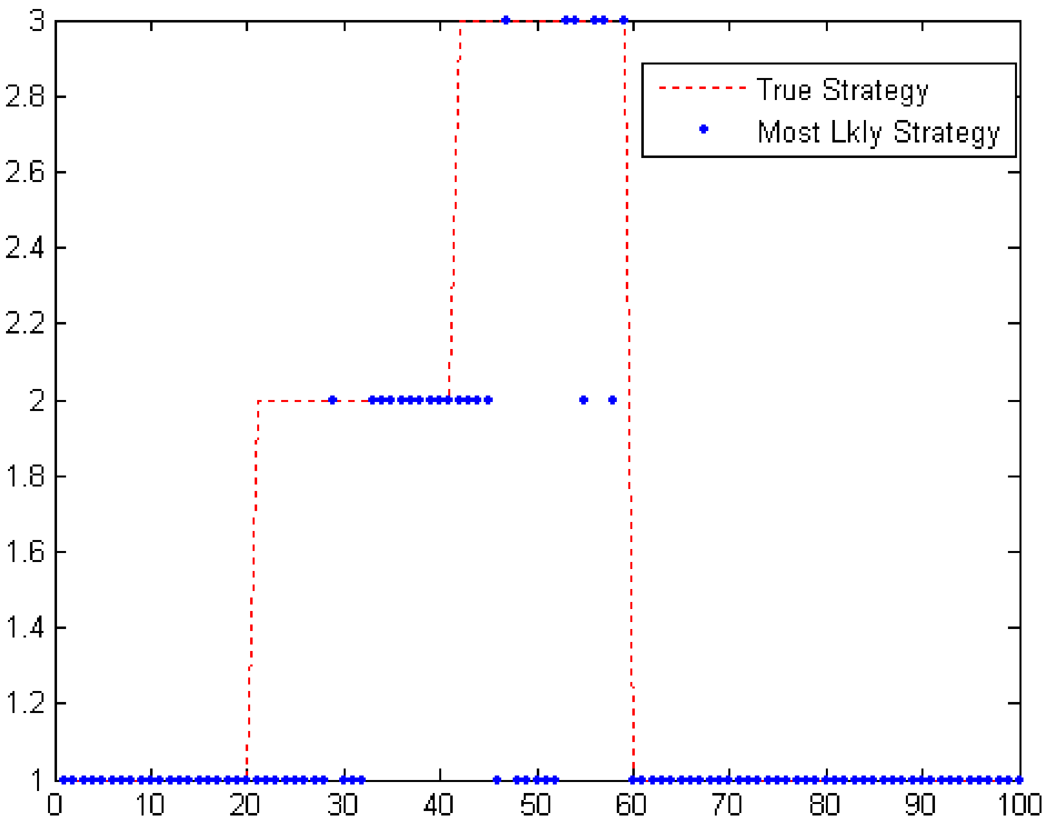
- Modeled by a finite state machine



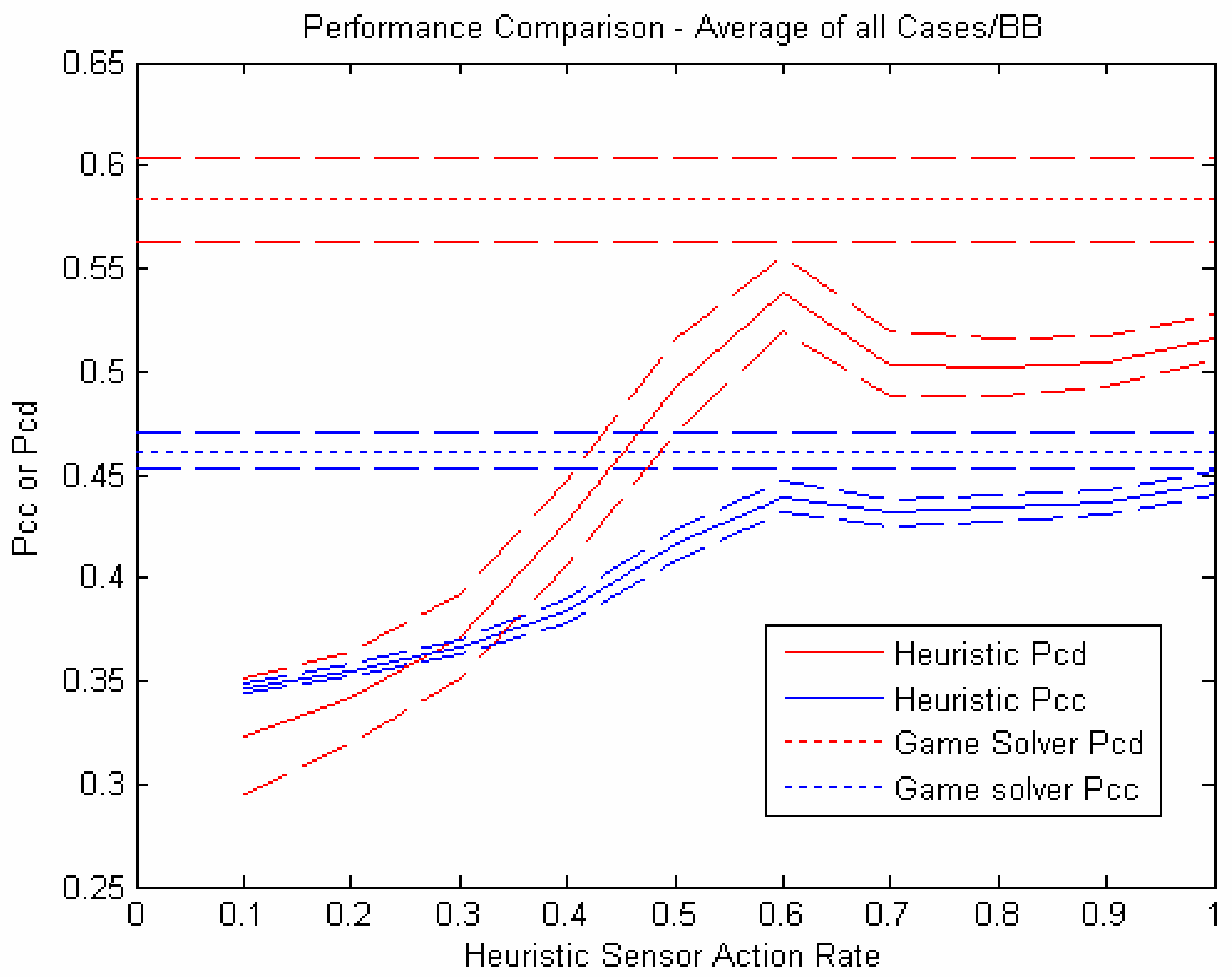
Sensor Mode Selection



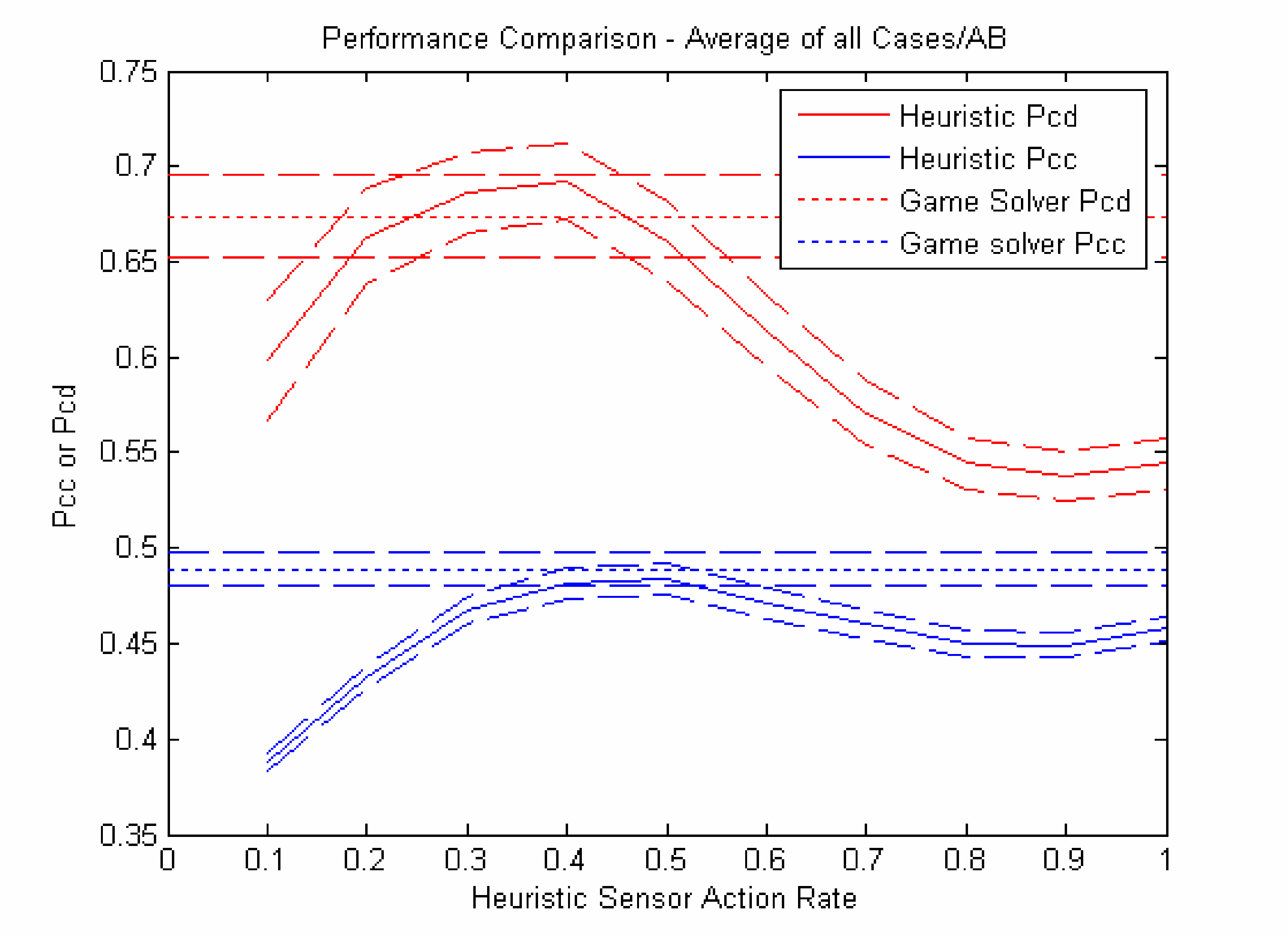
Predicting Adversarial Strategy



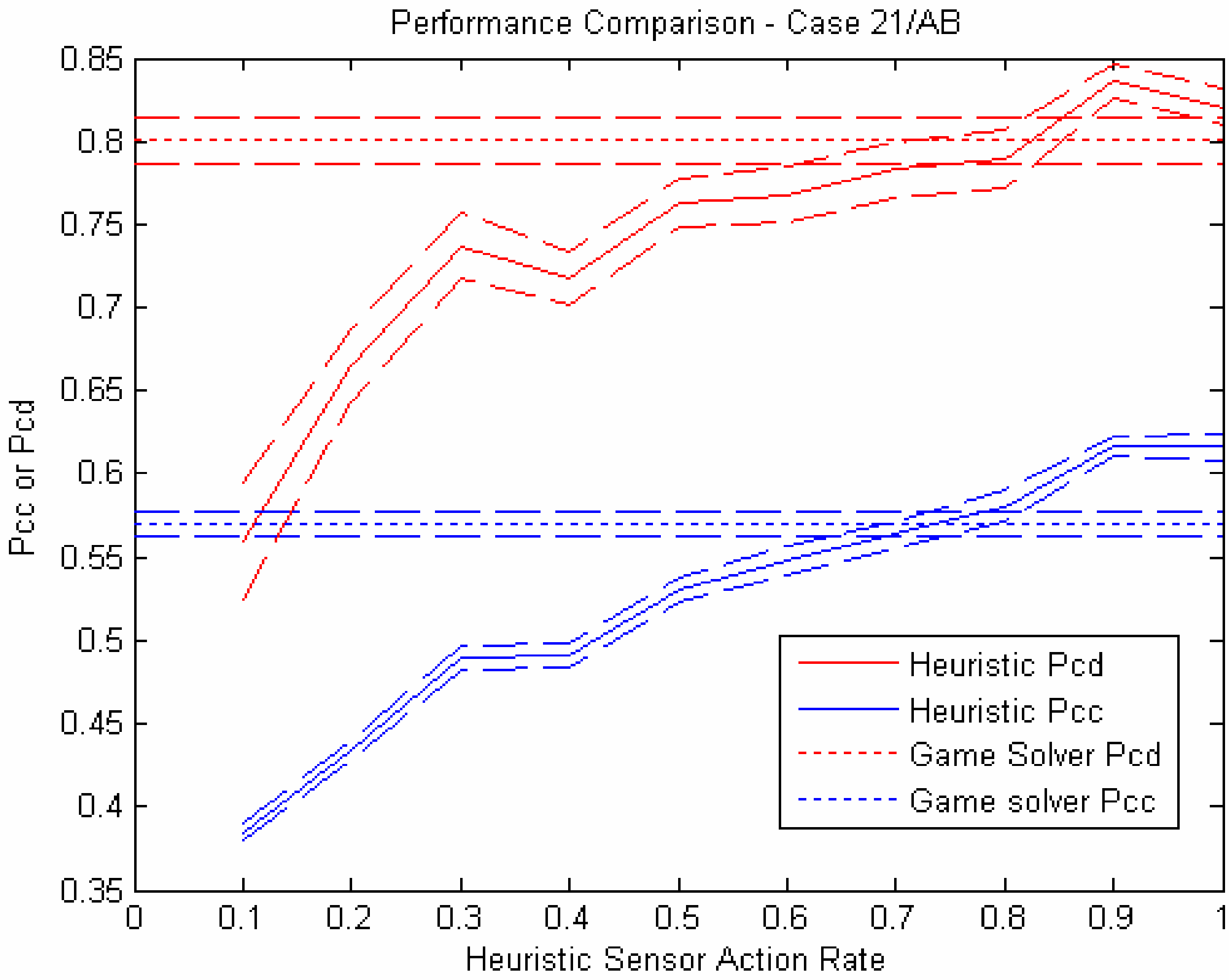
Heuristic Vs. Game Theory (I)



Heuristic Vs. Game Theory (II)



Heuristic Vs. Game Theory (III)



Outline

- Brief history & applications of game theory
- Game theory meets cyber defense
- ***Game theory meets topology***

Nash's Theorem and Searching for Equilibria

Nash's Theorem (PhD Thesis, 1951):

Every N-person non-cooperative game has an equilibrium solution, in pure or mixed strategies

Limitation:

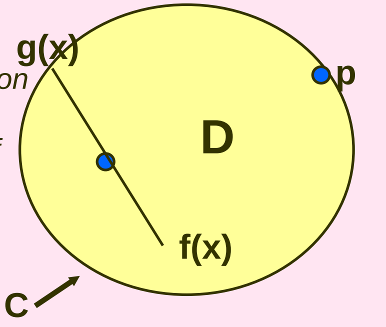
- Essentially an existence theorem
- Not readily obvious how to find them

New Insight

Crux of Nash's Theorem:

It boils down to Browder's fixed point theorem

Thm (Browder): *A continuous function from a ball (of any dimension) to it self must leave at least one point fixed.*



HOW IT WORKS:

Fixed points turn out to be ***equilibrium points***.

New Approach:

Look for fixed points of the strategy space of the following map: $T:\zeta \to \zeta'$ given by formula below

.

$$s_i' = \frac{s_i + \sum_{\alpha} \varphi_{i\alpha}(\zeta)\pi_{i\alpha}}{1 + \sum_{\alpha} \varphi_{i\alpha}(\zeta)}$$

$$\varphi_{i\alpha} = \max(0, p_{i\alpha}(\zeta) - p_i(\zeta))$$

ζ is an n-tuple of mixed strategies

$p_i(\zeta)$ is the corresponding strategy to player *i*

$p_{i\alpha}(\zeta)$ is the payoff to player *i* if he changes to pure α^{th} strategy

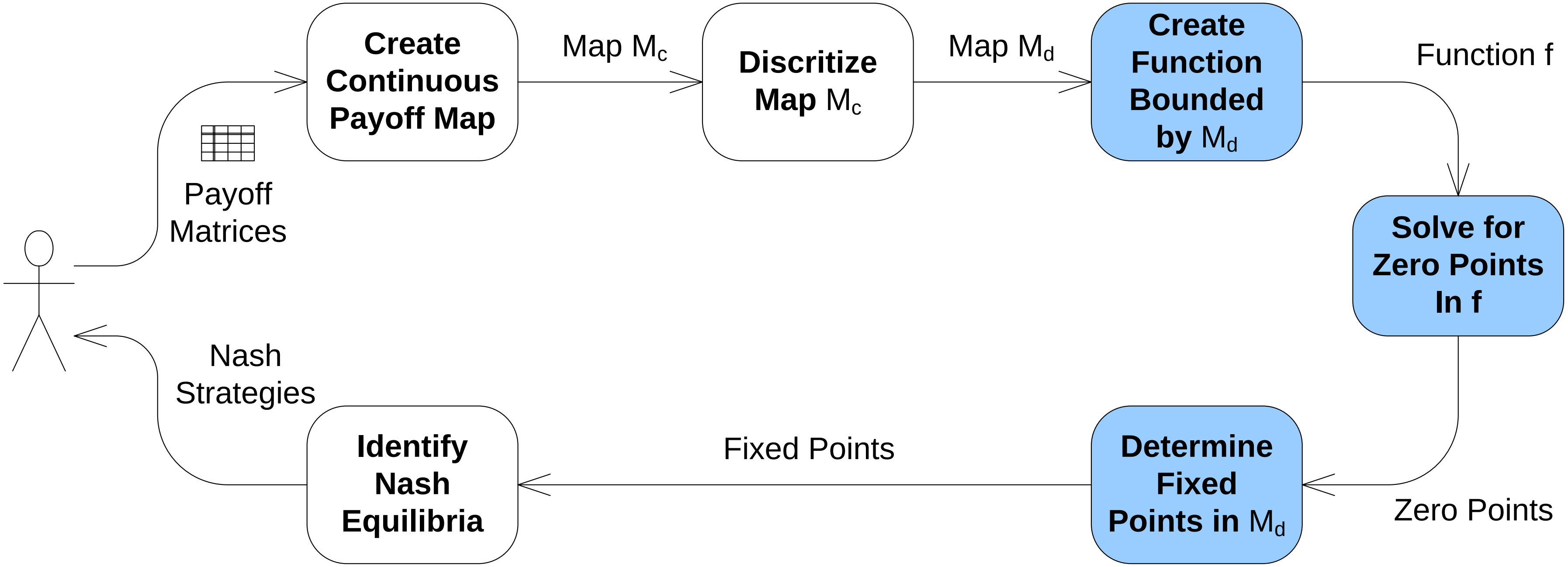
HOW IT WORKS:

Testitilate the strategy space and compute the following measure of fixed-pointed-ness at mesh points $C(\zeta) = \frac{\|T(\zeta)\|}{\|\zeta\|}$

ASSUMPTIONS AND LIMITATIONS:

- Convergence, Yes? Rate of Convergence?
- Scalability?

High-level View



Performance Improvements: Constant Map

Dimensions	Size	Complexity	Prev Solve Time (s)	New Solve Time (s)
3	5x6x5	36	0.015	0.000
5	6x6x6x6x6	1,296	2.500	0.391
3	200x200x200	40,400	28.860	1.062

Performance Improvements: Contract Map

Dimensions	Size	Complexity	Prev Solve Time (s)	New Solve Time (s)
3	5x6x5	36	0.015	0.000
5	6x6x6x6x6	1,296	2.532	0.406
3	200x200x200	40,400	26.922	1.109

Performance Improvements: Rotate Map

Dimensions	Size	Complexity	Prev Solve Time (s)	New Solve Time (s)
2	5x5	5	0.015	0.000
2	200x200	200	0.031	0.016

New Strategies for Large Problem Spaces for fixed point problem

- Chen/Deng provided “Cut” algorithm based on Dynamic Programming technique with algorithmic complexity $O(d^2(2n)^{d-1})$
  - As dimensions increase, memory needs explode
  - Example d=10, n=6 : complexity=10,077,696

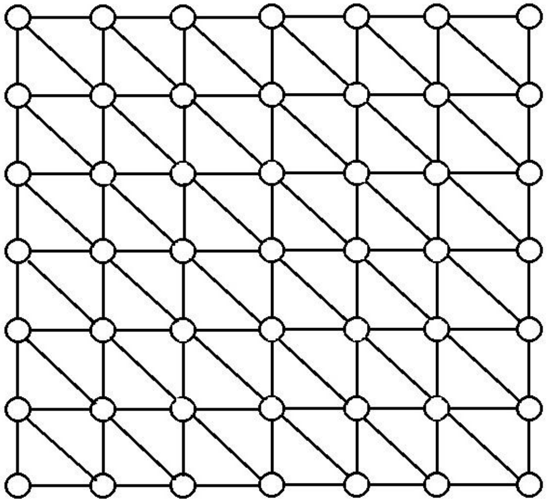
Nash is PPAD – compute PH

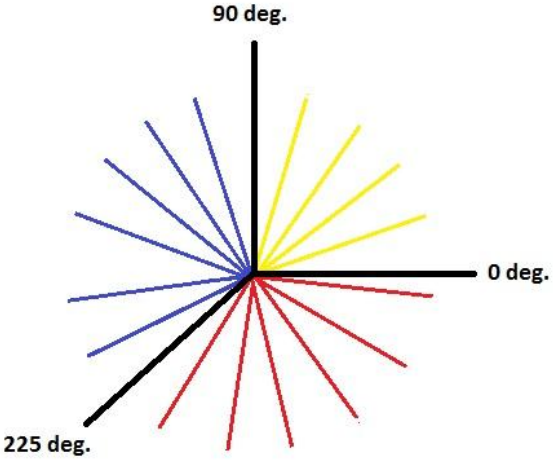
1. Reduce NASH to Brower.

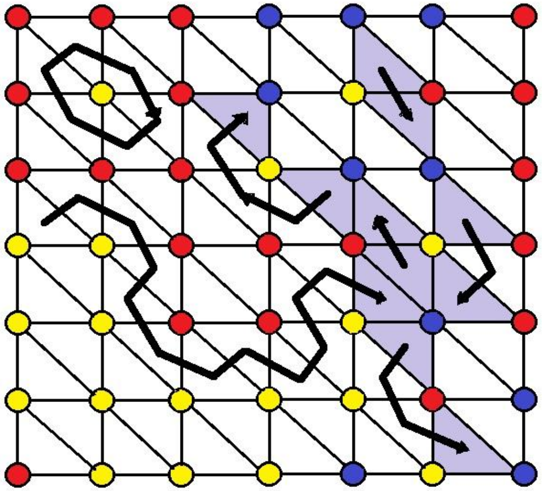
2. Reduce Brower to EOTL.

3. This implies NASH can be reduced to EOTL.

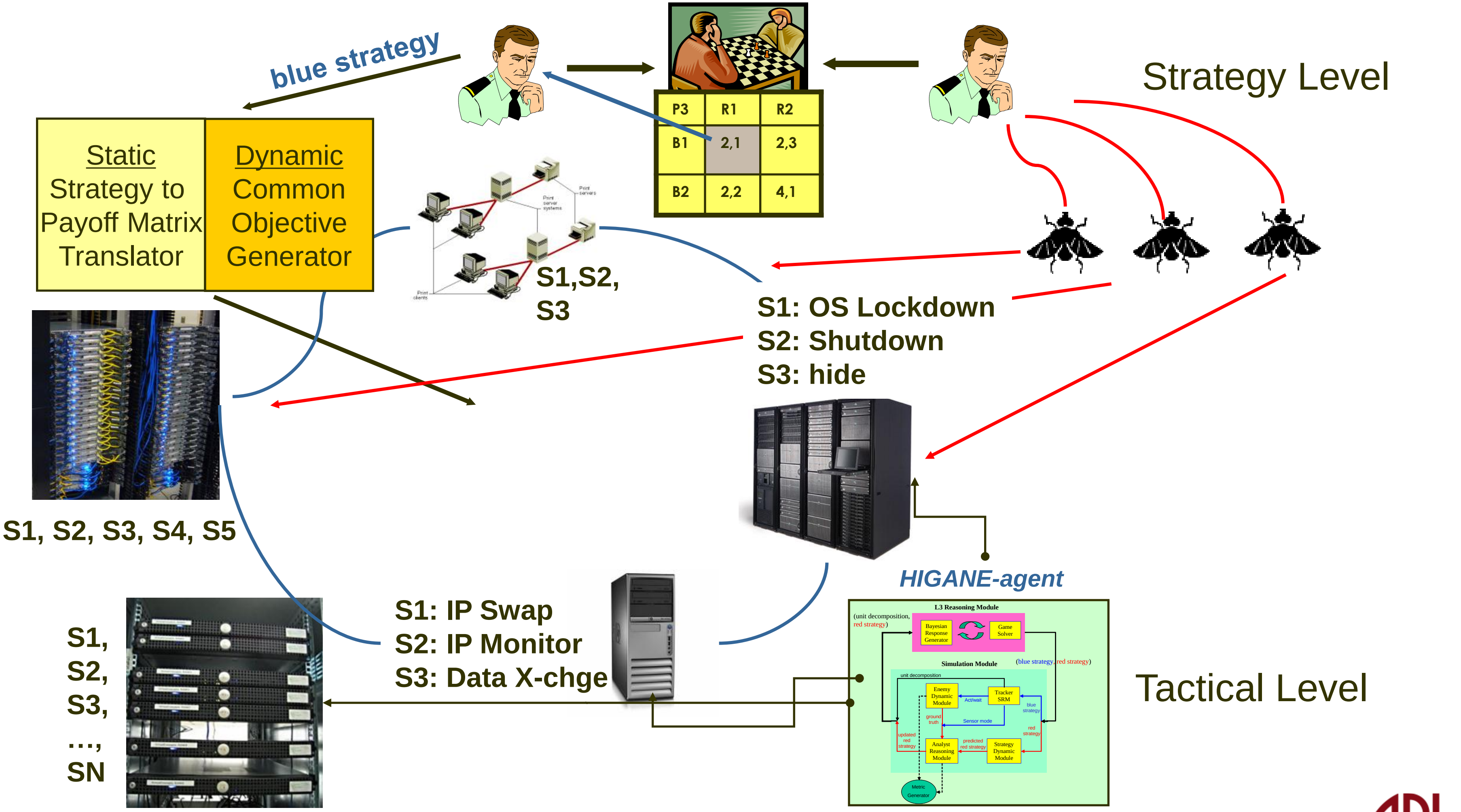
4. NASH is PPAD.







How can we agree?



blue strategy

P3	R1	R2
B1	2,1	2,3
B2	2,2	4,1

Strategy Level

Static Strategy to Payoff Matrix Translator

Dynamic Common Objective Generator

S1,S2, S3

S1: OS Lockdown
S2: Shutdown
S3: hide

S1, S2, S3, S4, S5

HIGANE-agent

S1: IP Swap
S2: IP Monitor
S3: Data X-chge

S1,
S2,
S3,
…,
SN

Tactical Level

Consensus Bundles on Networks

N = network

O = Opinion space

T = Topic space

X = clique complex of N

$$\xi = (O, E, X) \text{ Bundle of Opinions on } T$$

$\xi_{|X_0}$ = individual opinions

$\xi_{|X_p} = p -$ fold consensus

What's the obstruction to agreement?

When do the opinions of the whole override individual or smaller group disagreements?

Homology and Cohomology with Twisted Coefficients

X = simplicial complex

$R = \mathbb{Z}\pi_1(X)$

$\tilde{X}$ universal cover of X

M an R module

$$H_p(X, \tilde{M}) := H_p(C_*(\tilde{X}) \otimes_R M)$$

$$H^p(X, \tilde{M}) := H^p(Hom(C_*(\tilde{X}), M))$$

Obstruction Theory

$$\nu_k \in H^k(X, \tilde{\pi}_{k-1}(V_{d-k+1}F))$$

Obstruction to finding n-k+1

linearly independent sections

over the k-skeleton of X

Key idea:

Start with a co-cycle

Cohomologous to 0 means

it can be redefined to extend.

Consensus.

Outline

- Brief history & applications of game theory
- Game theory meets cyber defense
- Game theory meets topology
- ***Future ideas towards measurement***

Drivers of State Dynamics

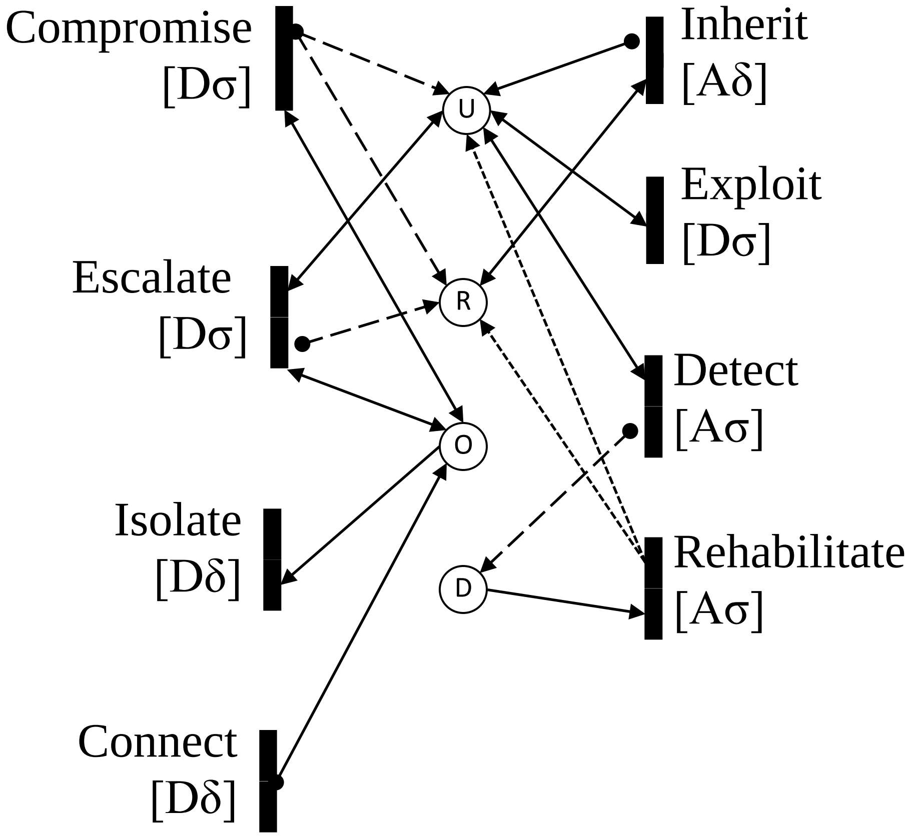
Attacker

- Deliberate
  - Exploit vulnerabilities to achieve increasing levels of privilege on network hosts
  - Use existing privileges to induce mission-critical system faults
- Autonomous
  - Privilege inheritance
  - Data exfiltration
  - Host functionality usurption

Defender

- Deliberate
  - Preemptively isolate hosts
  - Reactively isolate hosts
  - Repair hosts on-line
- Autonomous
  - Repair hosts (on-line or off-line)
  - Detect intrusion/network activity

Model Architecture: Host Specification



U = User access
R = Root access
O = Online host
D = Detected exploit
A/D = Autonomous/Deliberate
σ/δ = Stochastic/Deterministic

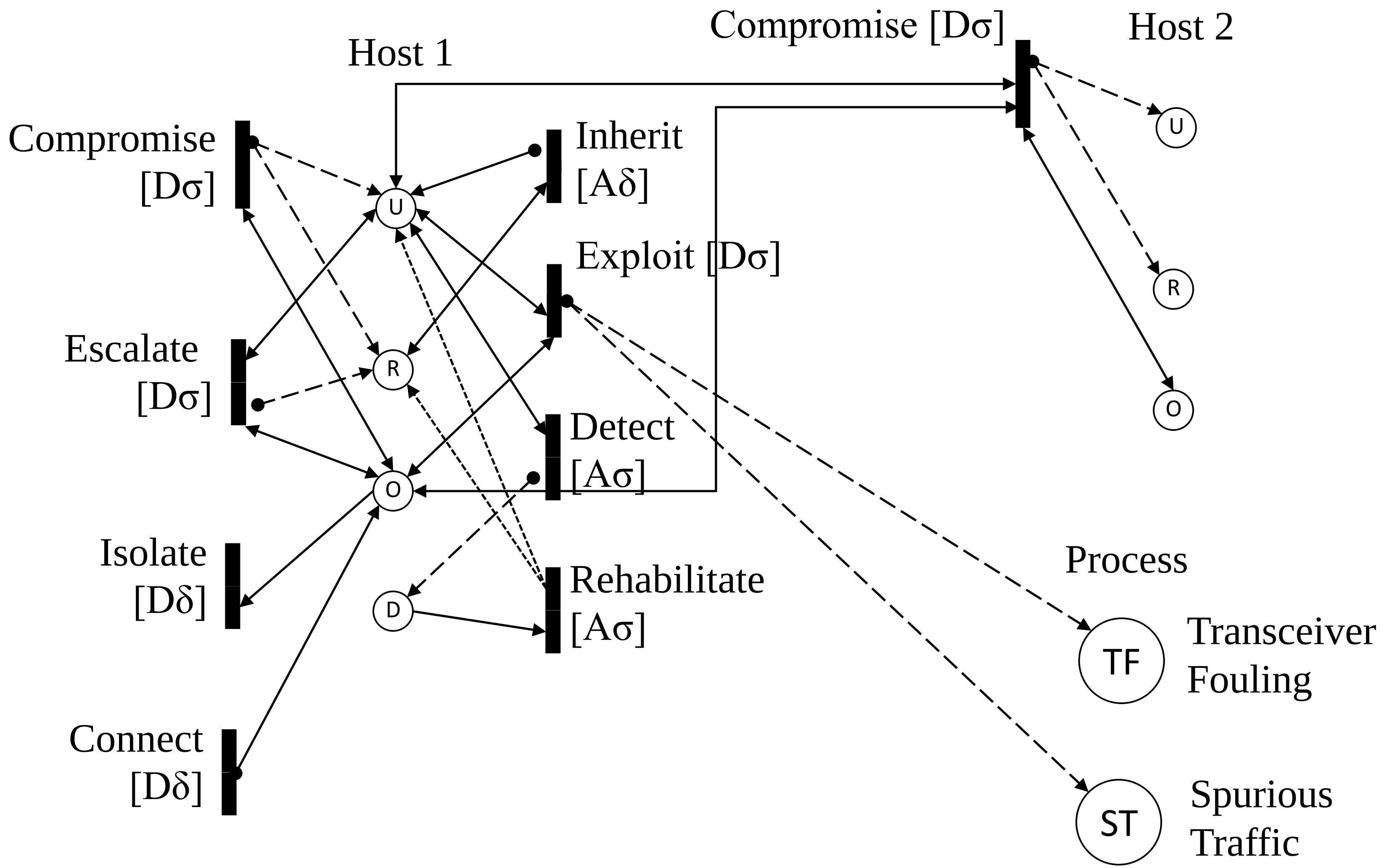
Compromises [Dσ]
couple hosts to hosts

Exploits [Dσ]
couple hosts to functionality

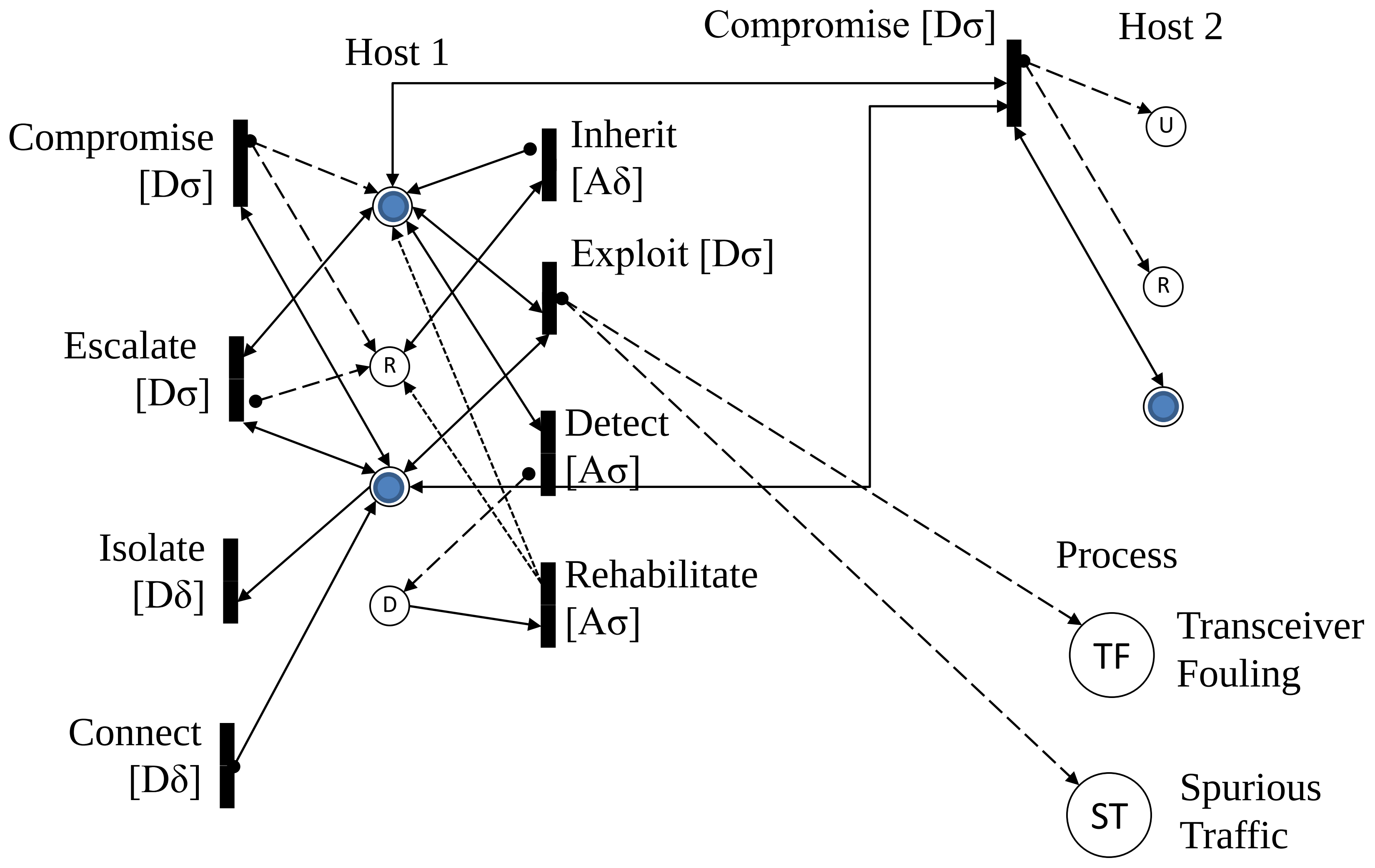
Decision Transitions [D]
couple the PN to the CMDP

Stochastic Transitions [σ]
spawn new branches in the tree

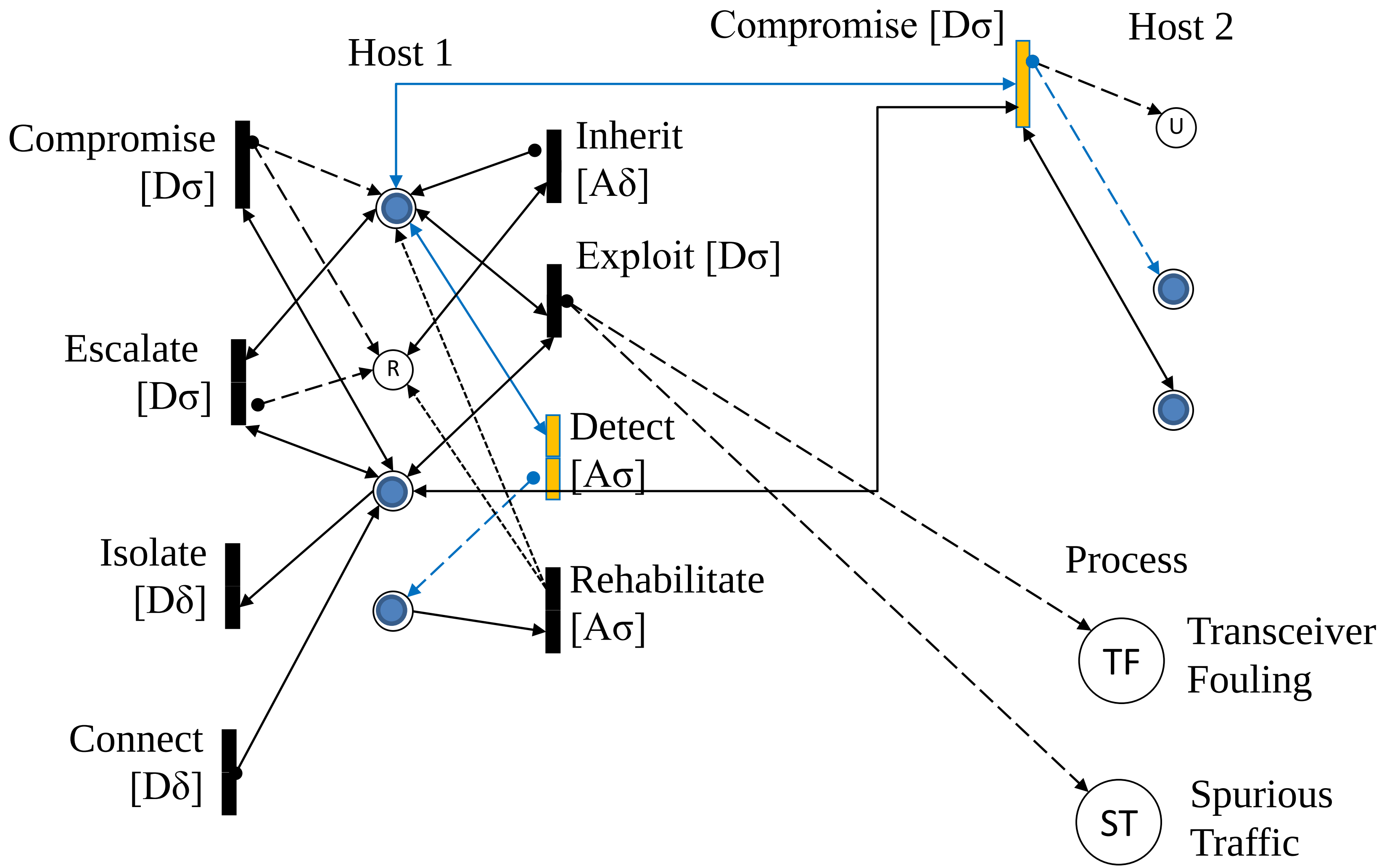
Model Architecture: PN Construction



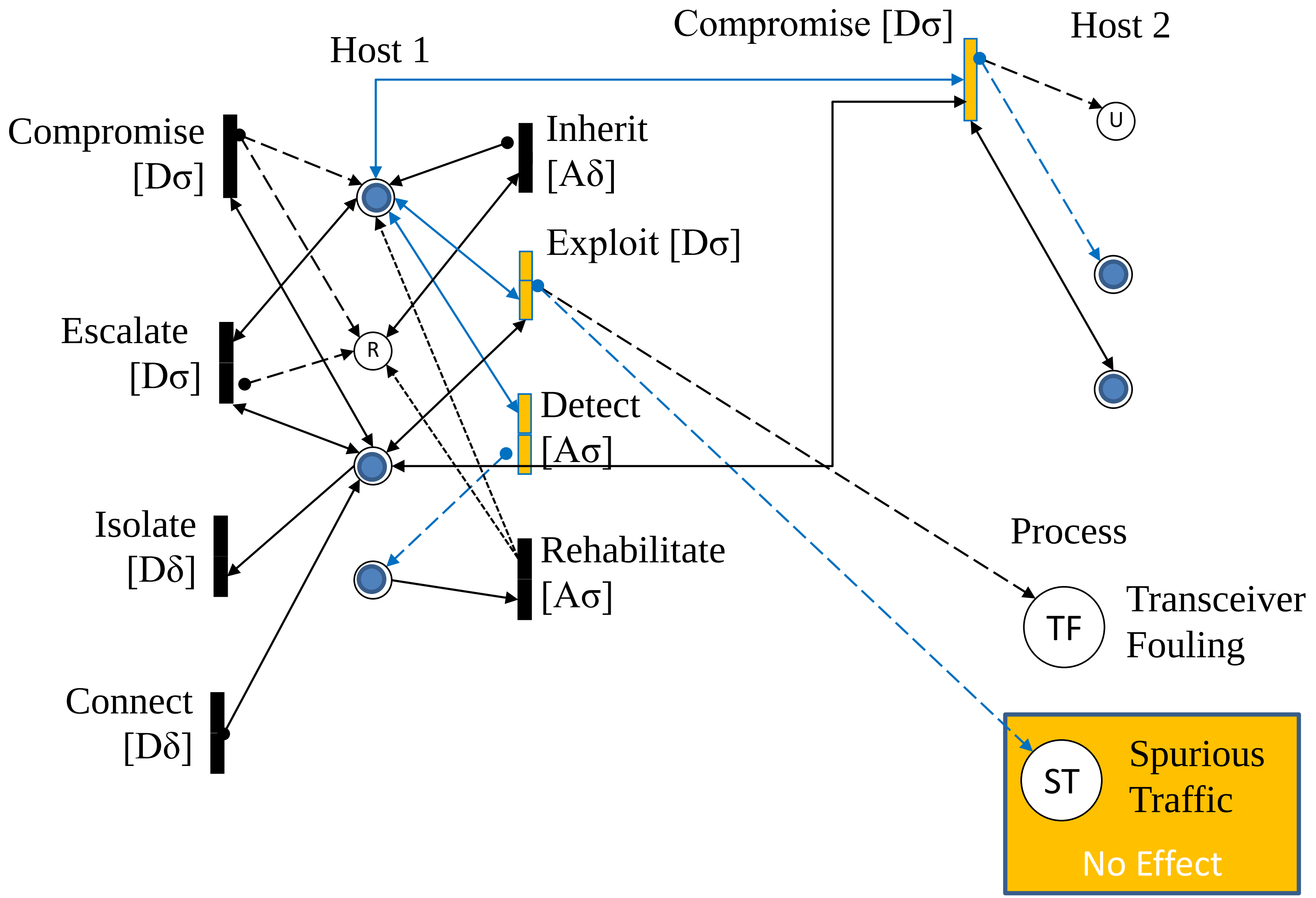
Example: Initial State



Attacker Attempts to Increase Access



Attacker Attempts to Send Spurious Traffic

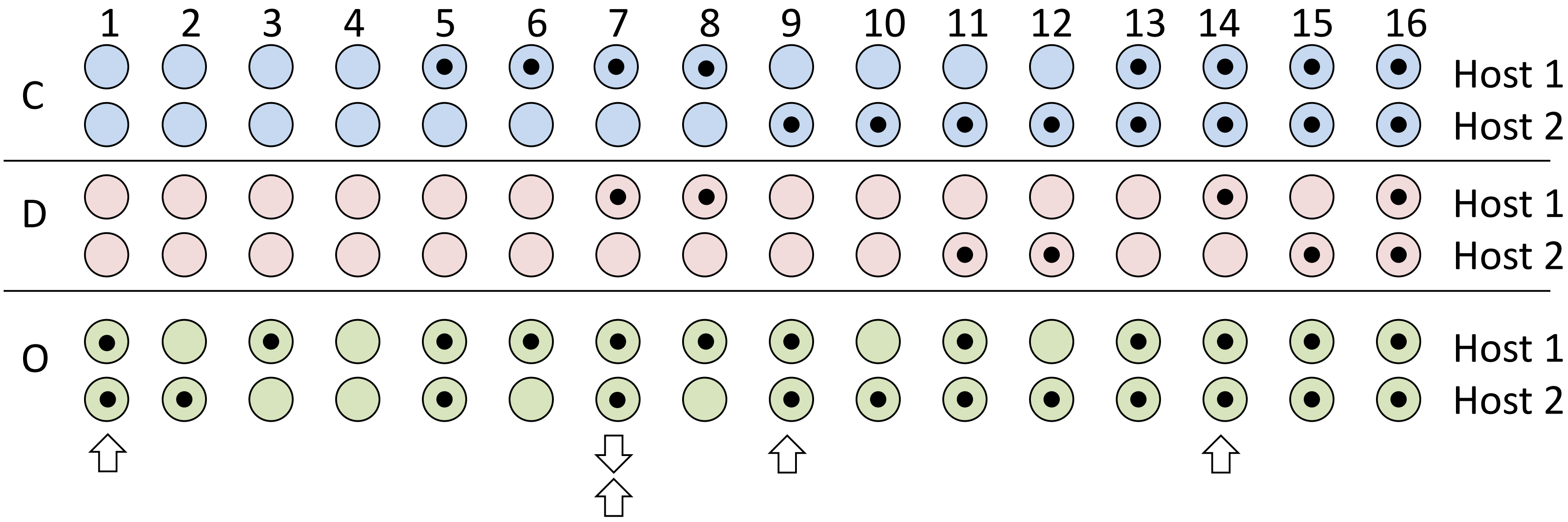


Transition Probabilities

Consider 2 hosts, on each of which 3 conditions are defined:

host is compromised (C), attack detected (D), host is online (O)

- Currently in State 7
- One Possible Attacker Action: Compromise Host 2 (C2)
- One Possible Defender Action: Remove Privileges Host 1 (R1)



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
C	○	○	○	○	●	●	●	●	○	○	○	○	●	●	●	●	Host 1
	○	○	○	○	○	○	○	○	●	●	●	●	●	●	●	●	Host 2
D	○	○	○	○	○	○	●	●	○	○	○	○	○	●	○	●	Host 1
	○	○	○	○	○	○	○	○	○	○	●	●	○	○	●	●	Host 2
O	●	○	●	○	●	●	●	●	●	○	●	○	●	●	●	●	Host 1
	●	●	○	○	●	○	●	○	●	●	●	●	●	●	●	●	Host 2

R1 success
C2 fail

R1 fail
C2 fail

R1 success
C2 success

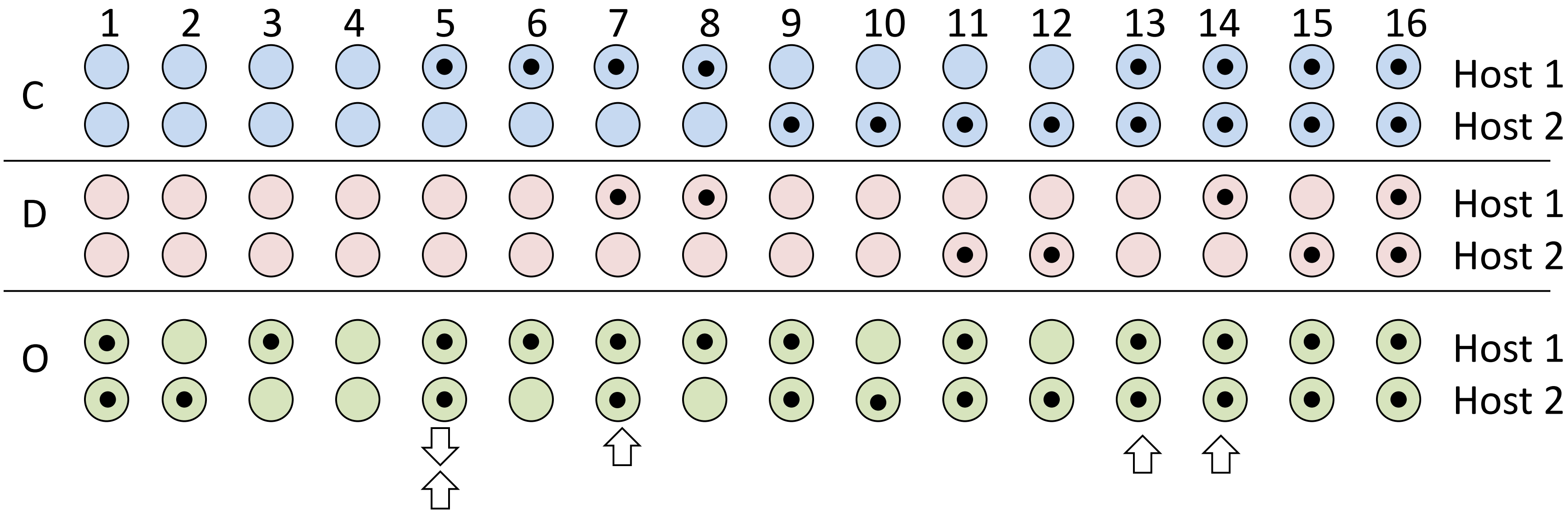
R1 fail
C2 success

Transition Probabilities

Consider 2 hosts, on each of which 3 conditions are defined:

host is compromised (C), attack detected (D), host is online (O)

- Currently in State 5
- One Possible Attacker Action: Compromise Host 2 (C2)
- One Possible Defender Action: Do Nothing



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
C	○	○	○	○	●	●	●	●	○	○	○	○	●	●	●	●	Host 1
	○	○	○	○	○	○	○	○	●	●	●	●	●	●	●	●	Host 2
D	○	○	○	○	○	○	●	●	○	○	○	○	○	●	○	●	Host 1
	○	○	○	○	○	○	○	○	○	○	●	●	○	○	●	●	Host 2
O	●	○	●	○	●	●	●	●	●	○	●	○	●	●	●	●	Host 1
	●	●	○	○	●	○	●	○	●	●	●	●	●	●	●	●	Host 2

C2 fail

C2 fail
D1 (detection)

C2 success

C2 success
D1 (detection)

Strategy Space, *example*

ATTACK STRATEGIES

- WEB DEFACEMENTS AND SEMANTIC ATTACKS
- DOMAIN NAME SERVICE (DNS) ATTACKS
- DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS
- WORMS
- ROUTING VULNERABILITIES
- INFRASTRUCTURE ATTACKS
- COMPOUND ATTACKS
- WHEN TO ATTACK
- WHERE TO ATTACK

Counter ACTIONS STRATEGIES

- Shut down the network
- Reconfiguration of Hosts
- Renumbering of IP addresses
- Moving critical data between different hosts
- Revealing part of the system

	R1	R2	R3	R4	R5	R5
B1	0	-1	2	2	2	2
B2	1	0	-1	2	2	2
B3	-2	1	0	-1	2	2
B4	-2	-2	1	0	-1	2
B5	-2	-2	-2	1	0	-1
B6	-2	-2	-2	-2	1	0

Blue = (¼, ½, ¼,0, 0, 0) vs. Red = (¼, ½, ¼,0, 0, 0)

THANK YOU!!!

- ***Wishing you a very MERRY Christmas!!!***