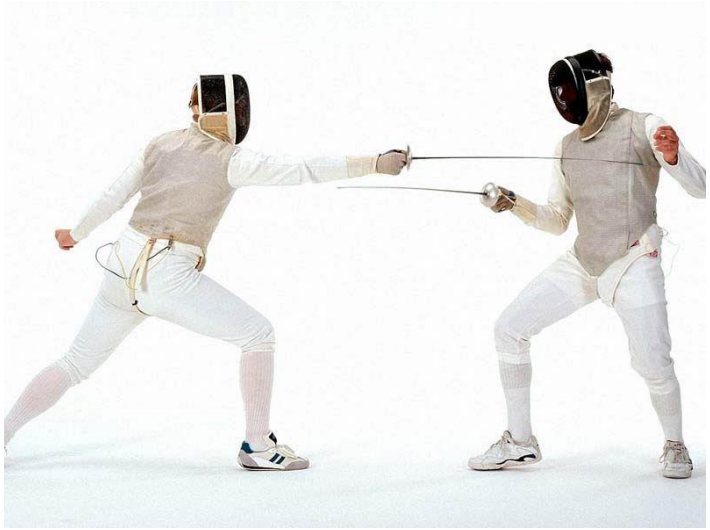
Moving Target Defense and Intelligent Cyberdeception



Ankur, Akshay, Chonghao, Zack

CSE591 Spring 2019

Feb 06, 2019

Ira A. Fulton Schools of Engineering
ARIZONA STATE UNIVERSITY

Agenda

1. **Moving Target Defense (MTD)**
   - What is MTD?
2. MTD Concepts and Network MTD
3. Application of MTD against cyber attacks (DDoS Case Study)
4. Intelligent Cyberdeception – Game Theoretic MTD Modeling.
5. MTD Effectiveness Evaluation
6. Conclusion and Research Opportunities

What is MTD? – Shell Game?

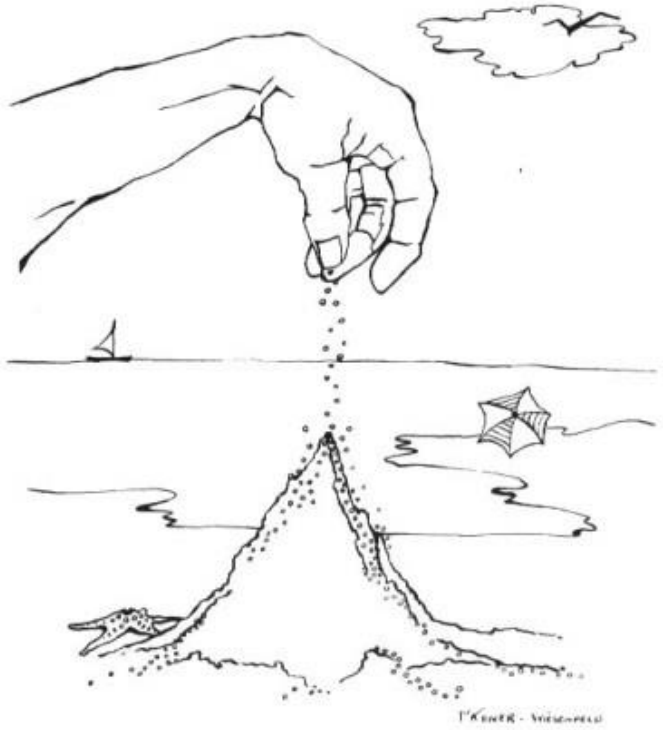
Static Target

vs

Moving Target

Motivation – MTD Challenge

- The challenge is to demonstrate that MTD introduced complexity is indeed a benefit and not a liability.



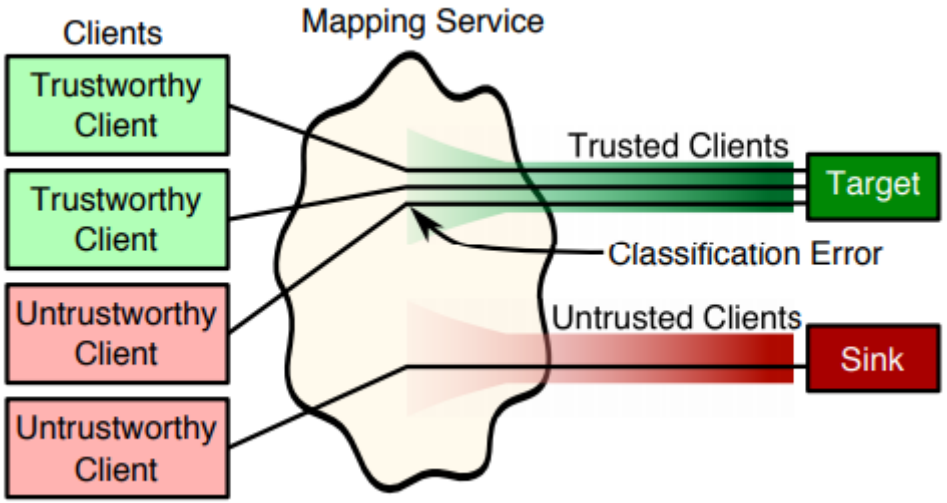
MTD Concepts and Network MTD

Network-based MTD

- Network reconnaissance is the first step for attackers to collect network and host information and prepare for future targeted attacks.
- Goal: reduce attack surface and enhance defense surface, i.e., make the scanning results expire soon or give the attacker a different view of the target system
- Examples: IP randomization, Port randomization

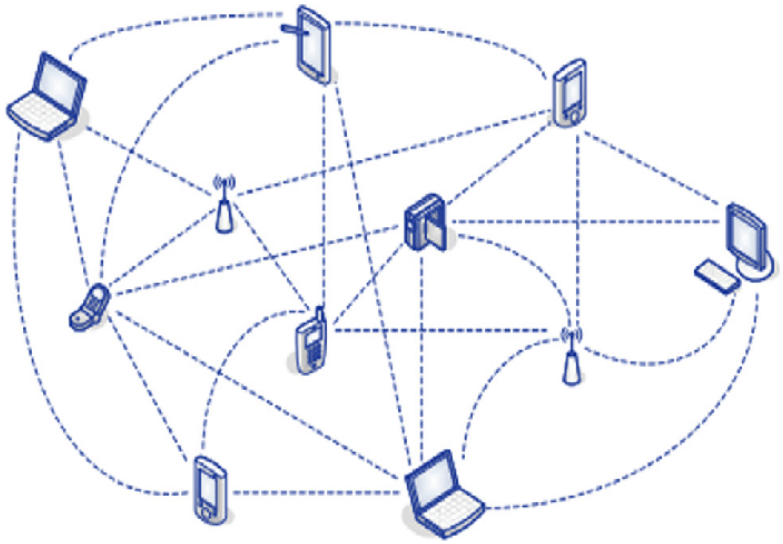
Network-based MTD

Overview:



Cyber Maneuvers Concepts

- Mobile Ad-Hoc Network (MANET)

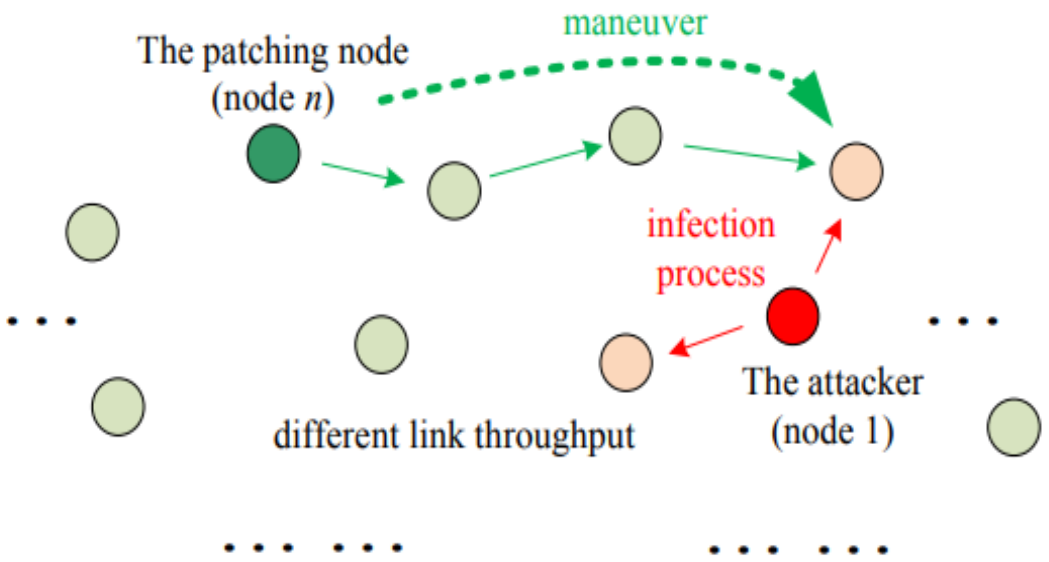


Cyber Maneuvers Concepts

- Cyber maneuver
  - An action in the cyber space towards achieving the goal in a mission
  - Examples: software upgrade, patching, node isolation/blocking, …
  - Type: reactive / proactive

An Analytical Framework

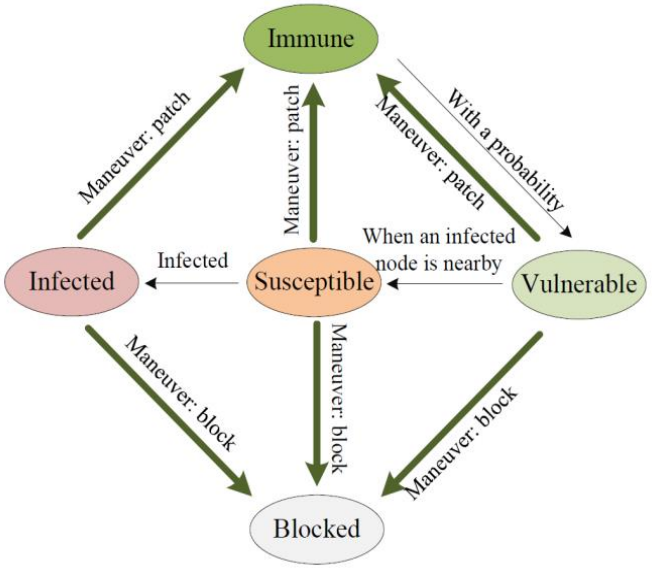
- Network model and attack scenario



An Analytical Framework

- Node States:

  S = {0: Patched, 1: quarantined, 2: blocked, 3: vulnerable, 4: susceptible, 5: infected}



Capability values used in simulations.

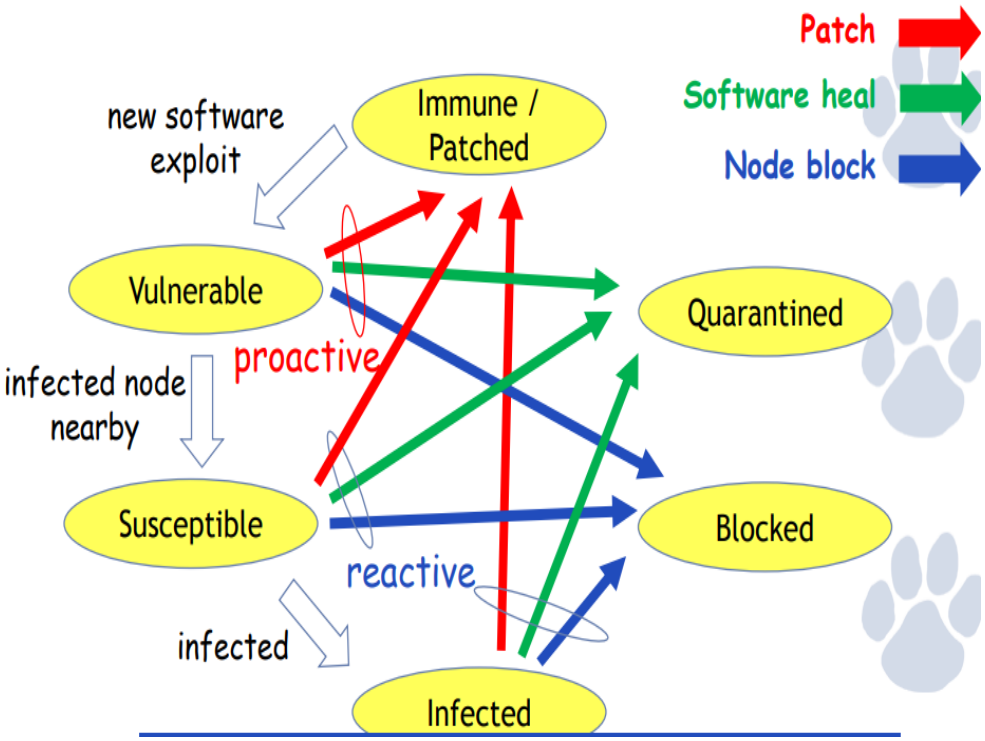
Immune:	4
Vulnerable:	2
Susceptible:	1
Infected:	0
Blocked:	0

An Analytical Framework

- Cyber maneuvers:

M = {M_0: No action, M_1: Patch, M_2 : Software Heal, M_3: Node Block}

Cost: $M_1 > M_2 > M_3 > M_0$



Goals and Strategy

- Maximize the lifetime of a critical path
- All nodes on the path must not be affected
- Sum of capabilities of all nodes in the network should be maximized
- And multiple constraints

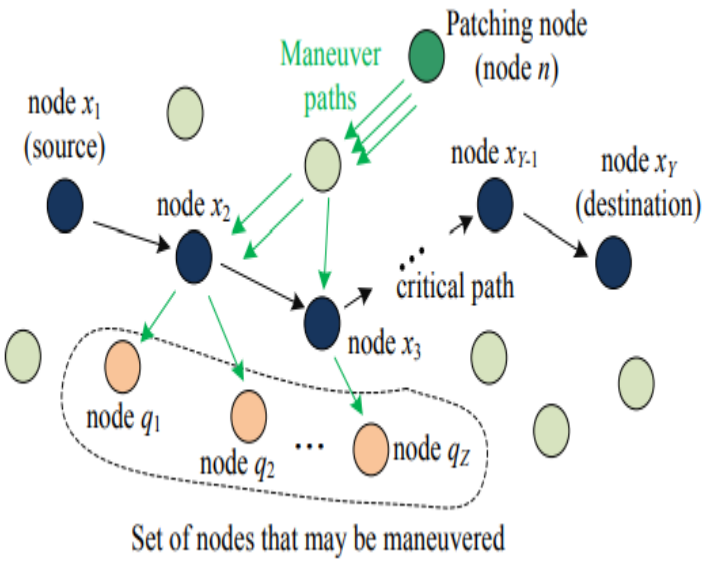
Cannot satisfy all at the same time

- Cost should be minimized…
- Based on two views: current view, statistical view

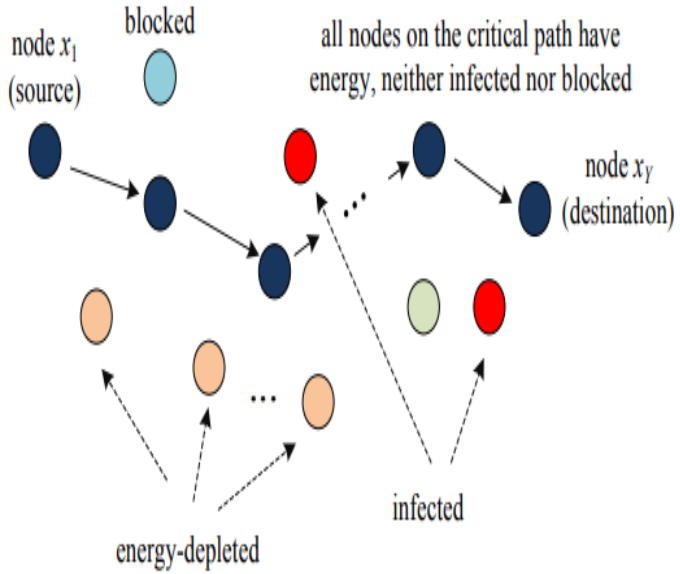
Ira A. Fulton Schools of Engineering
ARIZONA STATE UNIVERSITY

Current view vs. Statistical view

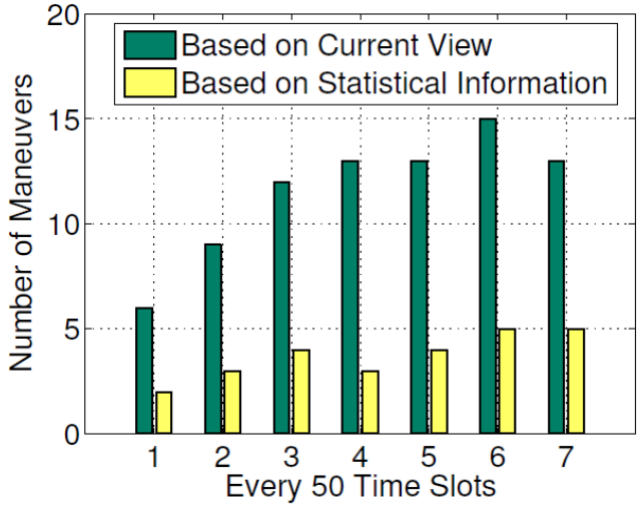
Current

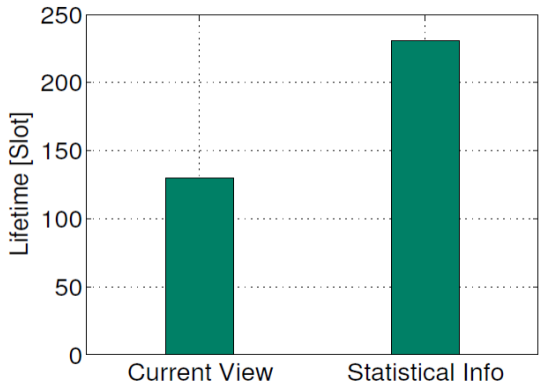


Statistical



Results


Based on Current View
Based on Statistical Information
Number of Maneuvers
0
5
10
15
20
1
2
3
4
5
6
7
Every 50 Time Slots


Lifetime [Slot]
0
50
100
150
200
250
Current View
Statistical Info


Lifetime [Slot]
0
50
100
150
200
250
Correct
Minor−error
Random

Key Insights

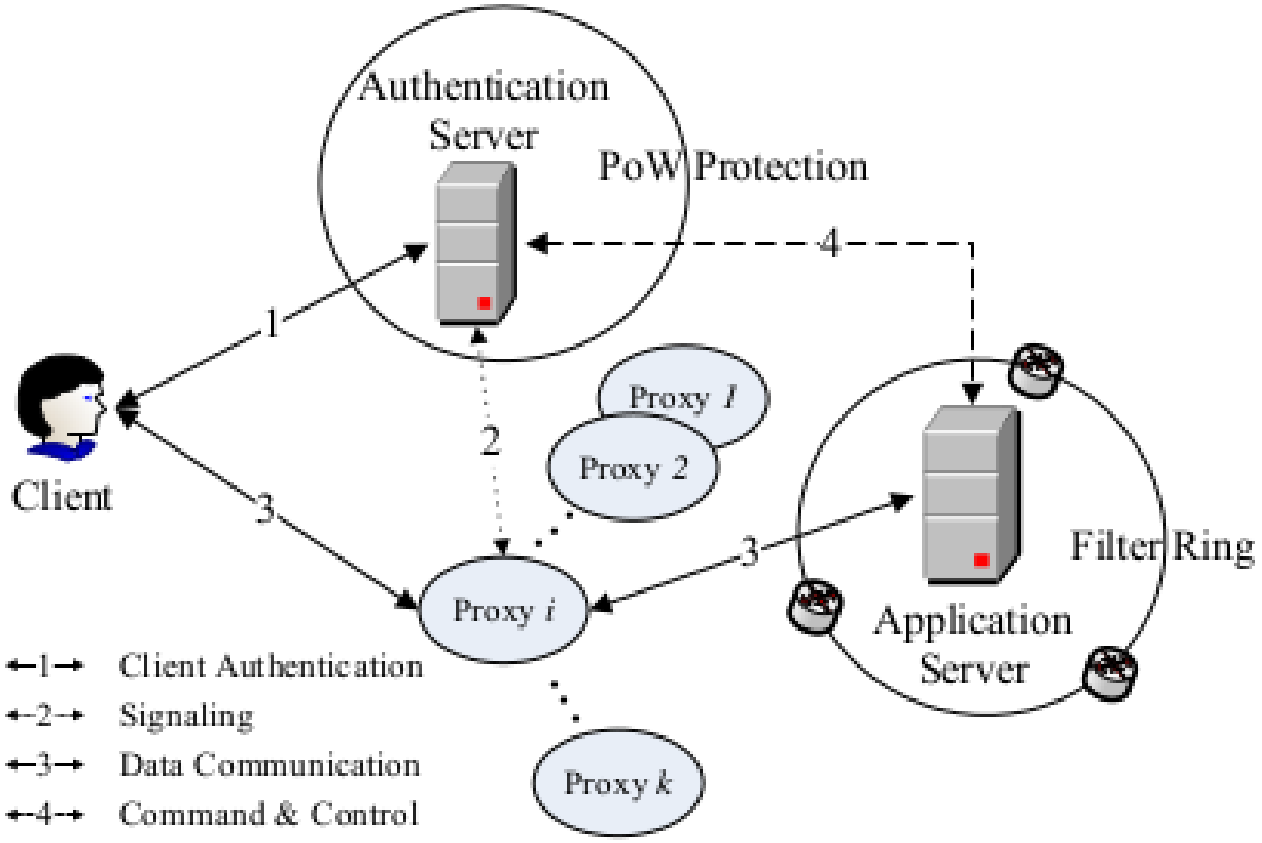
- Accurate statistical info is a key enabler for proactive cyber maneuvers for critical path protection
- **Less info**, **less proactive** strategies
- **Wrong info**, **worse** than knowing nothing

Application of MTD against Cyber Attacks (DDoS Case Study)

MTD Application against DDoS

- Significant number of increase in number of DDoS attacks of higher capacity and lower cost to attack
- What can be done?
  - Static approaches
  - Dynamic approach
- How can it be effective? (MTD timing problem)

MOTAG: Threat Model and Architecture



MOTAG: Client to proxy shuffling

- To mitigate insider attacks
- Problems
  - Finding the insider (who, how many)
  - Shuffling strategy
  - Shuffling Optimization: Maximize number of innocent clients with given number of shuffling proxies
- Solution:
  - The Greedy Shuffling Algorithm
  - Estimating number of insiders

MOTAG: Shuffling Algorithm

- Recursive Greedy approach
- 4 cases
  - If (clients ≤ proxies) assign to 1 proxy per client
  - if (proxy = 1 assign) all clients to the proxy
  - if (insiders = 0) evenly distribute clients
  - else find a number of clients per proxy that maximize number of client not under attack

$$E(N_{cu}) = \sum_{j=1}^{K} p_j A_j = \frac{\sum_{j=1}^{K} \binom{N-A_j}{N_i} A_j}{\binom{N}{N_i}}$$

- Estimating number of insiders is crucial

MOTAG: Results

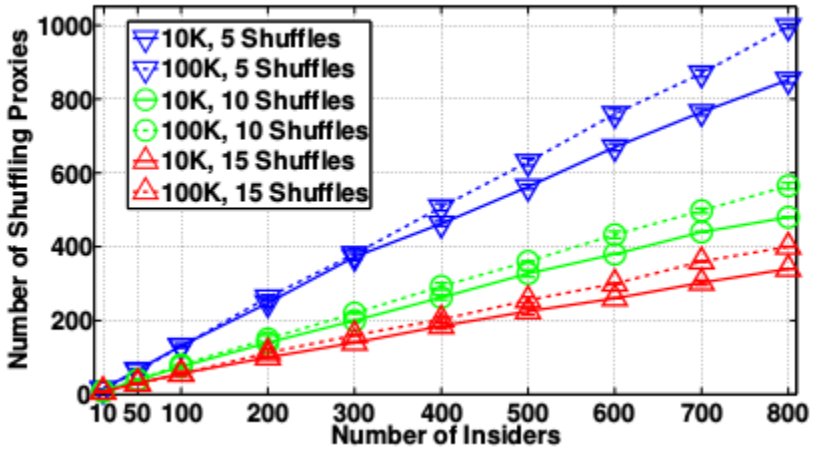


TABLE I
LATENCY OVERHEAD INTRODUCED BY PROXY INDIRECTION

	Direct	Indirect			
	RTT	Mean RTT	Overhead	Max RTT	Overhead
1	63ms	104ms	63.35%	143ms	125.41%
2	86ms	99ms	15.64%	128ms	49.45%
3	83ms	102ms	23.73%	133ms	60.47%
4	90ms	112ms	23.77%	131ms	45.18%
5	84ms	107ms	27.73%	120ms	42.48%

TABLE III
TIME TO SWITCH BETWEEN TWO PROXY NODES (SECONDS)

1	2	3	4	5
1.155	1.158	1.529	1.378	1.286

TABLE II
THROUGHPUT OVERHEAD INTRODUCED BY PROXY INDIRECTION (MB/S)

	1	2	3	4	5
Direct	90.66	83.46	86.24	123.30	121.20
Indirect	15.20	14.46	13.99	15.97	14.09

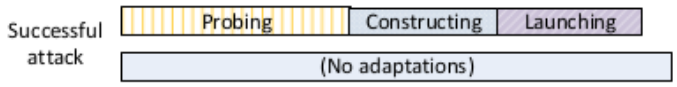
MTD timing problem

- MTD: Dynamic or unpredictable system/Network configurations AKA adaptation techniques
- Approach is promising. However, it comes with an overhead.
- Need to balance how much a system should be dynamic
- Reasonable to endure risks of being attacked if adaptation cost is high and resources are not much critical

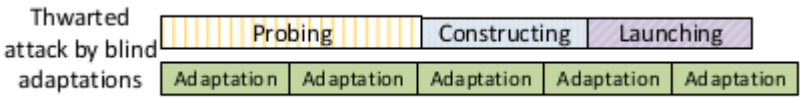
Criticality of timing of adaptations

- Attacks generally take place in phases
  - Probing
  - Constructing
  - Launching
- We want to increase cost of probing and attacking
- Adaptation before the launching phase is the key
- Let's discuss few strategies

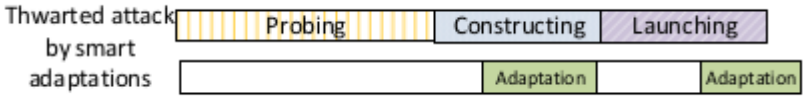
- No adaptation



- Blind adaptation



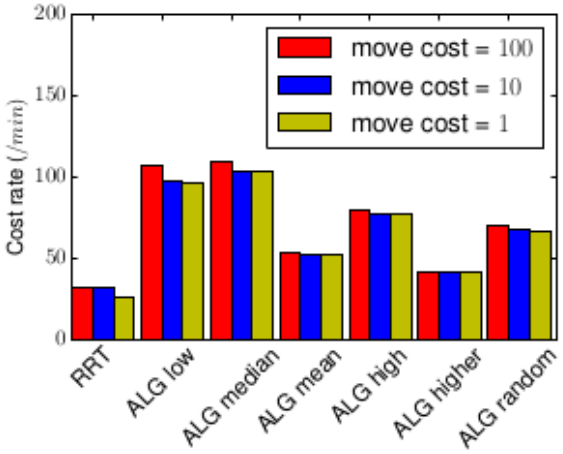
- Smart Adaptation



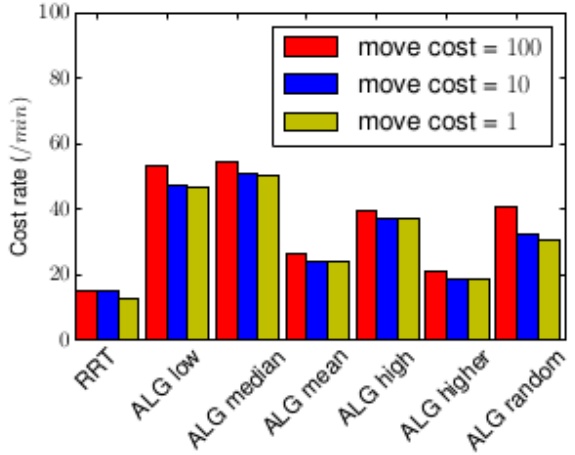
Algorithm for solving MTD timing problem

- Algorithm:
  - Measure cost of attack and cost of adaptation
  - Calculate time for next adaptation
  - Make adaptation if
    - Waited till calculated time
    - System is under attack
- Assumes defender can identify attacks

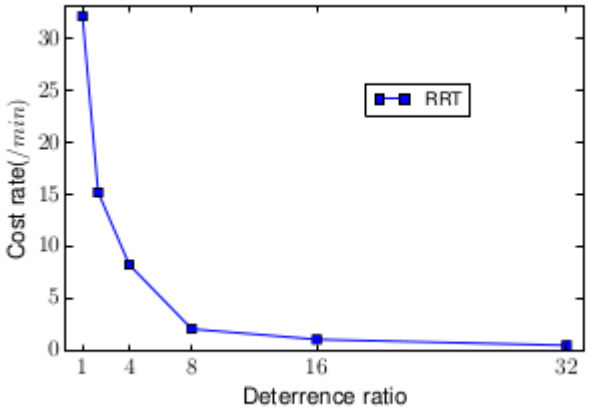
Comparison of the Algorithm

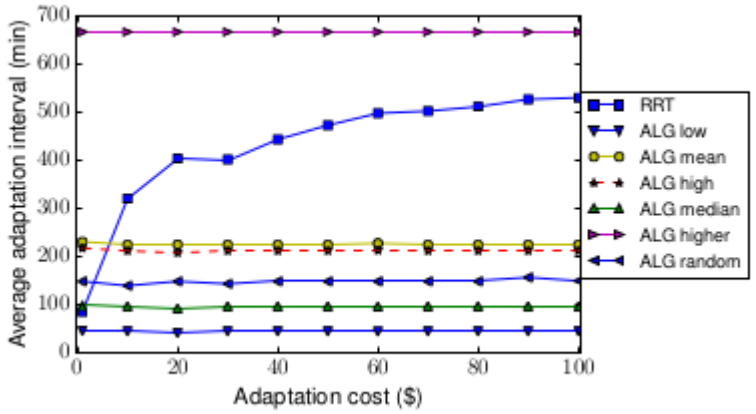


(a) Original attack traces



(b) Attack traces with deterrence ratio = 2





Ira A. Fulton Schools of Engineering
ARIZONA STATE UNIVERSITY

Intelligent Cyberdeception – Game Theoretic MTD Modeling - Ankur

Very Very Short Game Theory Tutorial

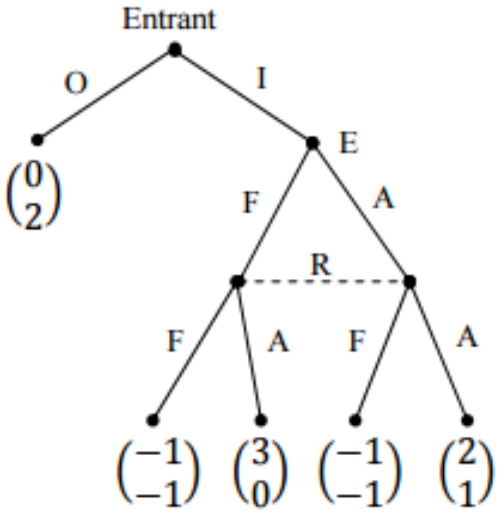
- Type of game (Static, dynamic, single player, multi-player)
- Information (No information, partial information, complete information)
- Players, States, Actions, Utilities
- Modeling – Normal form, Extensive form.

Prisoner's Dilemma – Payoff Matrix

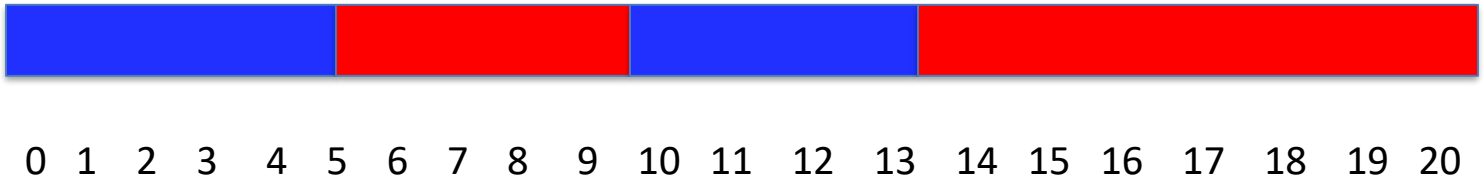
ROW \ COL	Co-operate	Defect
Co-operate	(3, 3)	(0, 5)
Defect	(5, 0)	(1, 1)

Preference to Move Based on Higher Payoff

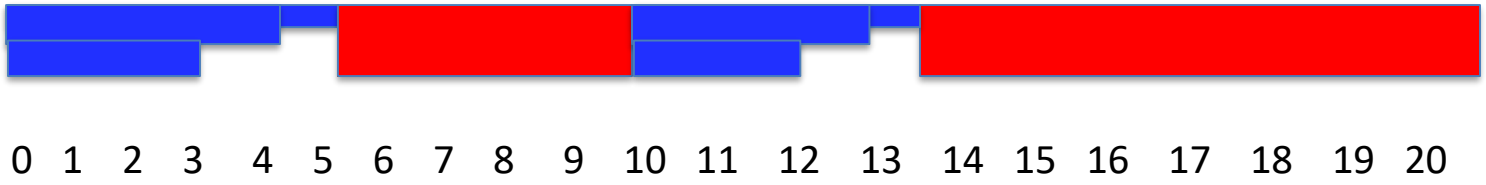
Nash Equilibrium



FlipIt Game Example



FlipIt Game



Progressive FlipIt Game

Game Specifications

- M = 10 instances.
- The attacker may attempt to wrest control of a server through a probe action, which succeeds with some probability
- Otherwise increases the success probability of subsequent probes
- The defender may at any time reimage a server

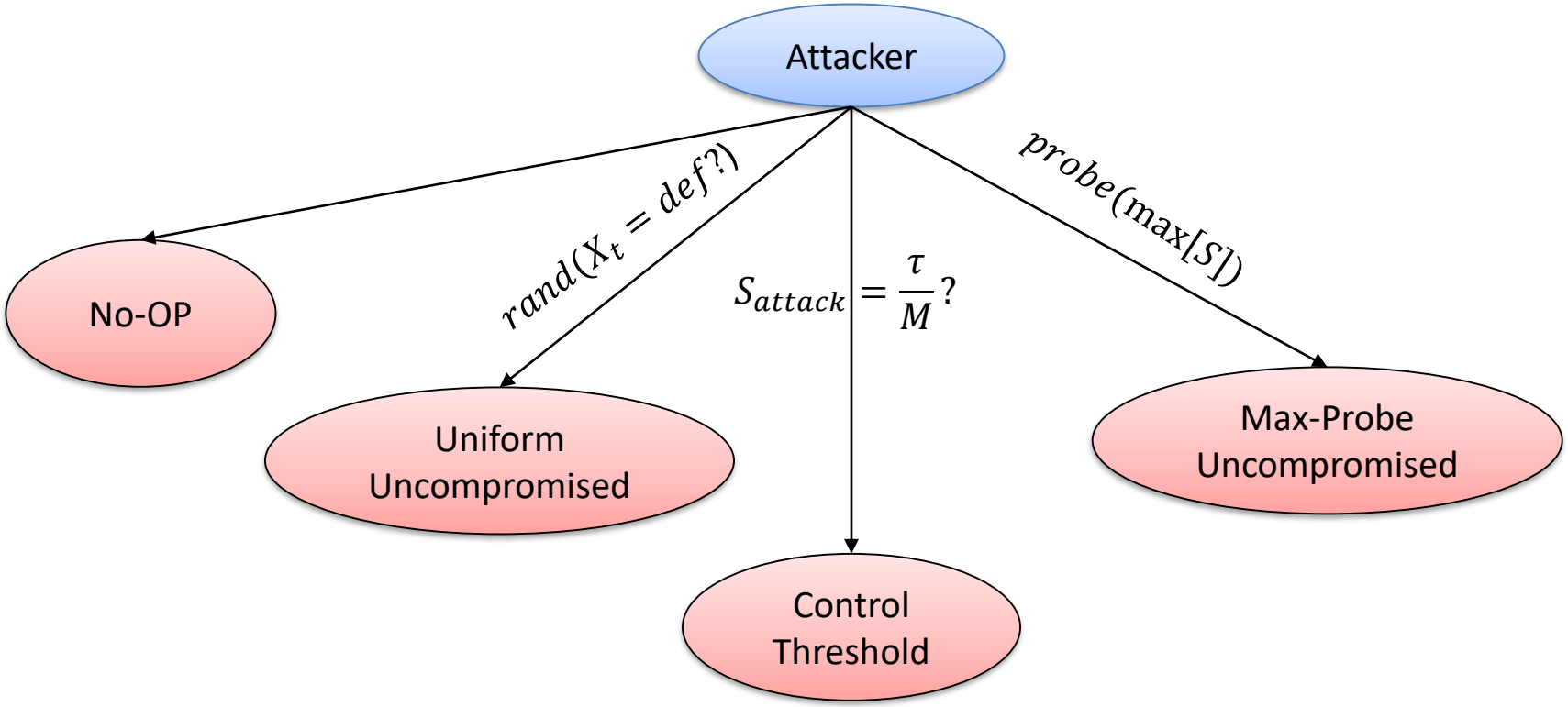
Game States and Actions

- Server State $< \chi, \nu, \rho >$
- $\chi = \{att, def\}$ – who controls the server.
- $\nu \in \{up\} \cup [0, T]$ – server is up/down from a reimage initiated at [0,T].
- ρ number of attack probes since the last defender reimage action.

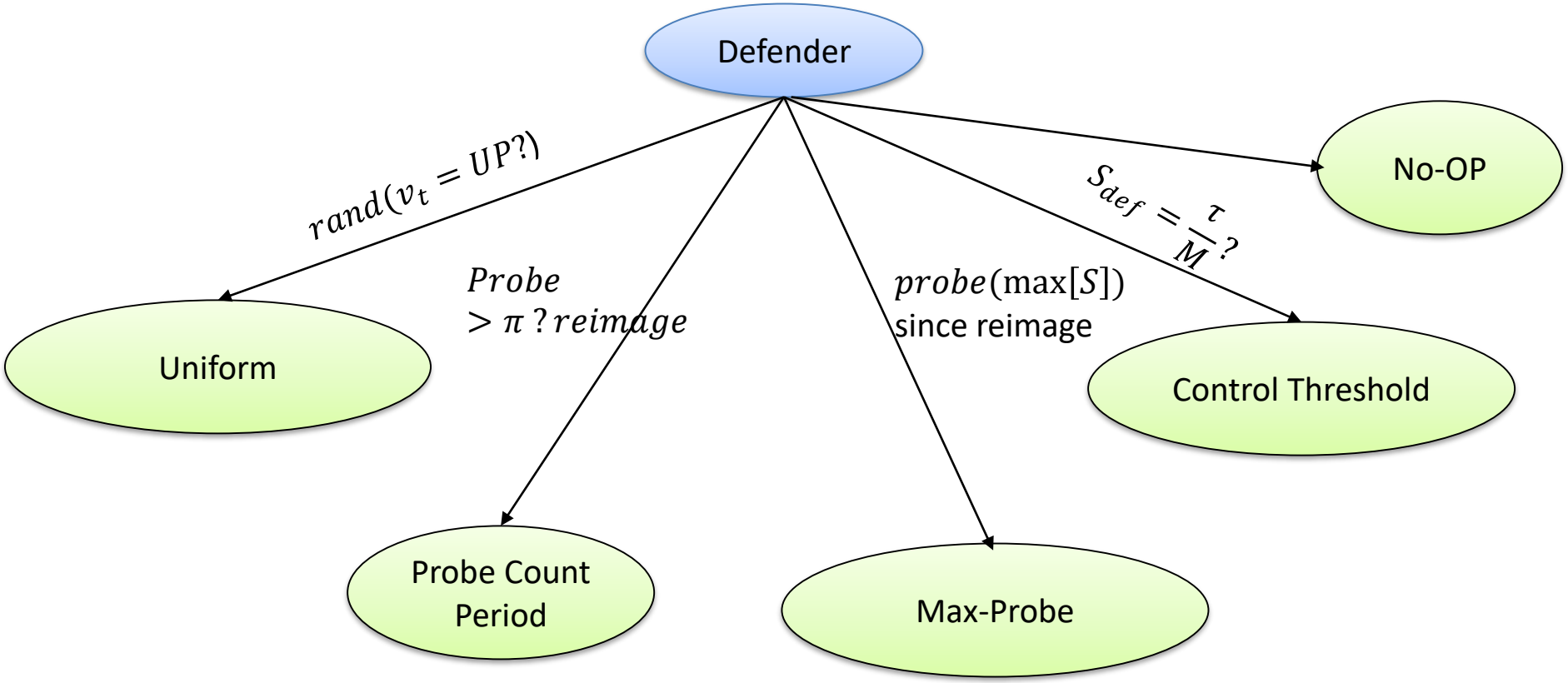
Utility

- Each player accrues utility based on the number of server up and in their control and the number of servers that are down
- Attacker – {disrupt, control}
- Defender – {confid, avail}
- $\boldsymbol{c_A} = \{0.2, 0.5, 1\}$, $\boldsymbol{Utility} = \{low, majority, high\}$

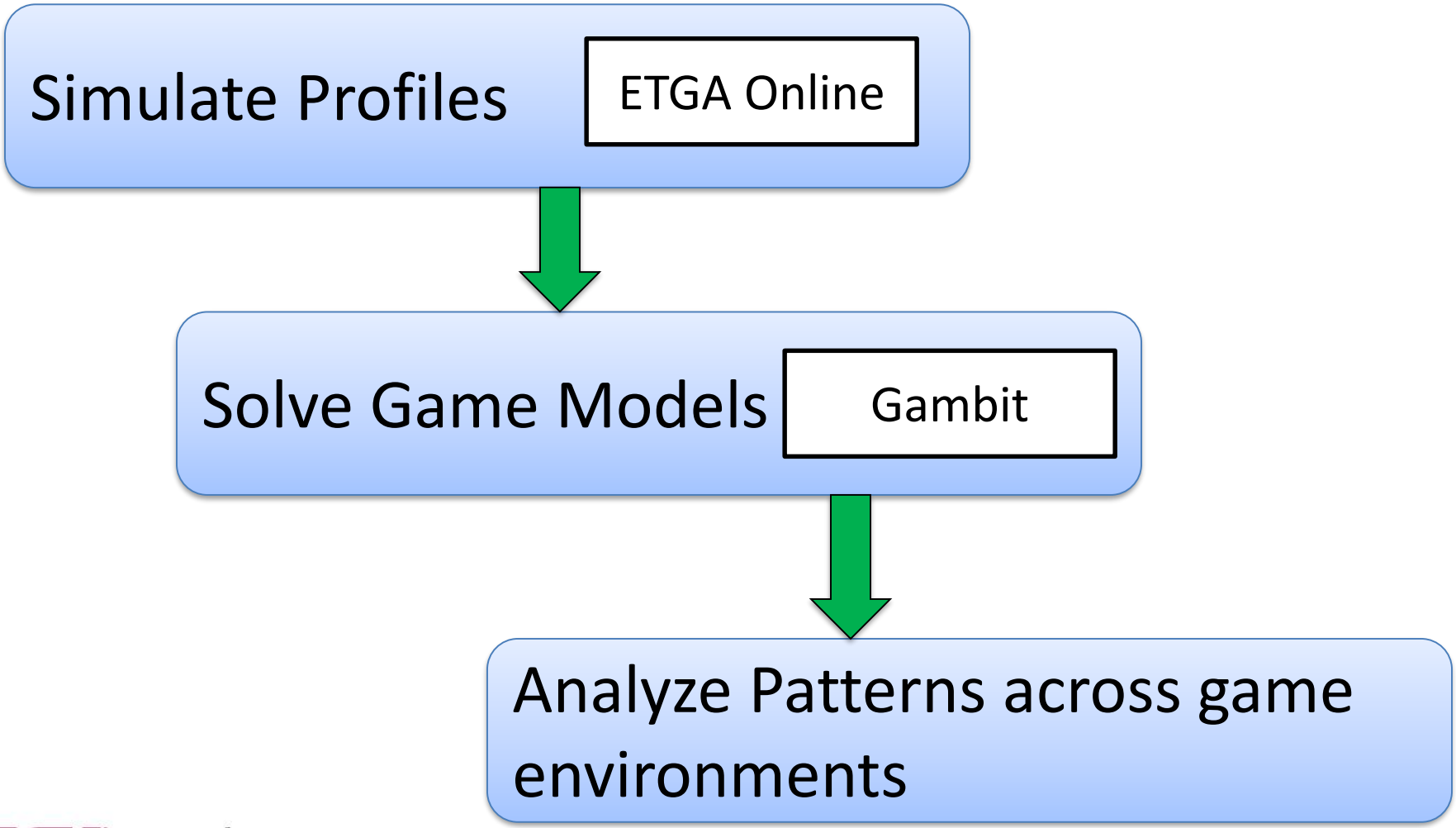
Attack Strategies



Defense Strategies



EGTA Pipeline

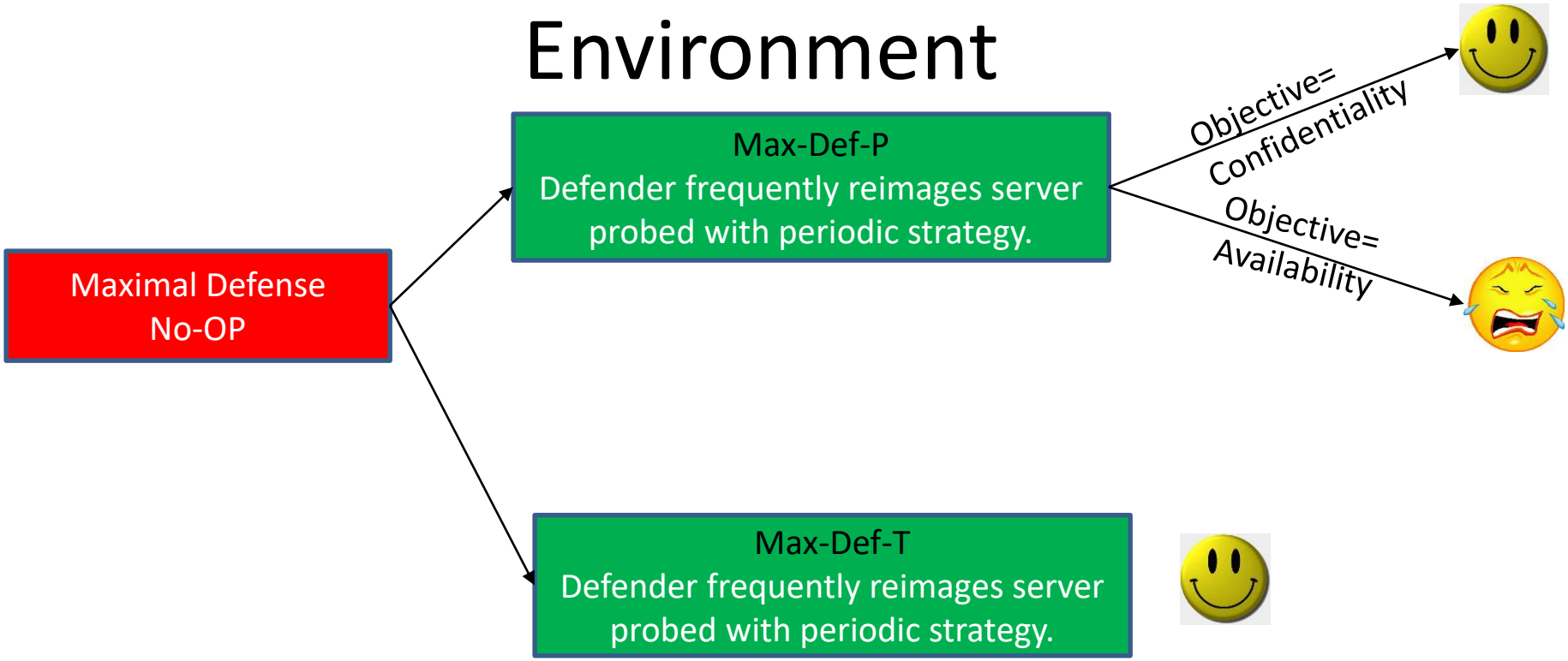


Results: Perfect Probe Detection Environment

		Utility Environments			
Utility threshold	c_A	disrupt/avail	disrupt/confid	control/avail	control/confid
low	1	MaxDef-T, Share	*MaxDef-P*	MaxDef-T, Share	*MaxDef-P*
low	0.5	Share	*MaxDef-P*	MaxDef-T	*MaxDef-P*
low	0.2	Share	*MaxDef-P*	MaxDef-T, Share	*MaxDef-P*
majority	1	MaxDef-T	MaxDef-P	MaxDef-T	MaxDef-P
majority	0.5	Fight	MaxDef-P	MaxDef-T	*MaxDef-P*
majority	0.2	Fight	MaxDef-P	MaxDef-T, MaxAtt	*MaxDef-P*
high	1	MaxDef-T, MaxAtt	*MaxDef-P*	MaxDef-T, MaxAtt, Fight	*MaxDef-P*
high	0.5	MaxDef-T, MaxAtt, Fight	*MaxDef-P*	MaxDef-T, MaxAtt, Fight	*MaxDef-P*
high	0.2	MaxDef-T, MaxAtt	*MaxDef-P*	MaxDef-T, MaxAtt, Fight	*MaxDef-P*

Table 4: Qualitative Nash equilibria for the thirty-six perfect probe detection environments. Cells in italics indicate games not actually simulated, but with obvious equilibria given the confid defense objective.

Results: Perfect Probe Detection Environment



Key Insights

- With perfect probe detection, **maximal defense** is always an equilibrium when attackers have **control** objectives, and pervasive as well for **disrupt** objectives.
- Maximal attack is **occasionally in equilibrium** among others with **perfect probe detection**, but becomes significantly more **prevalent** once **probe detection degrades**.
- **Fight** equilibria are generally **pervasive**, except when **contention** for servers is **particularly weak**.
- The **Control** strategies **appear widely** in equilibrium configurations.

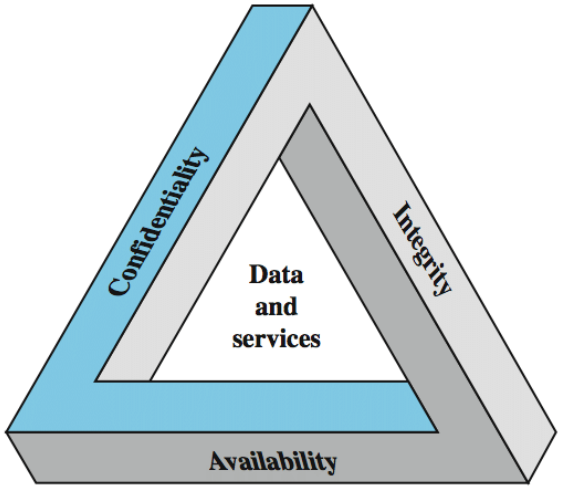
MTD Effectiveness Evaluation - Zack

MTD Effectiveness Evaluation

- Goal is to understand the effectiveness of countermeasures during the intrusion process.

Traditional Metrics

- CIA Triad: Confidentiality, Integrity, Availability.
- Designed to assist in policy creation to protect data.
- Limitations
  - Quantitative scale unclear.
  - Limited distinction between attacker and defender.
  - Doesn't reflect increased information about an attacker.



Proposed Metrics

- Assigns 0 to 1 for each item indicating their relative value.
- Metrics assigned independently to both defender (mission) and attacker.
  - Productivity – Tasks performed over time.
  - Success - Ability to complete tasks.
  - Confidentiality – Visibility of task activity.
  - Integrity – Accuracy of task output.

Experiment Details

- Intended to verify the usefulness of the metrics.
- Network topologies of 10 to 20 nodes built on VMWare.
- Tested on networks with two different methods of MTD.
- Experiment metric is the weighted average for each task.
- Assumptions:
  - Other metrics encapsulated within these metrics (IE network surface area being covered by Attack Productivity and Mission Confidentiality).
  - Network is continually running tasks to achieve an output.
  - Attacks are trying to compromise information (CIA Triad).

ARCSYNE

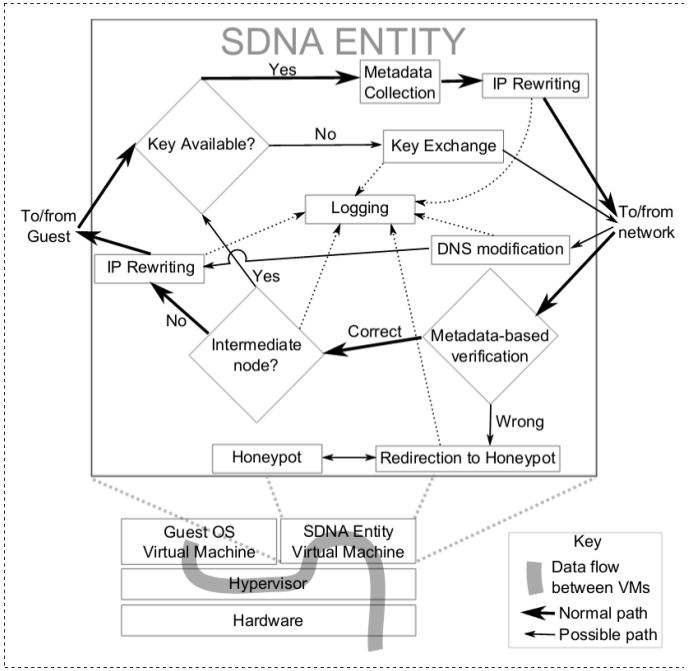
- Active Repositioning in Cyberspace for SYNchronized Evasion.
- Rotate IP addresses for all hosts on network simultaneously.
  - Hop time is the period after which addresses are reassigned.
  - Hop time Varies from fractions of a second to minutes.
- Shorter hop time means the network is harder to map but adds significant overhead.

Table 8: ARCSYNE CPU Usage vs Scale and Hop Delay

		Hop Delay		
		0.1	**1.0**	**10**
Scale	**10**	≈10%	≈3%	≈1%
	20	≈30%	≈5%	≈1%

SDNA

- Self-shielding Dynamic Network Architecture
- Multiple layers of security
  - Hypervisor between OS and network.
  - Masks OS of hosts through encapsulation.
  - Rewrites IP addresses to prevent mapping.
  - Randomizes packet routing.
  - Credentials hidden from hosts.
  - Redirecting of unauthenticated packets to a honeypot.
- Level of security determined by number of whitelisted protocols.



Results (ARCSYNE)

- Obfuscated hosts → hard to identify attacks from noise.
- Halting attacks quickly enables more tries per period, allowing attackers to try more attempts faster.
- More security operations → less resources for mission.

Table 4: Attack Metrics for MTD Configurations

Configuration	Confidentiality	Success	Productivity	Integrity
No ARCSYNE	0.7	1.0	0.5	1.0
ARCSYNE	1.0	0.2	0.7	0.0

Table 6: Mission Metrics for MTD Configurations

Configuration	Confidentiality	Success	Productivity	Integrity
No ARCSYNE	0.2	1.0	1.0	0.7
ARCSYNE	1.0	0.9	0.9	0.6

Results (ARCSYNE)

- Increasing hop delay reduces Mission Integrity, Mission Productivity, and Mission Success.

Table 7: ARCSYNE Mission Metrics vs. Hop Delay

Hop Delay	Confidentiality	Integrity	Productivity	Success
0.1s	1.0	0.75	1.0	1.0
1.0s	1.0	0.75	1.0	1.0
10.0s	1.0	0.45	0.8	0.75

Results (SDNA)

- Honeypot masks attack outcome, reducing attack productivity.
- Unclear why Mission Confidentiality dropped down for External case.

Table 4: Attack Metrics for MTD Configurations

Configuration	Confidentiality	Success	Productivity	Integrity
No SDNA	0.7	0.9	0.7	0.9
SDNA, External	1.0	0.3	0.7	0.0
SDNA, Internal	1.0	0.5	0.4	0.1

Table 6: Mission Metrics for MTD Configurations

Configuration	Confidentiality	Success	Productivity	Integrity
No SDNA	0.5	1.0	1.0	1.0
SDNA, External	0.2	0.5	0.4	0.5
SDNA, Internal	1.0	0.5	0.4	0.5

Results (SDNA)

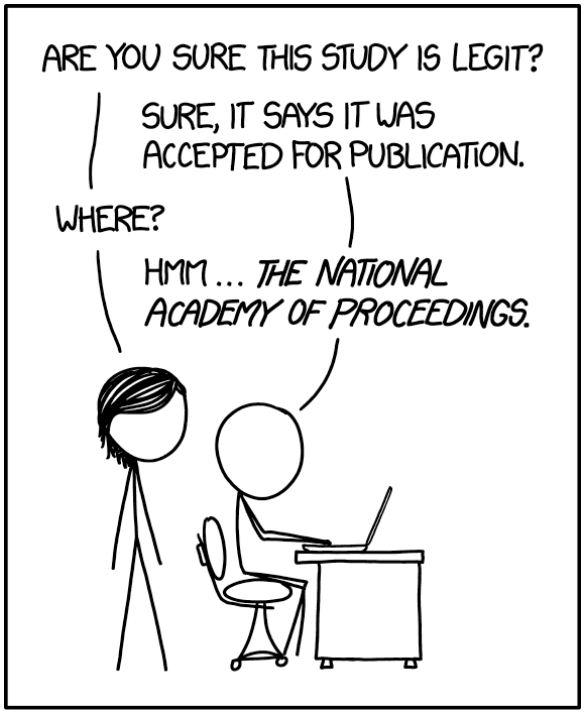
- Increasing SDNA security reduced Attack Success, Attack Productivity, and Attack Integrity.
  - Reducing permitted protocols doesn't affect network performance, but removes avenues of attack.

Table 5: SSHPass Attack Metrics for SDNA Security Levels

Configuration	Confidentiality	Success	Productivity	Integrity
No SDNA	1.0	1.0	1.0	1.0
SDNA, Low	1.0	0.4	0.6	0.4
SDNA, Med.	1.0	0.2	0.6	0.3
SDNA, High	1.0	0.0	0.5	0.0

Study Issues

- ARCSYNE and SDNA control don't match.
- Unclear if SDNA security levels run with internal or external.
- Unclear why external SDNA lowered Mission Confidentiality.
- Arguably insufficient study to show fidelity of metric system.



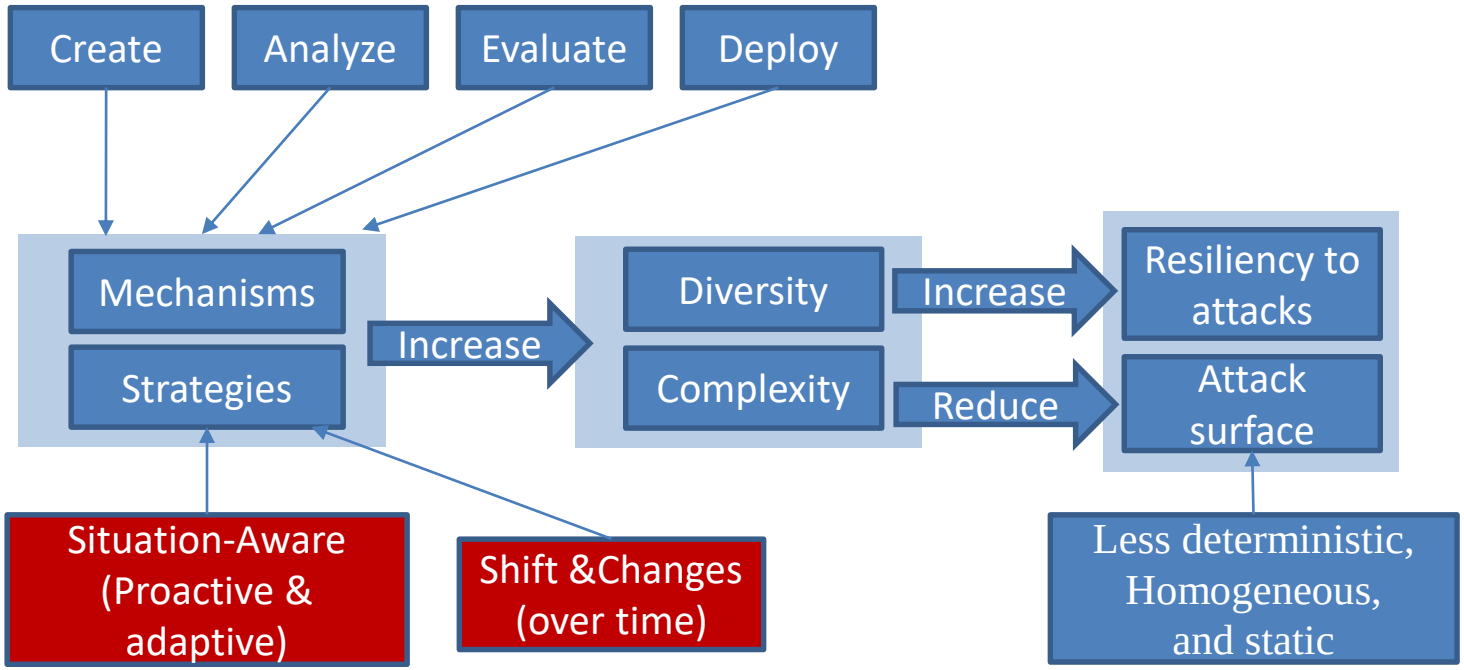
Question

- Identify the a pure strategy Nash Equilibrium in this game.

		Column Player (Attacker)	
Row Player (Defender)		**Attack**	**Reconnaissance**
	Randomize	-1,+1	0,0
	Migrate VM	0,0	+2,-2

a) Randomize, Attack
b) Migrate, Attack
c) Randomize, Recon
d) Migrate, Recon
e) None.
f) More than one

Conclusion and Research Opportunities for Moving Target Defense (MTD)



https://www.nitrd.gov/SUBCOMMITTEE/csia/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf

Challenges in Network-based MTD

1. Service availability
   - Authenticated clients should always know the new IP address/port number.
   - When the IP and Port changes, the connection still maintained, minimizing service downtime.
2. Service Security
   - Only the authenticated users can access the service.
   - How to mitigate insider attacks?

References

[1] To Be Proactive or Not: A Framework to Model Cyber Maneuvers for Critical Path Protection in MANETs, *Second ACM Workshop on Moving Target Defense*. ACM, 2015

[2] Characterizing Network-Based Moving Target Defenses, *Second ACM Workshop on Moving Target Defense*. ACM, 2015

[3] Towards Cost-Effective Moving Target Defense Against DDoS and Covert Channel Attacks, *Proceedings of the 2016 ACM Workshop on Moving Target Defense*. ACM, 2016.

[4] MOTAG: Moving Target Defense Against Internet Denial of Service Attacks, Computer Communications and Networks (ICCCN), 2013 22nd International Conference on, 2013

[5] Markov Modeling of Moving Target Defense Games, *Proceedings of the 2016 ACM Workshop on Moving Target Defense*. ACM, 2016

[6] Empirical Game-Theoretic Analysis for Moving Target Defense, *Proceedings of the Second ACM Workshop on Moving Target Defense*. ACM, 2015.

[7] A Quantitative Framework for Moving Target Defense Effectiveness Evaluation, *Proceedings of the Second ACM Workshop on Moving Target Defense. ACM, 2015*

[8] Automated Effectiveness Evaluation of Moving Target Defenses: Metrics for Missions and Attacks, *Proceedings of the 2016 ACM Workshop on Moving Target Defense*. ACM, 2016.