# (Self) Driving Under the Influence: Intoxicating Adversarial Network Inputs

I TOLD YOU WE NEEDED TO PAY MORE ATTENTION TO OUR SELF-DRIVING CAR!
Bill Whitehead

Roland Meier(1), Thomas Holterbach(1), Stephan Keck(1), Matthias Stähli(1), Vincent Lenders(2), Ankit Singla(1), Laurent Vanbever(1)

ACM HotNets 2019

(1) ETHzürich

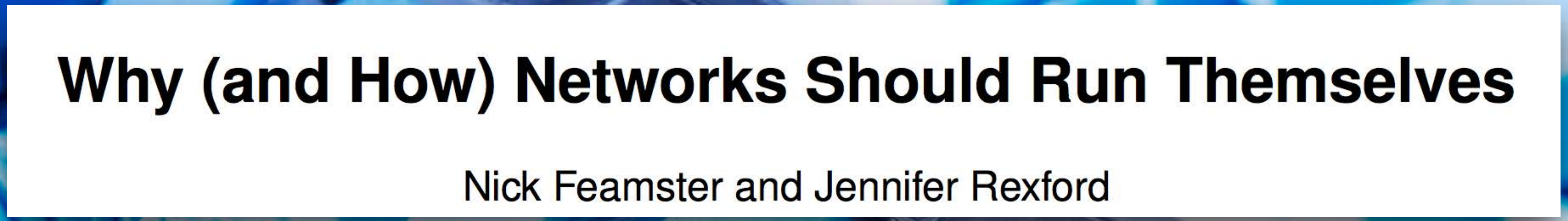
(2) Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

armasuisse

# In-band-signaling in the telephony system allowed “hackers” free long-distance calls

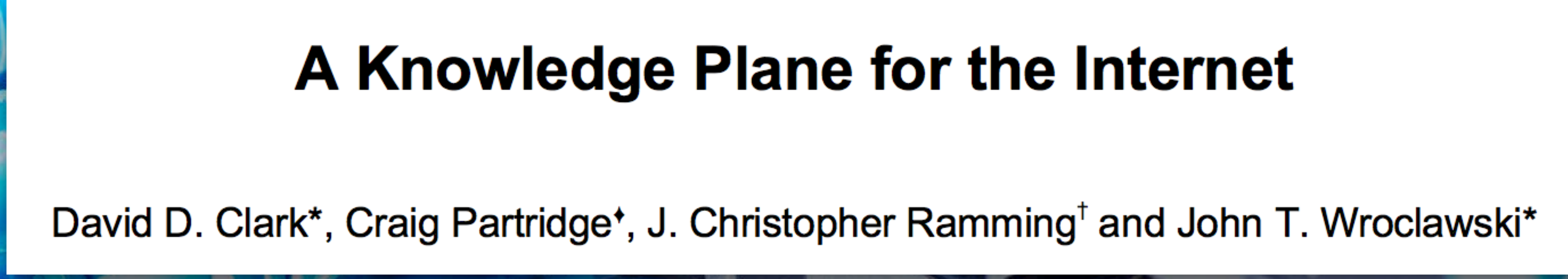
[Wikimedia]

# What does in-band-signaling enable in networks?



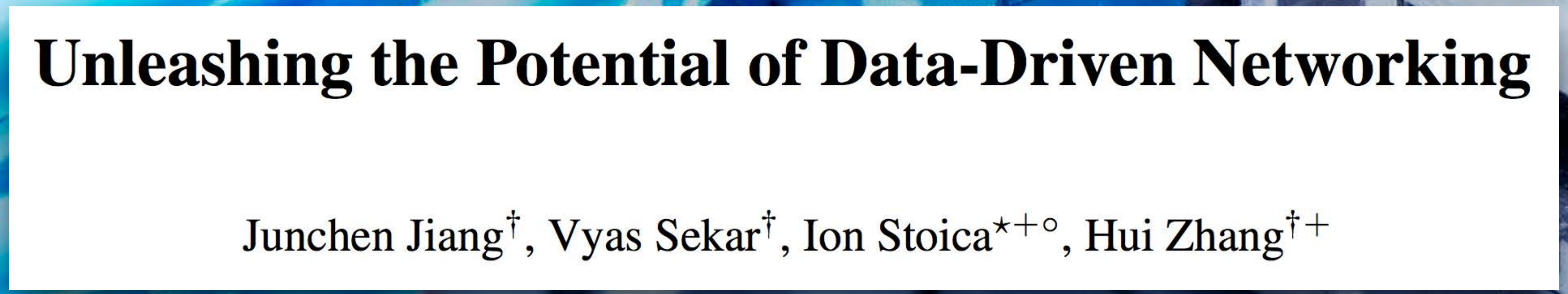
## Why (and How) Networks Should Run Themselves

Nick Feamster and Jennifer Rexford



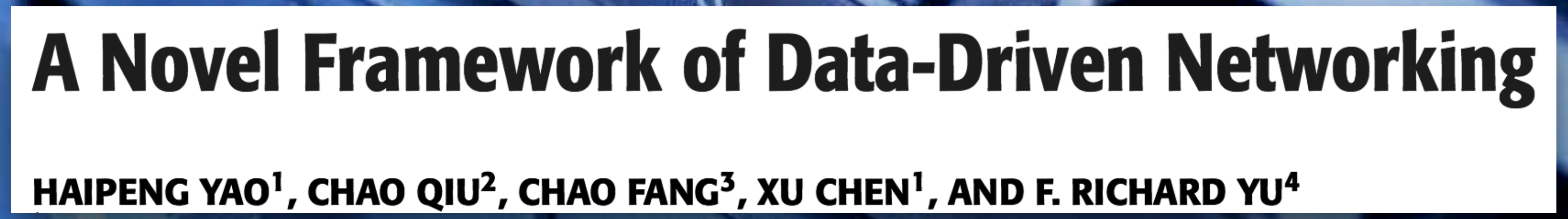
## A Knowledge Plane for the Internet

David D. Clark[*], Craig Partridge[♦], J. Christopher Ramming[†] and John T. Wroclawski[*]



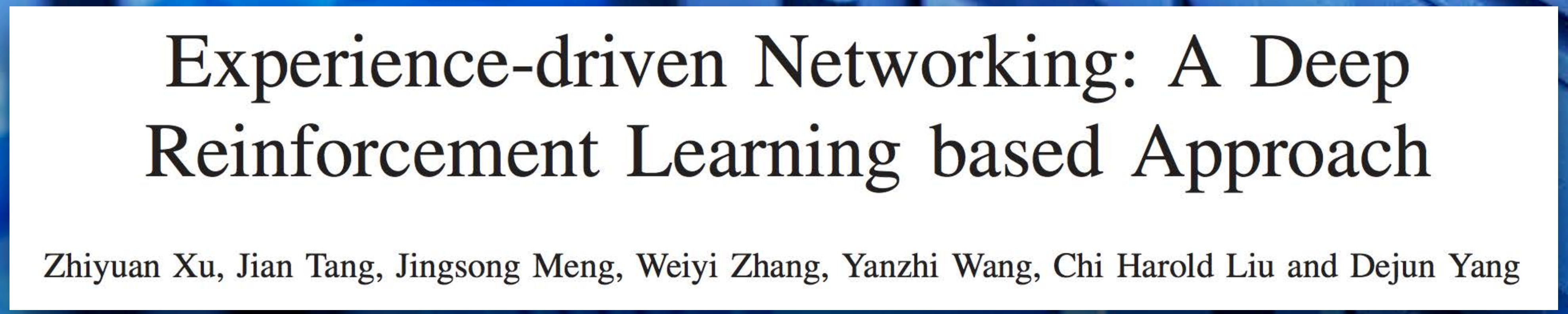
## Unleashing the Potential of Data-Driven Networking

Junchen Jiang[†], Vyas Sekar[†], Ion Stoica[⋆+∘], Hui Zhang[†+]



## A Novel Framework of Data-Driven Networking

HAIPENG YAO[1], CHAO QIU[2], CHAO FANG[3], XU CHEN[1], AND F. RICHARD YU[4]

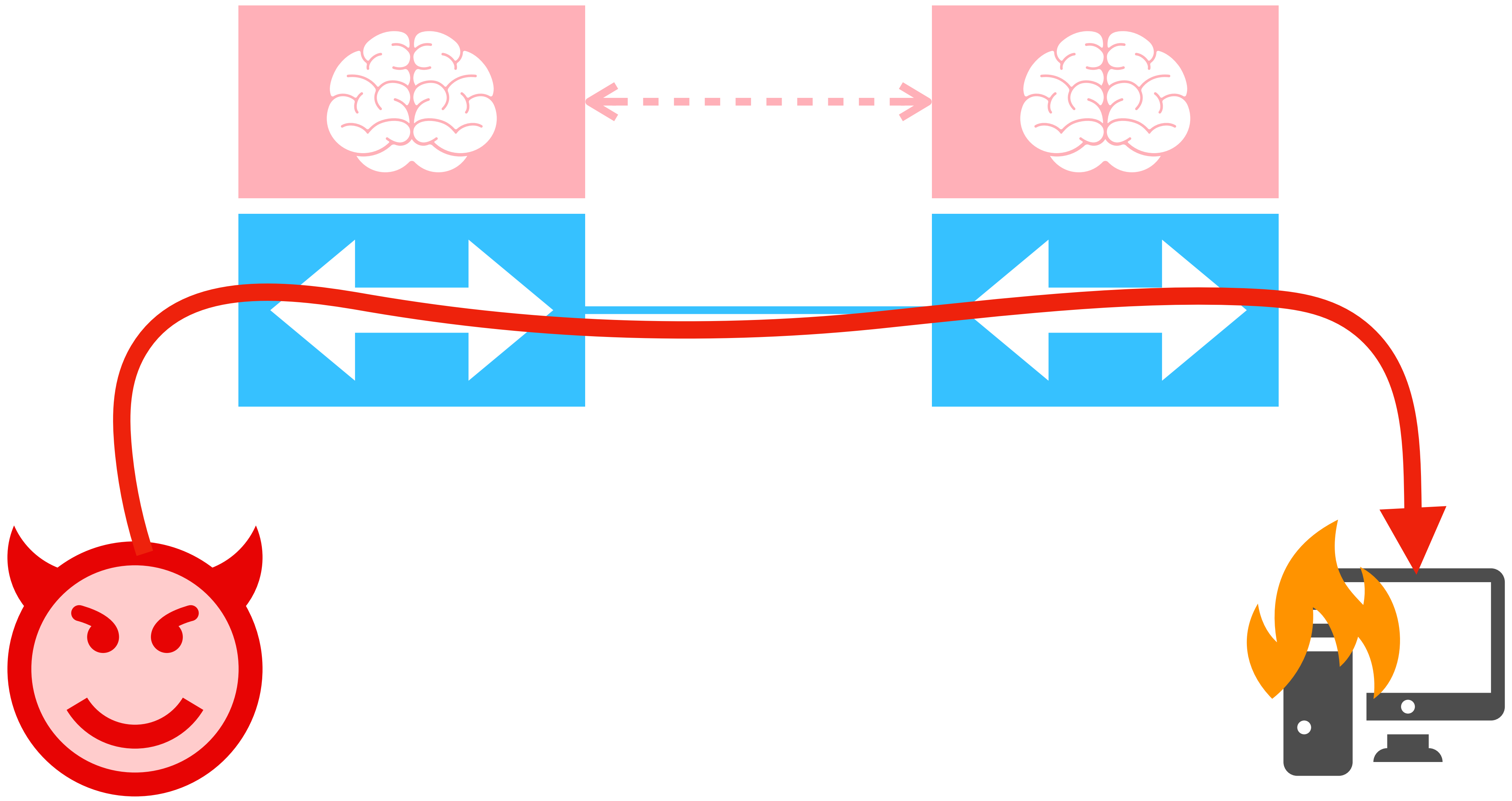


## Experience-driven Networking: A Deep Reinforcement Learning based Approach

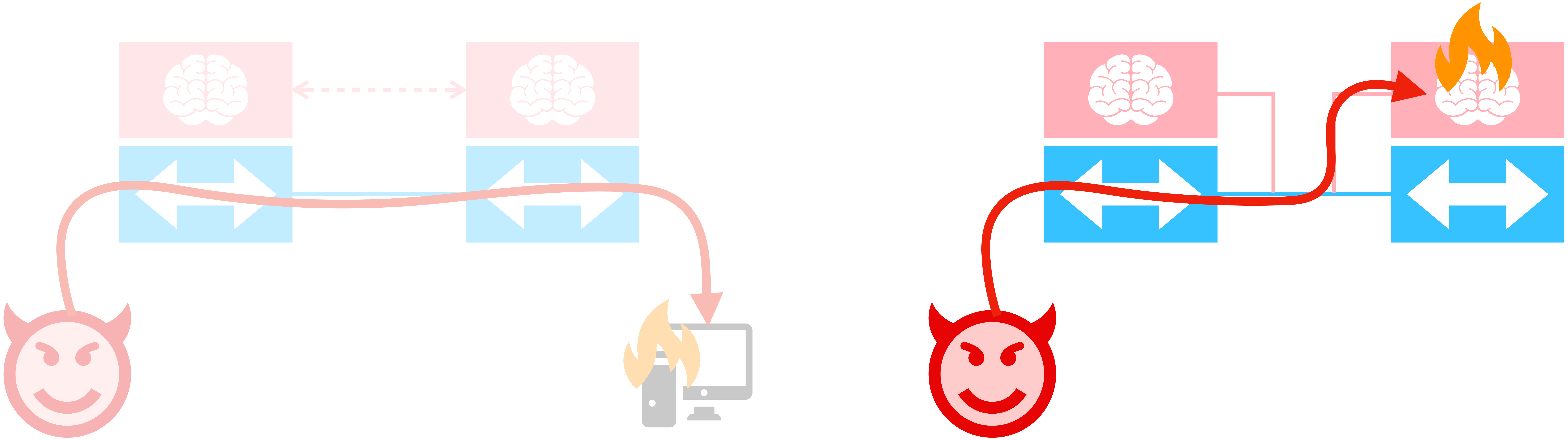
Zhiyuan Xu, Jian Tang, Jingsong Meng, Weiyi Zhang, Yanzhi Wang, Chi Harold Liu and Dejun Yang

[Dumont Telephone]

# Traditional networks separate data and control channels



# Self-driving networks merge data and control channels



*Attacking*

self-driving networks

*Defending*

self-driving networks

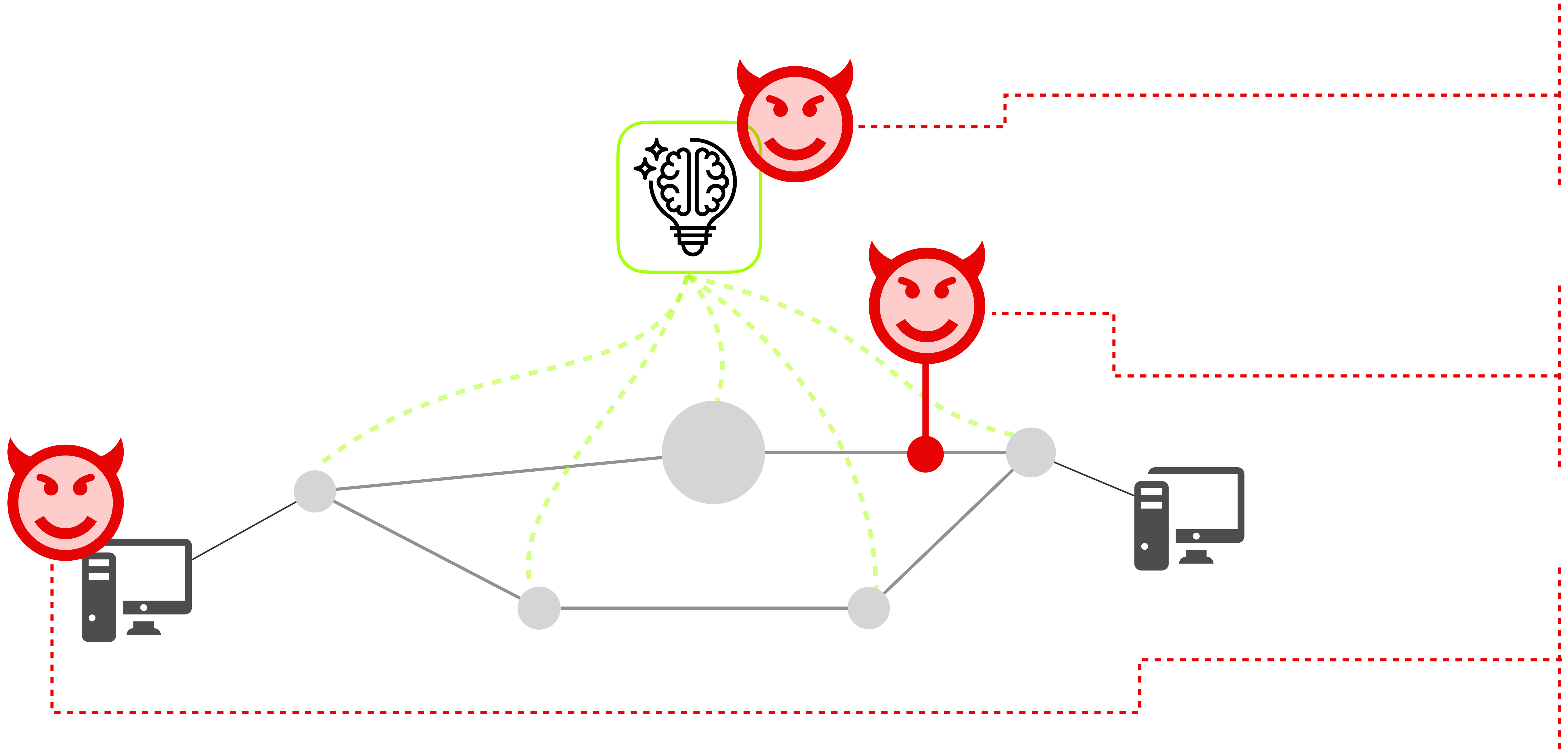
*Attacking*

self-driving networks

*Defending*

self-driving networks

# We distinguish between three privilege levels of an attacker



Operator

Controls the entire network

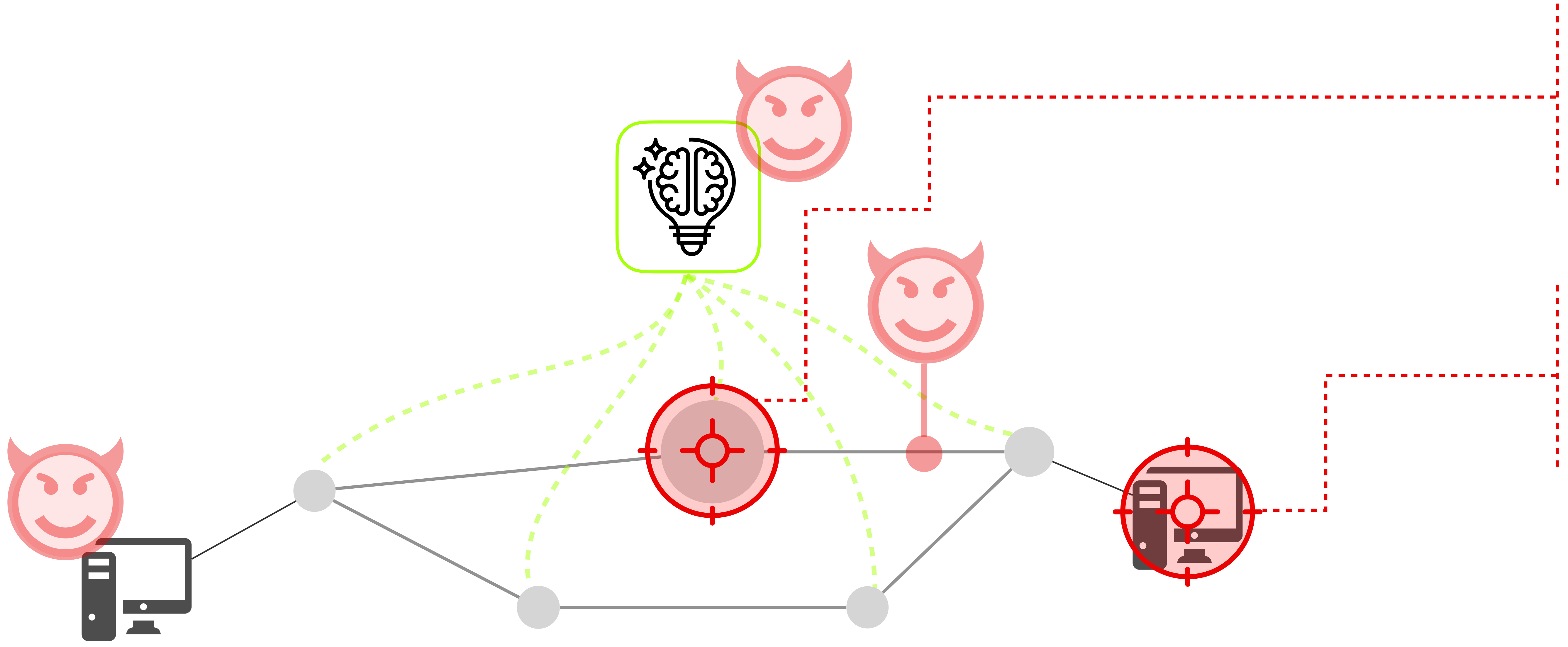
Man in the middle

Controls traffic on link(s)

Host

Controls host(s)

# We distinguish between two attack targets



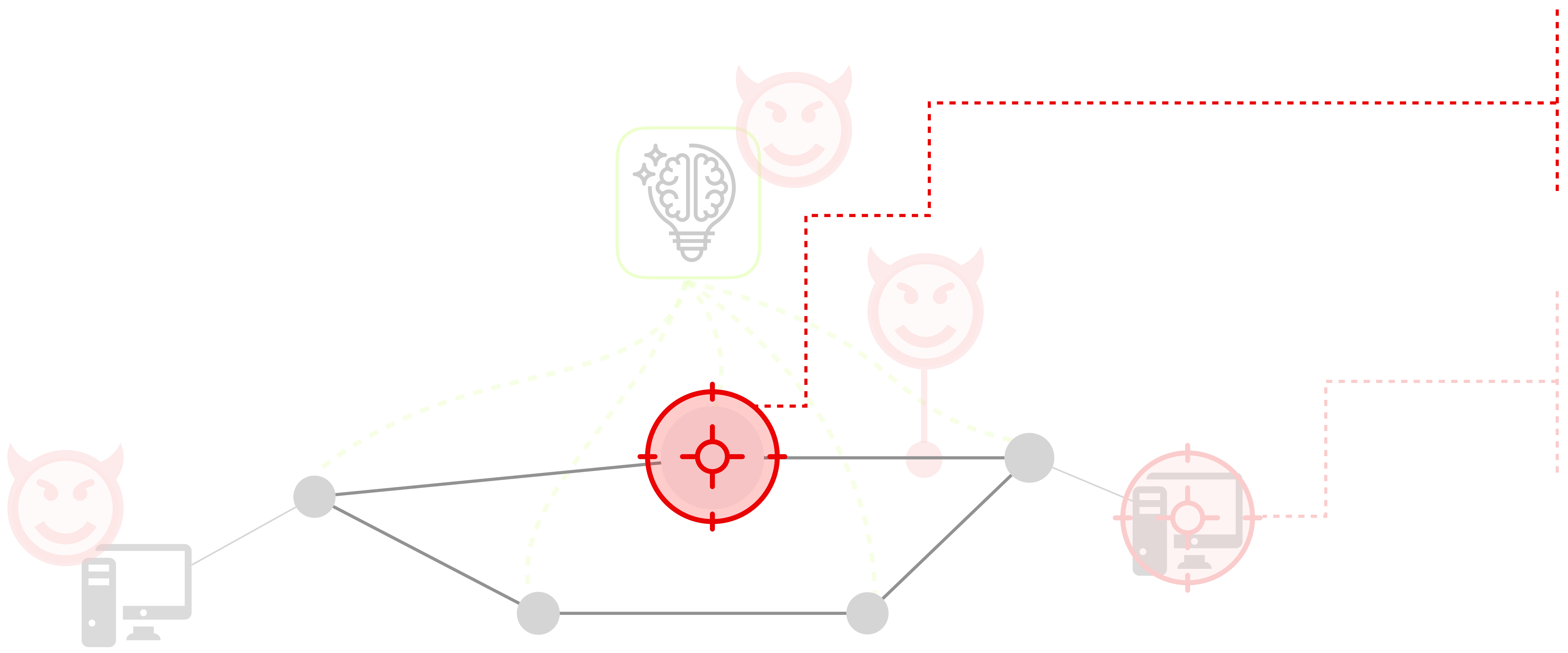
Network infrastructure

E.g., forwarding behavior

Endpoints

E.g., applications

# We distinguish between two attack targets



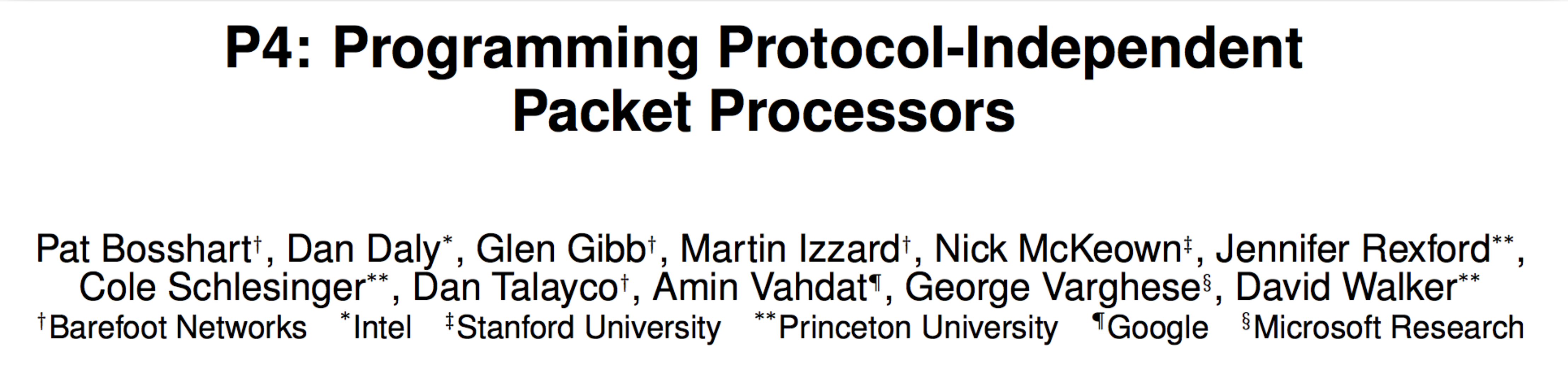
Network infrastructure

E.g., forwarding behavior

Endpoints

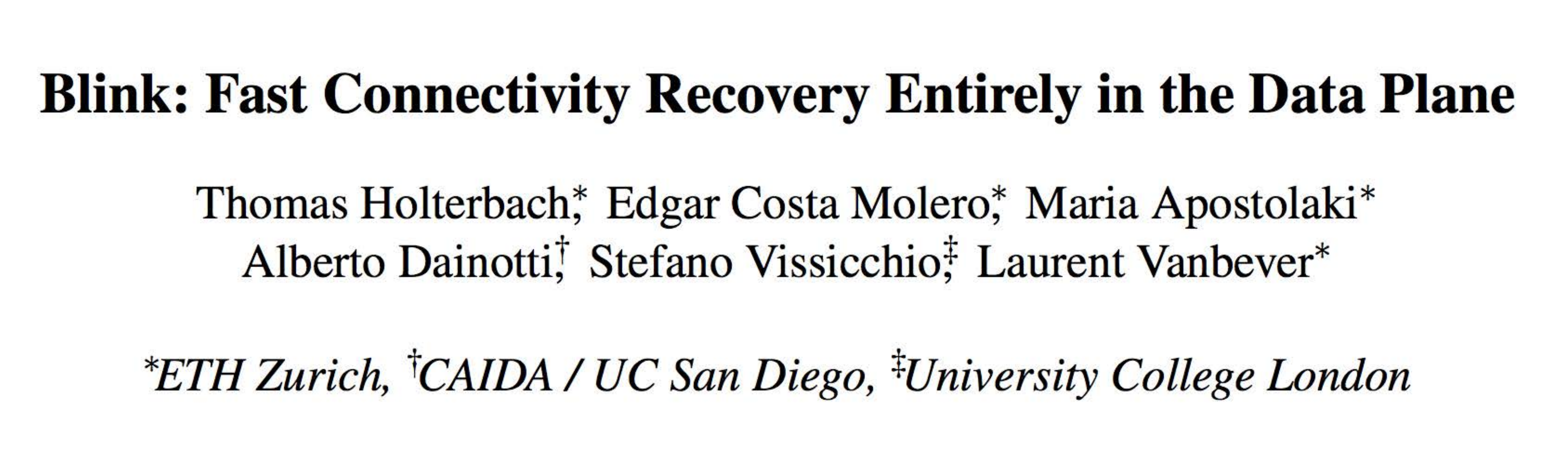
E.g., applications

# Advances in network programability allow to perform many decisions in the data plane



**P4: Programming Protocol-Independent Packet Processors**

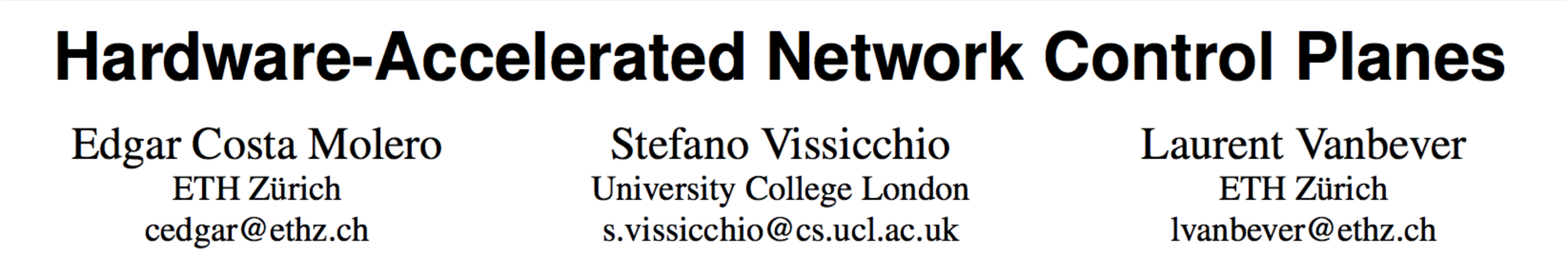
Pat Bosshart[†], Dan Daly[*], Glen Gibb[†], Martin Izzard[†], Nick McKeown[‡], Jennifer Rexford[**], Cole Schlesinger[**], Dan Talayco[†], Amin Vahdat[¶], George Varghese[§], David Walker[**]
[†]Barefoot Networks [*]Intel [‡]Stanford University [**]Princeton University [¶]Google [§]Microsoft Research



**Blink: Fast Connectivity Recovery Entirely in the Data Plane**

Thomas Holterbach[*], Edgar Costa Molero[*], Maria Apostolaki[*]
Alberto Dainotti[†], Stefano Vissicchio[‡], Laurent Vanbever[*]

*[*]ETH Zurich, [†]CAIDA / UC San Diego, [‡]University College London*

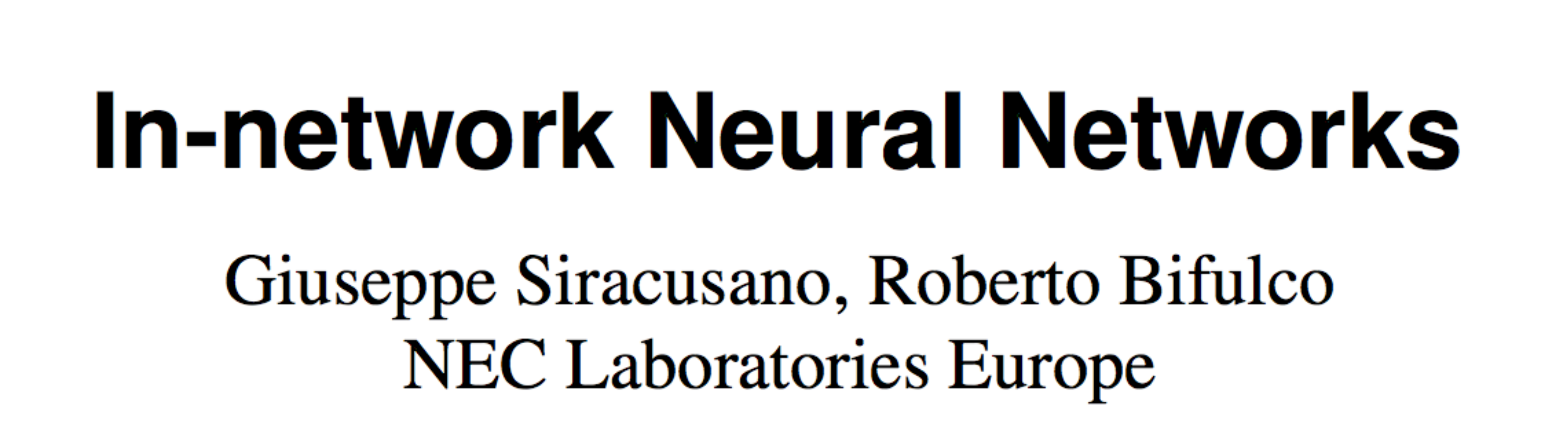


**Hardware-Accelerated Network Control Planes**

Edgar Costa Molero
ETH Zürich
cedgar@ethz.ch

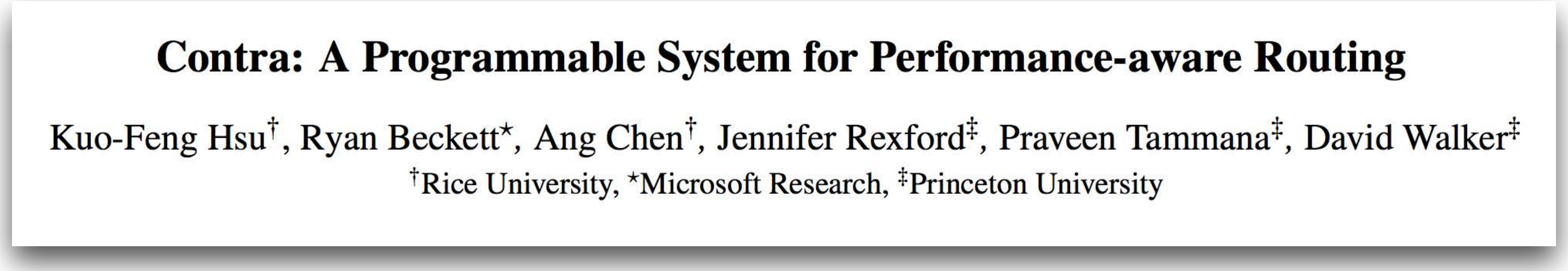
Stefano Vissicchio
University College London
s.vissicchio@cs.ucl.ac.uk

Laurent Vanbever
ETH Zürich
lvanbever@ethz.ch



**In-network Neural Networks**

Giuseppe Siracusano, Roberto Bifulco
NEC Laboratories Europe



**Contra: A Programmable System for Performance-aware Routing**

Kuo-Feng Hsu[†], Ryan Beckett[⋆], Ang Chen[†], Jennifer Rexford[‡], Praveen Tammana[‡], David Walker[‡]
[†]Rice University, [⋆]Microsoft Research, [‡]Princeton University

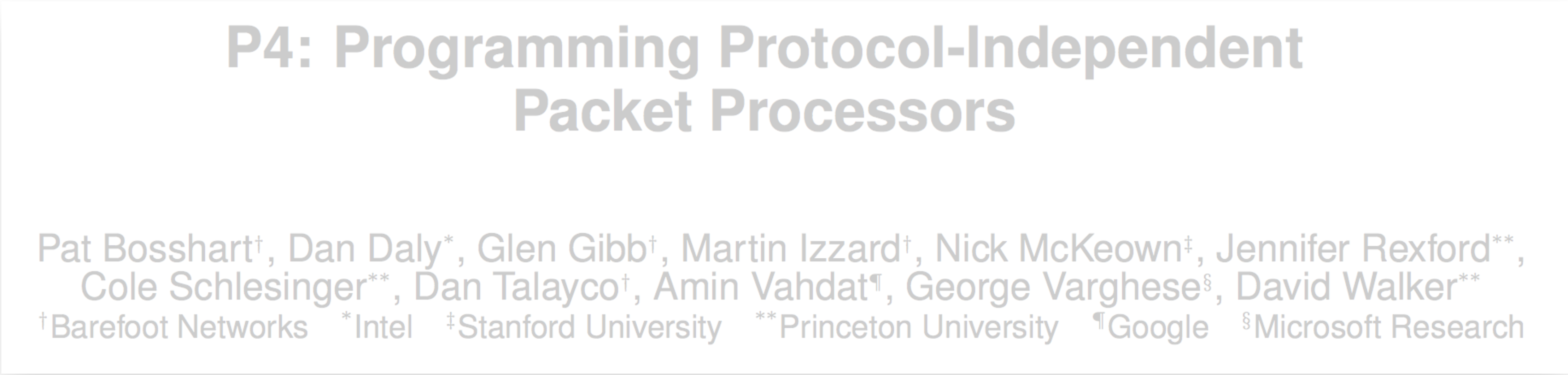
# Algorithms and their state determine the behavior of networks

| | Host | MitM | Operator |
|---|---|---|---|
| Algorithms<br>e.g., for forwarding | 👿 | 👿 | 😈 |
| State<br>e.g., forwarding table | 😈 | 😈 | 😈 |

# Adversarial inputs to data-driven networks can have big consequences

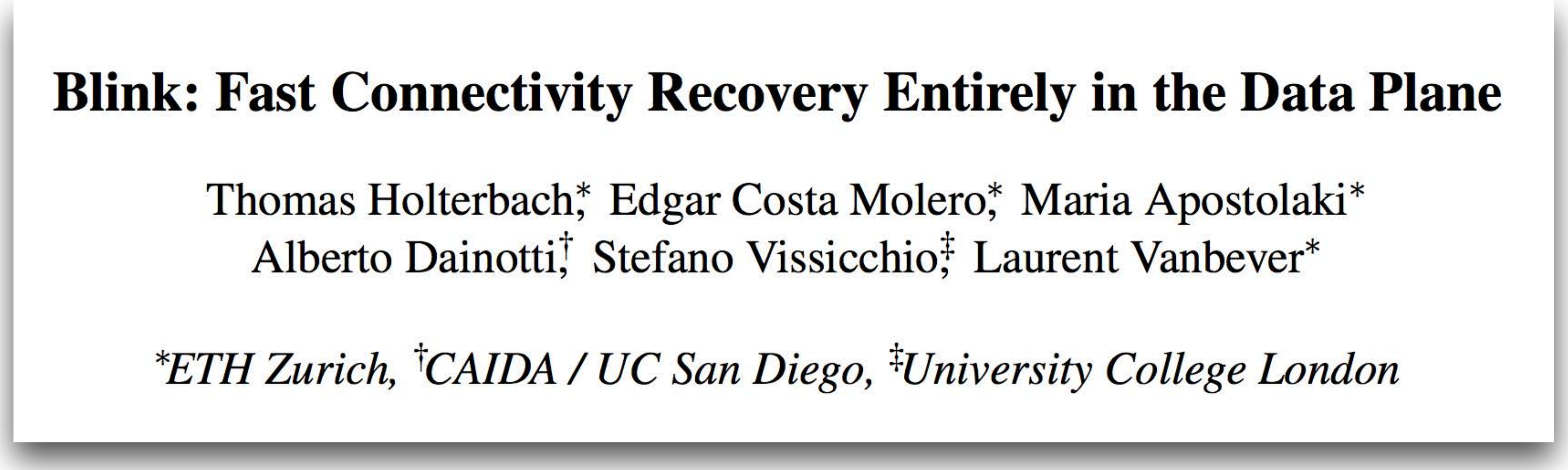
- Privacy violations
  e.g., traffic hijacking
- Performance degradation
  e.g., choosing longer paths
- Reachability problems
  e.g., disconnected network
- Revenue loss
  e.g., bad QoE for clients

# Advances in network programability allow to perform many decisions in the data plane



P4: Programming Protocol-Independent Packet Processors

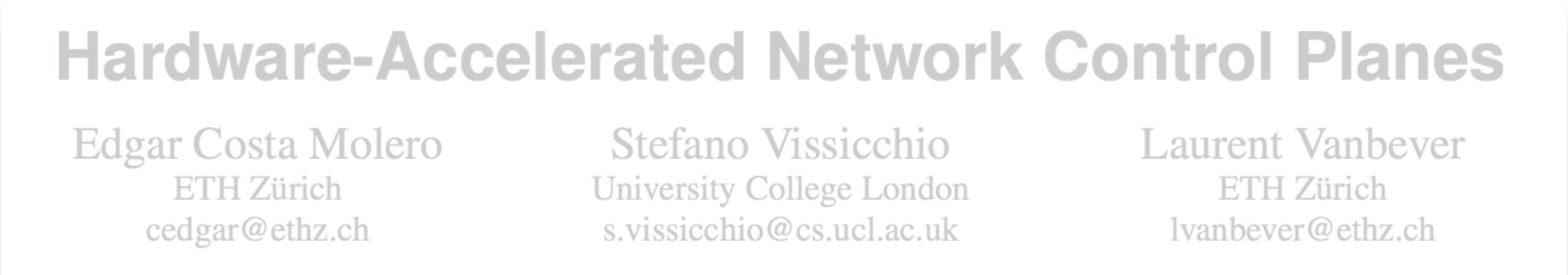
Pat Bosshart†, Dan Daly*, Glen Gibb†, Martin Izzard†, Nick McKeown‡, Jennifer Rexford**, Cole Schlesinger**, Dan Talayco†, Amin Vahdat¶, George Varghese§, David Walker**
†Barefoot Networks *Intel ‡Stanford University **Princeton University ¶Google §Microsoft Research



Blink: Fast Connectivity Recovery Entirely in the Data Plane

Thomas Holterbach,* Edgar Costa Molero,* Maria Apostolaki*
Alberto Dainotti,† Stefano Vissicchio,‡ Laurent Vanbever*

*ETH Zurich, †CAIDA / UC San Diego, ‡University College London

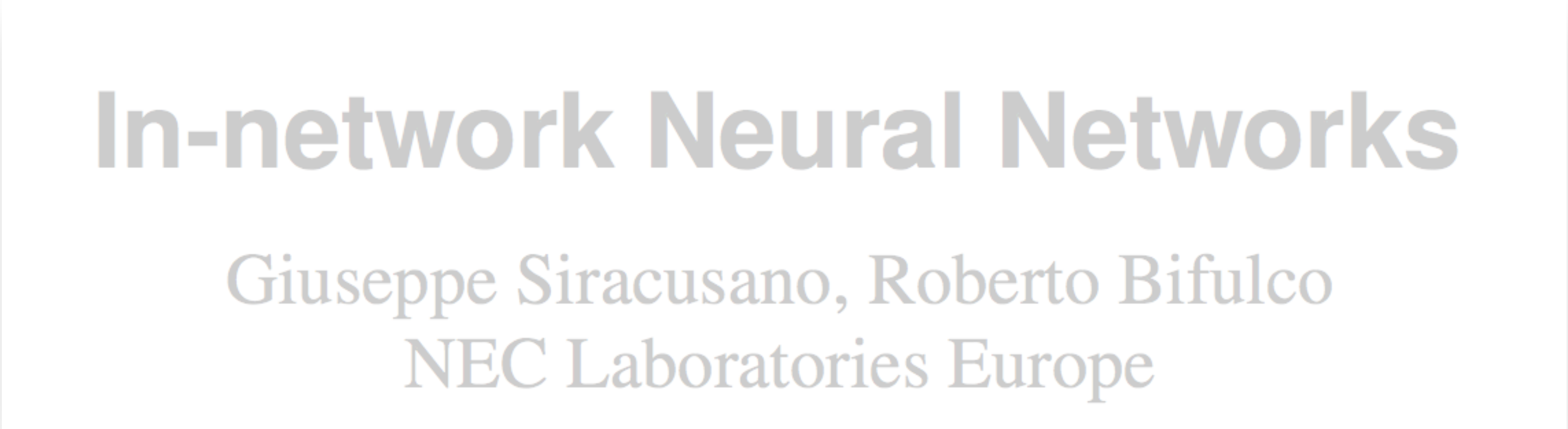


Hardware-Accelerated Network Control Planes

Edgar Costa Molero
ETH Zürich
cedgar@ethz.ch

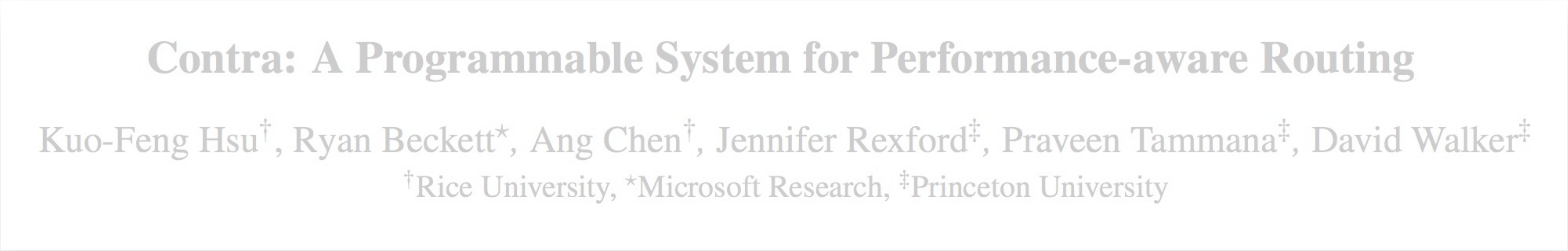
Stefano Vissicchio
University College London
s.vissicchio@cs.ucl.ac.uk

Laurent Vanbever
ETH Zürich
lvanbever@ethz.ch



In-network Neural Networks

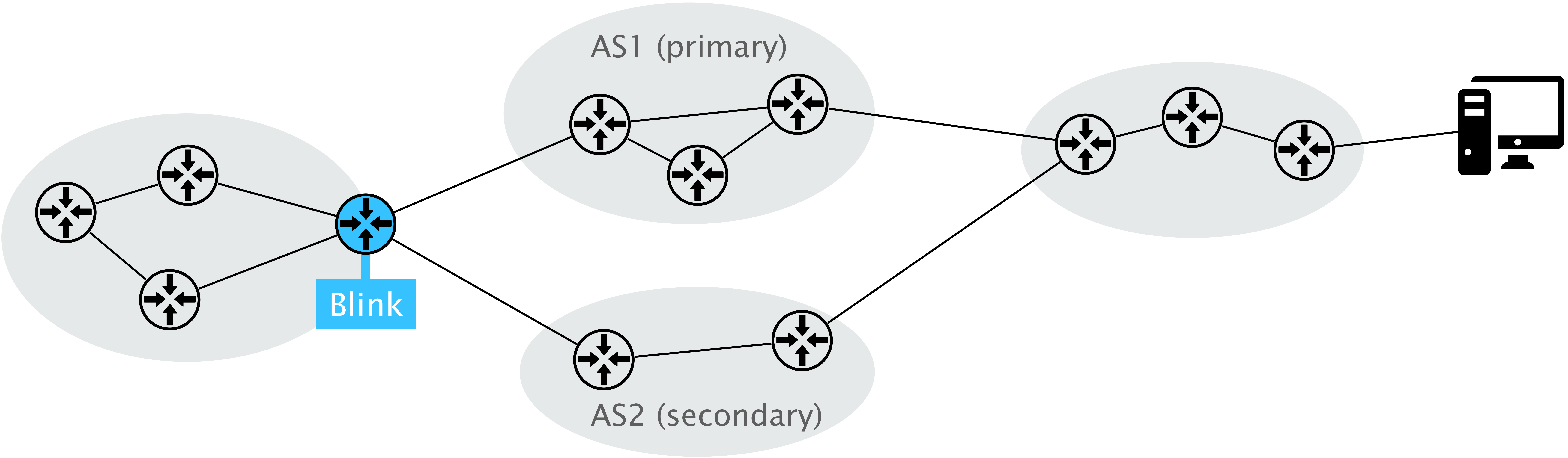
Giuseppe Siracusano, Roberto Bifulco
NEC Laboratories Europe



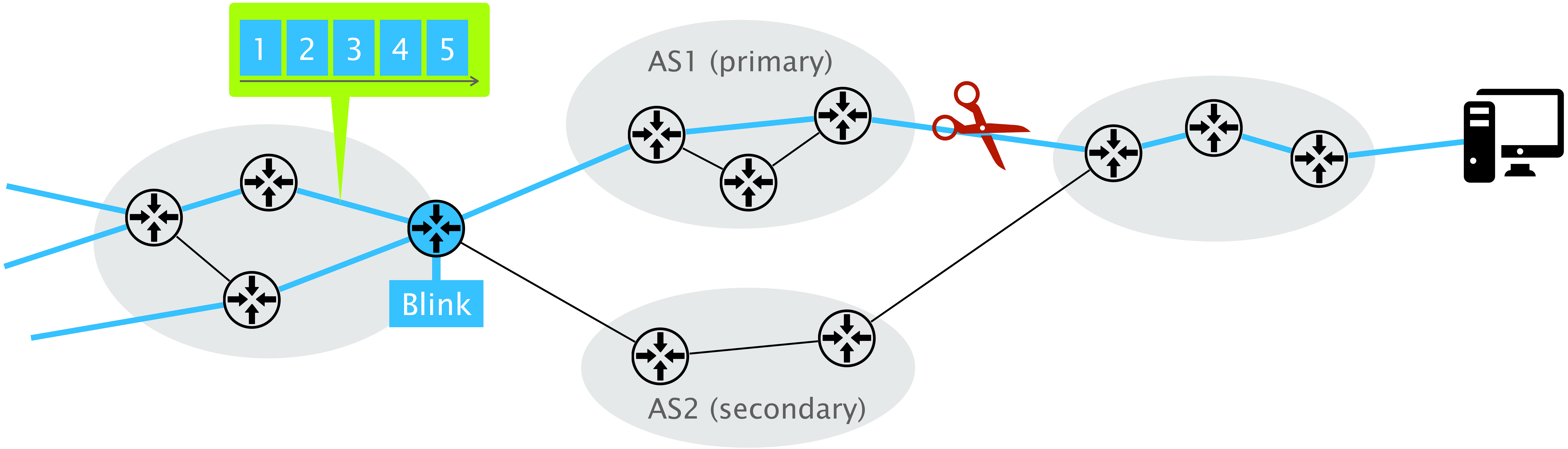
Contra: A Programmable System for Performance-aware Routing

Kuo-Feng Hsu†, Ryan Beckett*, Ang Chen†, Jennifer Rexford‡, Praveen Tammana‡, David Walker‡
†Rice University, *Microsoft Research, ‡Princeton University

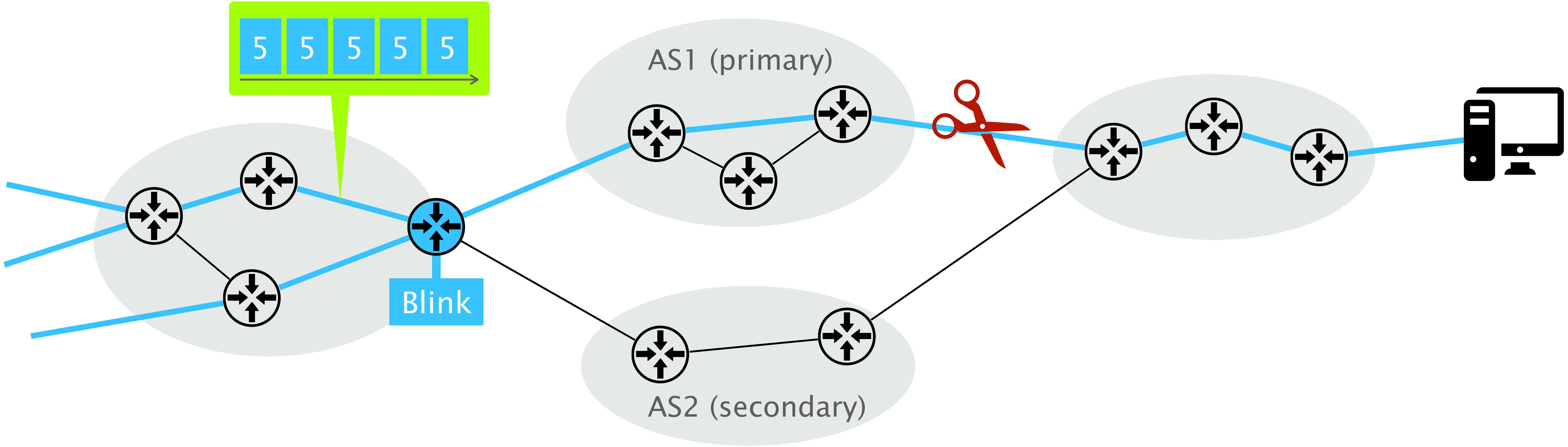
# Blink monitors TCP retransmissions to detect failed paths



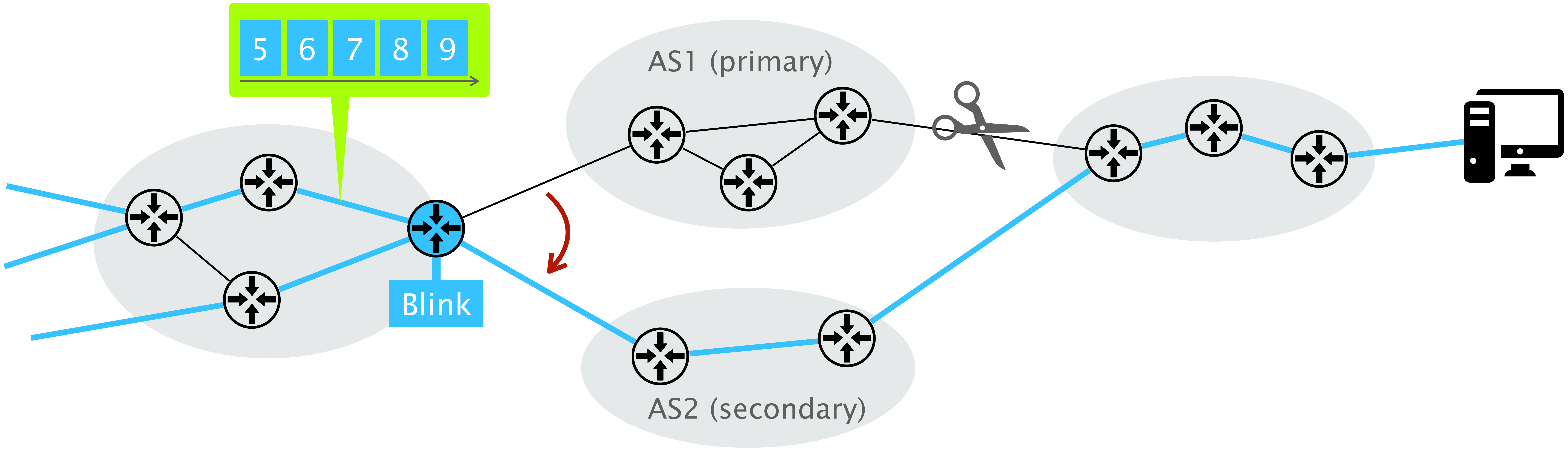
# Blink monitors TCP retransmissions to detect failed paths



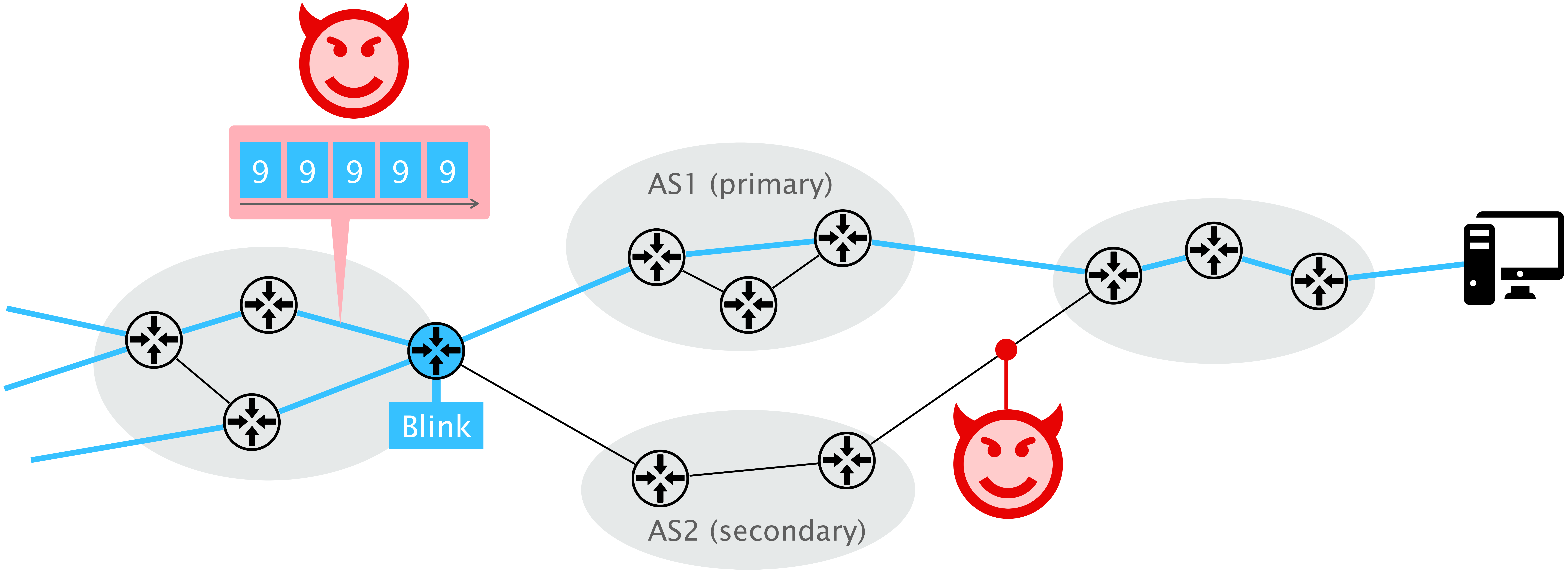
# Blink monitors TCP retransmissions to detect failed paths



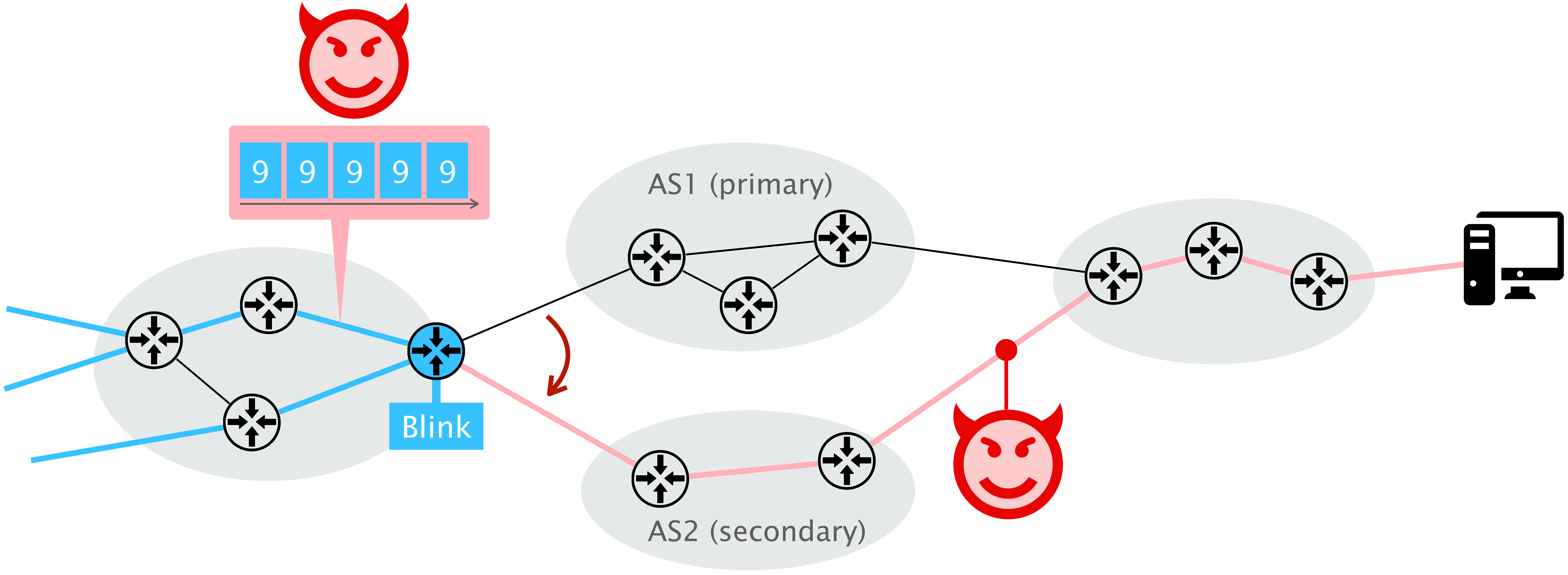
# Blink monitors TCP retransmissions to detect failed paths



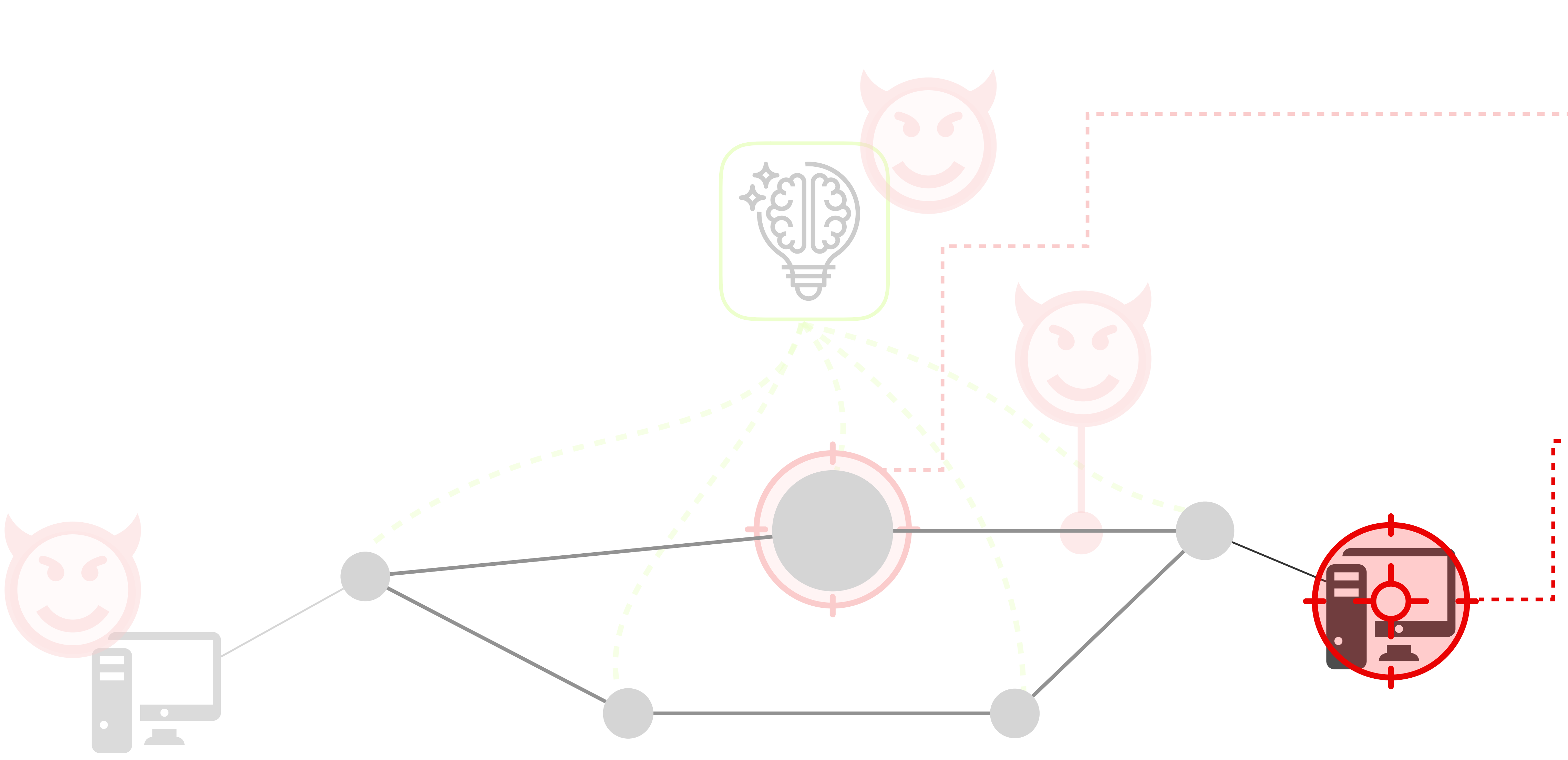
# Blink monitors TCP retransmissions to detect failed paths



# Blink monitors TCP retransmissions to detect failed paths



# We distinguish between two attack targets



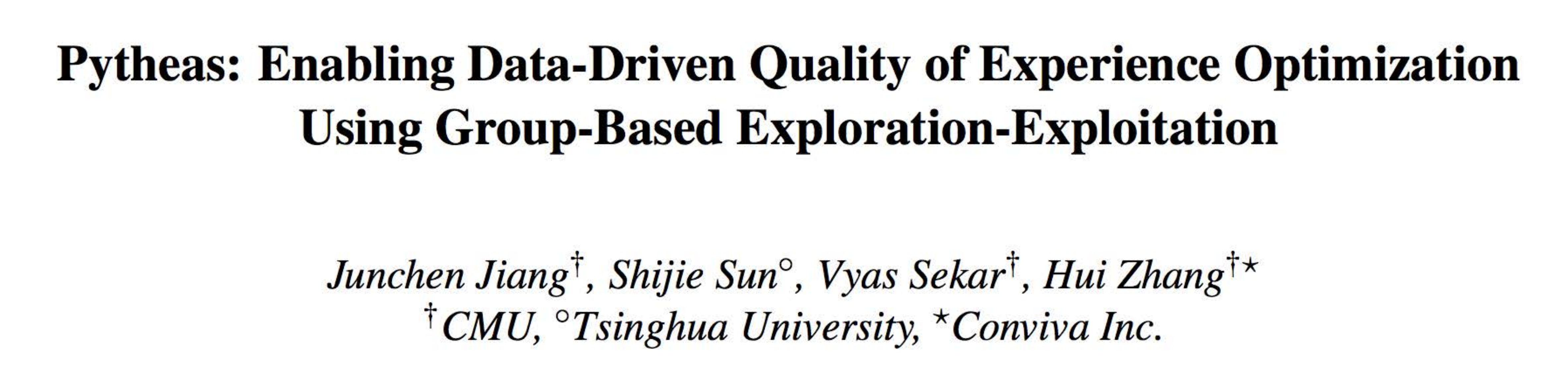
Network infrastructure

E.g., forwarding behavior

Endpoints

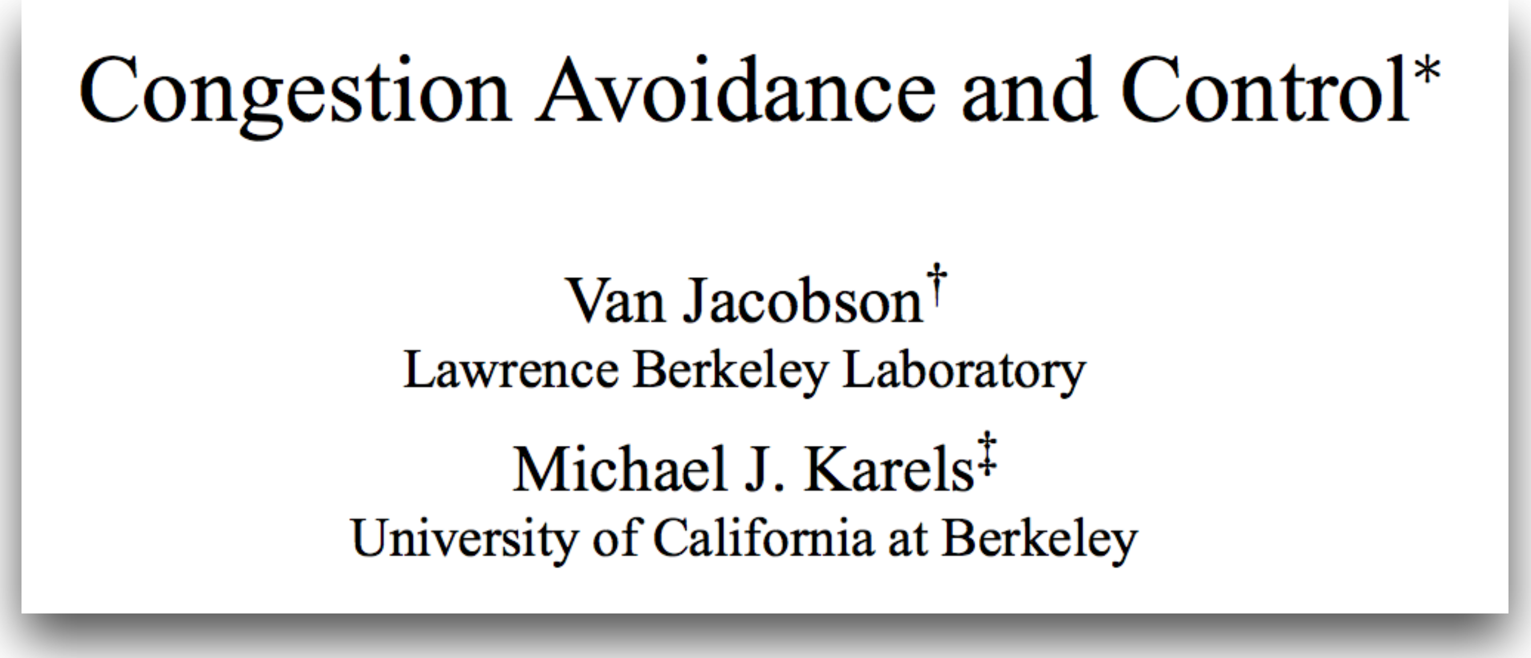
E.g., applications

# Many host-based protocols and applications rely on feedback from the network



**Pytheas: Enabling Data-Driven Quality of Experience Optimization Using Group-Based Exploration-Exploitation**

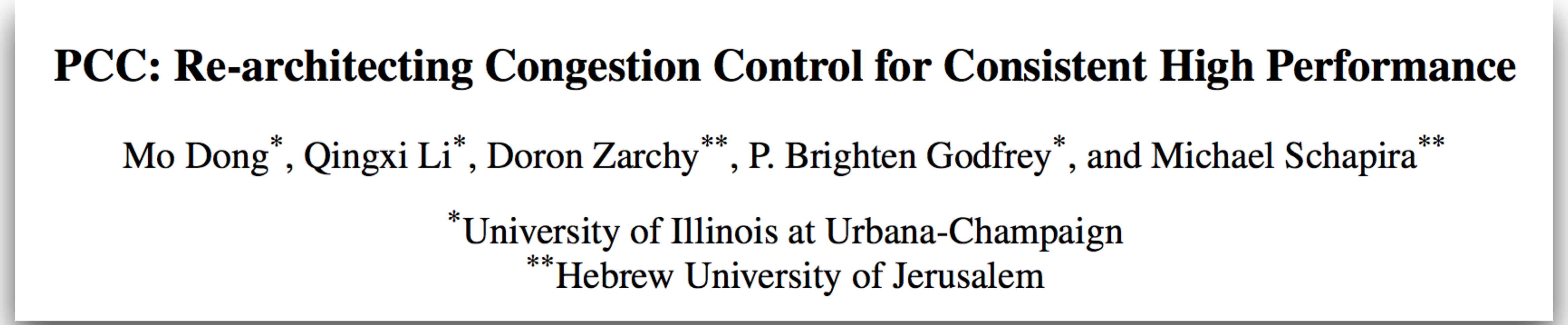
*Junchen Jiang[†], Shijie Sun[°], Vyas Sekar[†], Hui Zhang[†⋆]*
*[†]CMU, [°]Tsinghua University, [⋆]Conviva Inc.*



Congestion Avoidance and Control[*]

Van Jacobson[†]
Lawrence Berkeley Laboratory

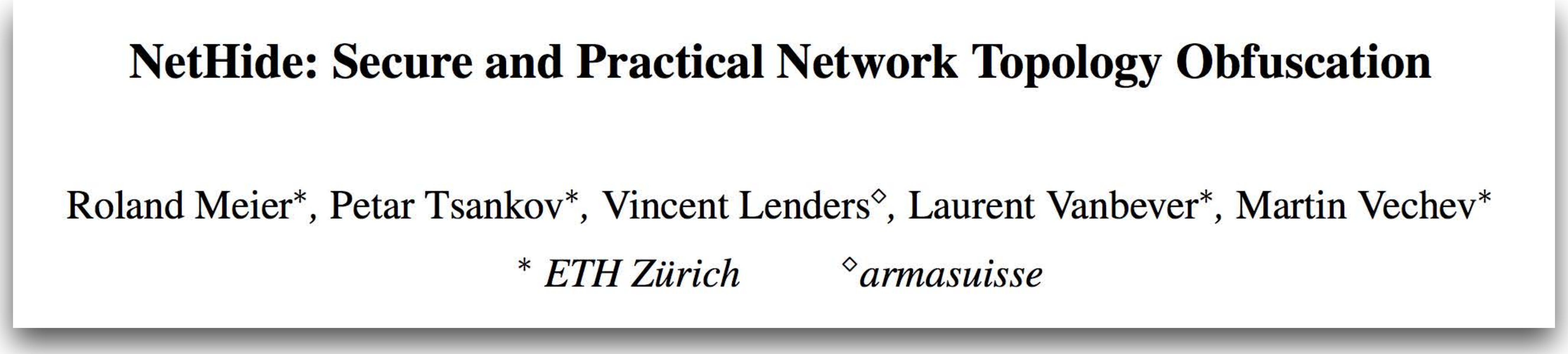
Michael J. Karels[‡]
University of California at Berkeley



**PCC: Re-architecting Congestion Control for Consistent High Performance**

Mo Dong[*], Qingxi Li[*], Doron Zarchy[**], P. Brighten Godfrey[*], and Michael Schapira[**]

[*]University of Illinois at Urbana-Champaign
[**]Hebrew University of Jerusalem



**NetHide: Secure and Practical Network Topology Obfuscation**

Roland Meier[*], Petar Tsankov[*], Vincent Lenders[◇], Laurent Vanbever[*], Martin Vechev[*]

[*] *ETH Zürich* [◇]*armasuisse*

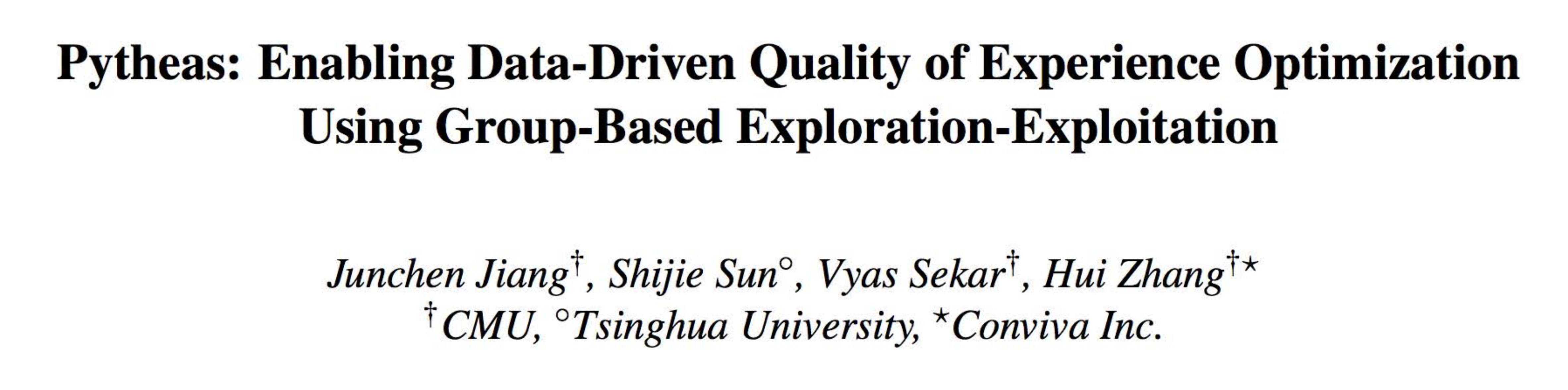
# Protocols and applications depend on different types of inputs

| | Host | MitM | Operator |
|---|---|---|---|
| ▪ Headers<br>e.g., sequence numbers | 😈 | 😈 | 😈 |
| ▪ Metadata<br>e.g., timing | 😈 | 😈 | 😈 |
| ▪ Payload<br>e.g., QoE | 😈 | 👿 | 👿 |

# Adversarial inputs to endpoints and applications can have big consequences

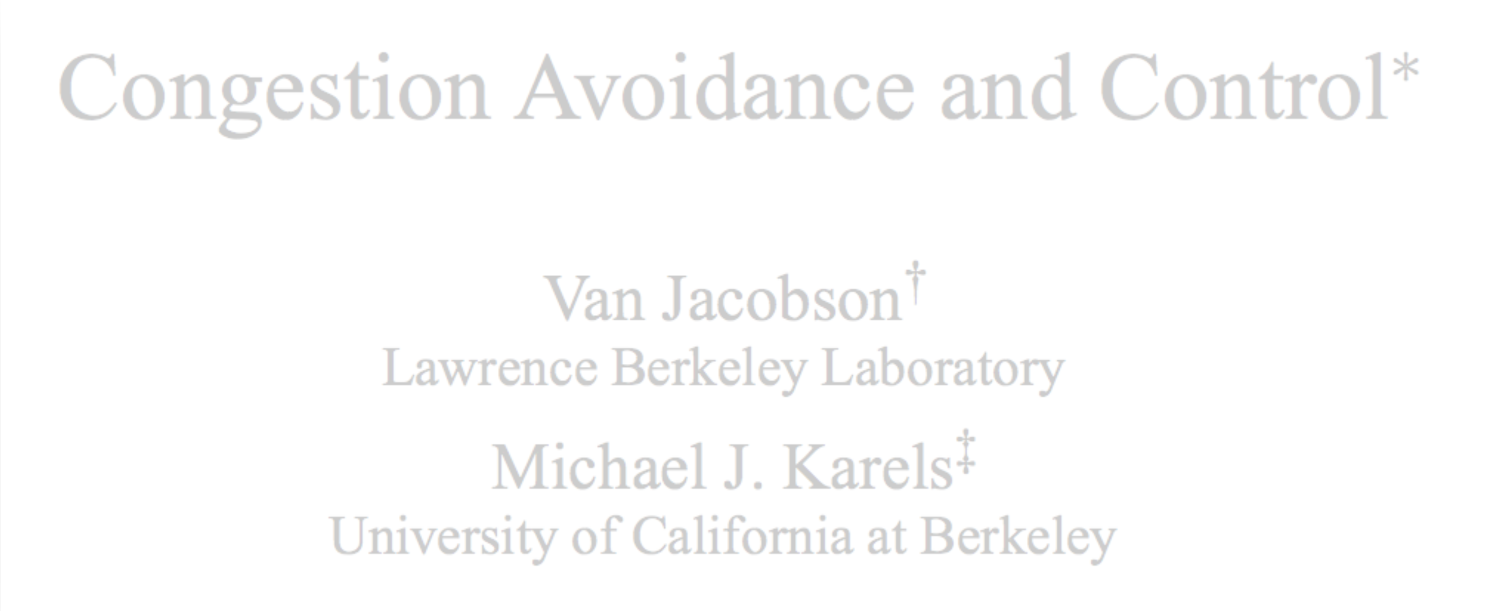
- Security and privacy issues
  e.g., modified addresses
- Loss of situational awareness
  e.g., manipulated measurements
- Performance degradation
  e.g., faked congestion
- Broken debugging tools
  e.g., manipulated ICMP messages

# Many host-based protocols and applications rely on feedback from the network



**Pytheas: Enabling Data-Driven Quality of Experience Optimization Using Group-Based Exploration-Exploitation**

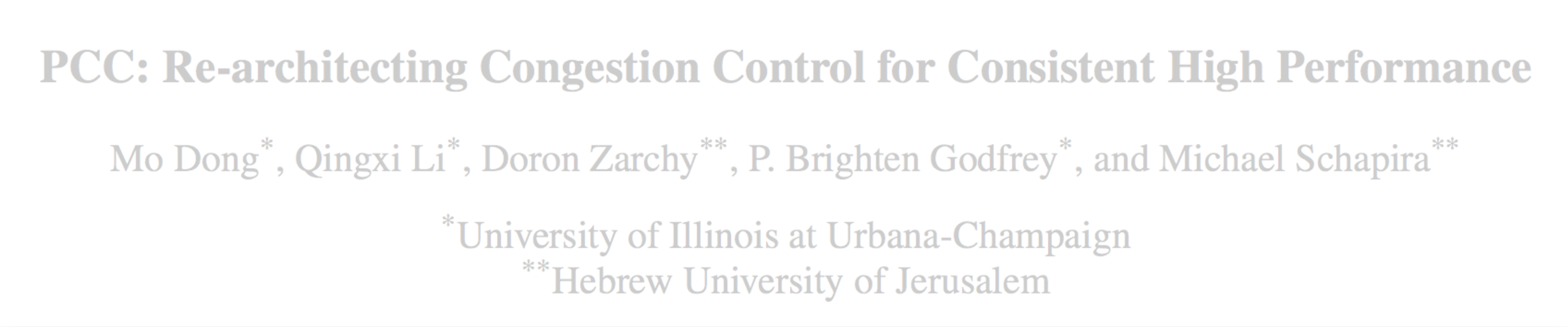
*Junchen Jiang[†], Shijie Sun[°], Vyas Sekar[†], Hui Zhang[†⋆]*
*[†]CMU, [°]Tsinghua University, [⋆]Conviva Inc.*



Congestion Avoidance and Control[*]

Van Jacobson[†]
Lawrence Berkeley Laboratory

Michael J. Karels[‡]
University of California at Berkeley



**PCC: Re-architecting Congestion Control for Consistent High Performance**

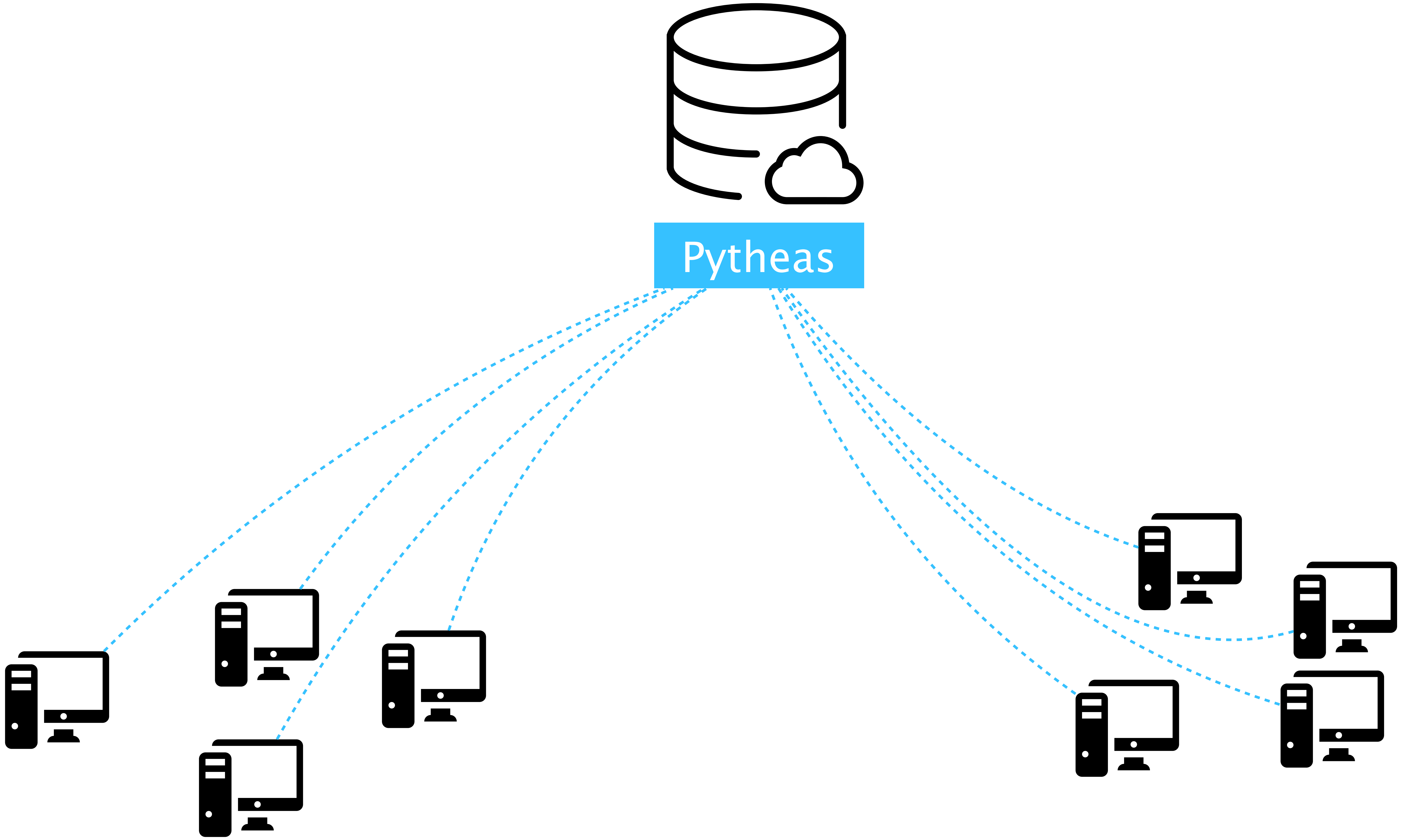
Mo Dong[*], Qingxi Li[*], Doron Zarchy[**], P. Brighten Godfrey[*], and Michael Schapira[**]

[*]University of Illinois at Urbana-Champaign
[**]Hebrew University of Jerusalem

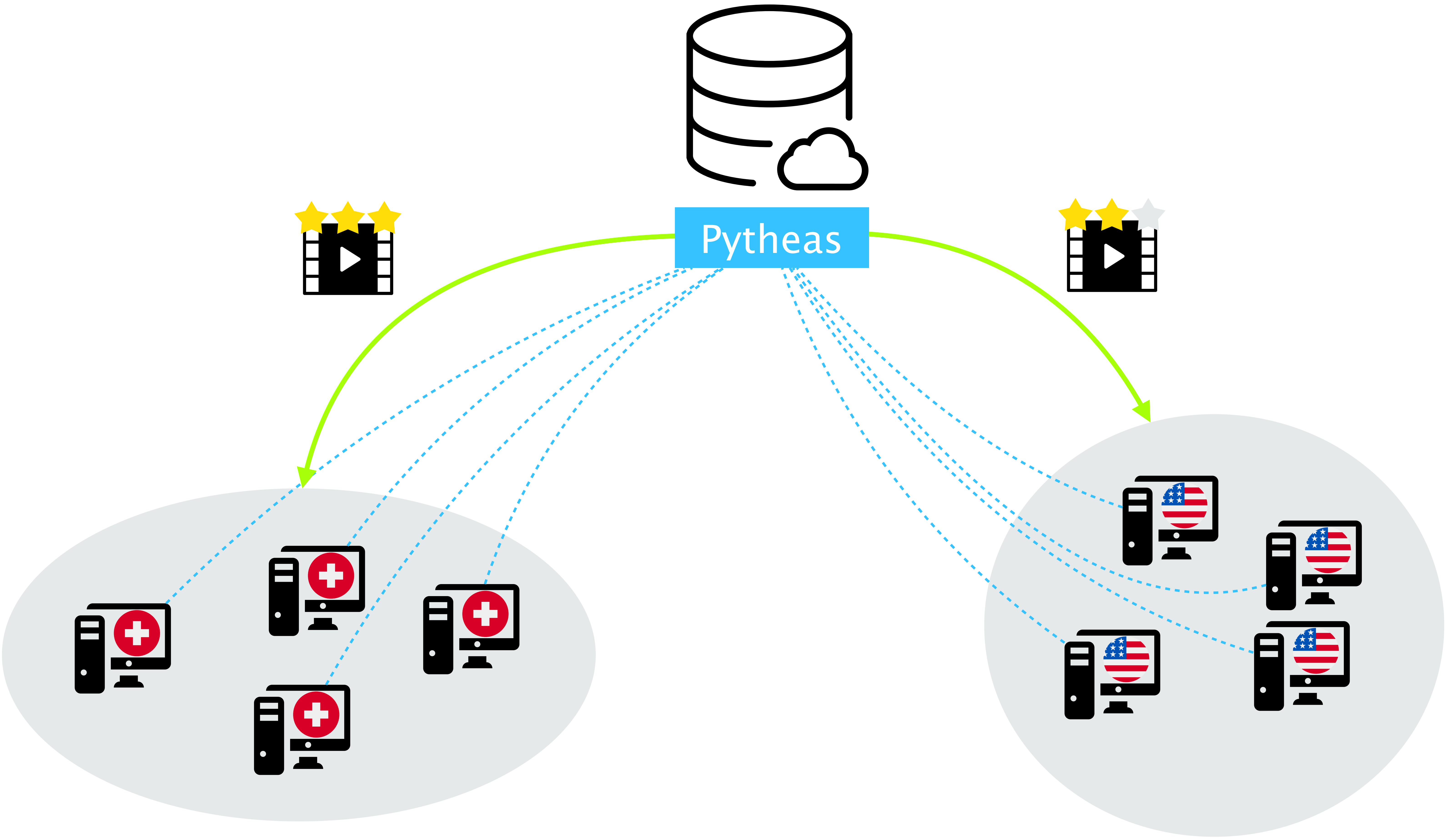
**NetHide: Secure and Practical Network Topology Obfuscation**

Roland Meier[*], Petar Tsankov[*], Vincent Lenders[◇], Laurent Vanbever[*], Martin Vechev[*]
[*] *ETH Zürich* [◇]*armasuisse*

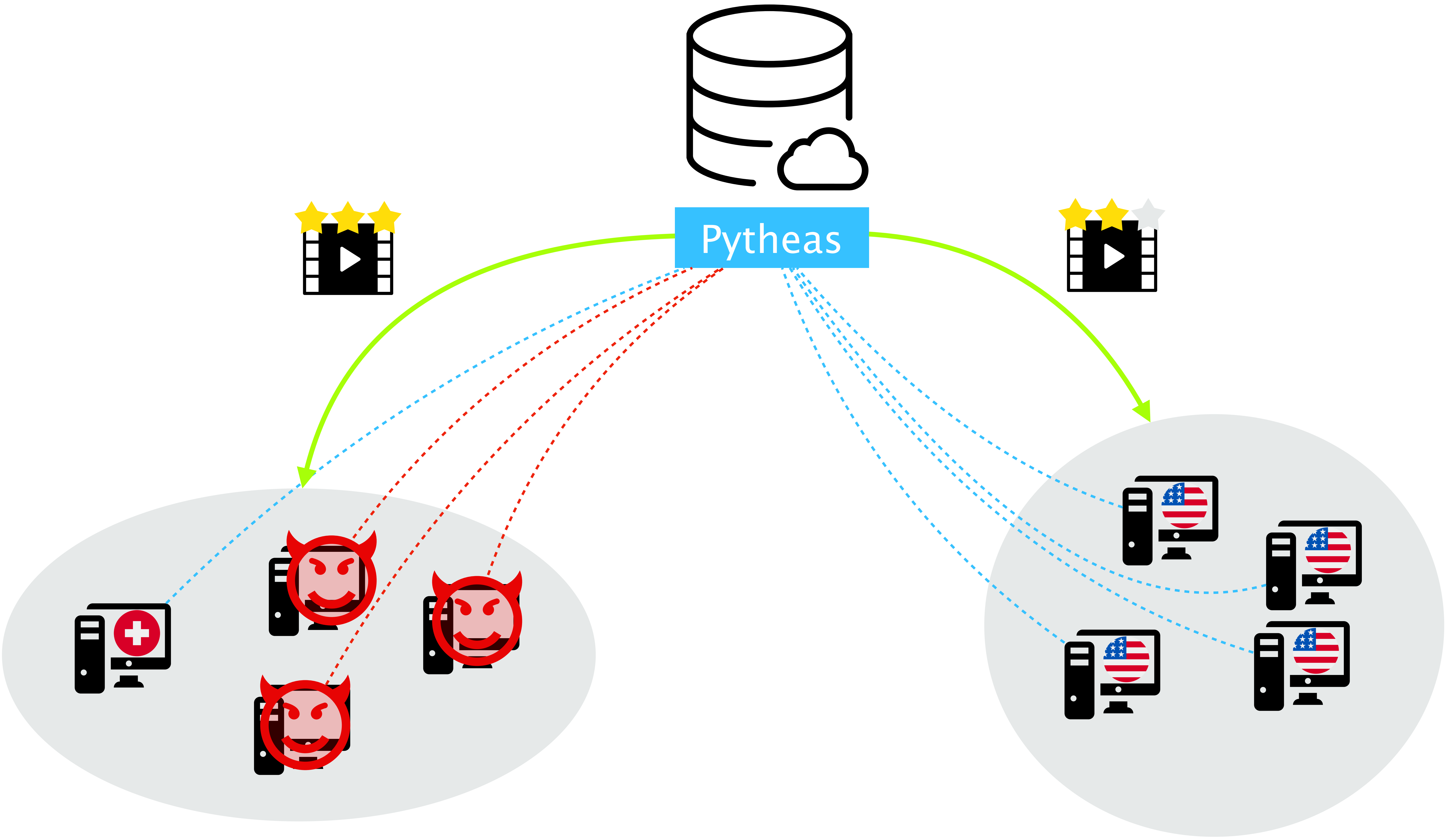
# Pytheas performs QoE optimization through a real-time exploration and exploitation process



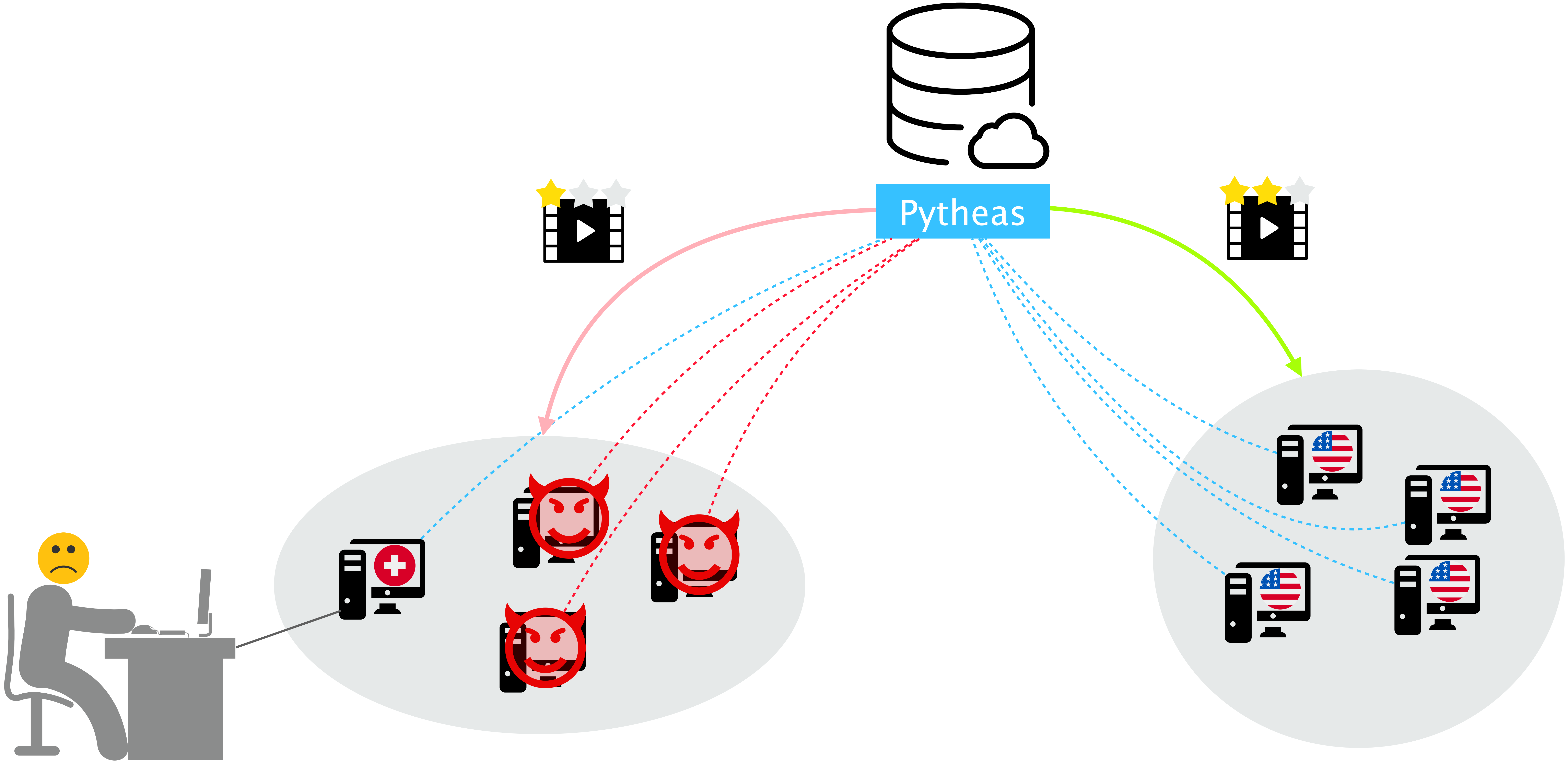
# Pytheas performs QoE optimization through a real-time exploration and exploitation process



# An adversary can report wrong data to Pytheas



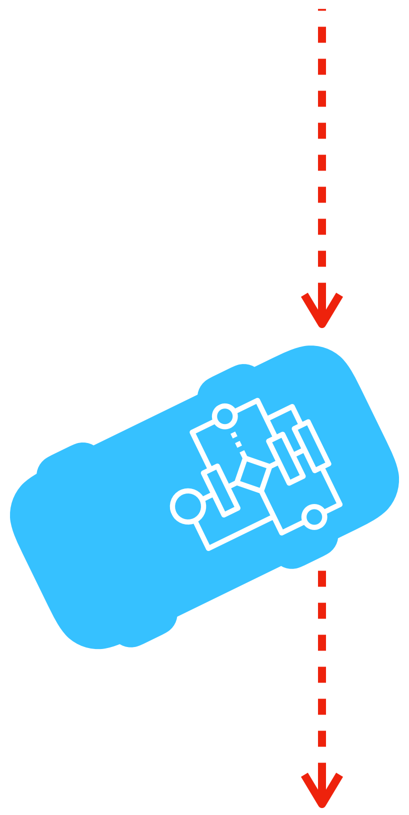
# Adversarial inputs from some clients in a group can lower QoE for the other clients in the same group



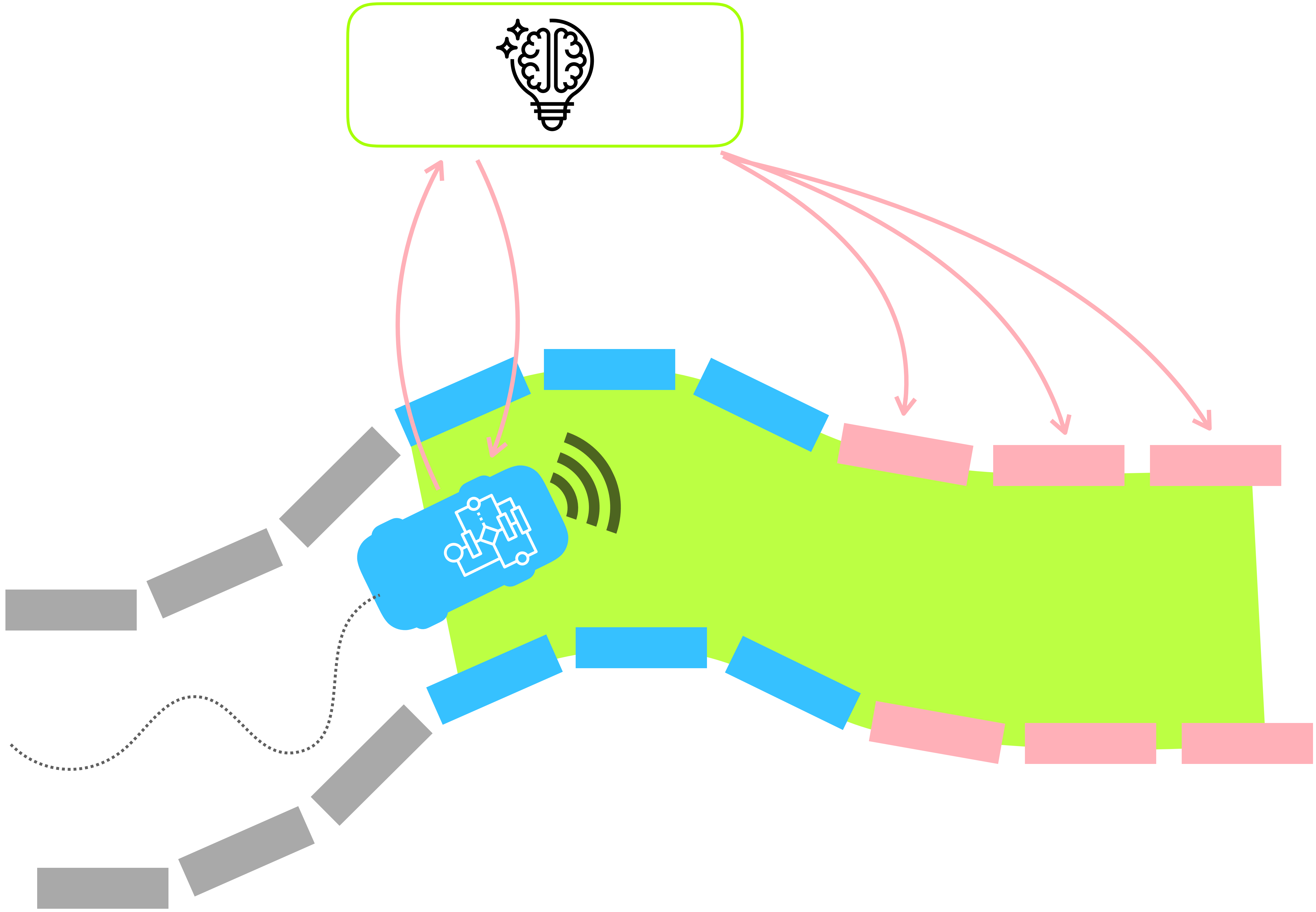
*Attacking*
self-driving networks

*Defending*
self-driving networks

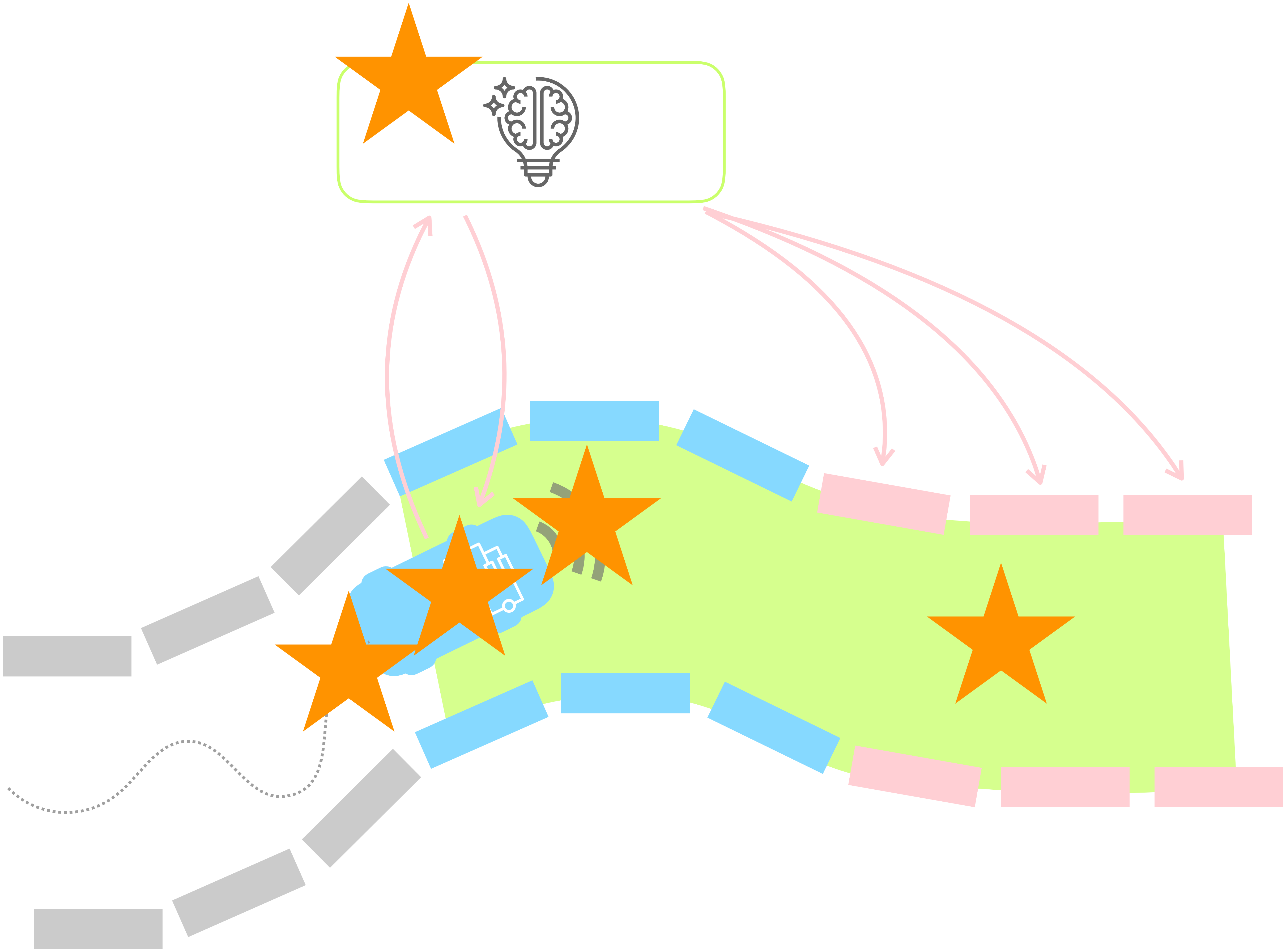
Let this car be our self-driving ~~car~~ network



How can we protect it?

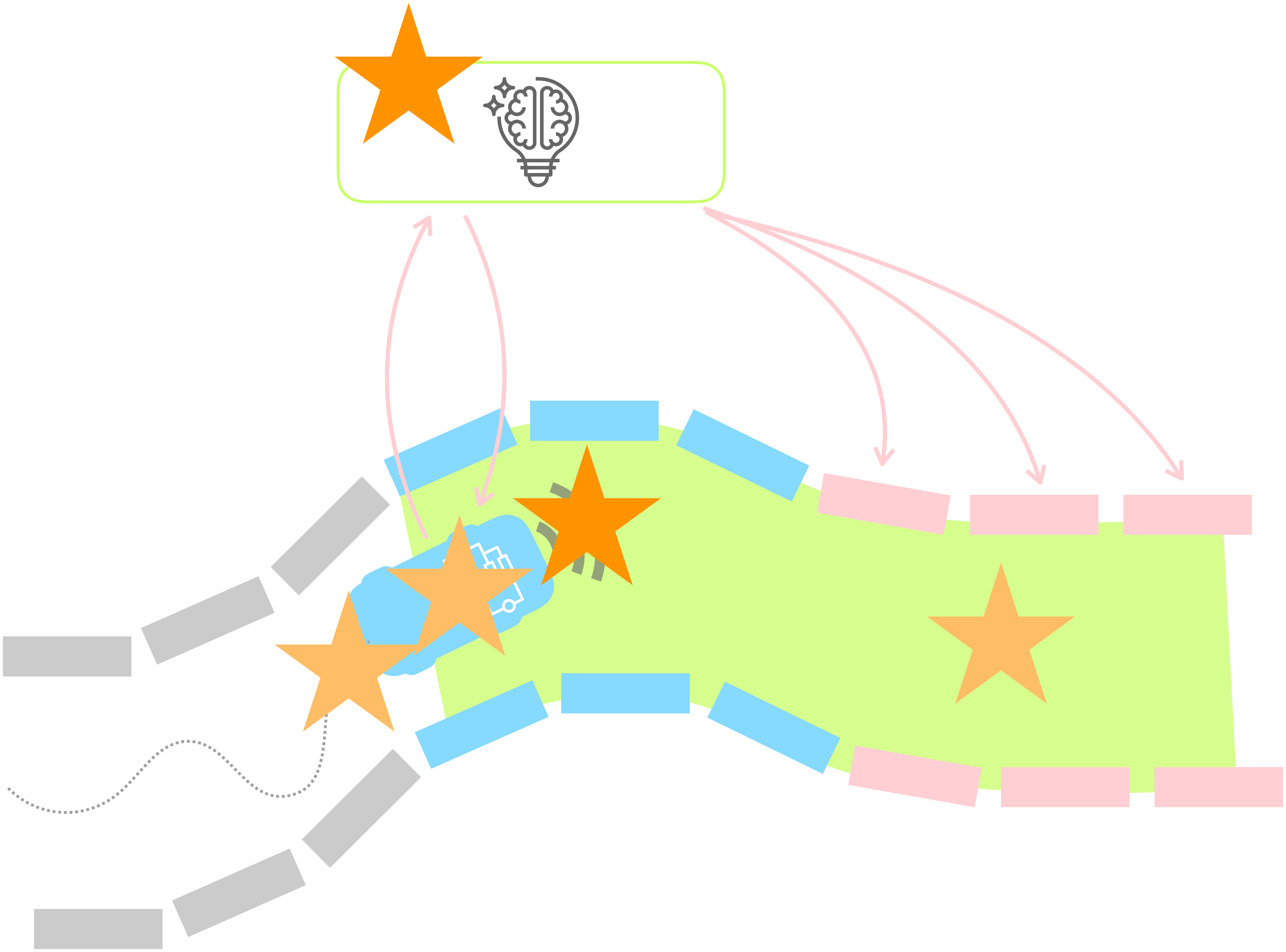


# Countermeasures can be applied at different points



- ★ Program testing
- ★ Program obfuscation
- ★ Input verification
- ★ State modeling
- ★ Behavior monitoring

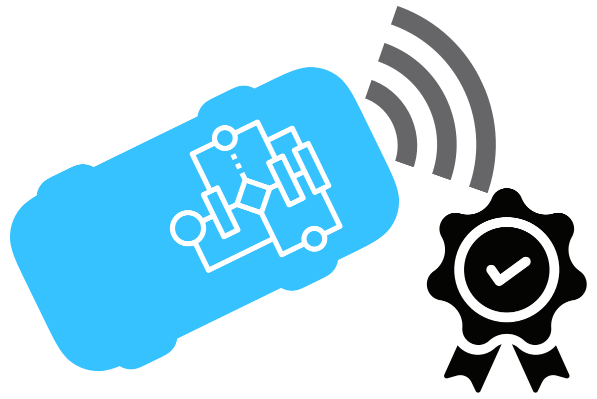
# Countermeasures can be applied at different points



- ★ Program testing
- ★ Program obfuscation
- ★ Input verification
- ★ State modeling
- ★ Behavior monitoring

# Ensuring input quality makes it harder to feed adversarial inputs

Possible approaches

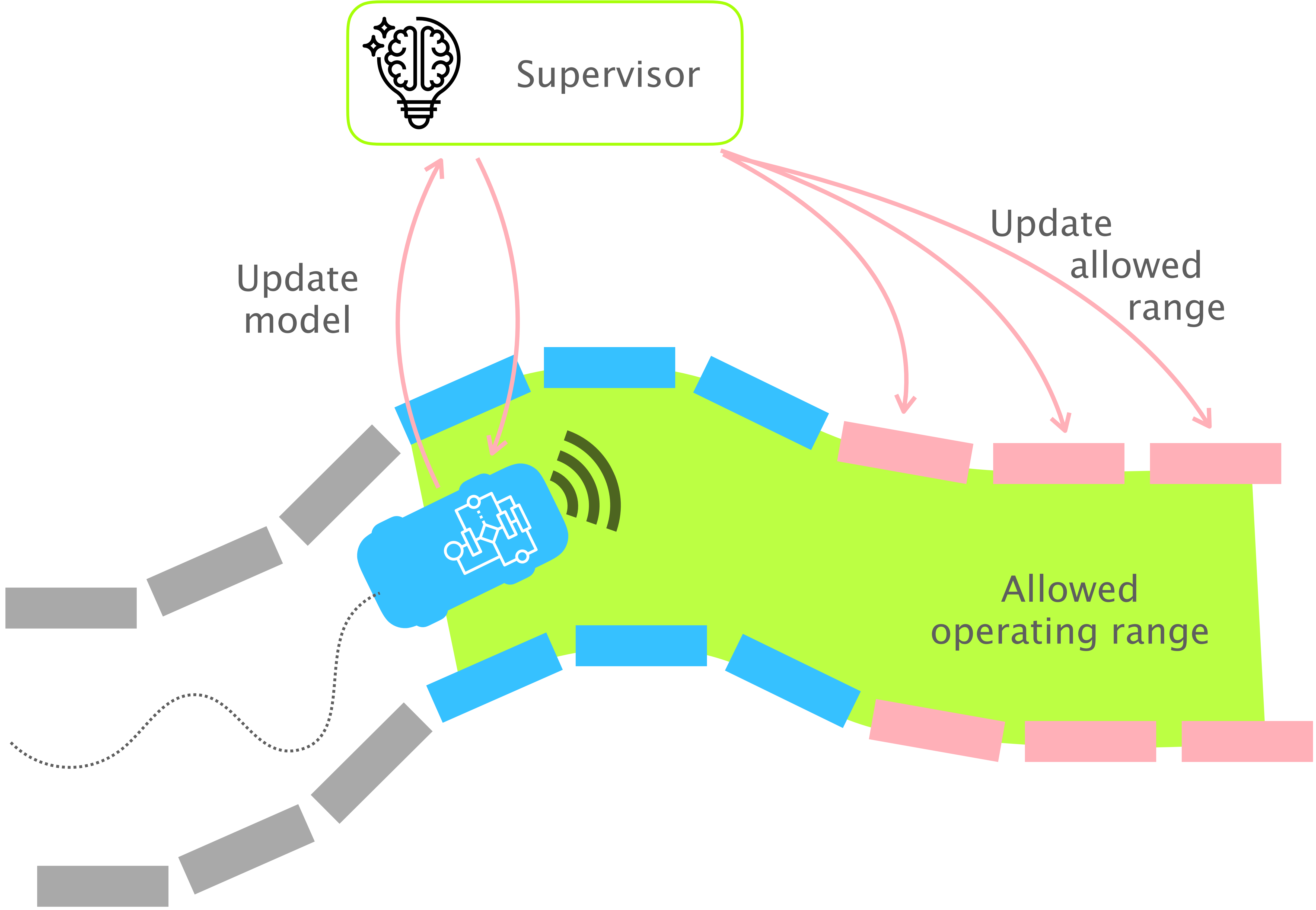


- Cryptography
  encryption or authentication
- Diversity
  use multiple, independent signals
- Verification
  verify legitimacy of signals

*Research question:*

Where is the sweet spot for maximizing input quality given the cost of modifying existing protocols, modifying applications, and impact on decision time?

# Invoking supervisor checks allows checks without degrading performance



- Supervisor runs “offline”
  more flexibility
- Driver gets some freedom
  to choose next state
- Driver is limited
  to plausible next states

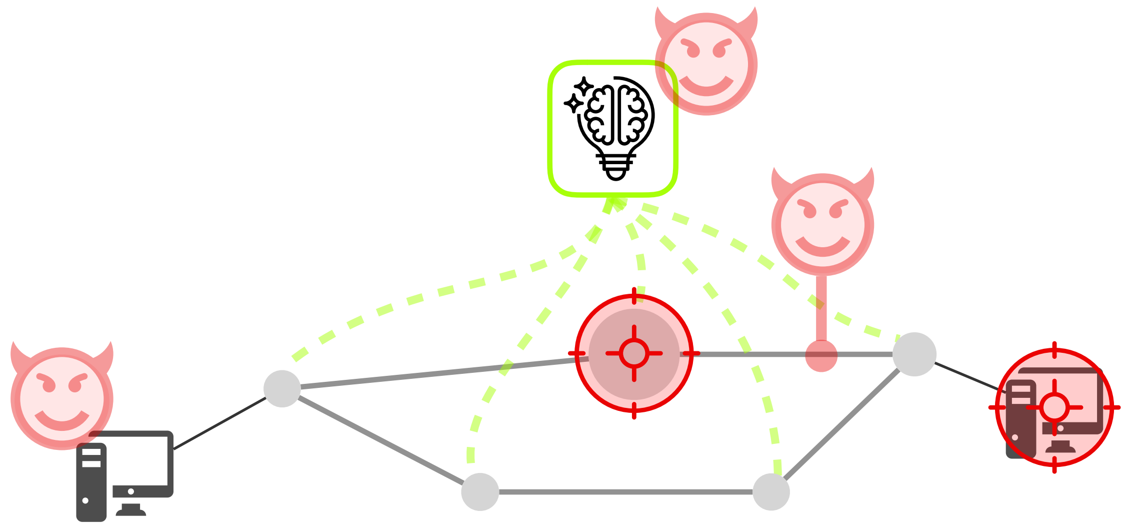
*Research question:*

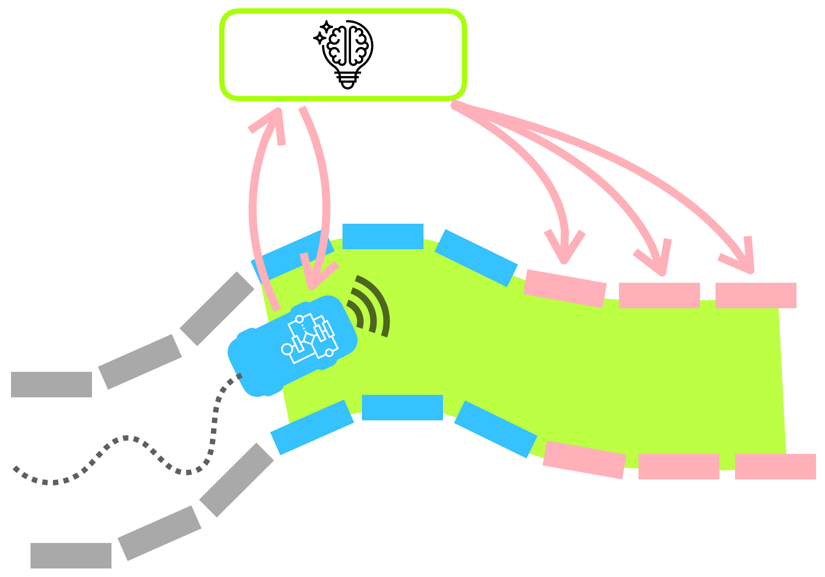
How does an efficient driver-supervisor interface look like, and how do we trade off fast, asynchronous operation against delays in enforcing safety?

# (Self) Driving Under the Influence: Intoxicating Adversarial Network Inputs

*Attacking*
self-driving networks

*Defending*
self-driving networks





Roland Meier
meierrol@ethz.ch
nsg.ee.ethz.ch

# ETH Zürich is hiring at all levels

Contact Laurent Vanbever (lvanbever@ethz.ch)

Professor/Assistant Professor (Tenure Track) of Cyber-Physical and Embedded Systems

+ PhD & post-doc positions in networking

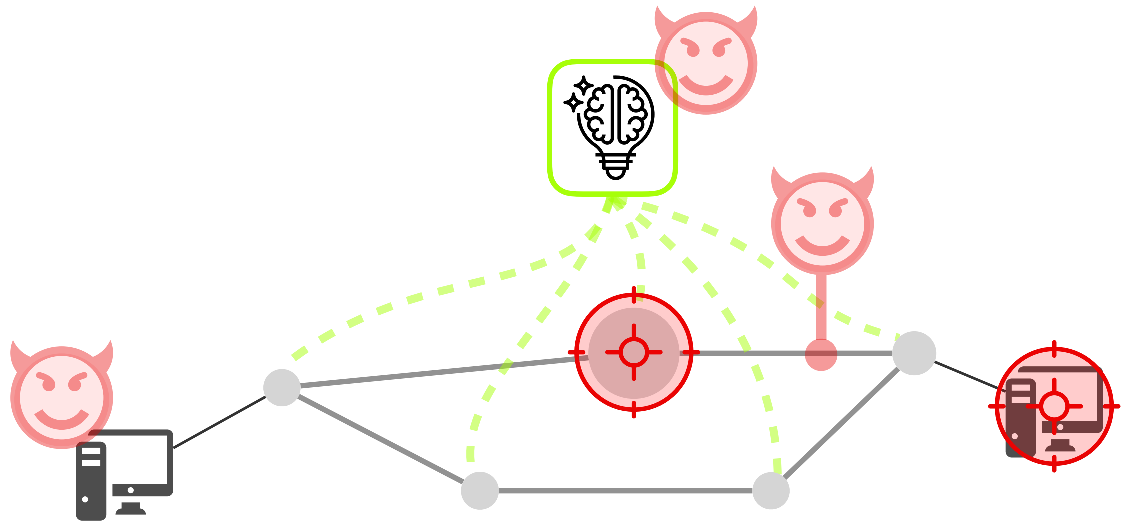
# (Self) Driving Under the Influence: Intoxicating Adversarial Network Inputs

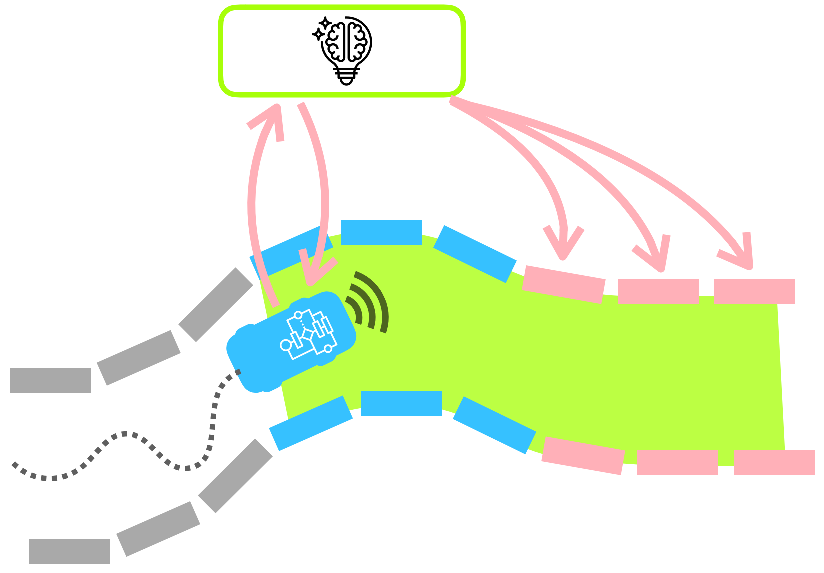
*Attacking*

self-driving networks

*Defending*

self-driving networks





Roland Meier
meierrol@ethz.ch
nsg.ee.ethz.ch