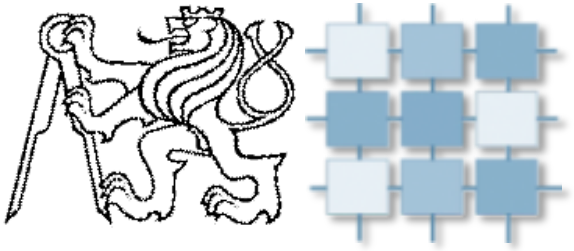
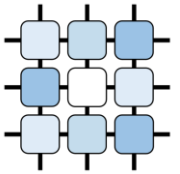


GAMNEP
Game-theoretic approach to network intrusion detection

Michal Pechoucek (PI), Karel Bartos , Branislav Bosanky, Martin Grill, Jan Jusko, Pavel Jisl, Martin Komon, Viliam Lisy, Tomas Pevny, Radek Pibil, Martin Rehak, Jan Stiborek, Michal Svoboda

Czech Technical University in Prague

Outline



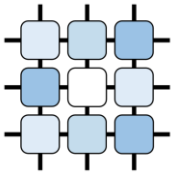
CAMNEP Intrusion Detection System

GAMNEP Project Objectives

Adversarial Plan Recognition Game (APRG)

- Monte-Carlo Tree Search
- Solving APRG
- Experimental Results

CAMNEP: Intrusion detection system



Goal: Identify illegitimate traffic and report it to the operator

- High accuracy vs. low number of **false positives**

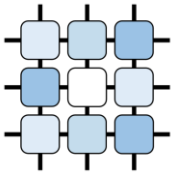
network flow data (no deep packet inspection)

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2009-03-20 01:11:12.923	364.932	TCP	147.251.198.84:2430	->	78.154.195.124:47575	8699	8.1 M	104
2009-03-20 01:12:38.215	276.256	UDP	92.240.244.30:27022	->	147.251.211.107:27005	19266	4.1 M	72
2009-03-20 01:11:51.690	308.352	TCP	62.67.50.133:80	->	147.251.68.5:3671	41696	53.3 M	55
2009-03-20 01:12:18.467	292.902	TCP	91.66.122.66:53858	->	147.251.215.168:23314	18189	1035699	51
2009-03-20 01:12:01.886	337.372	TCP	64.15.156.212:8000	->	147.251.146.27:1150	2028	2.0 M	47
2009-03-20 01:16:56.525	28.134	TCP	147.251.215.235:2517	->	213.134.25.222:27192	343	269375	45
2009-03-20 01:12:39.400	299.943	UDP	147.175.185.54:1693	->	147.251.206.207:29359	18214	2.4 M	44
2009-03-20 01:15:42.653	15.283	TCP	77.75.73.48:25	->	147.251.4.40:40166	186	16009	43
2009-03-20 01:13:46.343	213.639	TCP	147.251.210.122:55628	->	66.55.141.34:80	3864	155898	43
2009-03-20 01:08:00.699	578.690	TCP	147.251.211.172:64037	->	217.162.223.125:14817	4900	215352	41

anomaly detection (no pattern matching)

- Zero-day attacks
- Unusual legitimate behavior (changes in the network)
- Scalability

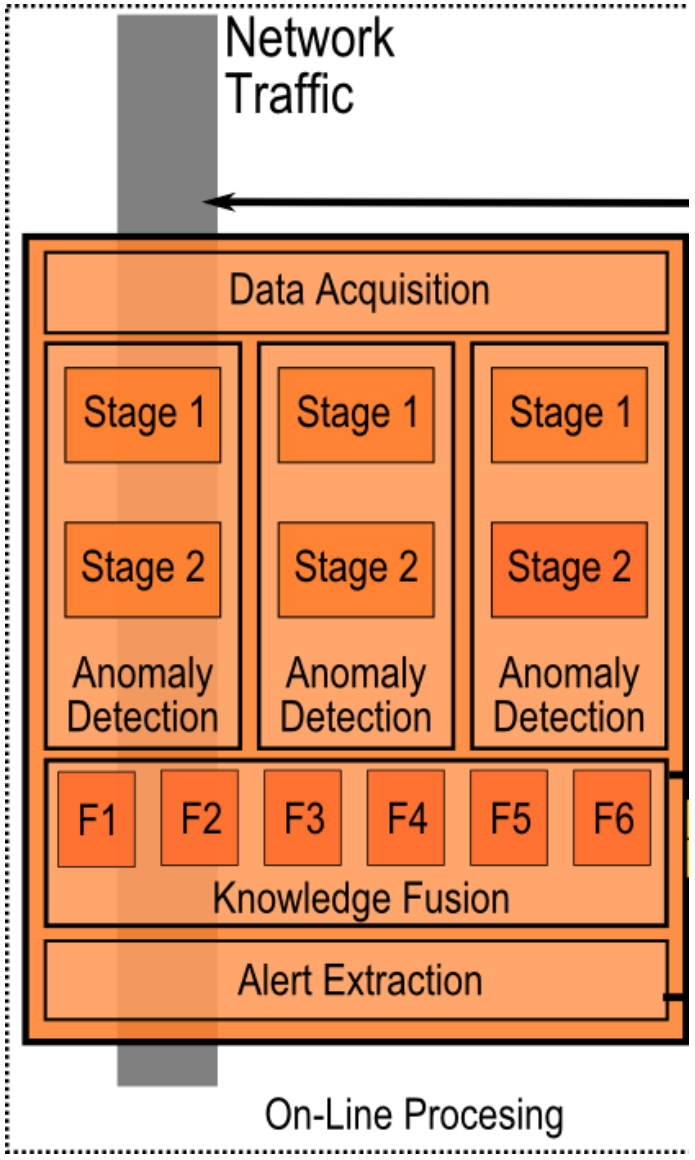
Anomaly Detection

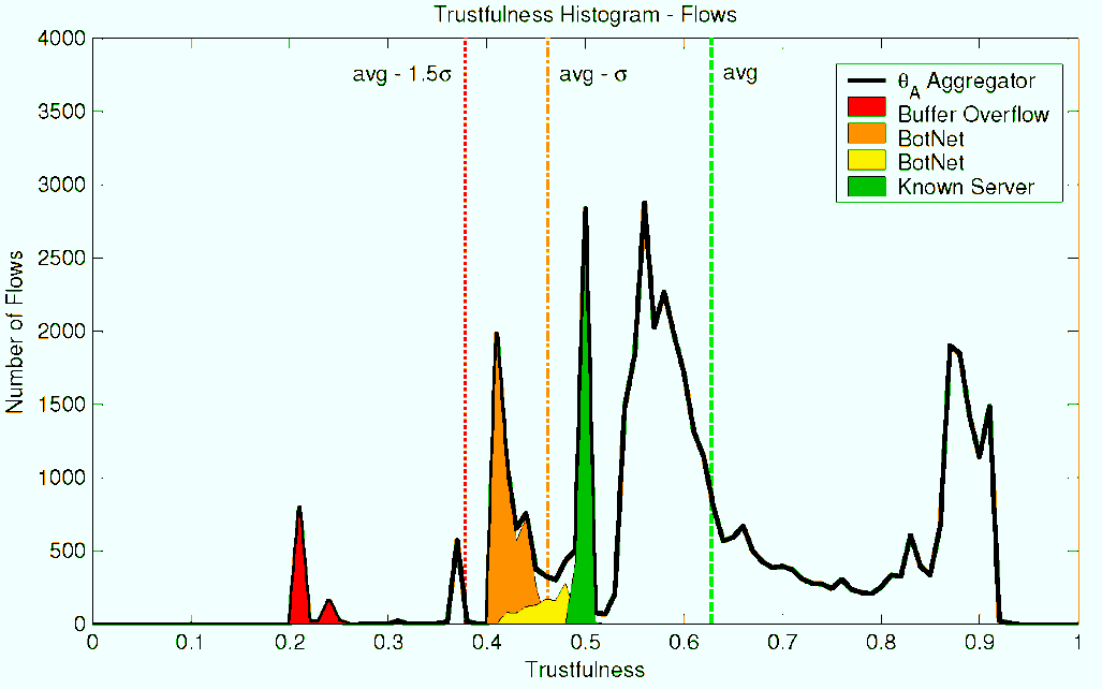


Method/Attack	Malware Brute force	Horizontal scanning	Vertical Sc. Fingerprint.	DoS/DDoS Flooding/Spoof.
MINDS	***	****	****	***
Xu	**	****	***	***
Xu-dst IP	*	*	**	*****
Lakhina - Volume	**	***	***	****
Lakhina - Entropy	***	****	**	***
TAPS	***	*****	*****	**

Entropy modeling, Trend modeling, Volume modeling, Principal components analysis, Information-theoretical measures

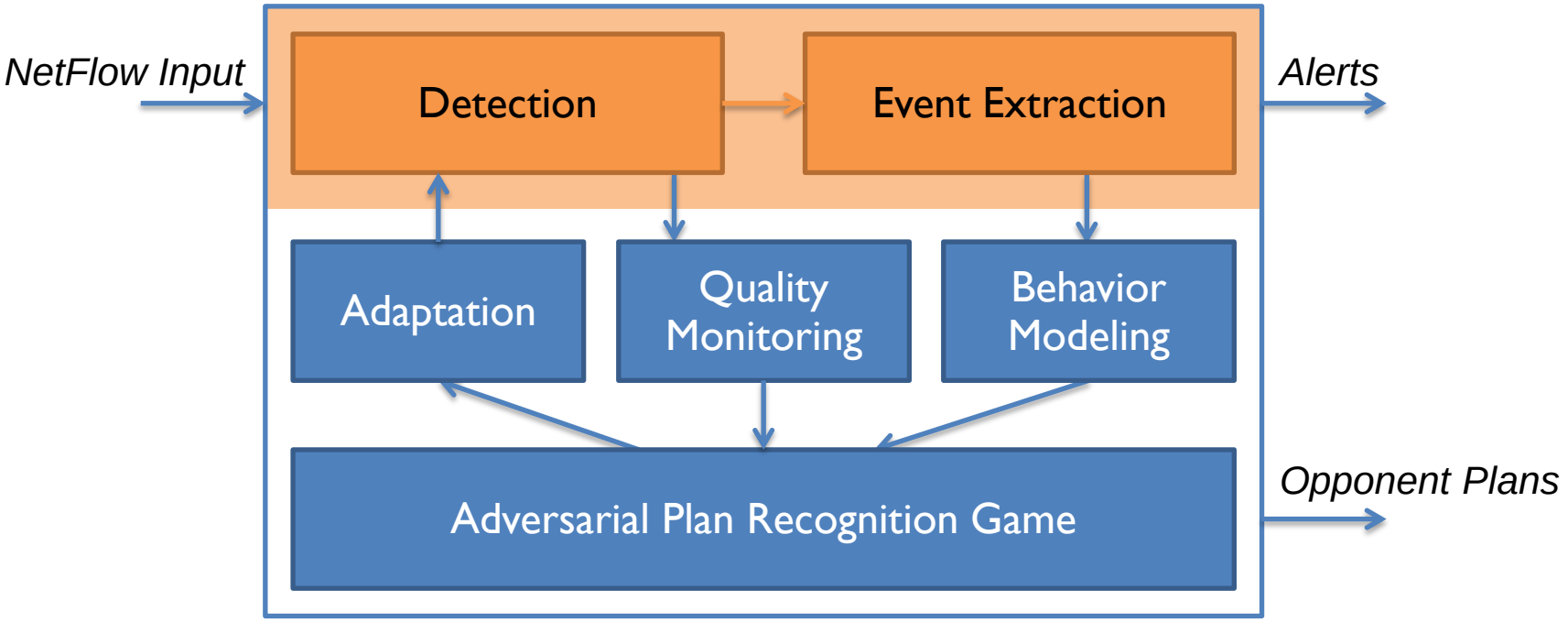
Inside CAMNEP





Event Extraction: **Converts the statistics into actionable output**

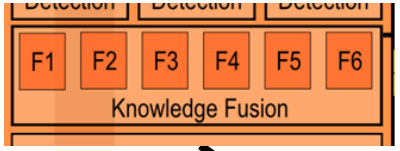
GAMNEP Concept



GAMNEP – IDS Interface

Parameter setting:

Selecting one of the knowledge fusion functions



Detection quality:

Reporting the current quality of each knowledge fusion function in form of confusion matrix

d_1

	a_1	a_2	a_3
o_1	0.5	0.1	0.1
o_2	0.2	0.7	0.1
o_3	0.3	0.2	0.8

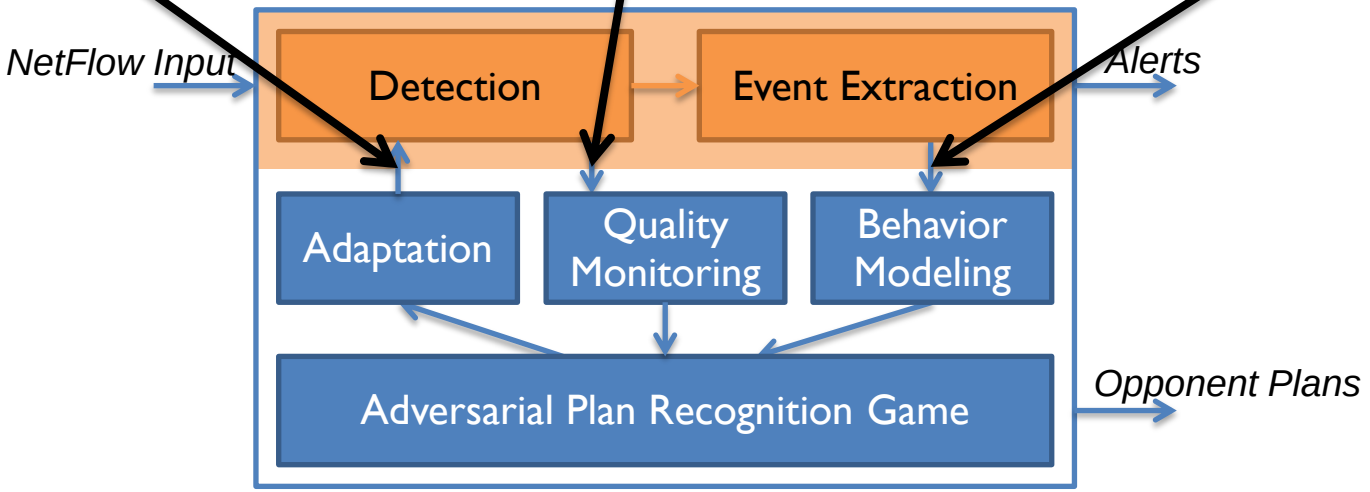
d_2

	a_1	a_2	a_3
o_1	0.9	0.3	0.2
o_2	0.1	0.3	0.4
a_3	0.0	0.4	0.4

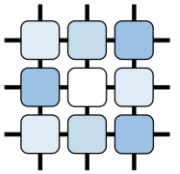
Observed attacker's action:

Reporting the detected action of the attacker

SSHscan
Portscan
Bruteforce
Webtraffic



Game Model Assumptions



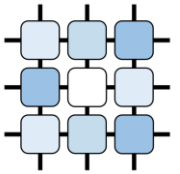
Realistic assumptions

- Both players, the attacker and the defender, are **rational**
- The defender can use only **one classier** at a time
- The quality of the classifiers **does not change**
- Both players know the full **plan library** of the attacker
- The **available classifiers** and their quality are known to both

Simplifying assumptions

- Everybody knows when the game starts
- All actions of the attacker have equal length

Adversarial Plan Recognition Game



Actions

- Attacker: One action per stage from an attack plan
- Defender: One of the classifiers in each stage

Information

- Attacker: Does not gain any information during the game
- Defender: Noisy observations of the attacker's action in each stage

Utilities

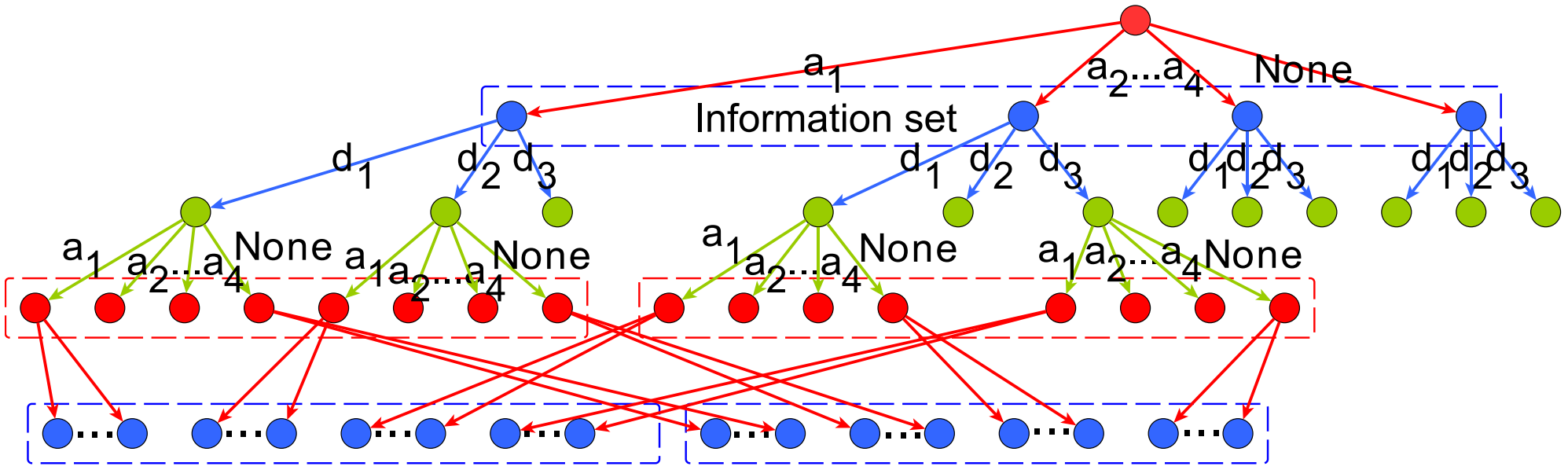
- Zero-sum: The attacker wants to execute the most dangerous plan unobserved

$$u_A(a_1 \dots a_h, d_1 \dots d_h, o_1 \dots o_h) = \frac{g(a_1 \dots a_h)}{1 + \sum_{i \in \{1 \dots h\}; o_i = a_i} 1}$$

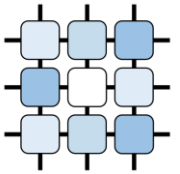
Solution

- Action selection: Nash equilibrium
- Plan recognition: The most likely plan of the attacker

Extensive Form Game Tree



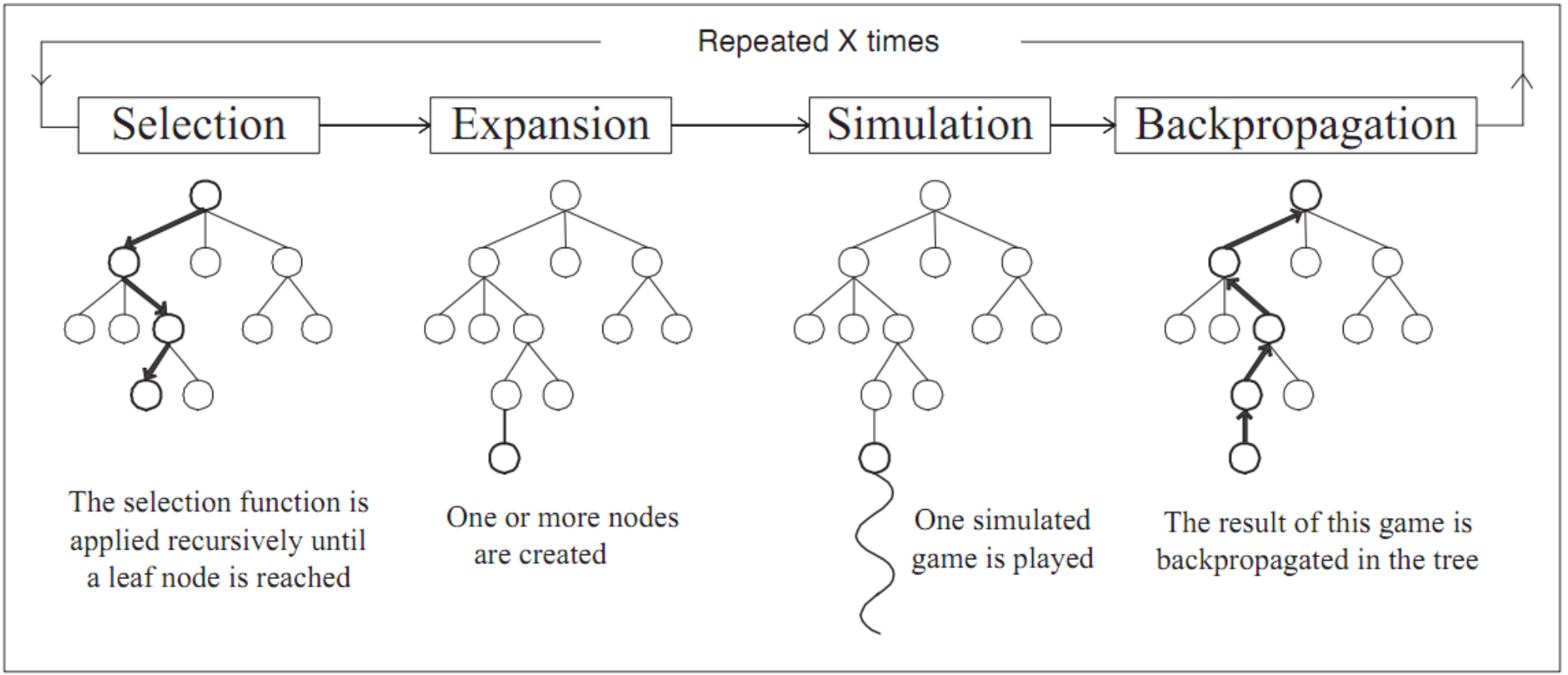
Monte-Carlo Tree Search



Designed for full information alternating moves games

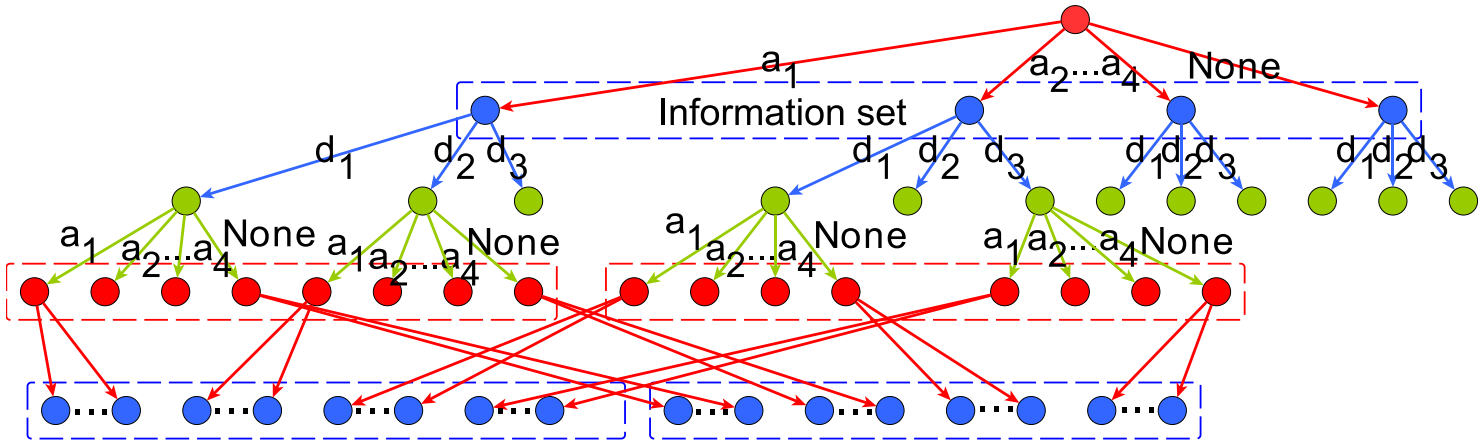
Very successful in GO

Applied to Amazons, Hex, Arimaa, and many other games

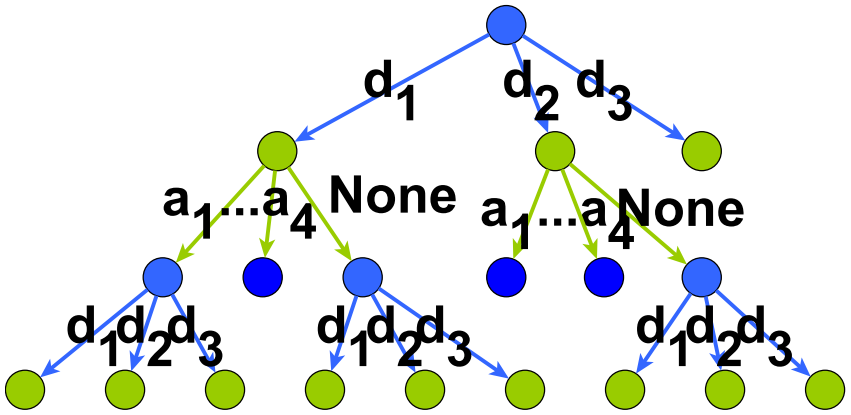


Picture from Chaslot et al. 2007

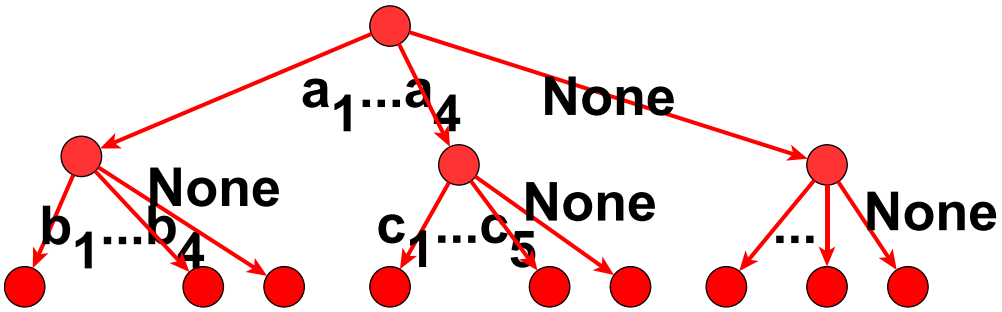
Concurrent MCTS for APRG



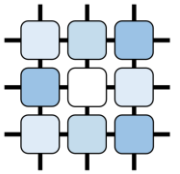
Defender's signal tree



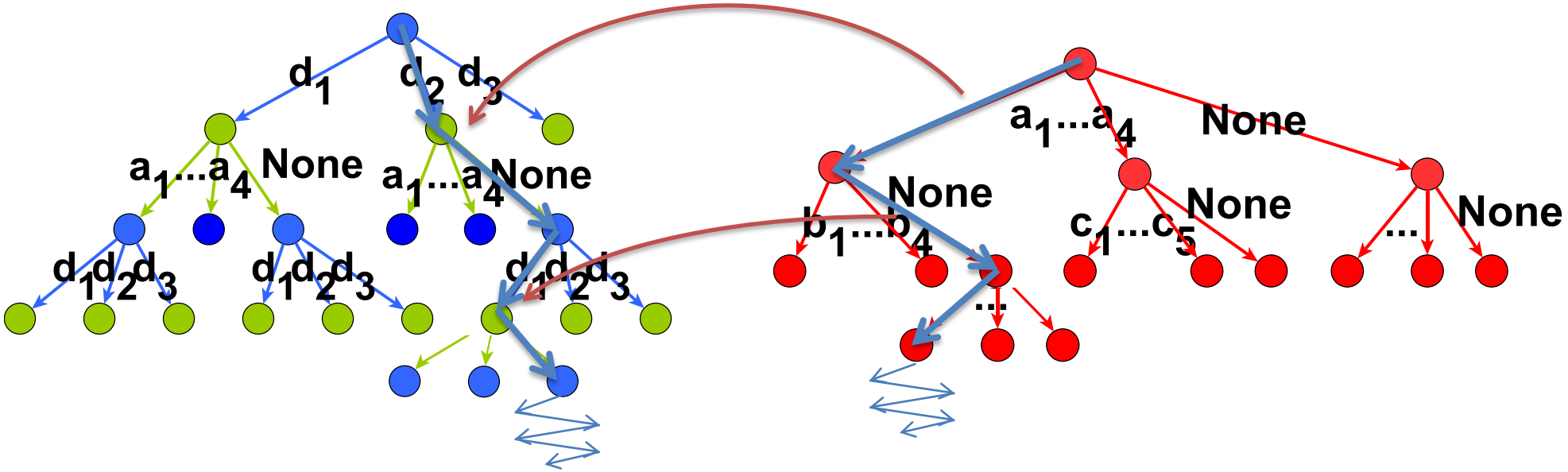
Attacker's signal tree



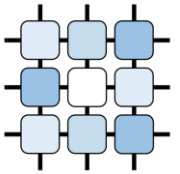
Concurrent MCTS for APRG



1. Select a plan in the attacker's tree using MCTS
2. Select a "plan" in the defender's tree with observation based on the attacker's plan
3. Compute the utility of the pair of plans
4. Back-propagate the value in both trees



Selection Strategy for MCTS in APRG



UCT: Standard selection strategy for perfect information games

Does not converge to a good solution with simultaneous moves

$$c_{t,s} = 2C_p\sqrt{\frac{\ln t}{s}}$$

Exp3.1: No regret strategy non-stochastic bandit problem

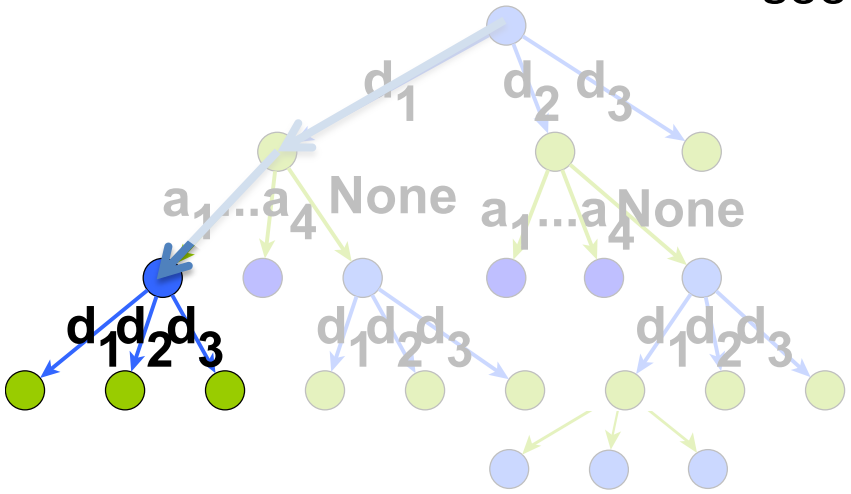
Empirical frequencies guaranteed to converge to NE if used by both players in unknown game setting

for $t = 1, 2, \ldots$ **do**
  Draw action a from distribution p
  $f_a = f_a + 1$
  $G_a = G_a + \frac{g_a}{p_a}$
  $p_i = (1-\gamma)\frac{\exp(\frac{\gamma}{K}G_i)}{\sum_{k=1}^{K}\exp(\frac{\gamma}{K}G_k)} + \frac{\gamma}{K}$
end for

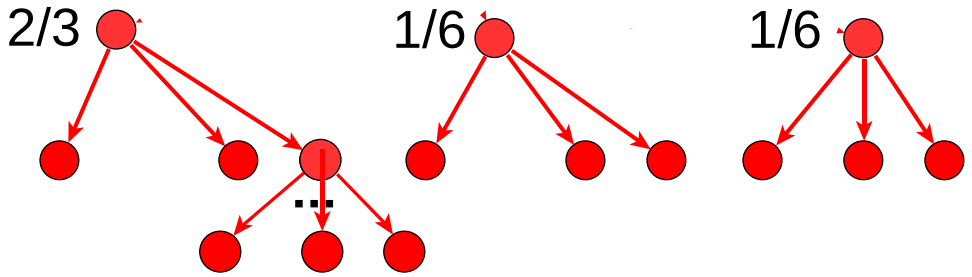
Continuous Reasoning of Observer

What happens in the progress of the game?

Transition using observations and Bayesian update



d_1 => p(detected | performed)
seen = **a_1**

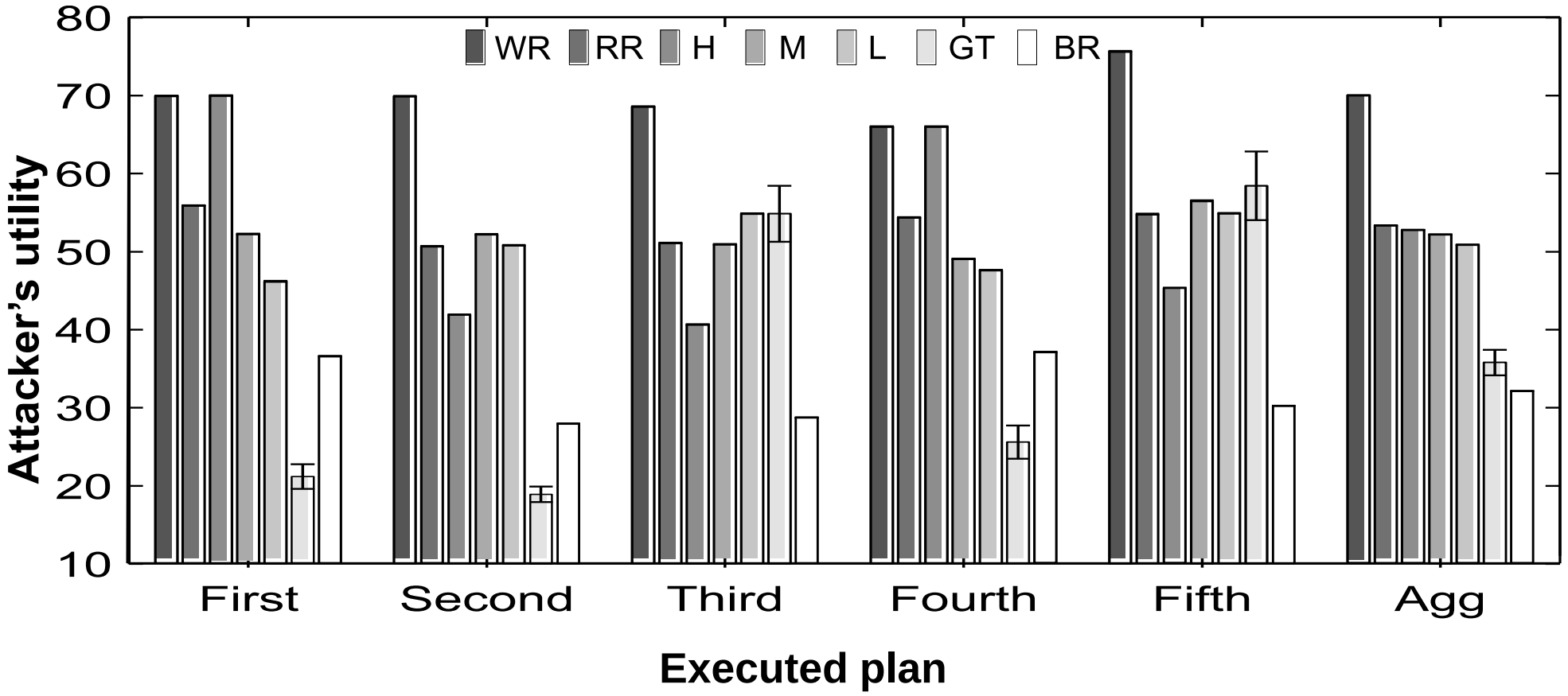


The probability of a root is probability of the plan from beginning

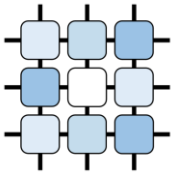
Syntetic Experiment Results

The executed plan was
- most likely: 38.6%
- median position: 5

WR – ex post worst selection of classifiers
RR – random classifiers selection
H,M,L – constant selection of one classifier
GT – the proposed approach (200 runs)
BR – ex post best selection of classifiers



Real World Data Experiments



5 minutes long stages

stages with attacker's actions are marked for the experiment

22 defender's classifiers (+ clustering)

0.6817	0.0023	0.2912	0.0	0.0	0.0	0.0	0.0113	0.0113	0.0	0.0	0.0023	0.0
0.0	0.3923	0.2152	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.3923	0.0002
0.0	0.25	0.5	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.25	0.0
0.0	0.0426	0.0426	0.0091	0.0091	0.8507	0.0	0.0033	0.0	0.0	0.0	0.0426	0.0
0.0	0.0426	0.0426	0.0091	0.0091	0.8507	0.0	0.0033	0.0	0.0	0.0	0.0426	0.0
0.0	0.0426	0.0426	0.0091	0.0091	0.8507	0.0	0.0033	0.0	0.0	0.0	0.0426	0.0
0.0	0.0	0.0	0.0	0.0	0.0	0.5	0.0	0.0	0.5	0.0	0.0	0.0
0.0273	0.0023	0.0343	0.0	0.0	0.0	0.0433	0.4788	0.3662	0.0433	0.0	0.0023	0.0023
0.0307	0.0026	0.0387	0.0	0.0	0.0	0.0488	0.4127	0.4127	0.0488	0.0	0.0026	0.0026
0.0	0.0	0.0	0.0	0.0	0.0	0.5	0.0	0.0	0.5	0.0	0.0	0.0
0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1	0.0	0.0
0.0	0.333	0.1826	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.4842	0.0002
0.0	0.0048	0.0027	0.0	0.0	0.0	0.0011	0.0016	0.0016	0.0011	0.0	0.0048	0.9822

13 basic attacker's actions with preconditions (PDDL)

DNS requests, Horizontal scan, Port scan, DDOS to specific service, etc.

One real and 10 simulated attacks in the data

Experiment Results

Mean	Classifier selection method
36.17	BR – ex post optimal selection of the classifiers
38.68	GT – the proposed approach (limited number of samples)
41.48	Random – selection of random classifier
41.99	Camnep – original IDS without strategic reasoning
47.88	WR – ex post worst selection of classifiers
95.00	BU – the utility of attacker's plan if it has not been observed