TARANET: Traffic-Analysis Resistant Anonymity at the Network Layer

Chen Chen *(CMU)*, **Daniele E. Asoni**, Adrian Perrig *(ETH Zürich)*,
David Barrera *(Polytechnique Montreal)*,
George Danezis *(UCL)*, Carmela Troncoso *(EPFL)*

Our vision:

An Internet that hides communication metadata

Our vision:

An Internet that hides communication metadata

Anonymous communication

Our vision:

An Internet that hides communication metadata

Anonymous communication

- Non-discrimination

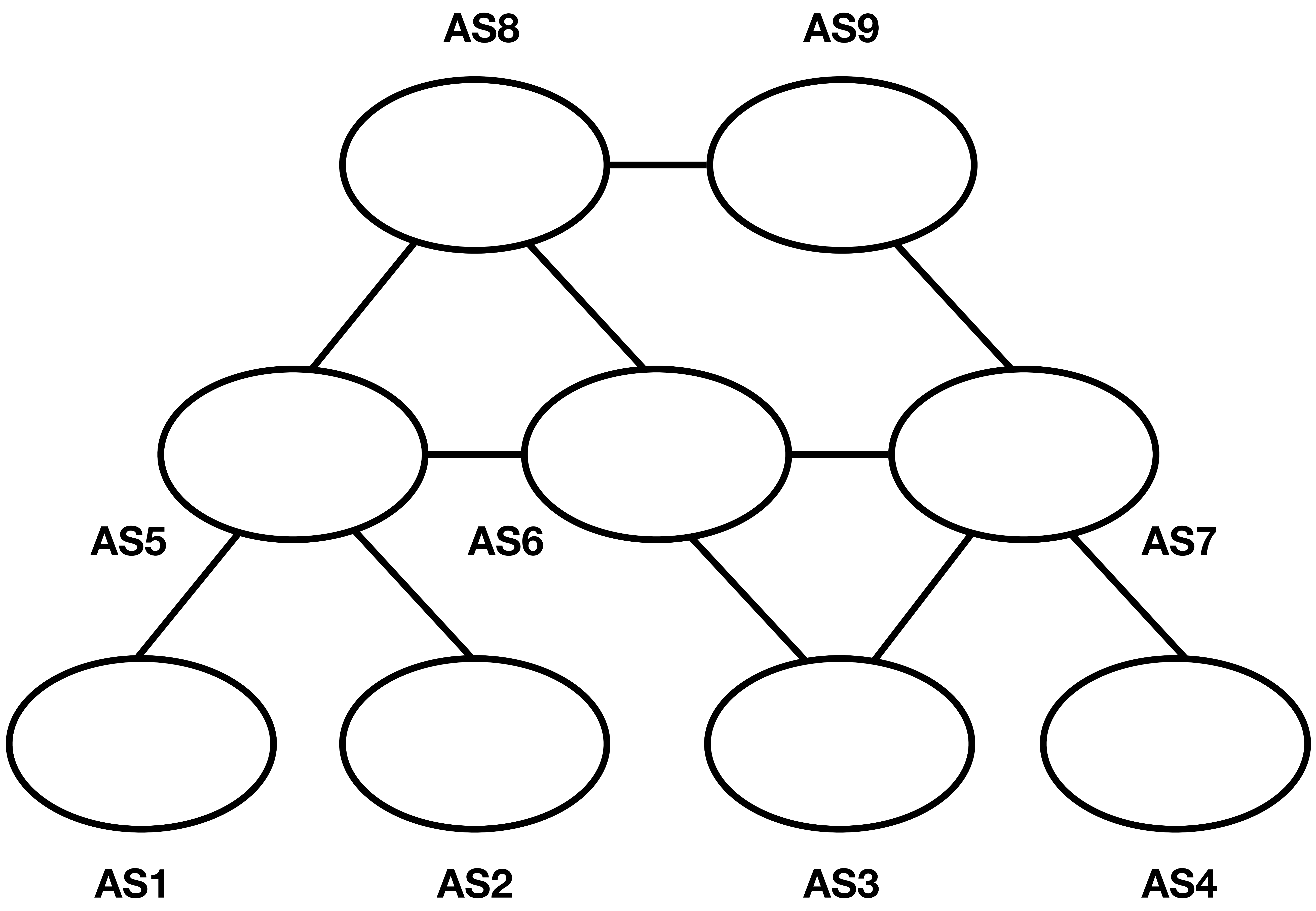
Our vision:

An Internet that hides communication metadata

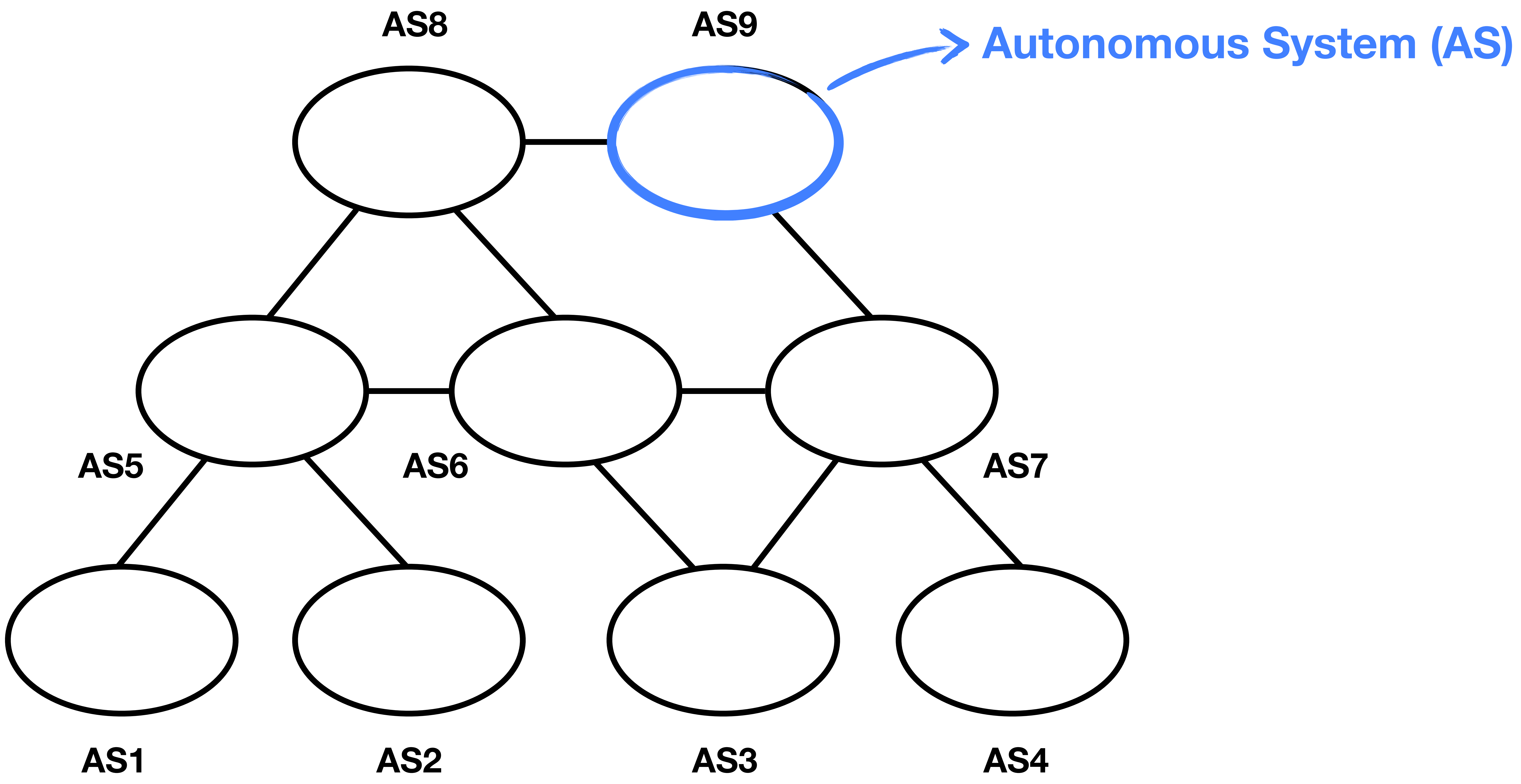
Anonymous communication

- Non-discrimination
- Prevent industrial espionage

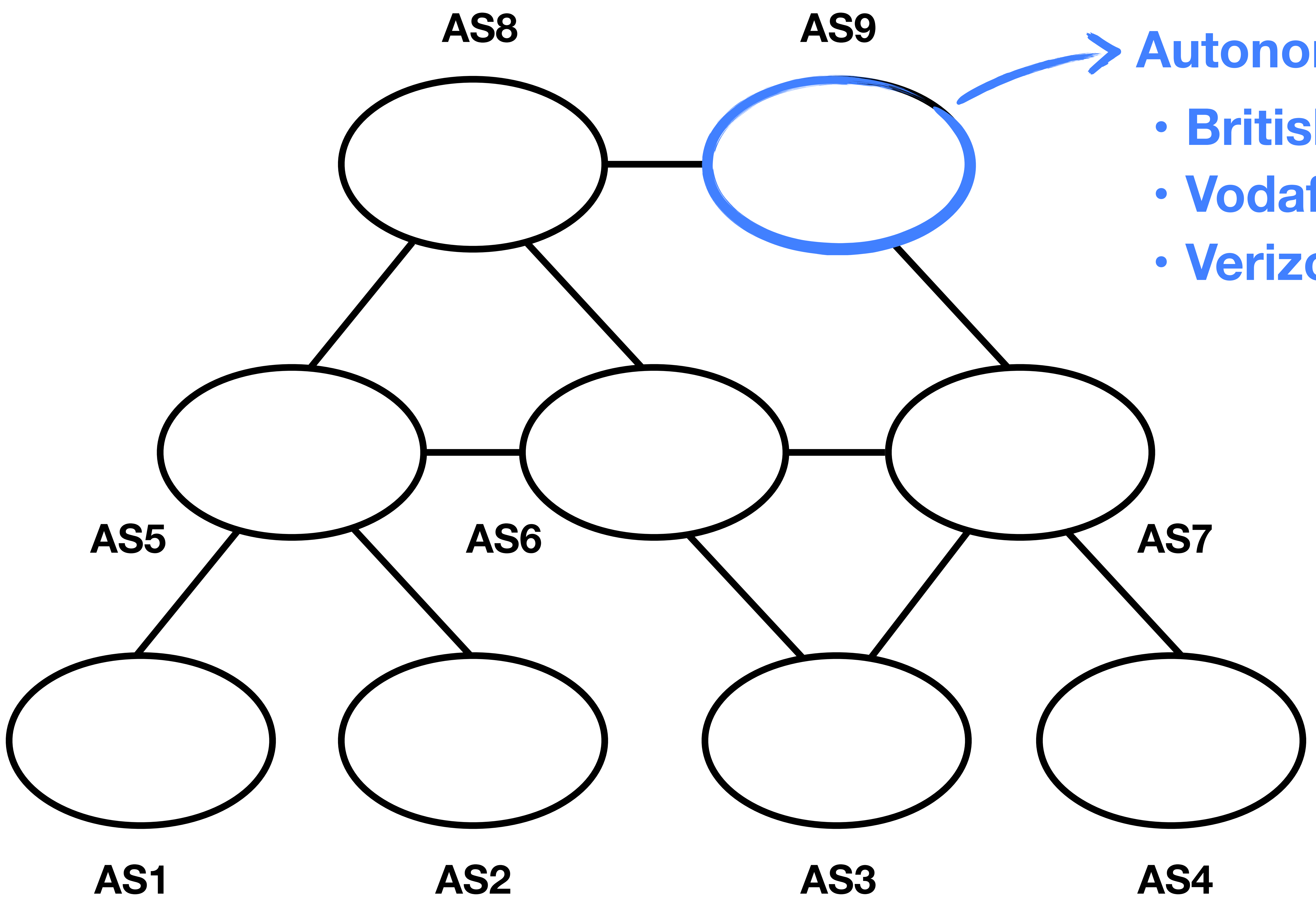
Network-layer anonymity



Network-layer anonymity



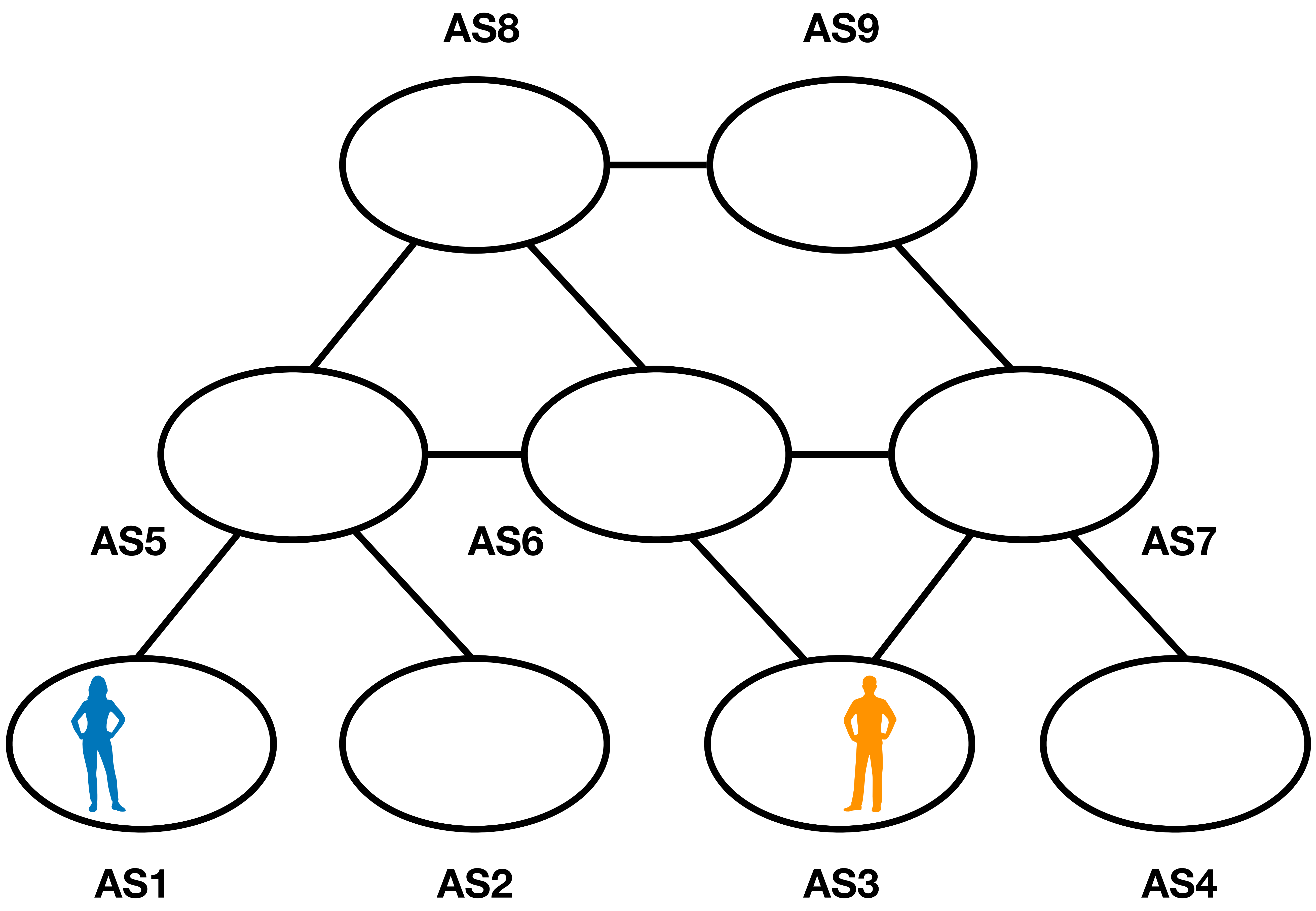
Network-layer anonymity



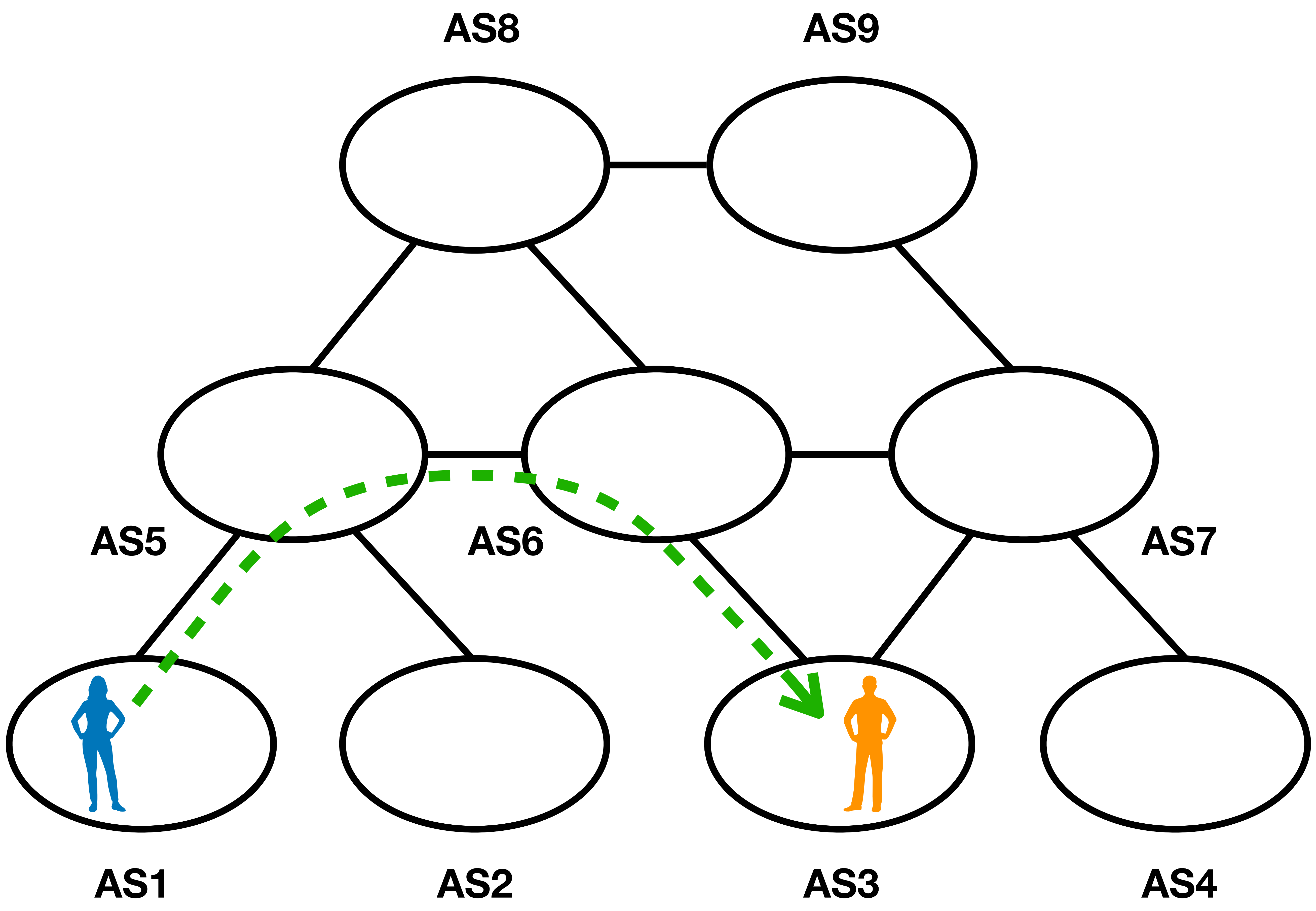
Autonomous System (AS)

- British Telecom
- Vodafone
- Verizon

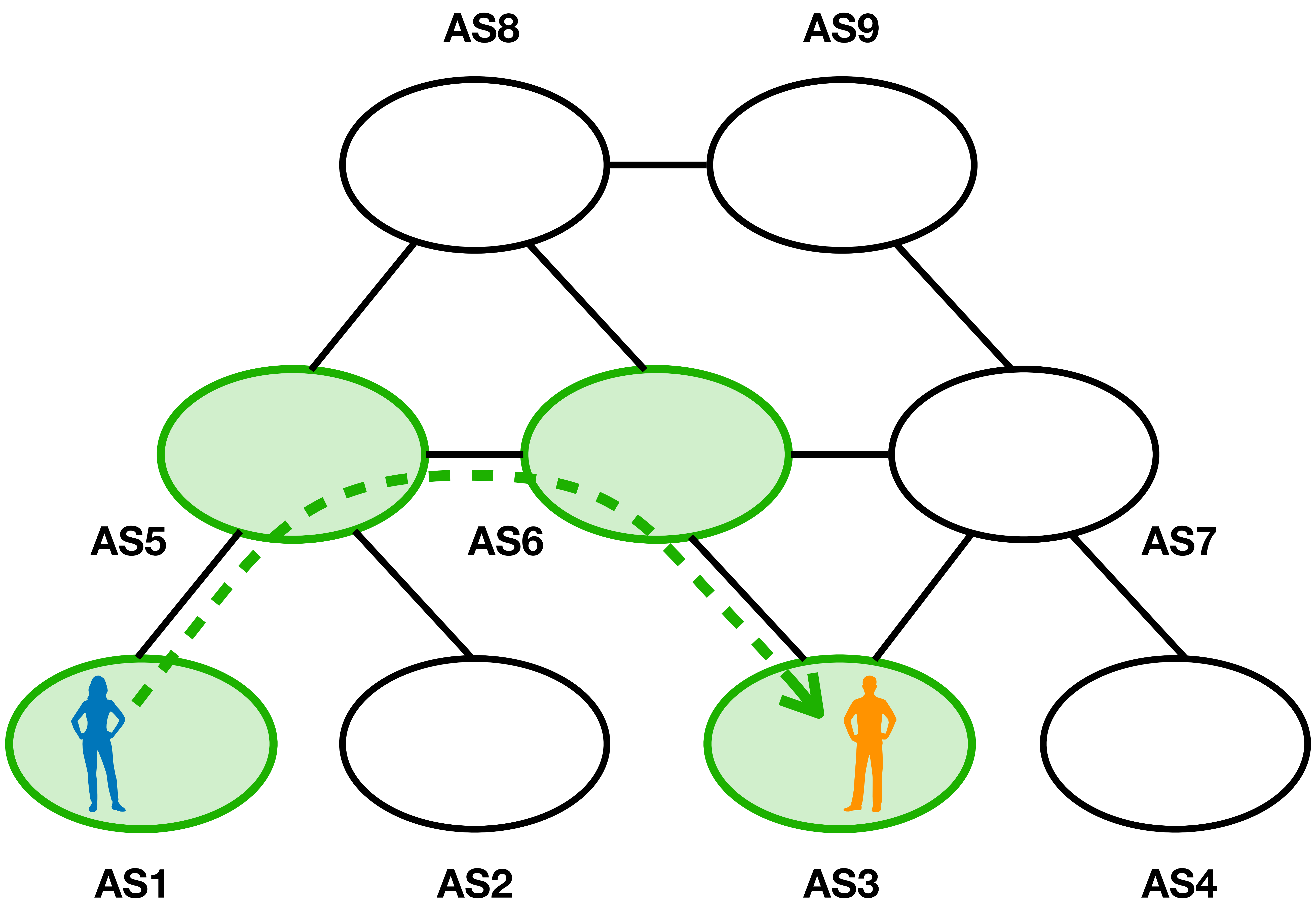
Network-layer anonymity



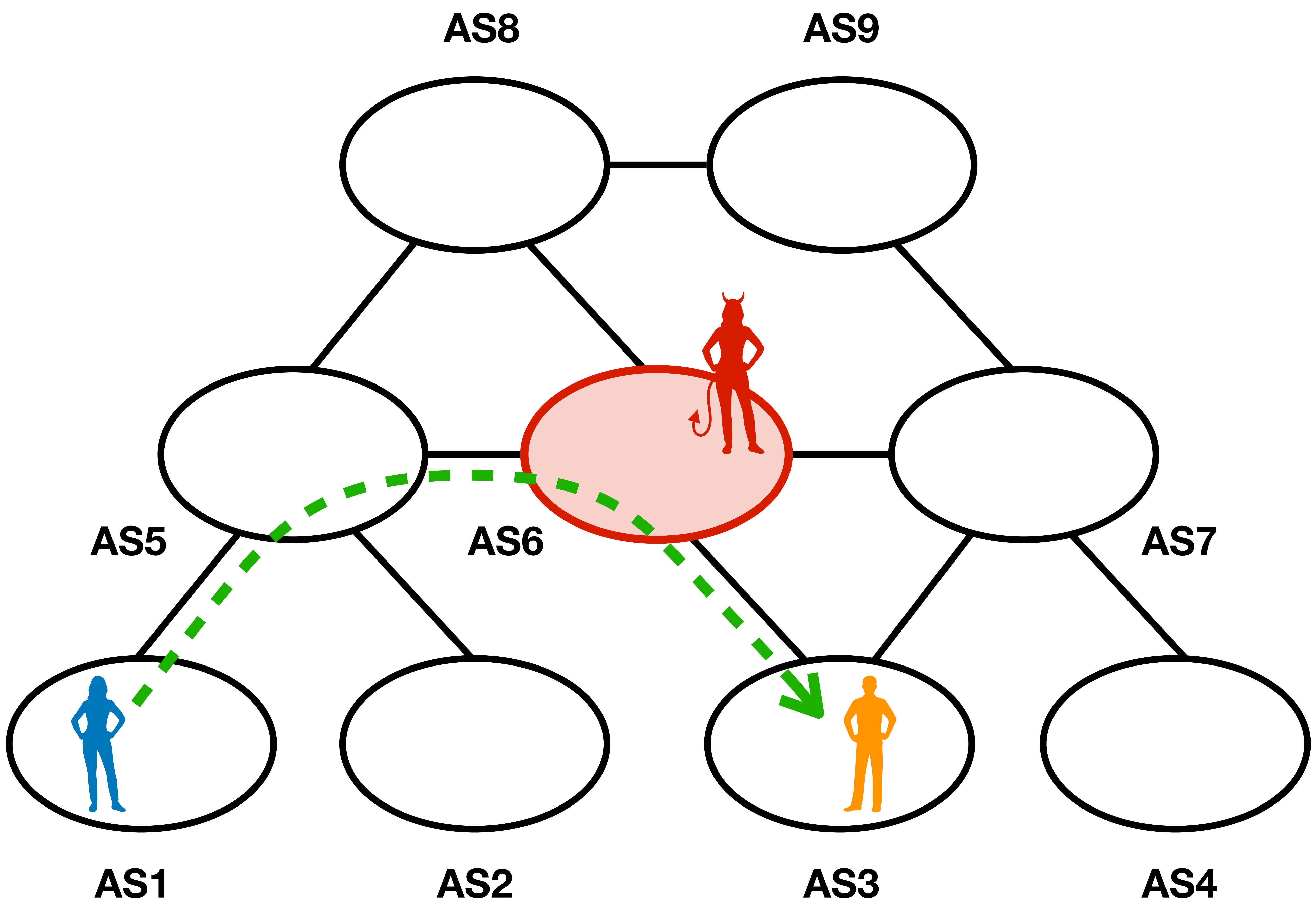
Network-layer anonymity



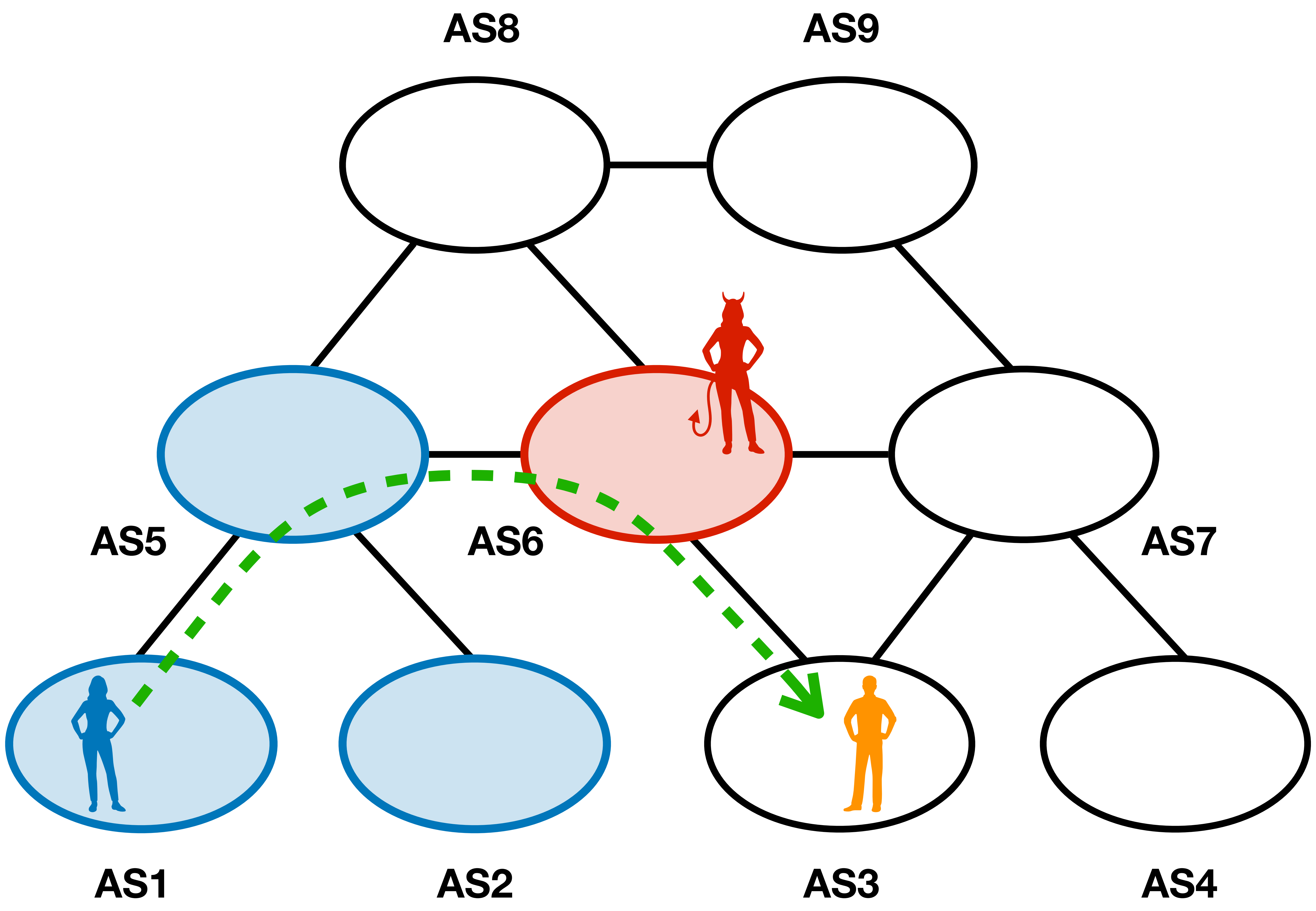
Network-layer anonymity



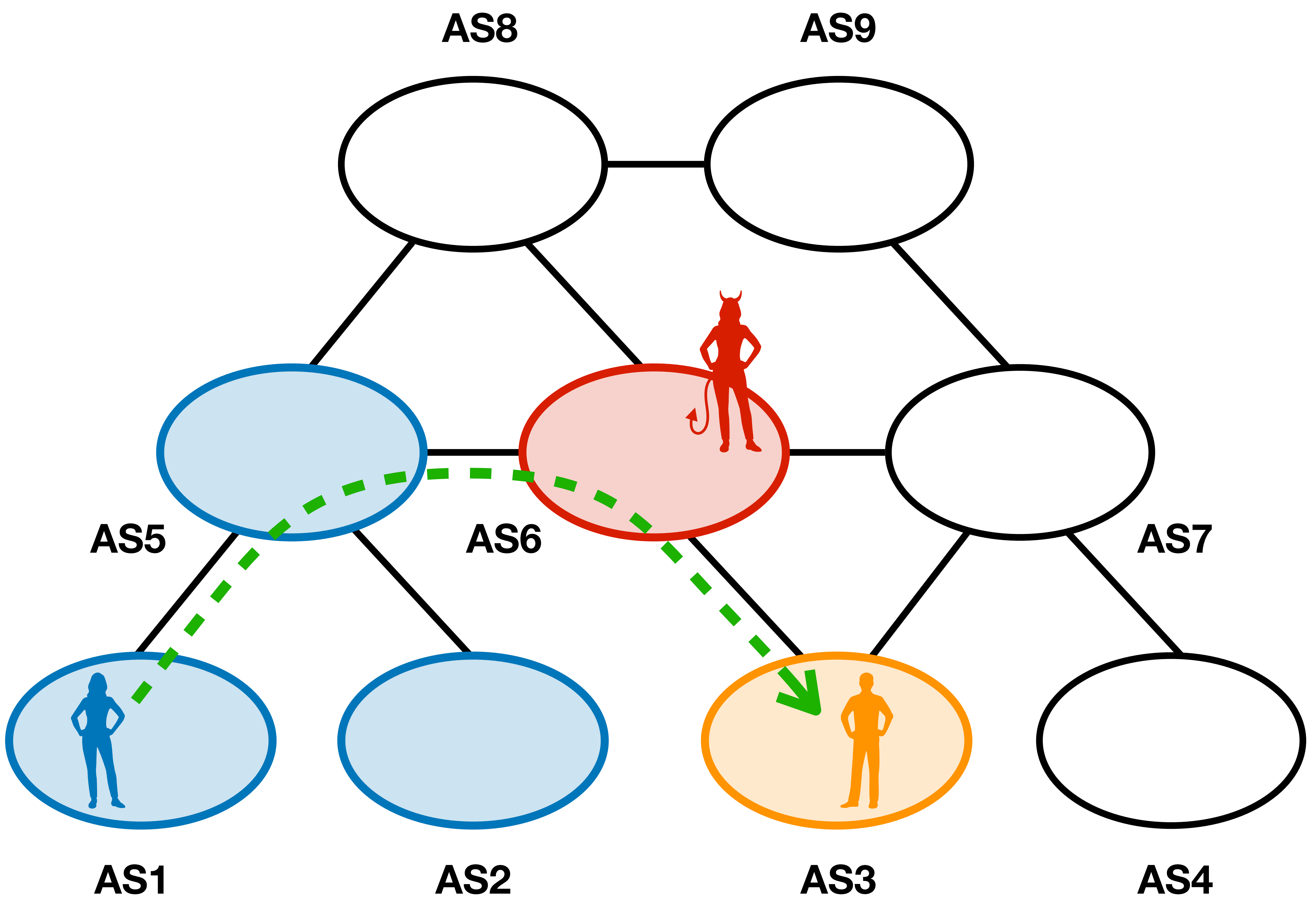
Network-layer anonymity



Network-layer anonymity

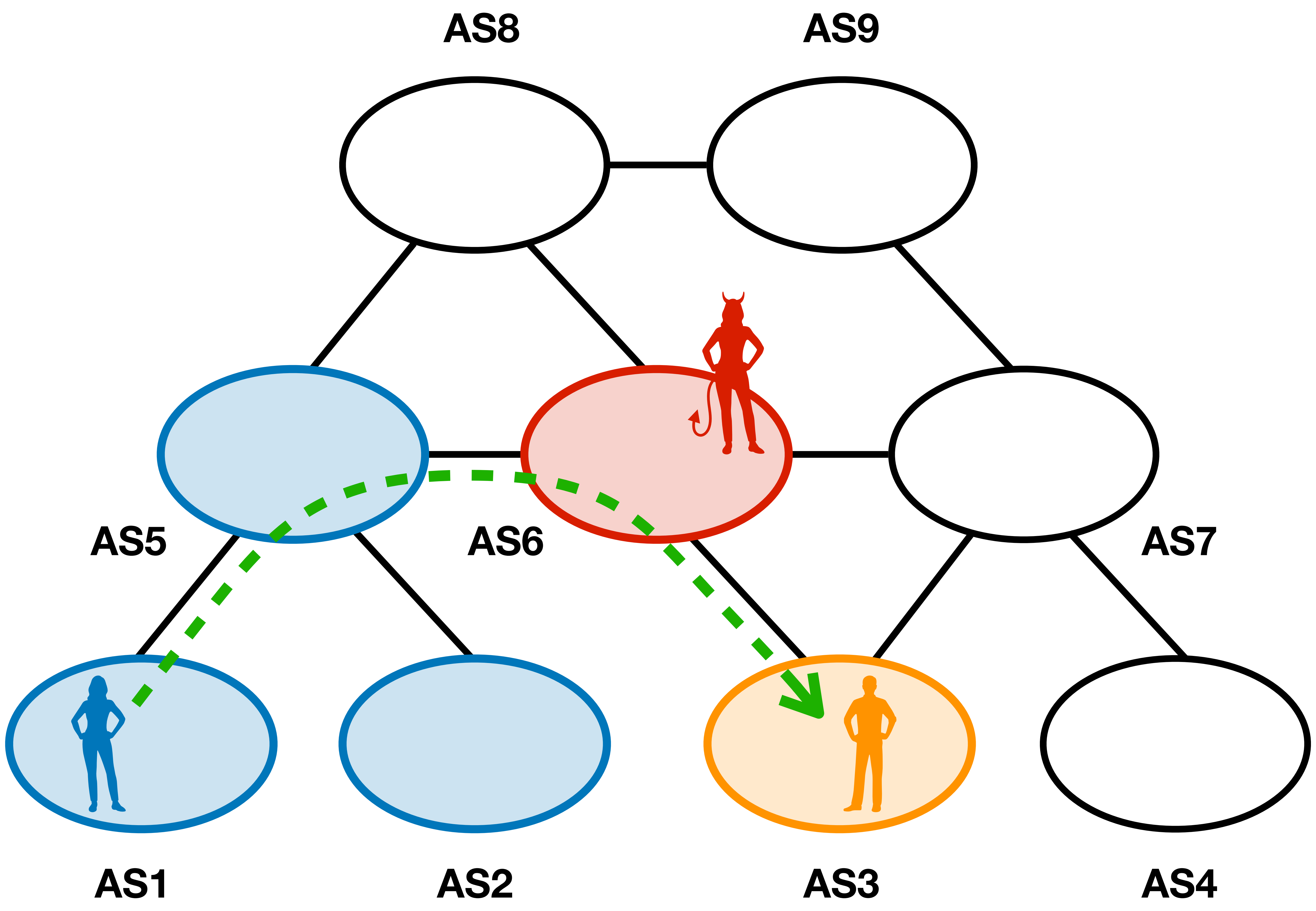


Network-layer anonymity



Network-layer anonymity

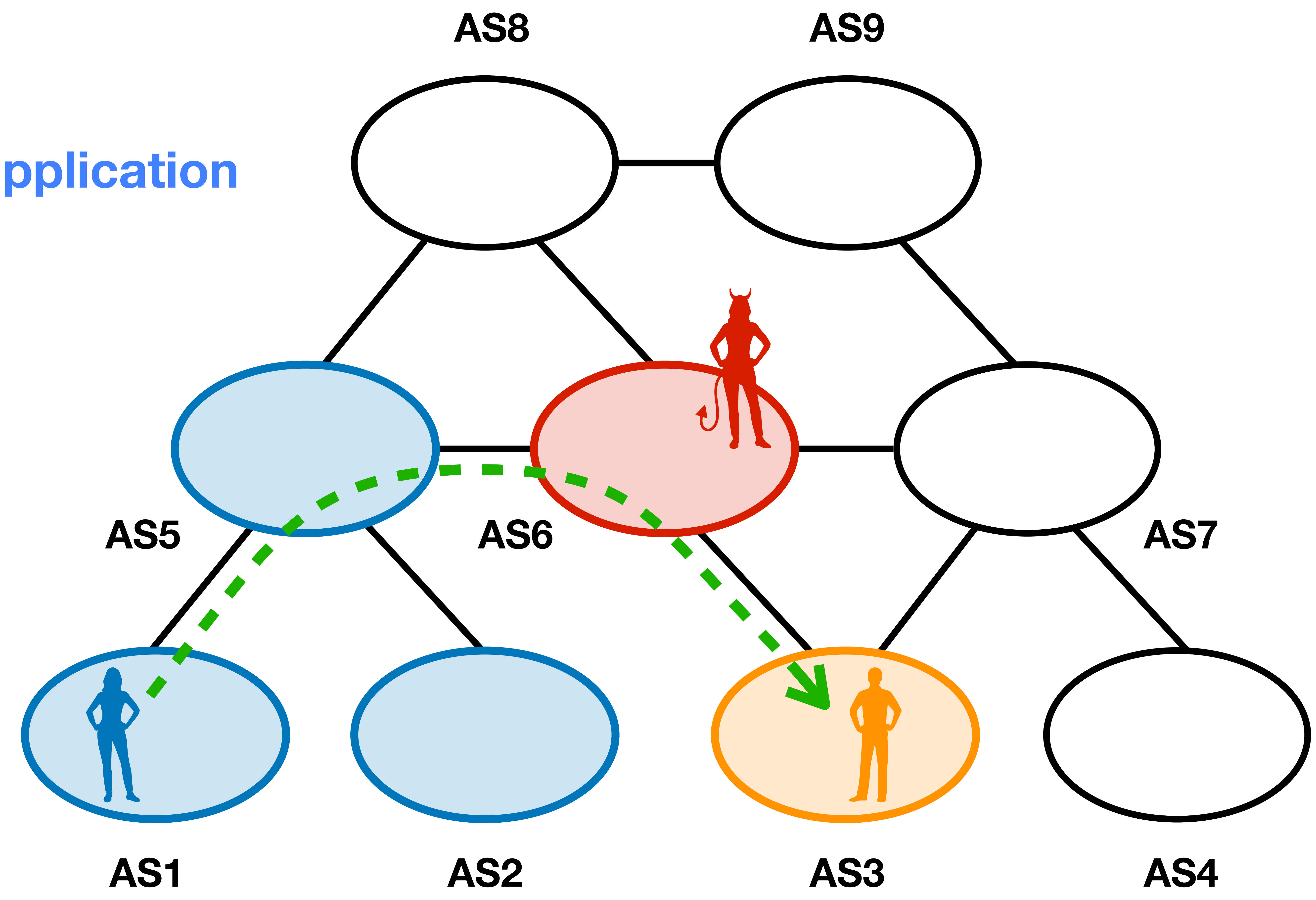
Advantages:



Network-layer anonymity

Advantages:

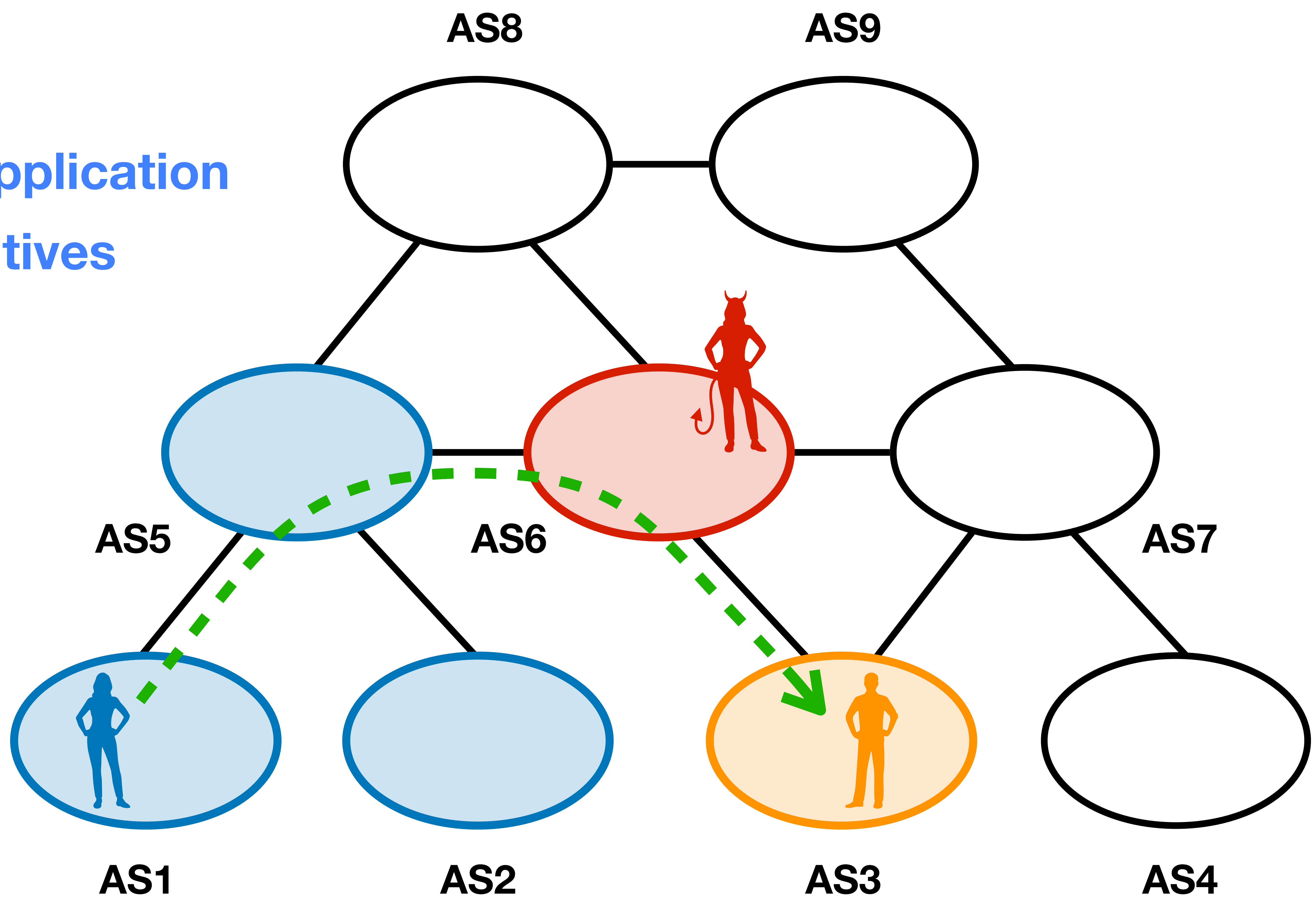
- Works for any application



Network-layer anonymity

Advantages:

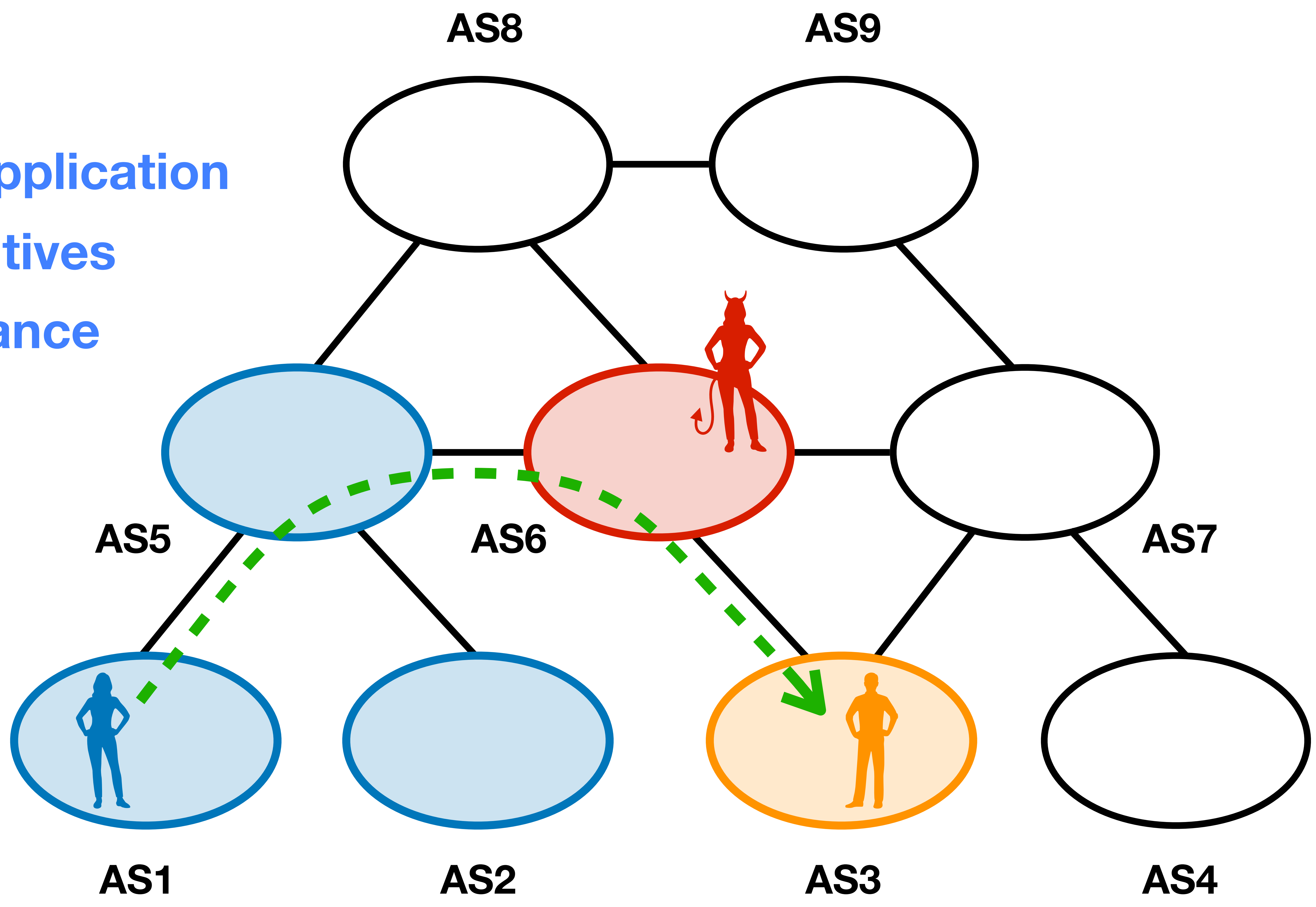
- Works for any application
- Economic incentives



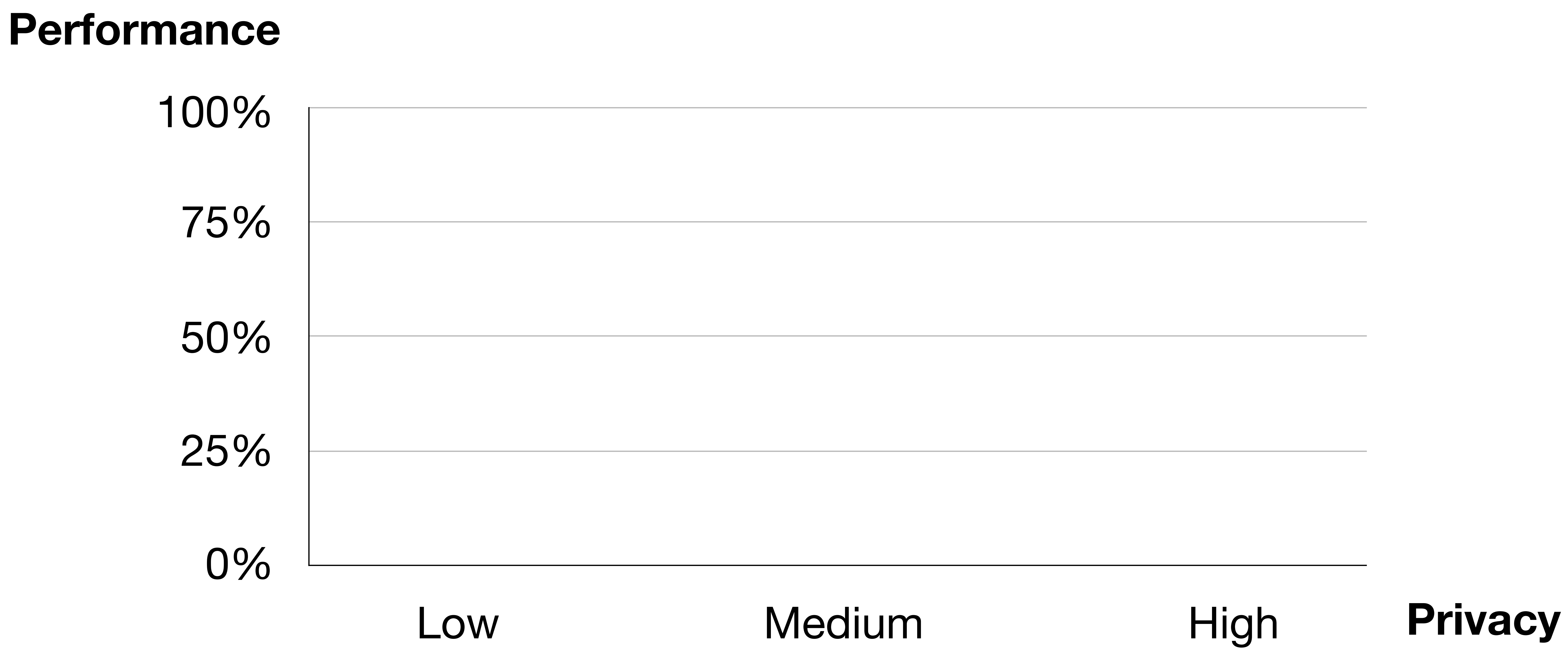
Network-layer anonymity

Advantages:

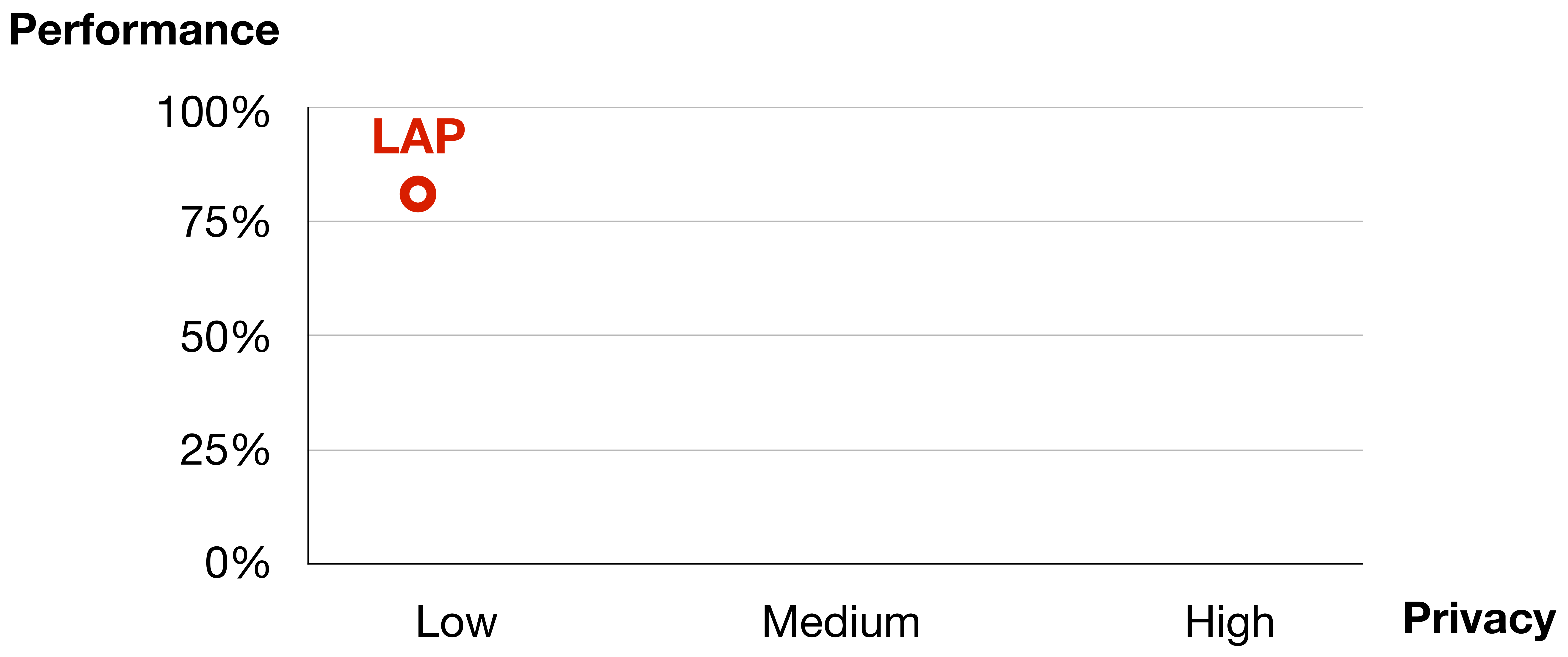
- Works for any application
- Economic incentives
- Higher performance



Previous work

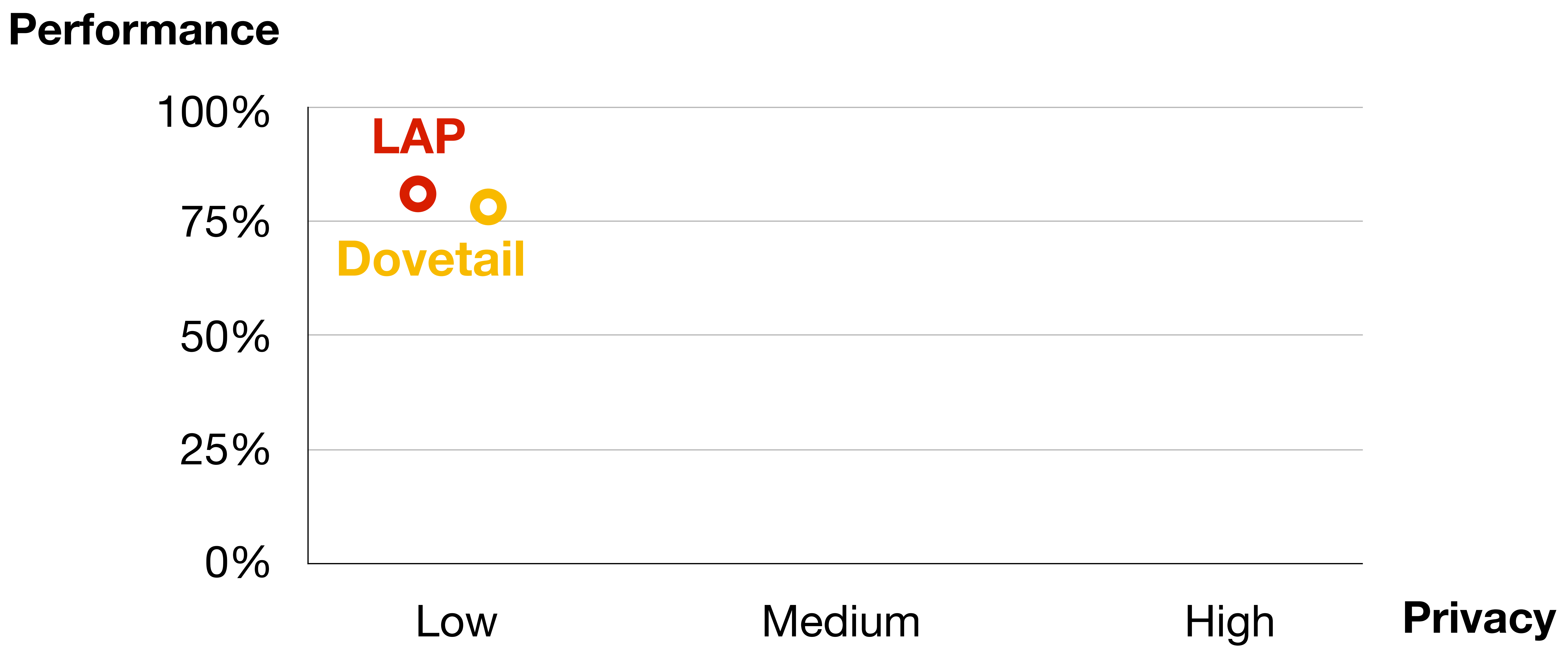


Previous work



- Hsiao et al. *LAP: Lightweight Anonymity and Privacy*. In IEEE **S&P**, 2012

Previous work

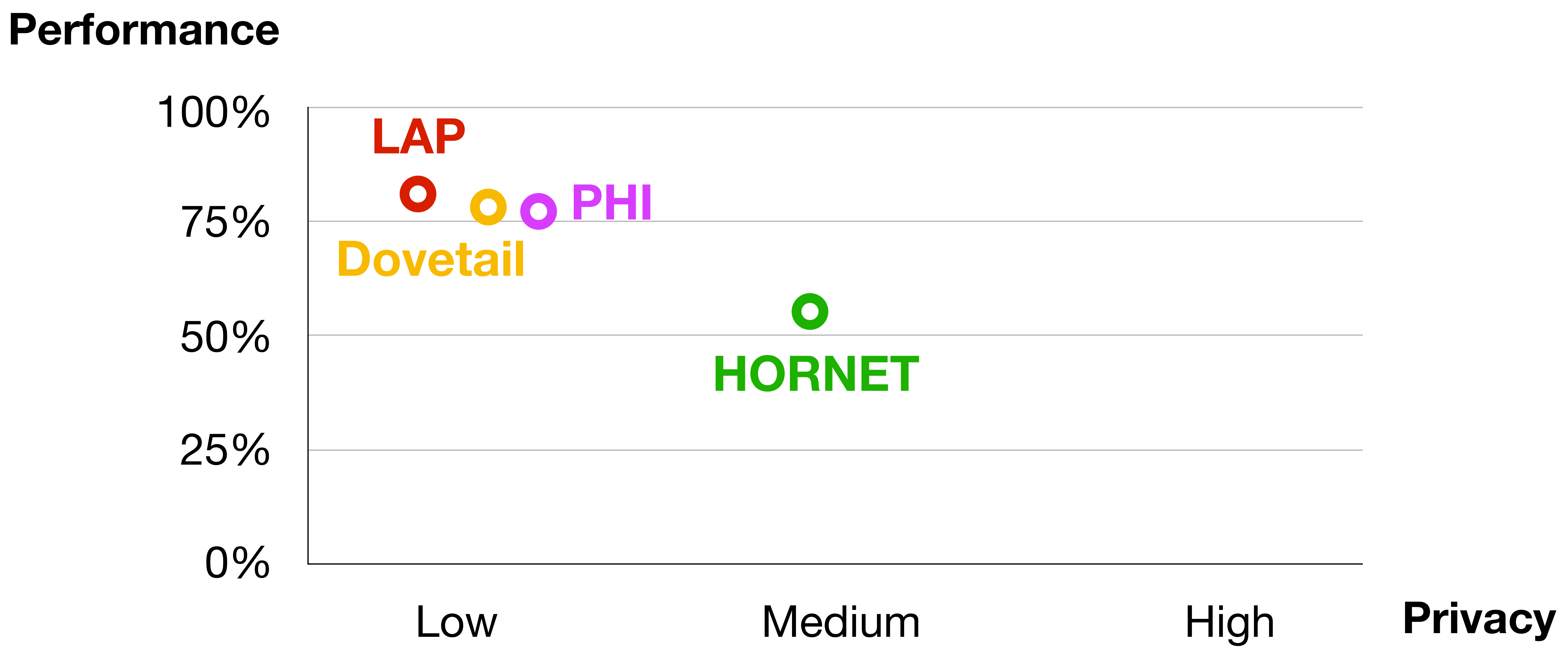


- Hsiao et al. *LAP: Lightweight Anonymity and Privacy*. In IEEE **S&P**, 2012
- Sankey, Wright. *Dovetail: Stronger anonymity in next-generation internet routing*. In **PETS**, 2014

Previous work

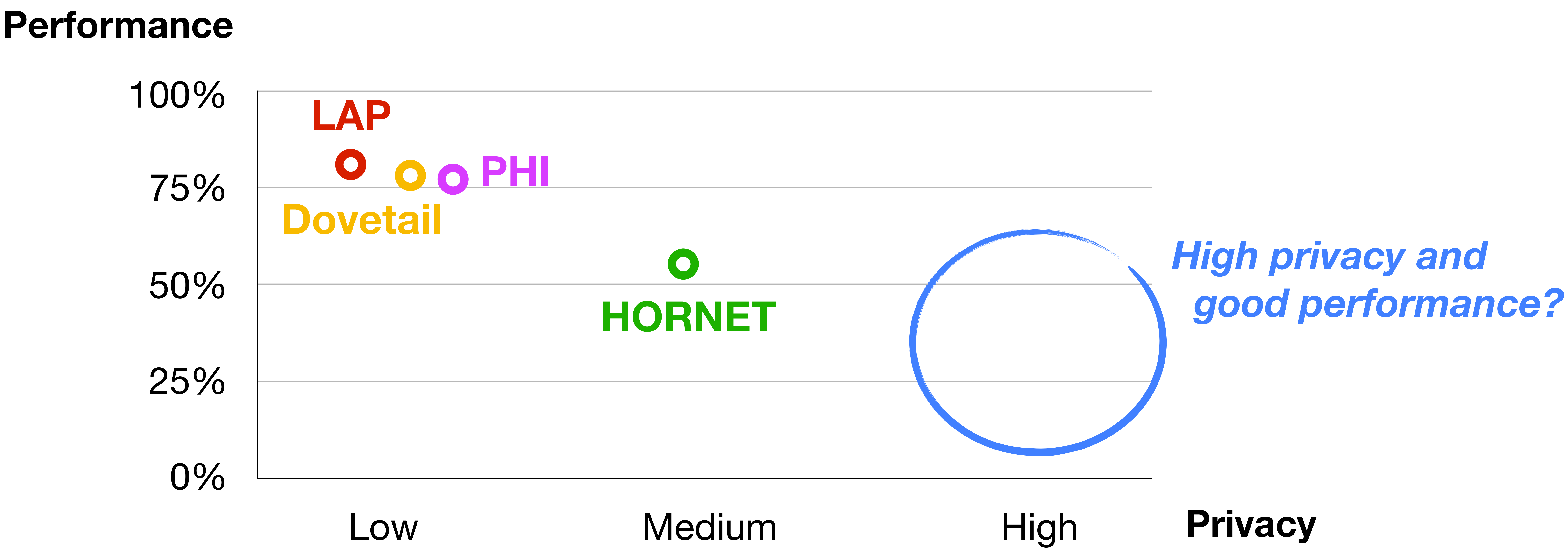
- Hsiao et al. *LAP: Lightweight Anonymity and Privacy*. In IEEE **S&P**, 2012
- Sankey, Wright. *Dovetail: Stronger anonymity in next-generation internet routing*. In **PETS**, 2014
- Chen, Perrig. *PHI: Path-Hidden Lightweight Anonymity Protocol at Network Layer*. In **PETS**, 2017

Previous work



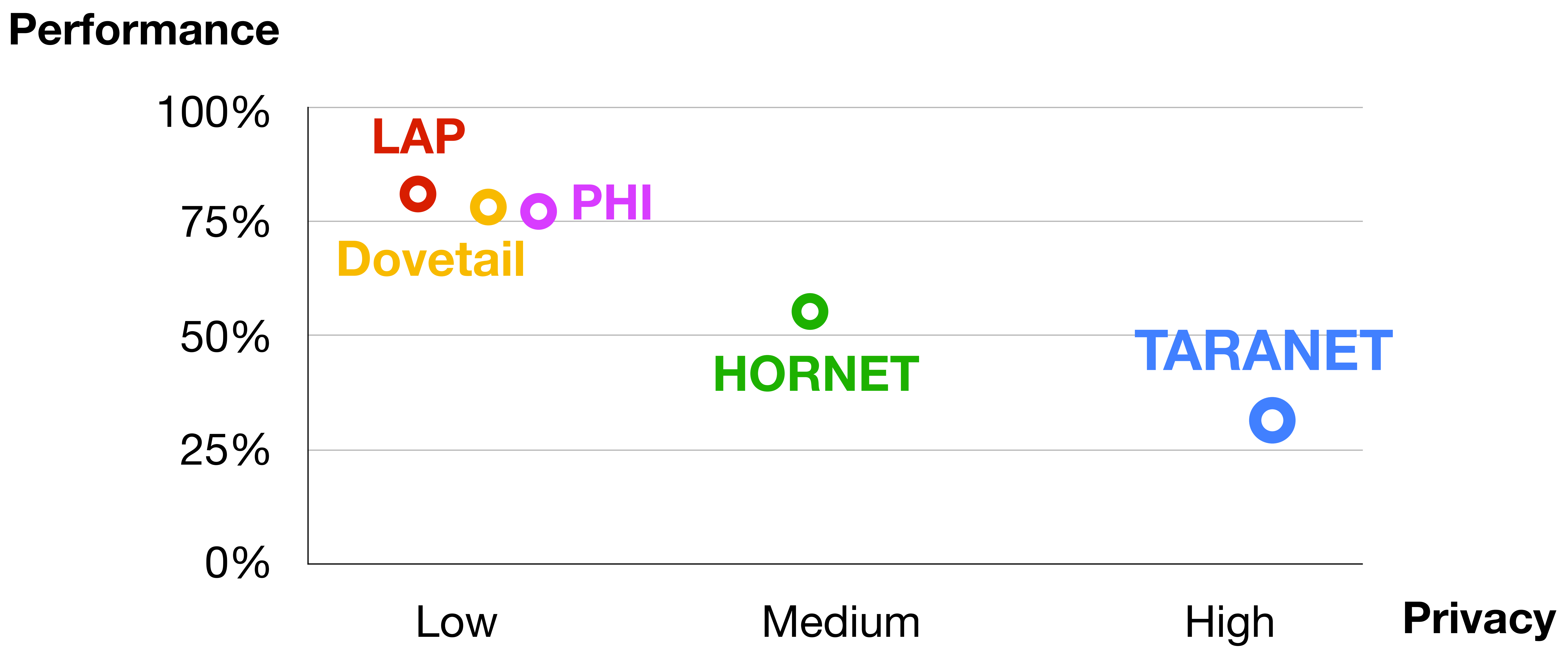
- Hsiao et al. *LAP: Lightweight Anonymity and Privacy*. In IEEE **S&P**, 2012
- Sankey, Wright. *Dovetail: Stronger anonymity in next-generation internet routing*. In **PETS**, 2014
- Chen, Perrig. *PHI: Path-Hidden Lightweight Anonymity Protocol at Network Layer*. In **PETS**, 2017
- Chen et al. *HORNET: High-speed Onion Routing at the Network Layer*. In ACM **CCS**, 2015

Previous work



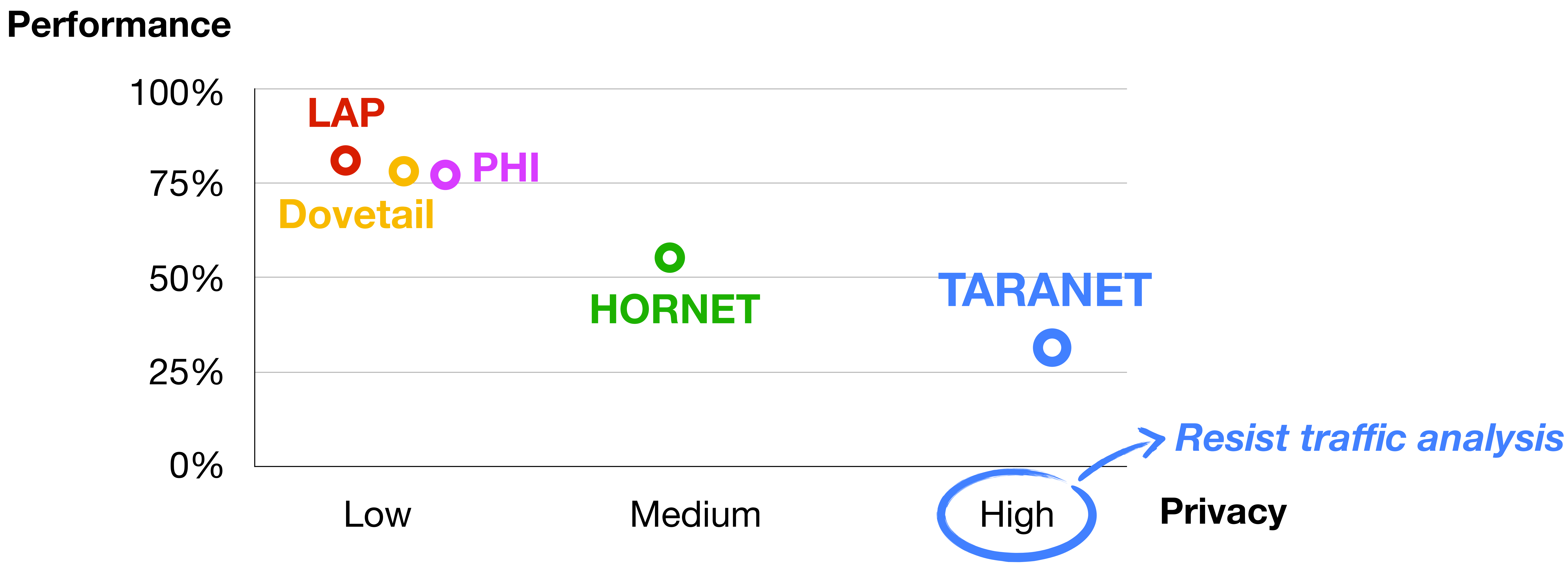
- Hsiao et al. *LAP: Lightweight Anonymity and Privacy*. In IEEE **S&P**, 2012
- Sankey, Wright. *Dovetail: Stronger anonymity in next-generation internet routing*. In **PETS**, 2014
- Chen, Perrig. *PHI: Path-Hidden Lightweight Anonymity Protocol at Network Layer*. In **PETS**, 2017
- Chen et al. *HORNET: High-speed Onion Routing at the Network Layer*. In ACM **CCS**, 2015

Previous work



- Hsiao et al. *LAP: Lightweight Anonymity and Privacy*. In IEEE **S&P**, 2012
- Sankey, Wright. *Dovetail: Stronger anonymity in next-generation internet routing*. In **PETS**, 2014
- Chen, Perrig. *PHI: Path-Hidden Lightweight Anonymity Protocol at Network Layer*. In **PETS**, 2017
- Chen et al. *HORNET: High-speed Onion Routing at the Network Layer*. In ACM **CCS**, 2015

Previous work

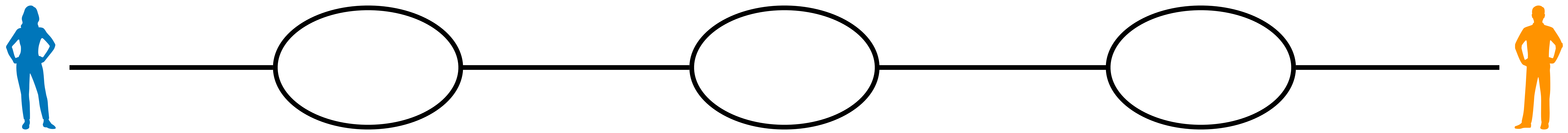


- Hsiao et al. *LAP: Lightweight Anonymity and Privacy*. In IEEE **S&P**, 2012
- Sankey, Wright. *Dovetail: Stronger anonymity in next-generation internet routing*. In **PETS**, 2014
- Chen, Perrig. *PHI: Path-Hidden Lightweight Anonymity Protocol at Network Layer*. In **PETS**, 2017
- Chen et al. *HORNET: High-speed Onion Routing at the Network Layer*. In ACM **CCS**, 2015

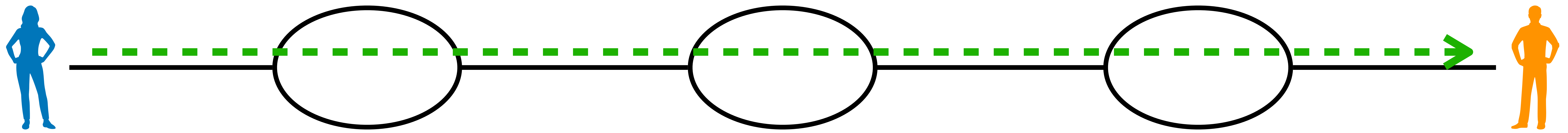
Traffic analysis

Severe threat to anonymous communication

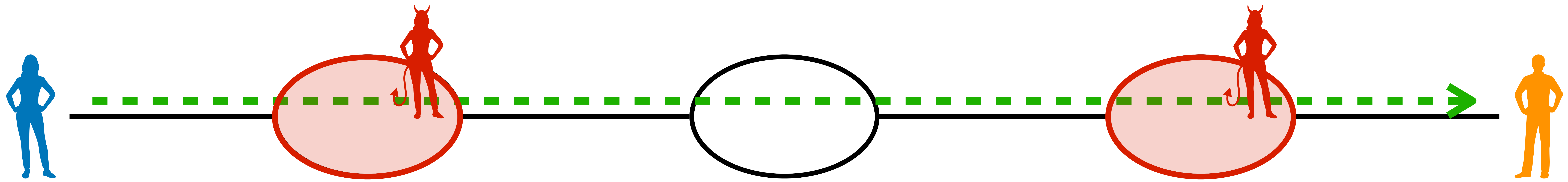
(Passive) Traffic analysis



(Passive) Traffic analysis



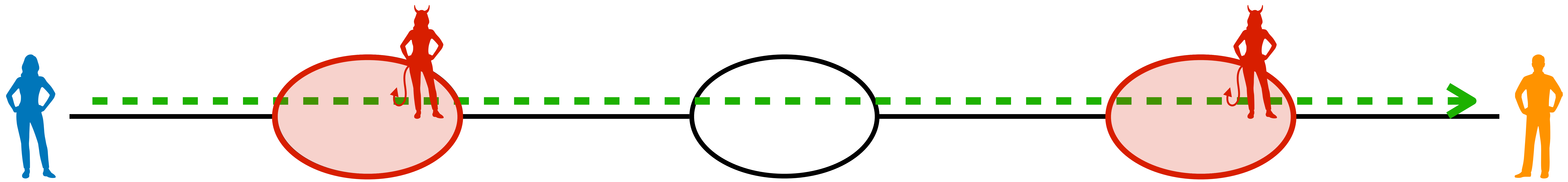
(Passive) Traffic analysis



(Passive) Traffic analysis

Starting point

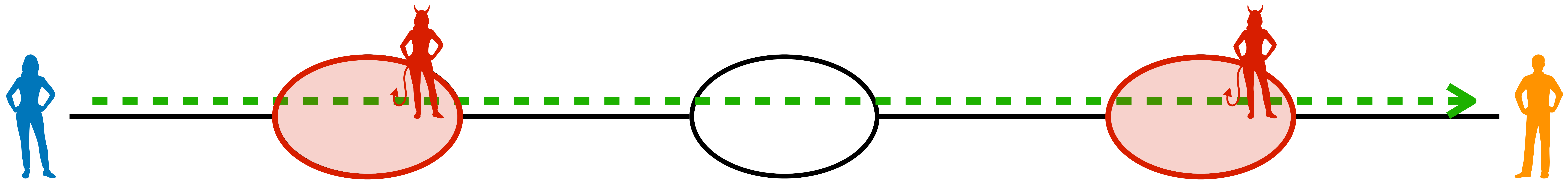
- **Layered encryption**



(Passive) Traffic analysis

Starting point

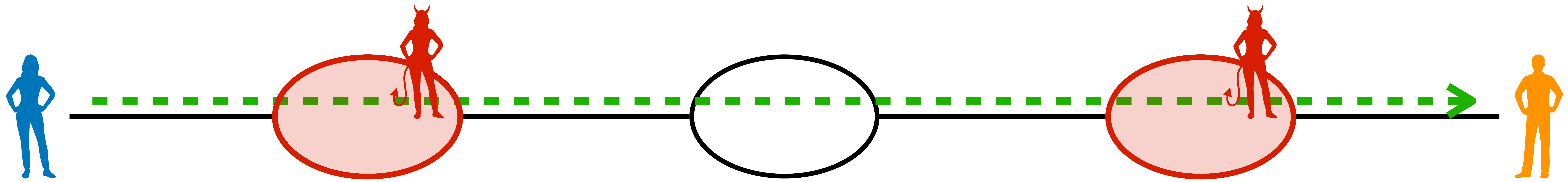
- **Layered encryption**
- **Per-hop authentication**



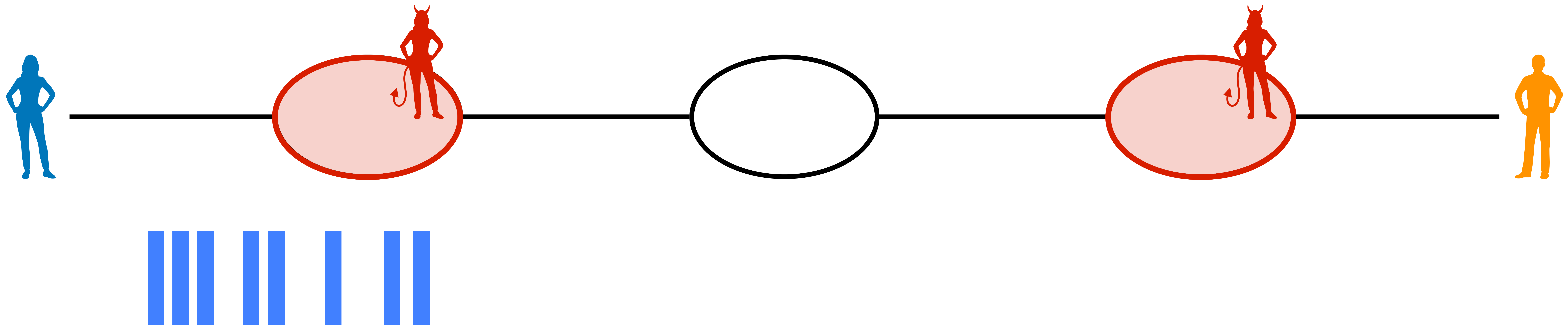
(Passive) Traffic analysis

Starting point

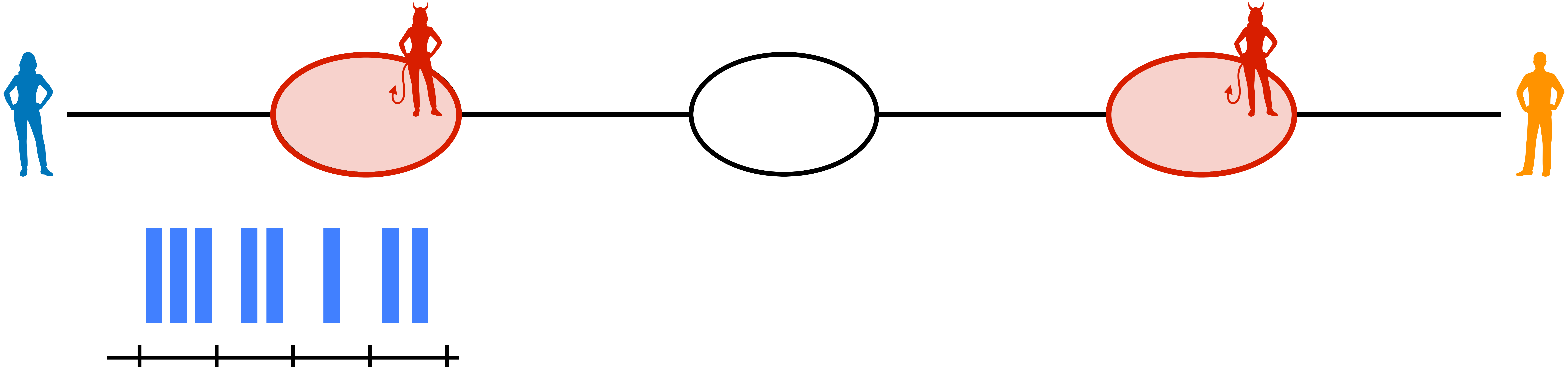
- Layered encryption
- Per-hop authentication
- Fixed packet length



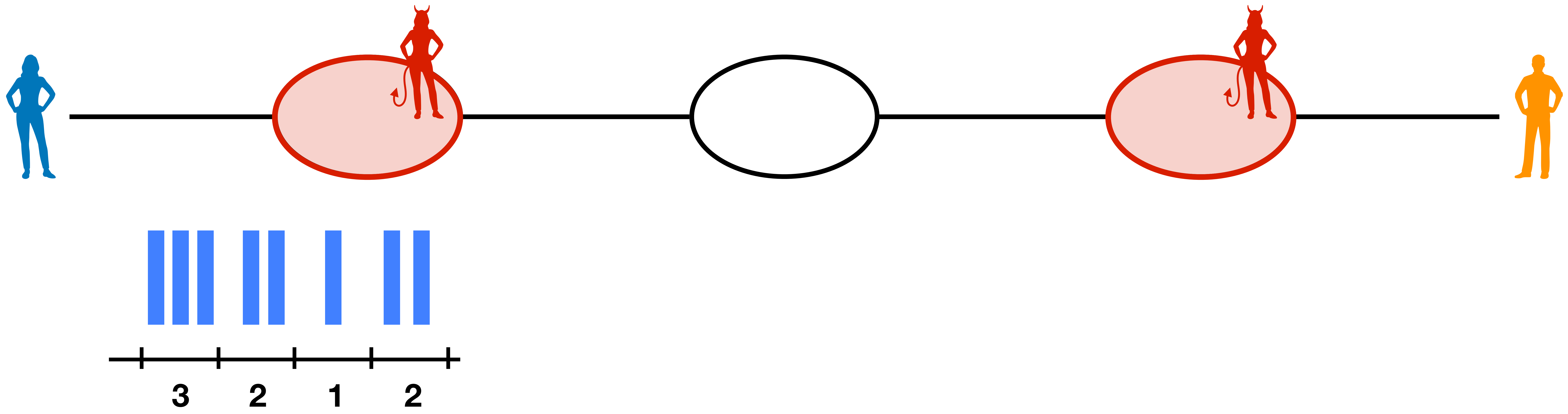
(Passive) Traffic analysis



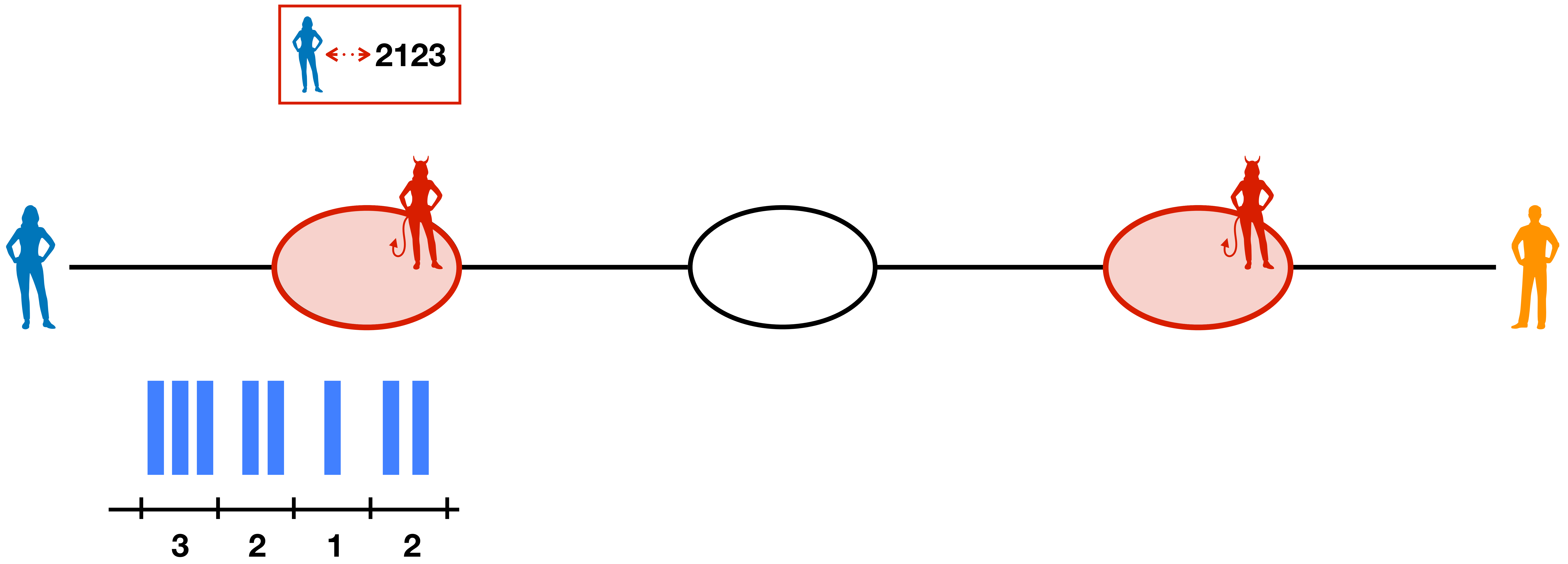
(Passive) Traffic analysis



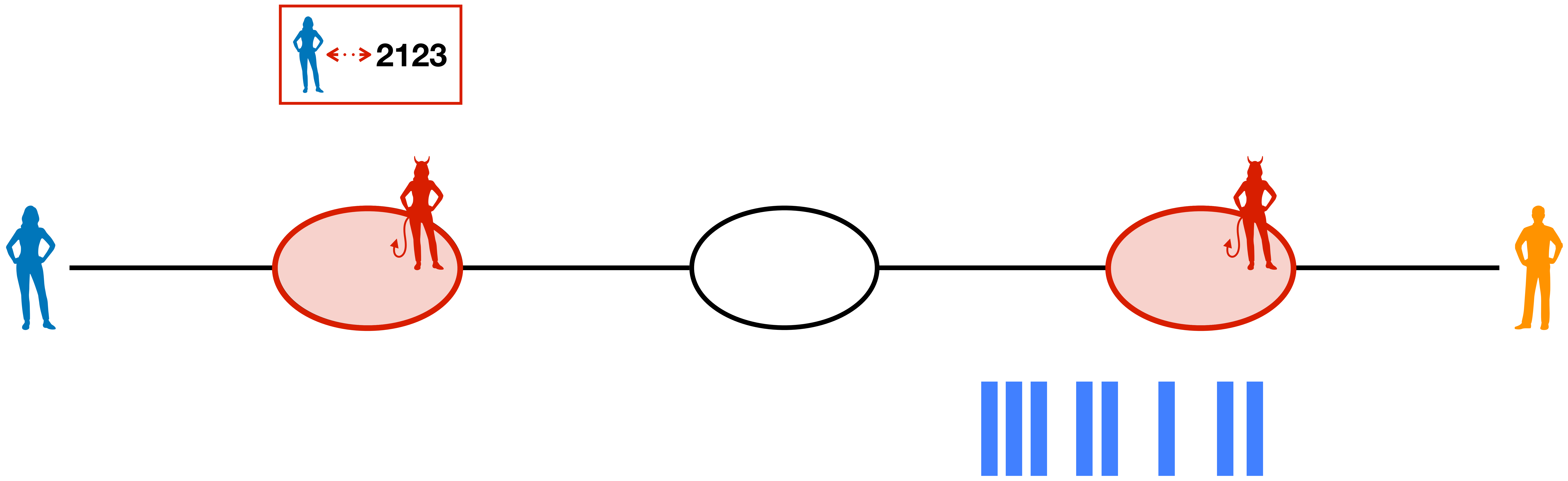
(Passive) Traffic analysis



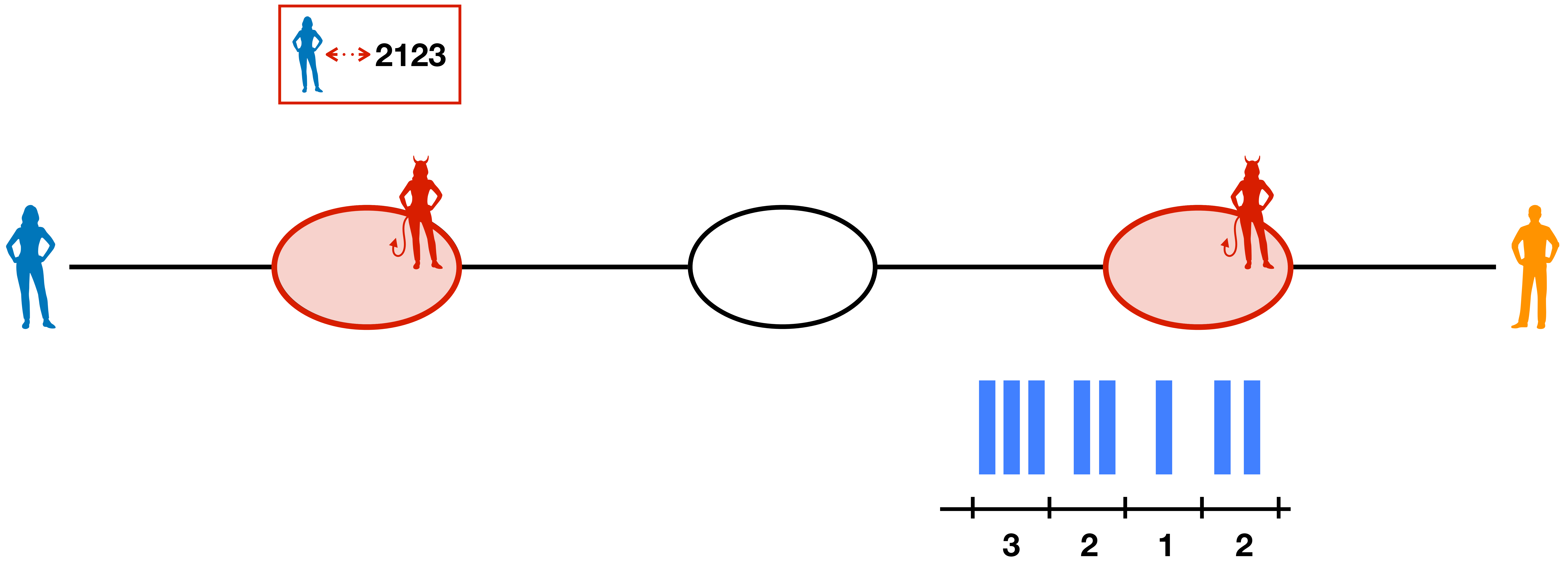
(Passive) Traffic analysis



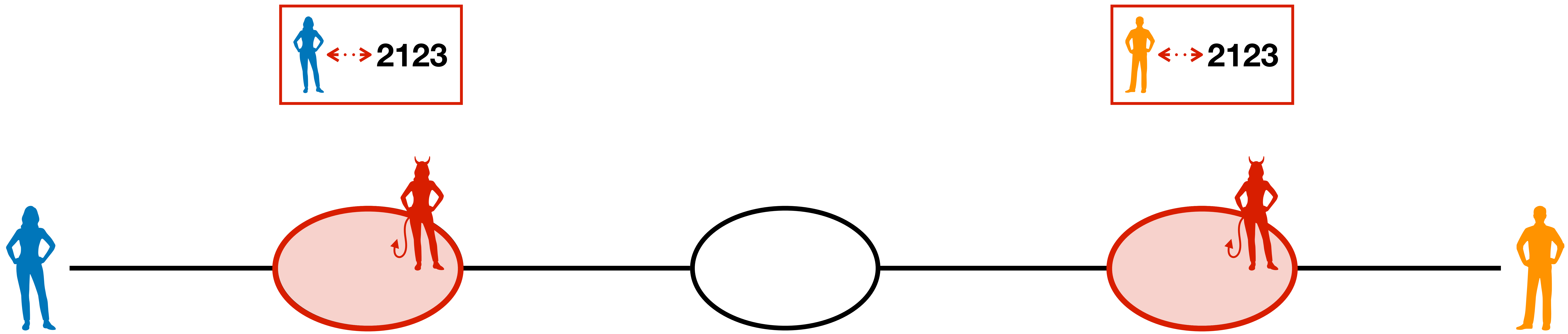
(Passive) Traffic analysis



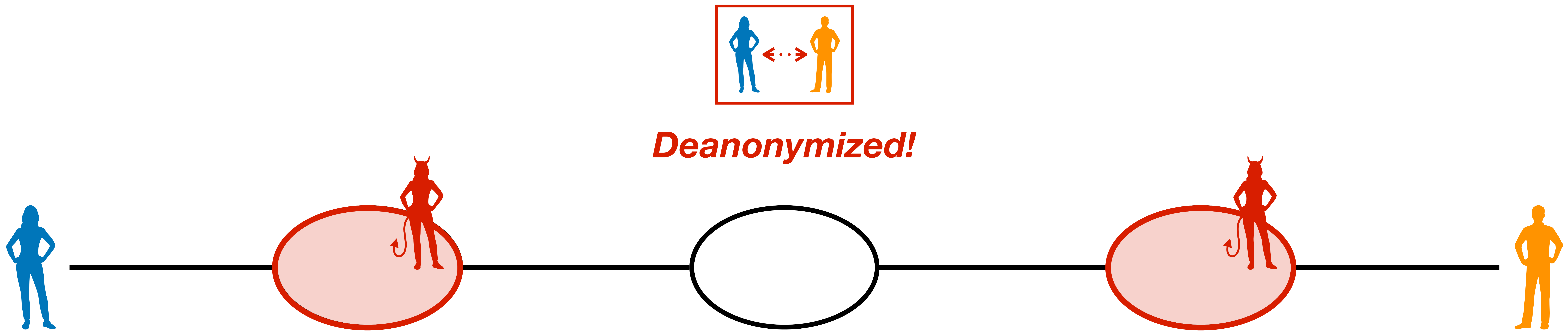
(Passive) Traffic analysis



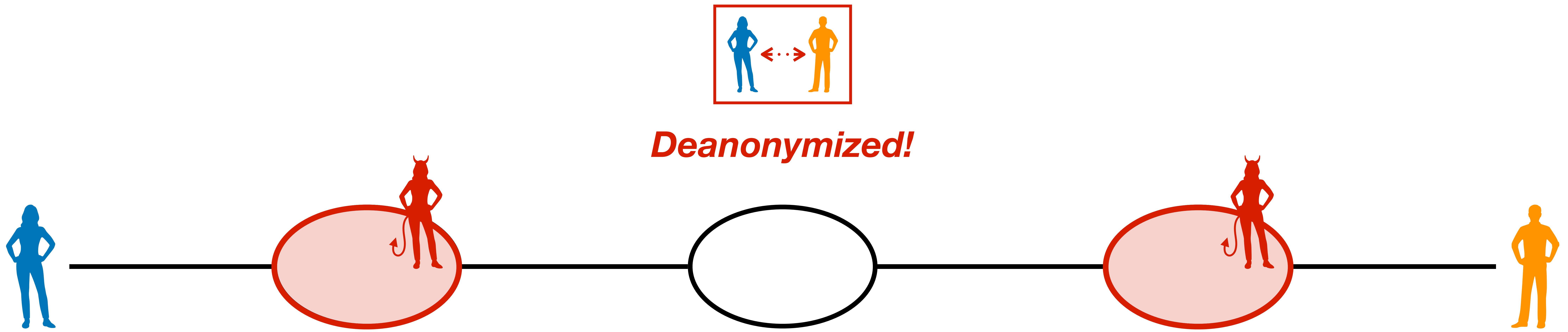
(Passive) Traffic analysis



(Passive) Traffic analysis

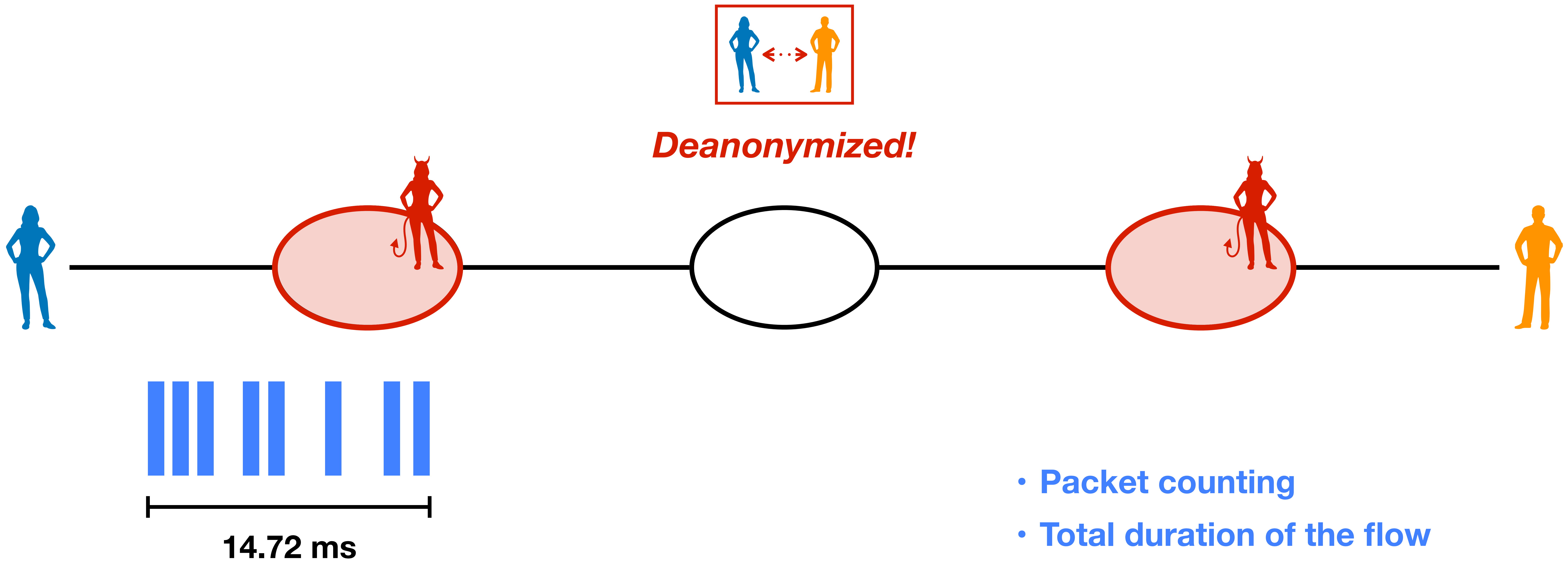


(Passive) Traffic analysis



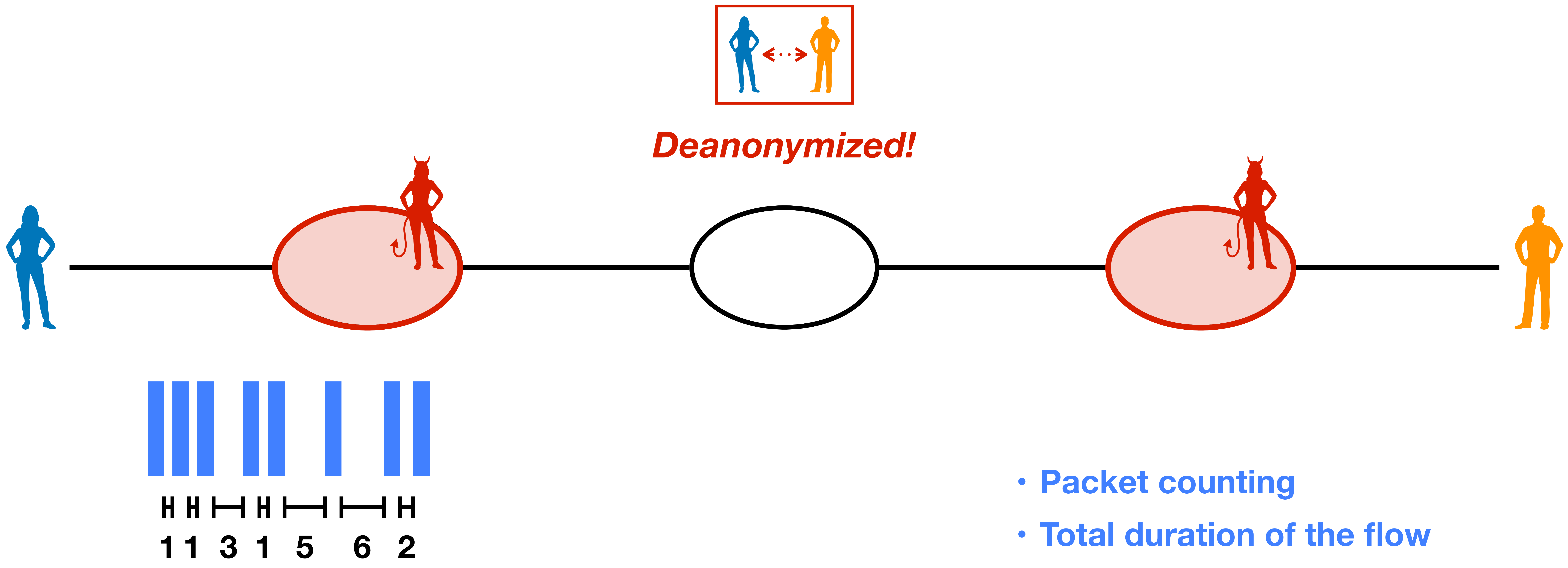
- **Packet counting**

(Passive) Traffic analysis



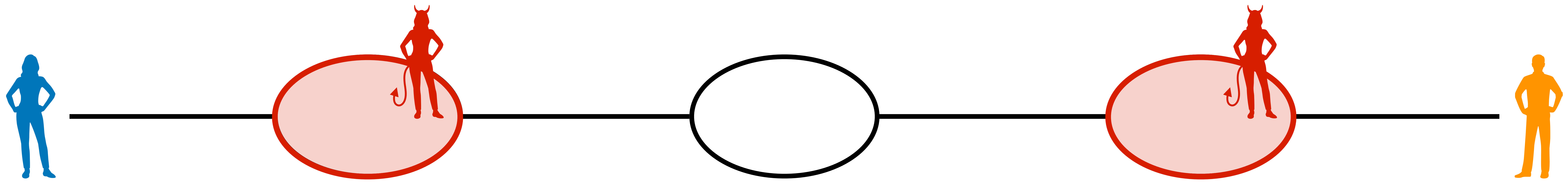
- Packet counting
- Total duration of the flow

(Passive) Traffic analysis

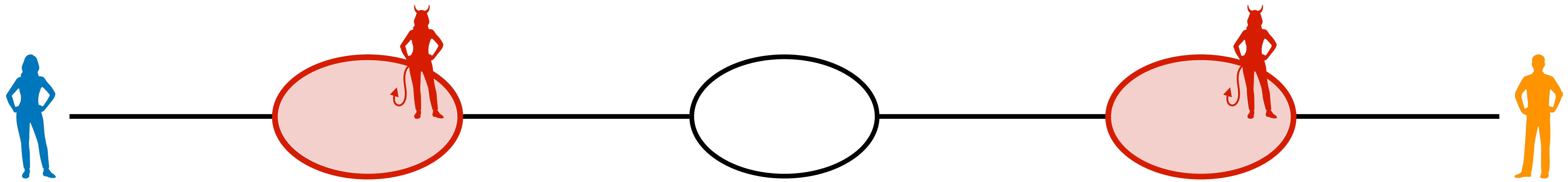


- Packet counting
- Total duration of the flow
- Inter-packet timing

Active traffic analysis

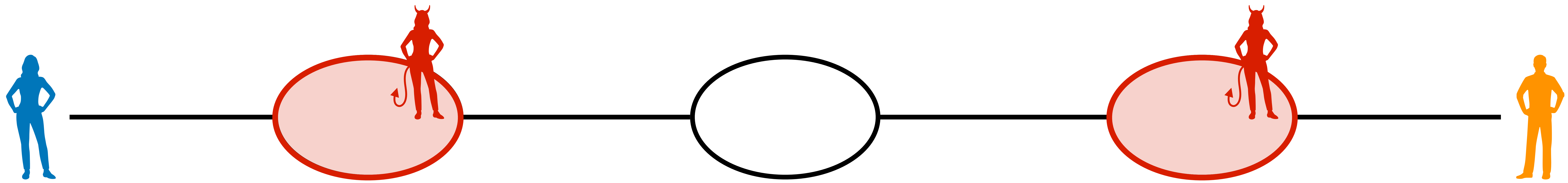


Active traffic analysis



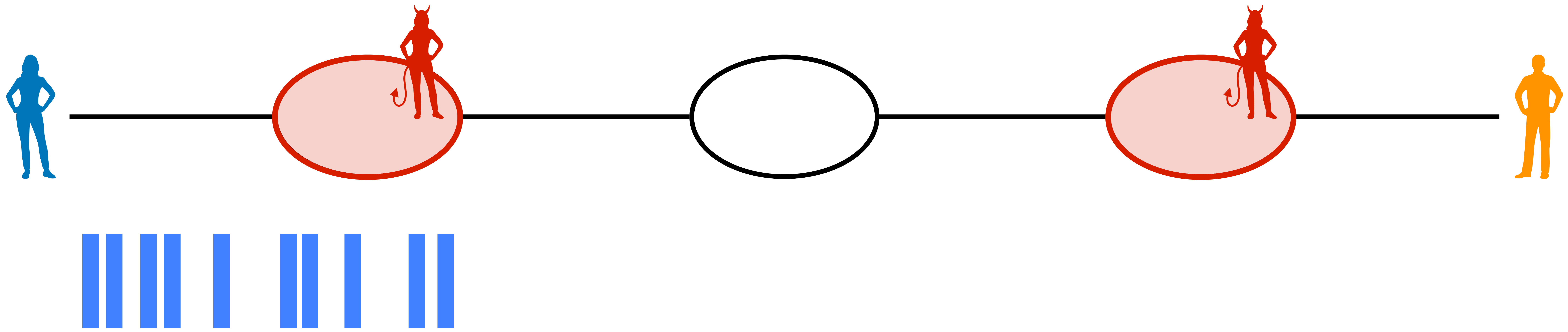
Active traffic analysis

Packet dropping



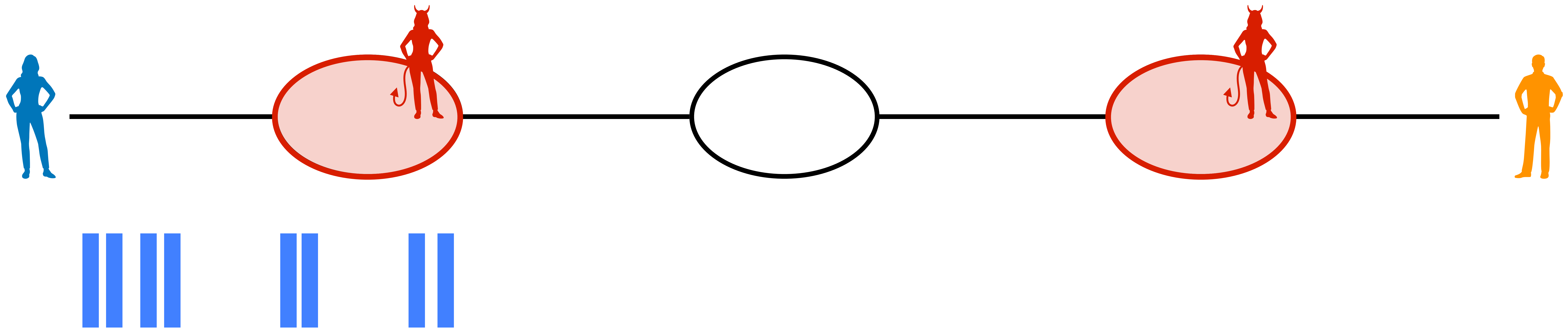
Active traffic analysis

Packet dropping



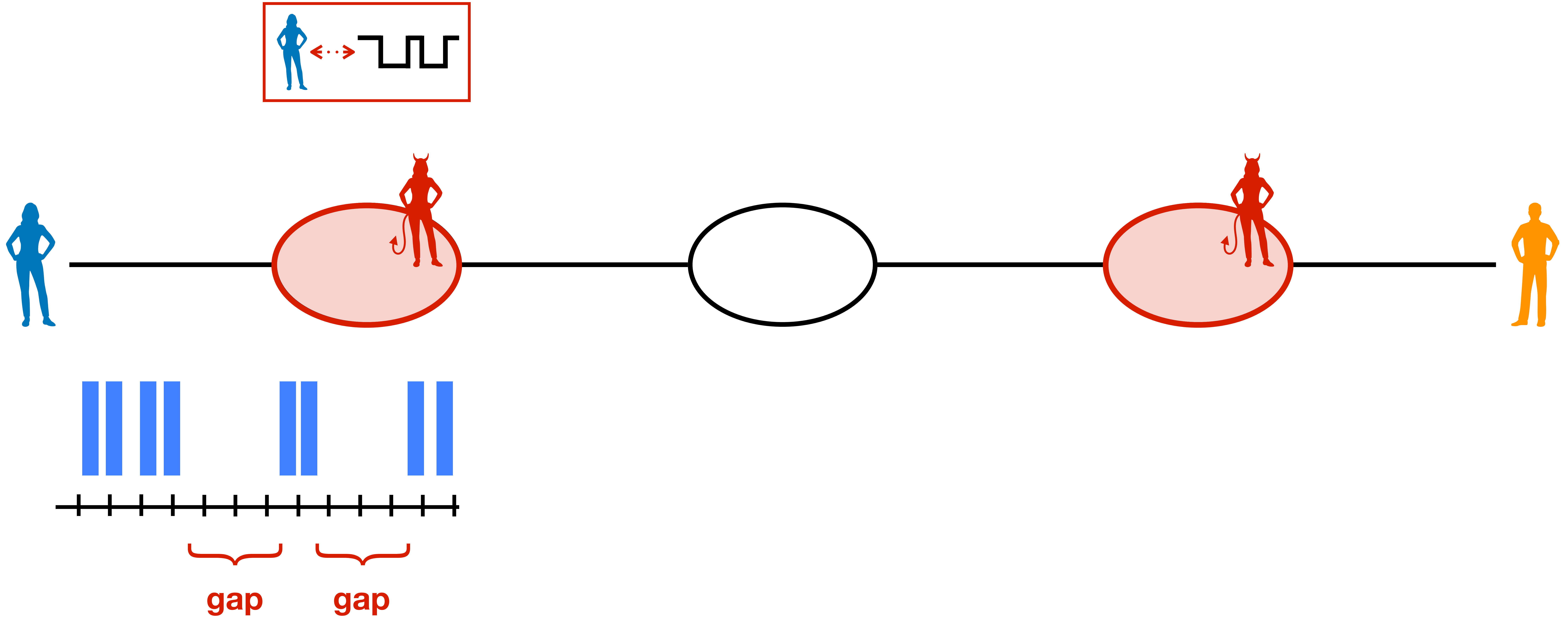
Active traffic analysis

Packet dropping



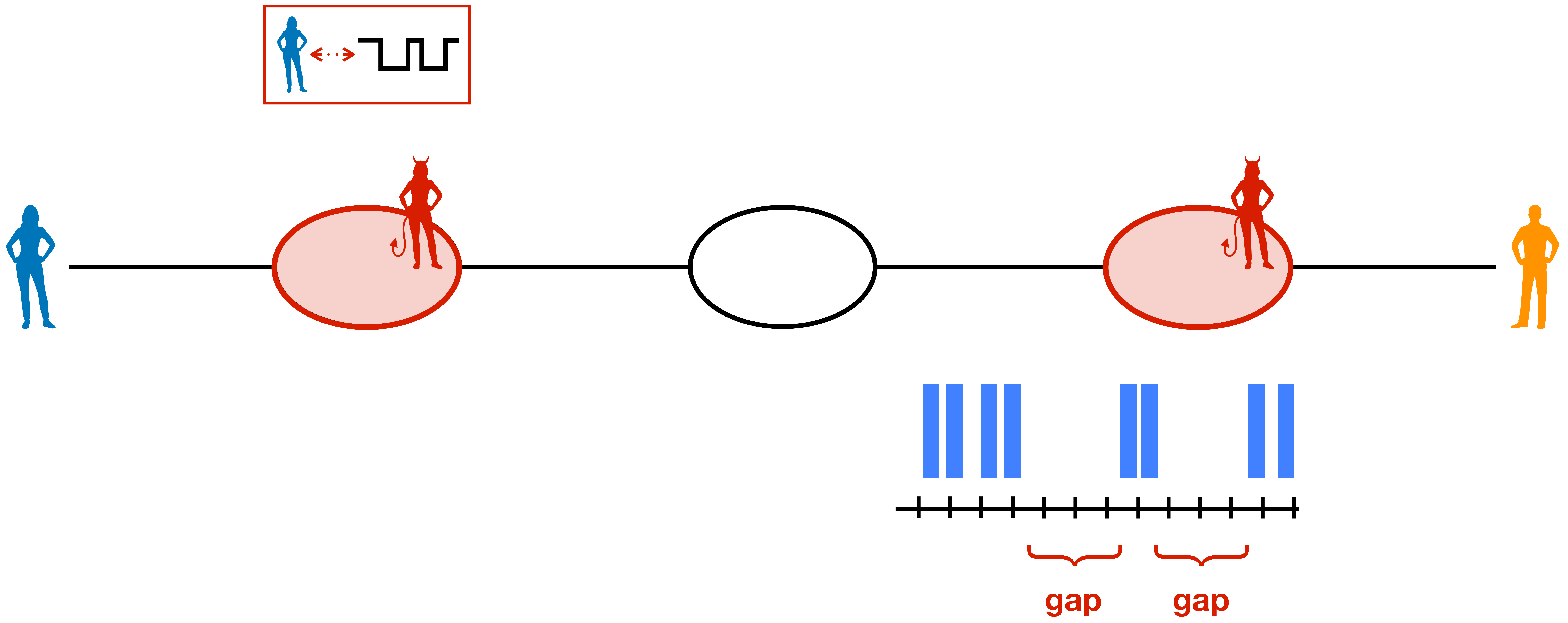
Active traffic analysis

Packet dropping



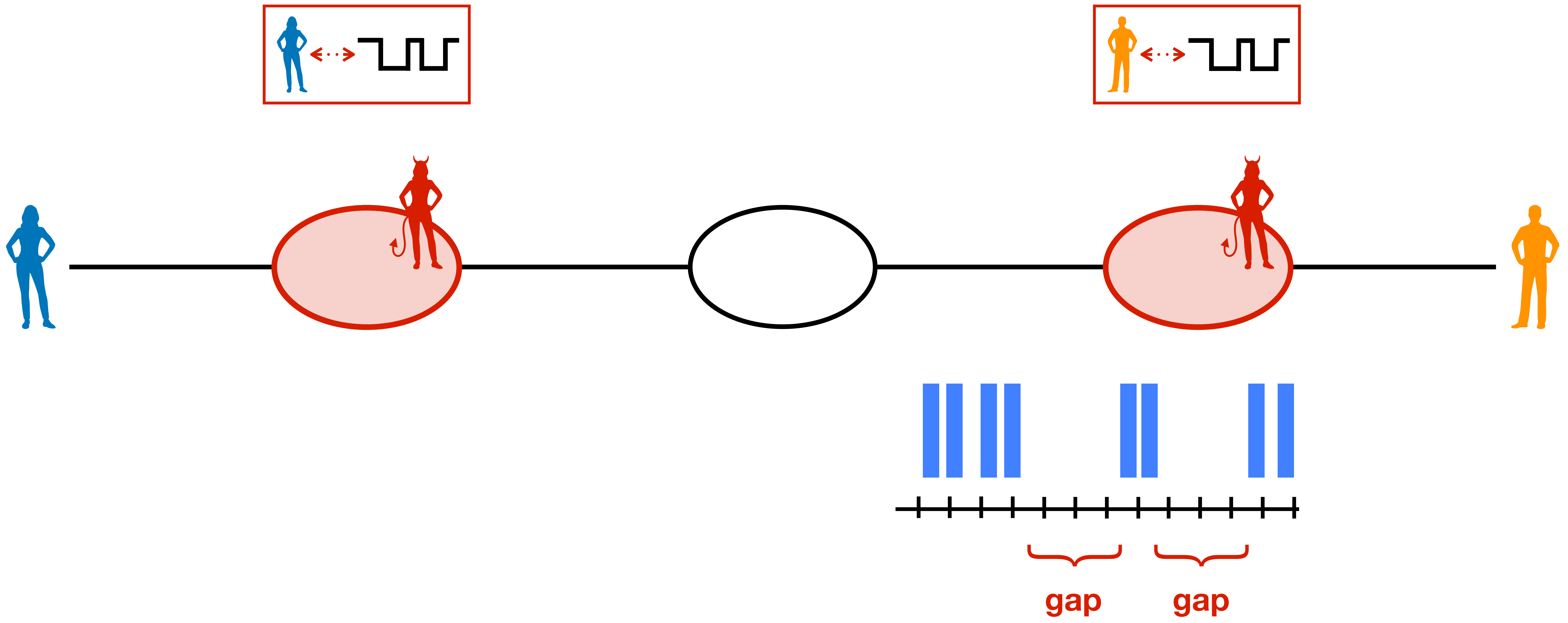
Active traffic analysis

Packet dropping



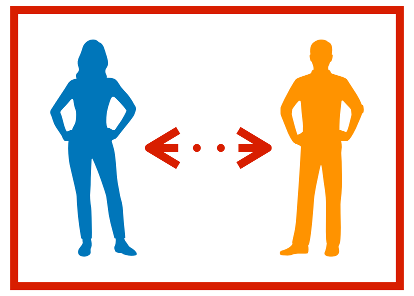
Active traffic analysis

Packet dropping

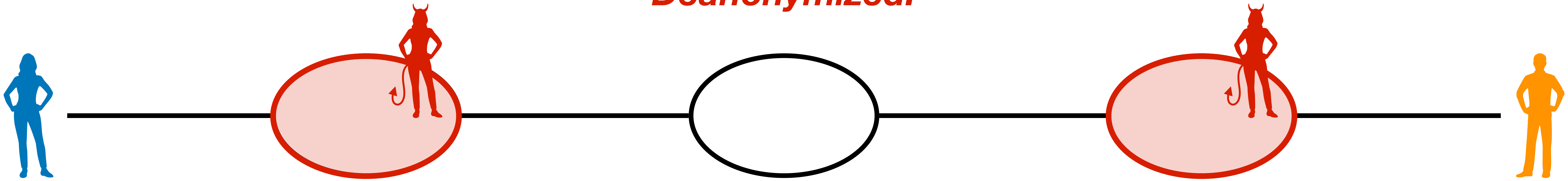


Active traffic analysis

Packet dropping



Deanonymized!



TARANET

Resisting traffic analysis attacks

Network-layer anonymity

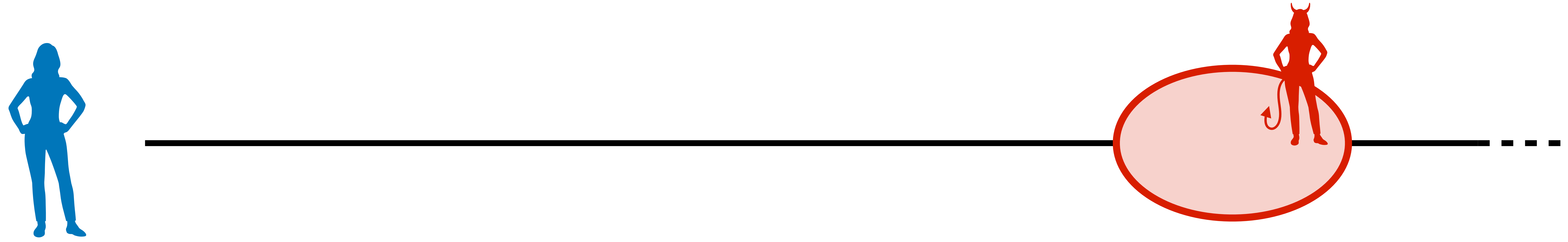
Traffic analysis

TARANET

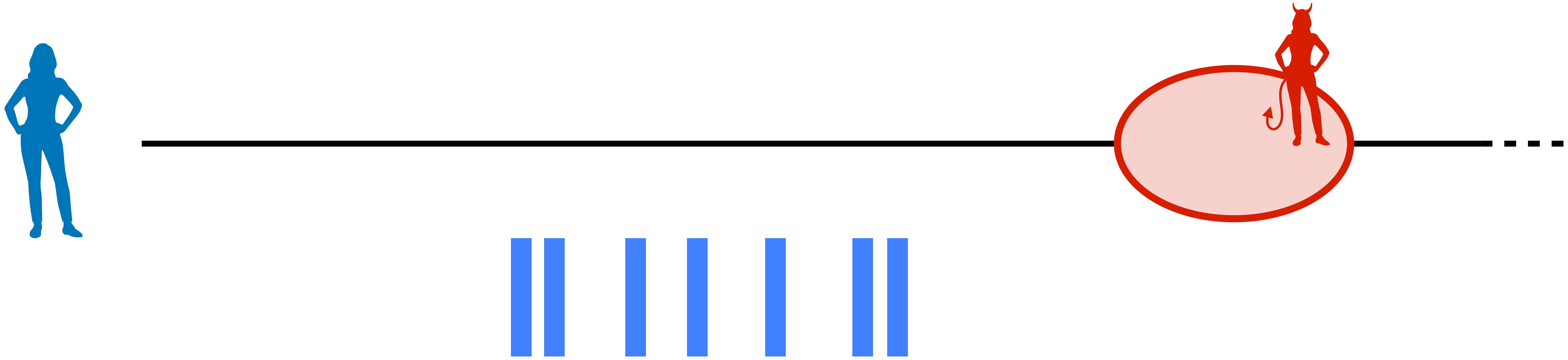
TARANET Performance

Summary

Resisting passive traffic analysis

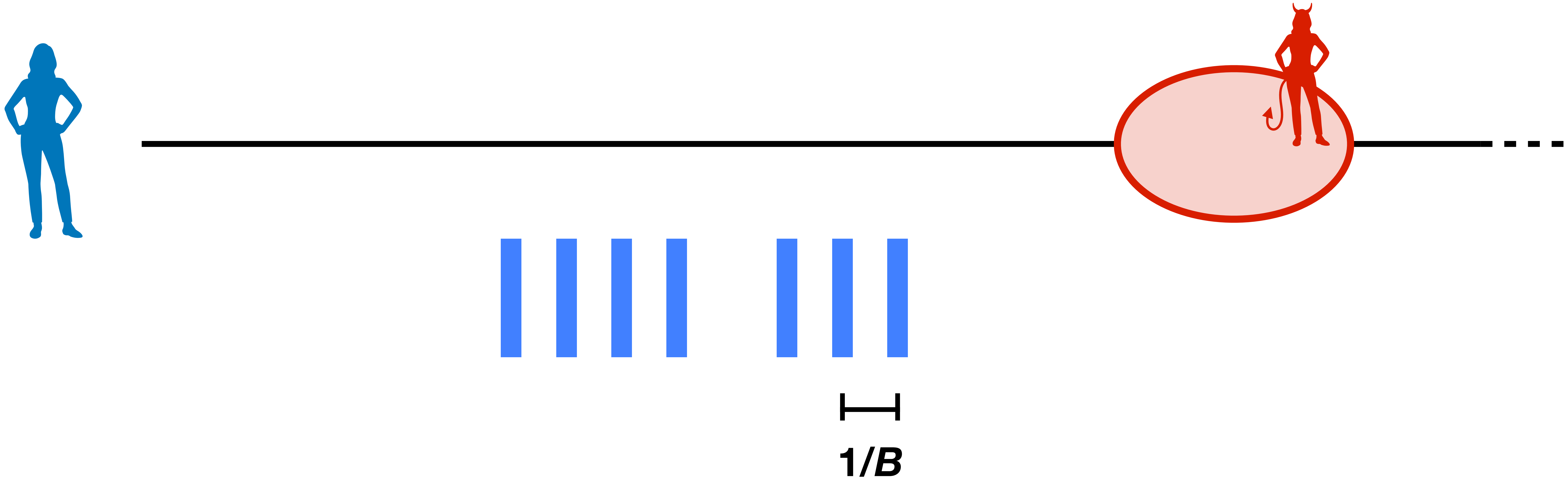


Resisting passive traffic analysis



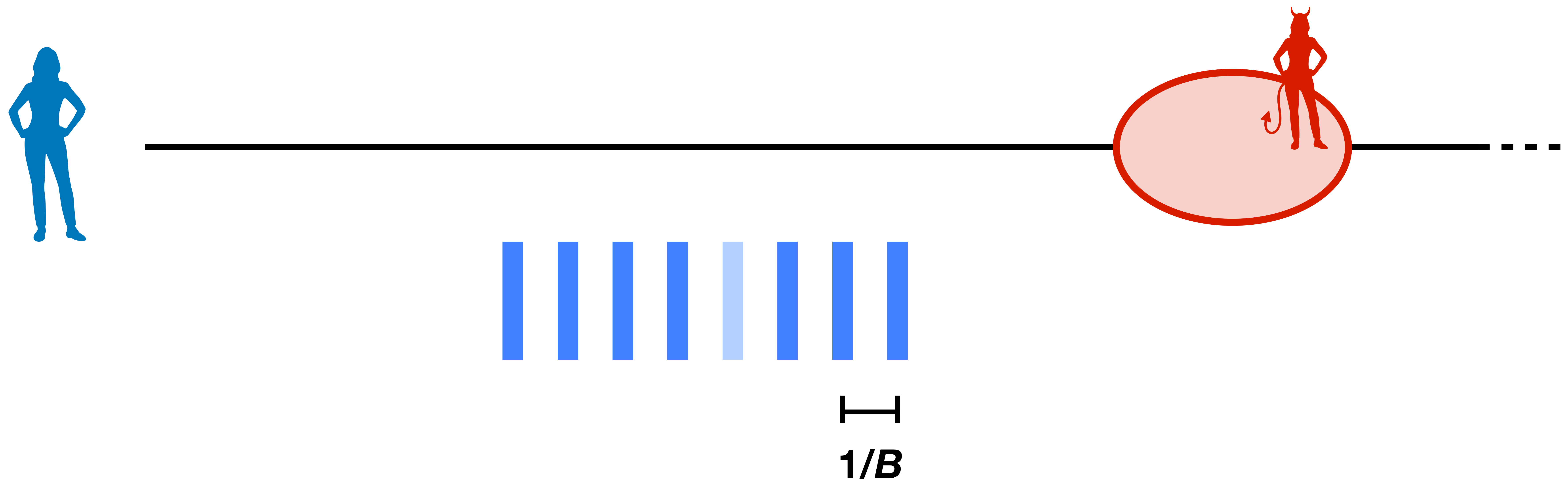
Resisting passive traffic analysis

- **Fixed rate 1/B**



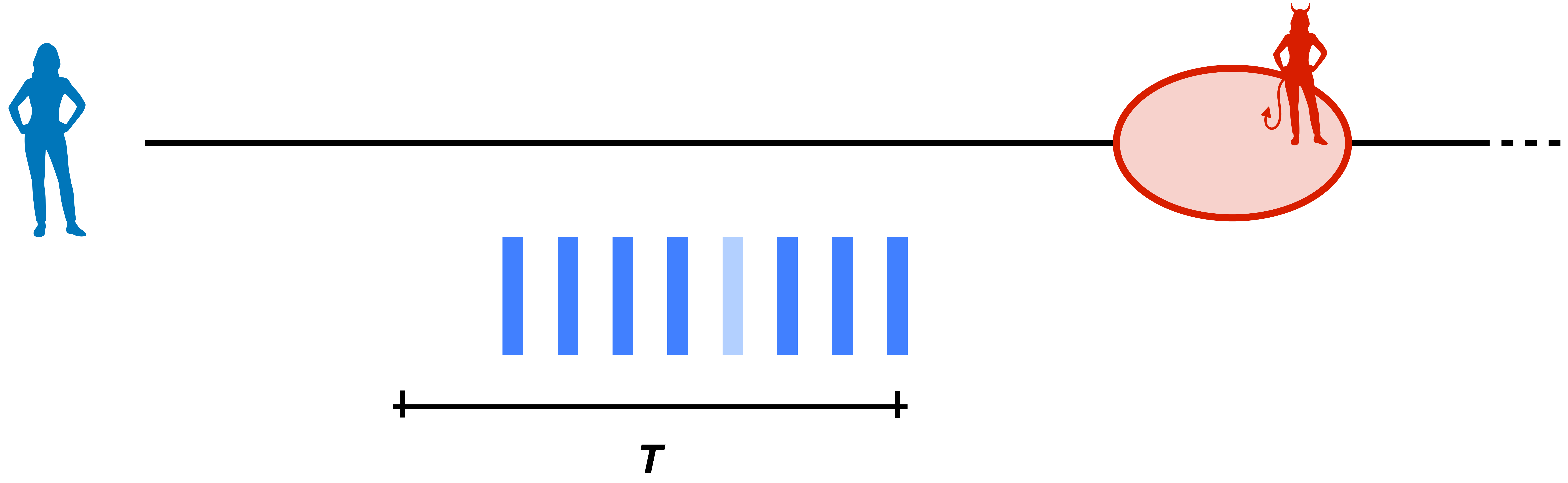
Resisting passive traffic analysis

- Fixed rate 1/B
- Chaff packets



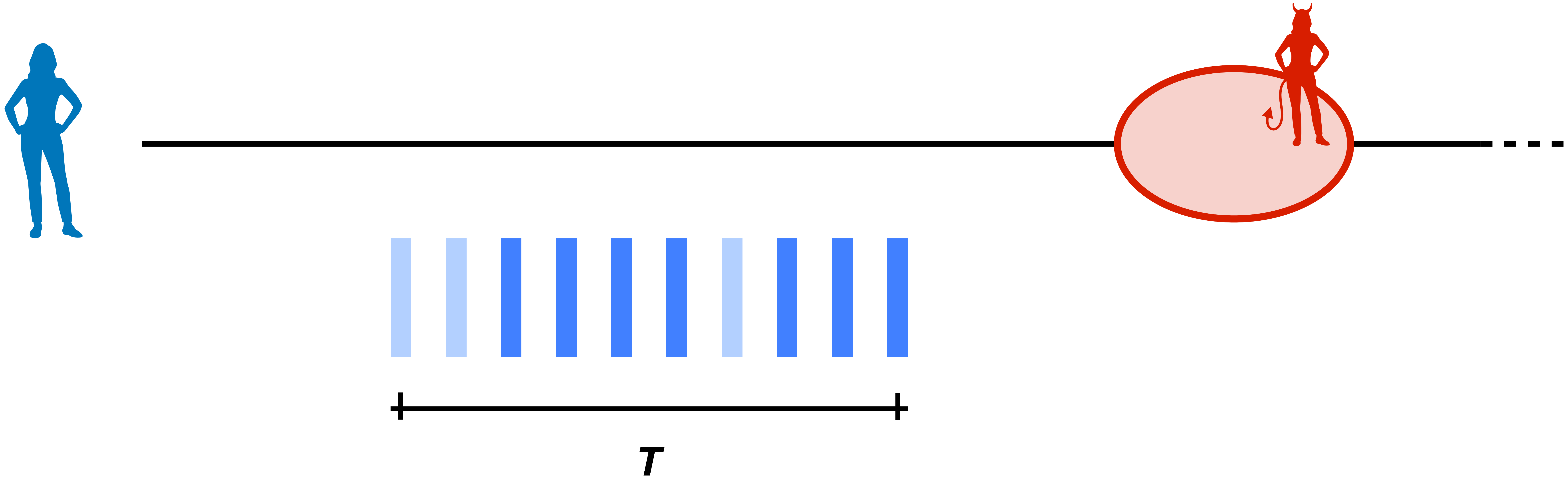
Resisting passive traffic analysis

- Fixed rate 1/B
- Chaff packets
- Fixed duration *T*



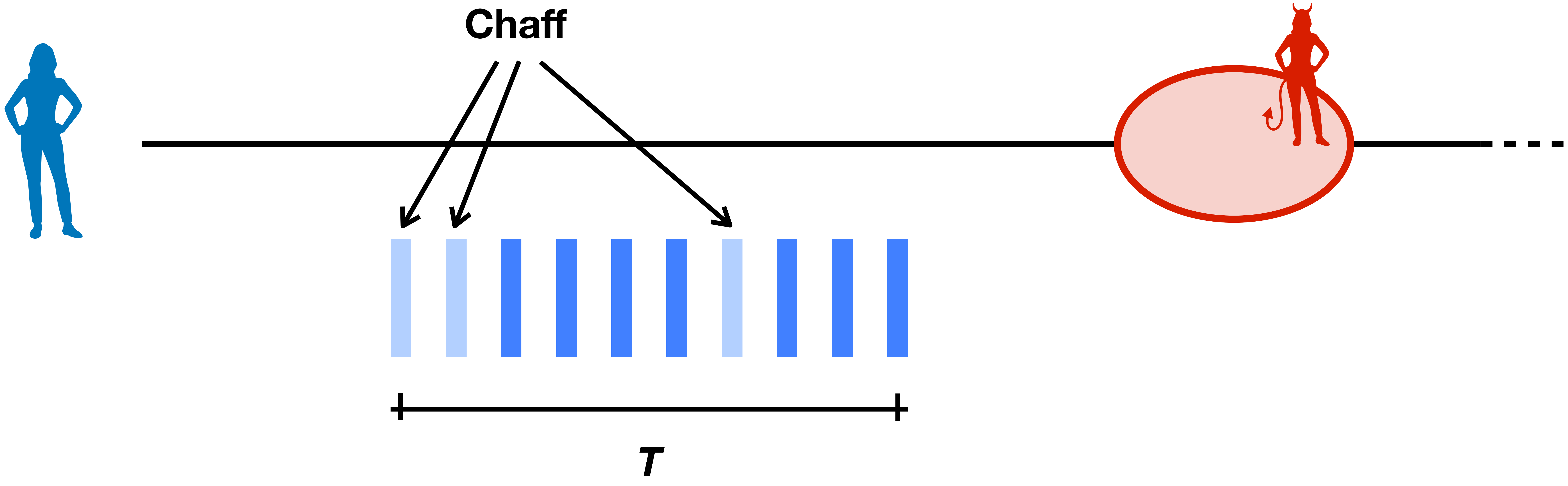
Resisting passive traffic analysis

- Fixed rate 1/B
- Chaff packets
- Fixed duration *T*



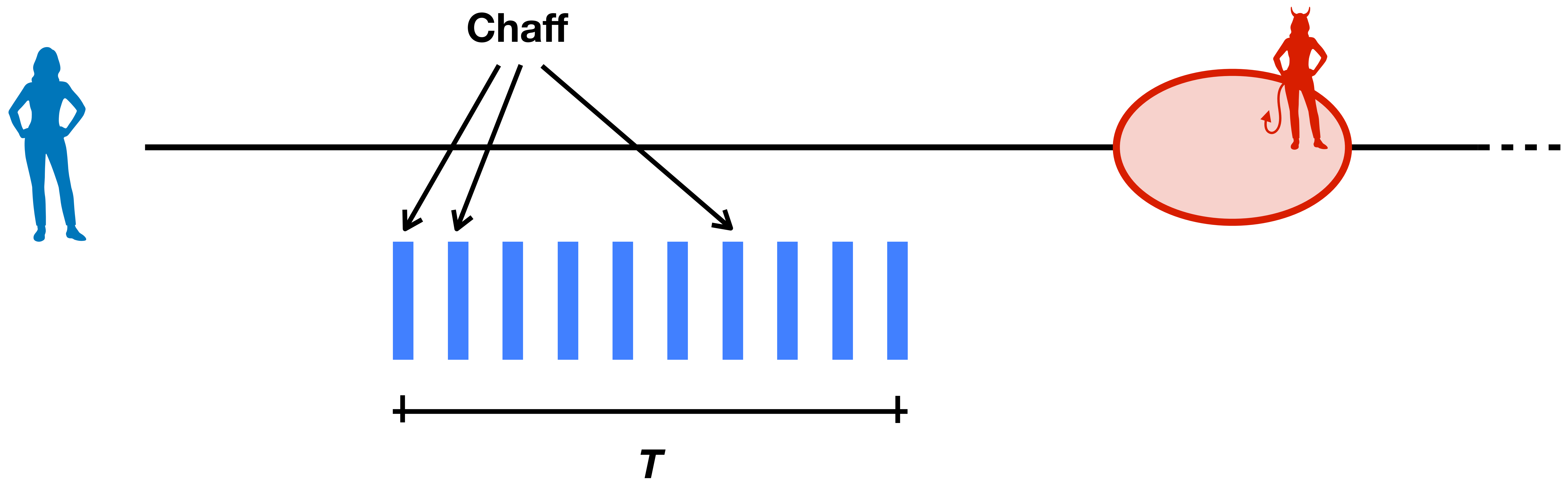
Resisting passive traffic analysis

- Fixed rate 1/B
- Chaff packets
- Fixed duration *T*



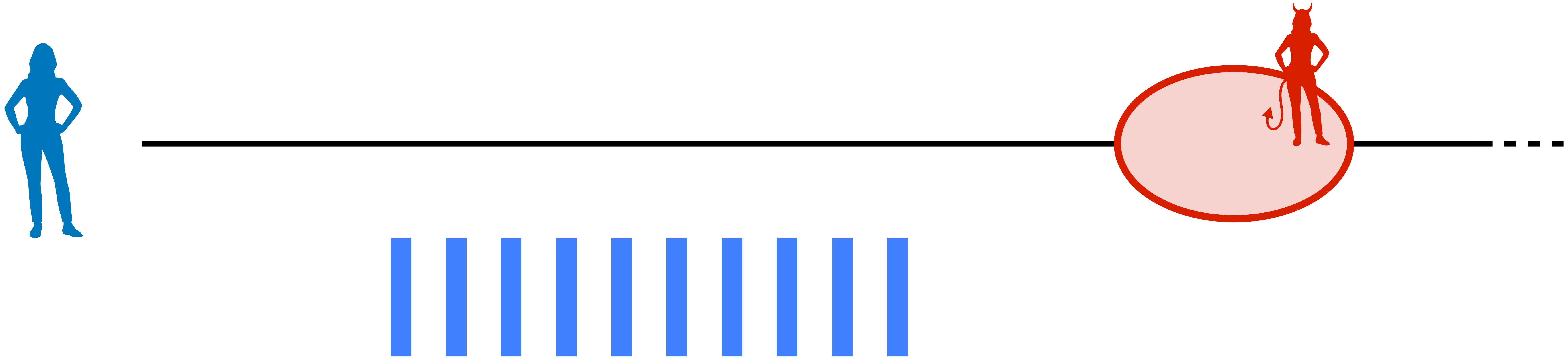
Resisting passive traffic analysis

- Fixed rate 1/B
- Chaff packets
- Fixed duration *T*



Resisting passive traffic analysis

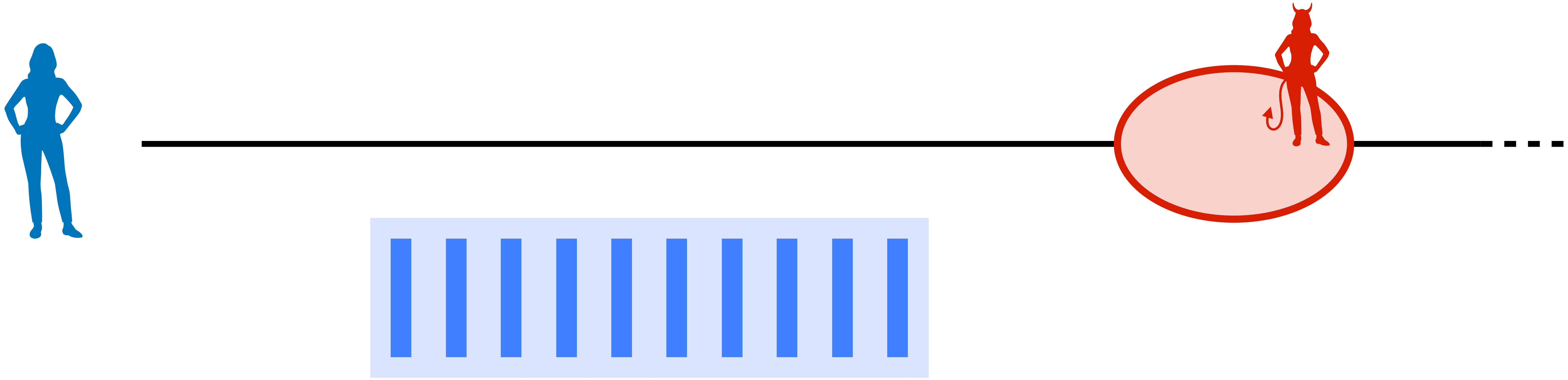
- Fixed rate 1/B
- Chaff packets
- Fixed duration *T*
- *Same for everyone*



Resisting passive traffic analysis

- Fixed rate 1/B
- Chaff packets
- Fixed duration *T*
- *Same for everyone*

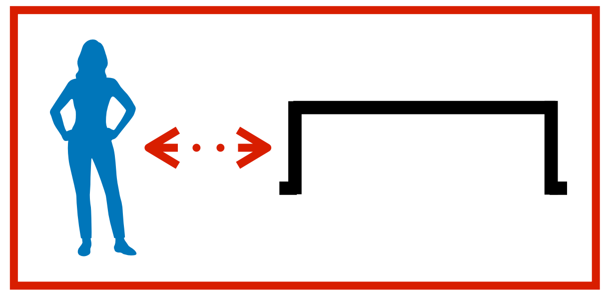
Flowlet

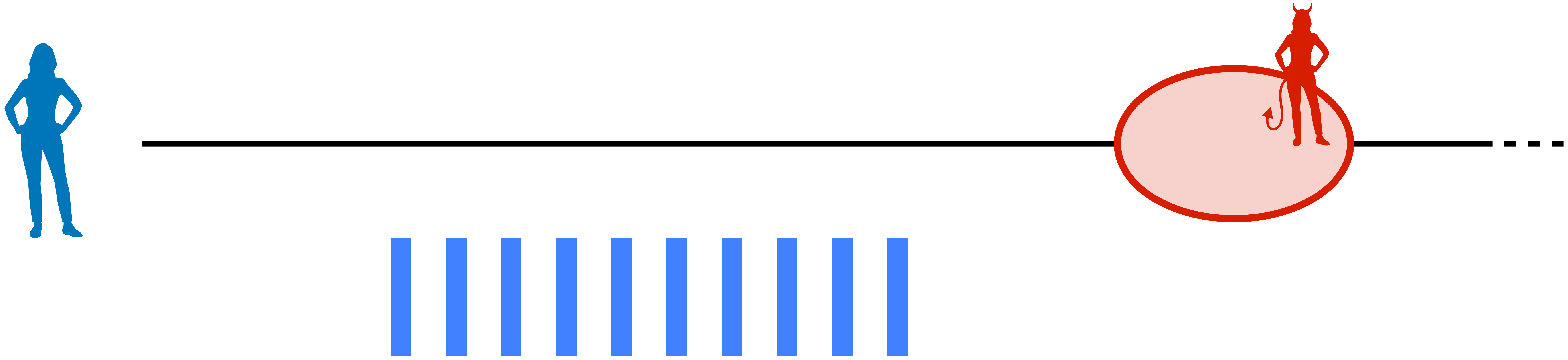


Resisting passive traffic analysis

- **Fixed rate 1/B**
- **Chaff packets**
- **Fixed duration *T***
- ***Same for everyone***

Flowlet

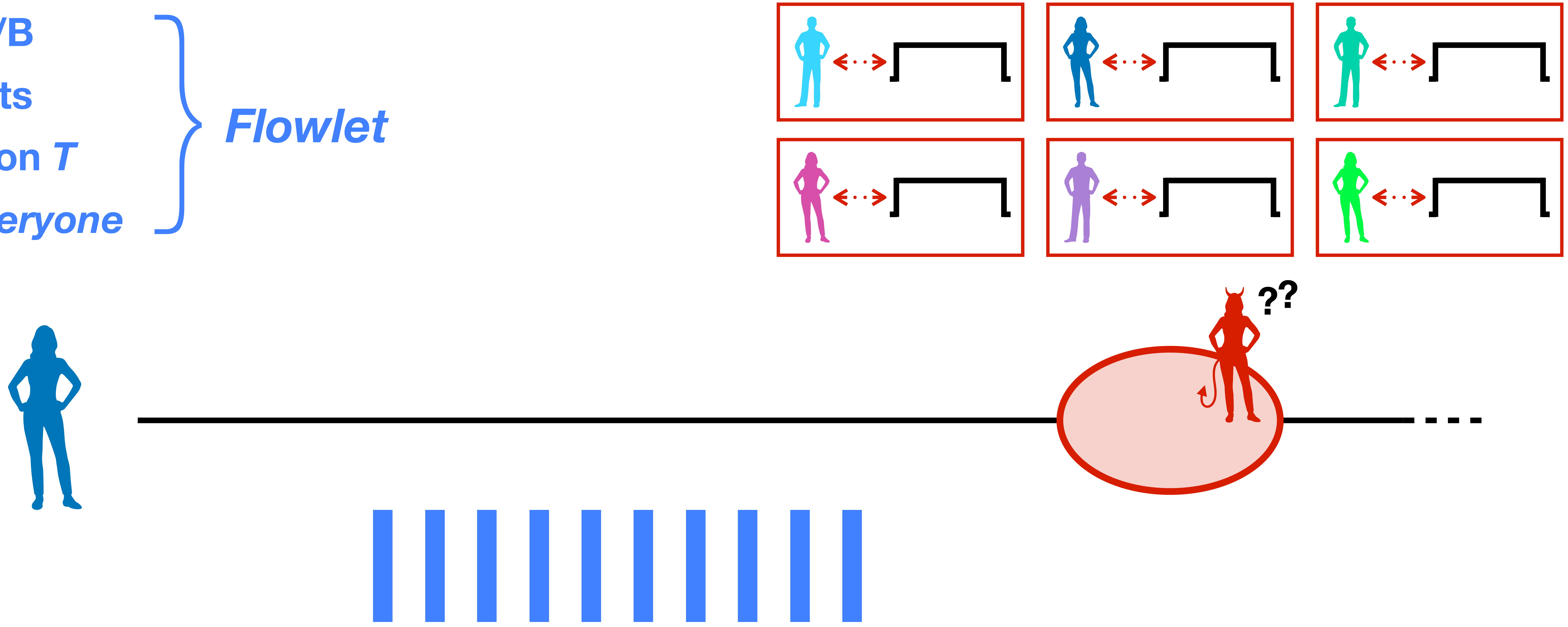




Resisting passive traffic analysis

- **Fixed rate 1/B**
- **Chaff packets**
- **Fixed duration *T***
- ***Same for everyone***

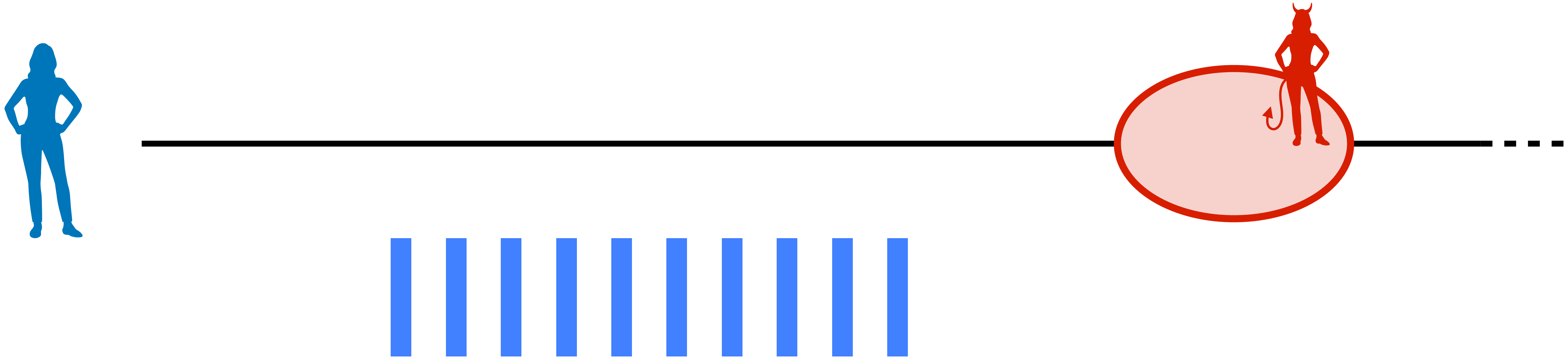
Flowlet



Resisting passive traffic analysis

- **Fixed rate 1/B**
- **Chaff packets**
- **Fixed duration *T***
- ***Same for everyone***

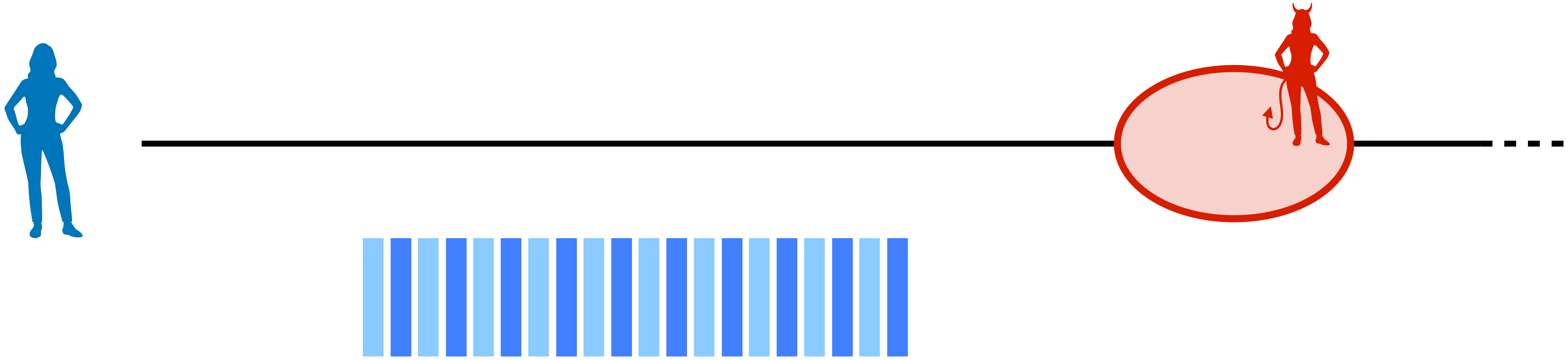
Flowlet



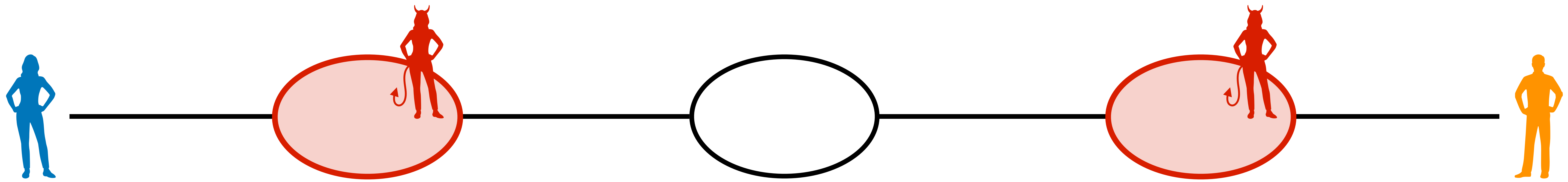
Resisting passive traffic analysis

- Fixed rate 1/B
- Chaff packets
- Fixed duration *T*
- *Same for everyone*

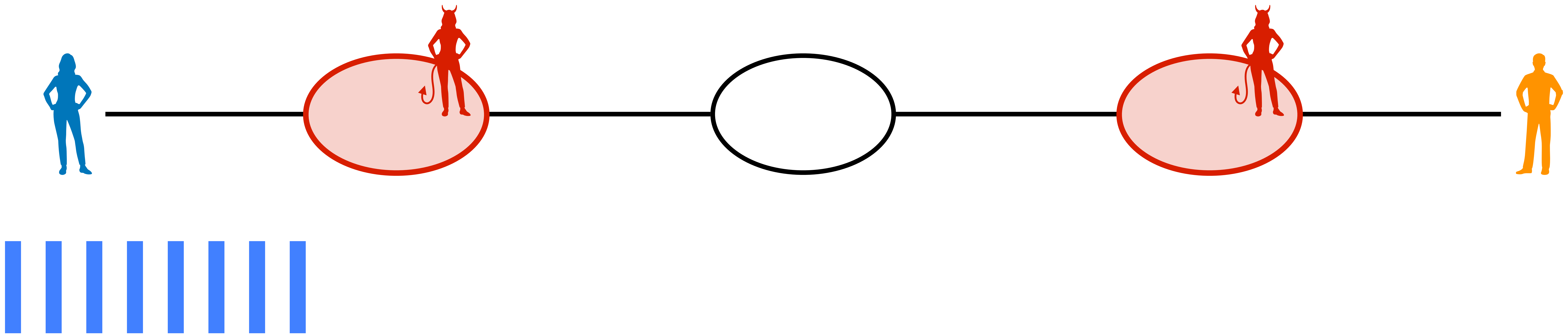
Flowlet



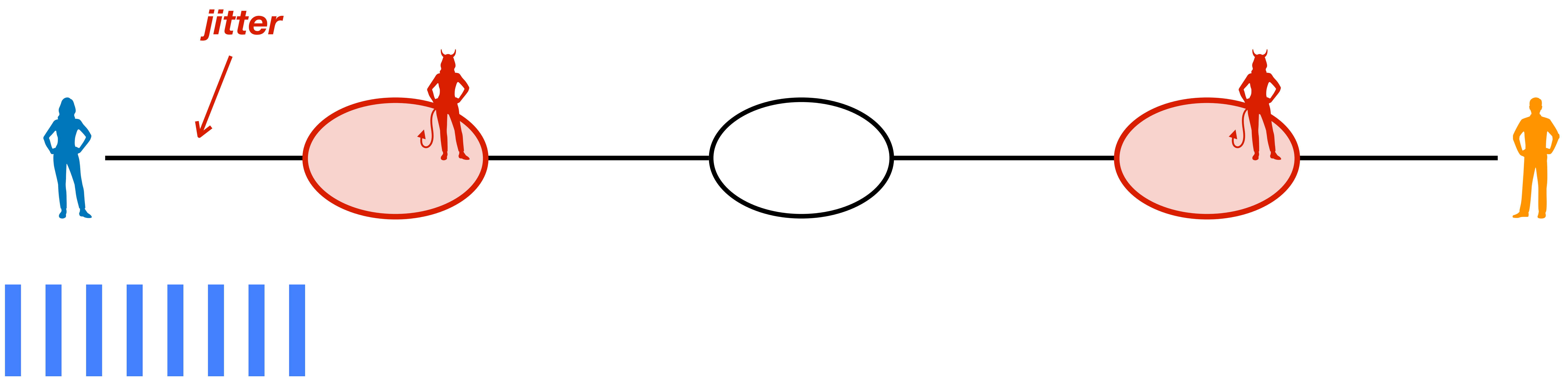
Resisting passive traffic analysis



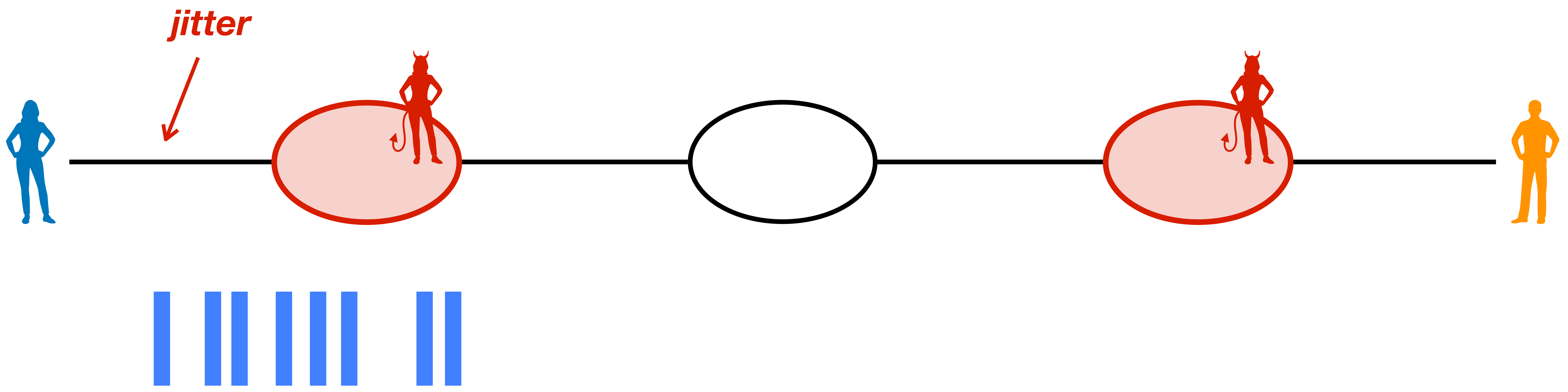
Resisting passive traffic analysis



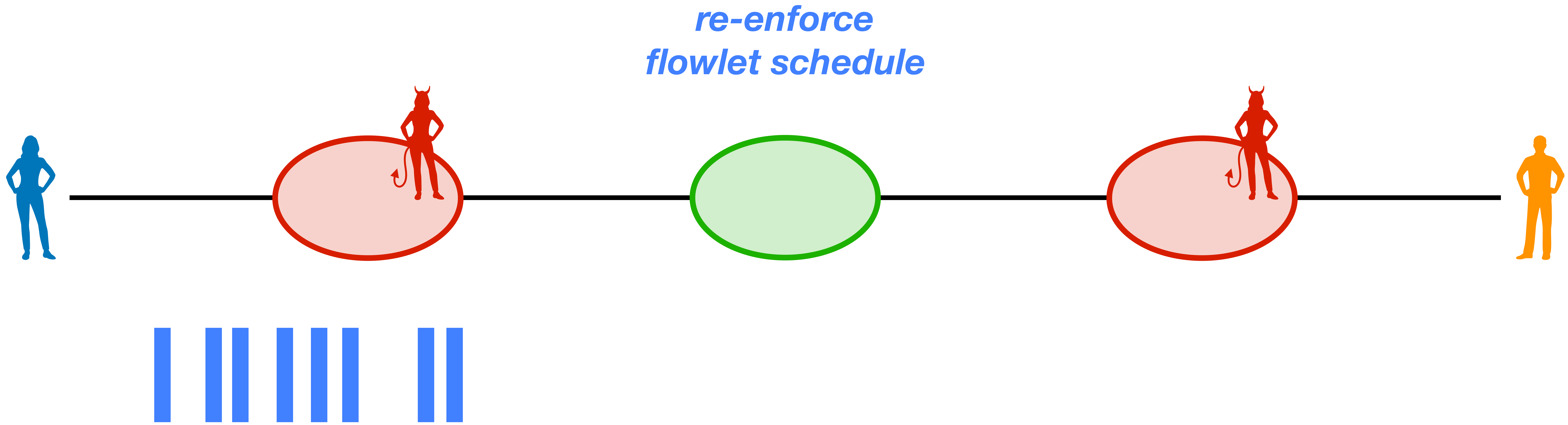
Resisting passive traffic analysis



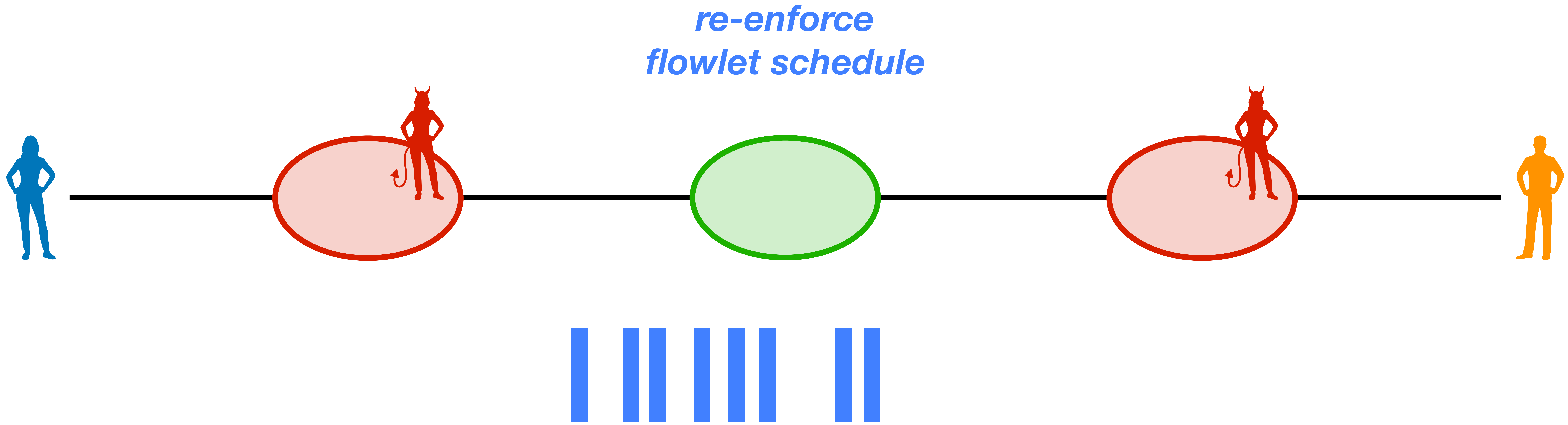
Resisting passive traffic analysis



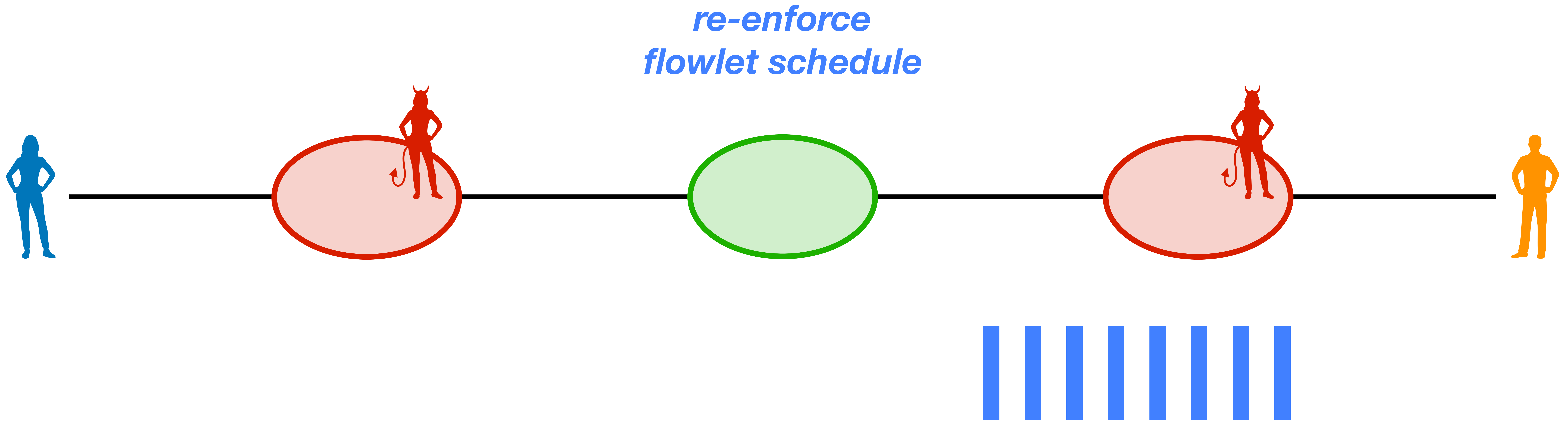
Resisting passive traffic analysis



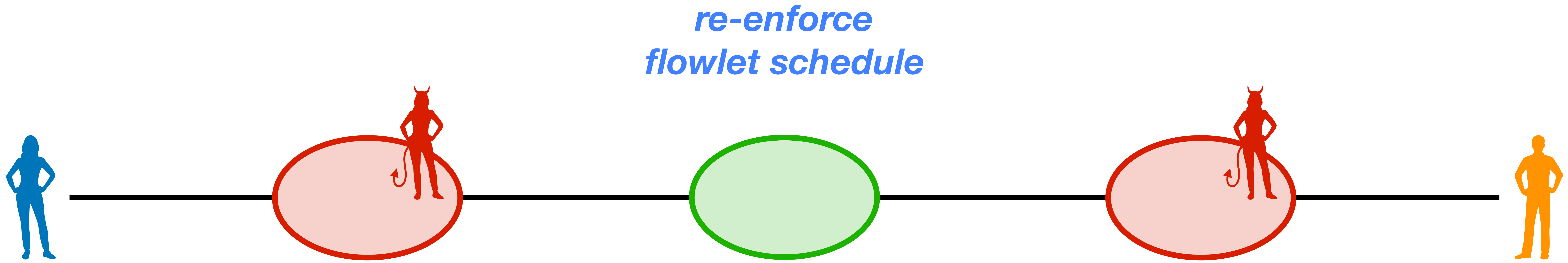
Resisting passive traffic analysis



Resisting passive traffic analysis

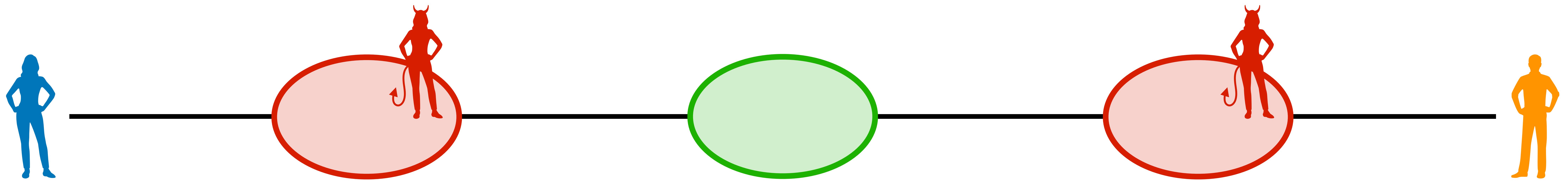


Resisting passive traffic analysis



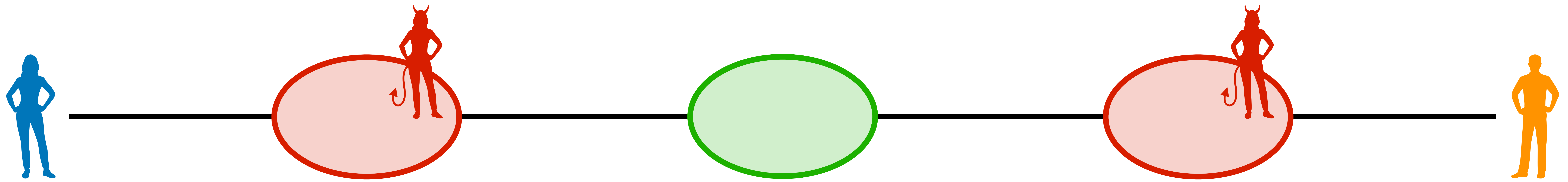
Resisting active traffic analysis

Packet dropping



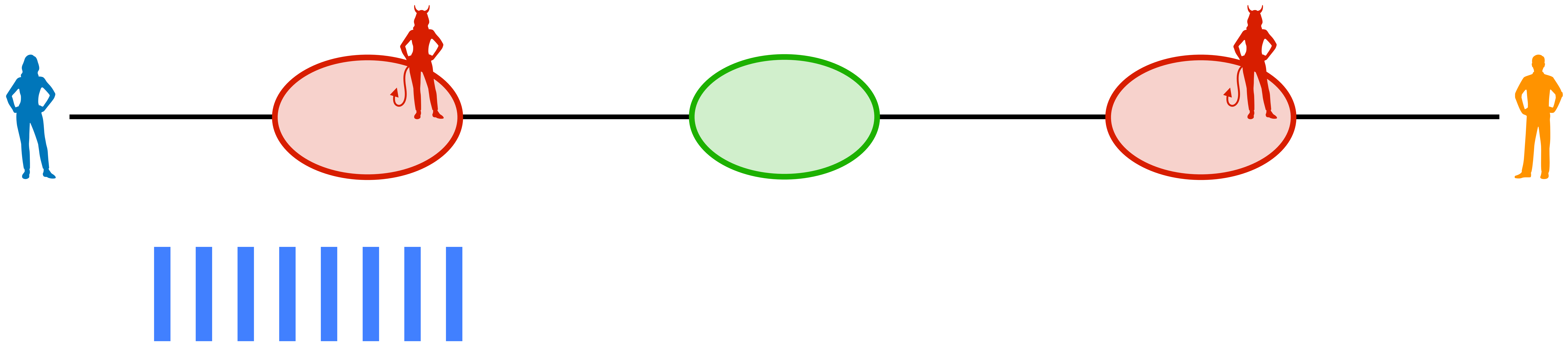
Resisting active traffic analysis

Packet dropping



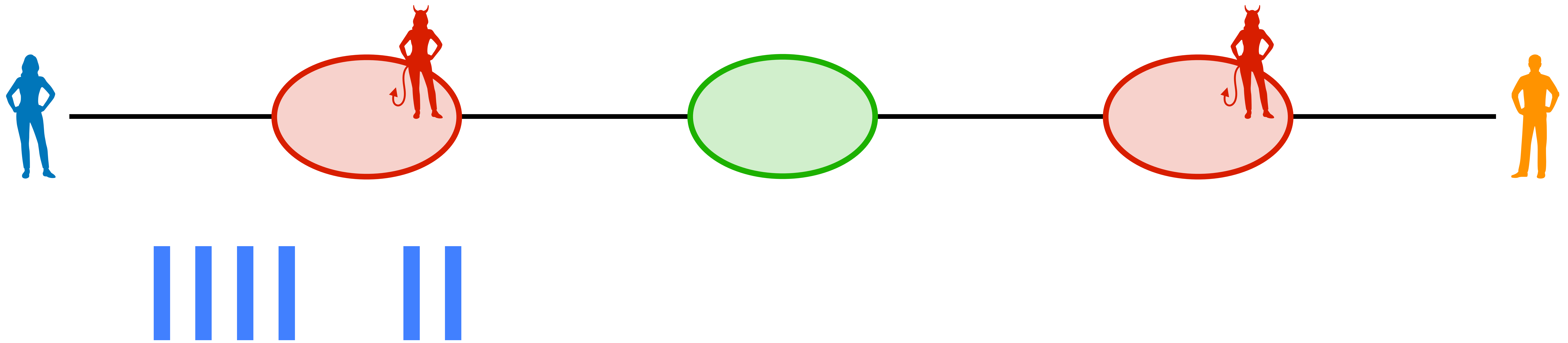
Resisting active traffic analysis

Packet dropping



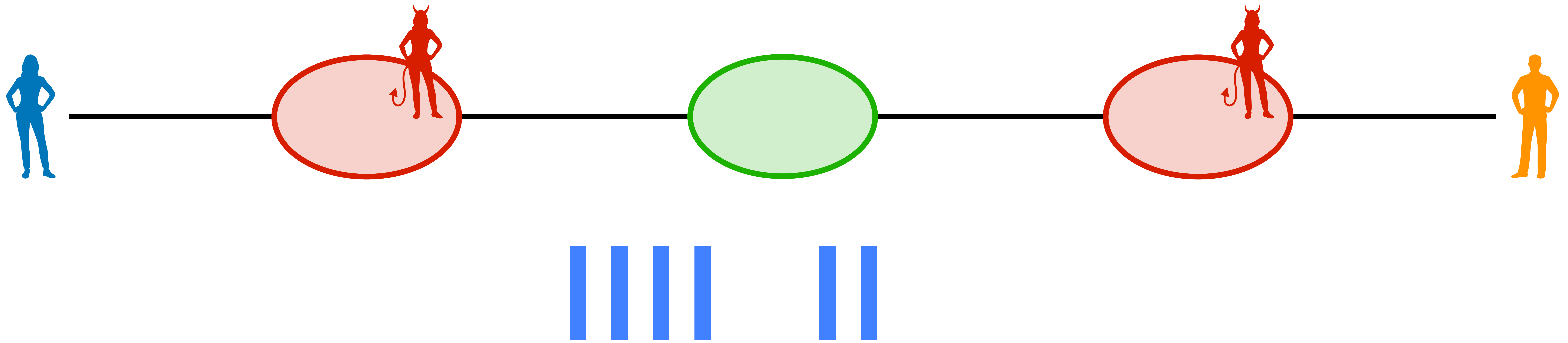
Resisting active traffic analysis

Packet dropping



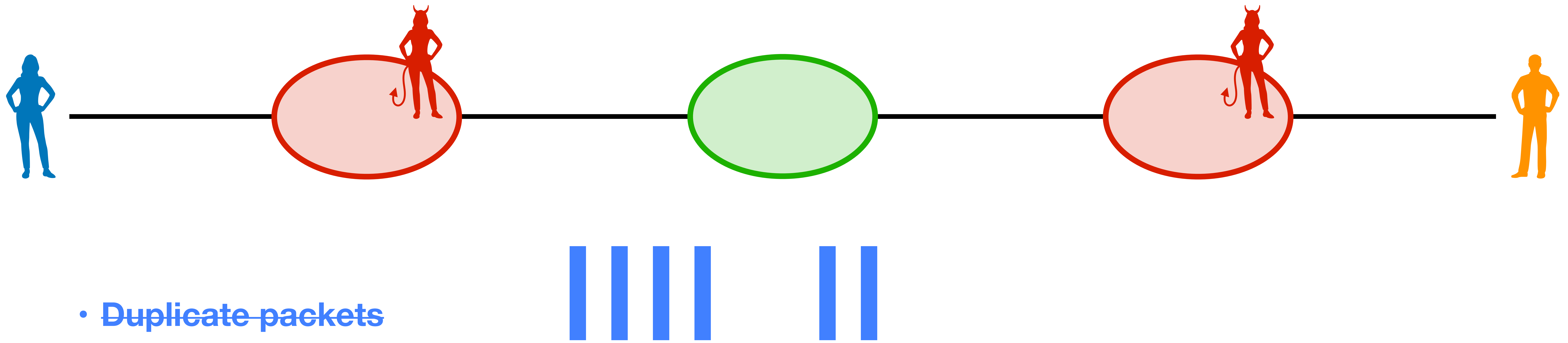
Resisting active traffic analysis

Packet dropping



Resisting active traffic analysis

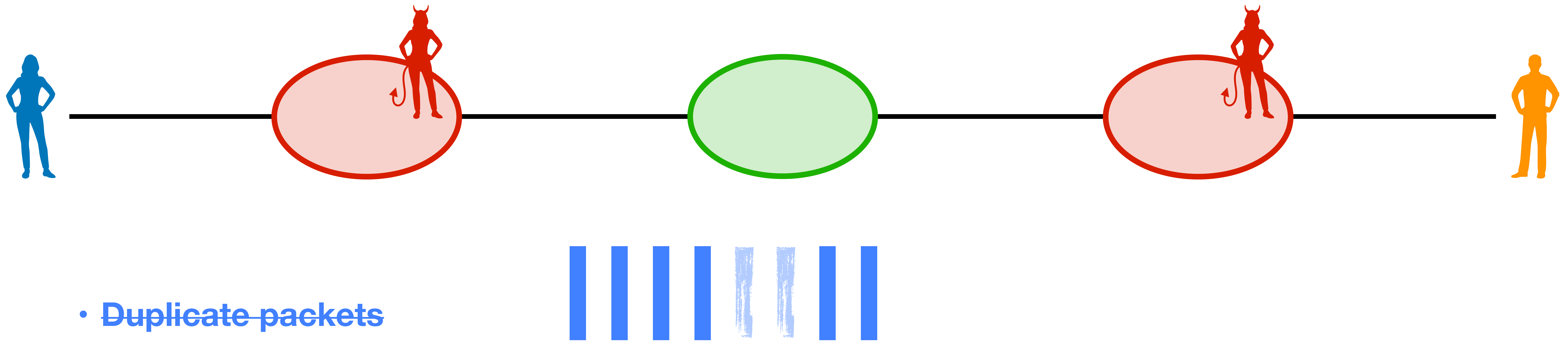
Packet dropping



- ~~**Duplicate packets**~~

Resisting active traffic analysis

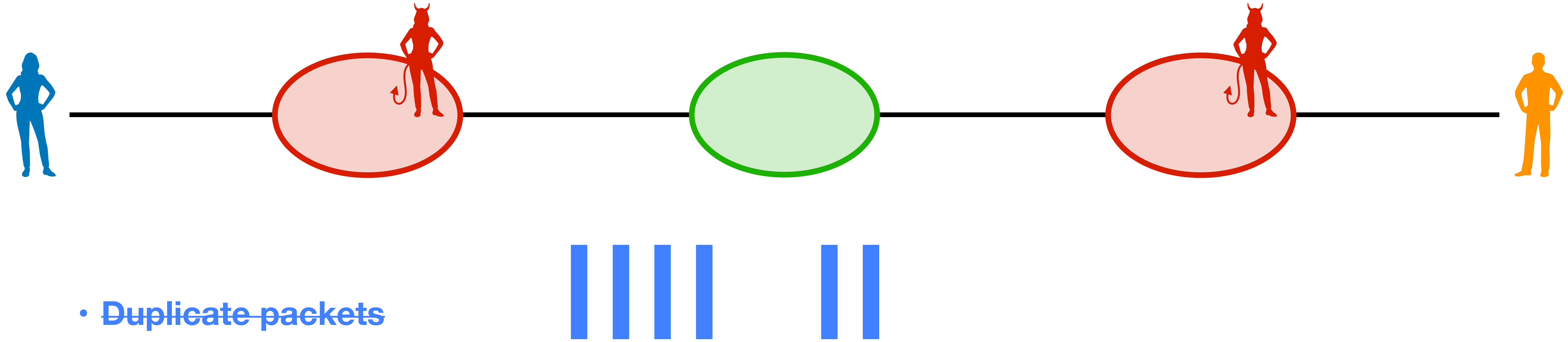
Packet dropping



- ~~Duplicate packets~~
- ~~Create new packets~~

Resisting active traffic analysis

Packet dropping

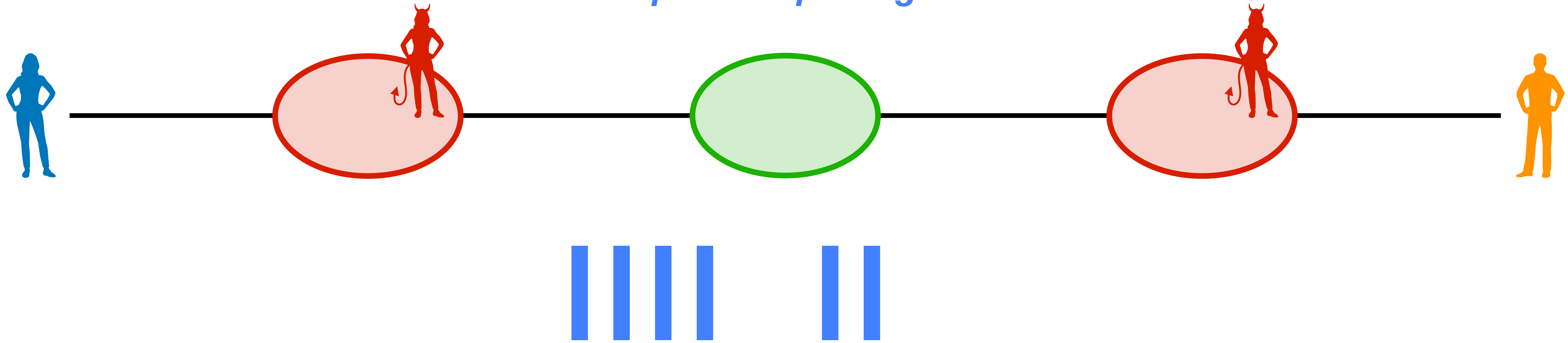


- ~~Duplicate packets~~
- ~~Create new packets~~
- Sender send more?

Resisting active traffic analysis

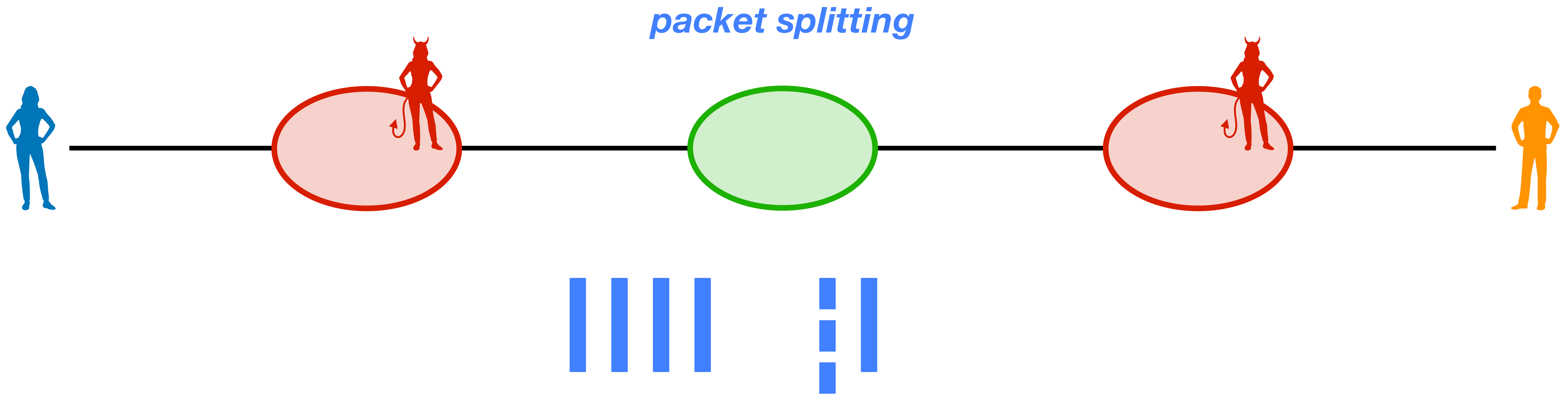
Packet dropping

packet splitting



Resisting active traffic analysis

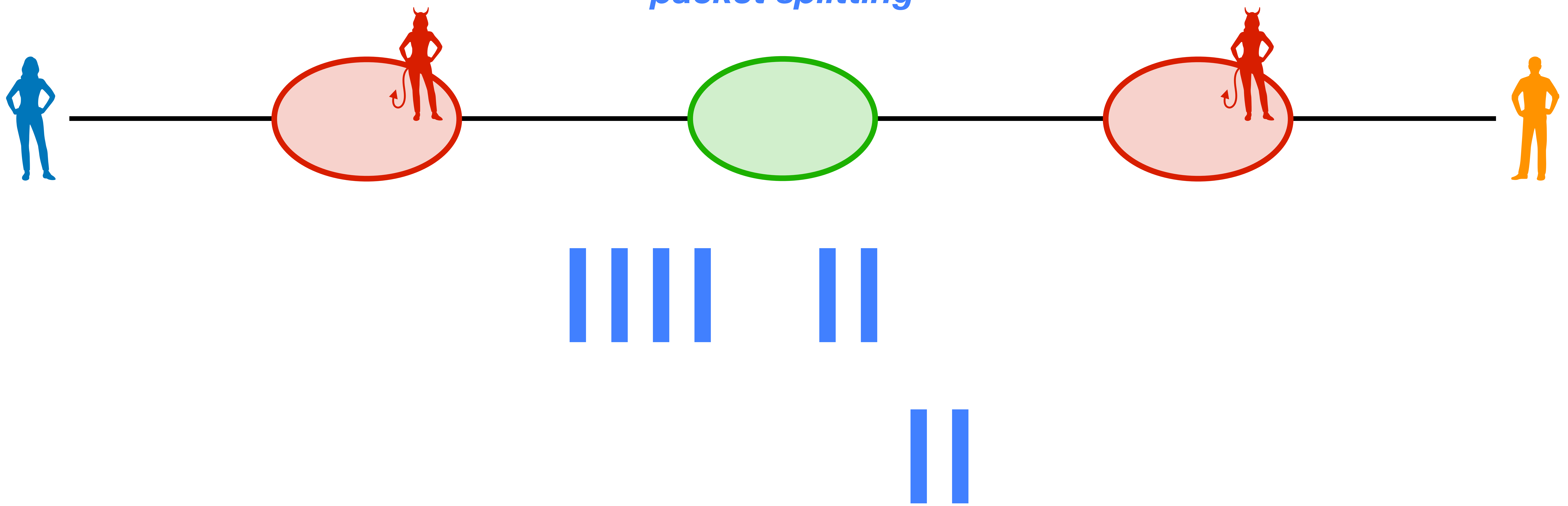
Packet dropping



Resisting active traffic analysis

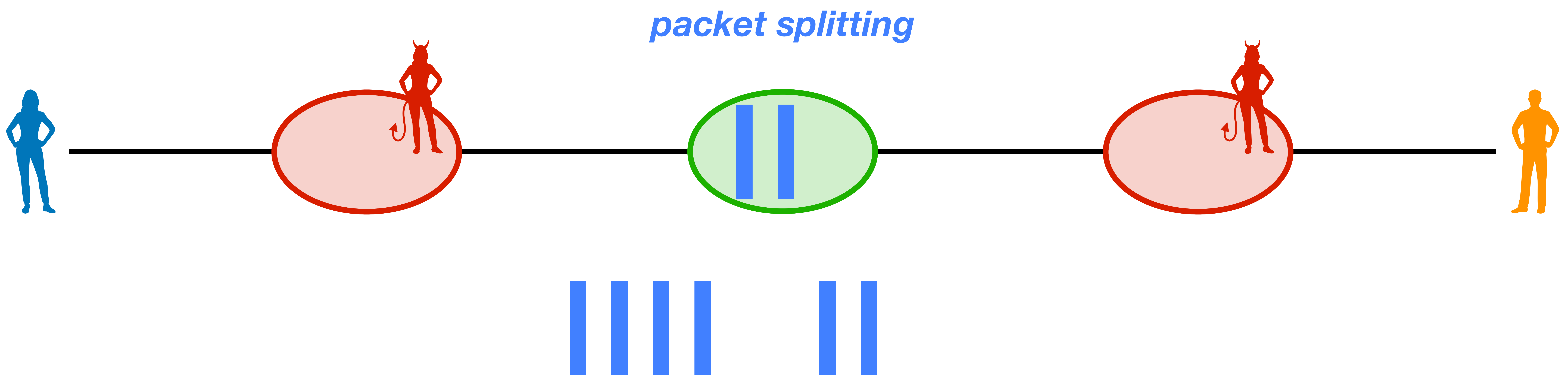
Packet dropping

packet splitting



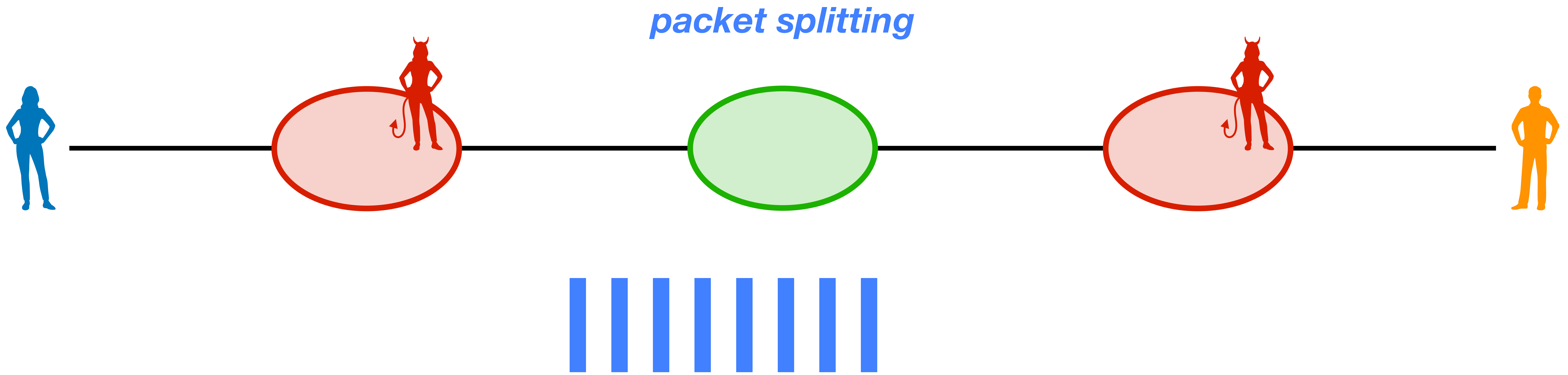
Resisting active traffic analysis

Packet dropping



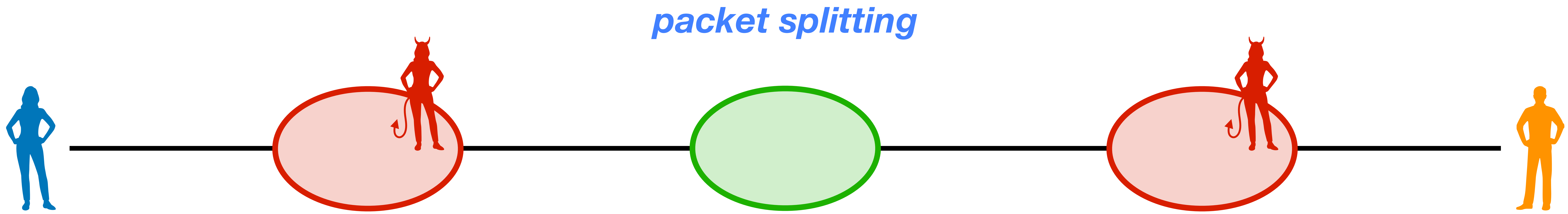
Resisting active traffic analysis

Packet dropping



Resisting active traffic analysis

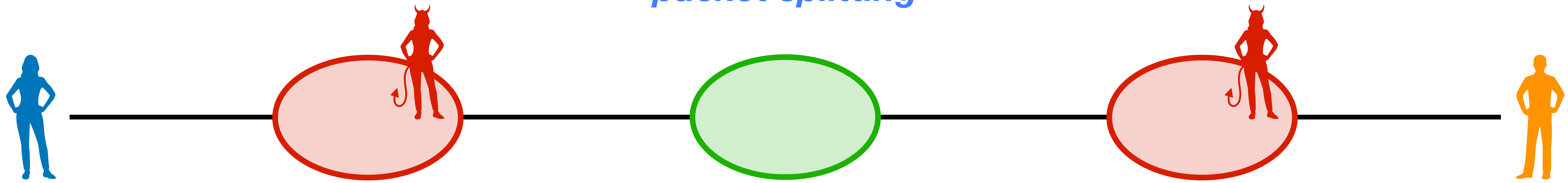
Packet dropping



Resisting active traffic analysis

Packet dropping

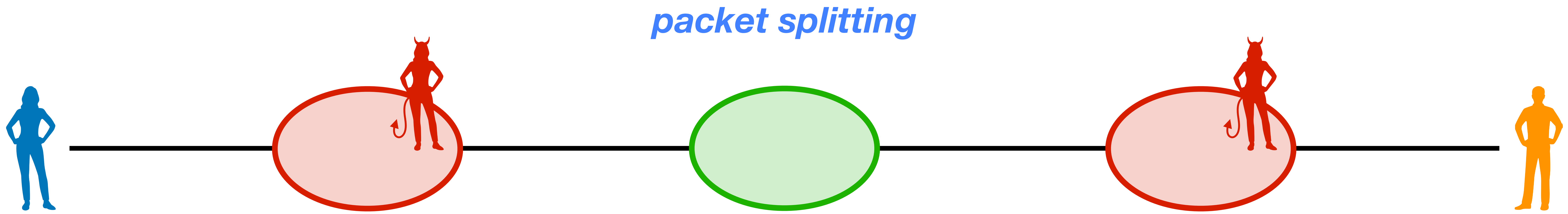
packet splitting



When is packet splitting done?

Resisting active traffic analysis

Packet dropping



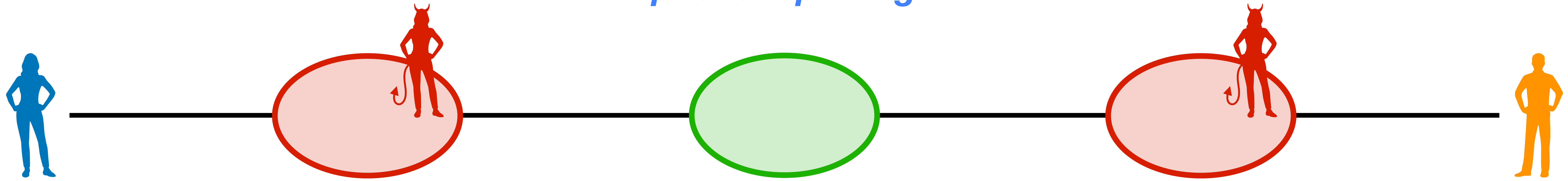
When is packet splitting done?

- **Sender includes splittable packets**

Resisting active traffic analysis

Packet dropping

packet splitting

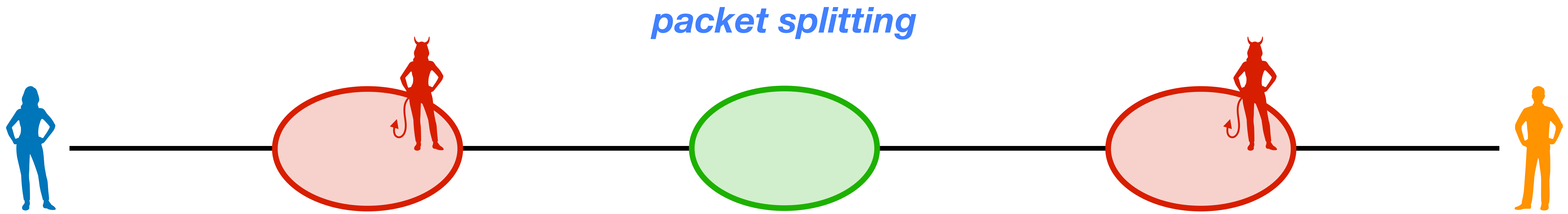


When is packet splitting done?

- **Sender includes splittable packets**
- **… for each AS on the path**

Resisting active traffic analysis

Packet dropping



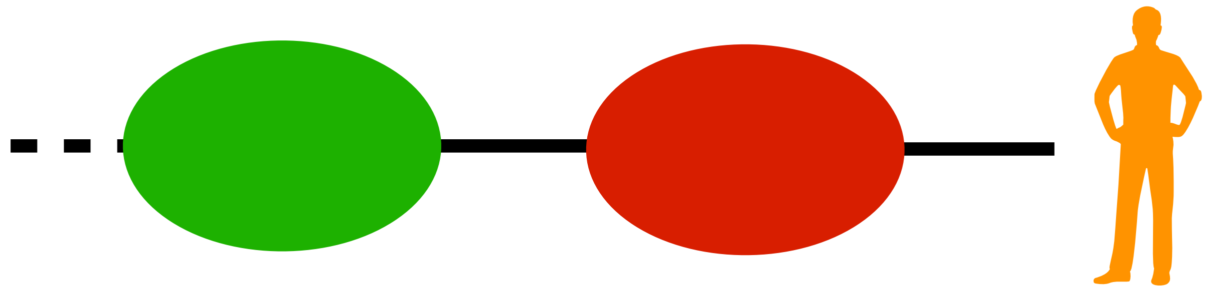
When is packet splitting done?

- **Sender includes splittable packets**
- **… for each AS on the path**
- **… at random intervals**

Packet splitting

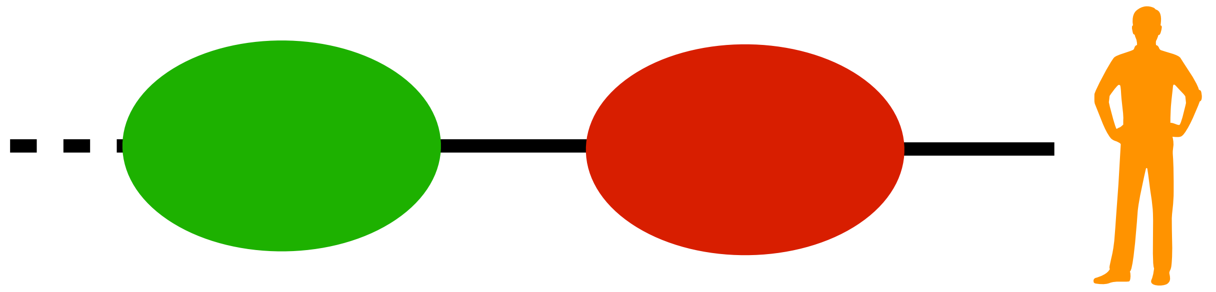
How does splitting work concretely?

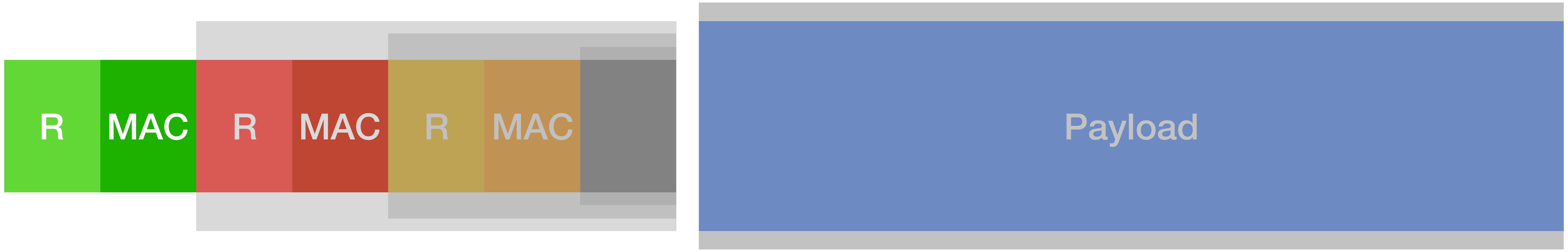
Packet splitting



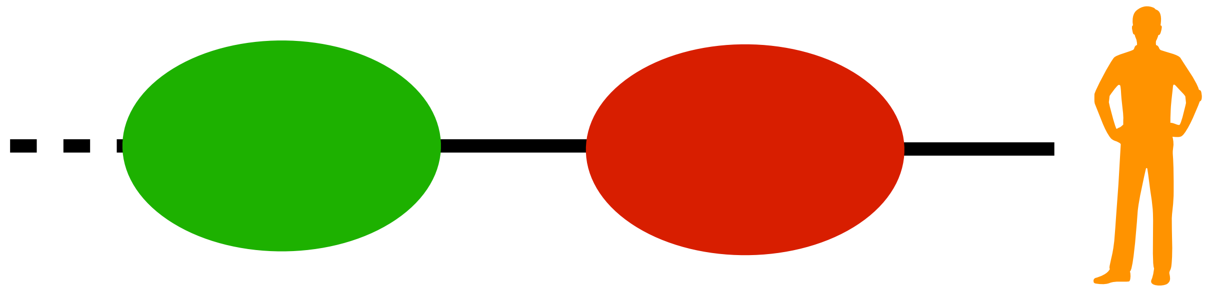
How does splitting work concretely?

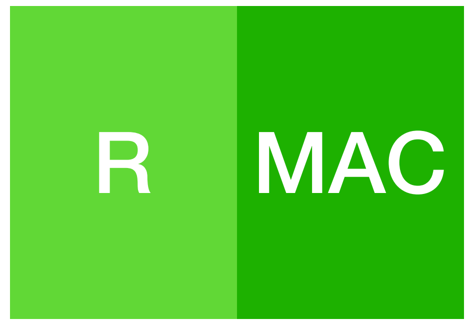
Packet splitting



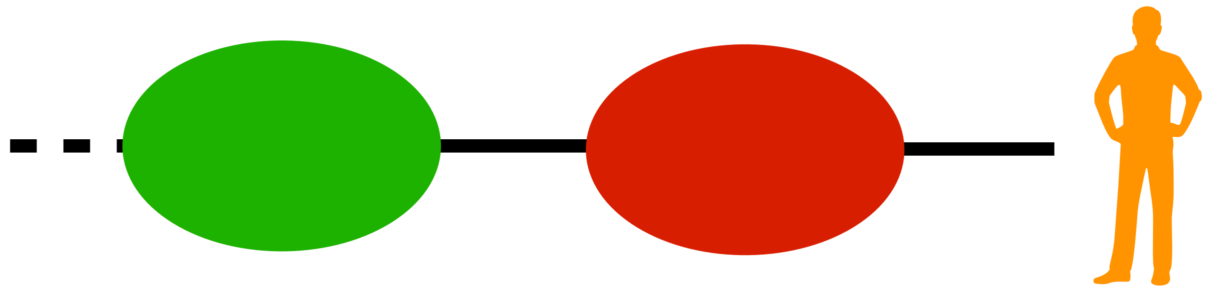


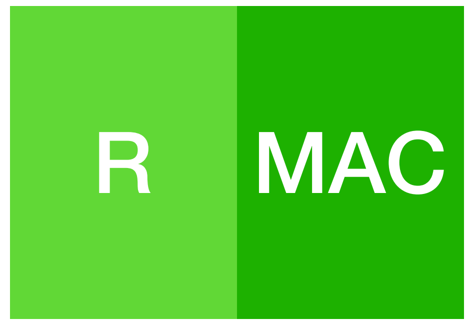
Packet splitting



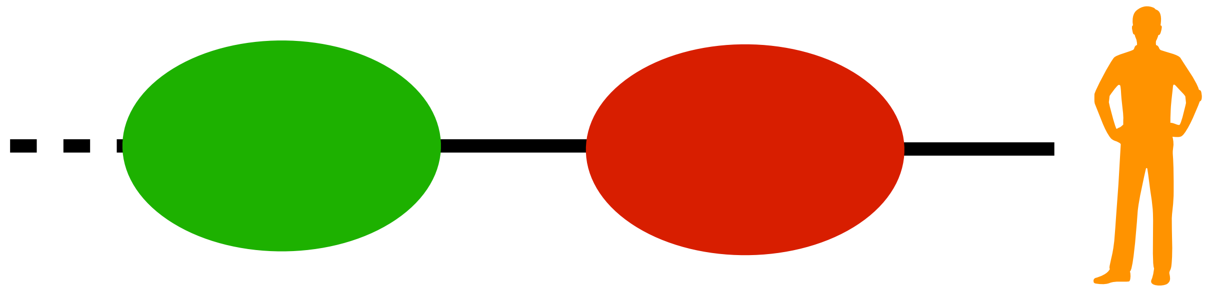


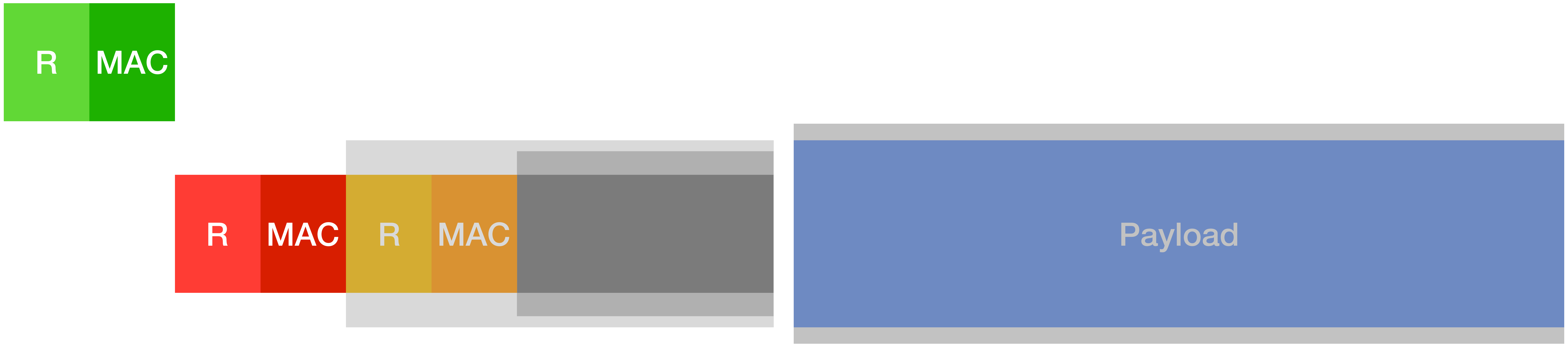
Packet splitting



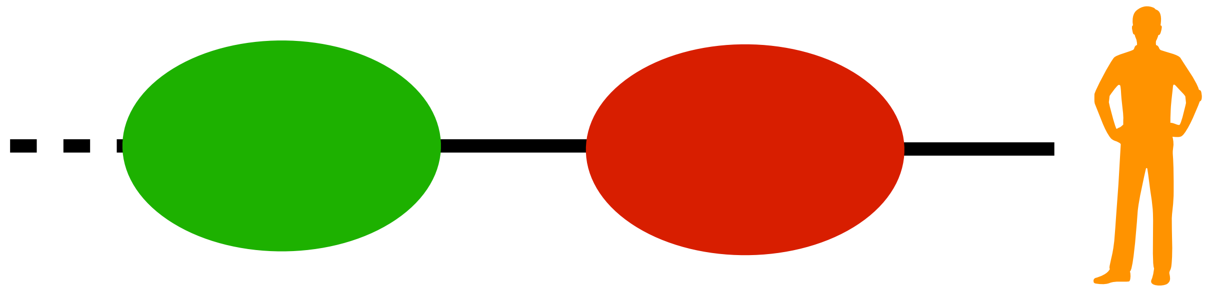


Packet splitting

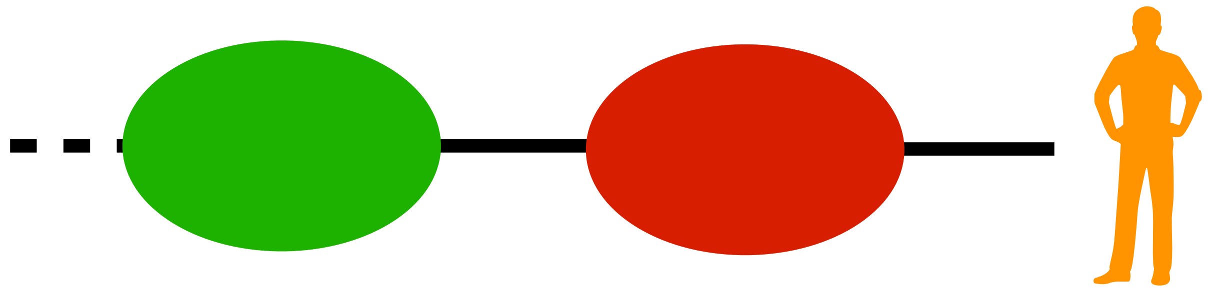




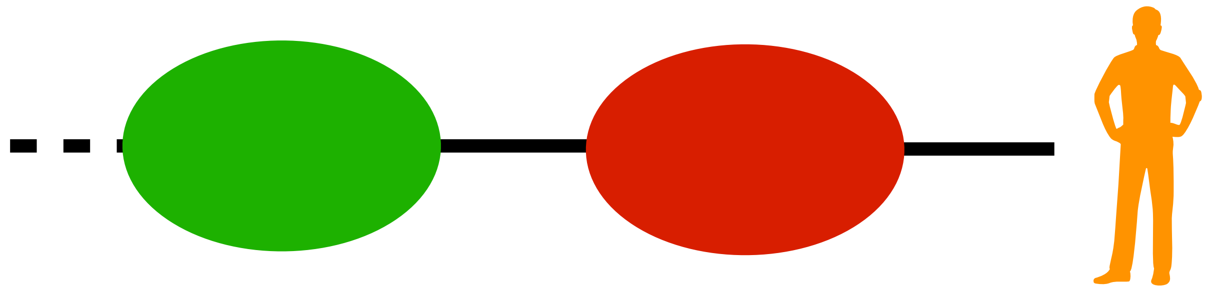
Packet splitting



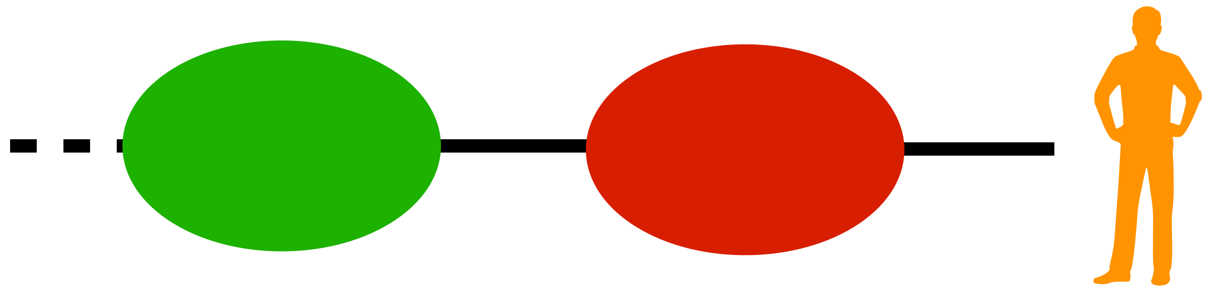
Packet splitting



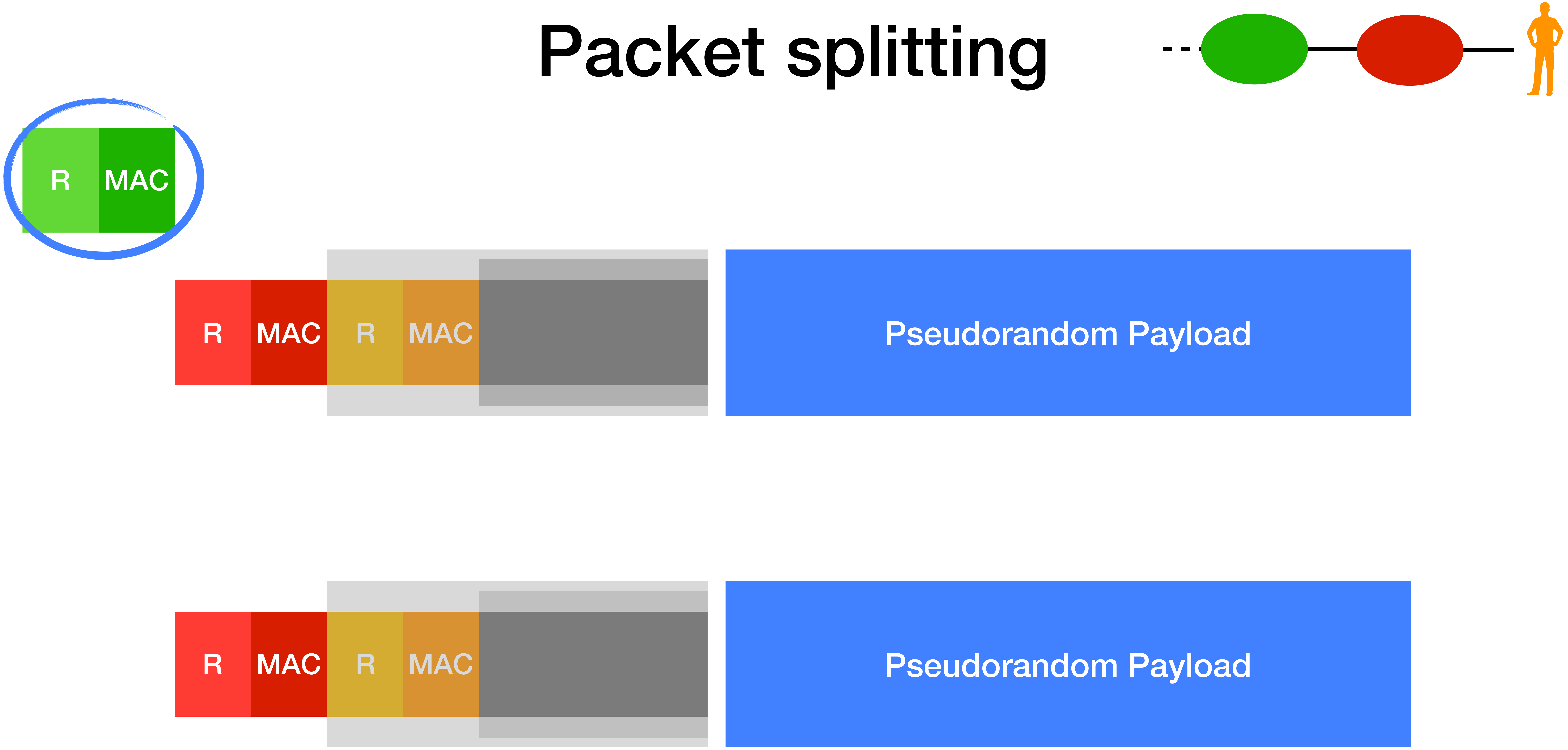
Packet splitting



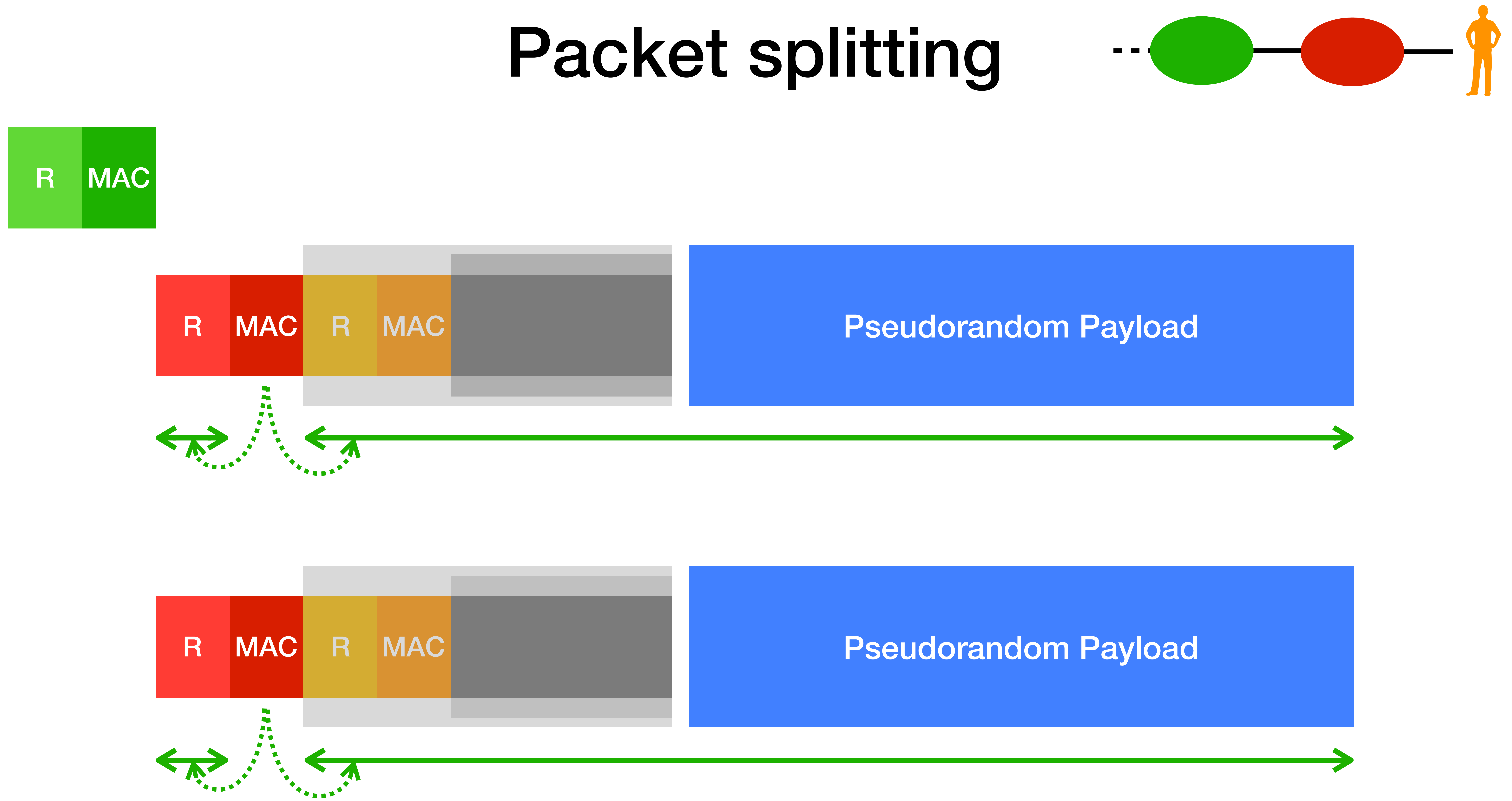
Packet splitting



Packet splitting



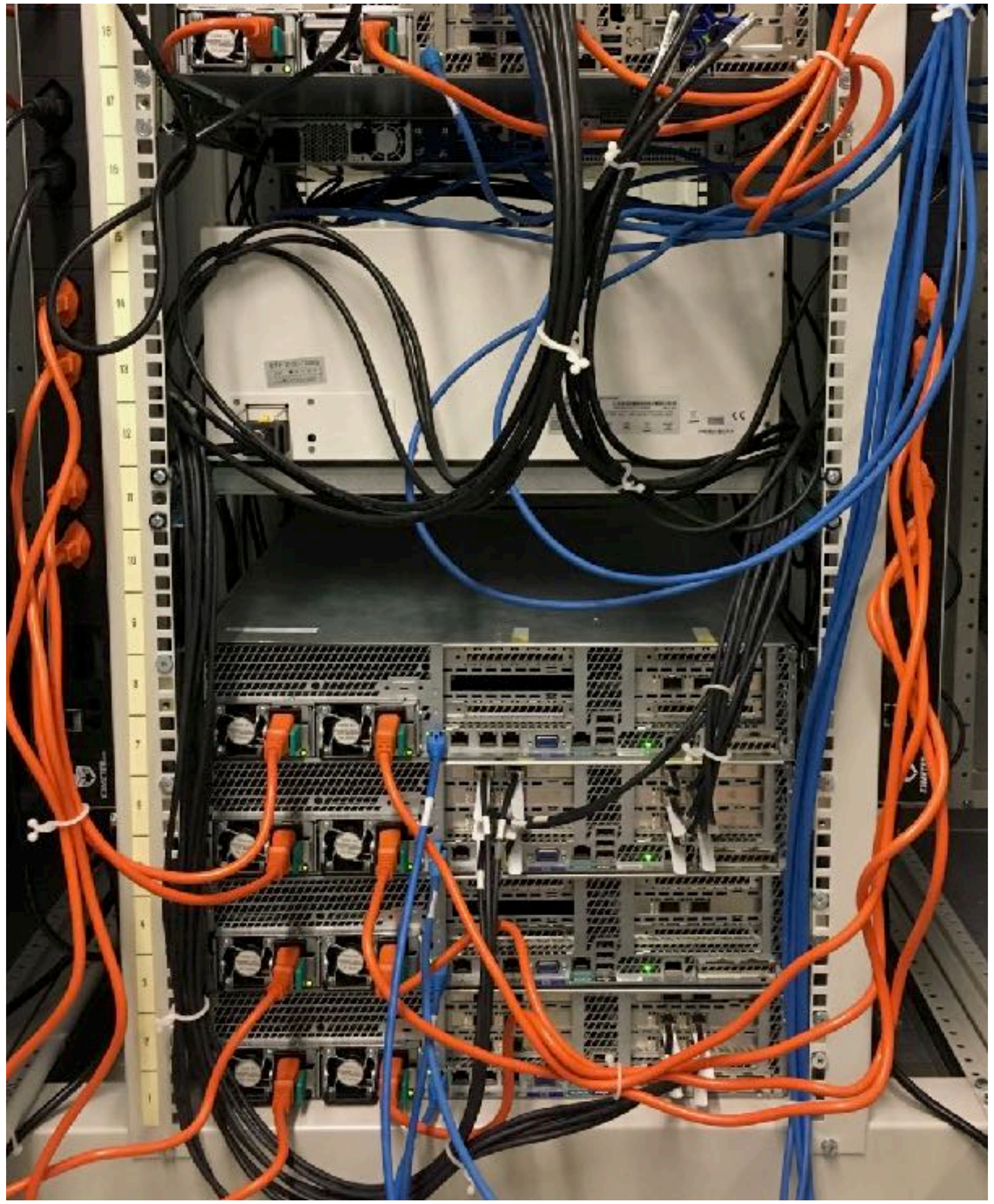
Packet splitting



TARANET Performance

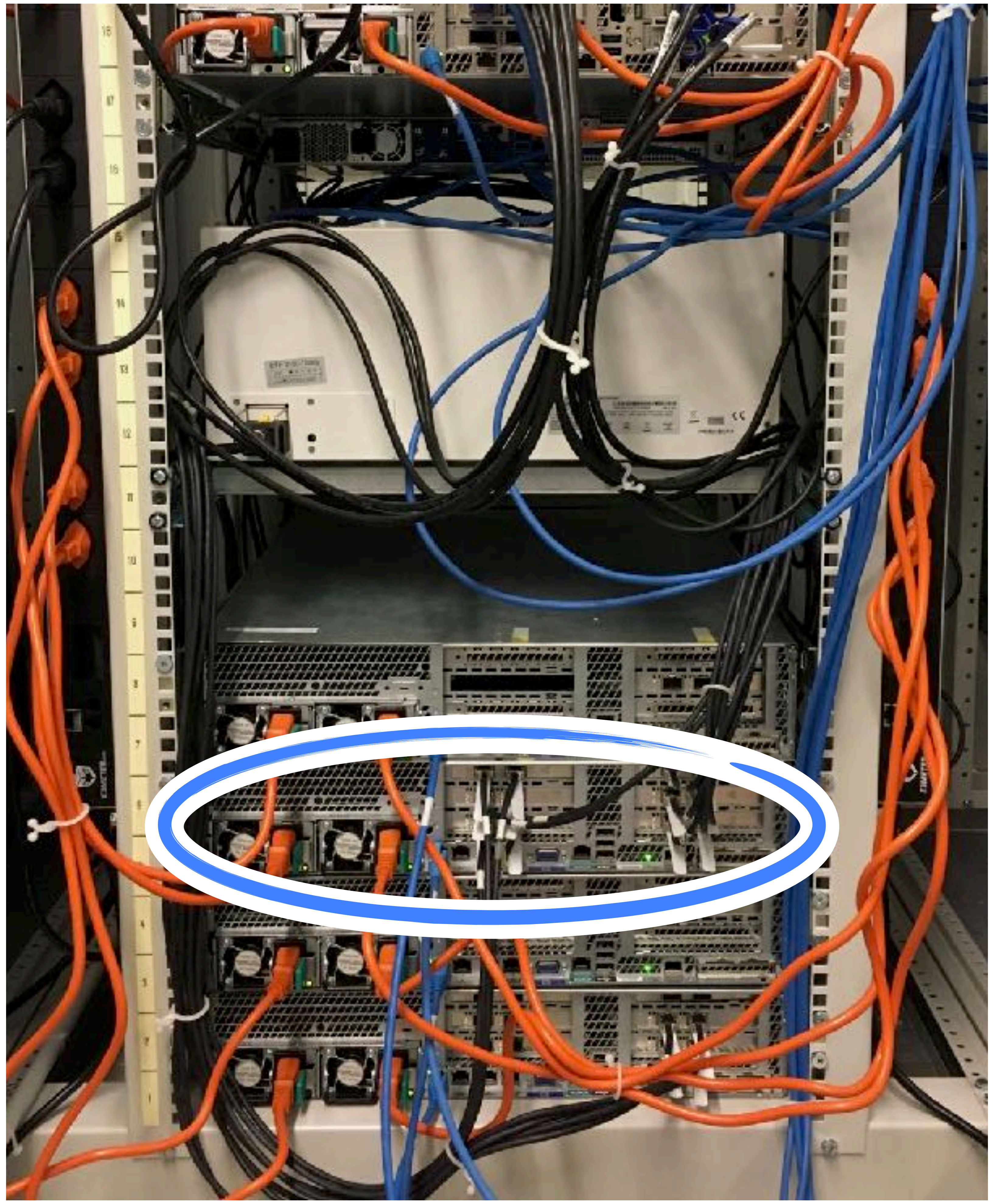
Evaluation setup, Throughput, Latency

Evaluation setup



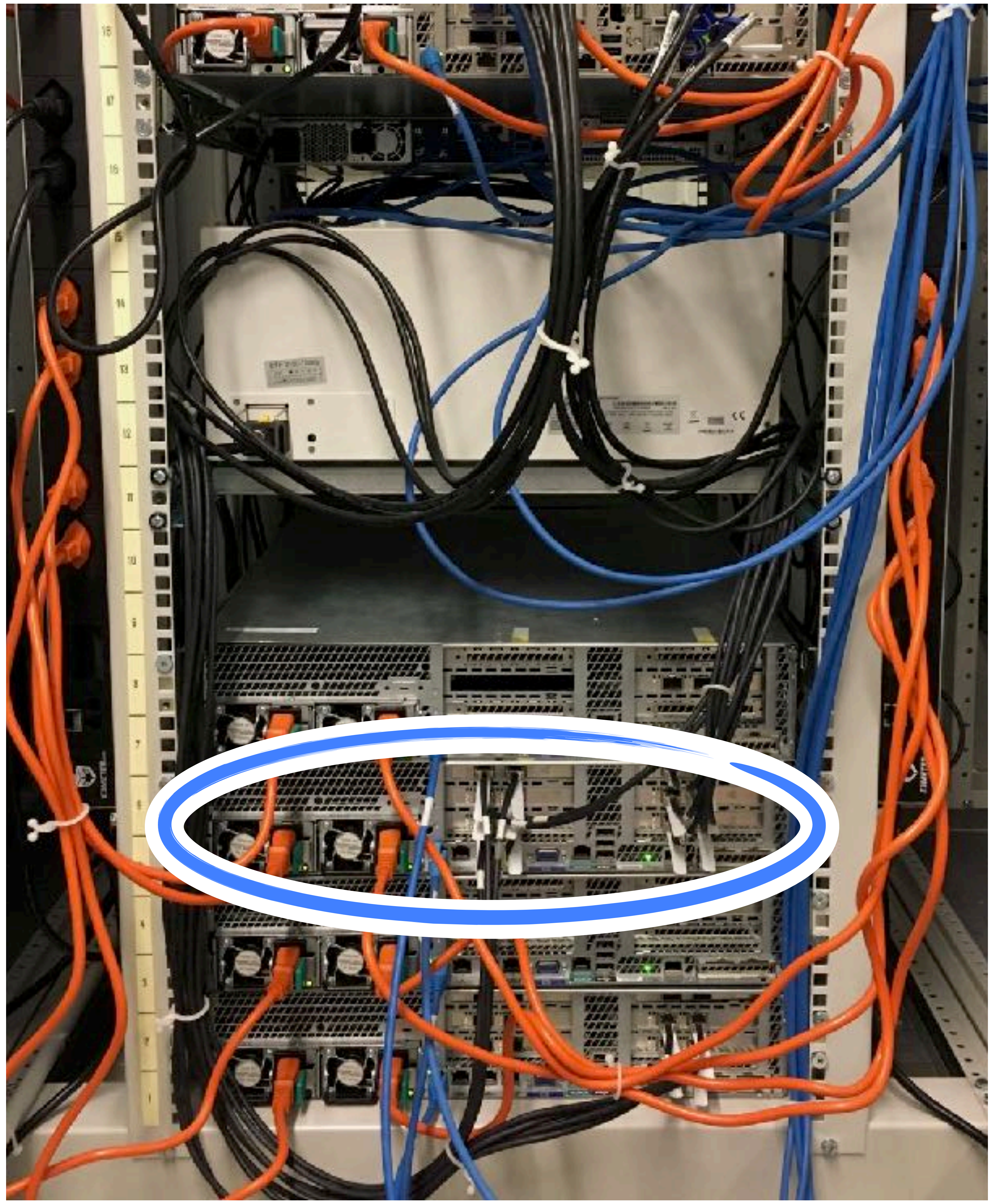
- Prototype implementation
  - Data-Plane Development Kit (DPDK)

Evaluation setup



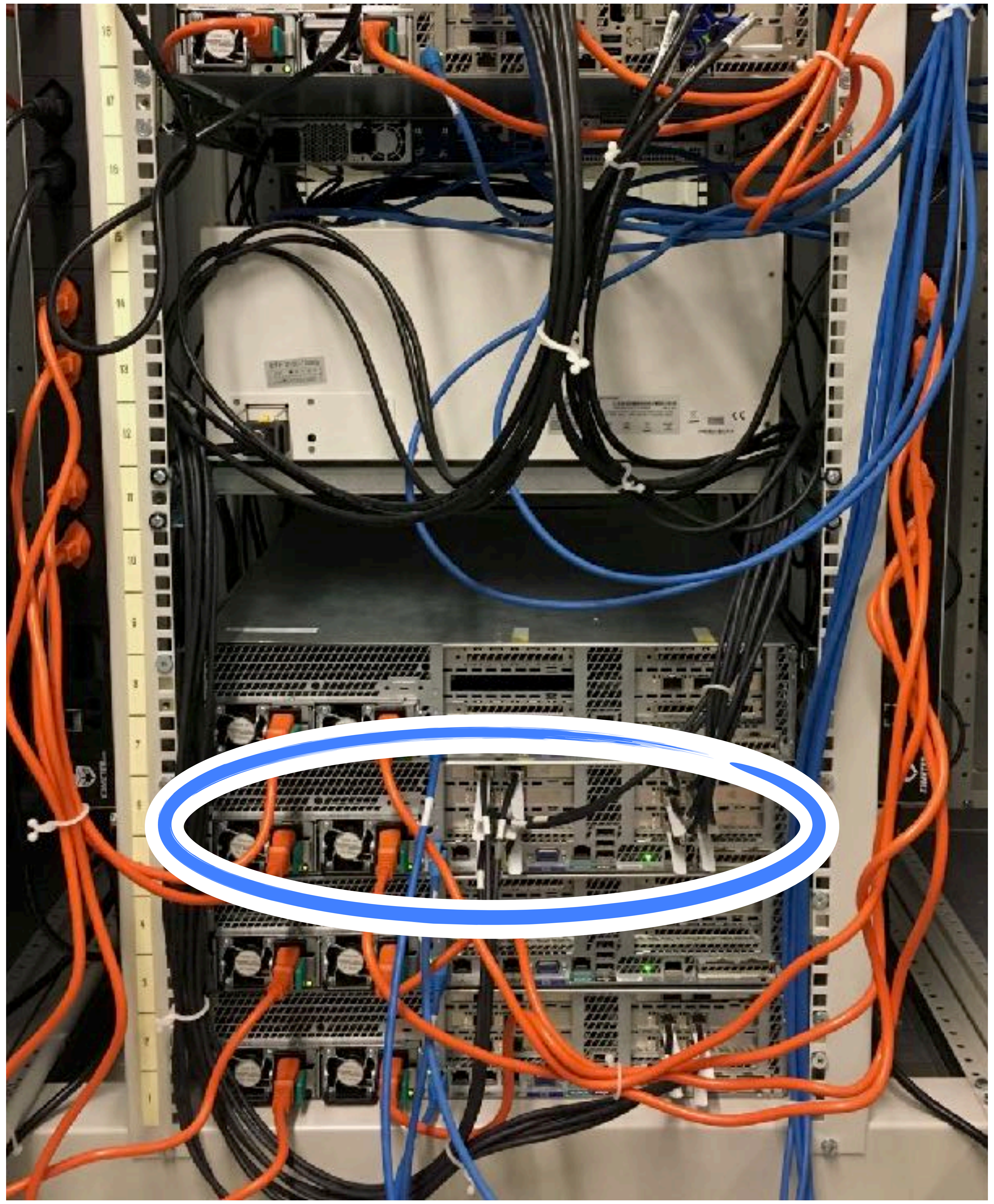
- Prototype implementation
  - Data-Plane Development Kit (DPDK)
- Software router
  - 12x 10 GbE NICs
  - Intel Xeon 2.7 GHz (2x 8 cores)

Evaluation setup



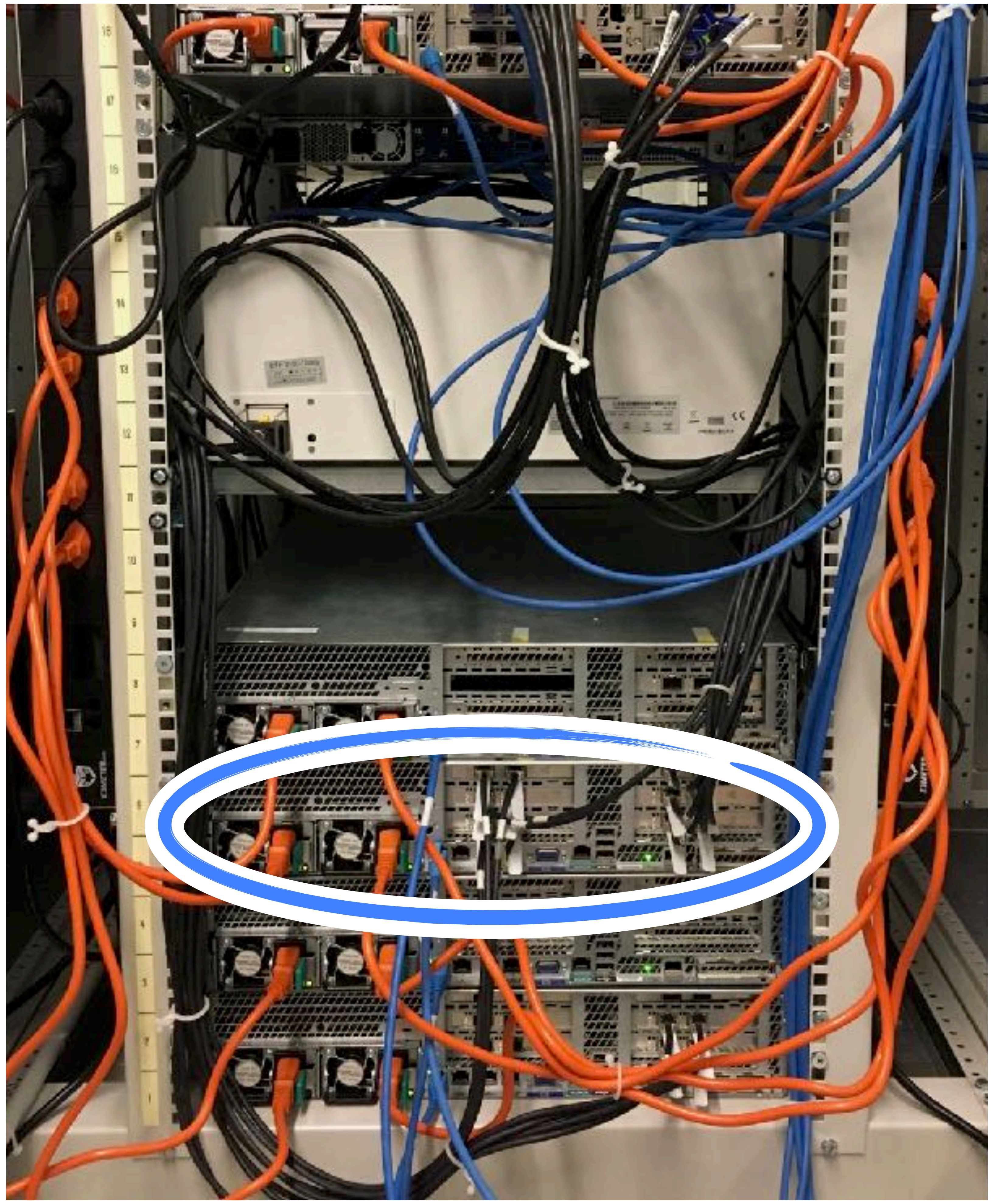
- Prototype implementation
  - Data-Plane Development Kit (DPDK)
- Software router
  - 12x 10 GbE NICs
  - Intel Xeon 2.7 GHz (2x 8 cores)
- *Results in this presentation*

Evaluation setup



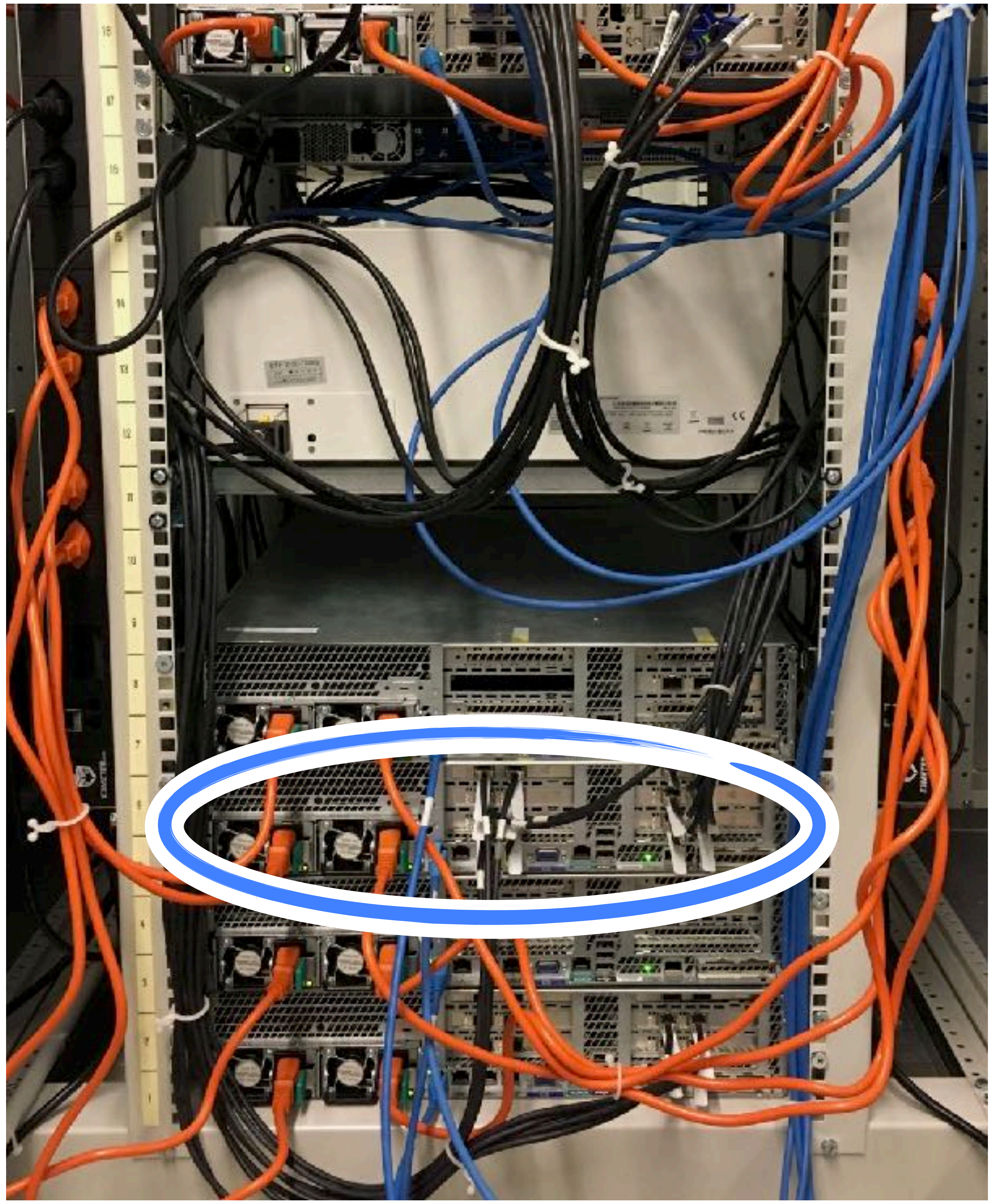
- Prototype implementation
  - Data-Plane Development Kit (DPDK)
- Software router
  - 12x 10 GbE NICs
  - Intel Xeon 2.7 GHz (2x 8 cores)
- *Results in this presentation*
  - Performance of **one node**

Evaluation setup



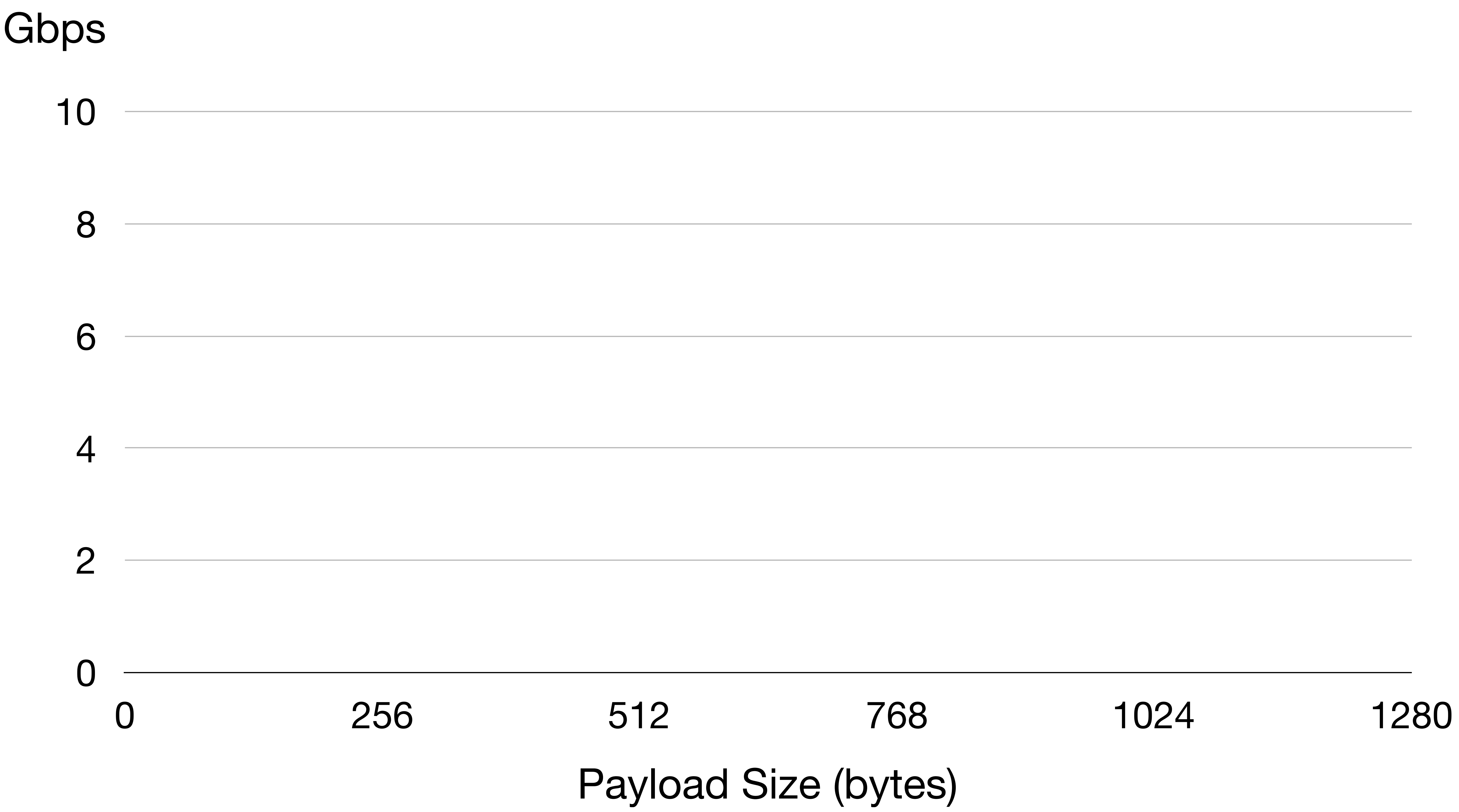
- Prototype implementation
  - Data-Plane Development Kit (DPDK)
- Software router
  - 12x 10 GbE NICs
  - Intel Xeon 2.7 GHz (2x 8 cores)
- *Results in this presentation*
  - Performance of **one node**
  - **Single 10 GbE interface**

Evaluation setup



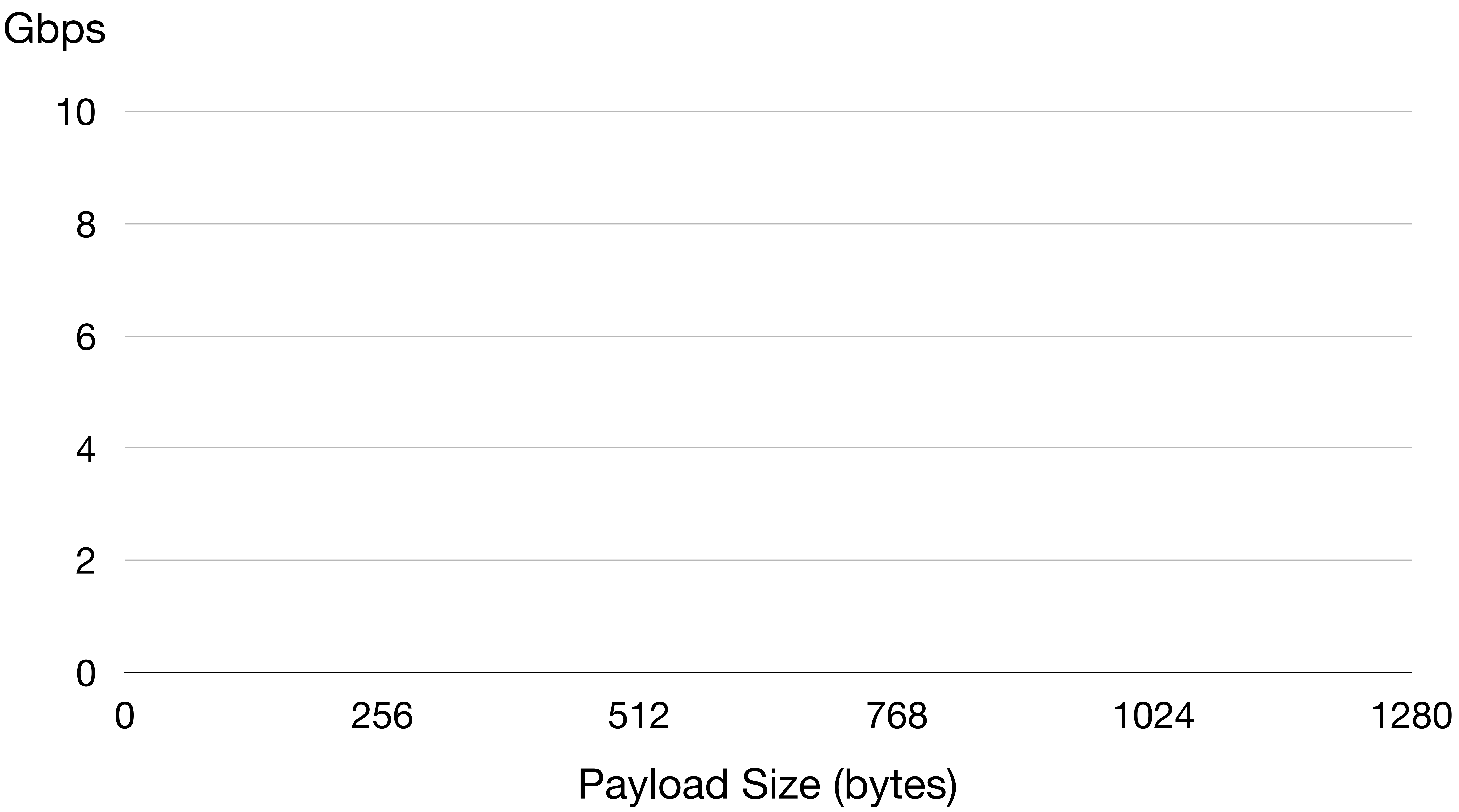
- Prototype implementation
  - Data-Plane Development Kit (DPDK)
- Software router
  - 12x 10 GbE NICs
  - Intel Xeon 2.7 GHz (2x 8 cores)
- *Results in this presentation*
  - Performance of **one node**
  - **Single 10 GbE interface**
  - **Single processing core**

Throughput



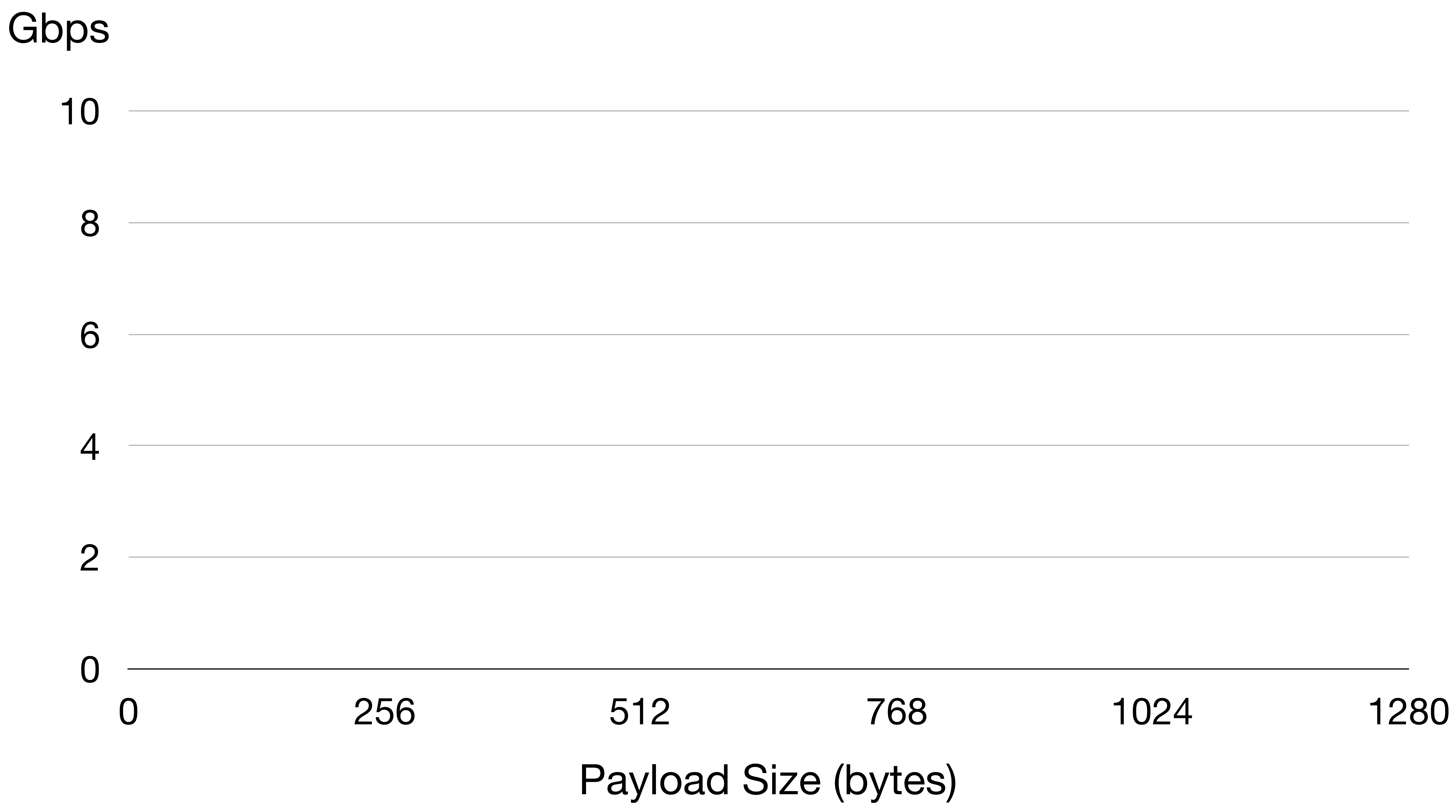
Headers can be large

Throughput



Headers can be large

~~Throughput~~ Goodput

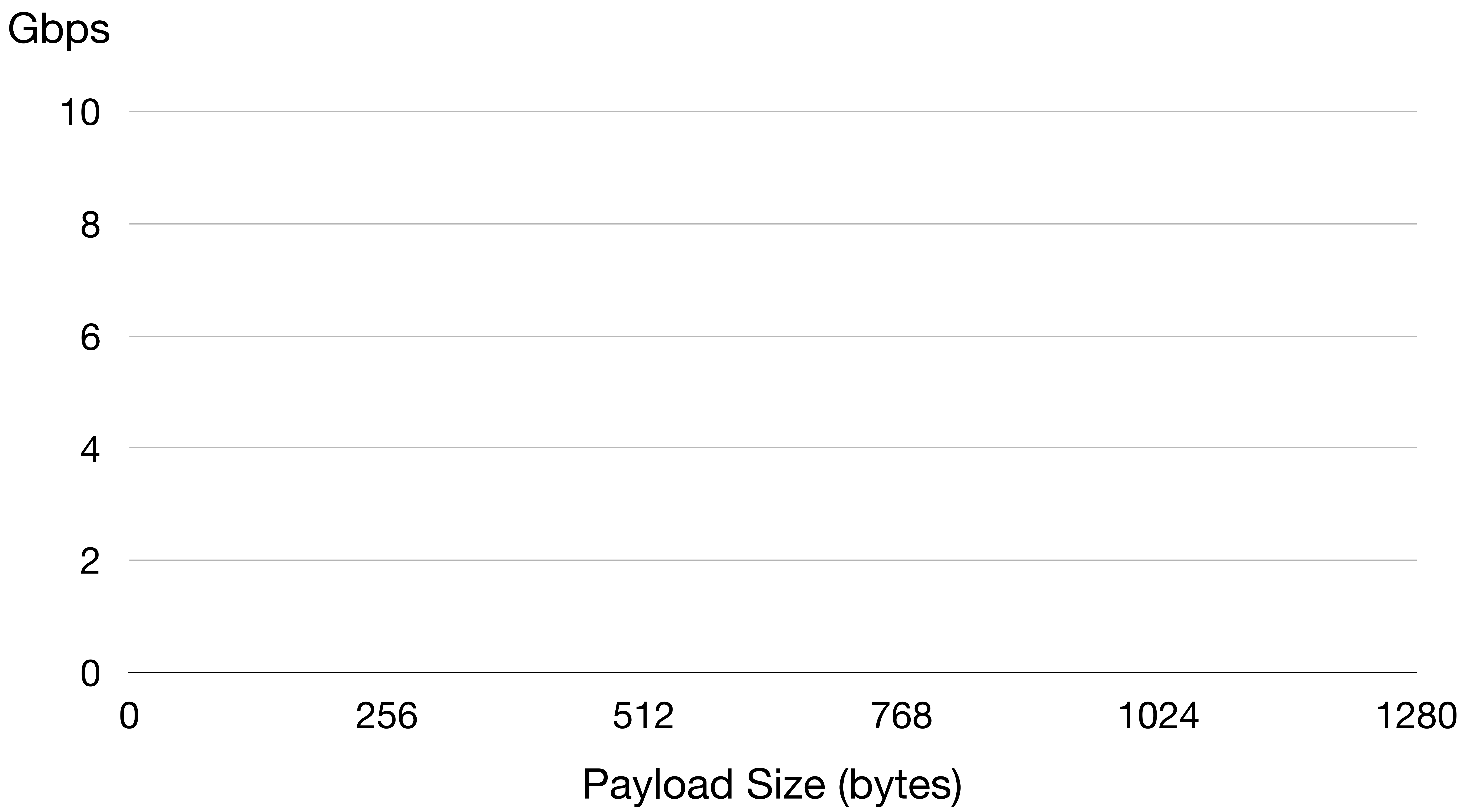


Goodput

~~Throughput~~

Headers can be large

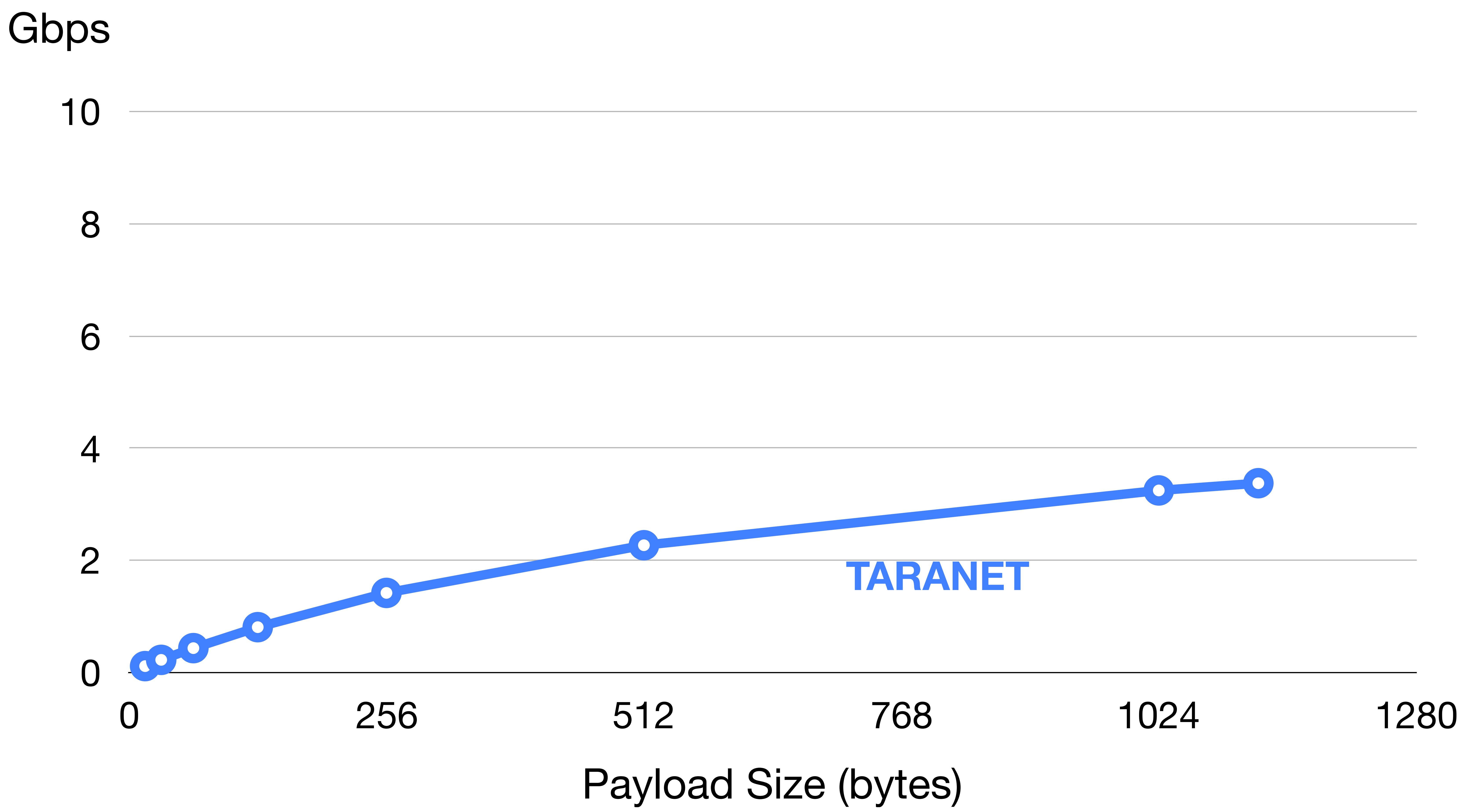
- **Path length: 7 nodes**



Goodput
~~Throughput~~

Headers can be large

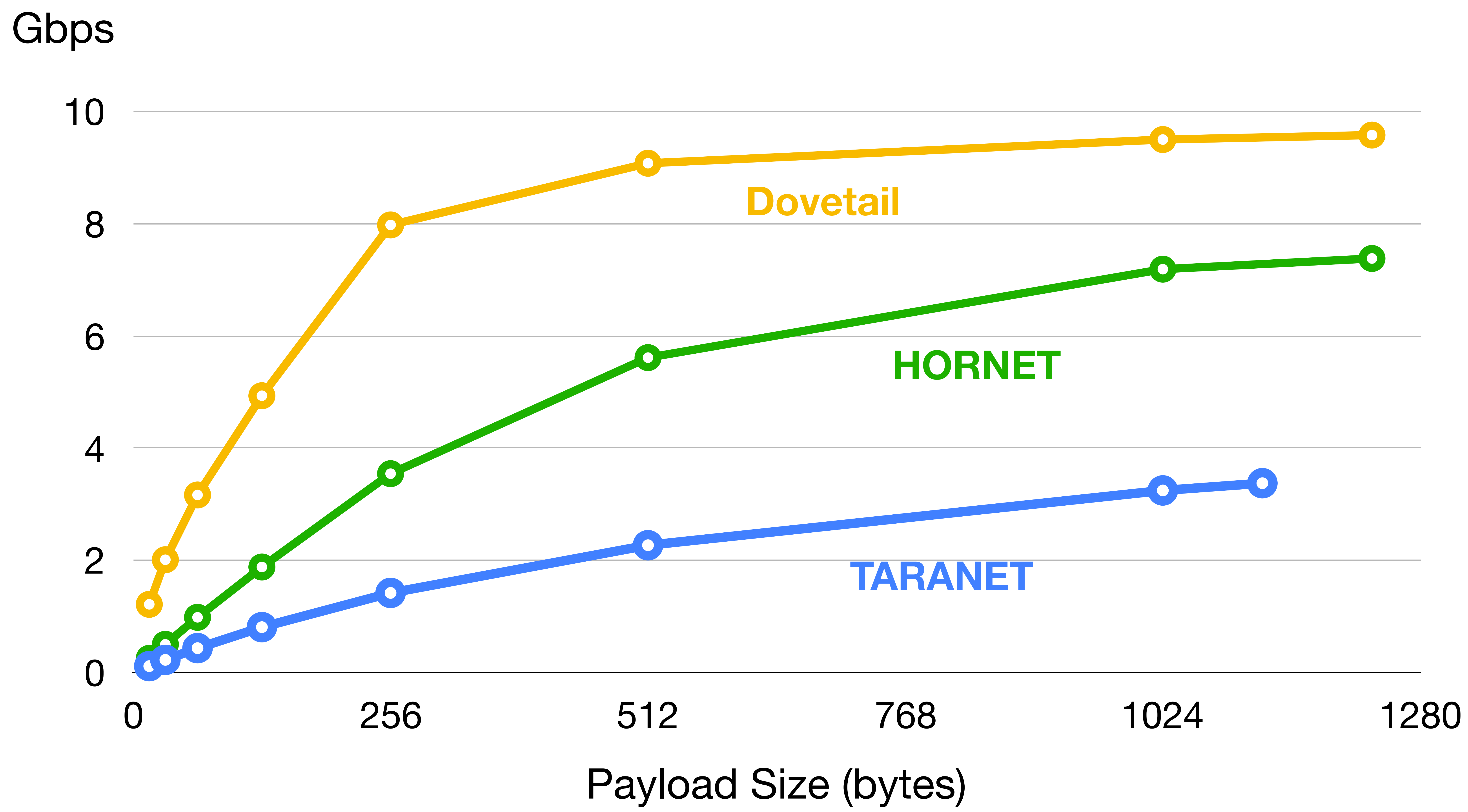
- **Path length: 7 nodes**



Goodput
~~Throughput~~

Headers can be large

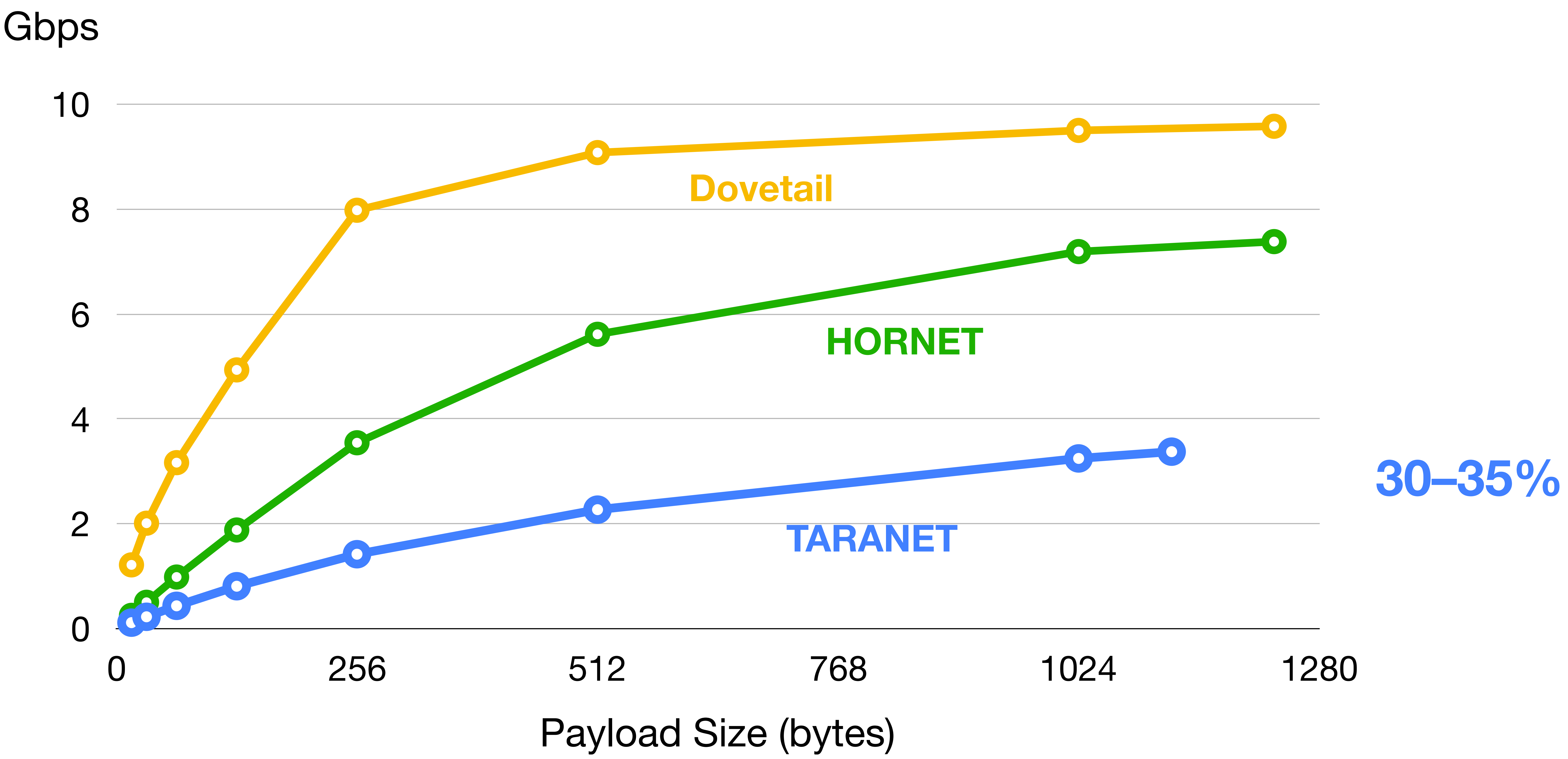
- **Path length: 7 nodes**



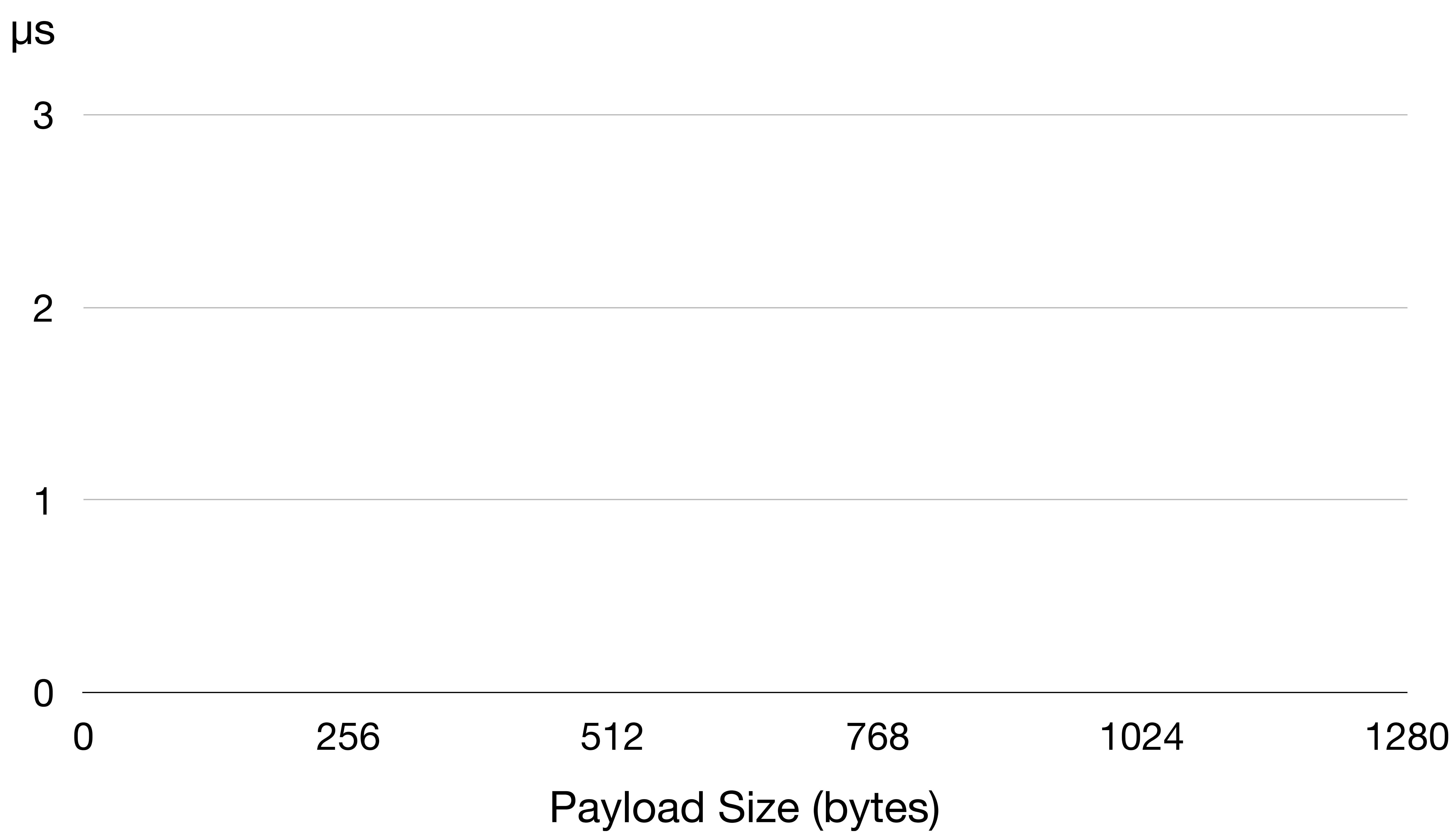
Goodput
~~Throughput~~

Headers can be large

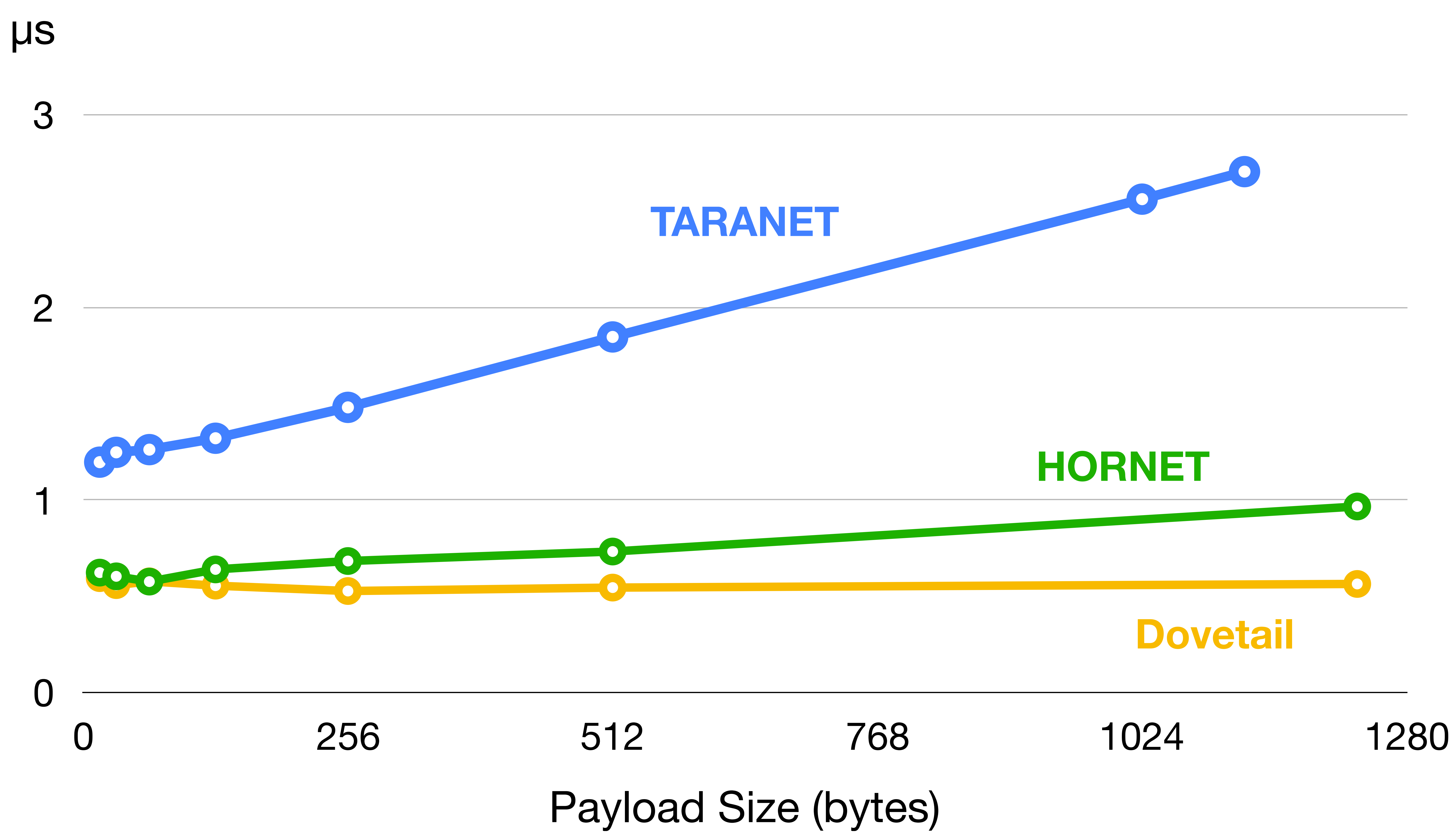
- **Path length: 7 nodes**



Latency



Latency



µs
3
2
1
0
TARANET
HORNET
Dovetail
0
256
512
768
1024
1280
Payload Size (bytes)

Summary

Highlights, Limitations

Summary

- TARANET highlights:
    - Protection against passive traffic analysis with *flowlets*
    - Protection against *active* traffic analysis with *packet splitting*

Summary

- TARANET highlights:
  - Protection against passive traffic analysis with *flowlets*
  - Protection against *active* traffic analysis with *packet splitting*
  - Good performance – *3 Gbps* on single core, acceptable latency

Summary

- TARANET highlights:
  - Protection against passive traffic analysis with *flowlets*
  - Protection against *active* traffic analysis with *packet splitting*
  - Good performance – *3 Gbps* on single core, acceptable latency
- Limitations:

Summary

- TARANET highlights:
  - Protection against passive traffic analysis with *flowlets*
  - Protection against *active* traffic analysis with *packet splitting*
  - Good performance – *3 Gbps* on single core, acceptable latency
- Limitations:
  - Chaff traffic creates a non-negligible *bandwidth overhead*

Summary

- TARANET highlights:
  - Protection against passive traffic analysis with *flowlets*
  - Protection against *active* traffic analysis with *packet splitting*
  - Good performance – *3 Gbps* on single core, acceptable latency
- Limitations:
  - Chaff traffic creates a non-negligible *bandwidth overhead*
  - Third-party anonymity

In the paper

TARANET: Traffic-Analysis Resistant Anonymity at the Network Layer

Chen Chen
chenche1@andrew.cmu.edu
Carnegie Mellon University

Daniele E. Asoni
daniele.asoni@inf.ethz.ch
ETH Zürich

Adrian Perrig
adrian.perrig@inf.ethz.ch
ETH Zürich

David Barrera
david.barrera@polymtl.ca
Polytechnique Montreal

George Danezis
g.danezis@ucl.ac.uk
University College London

Carmela Troncoso
carmela.troncoso@epfl.ch
EPFL

***Abstract*—Modern low-latency anonymity systems, no matter whether constructed as an overlay or implemented at the network layer, offer limited security guarantees against traffic analysis. On the other hand, high-latency anonymity systems offer strong security guarantees at the cost of computational overhead and long delays, which are excessive for interactive applications. We propose TARANET, an anonymity system that implements protection against traffic analysis at the network layer, and limits the incurred latency and overhead. In TARANET's setup phase, traffic analysis is thwarted by mixing. In the data transmission phase, end hosts and ASes coordinate to shape traffic into constant-rate transmission using packet splitting. Our prototype implementation shows that TARANET can forward anonymous traffic at over 50 Gbps using commodity hardware.**

1. Introduction

Users are increasingly aware of their lack of privacy and in forwarding anonymous traffic. Intermediate anonymity supporting network nodes (or nodes for short) first cooperate with senders to establish anonymous sessions or circuits, and then process and forward traffic from those senders to receivers. While these systems achieve high throughput and low latency, the security guarantees of these systems are no stronger than Tor's. Moreover, LAP and Dovetail leak the position of intermediate nodes on the path and the total path length, which reduces the anonymity set size, facilitating de-anonymization [21].

The problem space appears to have an unavoidable tradeoff: *strong anonymity appears achievable only through drastically higher overhead* [27]. In this paper, we aim to push the boundaries of this anonymity/performance tradeoff by combining the speed of network-layer anonymity systems with strong defenses.

To improve the anonymity guarantees, traffic analysis attacks need to be prevented, or made significantly harder for the adversary to perform. The common method to achieve

- Flowlet setup (asymm. crypto)
- Link padding (security in depth)
- Anonymity set size analysis
- Security analysis
- Chaff/setup packet trade-off
- Deployment incentives
- …

Thank you!

Contacts:

Chen Chen: chenche1@andrew.cmu.edu
Daniele E. Asoni: daniele.asoni@inf.ethz.ch