NDSS SYMPOSIUM

San Diego, California
23-27 February 2026

STRATEGIC GAMES AND ZERO SHOT ATTACKS ON HEAVY-HITTER NETWORK FLOW MONITORING

FRANCESCO DA DALT (ETH ZÜRICH) (Presenter)

ADRIAN PERRIG (ETH ZÜRICH)

ETH zürich

CHALLENGE

CHALLENGE

Configure complex systems

to be **optimally secure** against

PAST and FUTURE attack strategies

CHALLENGE

Configure complex systems

to be **optimally secure** against

PAST and FUTURE attack strategies

Alice

Bob

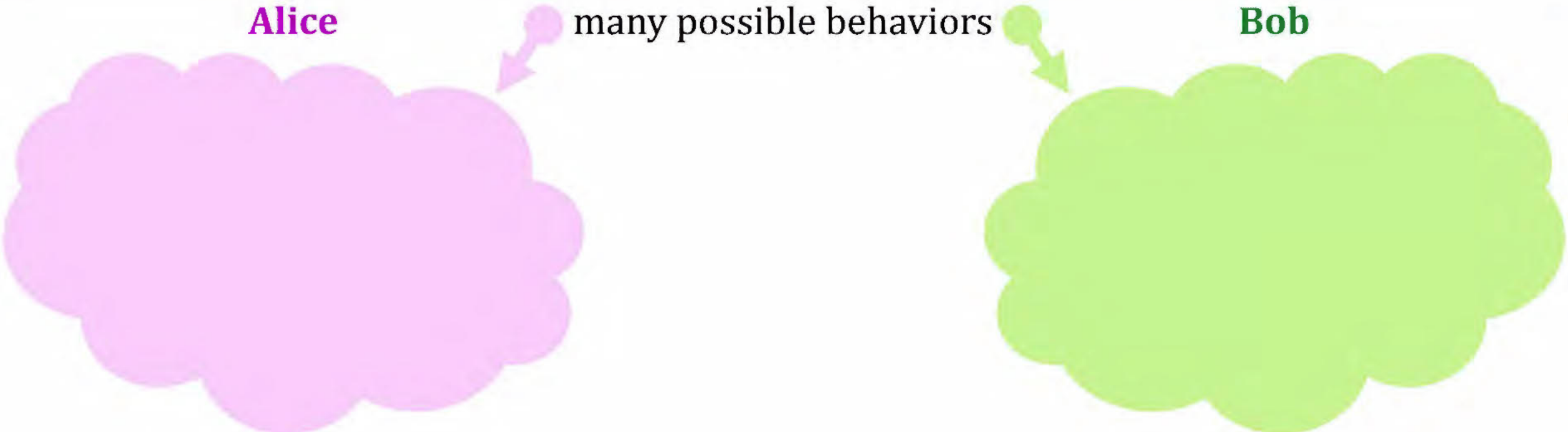
CHALLENGE

Configure complex systems

to be **optimally secure** against

PAST and FUTURE attack strategies

Alice many possible behaviors **Bob**



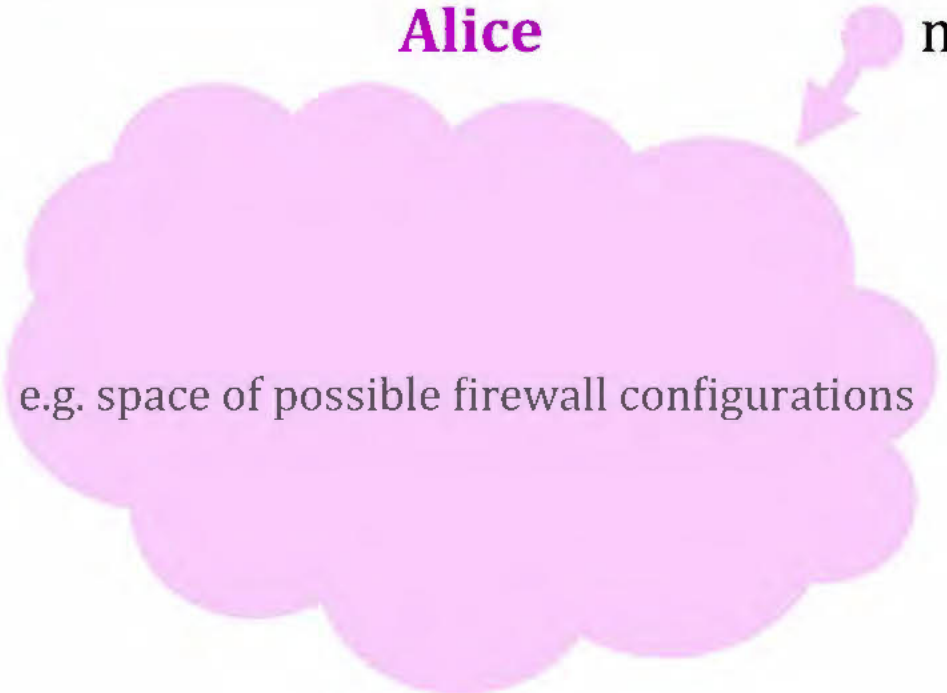
CHALLENGE

Configure complex systems

to be **optimally secure** against

PAST and FUTURE attack strategies

Alice many possible behaviors **Bob**



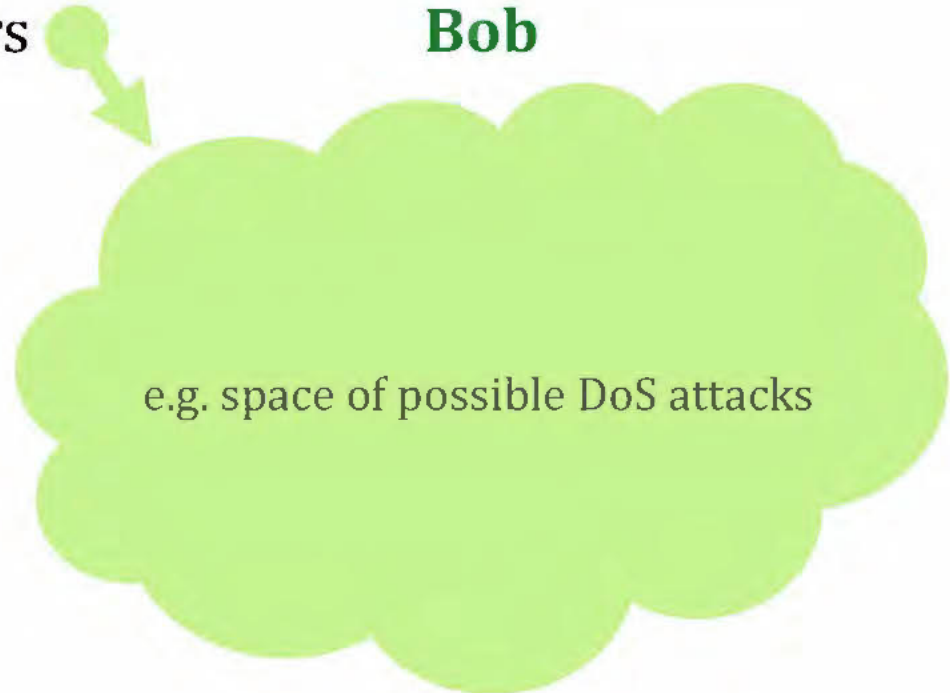
CHALLENGE

Configure complex systems

to be **optimally secure** against

PAST and FUTURE attack strategies

Alice many possible behaviors **Bob**



CHALLENGE

Configure complex systems

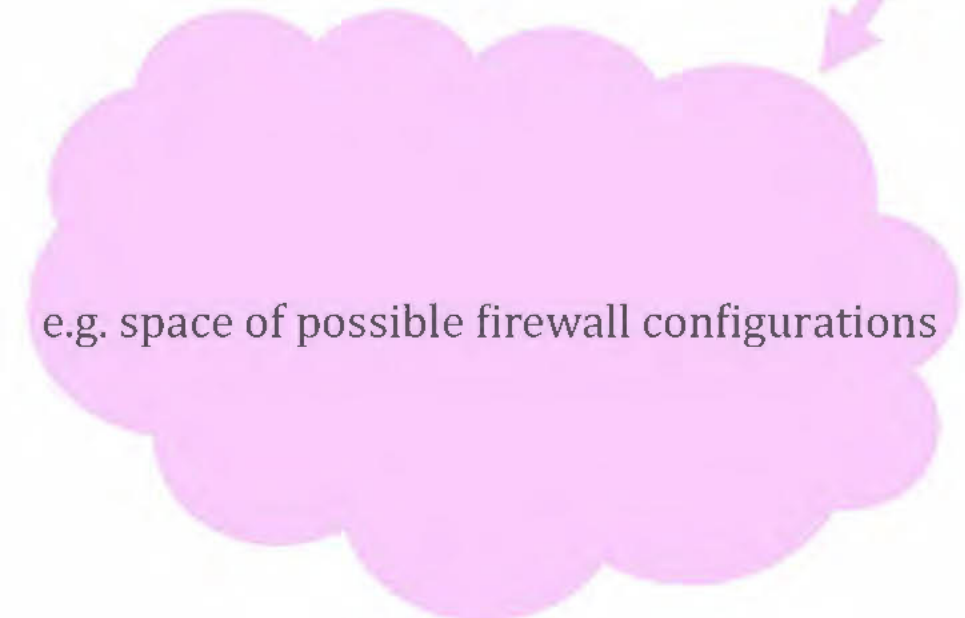
to be **optimally secure** against

PAST and FUTURE attack strategies

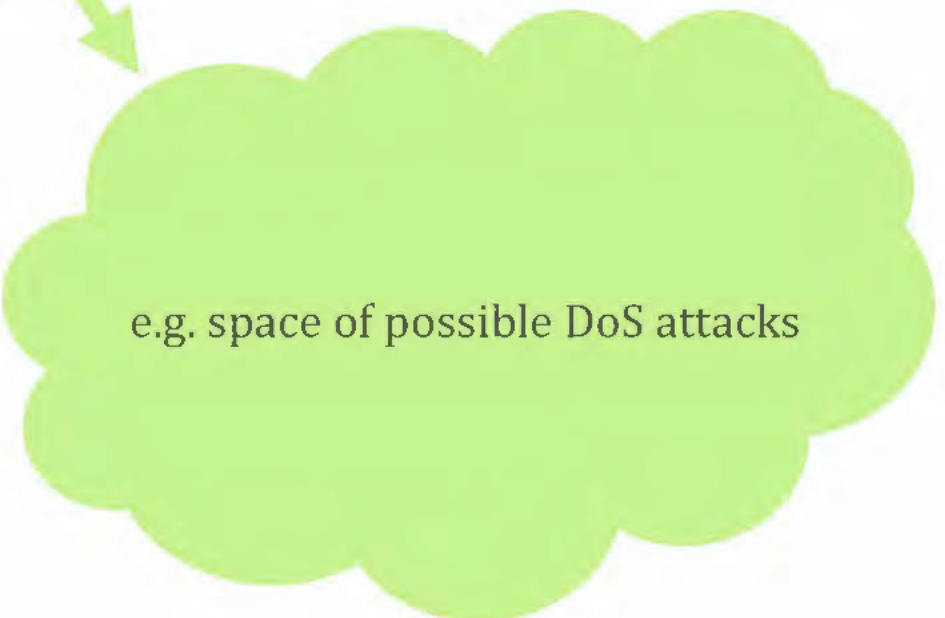
Alice

many possible behaviors

Bob



heuristic

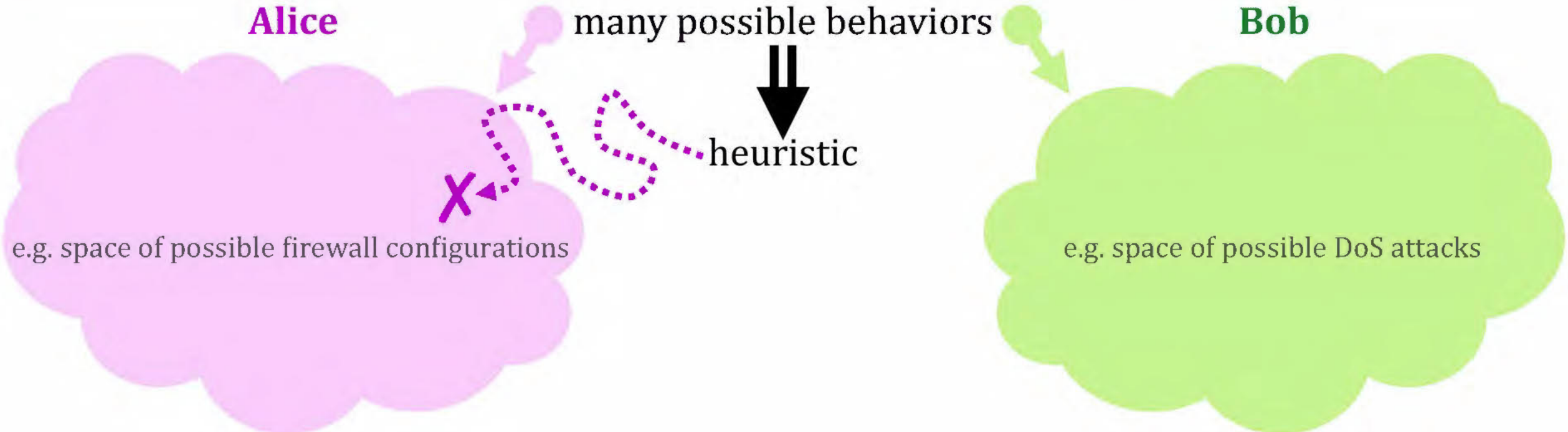


CHALLENGE

Configure complex systems

to be **optimally secure** against

PAST and FUTURE attack strategies

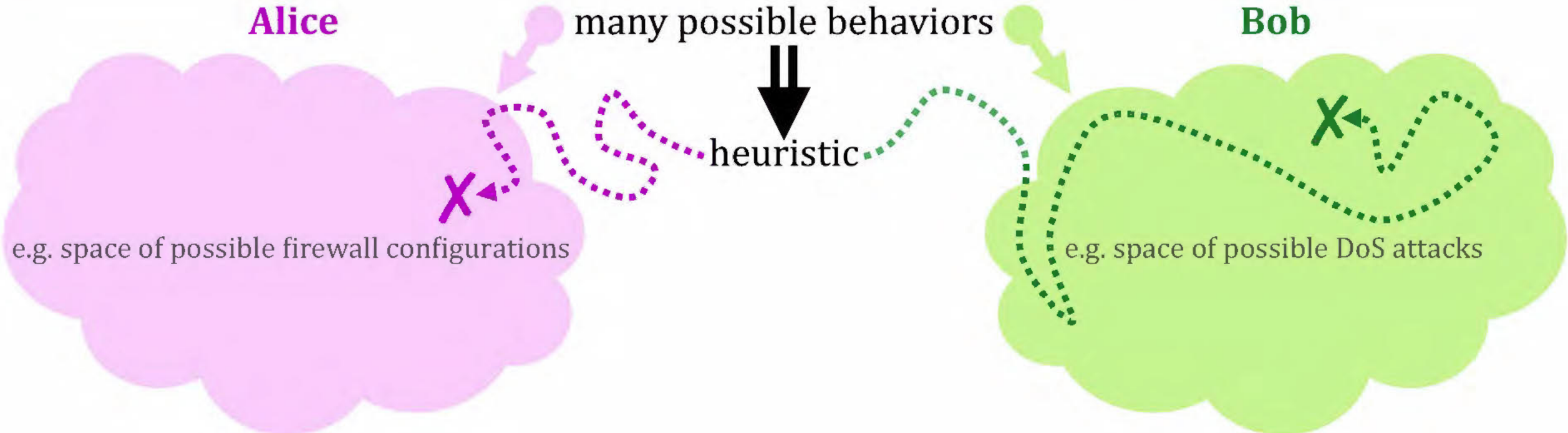


CHALLENGE

Configure complex systems

to be **optimally secure** against

PAST and FUTURE attack strategies

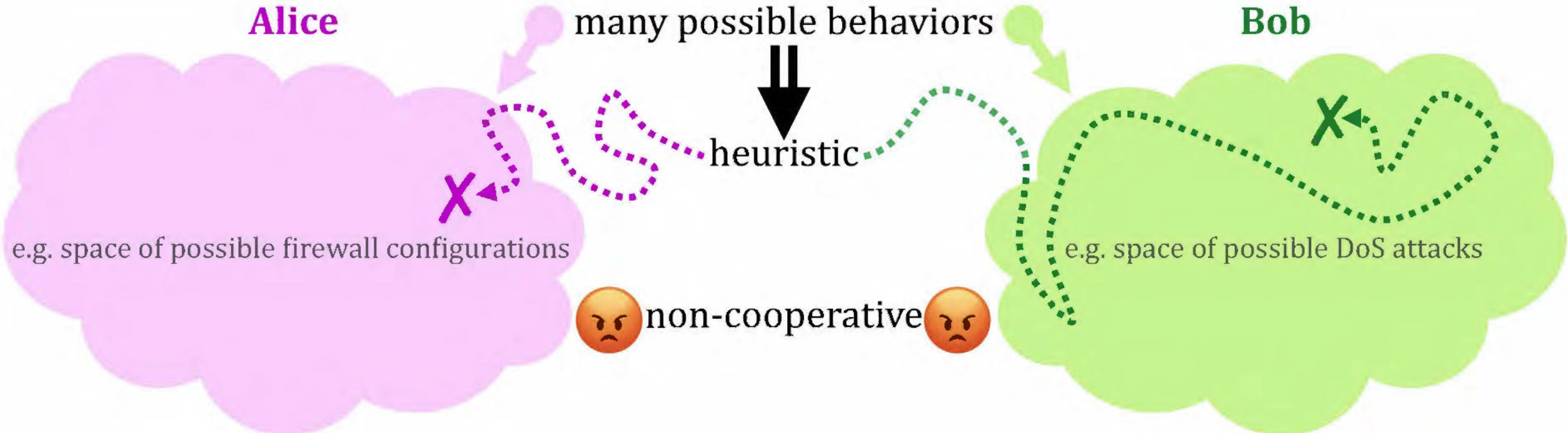


CHALLENGE

Configure complex systems

to be **optimally secure** against

PAST and FUTURE attack strategies

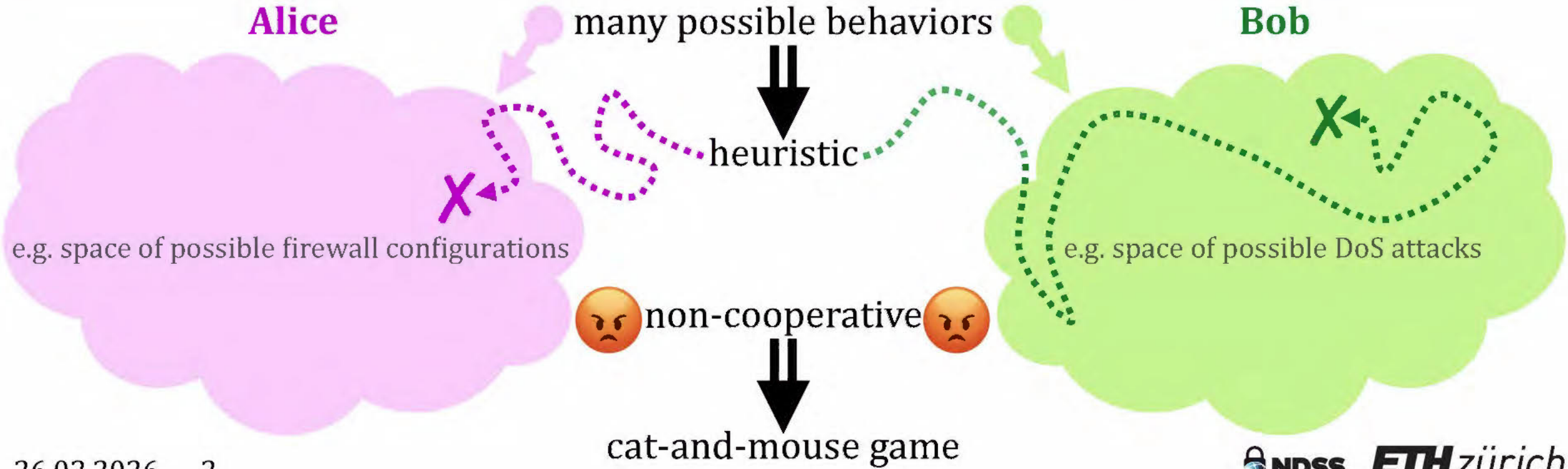


CHALLENGE

Configure complex systems

to be **optimally secure** against

PAST and FUTURE attack strategies

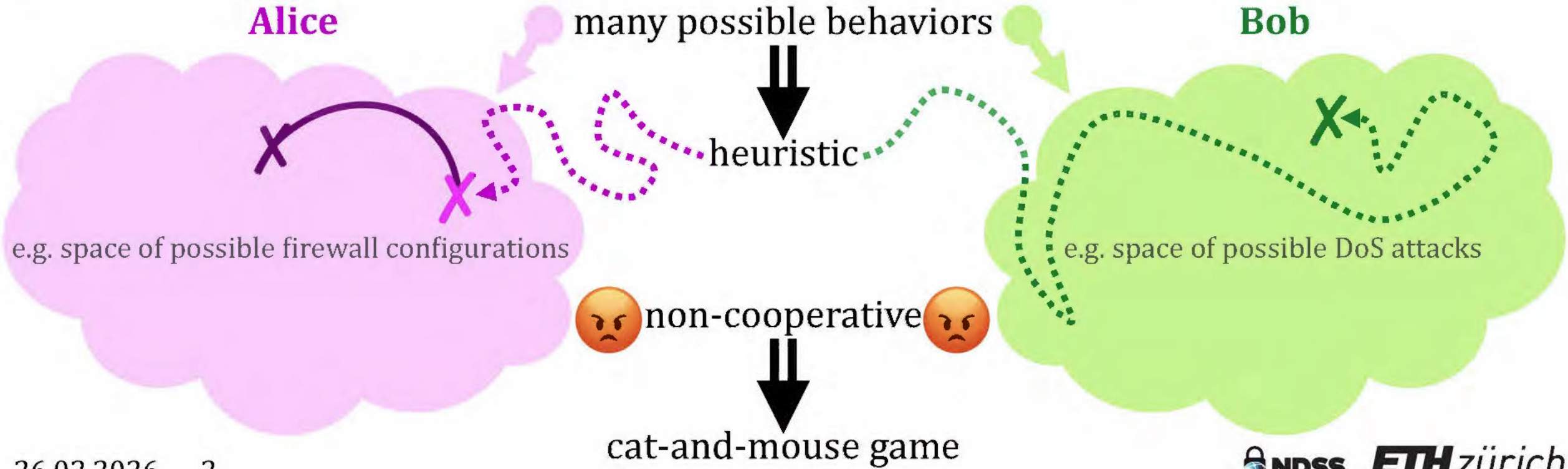


CHALLENGE

Configure complex systems

to be **optimally secure** against

PAST and FUTURE attack strategies



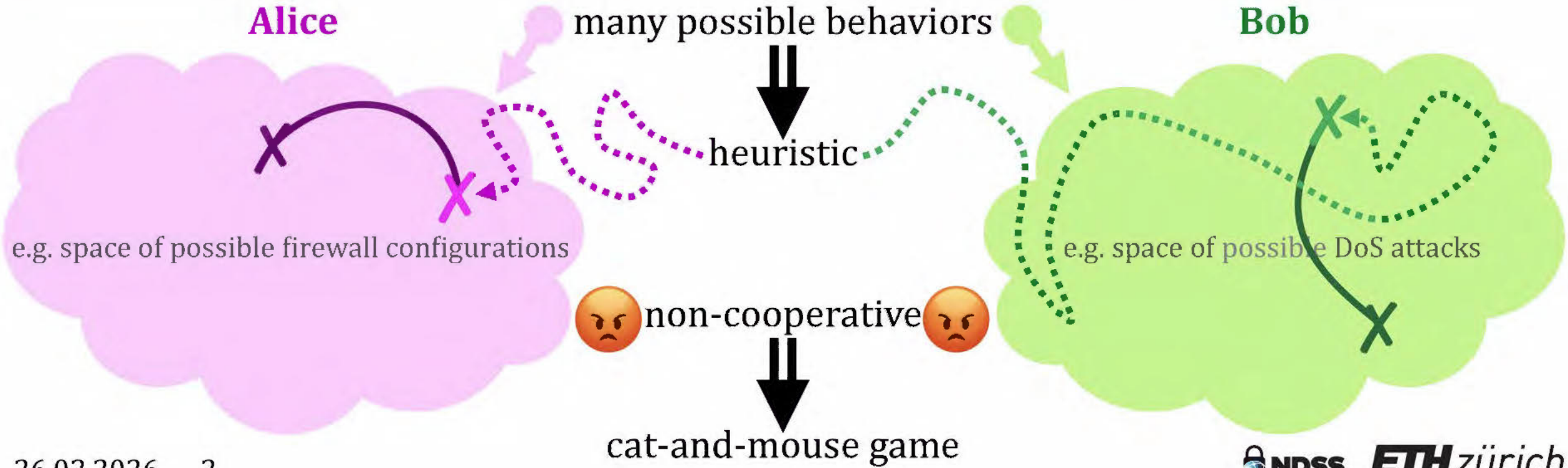
NDSS ETH zürich

CHALLENGE

Configure complex systems

to be **optimally secure** against

PAST and FUTURE attack strategies



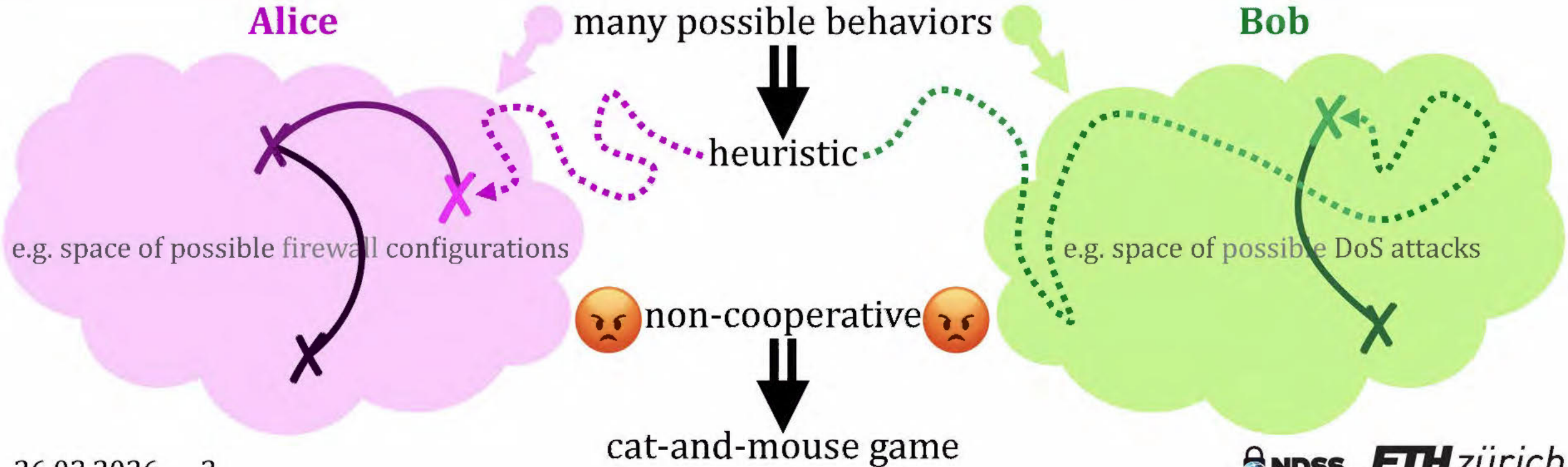
NDSS ETH zürich

CHALLENGE

Configure complex systems

to be **optimally secure** against

PAST and FUTURE attack strategies



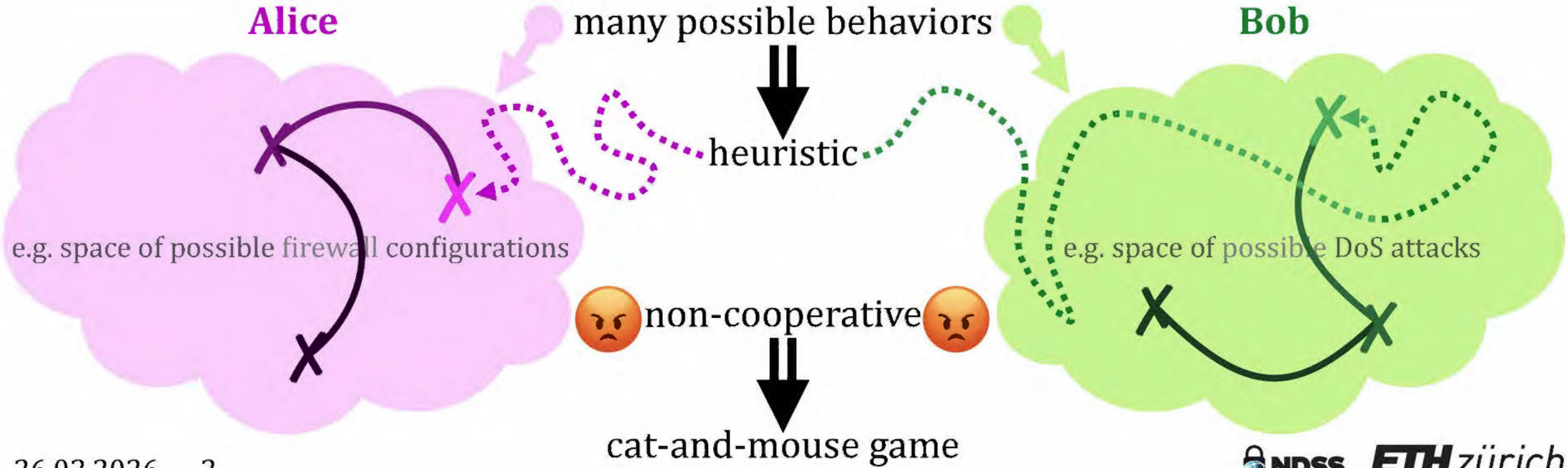
NDSS ETH zürich

CHALLENGE

Configure complex systems

to be **optimally secure** against

PAST and FUTURE attack strategies



NDSS ETH zürich

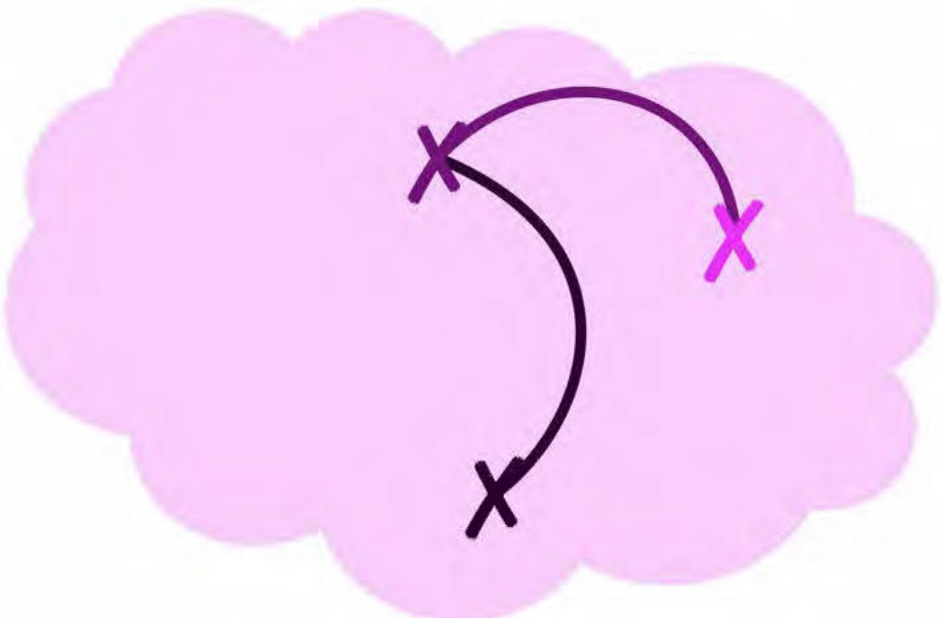
CHALLENGE

Configure complex systems

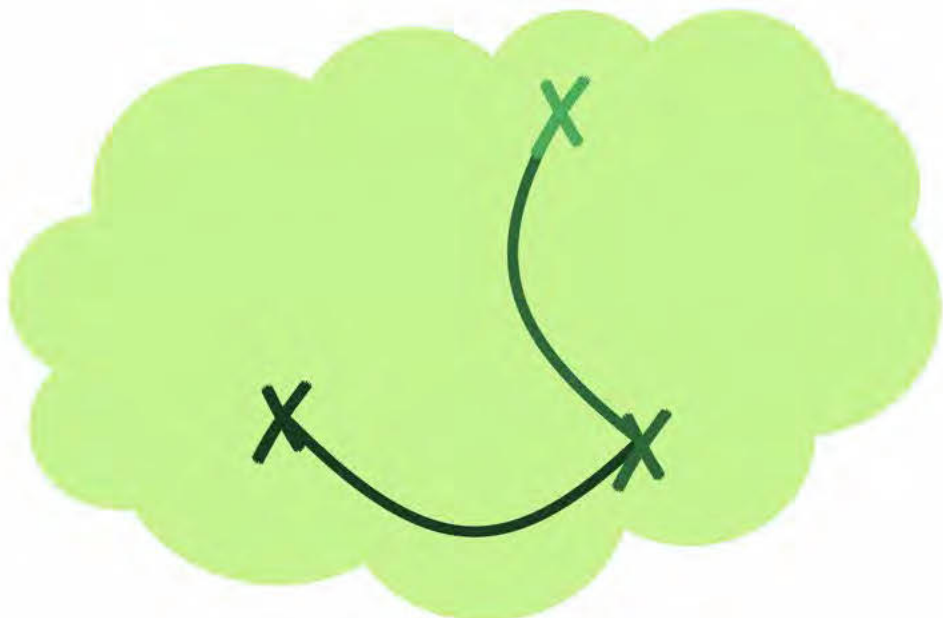
to be **optimally secure** against

PAST and FUTURE attack strategies

Alice



Bob



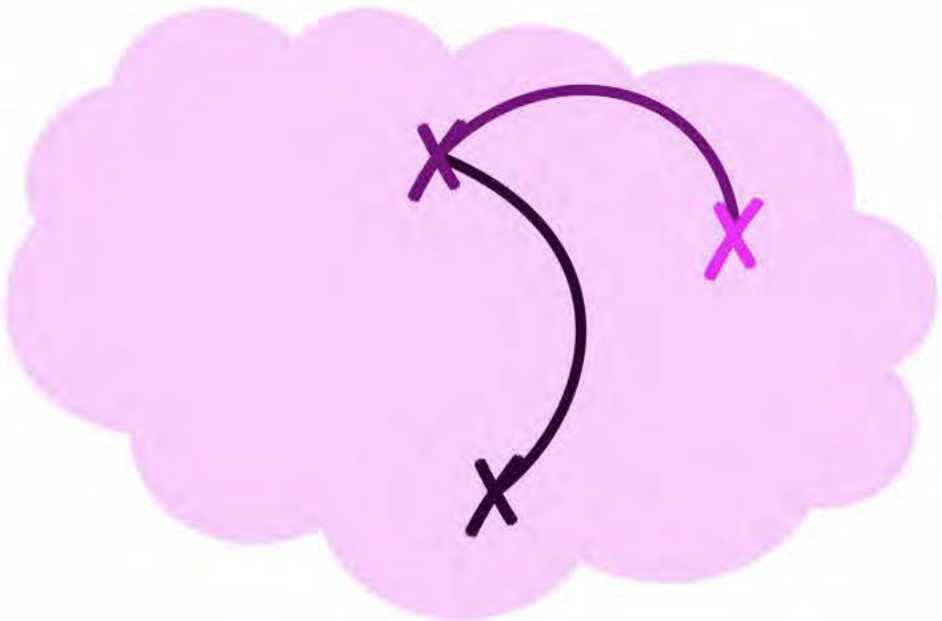
CHALLENGE

Configure complex systems

to be **optimally secure** against

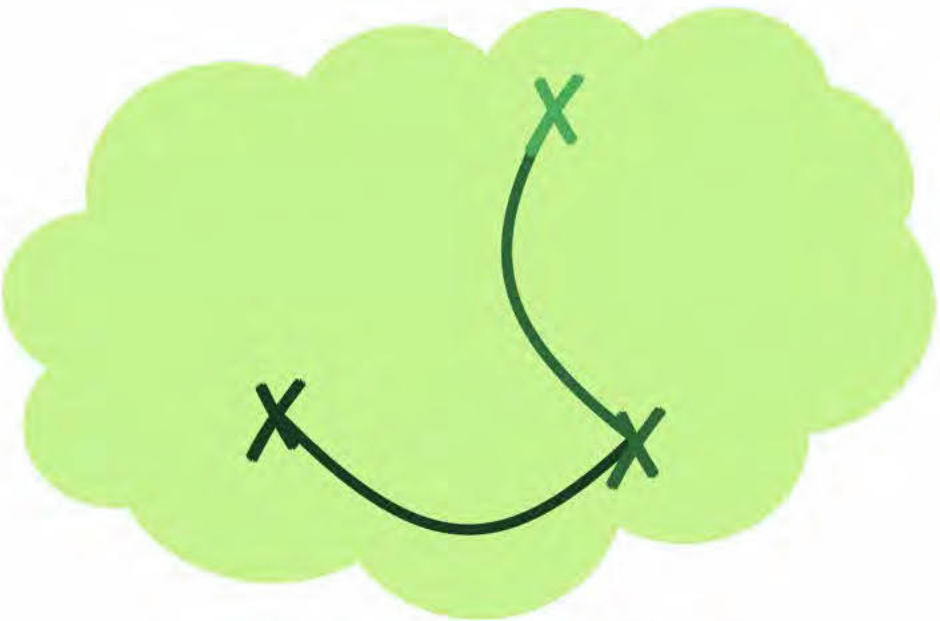
PAST and FUTURE attack strategies

Alice

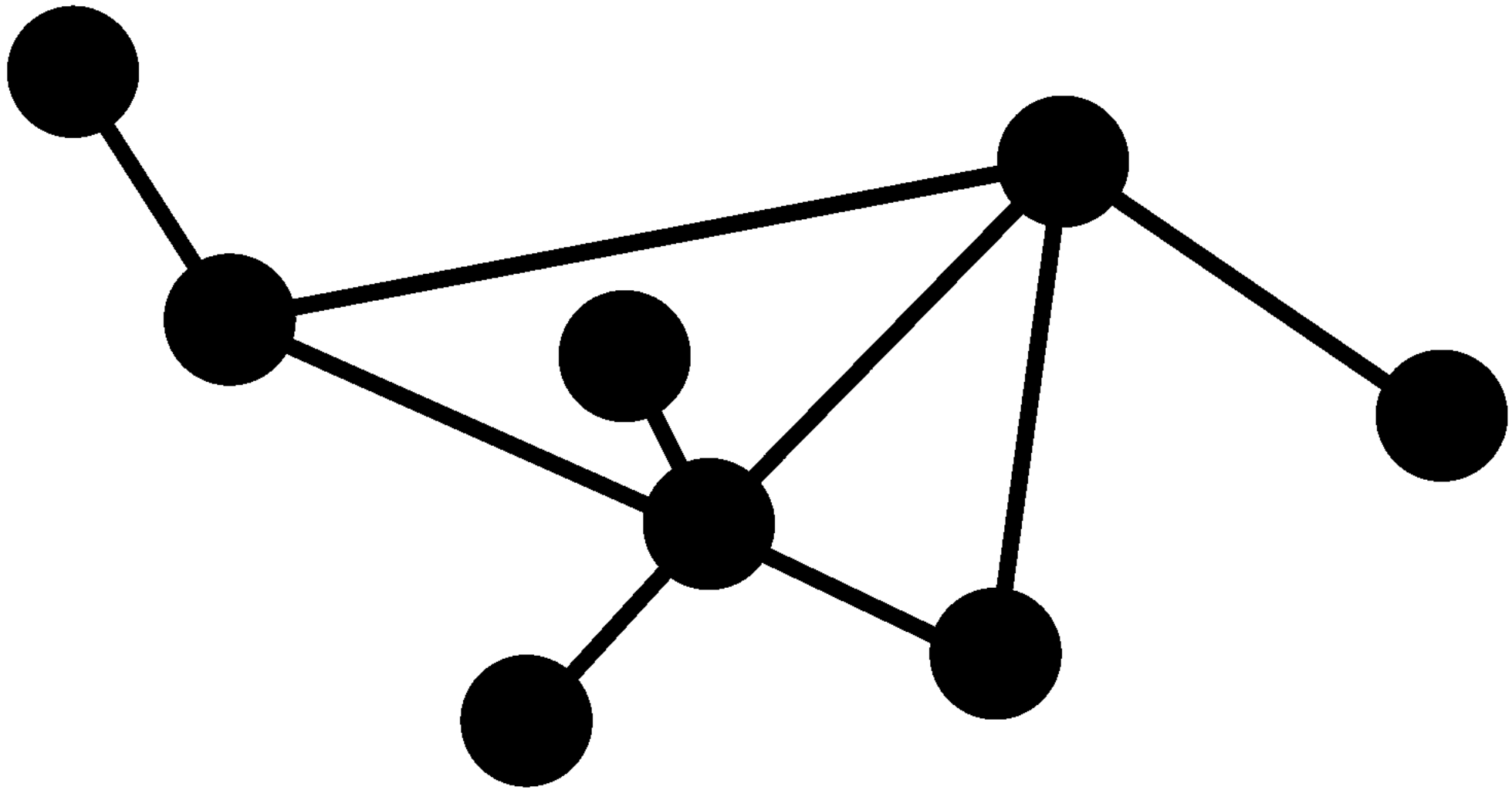


Do in Principled Way

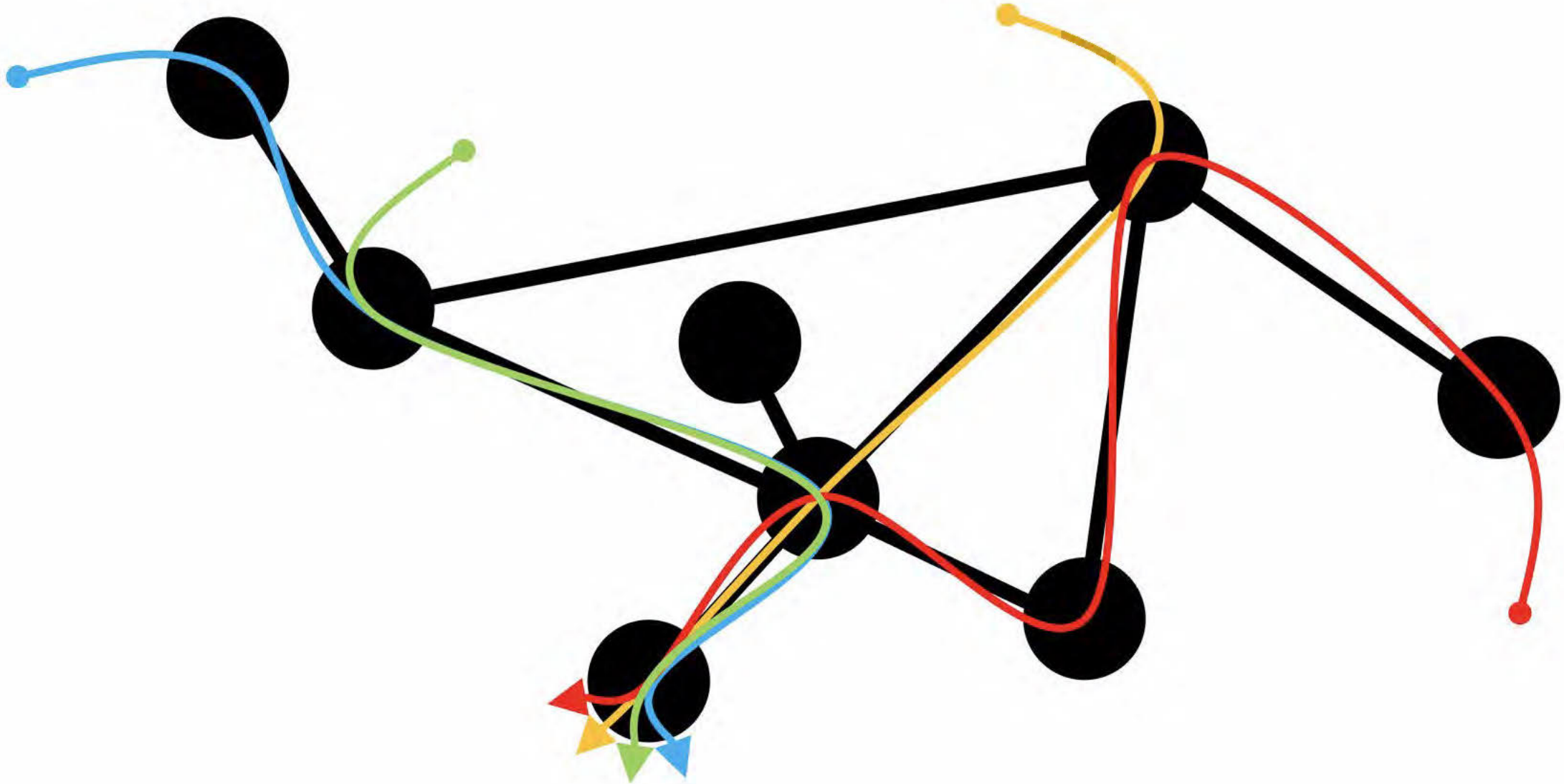
Bob



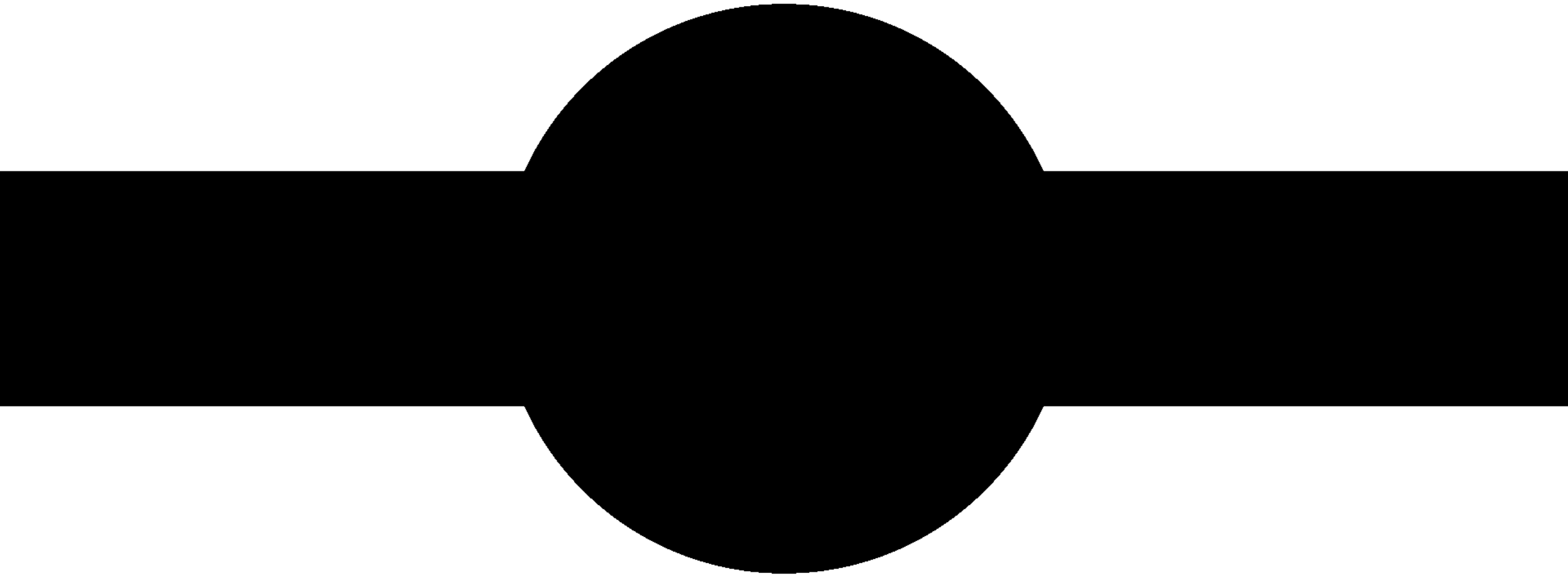
FLOW MONITORING



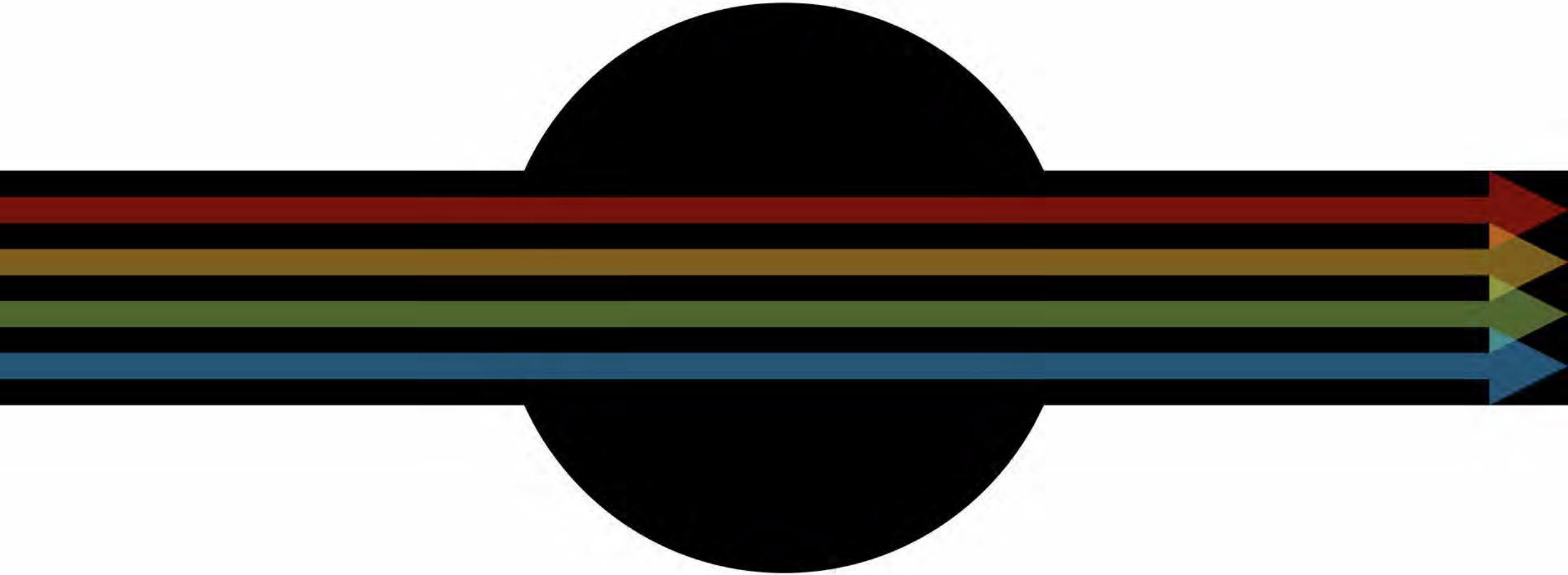
FLOW MONITORING



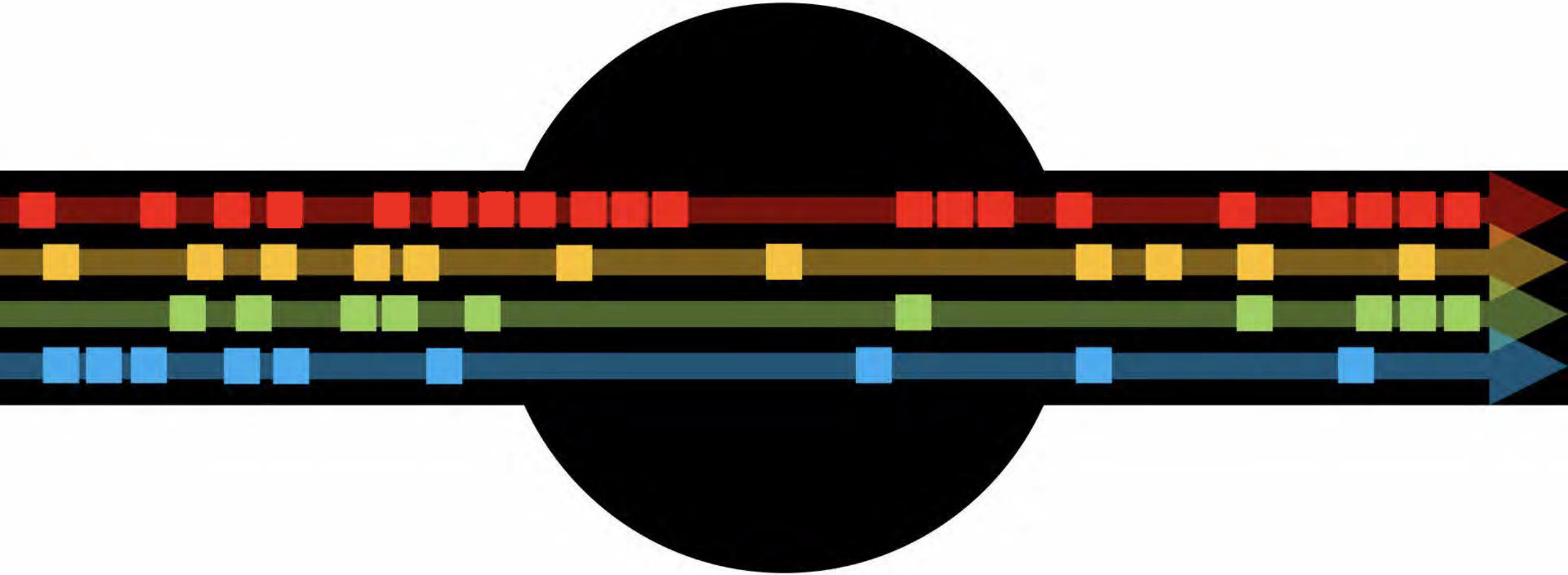
FLOW MONITORING



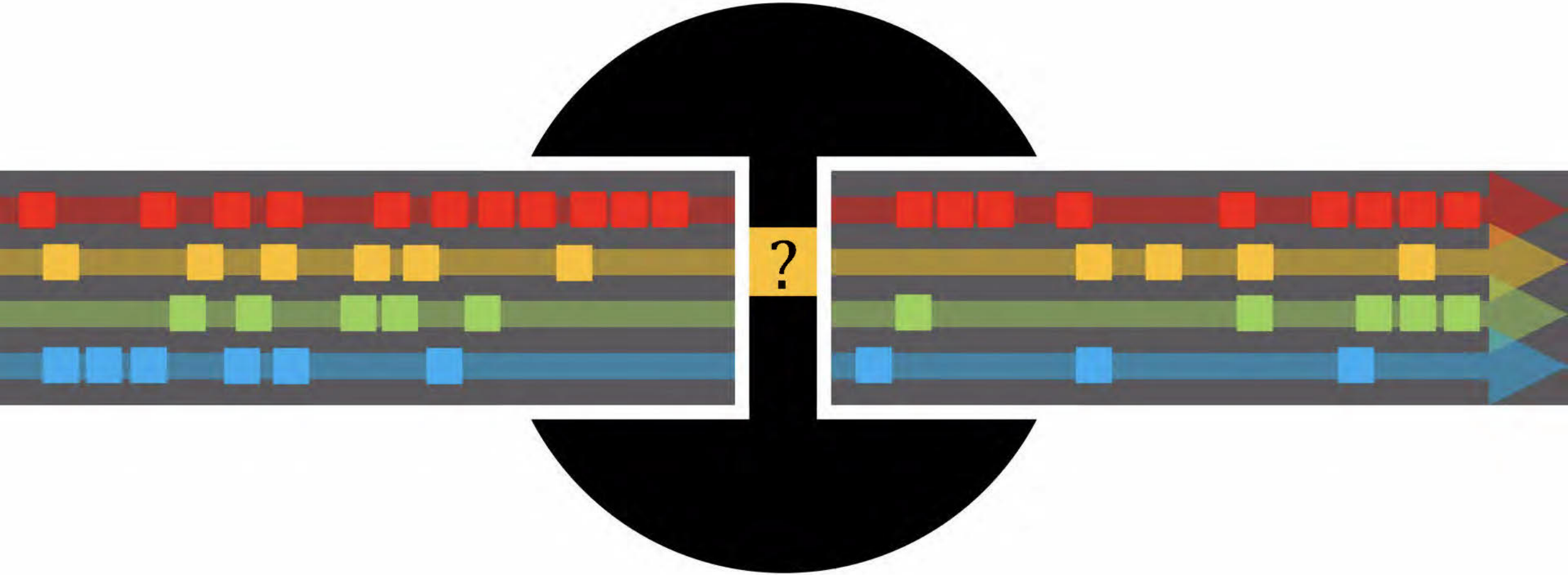
FLOW MONITORING



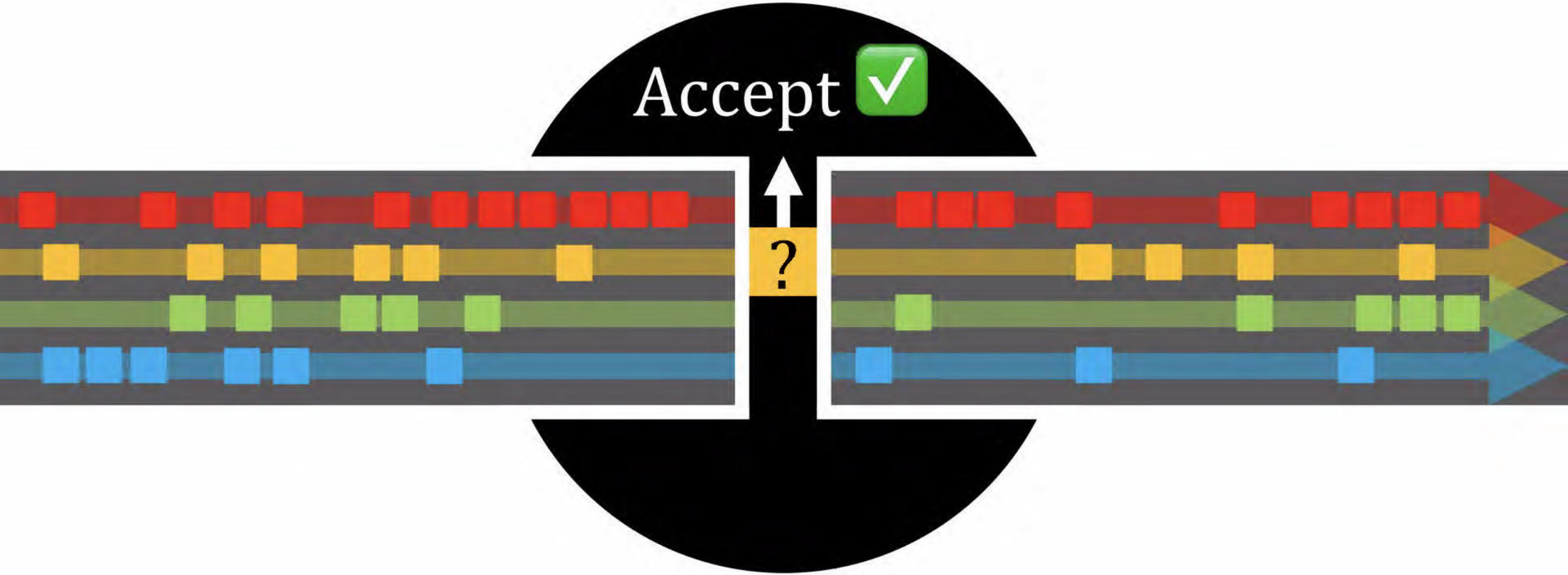
FLOW MONITORING



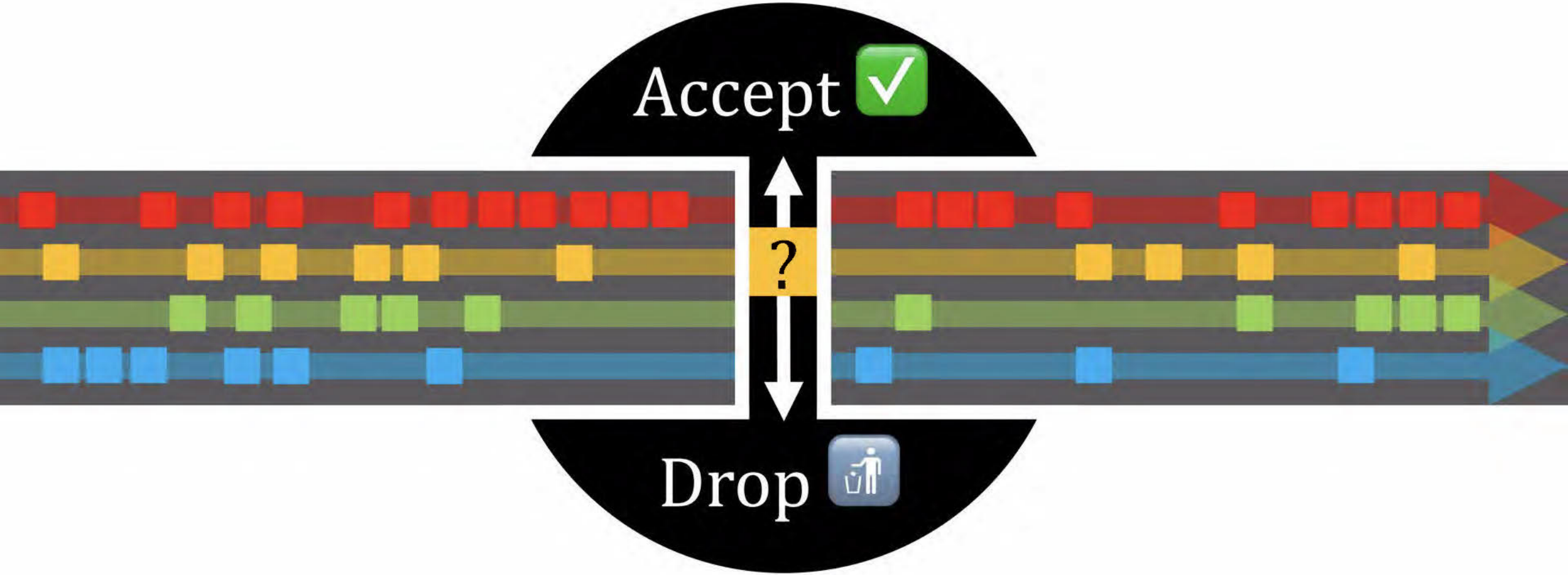
FLOW MONITORING



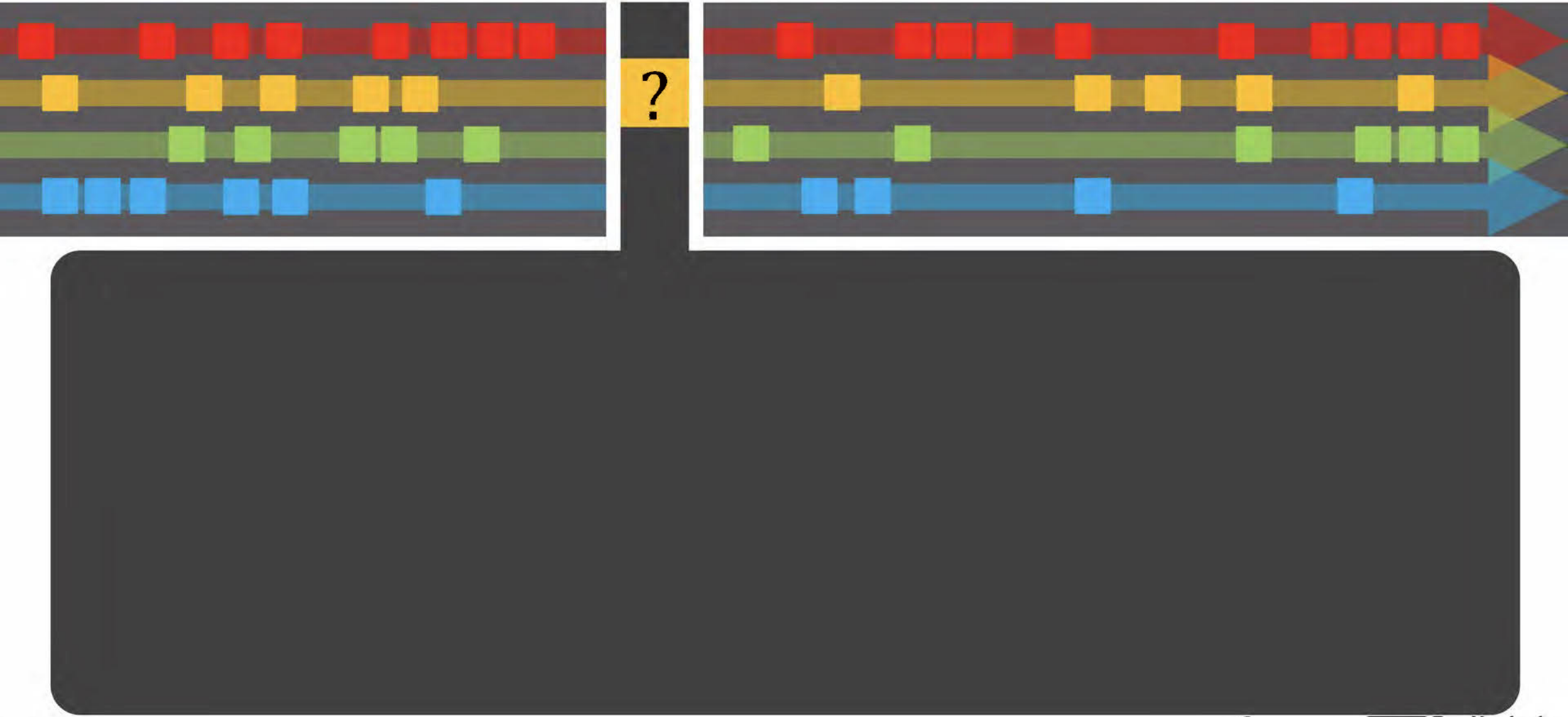
FLOW MONITORING



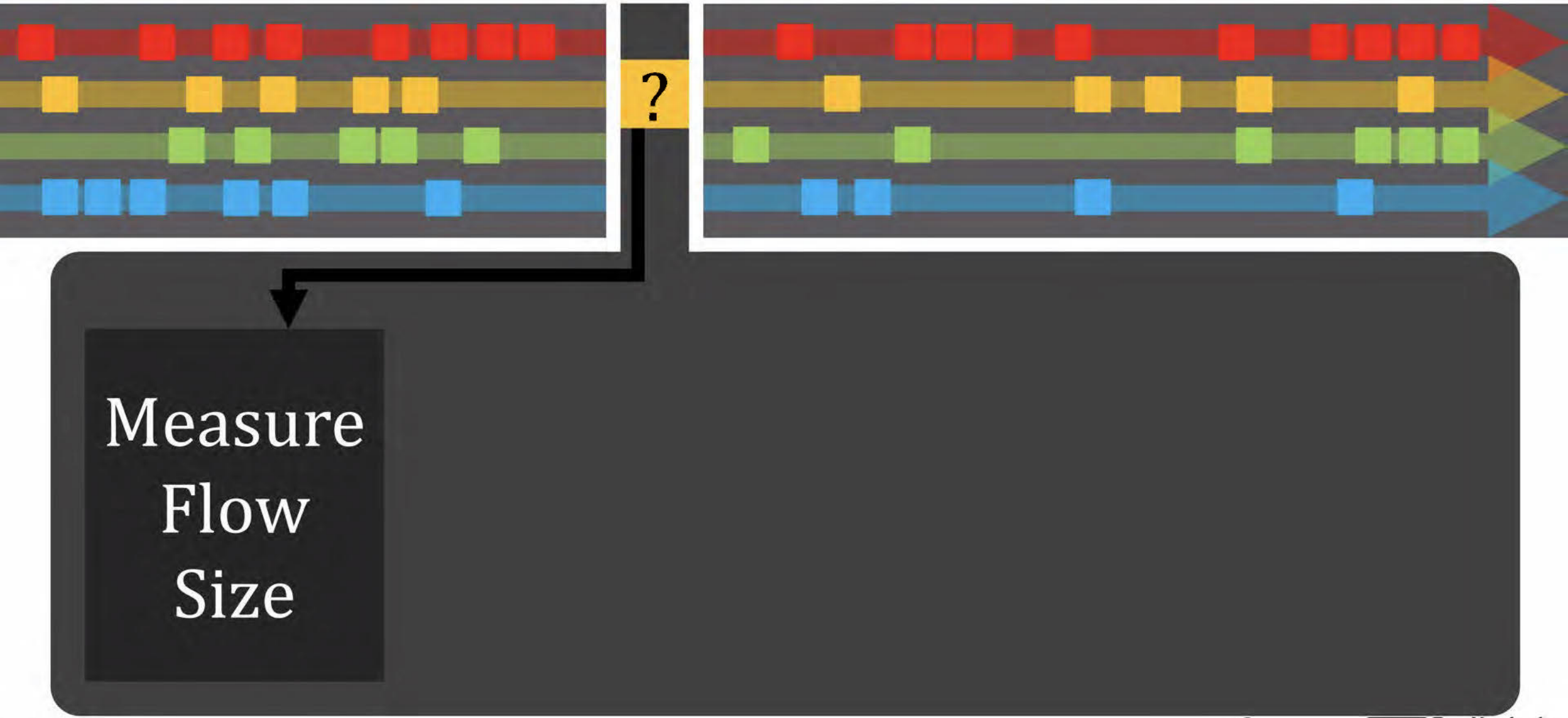
FLOW MONITORING



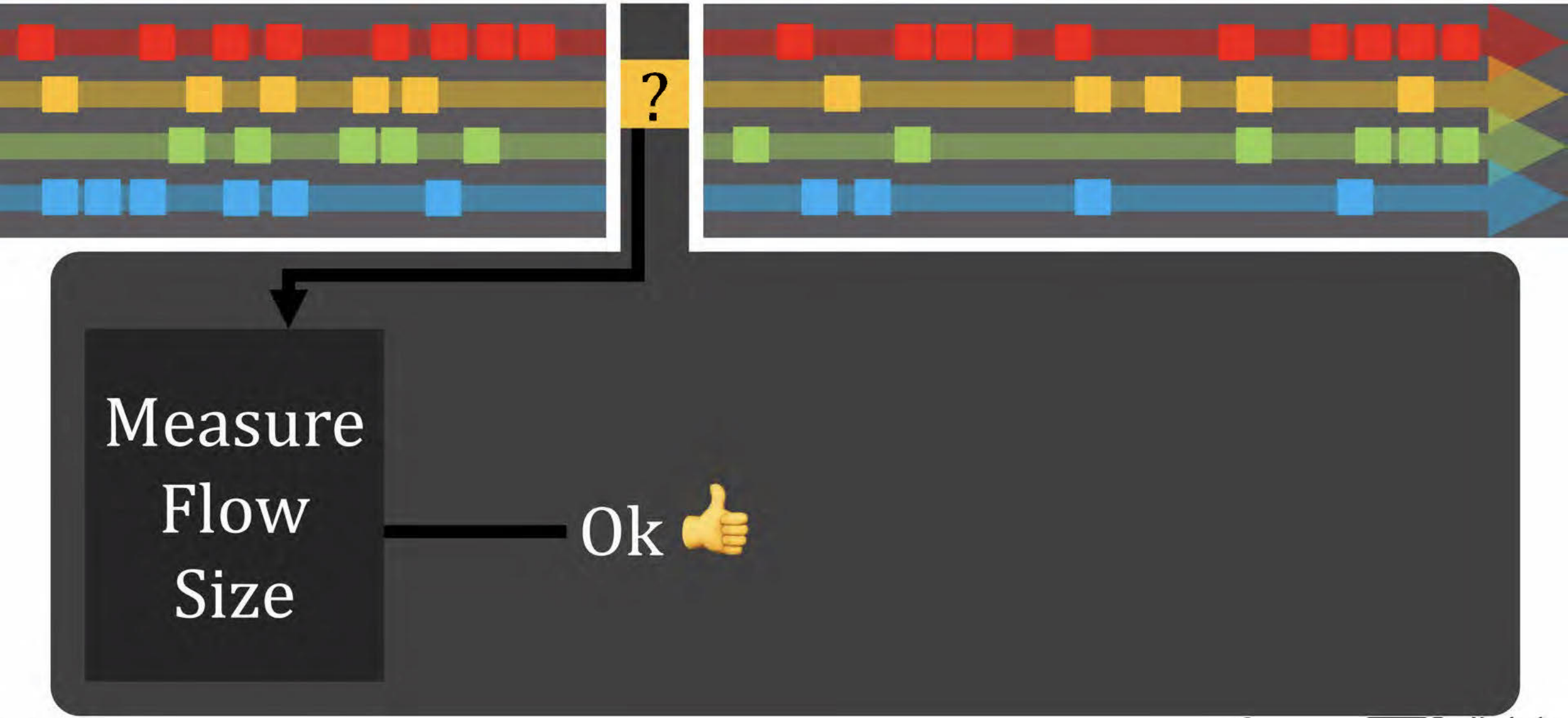
RATE MONITORING AND LIMITING



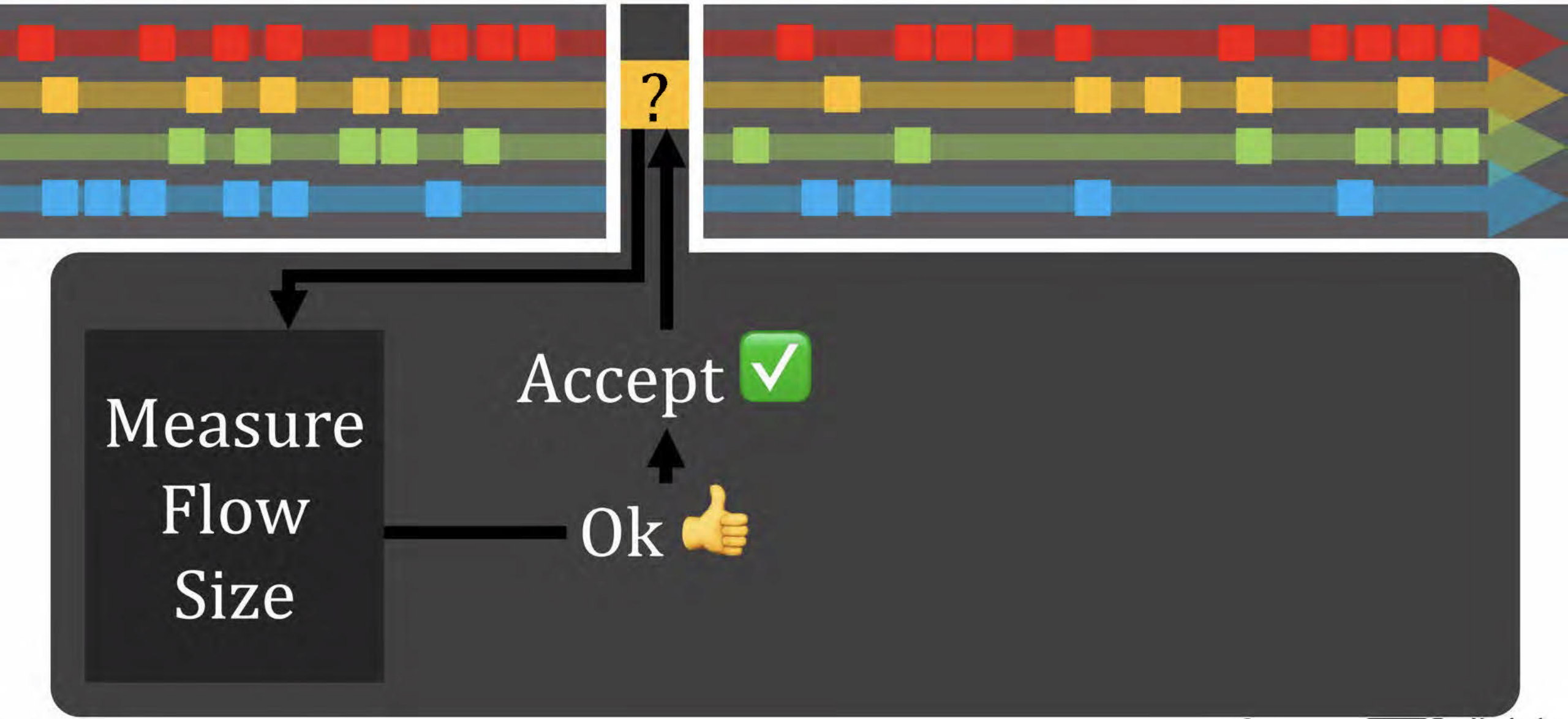
RATE MONITORING AND LIMITING



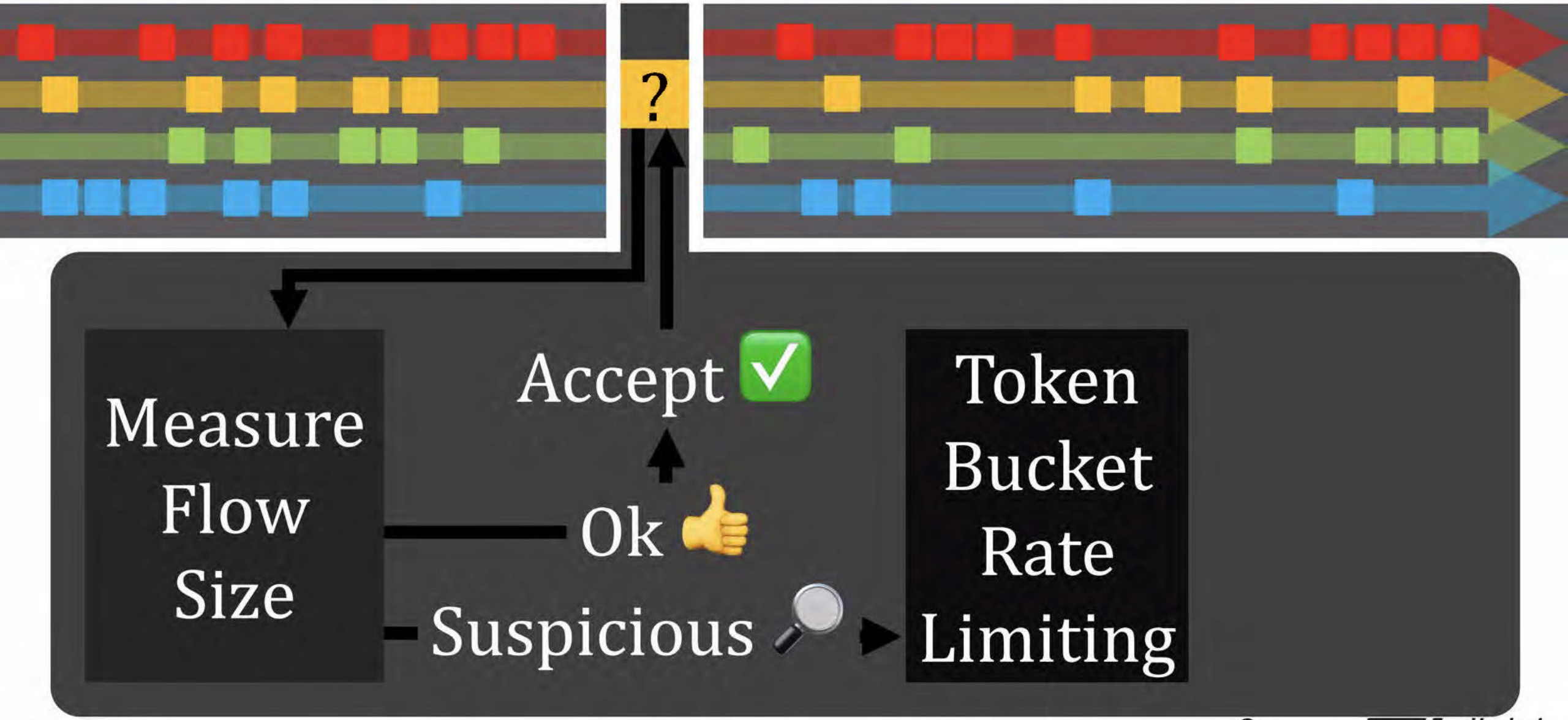
RATE MONITORING AND LIMITING



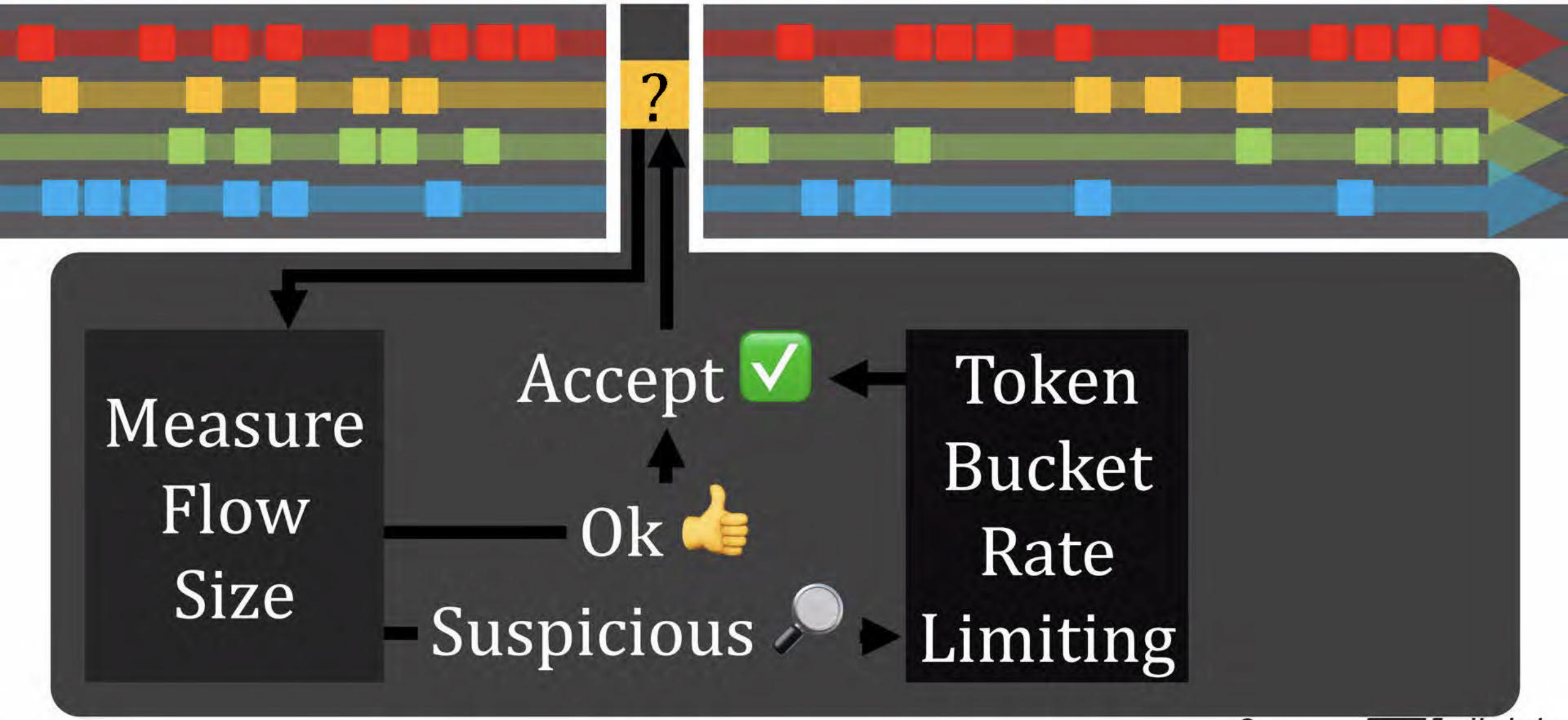
RATE MONITORING AND LIMITING



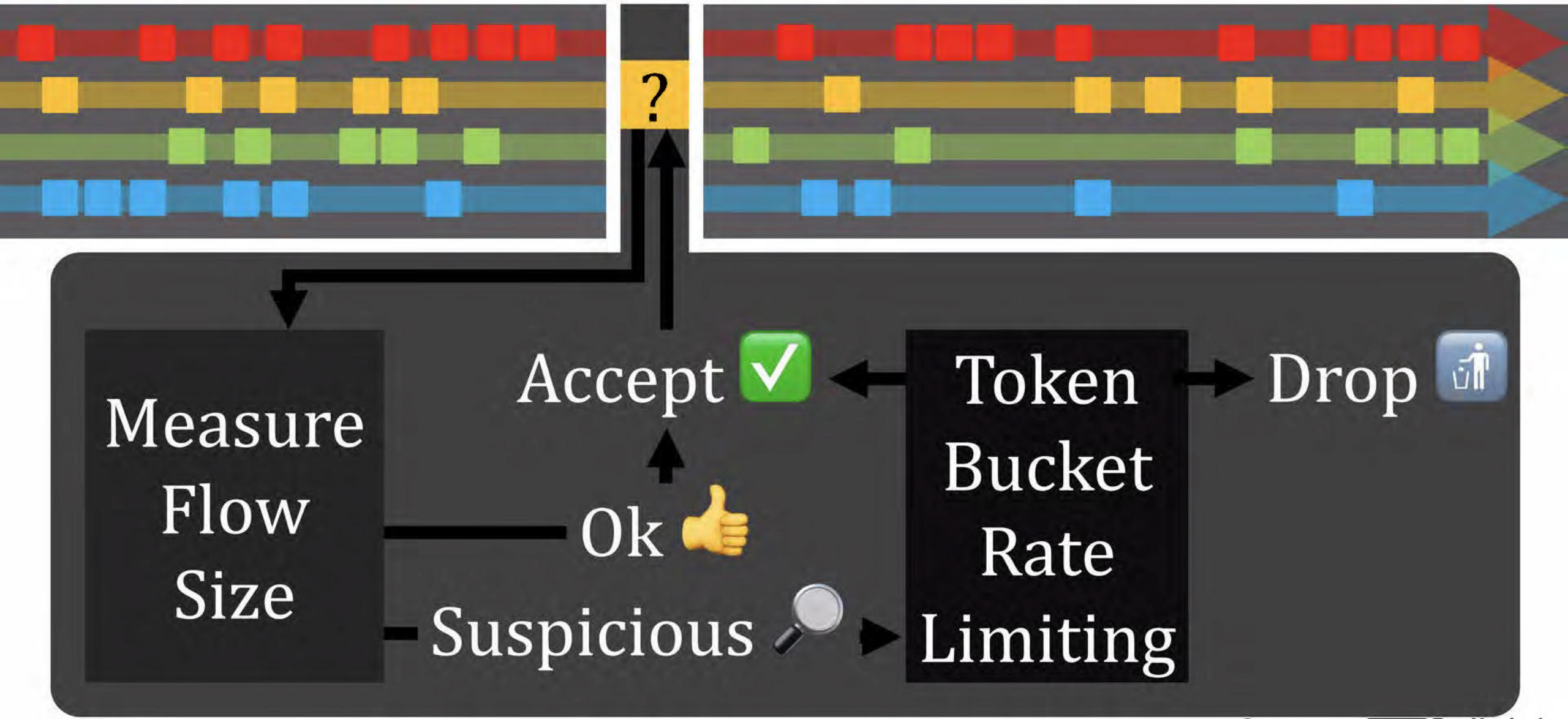
RATE MONITORING AND LIMITING



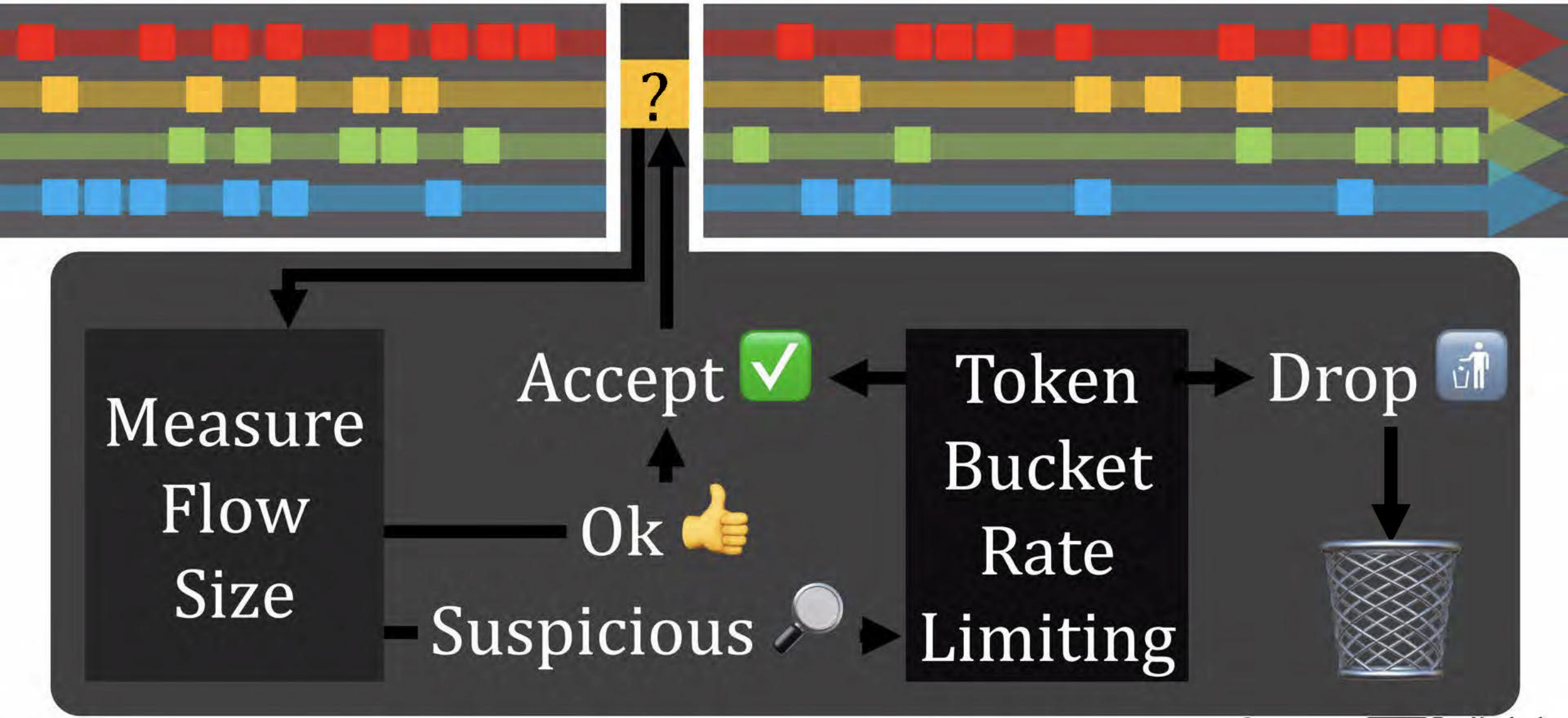
RATE MONITORING AND LIMITING



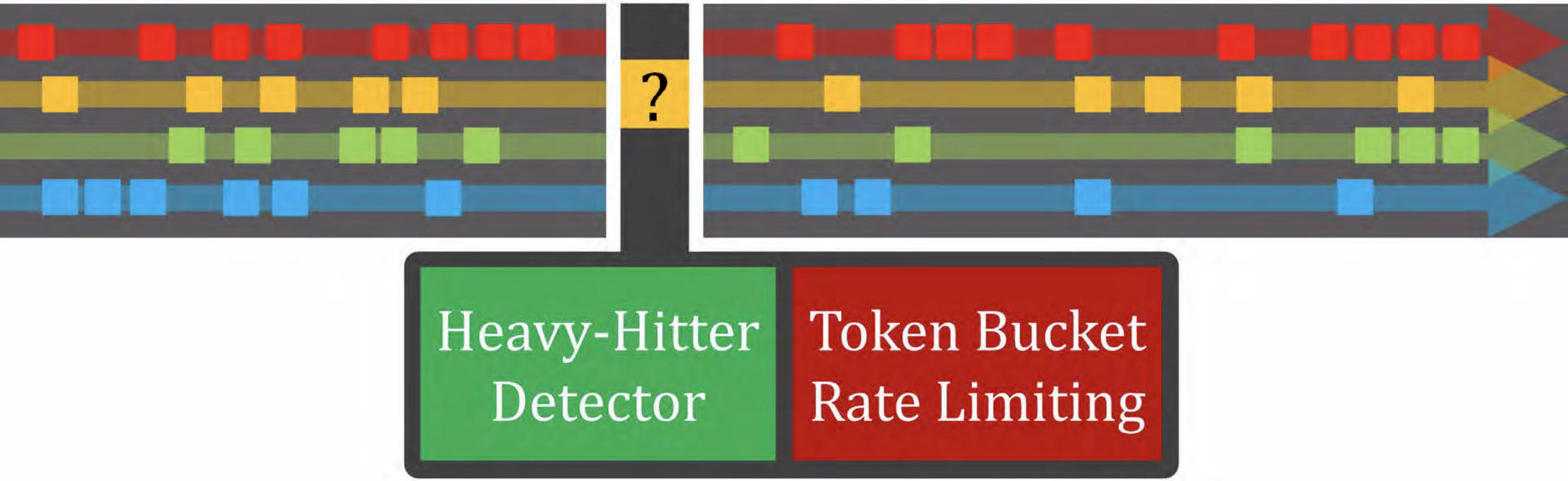
RATE MONITORING AND LIMITING



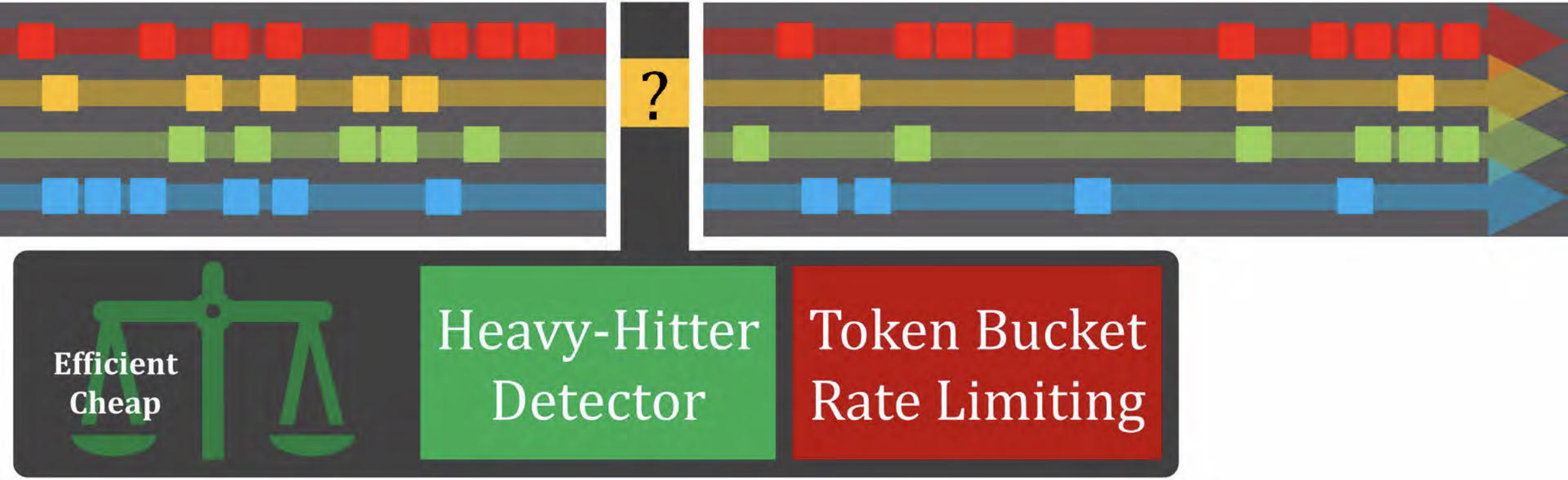
RATE MONITORING AND LIMITING



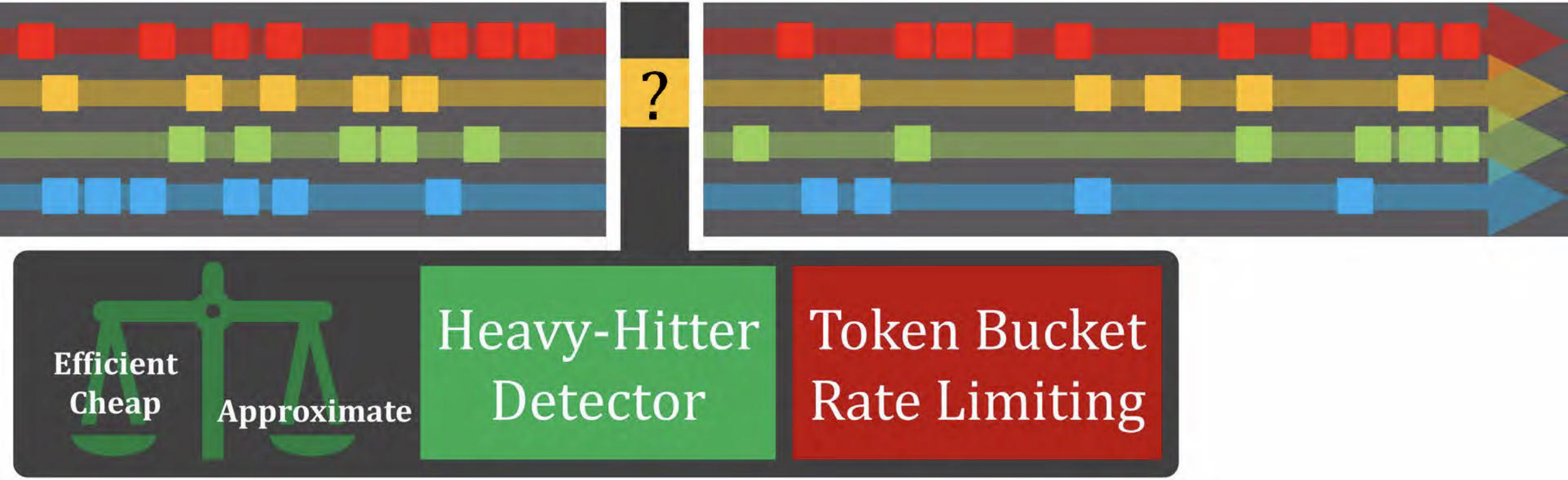
RATE MONITORING AND LIMITING



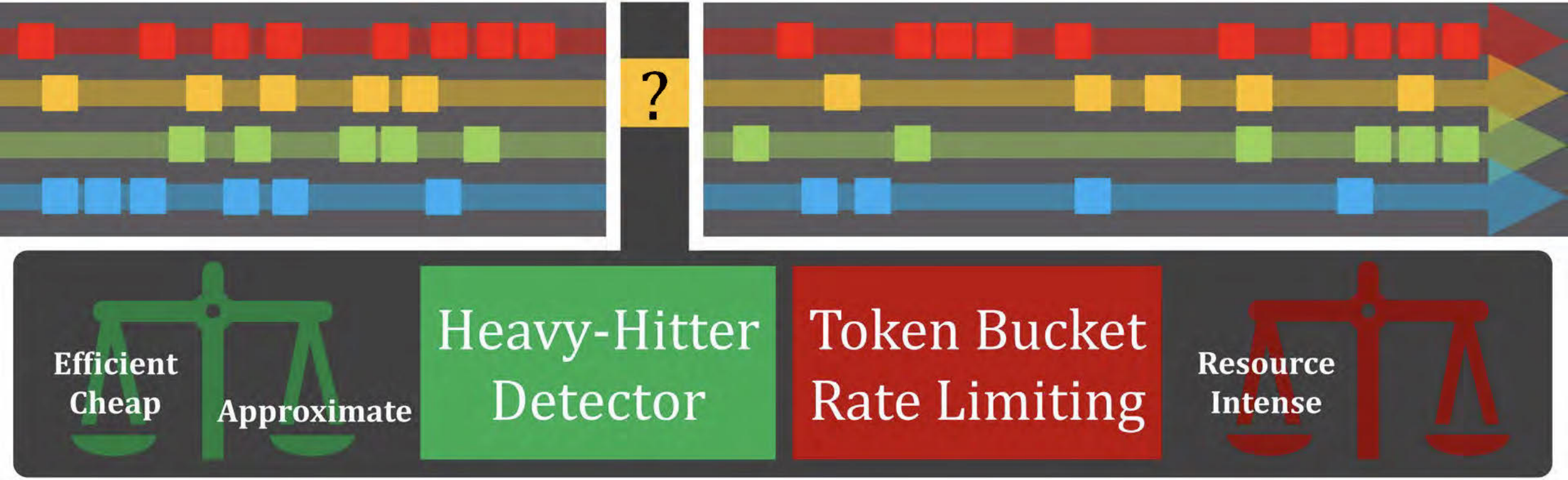
RATE MONITORING AND LIMITING



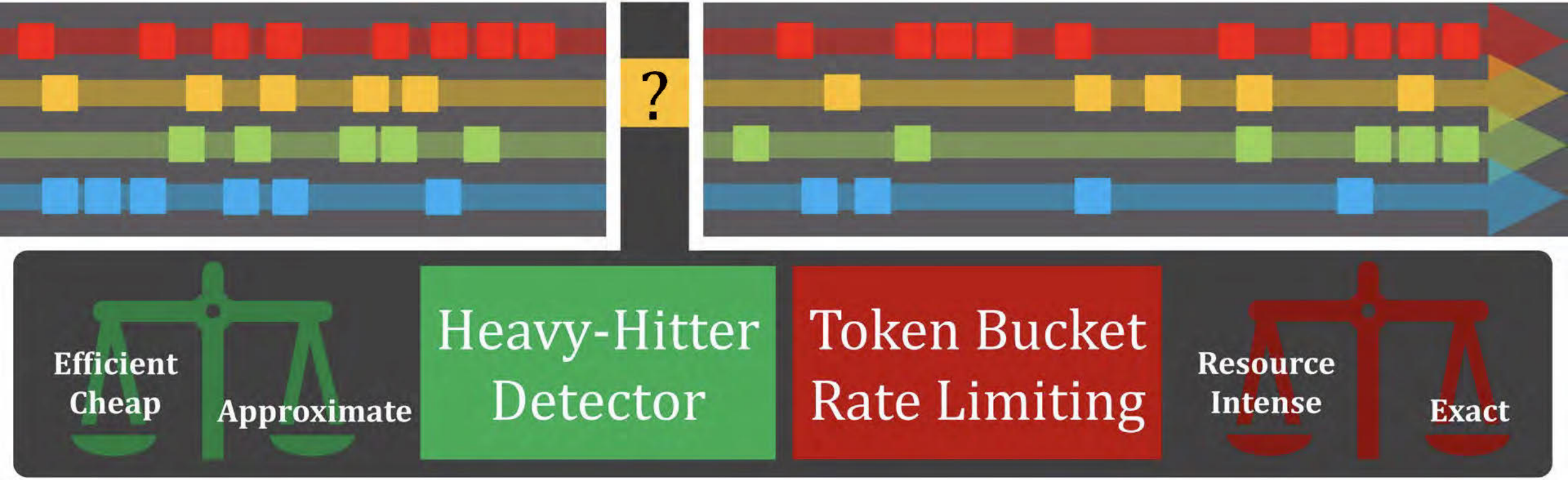
RATE MONITORING AND LIMITING



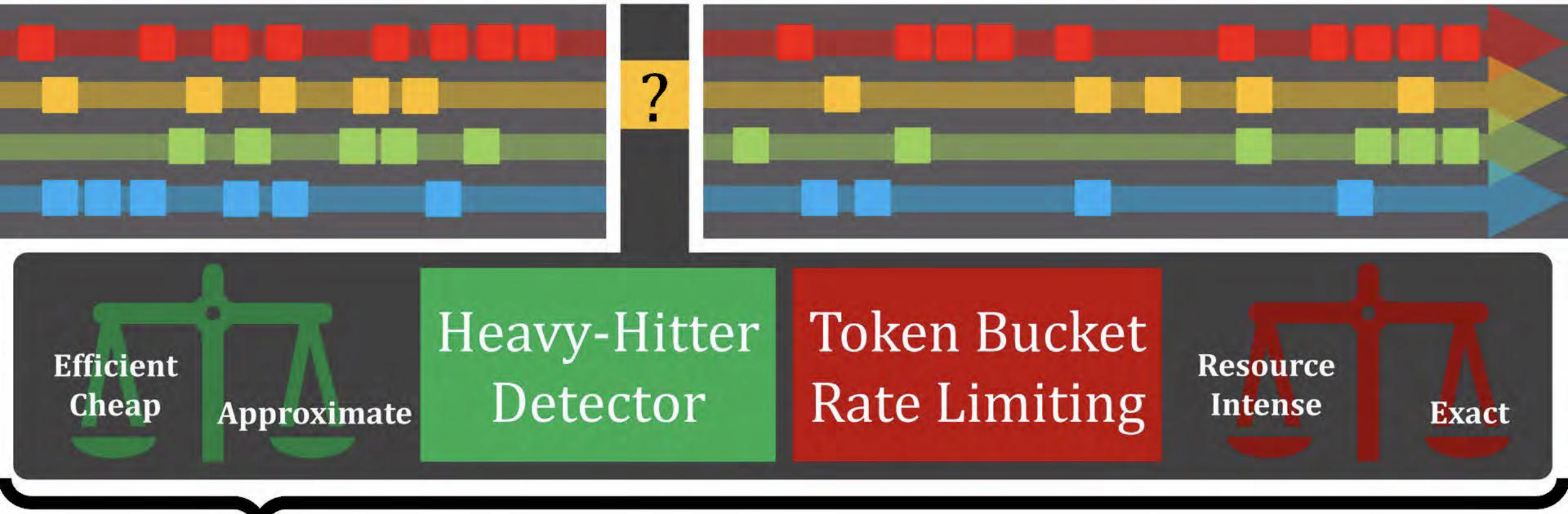
RATE MONITORING AND LIMITING



RATE MONITORING AND LIMITING

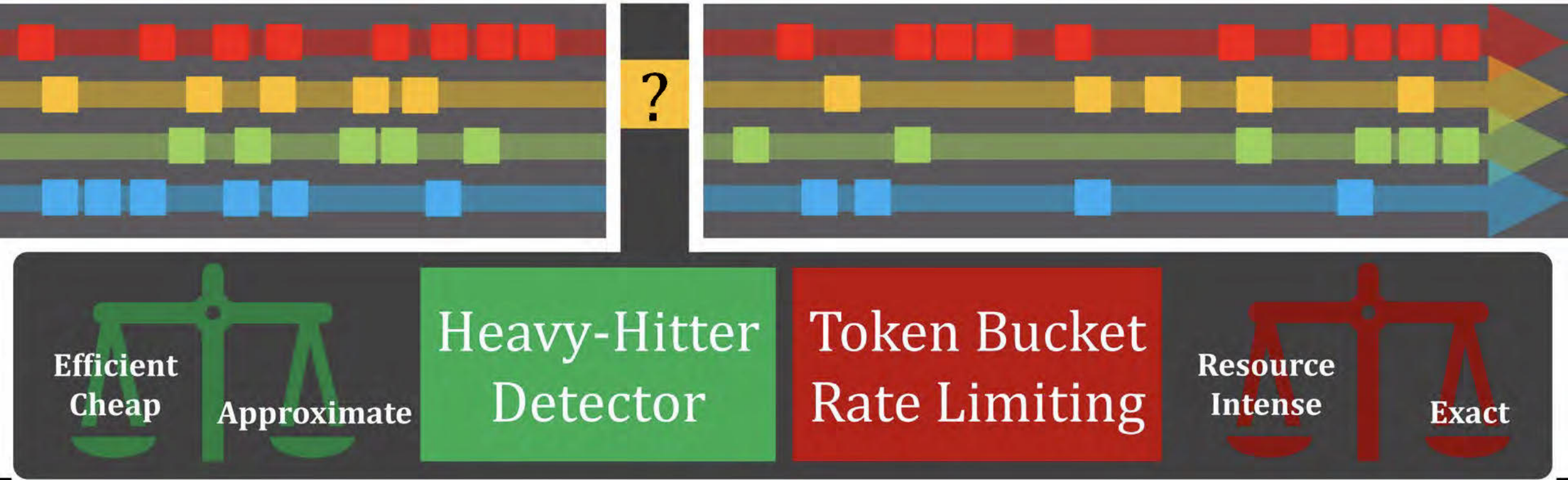


RATE MONITORING AND LIMITING



How to configure optimally ?

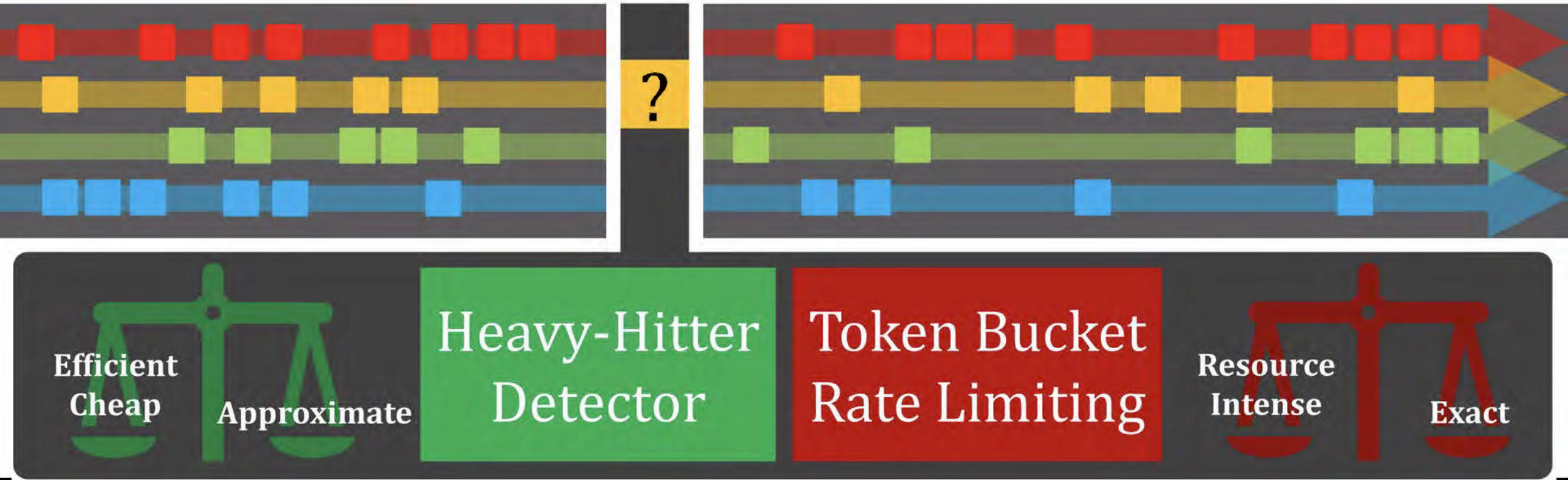
RATE MONITORING AND LIMITING



How to configure optimally ?

Depends on attack.

RATE MONITORING AND LIMITING

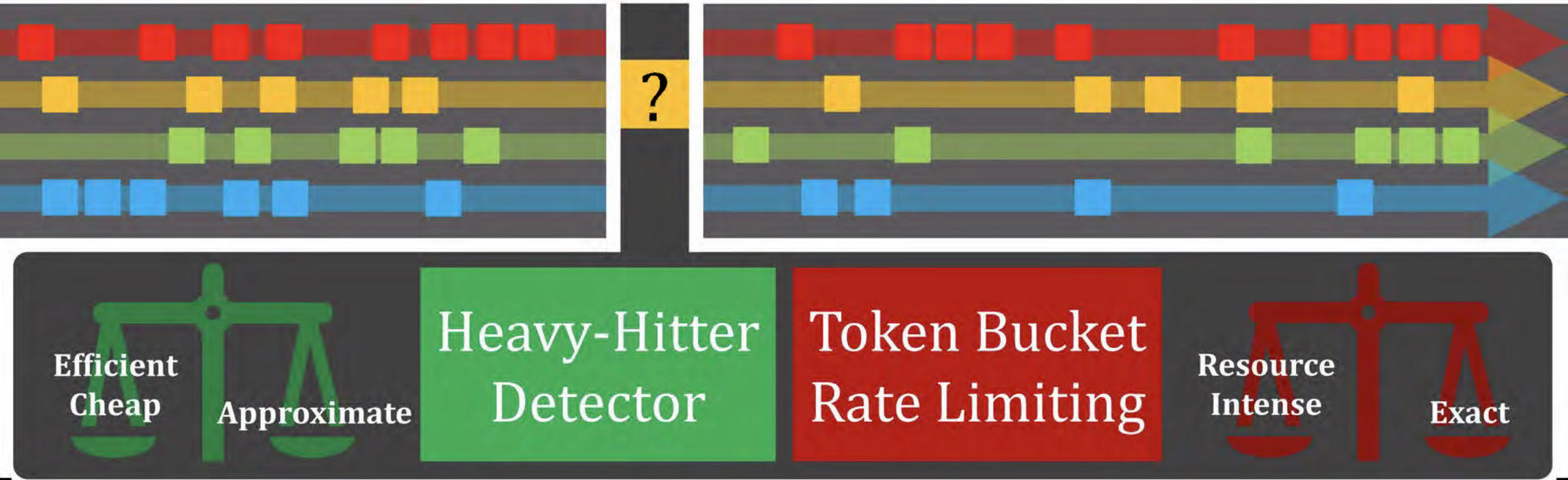


How to configure optimally ?

Depends on attack.

Whats the optimal attack?

RATE MONITORING AND LIMITING



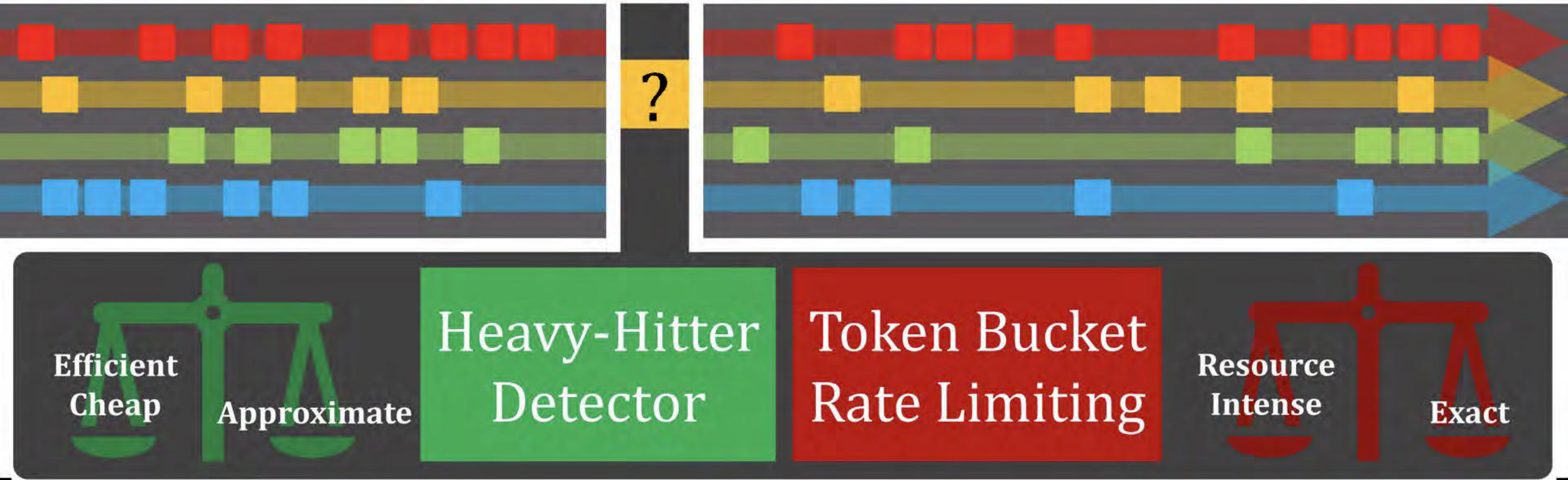
How to configure optimally ?

Depends on attack.

Whats the optimal attack?

Depends on configuration.

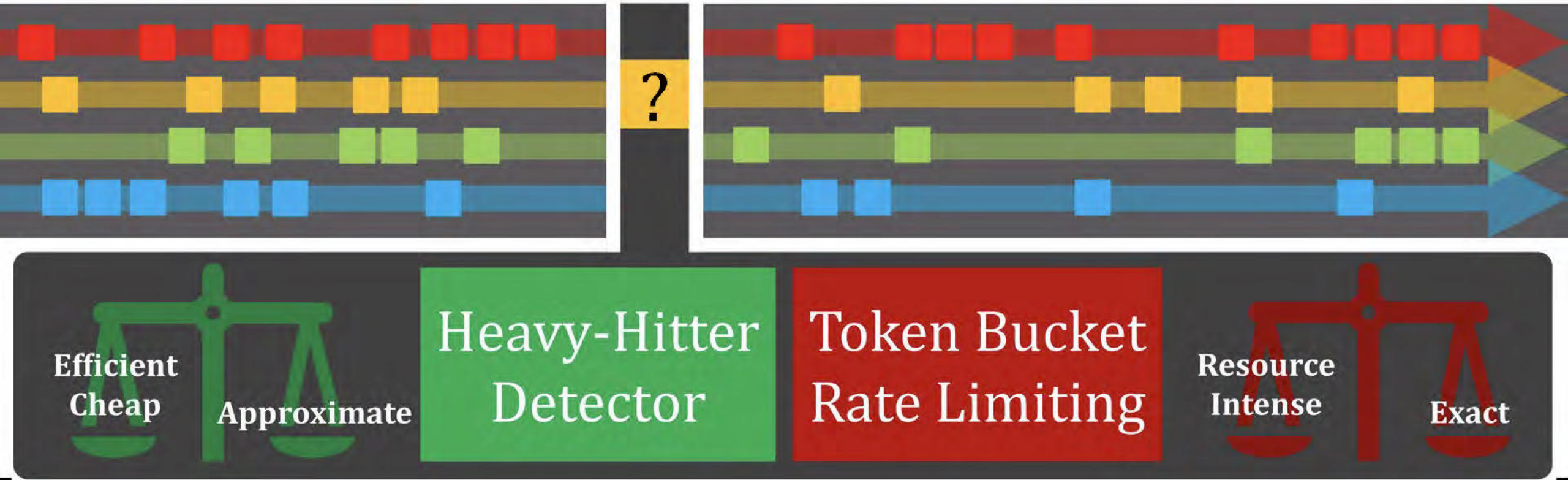
RATE MONITORING AND LIMITING



How to configure optimally ? → **Depends on attack.**

Whats the optimal attack? → **Depends on configuration.**

RATE MONITORING AND LIMITING

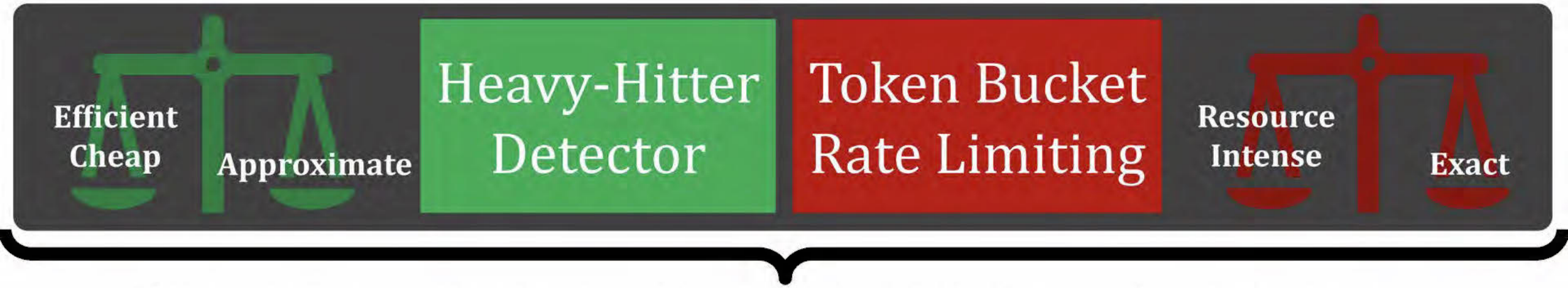


How to configure optimally ? → **Depends on attack.**

Whats the optimal attack? → **Depends on configuration.**

Nobody knows

RATE MONITORING AND LIMITING



How to configure optimally ? → **Depends on attack.**

Whats the optimal attack? → **Depends on configuration.**

RATE MONITORING AND LIMITING

How to configure optimally ?

Depends on attack.

Whats the optimal attack?

Depends on configuration.

RATE MONITORING AND LIMITING

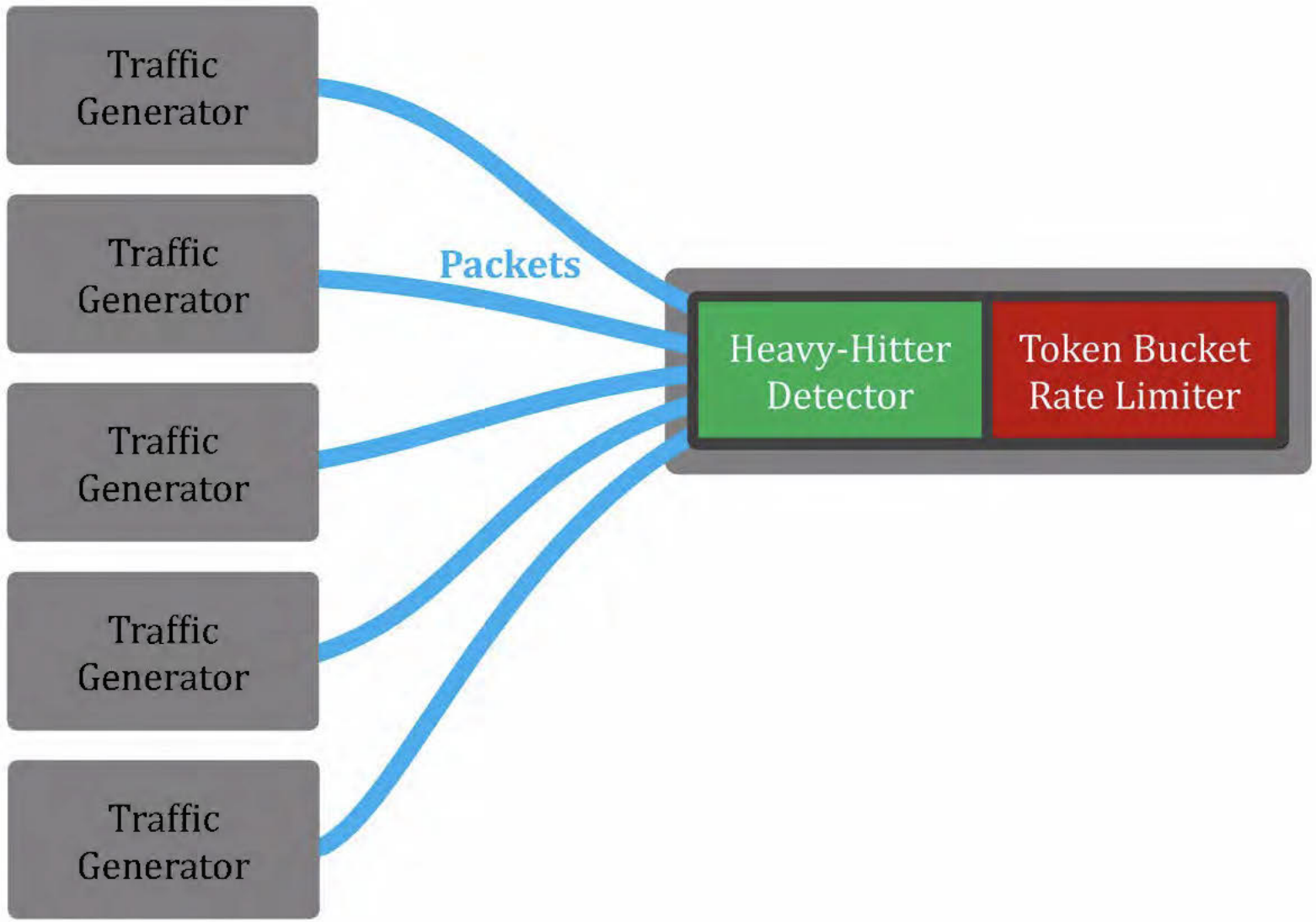
How to configure optimally ? **Whats the optimal attack?**

Depends on attack. **Depends on configuration.**

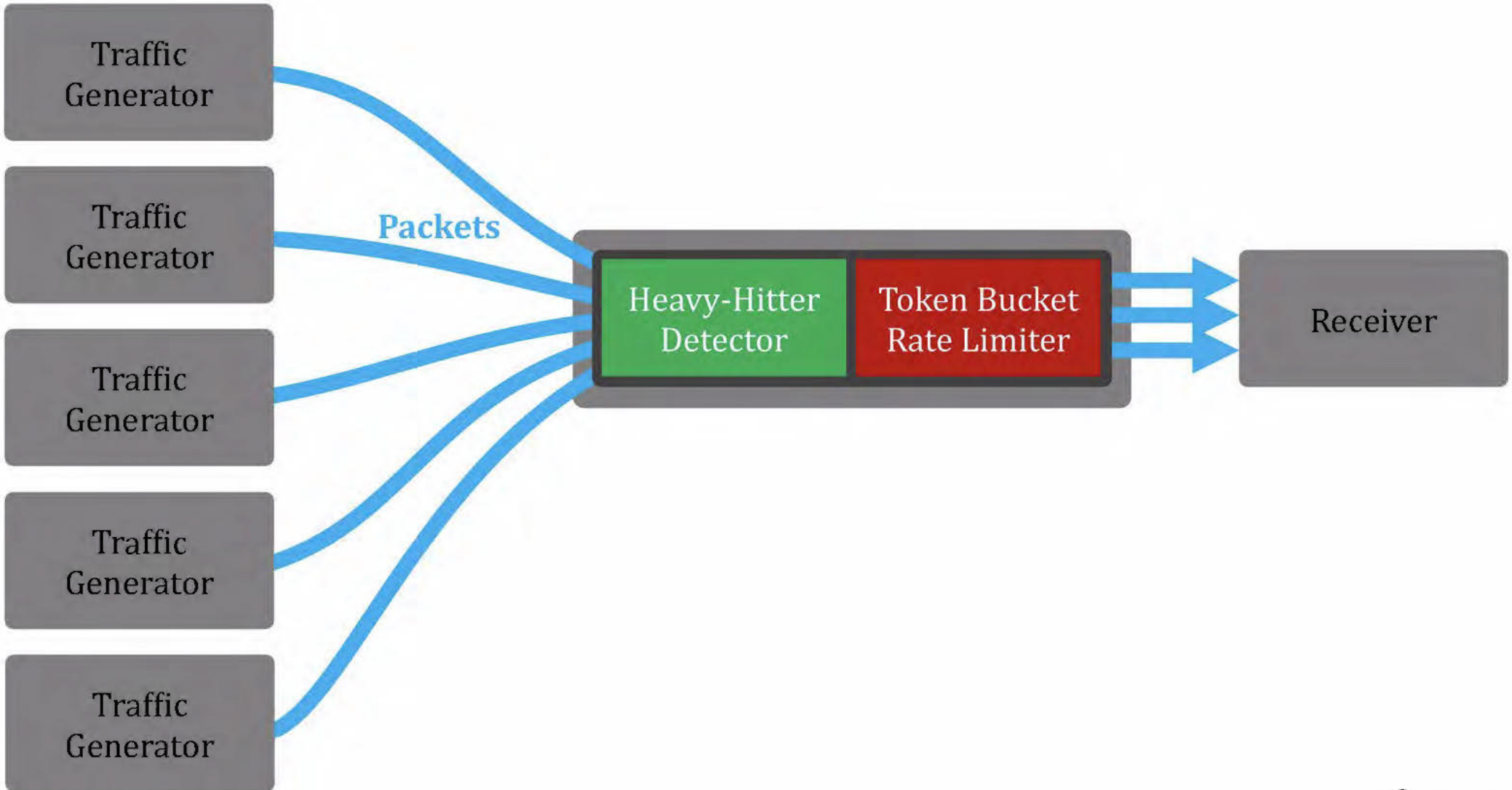
Ignoring this dependency leaves one vulnerable to adaptive adversaries.

SYSTEM STRUCTURE AND DYNAMICS

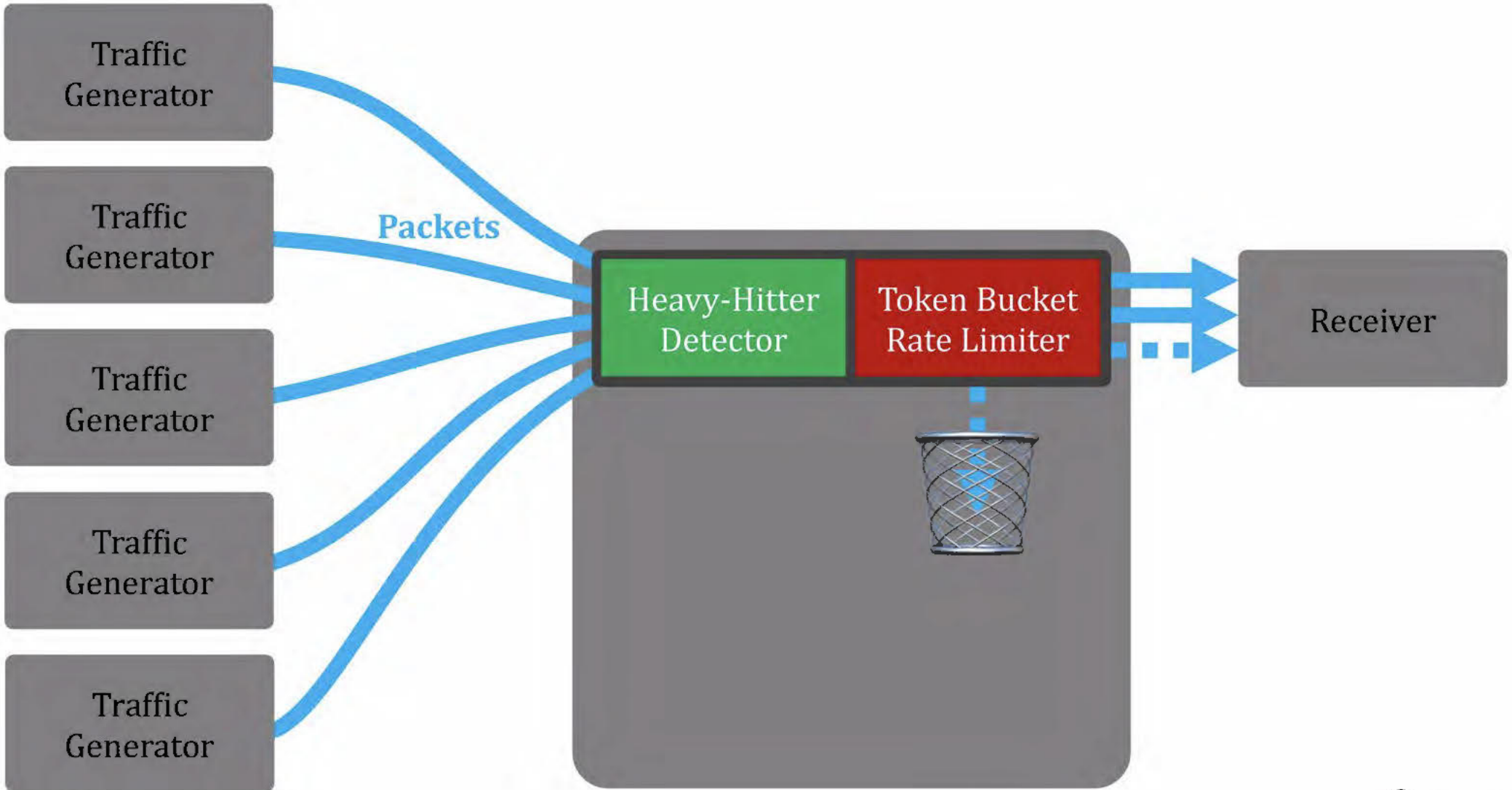
SYSTEM STRUCTURE AND DYNAMICS



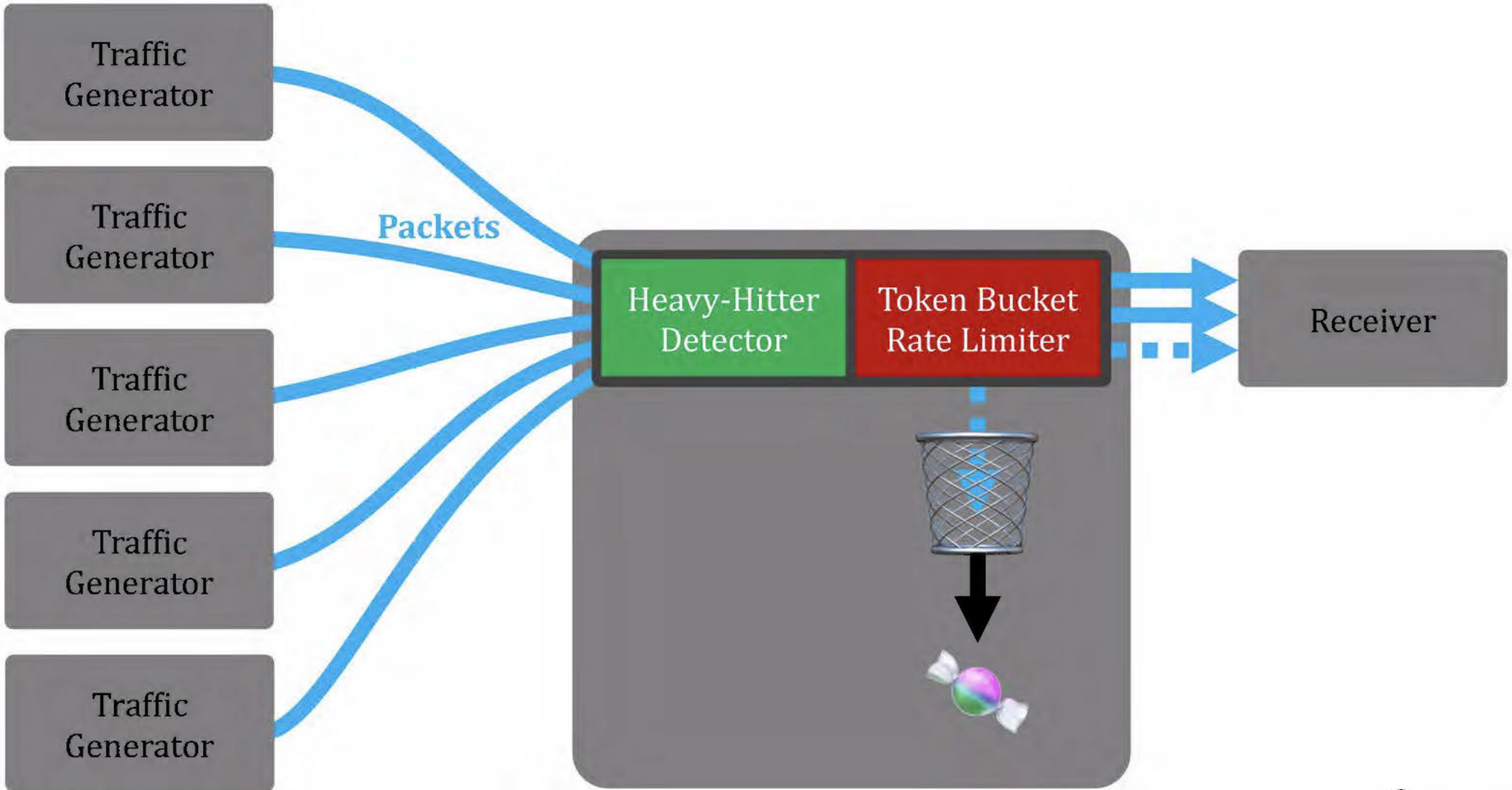
SYSTEM STRUCTURE AND DYNAMICS



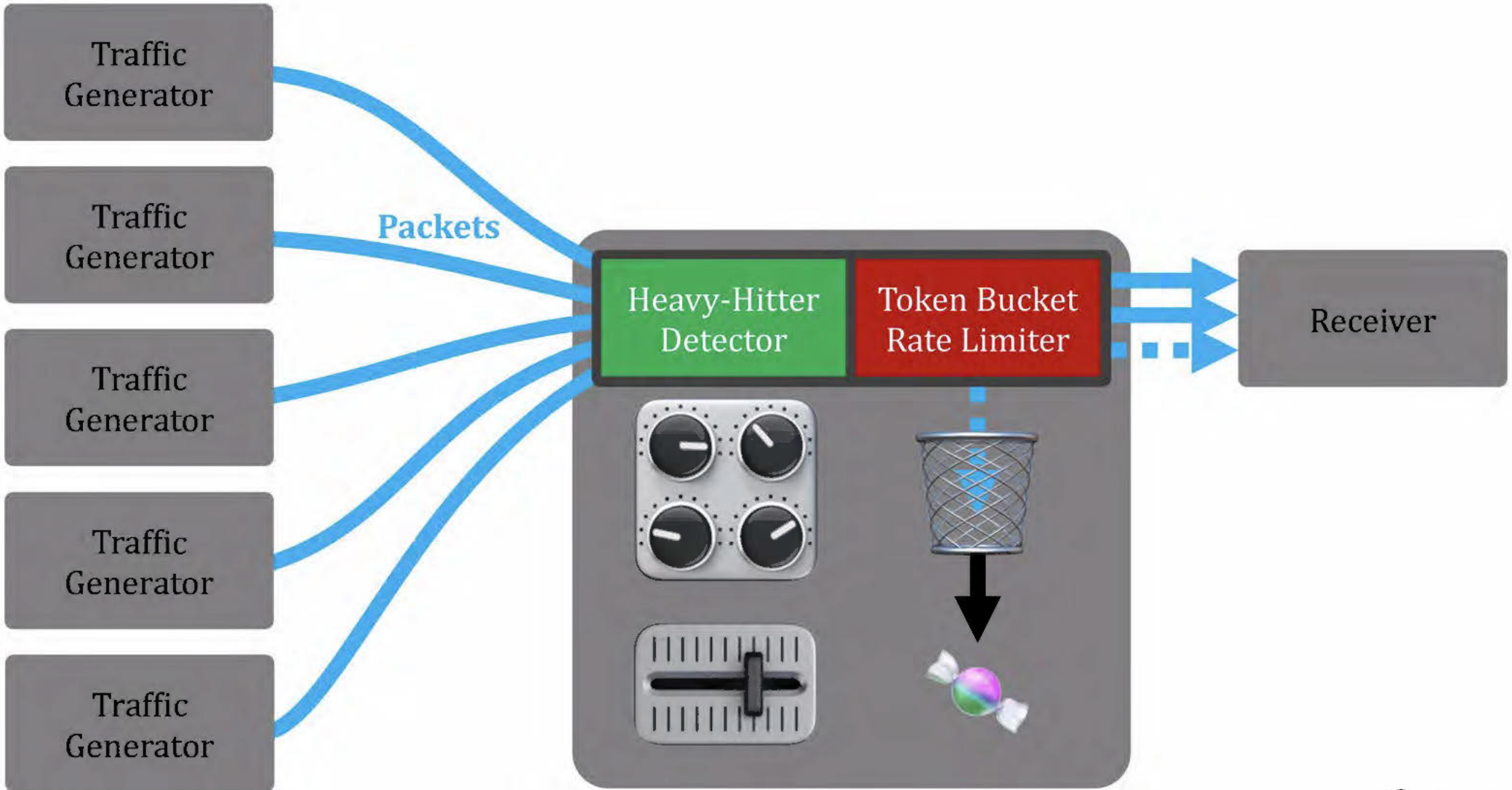
SYSTEM STRUCTURE AND DYNAMICS



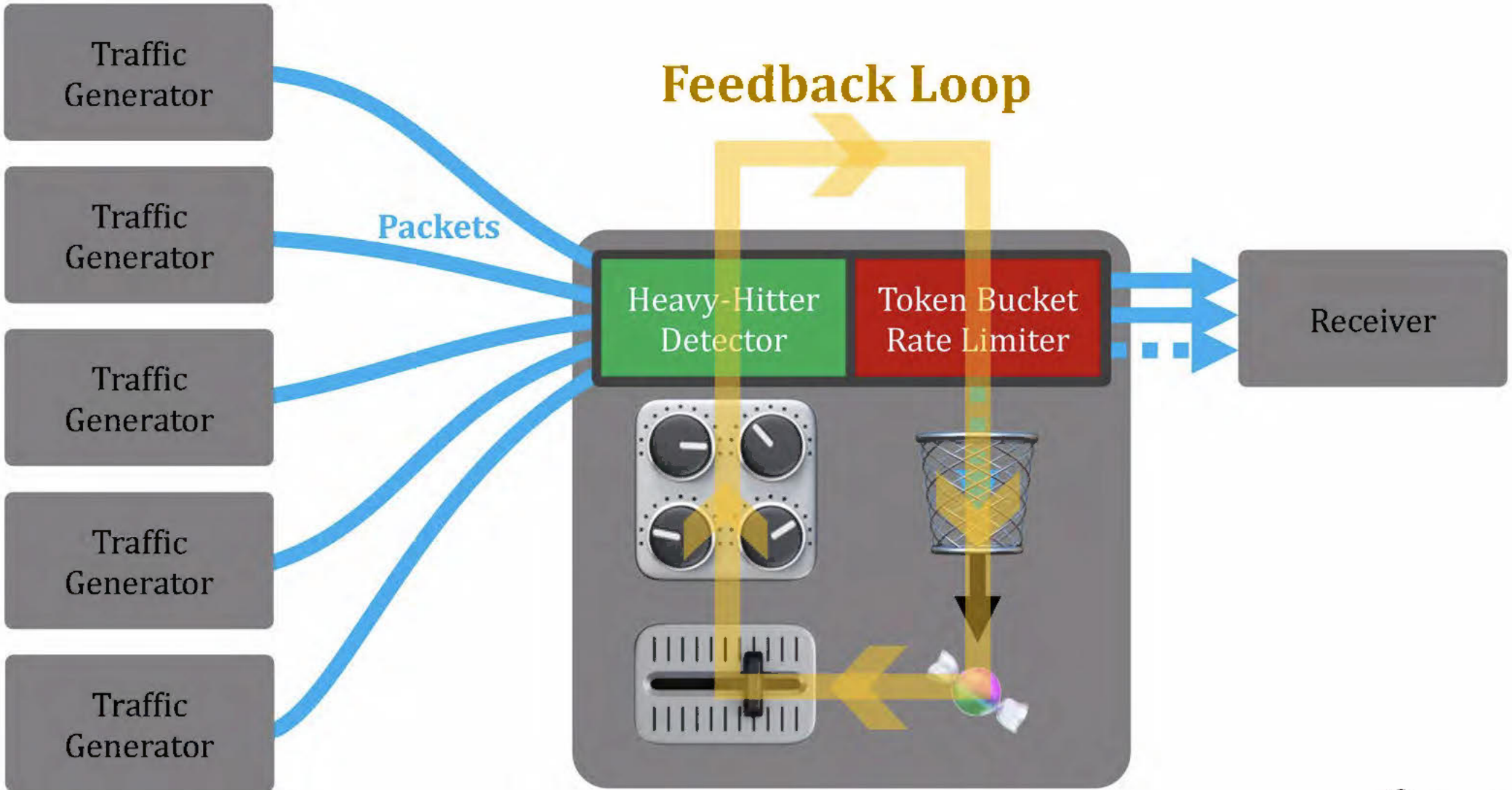
SYSTEM STRUCTURE AND DYNAMICS



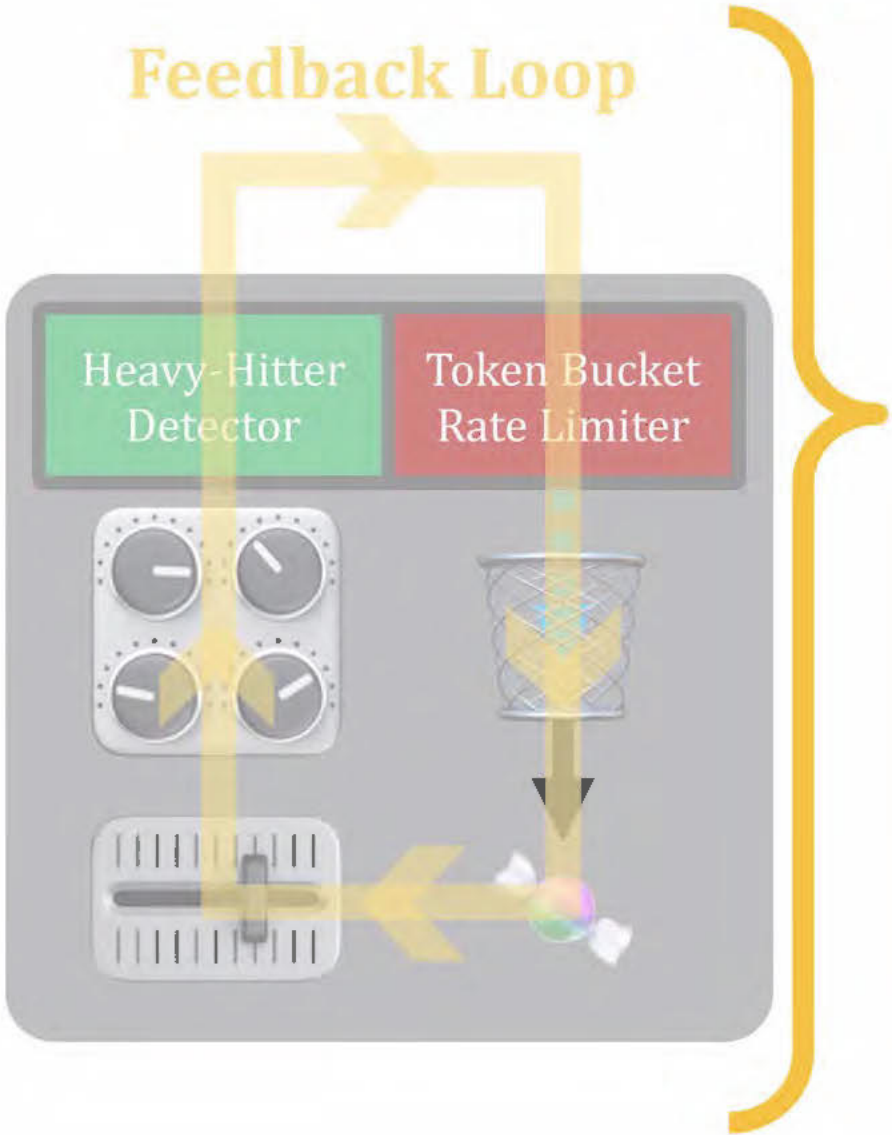
SYSTEM STRUCTURE AND DYNAMICS



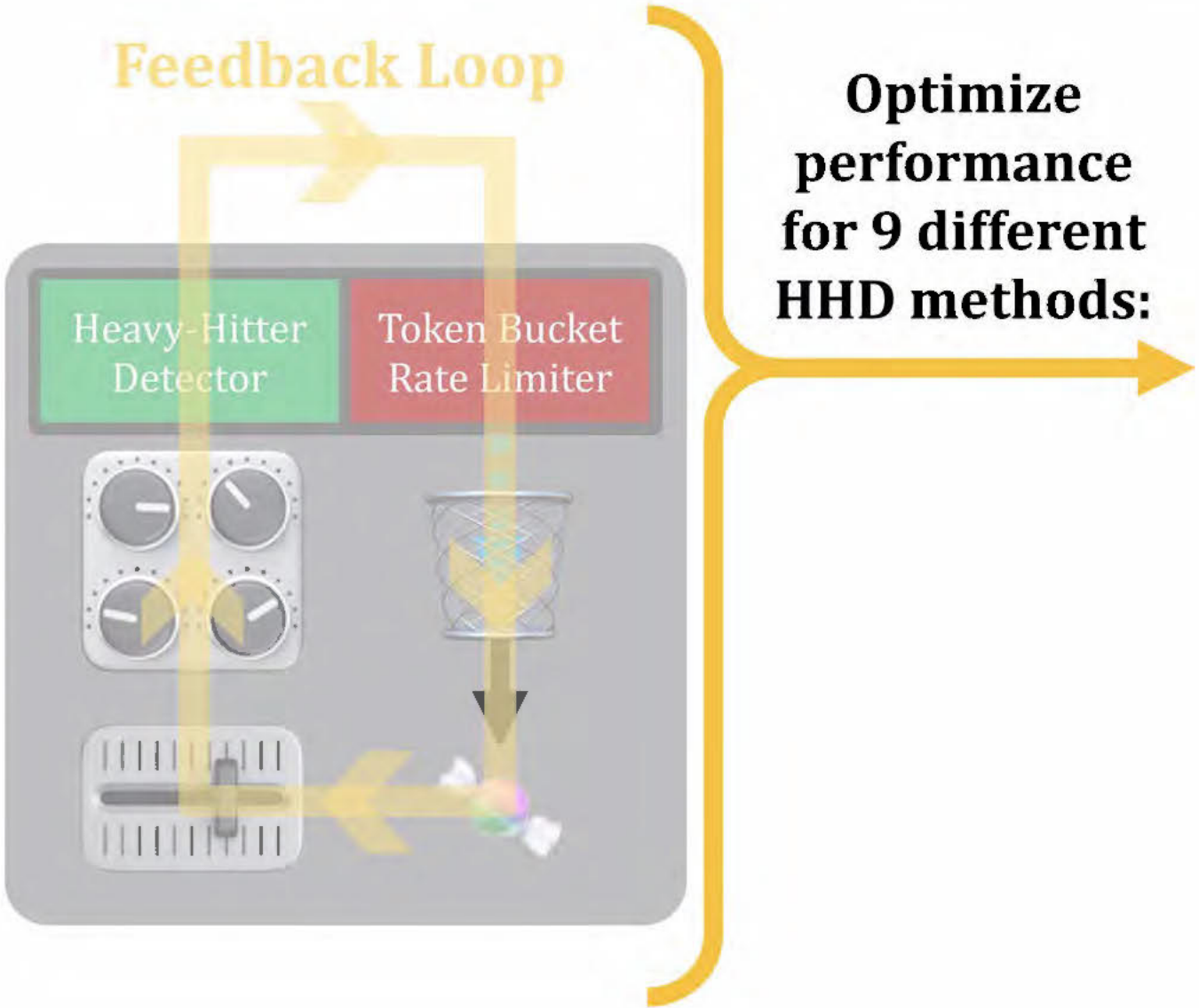
SYSTEM STRUCTURE AND DYNAMICS



TUNING HHD PARAMETERS

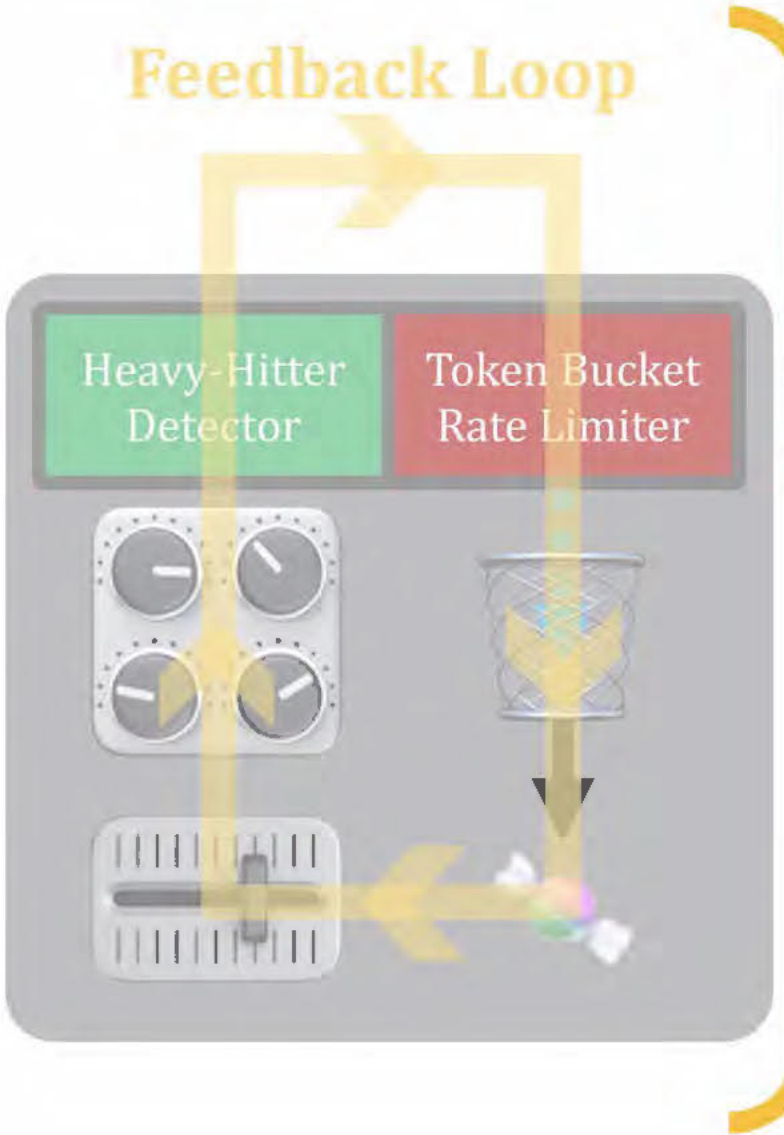


TUNING HHD PARAMETERS

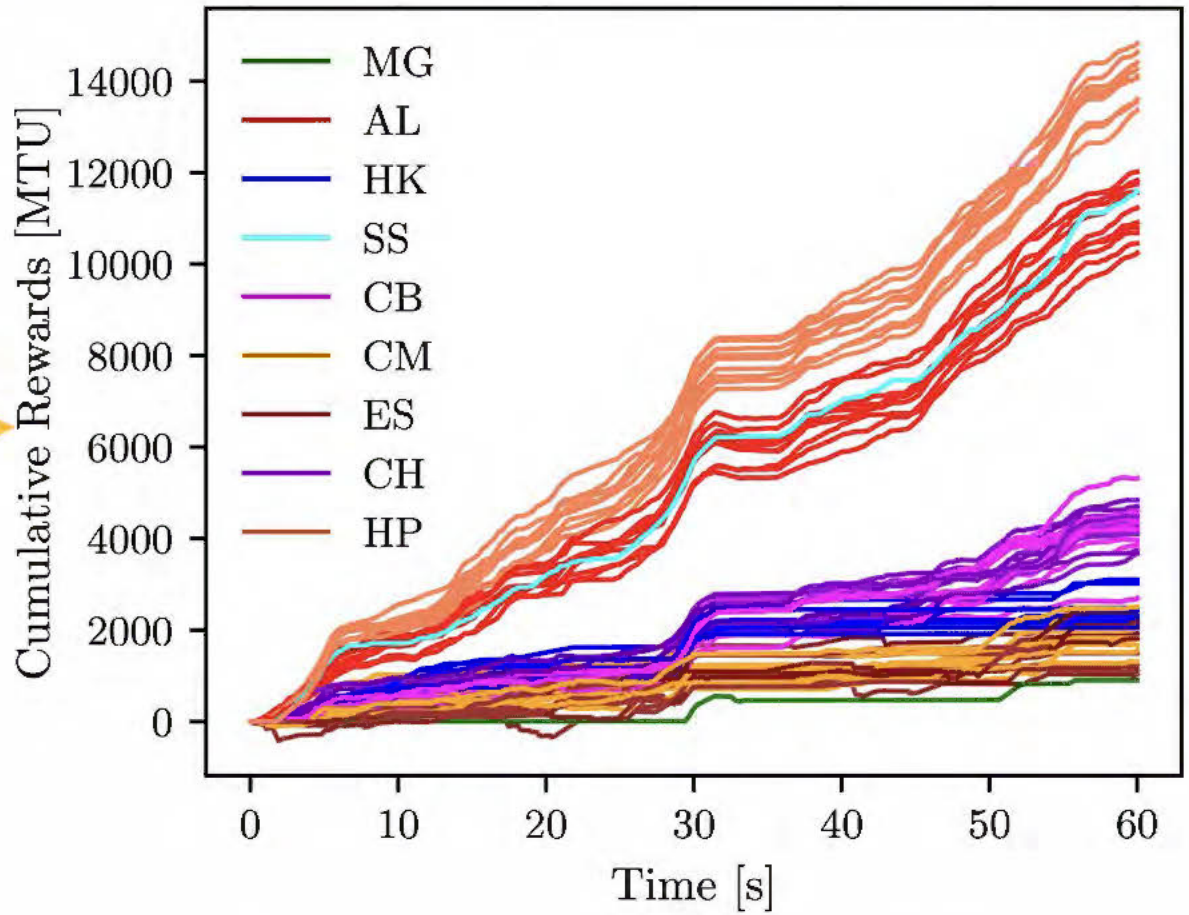


Optimize performance for 9 different HHD methods:

TUNING HHD PARAMETERS

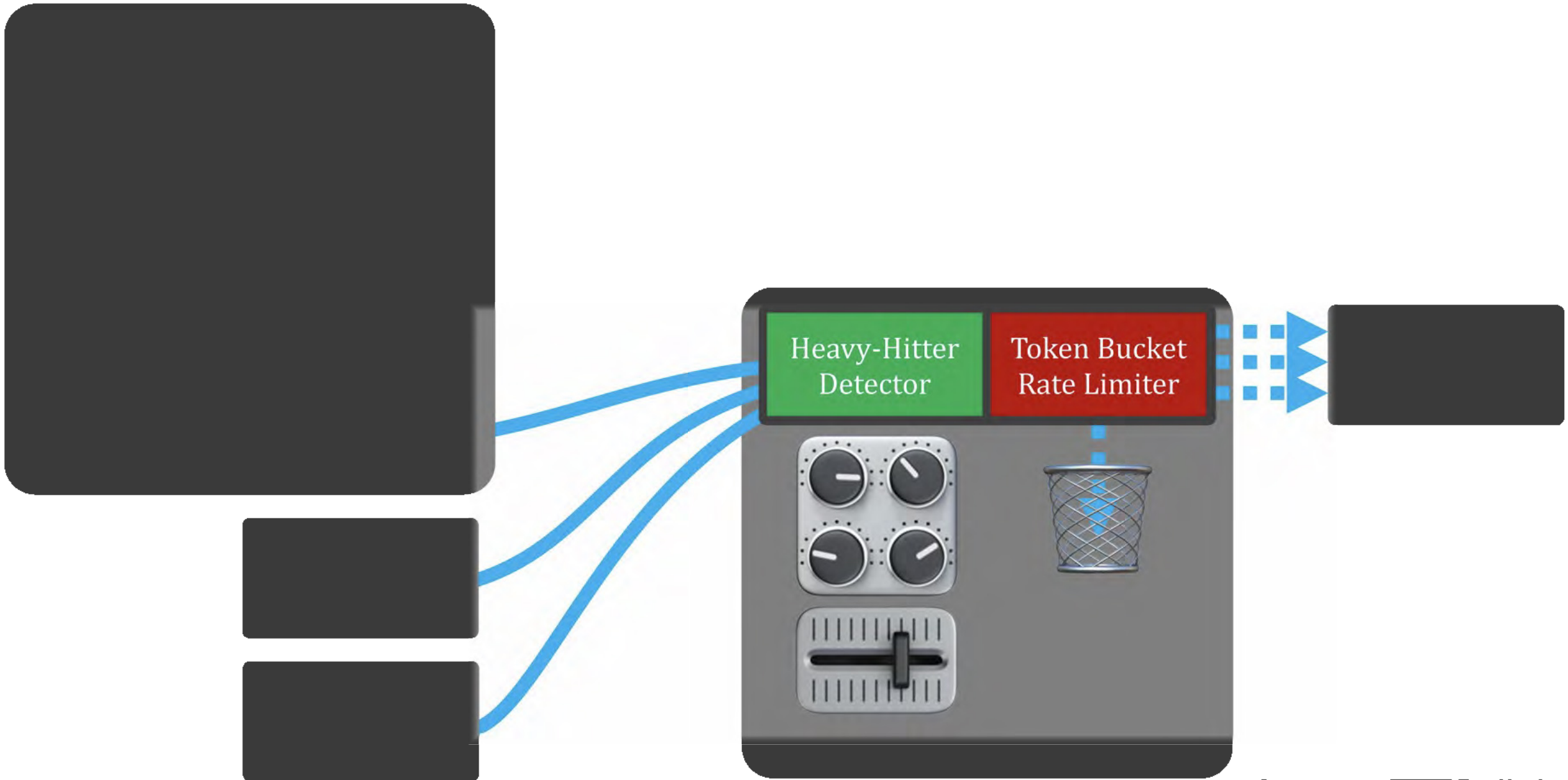


Optimize performance for 9 different HHD methods:

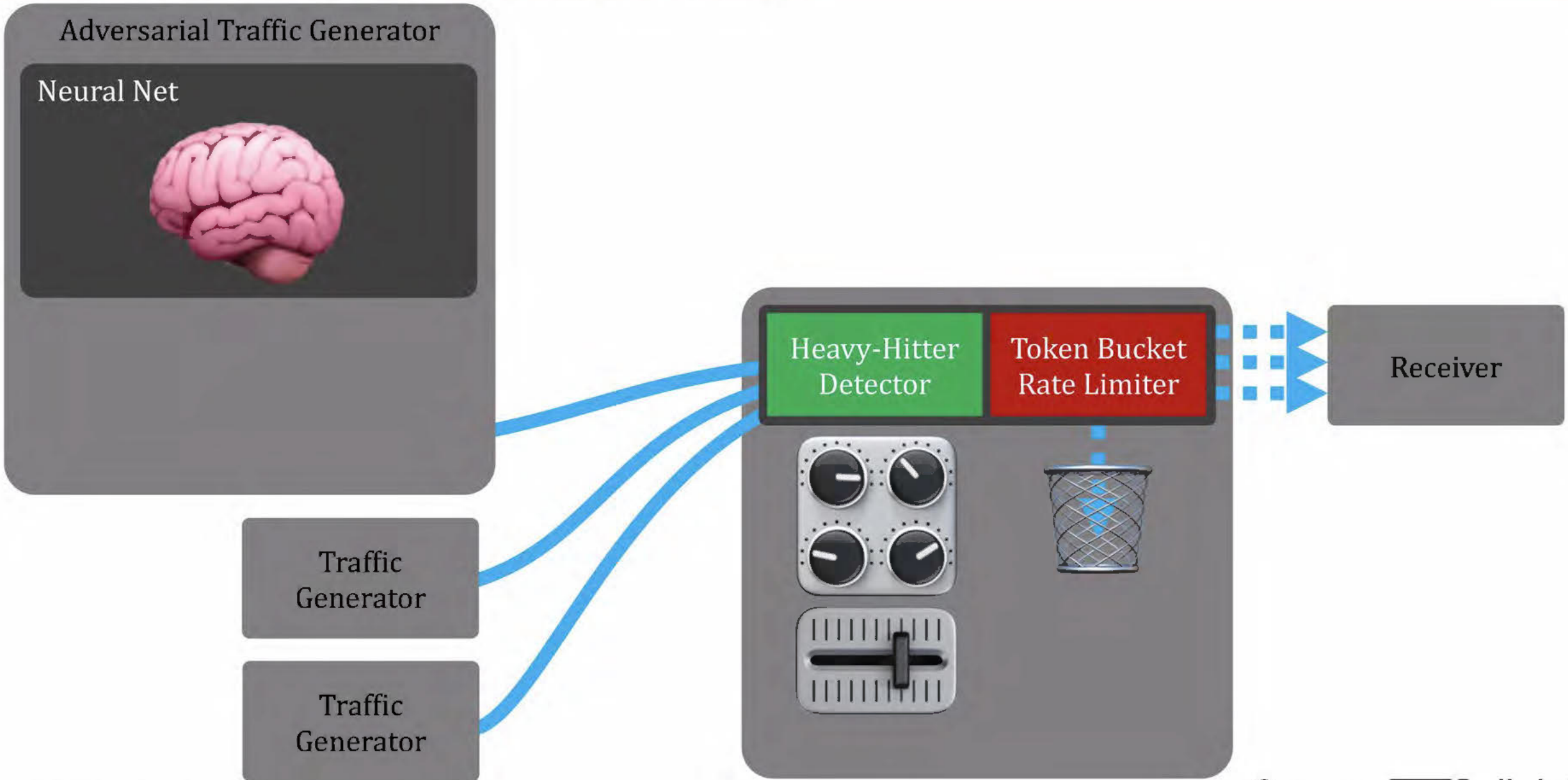


Rewards earned by the HHDs as a function of time

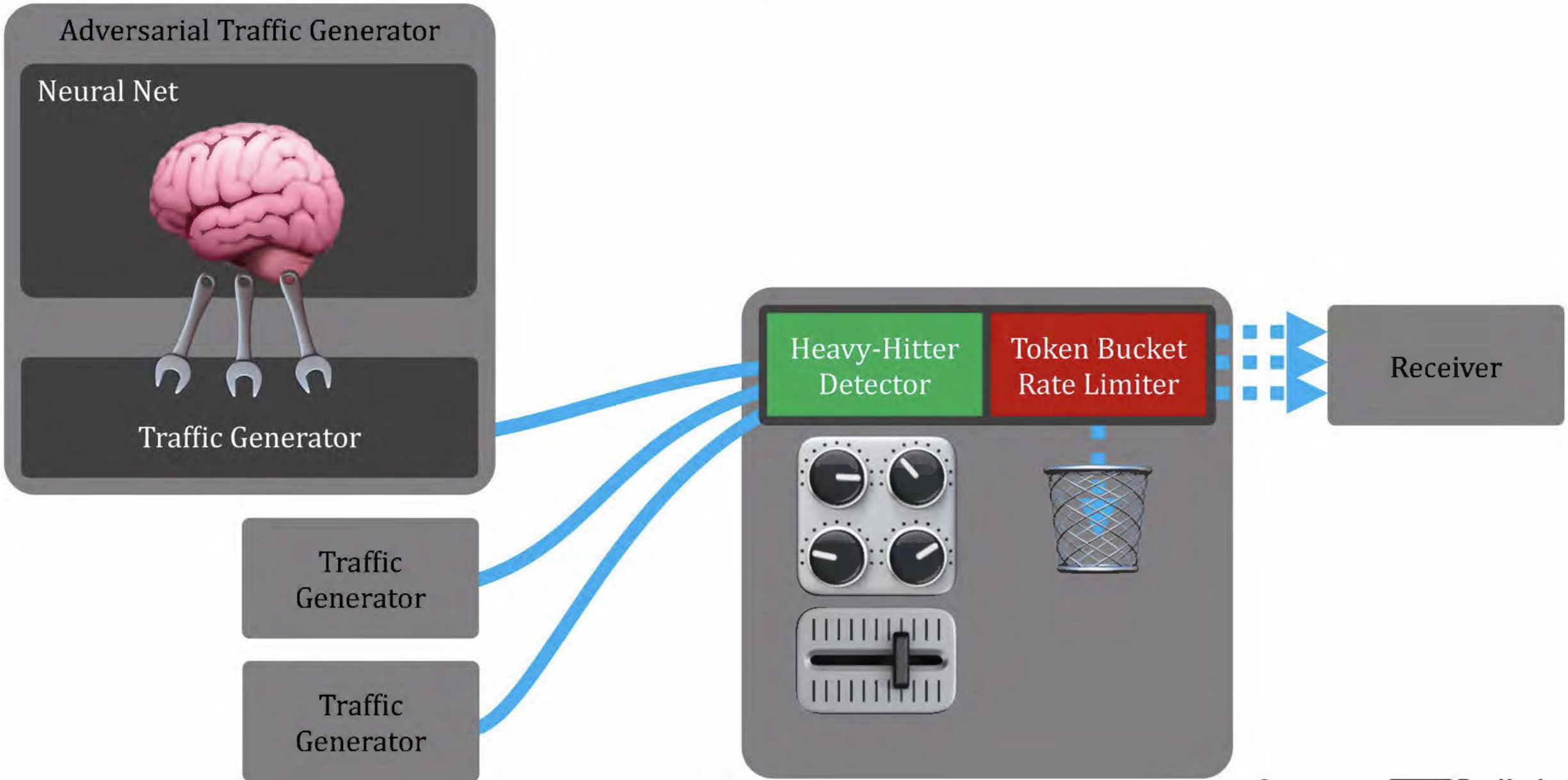
ADVERSARIAL BEHAVIOR



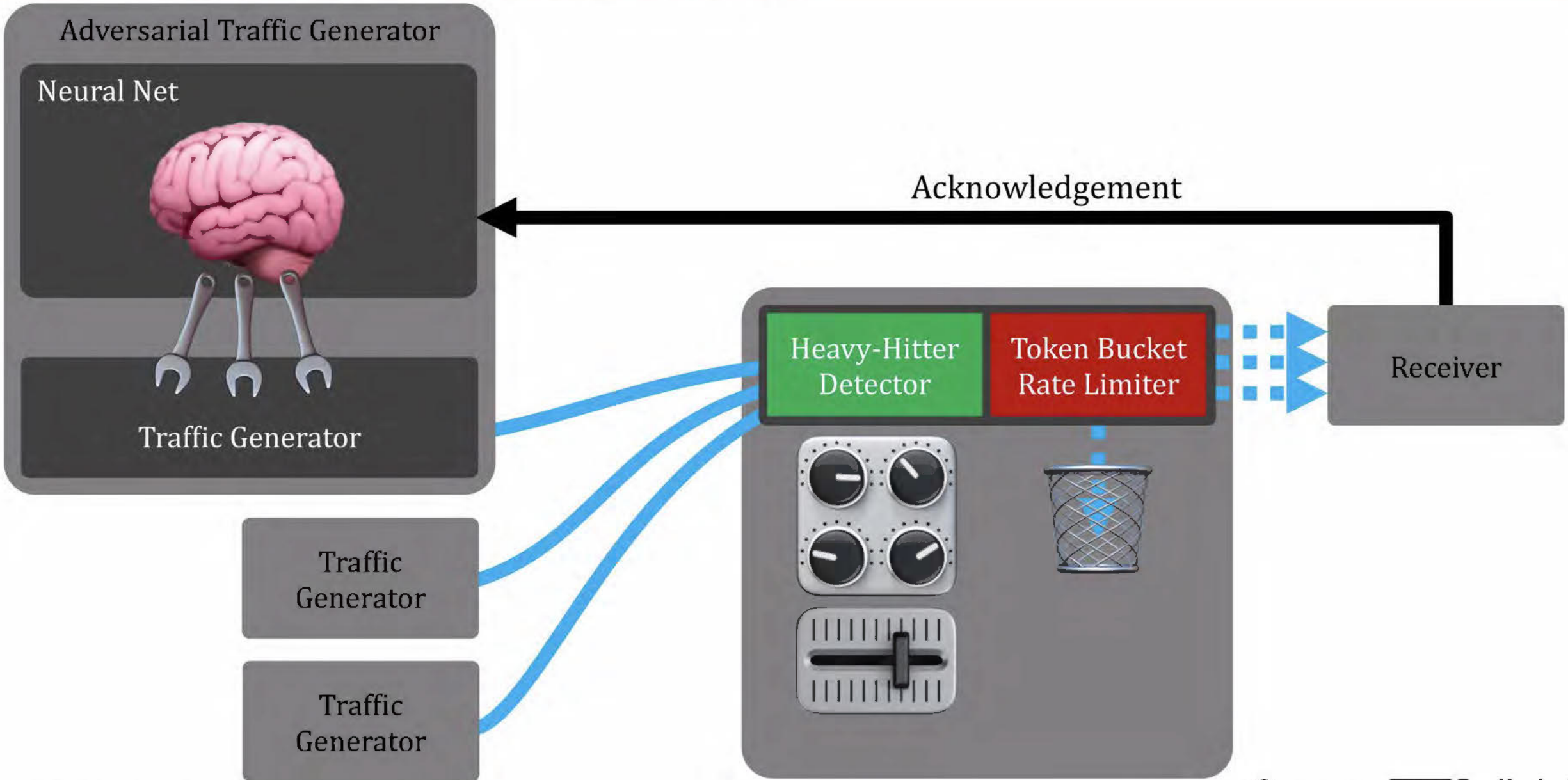
ADVERSARIAL BEHAVIOR



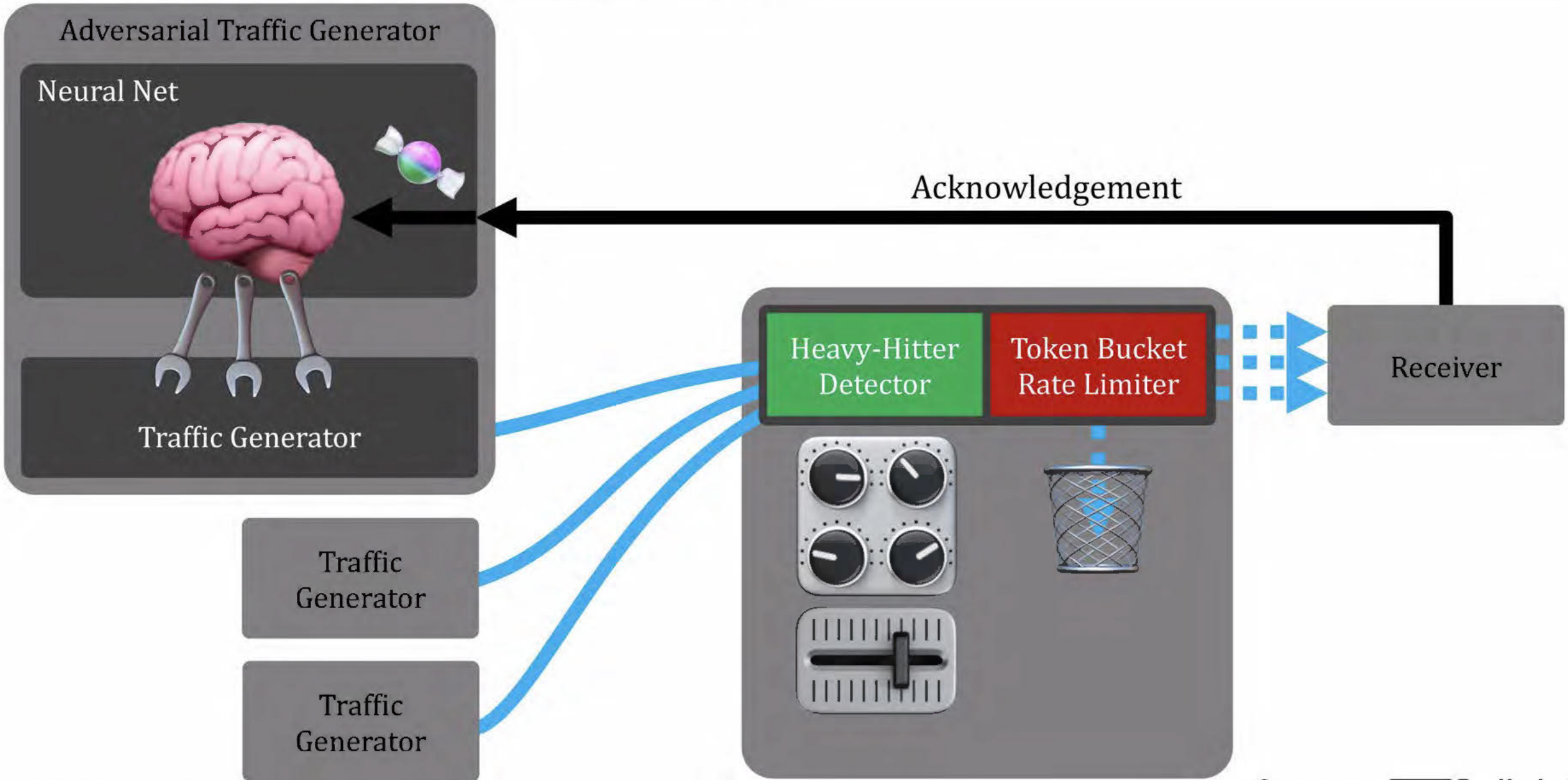
ADVERSARIAL BEHAVIOR



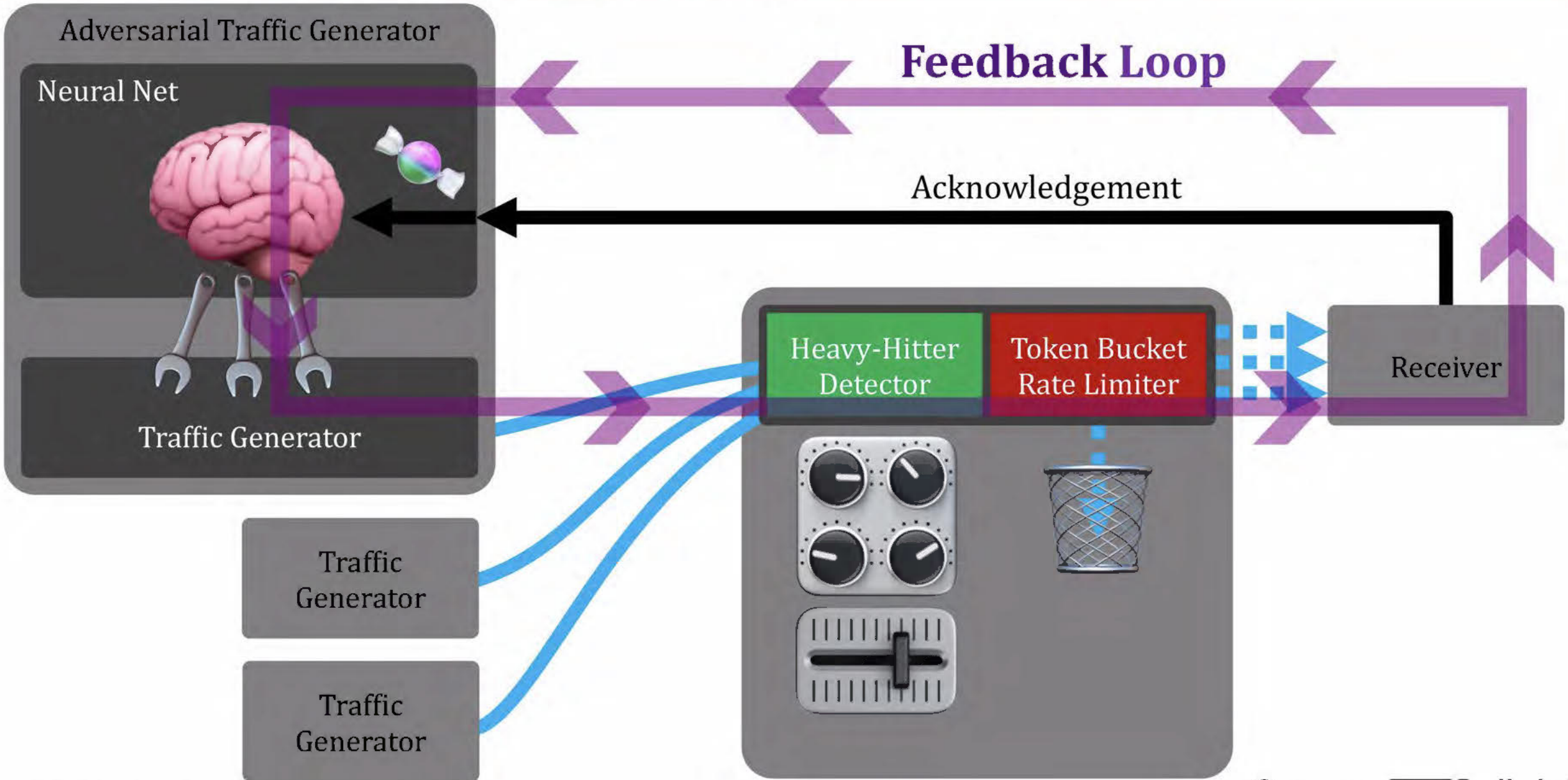
ADVERSARIAL BEHAVIOR



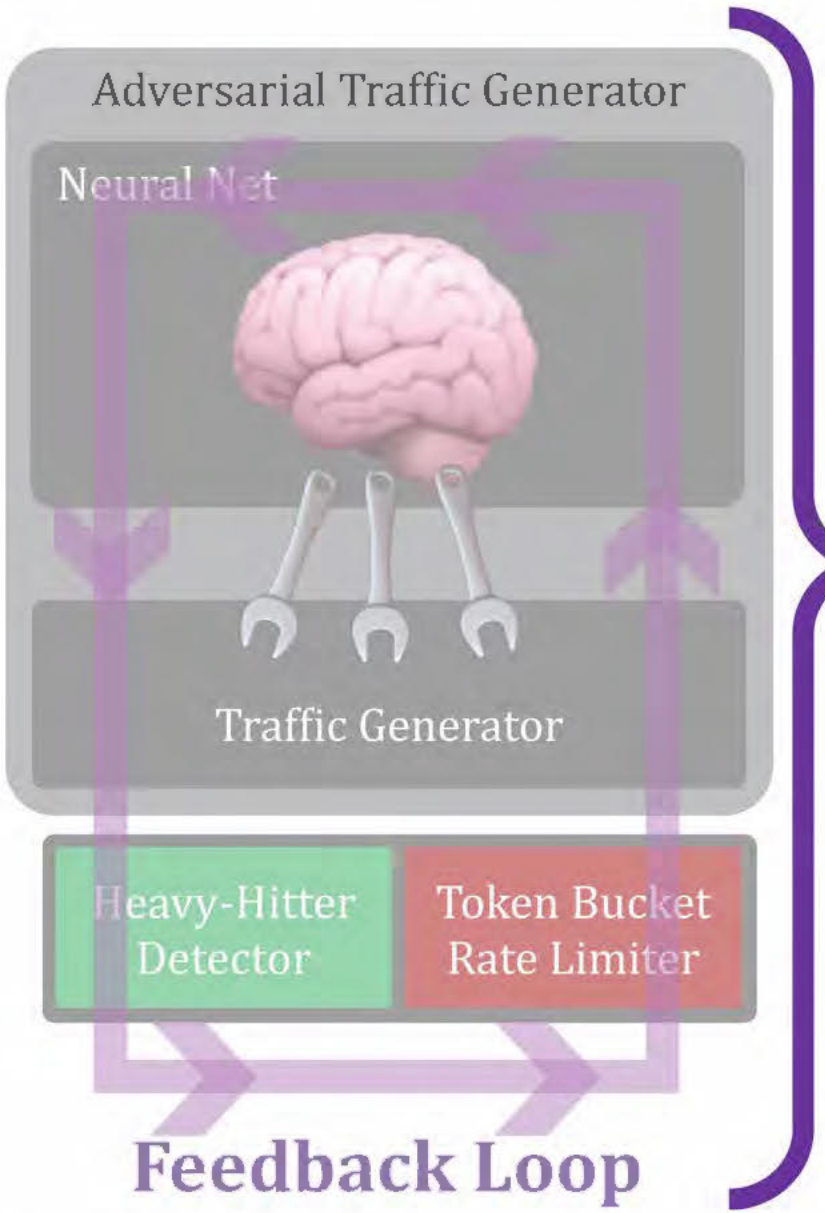
ADVERSARIAL BEHAVIOR



ADVERSARIAL BEHAVIOR

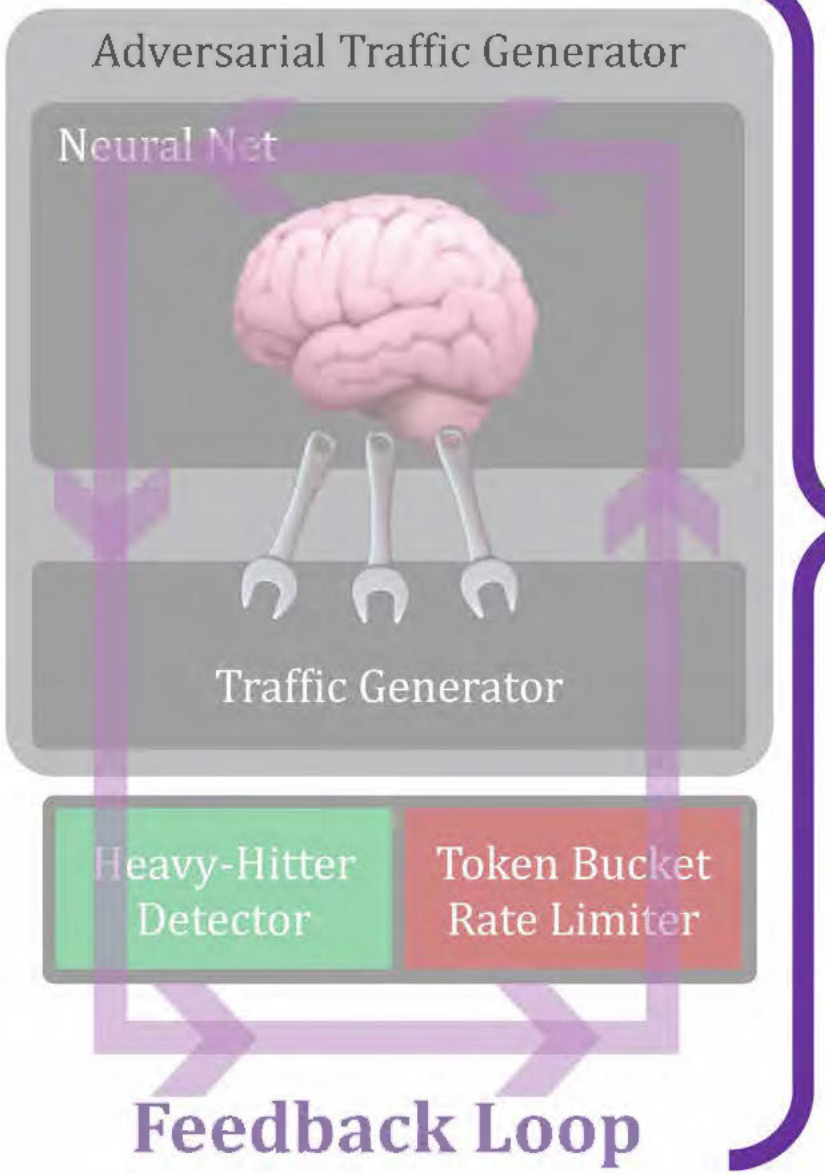


ADVERSARIAL BEHAVIOR



Generate adversarial traffic for each HHD method individually

ADVERSARIAL BEHAVIOR



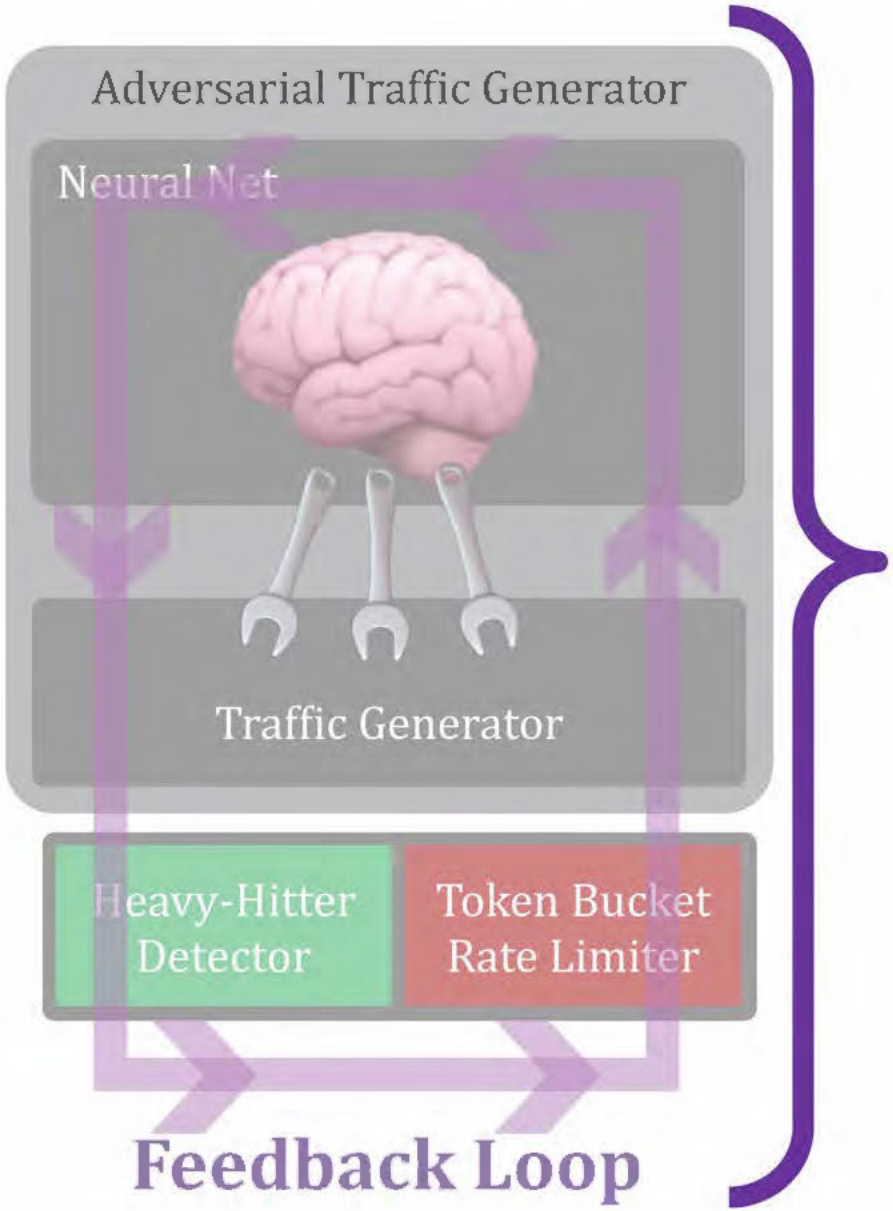
Generate adversarial traffic for each HHD method individually

Evaluated for 9 different heavy-hitter detectors

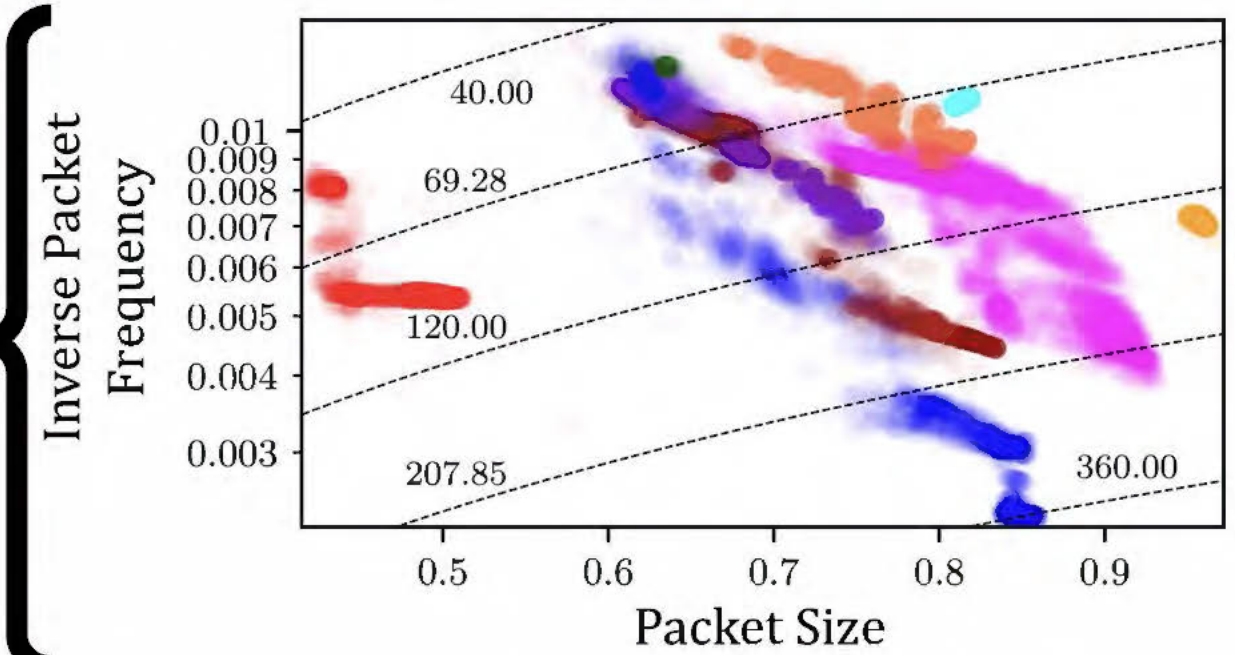
	AL	CB	CM	ES	HK	MG	SS	CH	HP
Synthetic traffic	85%	78%	138%	299%	10%	37%	68%	67%	54%
Captured traffic	90%	185%	326%	670%	-21%	78%	88%	161%	82%

Adversary Overuse

ADVERSARIAL BEHAVIOR



Phase-Space Diagram



Evaluated for 9 different heavy-hitter detectors

	AL	CB	CM	ES	HK	MG	SS	CH	HP
Synthetic traffic	85%	78%	138%	299%	10%	37%	68%	67%	54%
Captured traffic	90%	185%	326%	670%	-21%	78%	88%	161%	82%

Adversary Overuse

LEARN FROM AN ADAPTIVE ADVERSARY

LEARN FROM AN ADAPTIVE ADVERSARY

Problem: HHD algorithm not ready for adaptive adversary…

LEARN FROM AN ADAPTIVE ADVERSARY

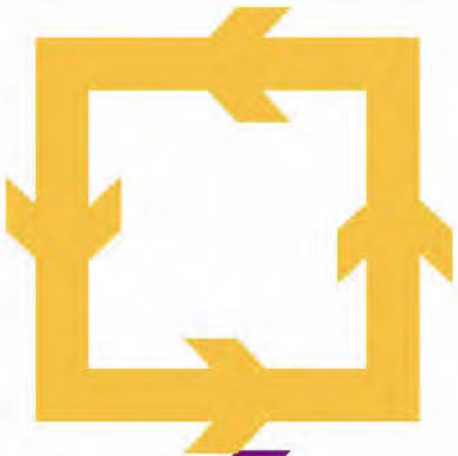
Problem: HHD algorithm not ready for adaptive adversary…

Solution: Let HHD and adversary learn from each other!

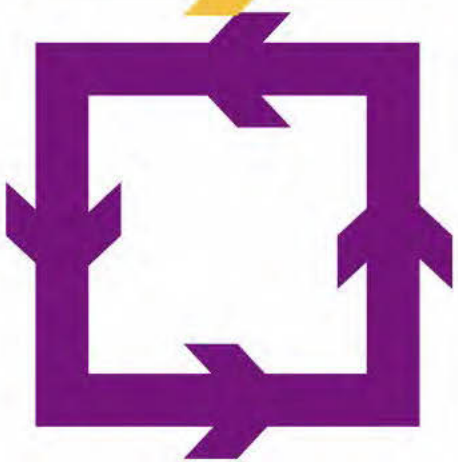
LEARN FROM AN ADAPTIVE ADVERSARY

Problem: HHD algorithm not ready for adaptive adversary…

Solution: Let HHD and adversary learn from each other!



HHD Feedback Loop

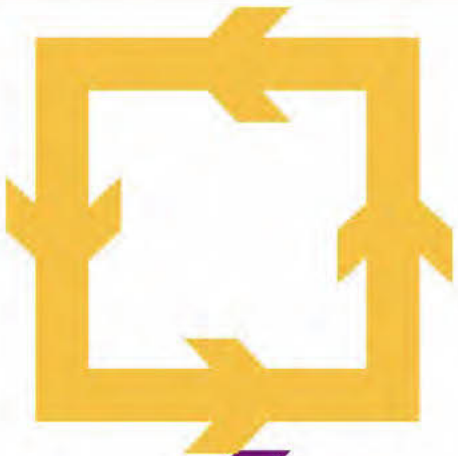


Adversary Feedback Loop

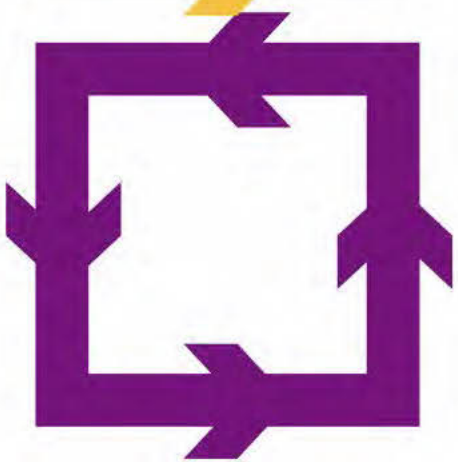
LEARN FROM AN ADAPTIVE ADVERSARY

Problem: HHD algorithm not ready for adaptive adversary…

Solution: Let HHD and adversary learn from each other!



HHD Feedback Loop



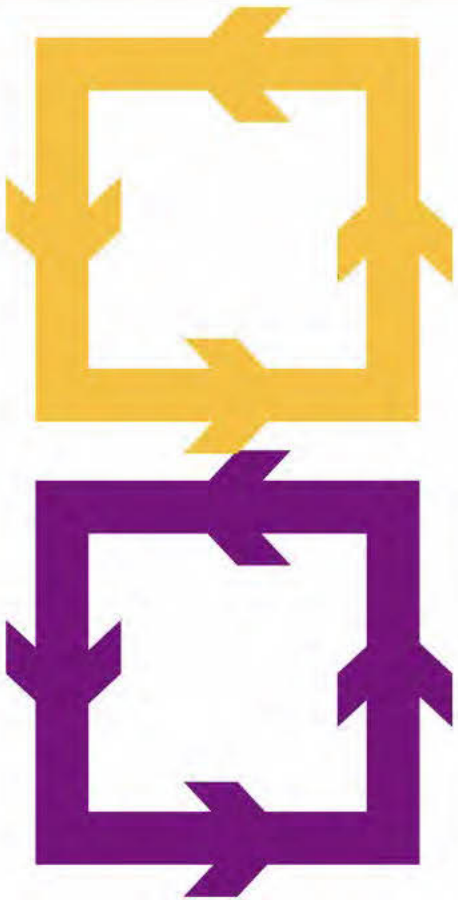
Adversary Feedback Loop

Co-train entities

LEARN FROM AN ADAPTIVE ADVERSARY

Problem: HHD algorithm not ready for adaptive adversary…

Solution: Let HHD and adversary learn from each other!



HHD Feedback Loop

Adversary Feedback Loop

Co-train entities

Each learns to exploit the other's weakness

LEARN FROM AN ADAPTIVE ADVERSARY

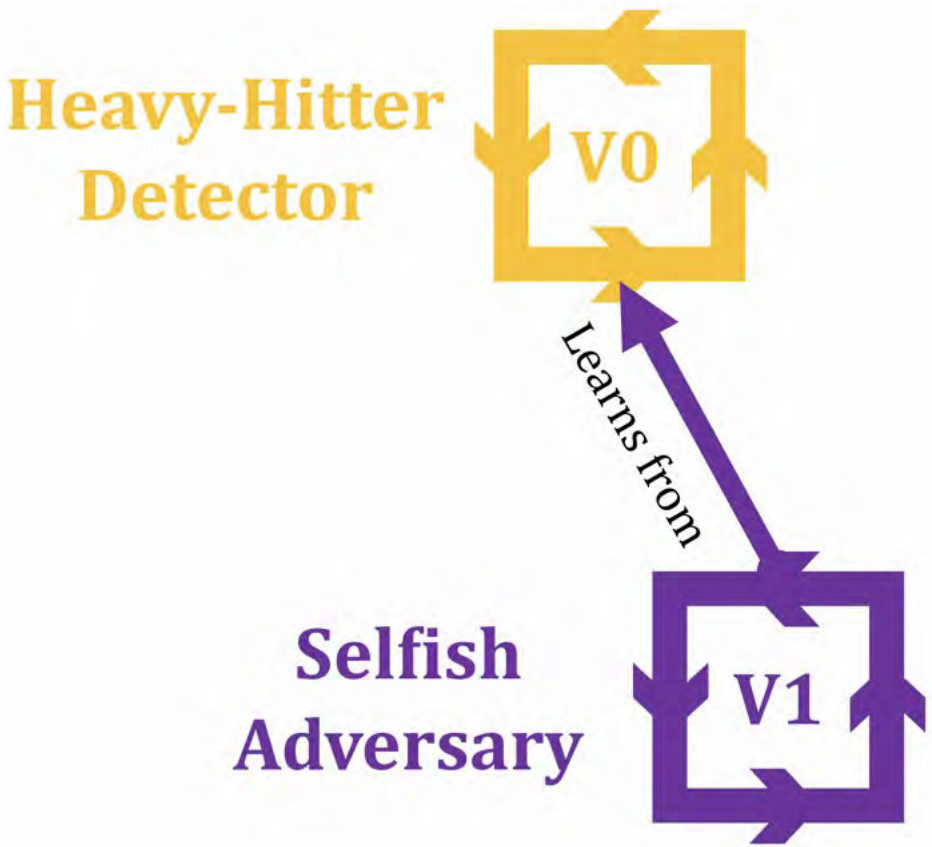
Problem: HHD algorithm not ready for adaptive adversary…

Solution: Let HHD and adversary learn from each other!

LEARN FROM AN ADAPTIVE ADVERSARY

Problem: HHD algorithm not ready for adaptive adversary…

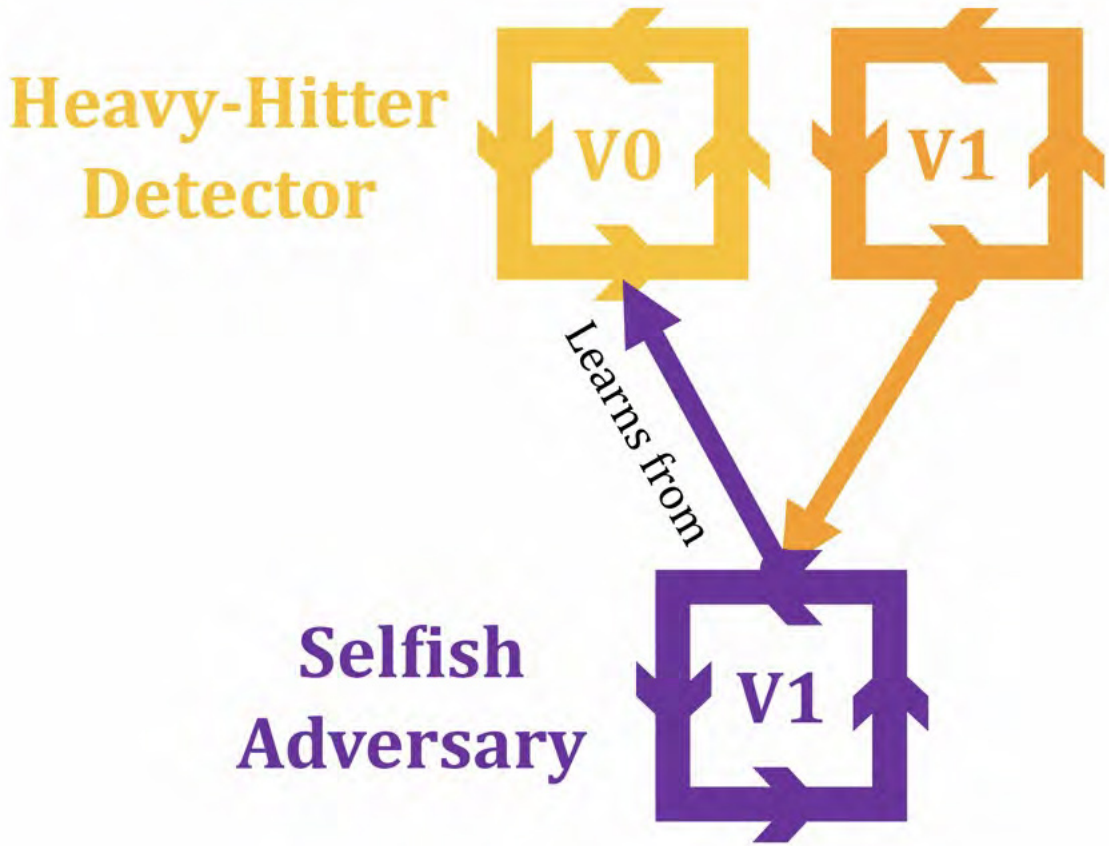
Solution: Let HHD and adversary learn from each other!



LEARN FROM AN ADAPTIVE ADVERSARY

Problem: HHD algorithm not ready for adaptive adversary…

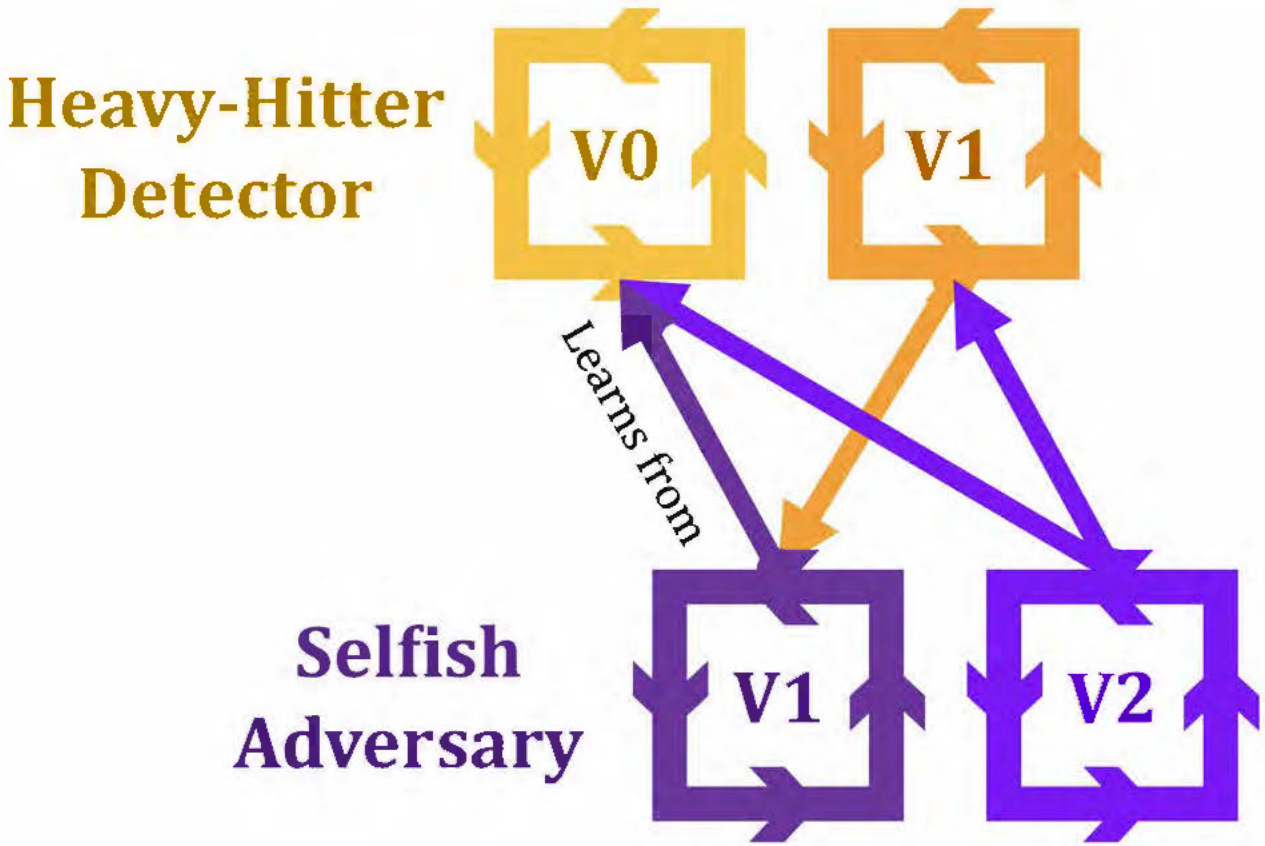
Solution: Let HHD and adversary learn from each other!



LEARN FROM AN ADAPTIVE ADVERSARY

Problem: HHD algorithm not ready for adaptive adversary…

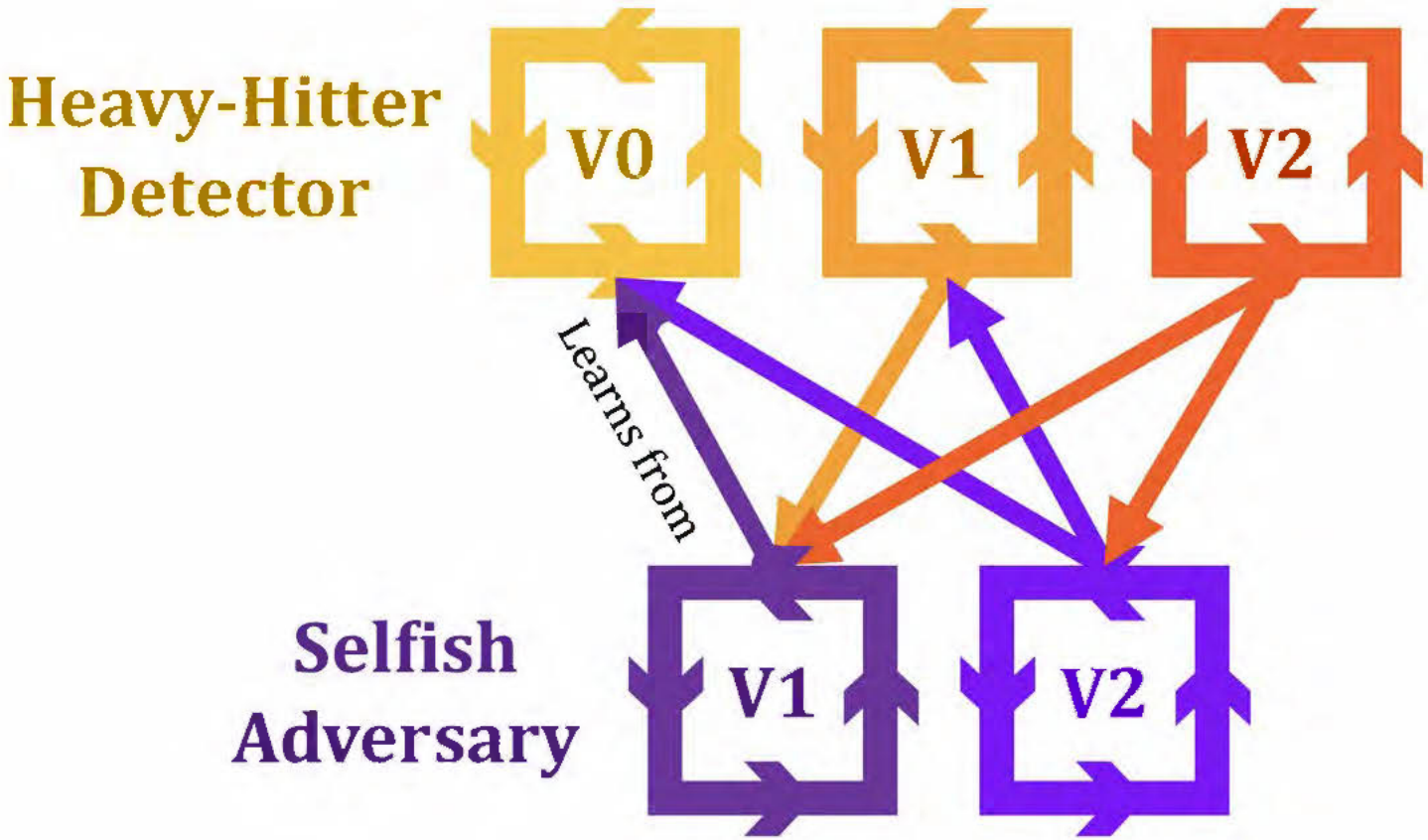
Solution: Let HHD and adversary learn from each other!



LEARN FROM AN ADAPTIVE ADVERSARY

Problem: HHD algorithm not ready for adaptive adversary…

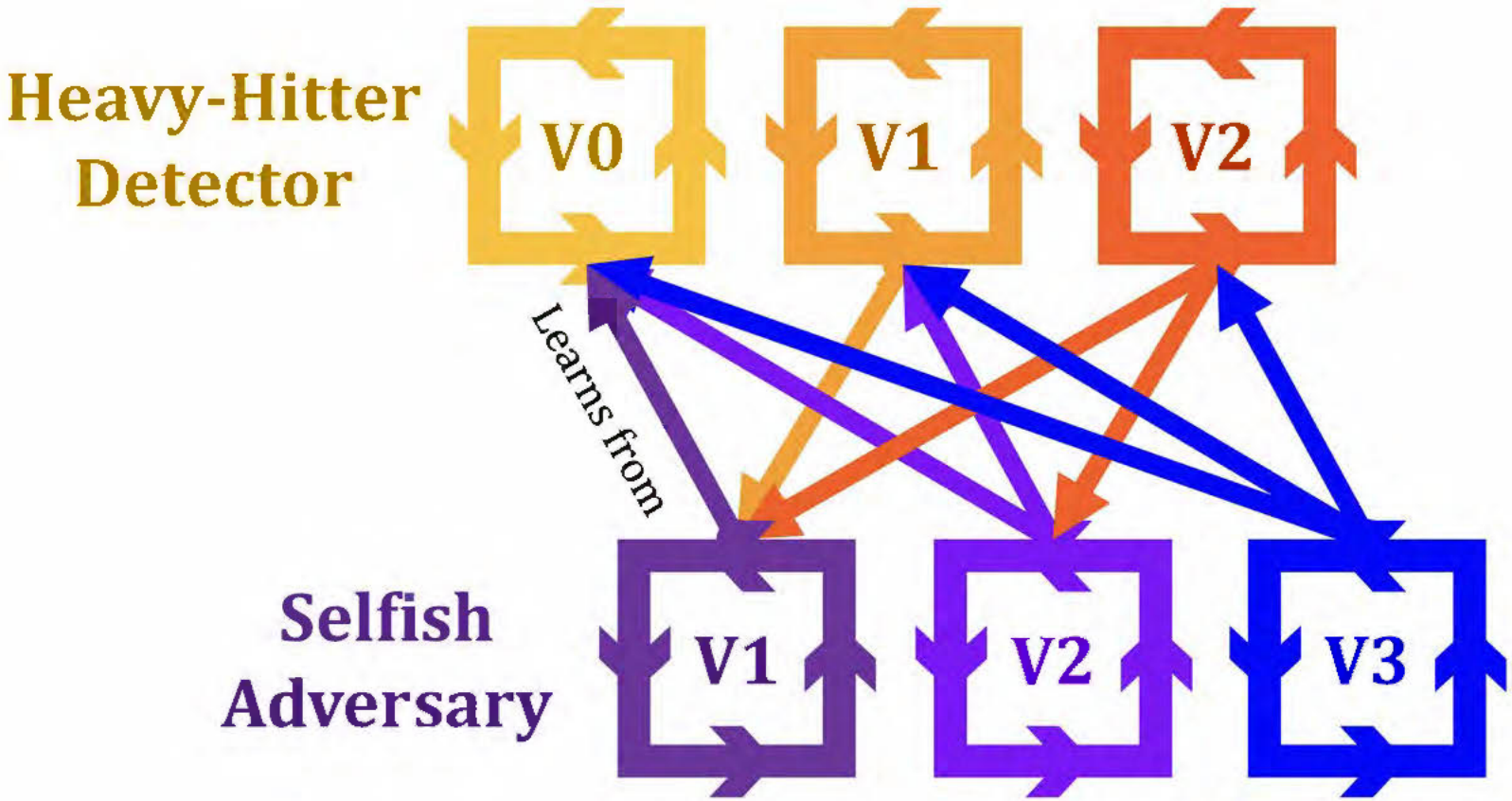
Solution: Let HHD and adversary learn from each other!



LEARN FROM AN ADAPTIVE ADVERSARY

Problem: HHD algorithm not ready for adaptive adversary…

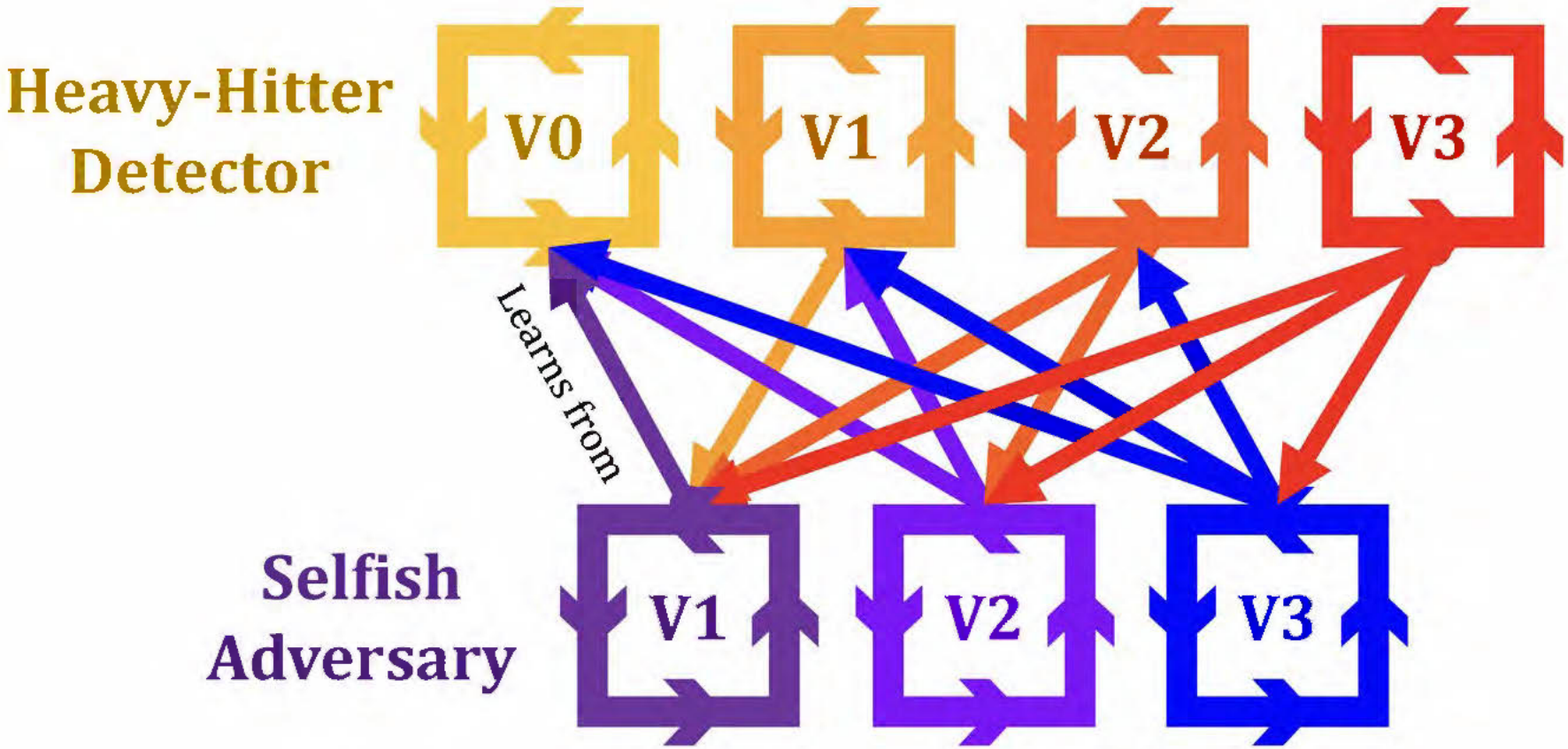
Solution: Let HHD and adversary learn from each other!



LEARN FROM AN ADAPTIVE ADVERSARY

Problem: HHD algorithm not ready for adaptive adversary…

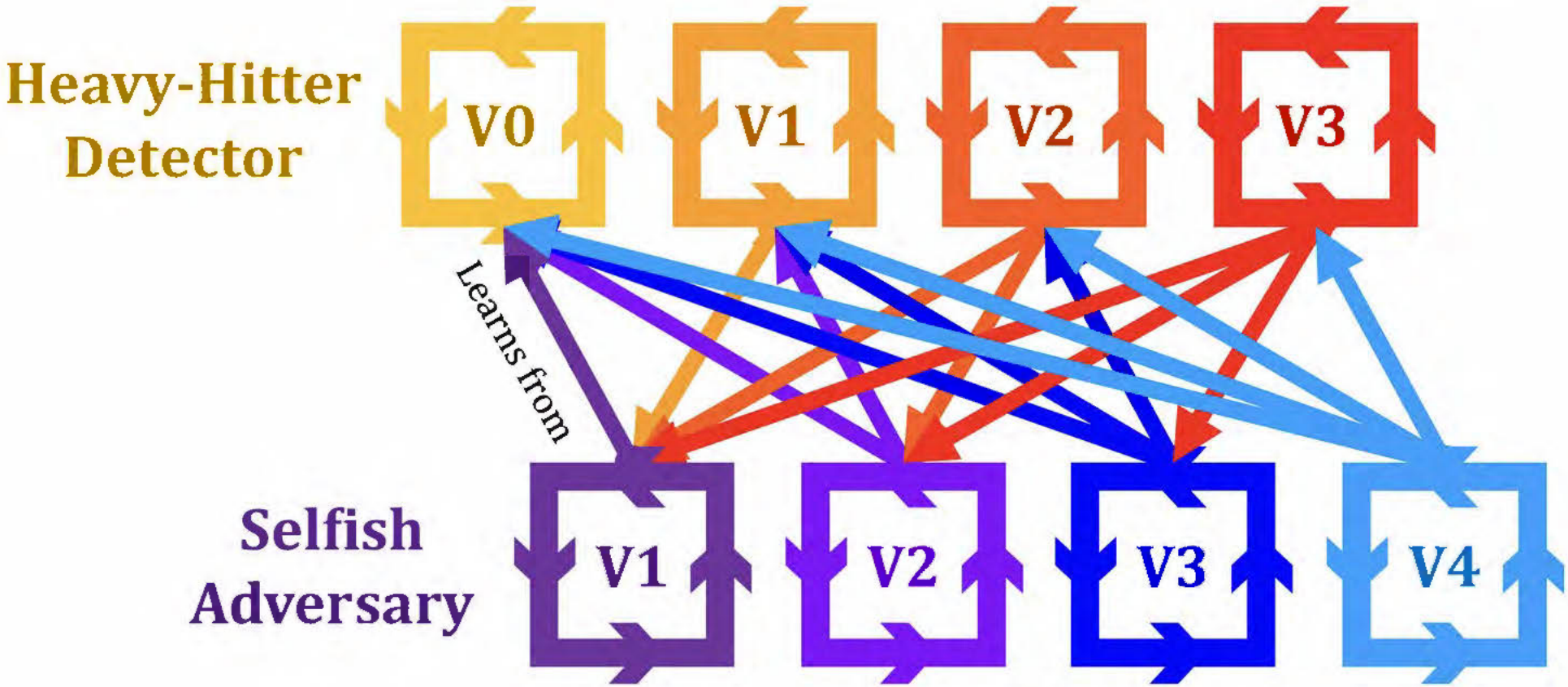
Solution: Let HHD and adversary learn from each other!



LEARN FROM AN ADAPTIVE ADVERSARY

Problem: HHD algorithm not ready for adaptive adversary…

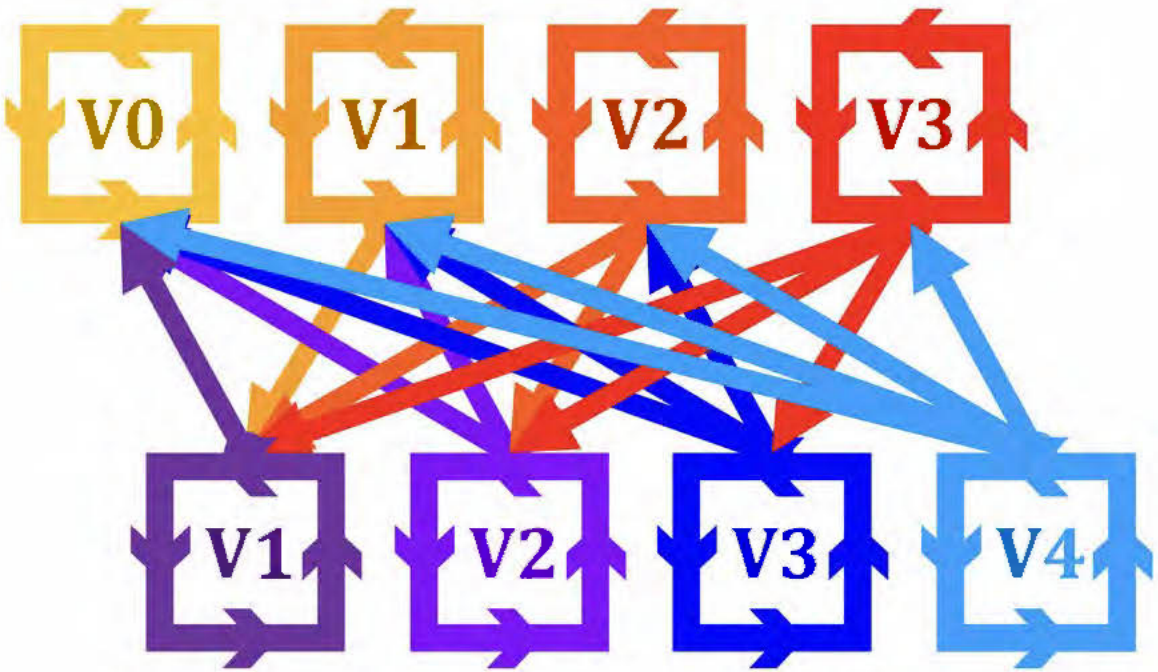
Solution: Let HHD and adversary learn from each other!



LEARN FROM AN ADAPTIVE ADVERSARY

Problem: HHD algorithm not ready for adaptive adversary…

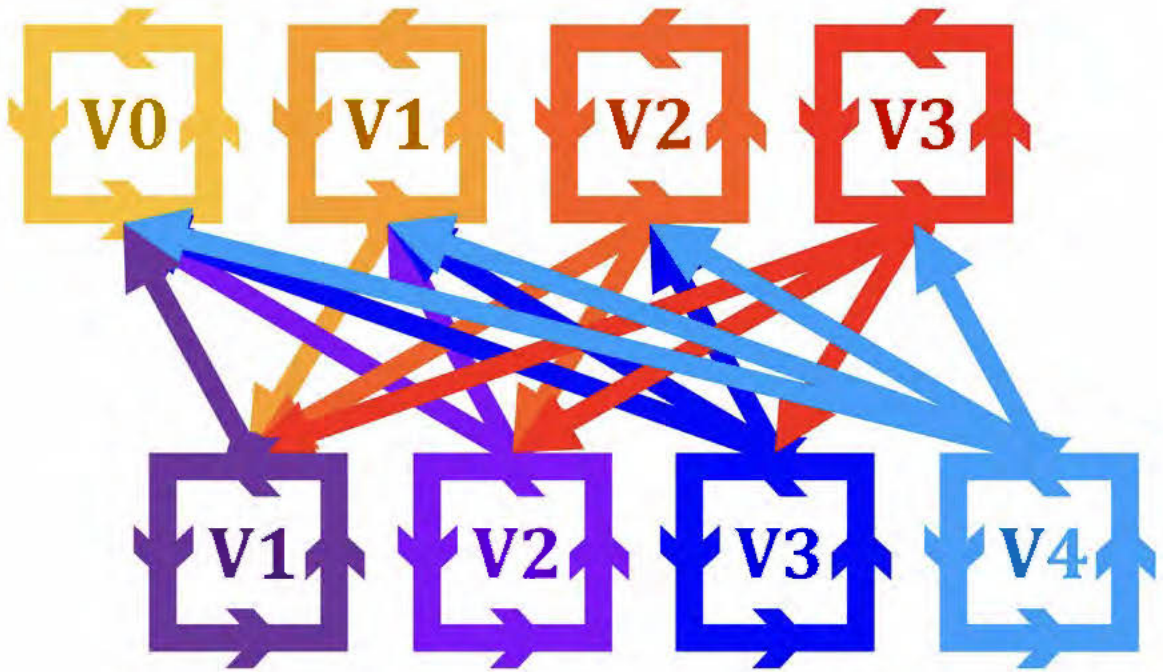
Solution: Let HHD and adversary learn from each other!



LEARN FROM AN ADAPTIVE ADVERSARY

Problem: HHD algorithm not ready for adaptive adversary…

Solution: Let HHD and adversary learn from each other!



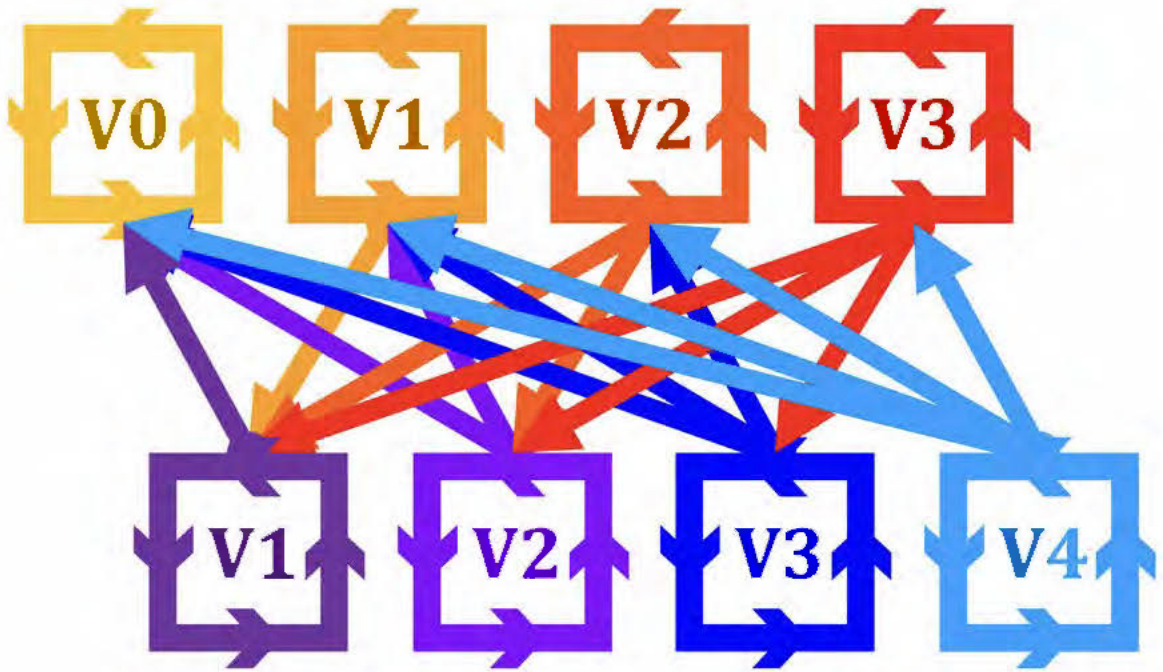
Example results (HHD = Elastic-Sketch):

Before co-training: 300% adversary overuse.

LEARN FROM AN ADAPTIVE ADVERSARY

Problem: HHD algorithm not ready for adaptive adversary…

Solution: Let HHD and adversary learn from each other!



Example results (HHD = Elastic-Sketch):

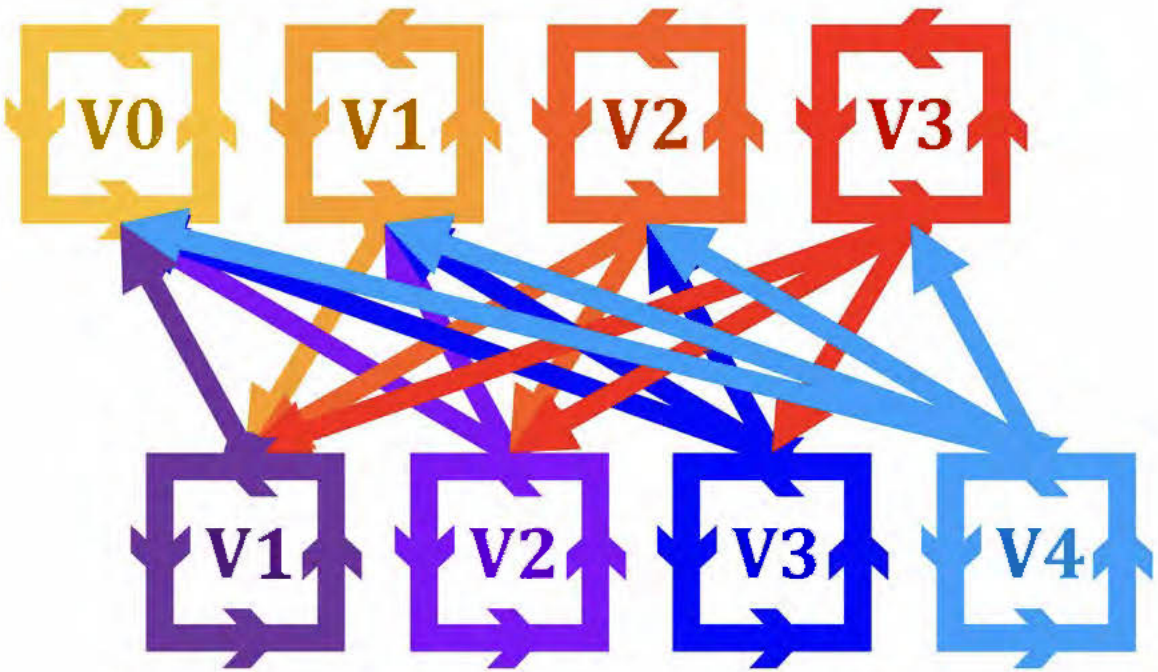
Before co-training: 300% adversary overuse.

After co-training: 139% adversary overuse.

LEARN FROM AN ADAPTIVE ADVERSARY

Problem: HHD algorithm not ready for adaptive adversary…

Solution: Let HHD and adversary learn from each other!



Example results (HHD = Elastic-Sketch):

Before co-training: 300% adversary overuse.

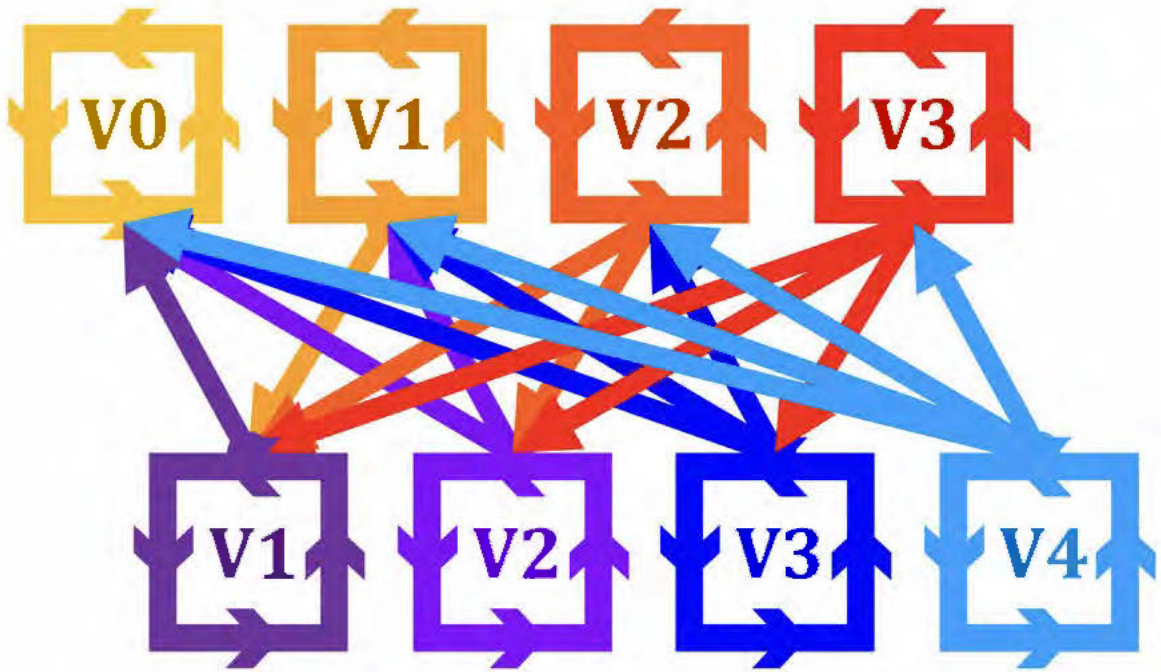
After co-training: 139% adversary overuse.

Reduction by x2.2 “for free”.

LEARN FROM AN ADAPTIVE ADVERSARY

Problem: HHD algorithm not ready for adaptive adversary…

Solution: Let HHD and adversary learn from each other!



Example results (HHD = Elastic-Sketch):

Before co-training: 300% adversary overuse.

After co-training: 139% adversary overuse.

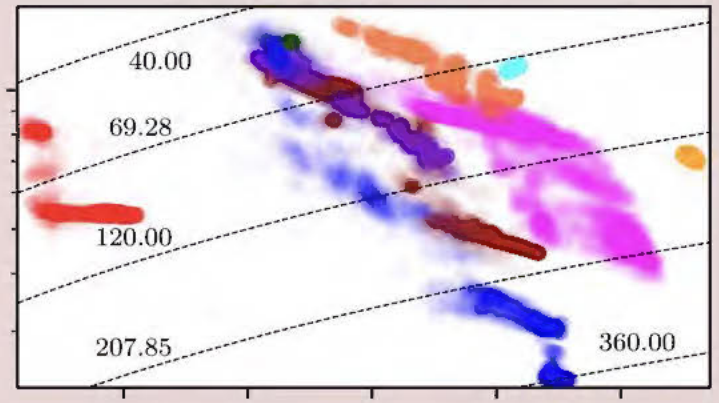
Reduction by x2.2 “for free”.

HHD score increased by x1.6 “for free”.

WHERE WE STAND

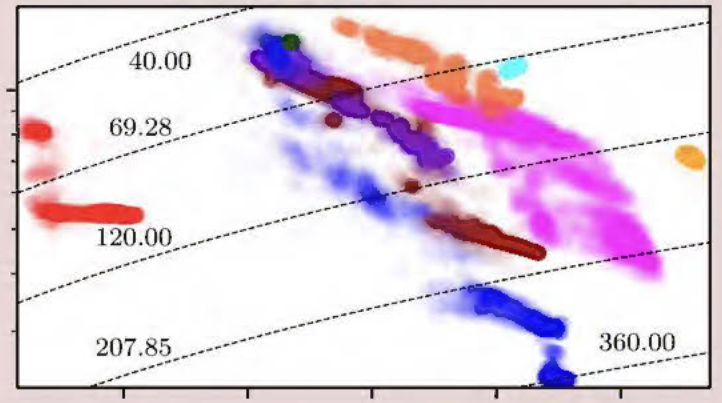
WHERE WE STAND

1) Shown that **adversaries can adapt** to monitoring systems.

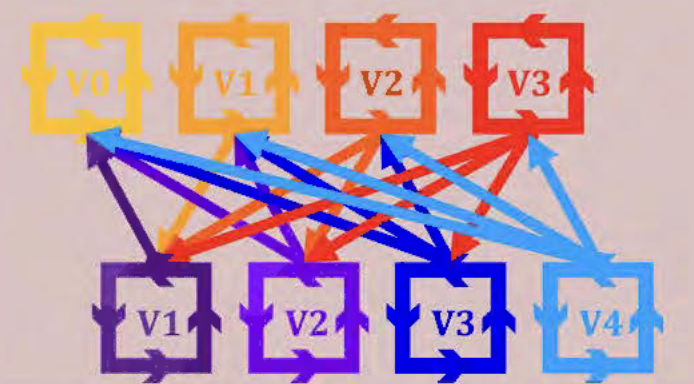


WHERE WE STAND

1) Shown that **adversaries can adapt** to monitoring systems.

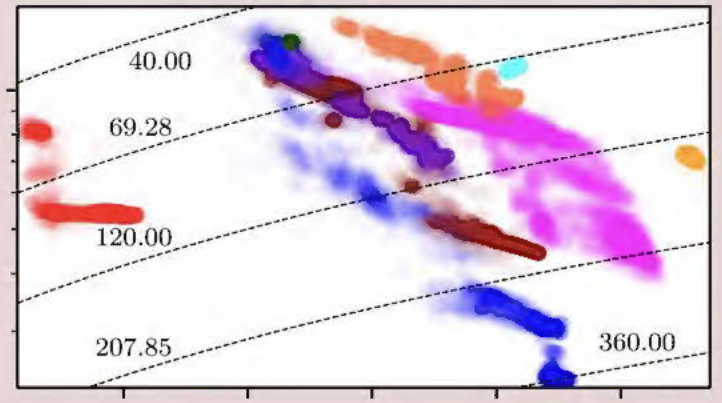


2) Shown that we can **prepare monitors** to **deal with any adversary**.

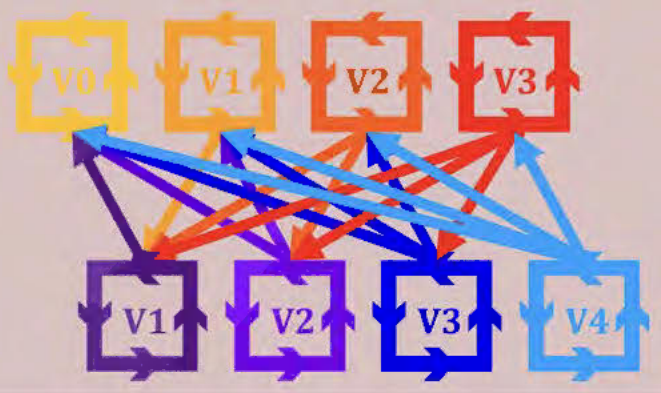


WHERE WE STAND

1) Shown that **adversaries can adapt** to monitoring systems.



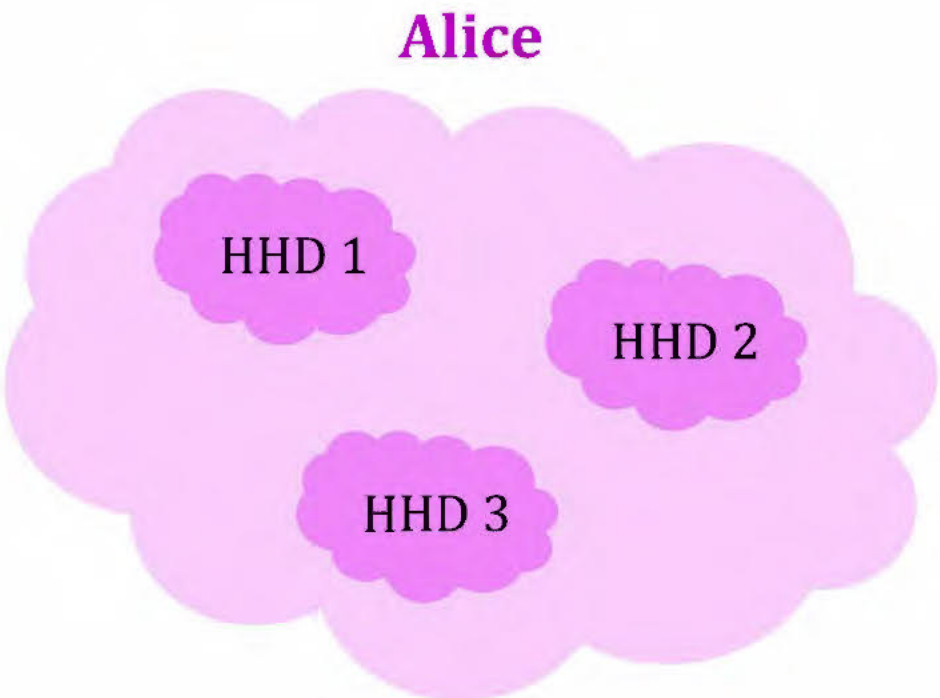
2) Shown that we can **prepare monitors** to **deal with any adversary**.



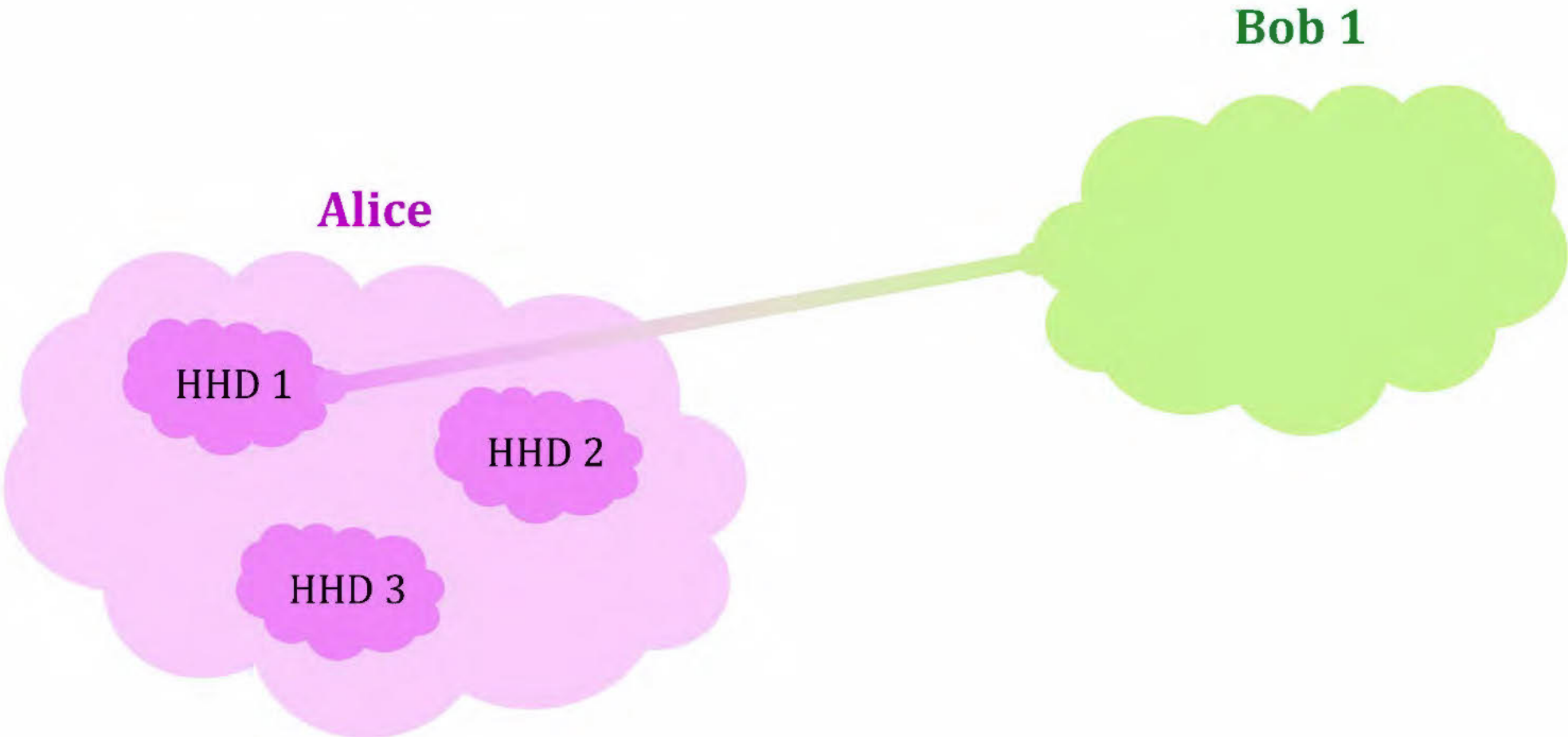
3) Can we also **create adversaries** that can **deal with any monitor?**

THE ROADBLOCK

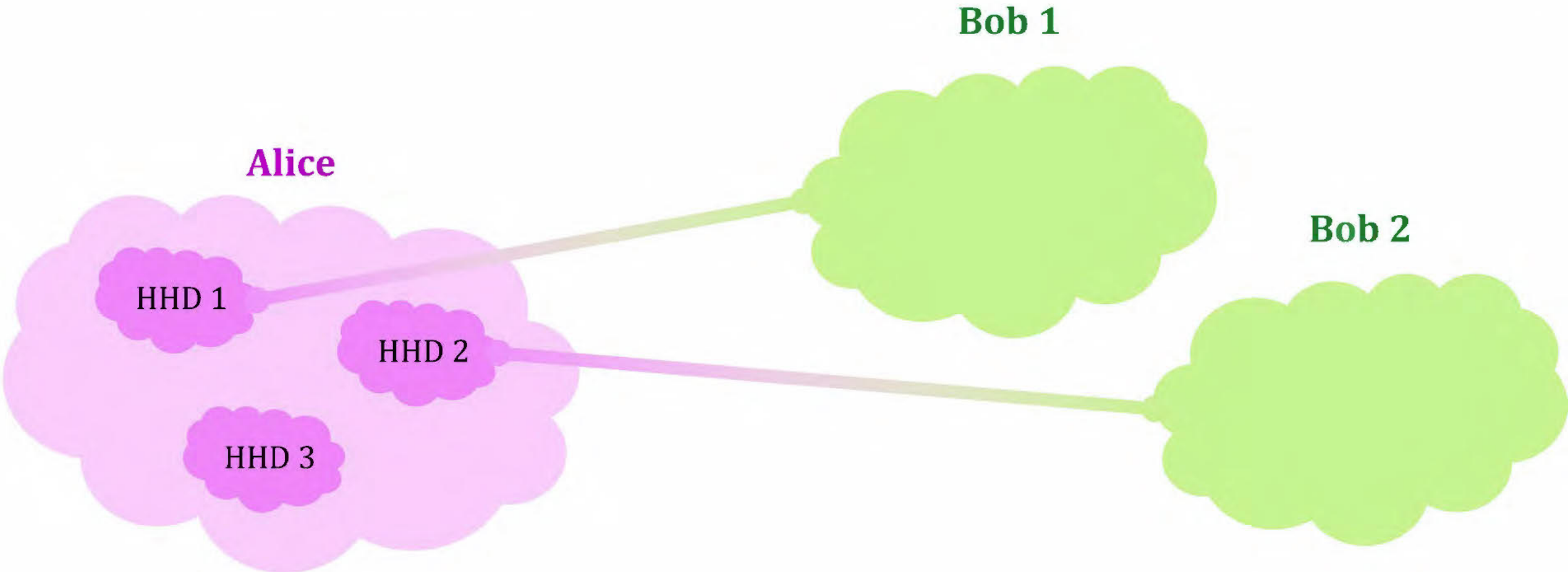
THE ROADBLOCK



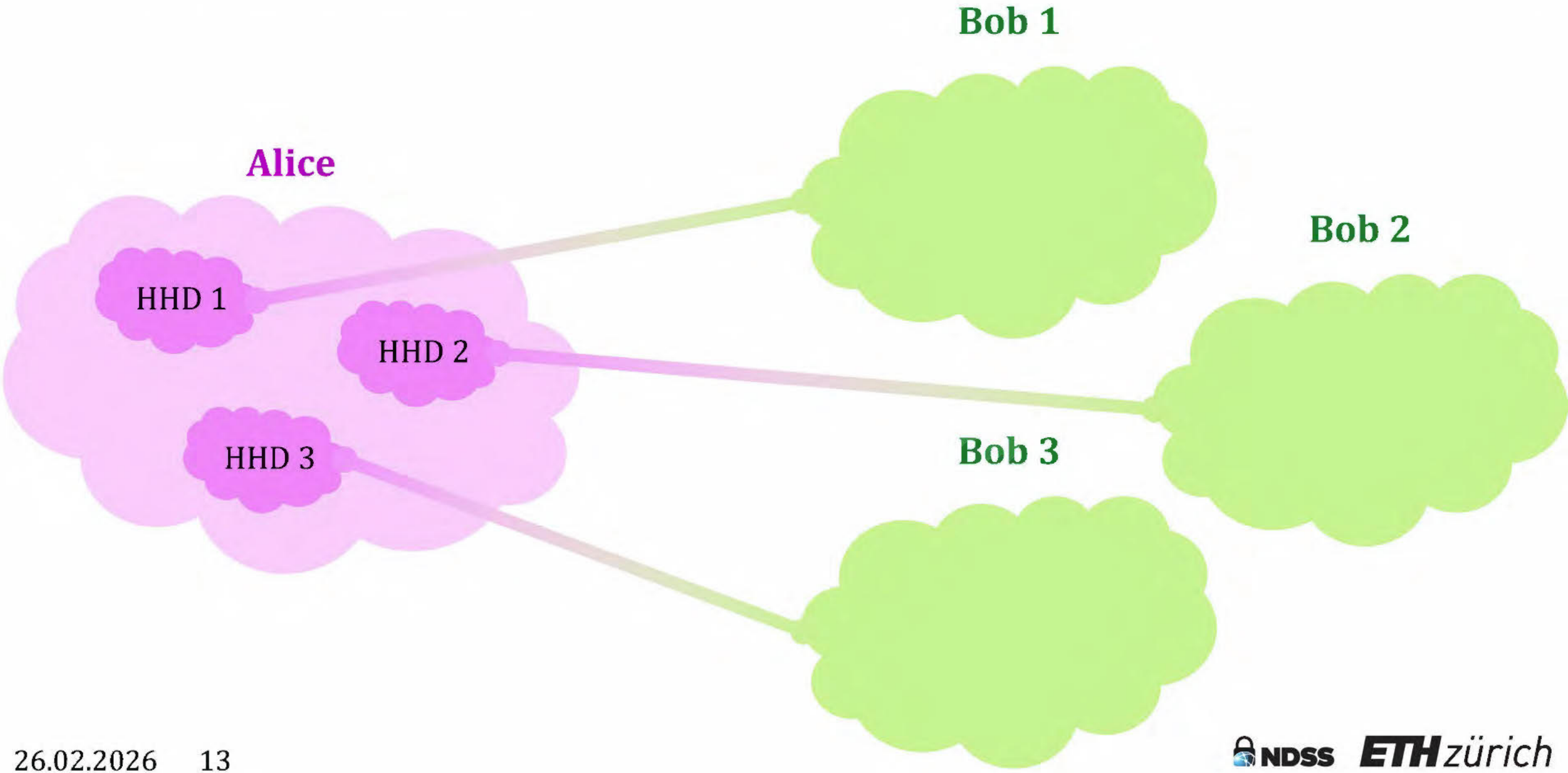
THE ROADBLOCK



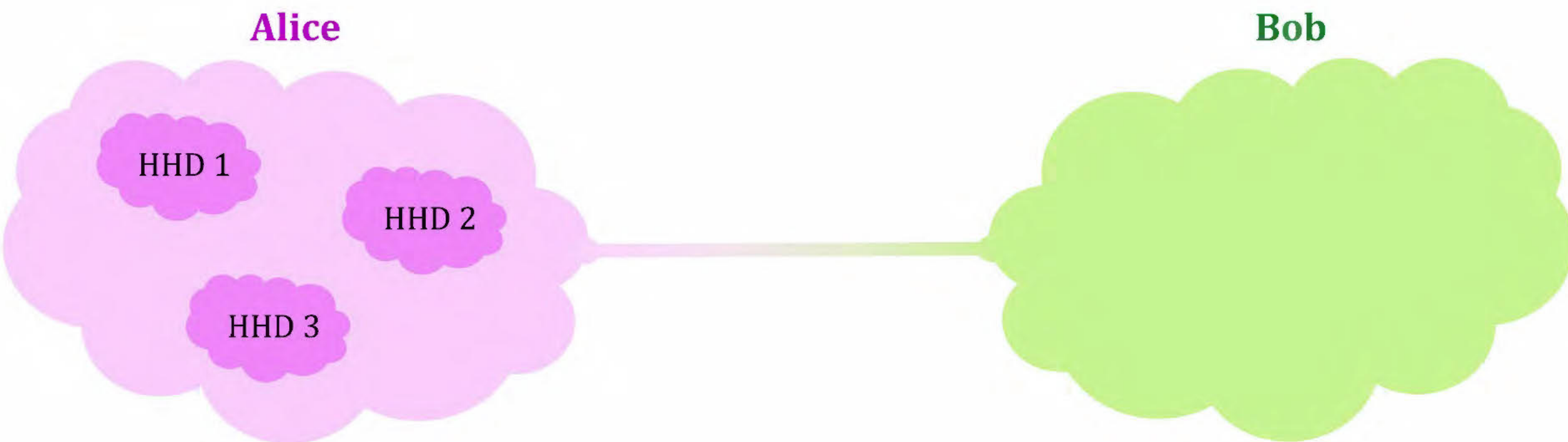
THE ROADBLOCK



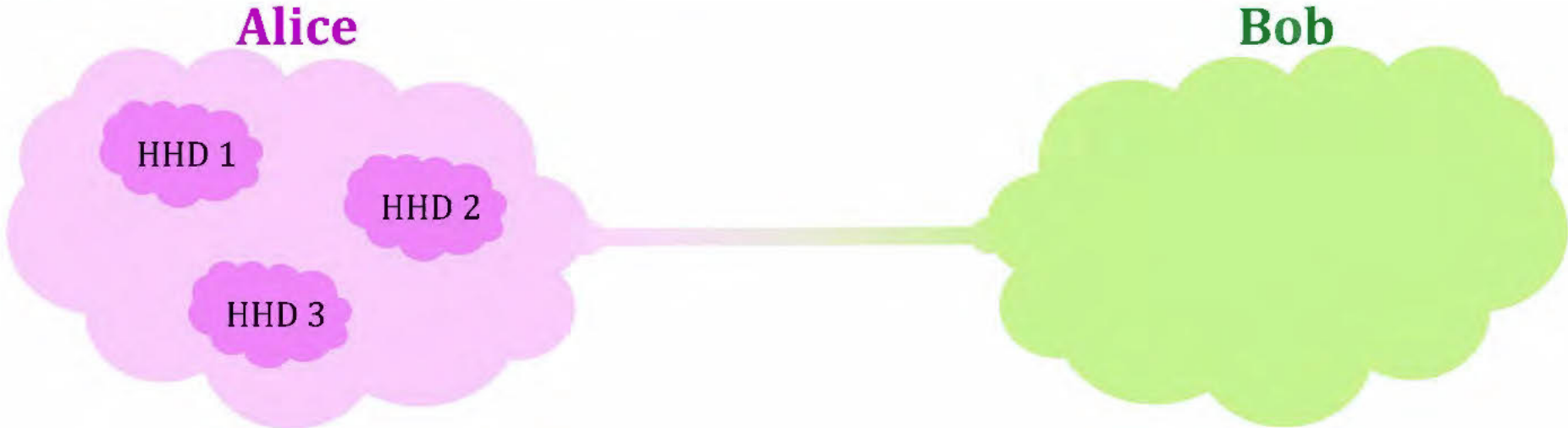
THE ROADBLOCK



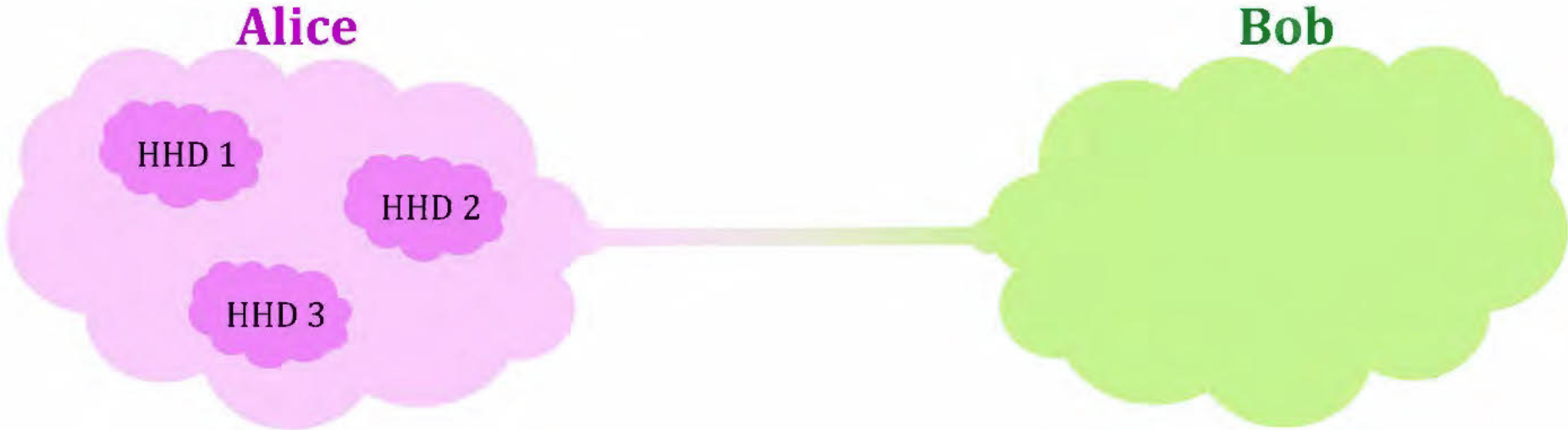
THE ROADBLOCK



ZERO-SHOT ATTACKS

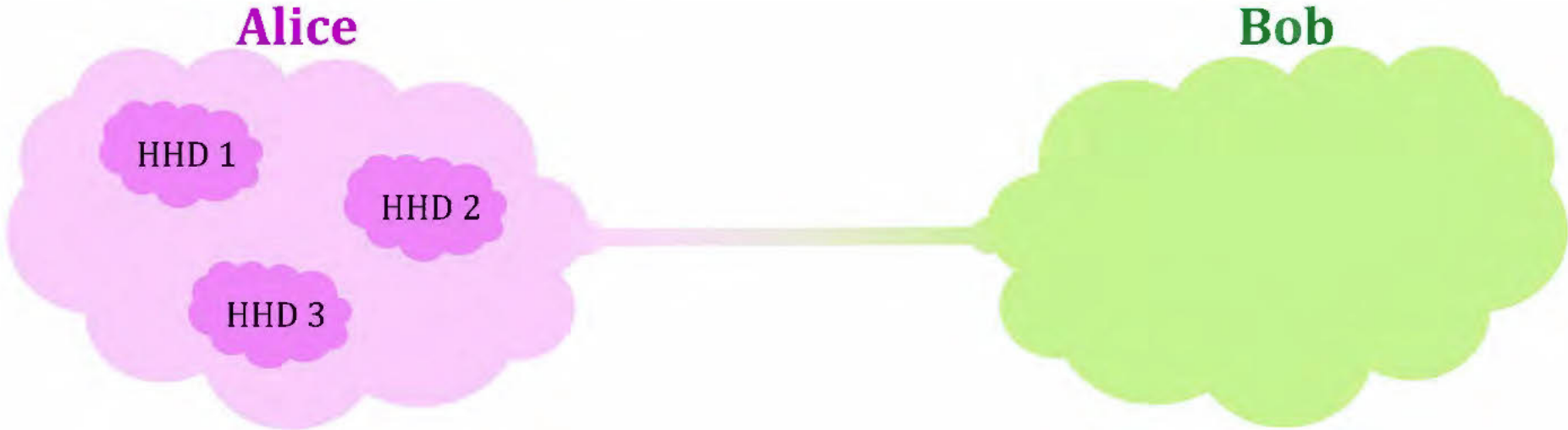


ZERO-SHOT ATTACKS

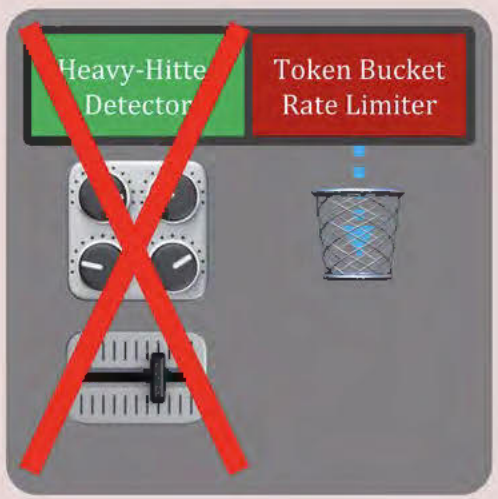


Step 1: More Flexibility

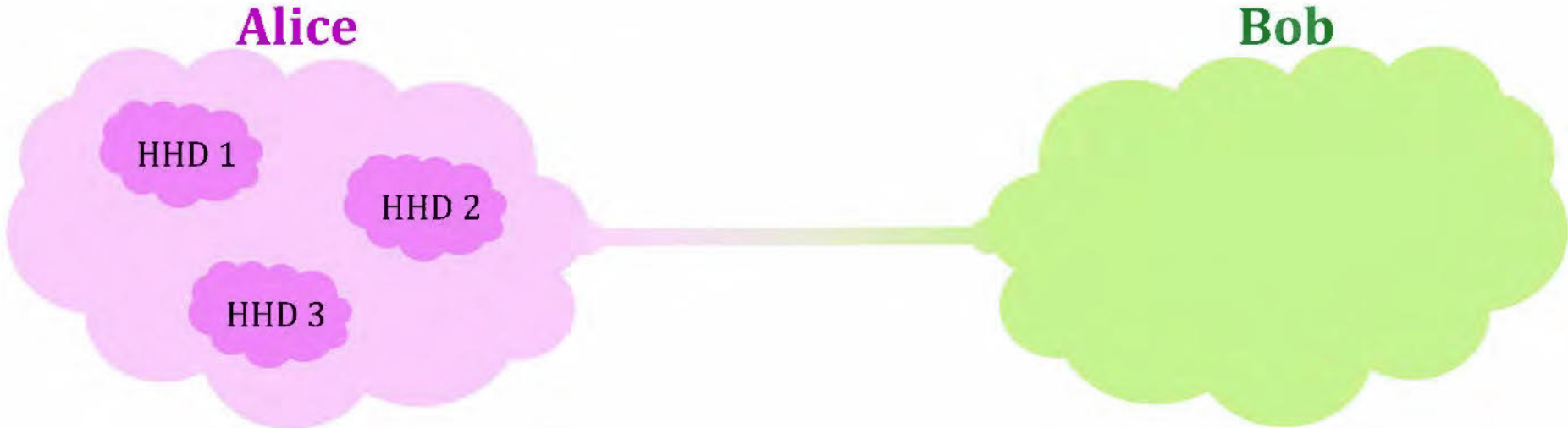
ZERO-SHOT ATTACKS



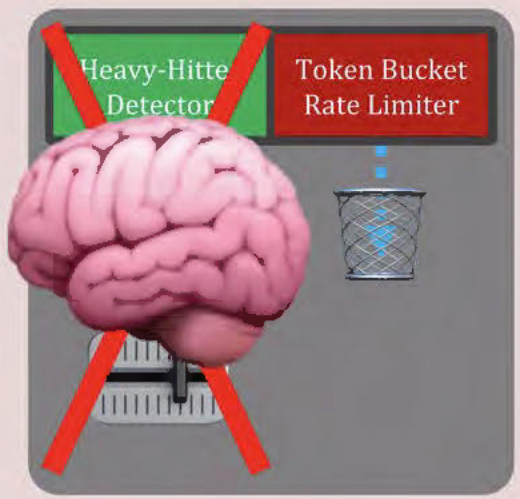
Step 1: More Flexibility



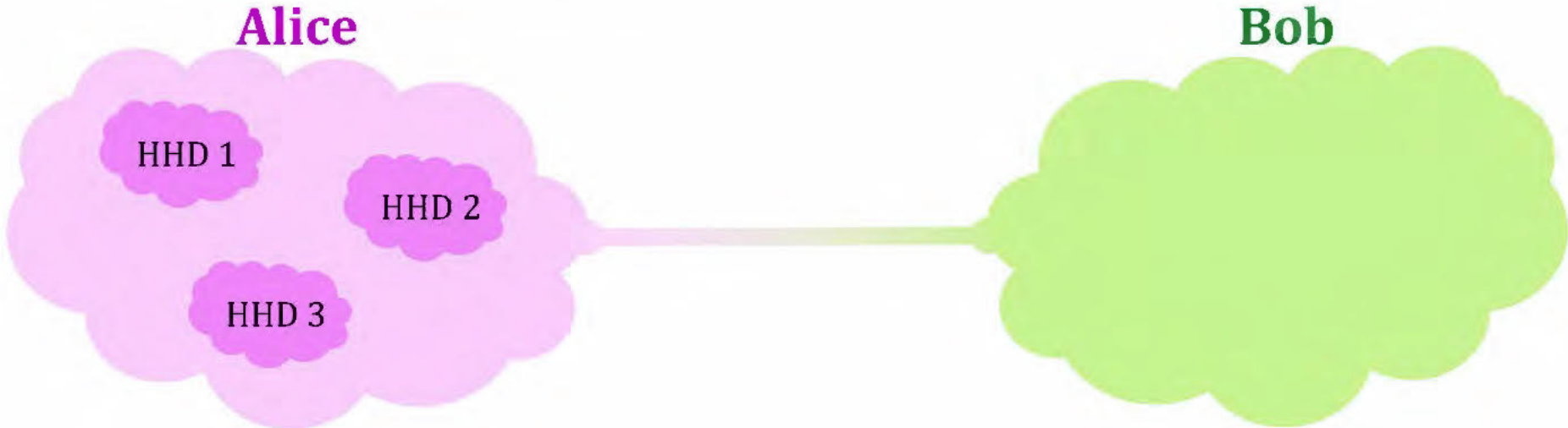
ZERO-SHOT ATTACKS



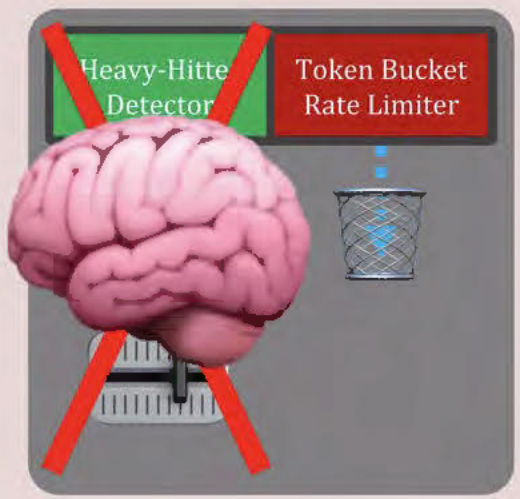
Step 1: More Flexibility



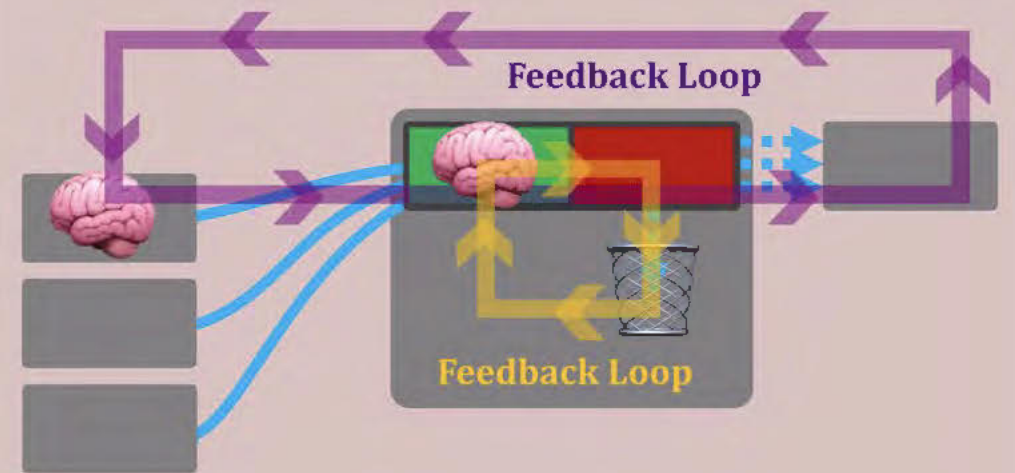
ZERO-SHOT ATTACKS



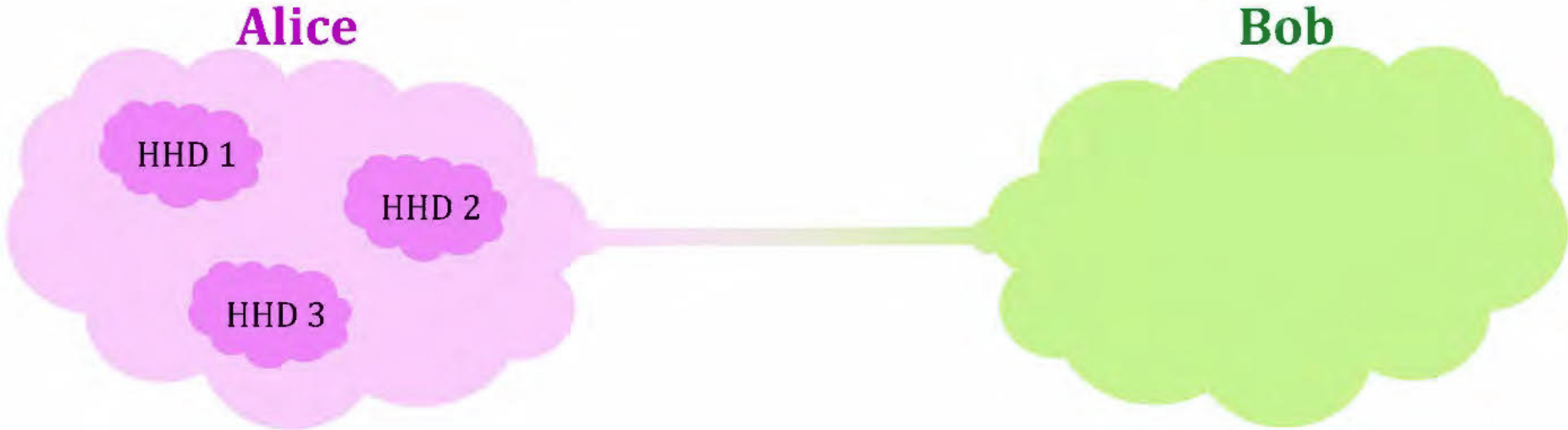
Step 1: More Flexibility



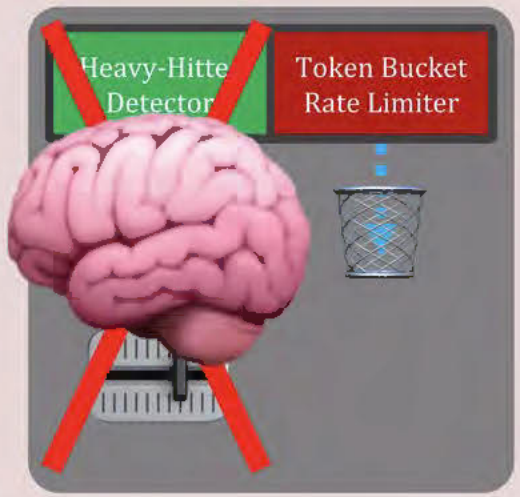
Step 2: Adversarial Co-Training



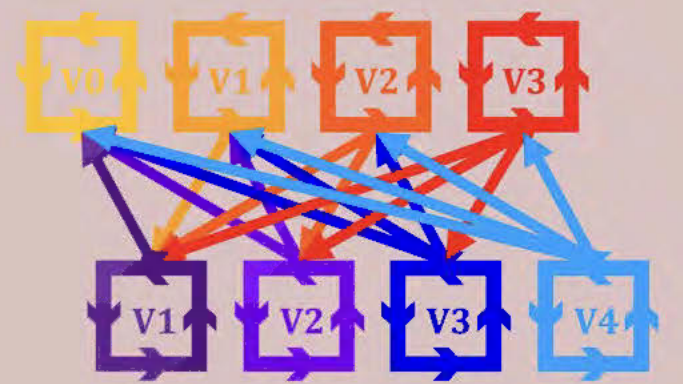
ZERO-SHOT ATTACKS



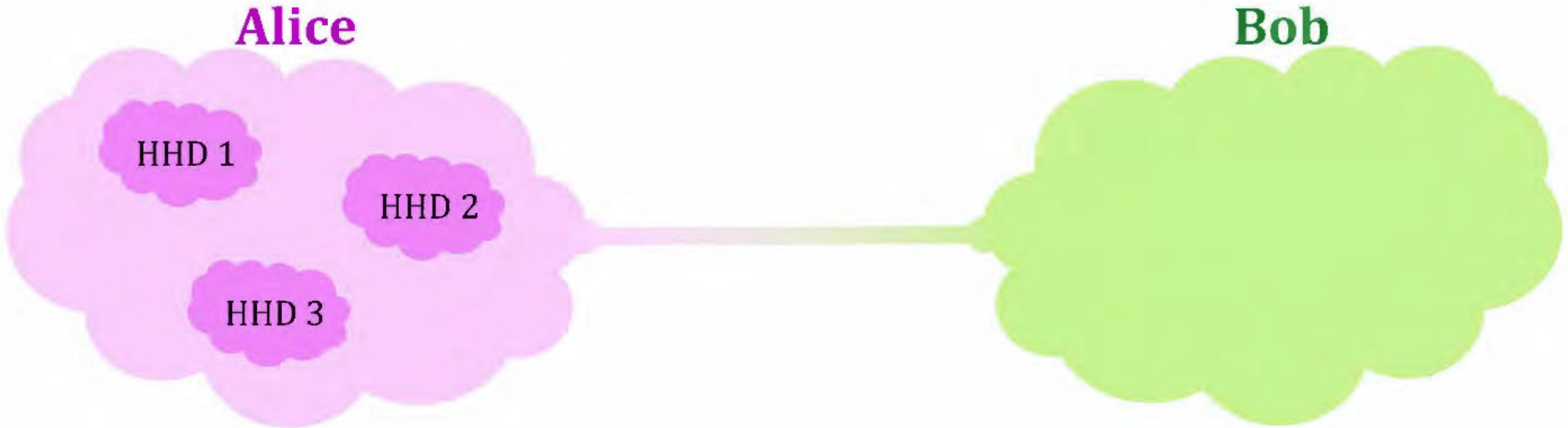
Step 1: More Flexibility



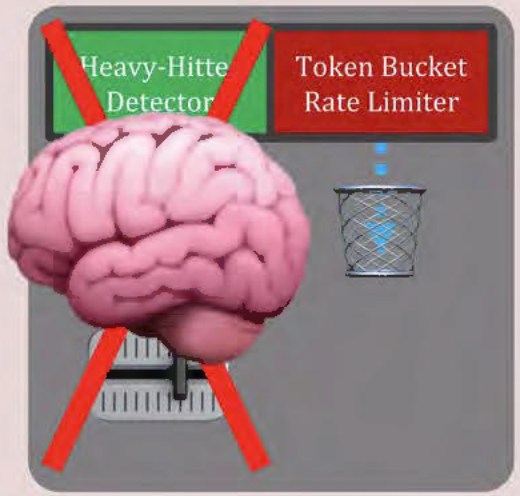
Step 2: Adversarial Co-Training



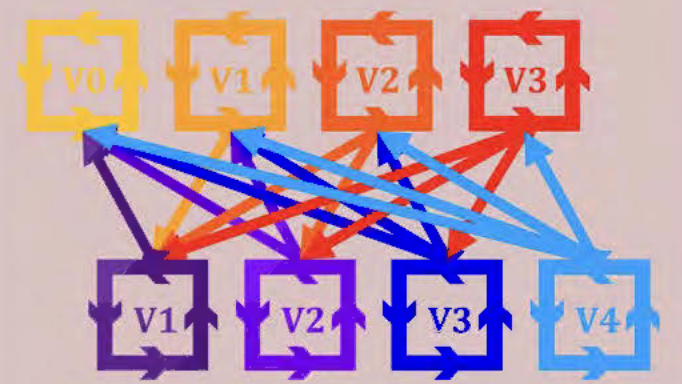
ZERO-SHOT ATTACKS



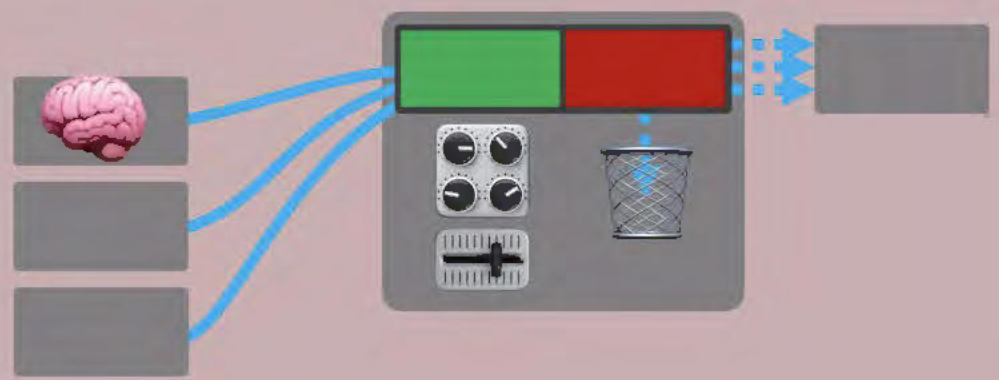
Step 1: More Flexibility



Step 2: Adversarial Co-Training

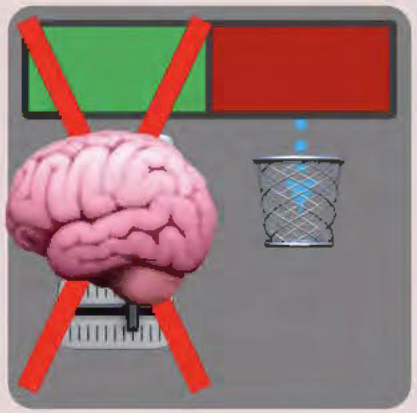


Step 3: Evaluate against HHDs

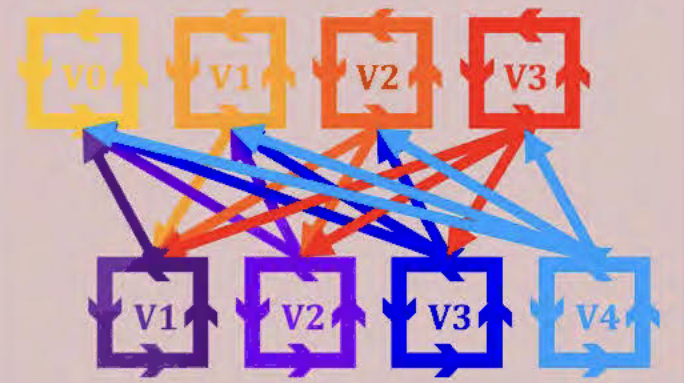


ZERO-SHOT ATTACKS

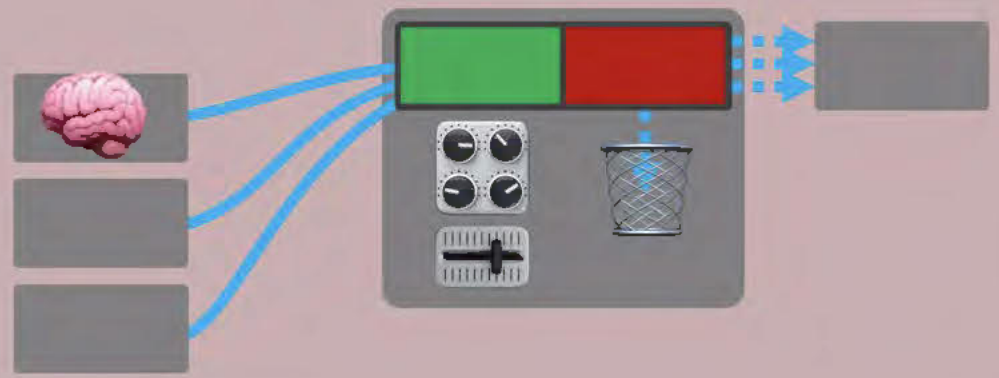
Step 1: More Flexibility



Step 2: Adversarial Co-Training

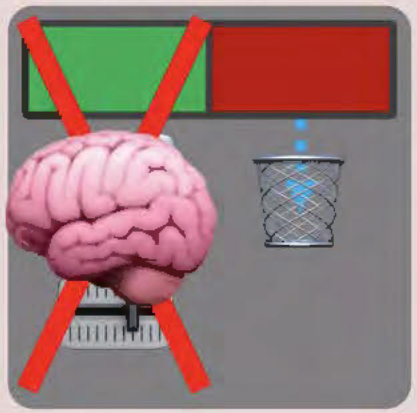


Step 3: Evaluate against HHDs

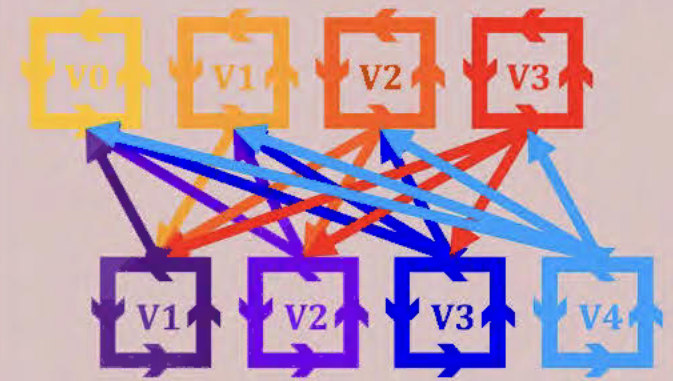


ZERO-SHOT ATTACKS

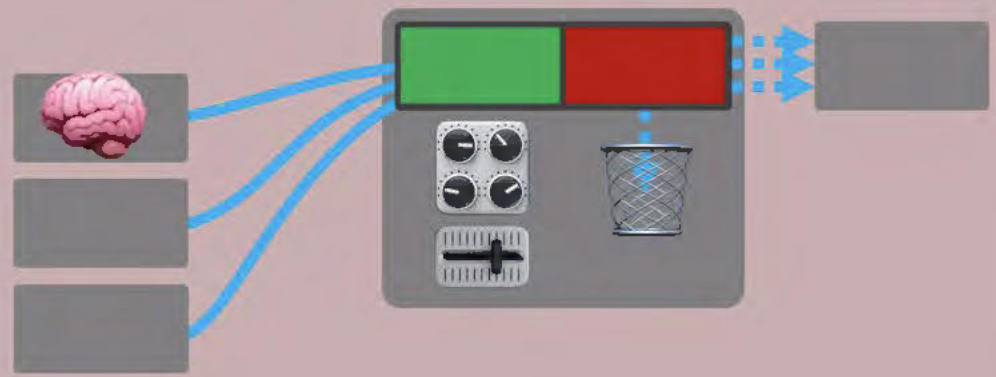
Step 1: More Flexibility



Step 2: Adversarial Co-Training



Step 3: Evaluate against HHDs



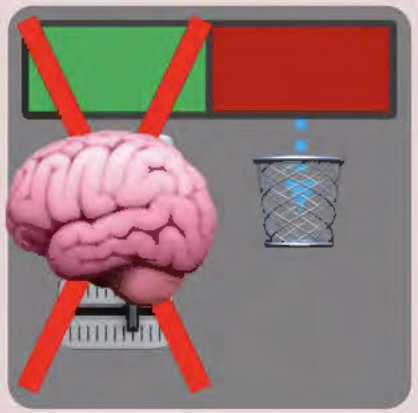
Evaluated for 9 different heavy-hitter detectors

	AL	CB	CM	ES	HK	MG	SS	CH	HP
Synthetic traffic	50%	82%	113%	117%	-20%	27%	58%	86%	38%
Captured traffic	103%	130%	125%	184%	162%	130%	148%	127%	119%

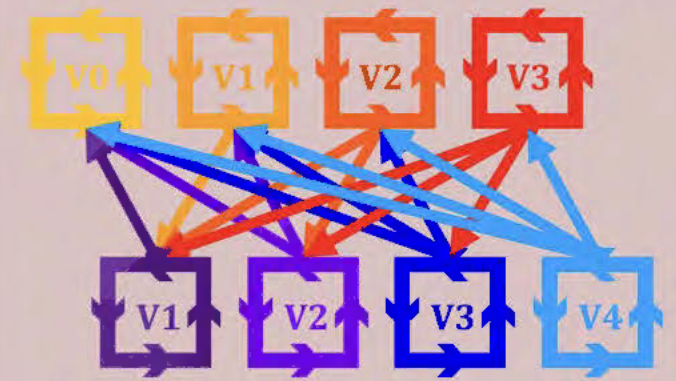
Adversary Overuse

ZERO-SHOT ATTACKS

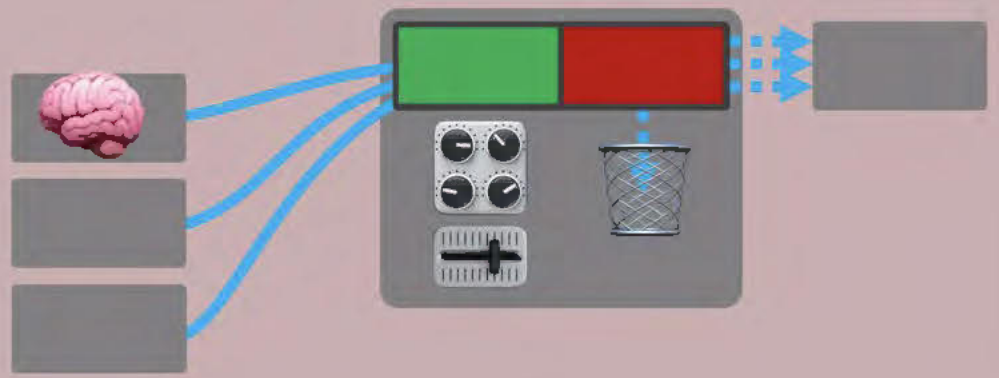
Step 1: More Flexibility



Step 2: Adversarial Co-Training



Step 3: Evaluate against HHDs

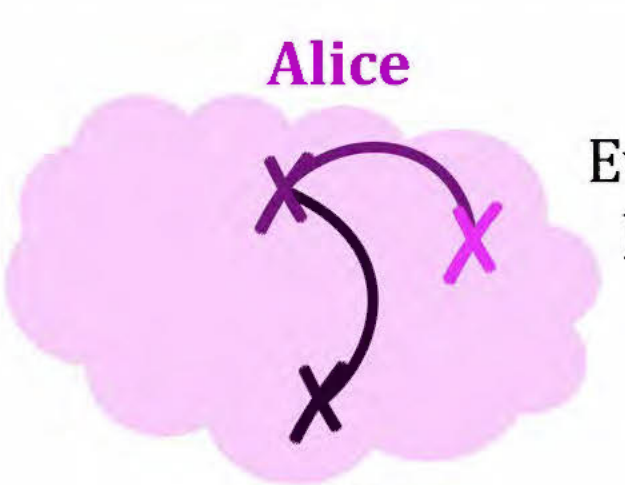


Evaluated for 9 different heavy-hitter detectors

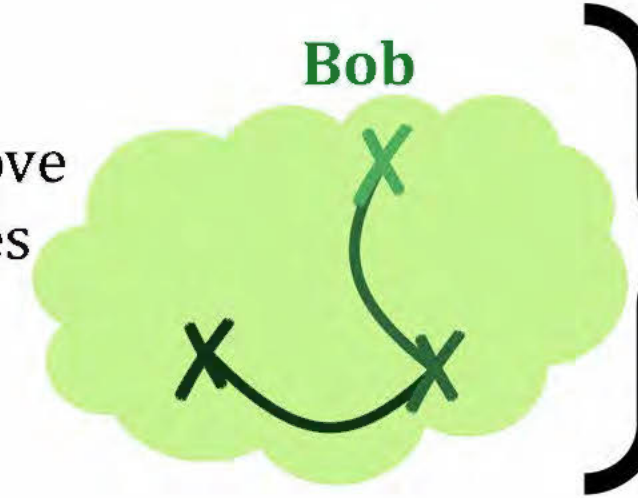
	AL	CB	CM	ES	HK	MG	SS	CH	HP	
Synthetic traffic	50%	82%	113%	117%	-20%	27%	58%	86%	38%	**8/9**
Captured traffic	103%	130%	125%	184%	162%	130%	148%	127%	119%	**9/9**

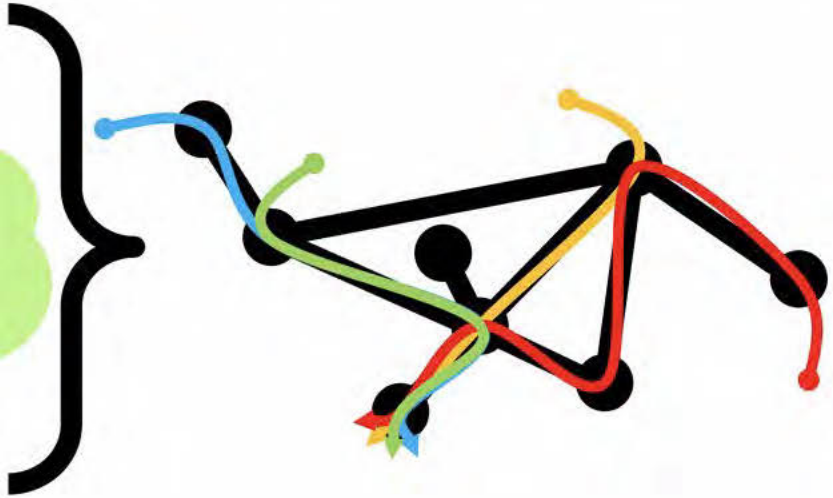
Adversary Overuse

CONCLUSIONS

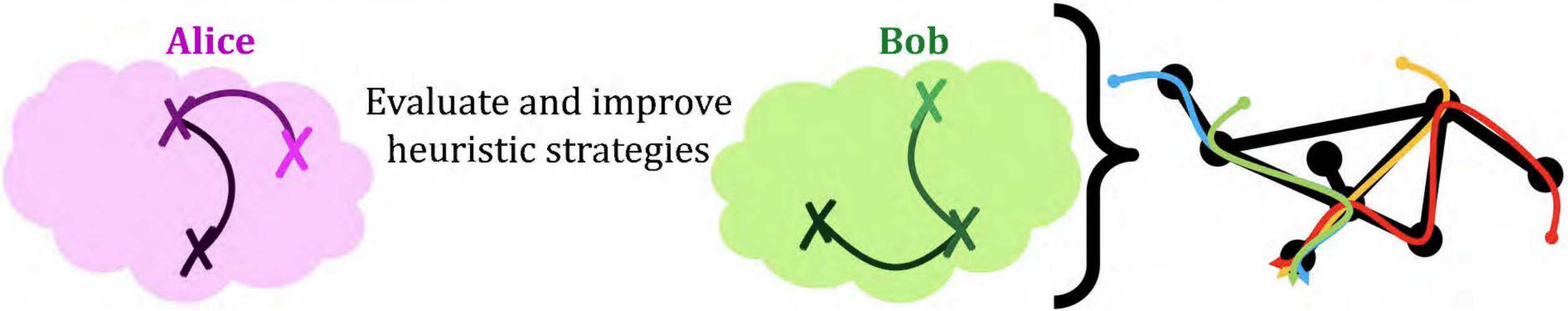


Evaluate and improve heuristic strategies



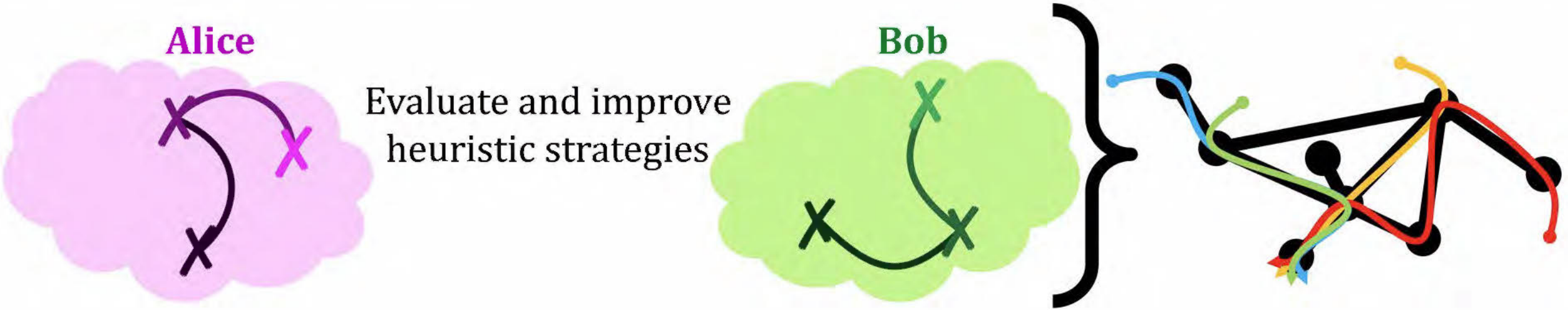


CONCLUSIONS



1) Works with label-free data or no data at all

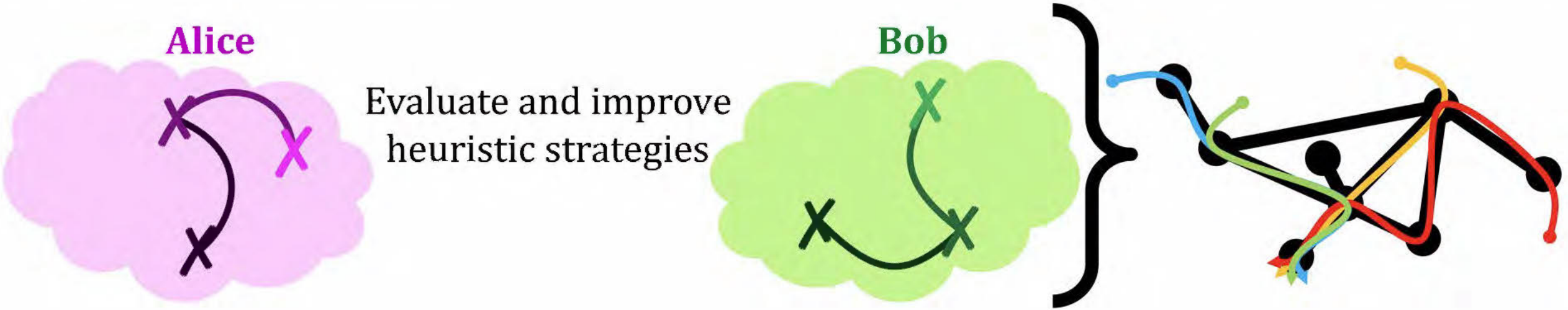
CONCLUSIONS



1) Works with label-free data or no data at all

2) Core ideas can be applied to other scenarios

CONCLUSIONS



1) Works with label-free data or no data at all

2) Core ideas can be applied to other scenarios

3) Code and framework is available online