ETH zürich
Network Security Group

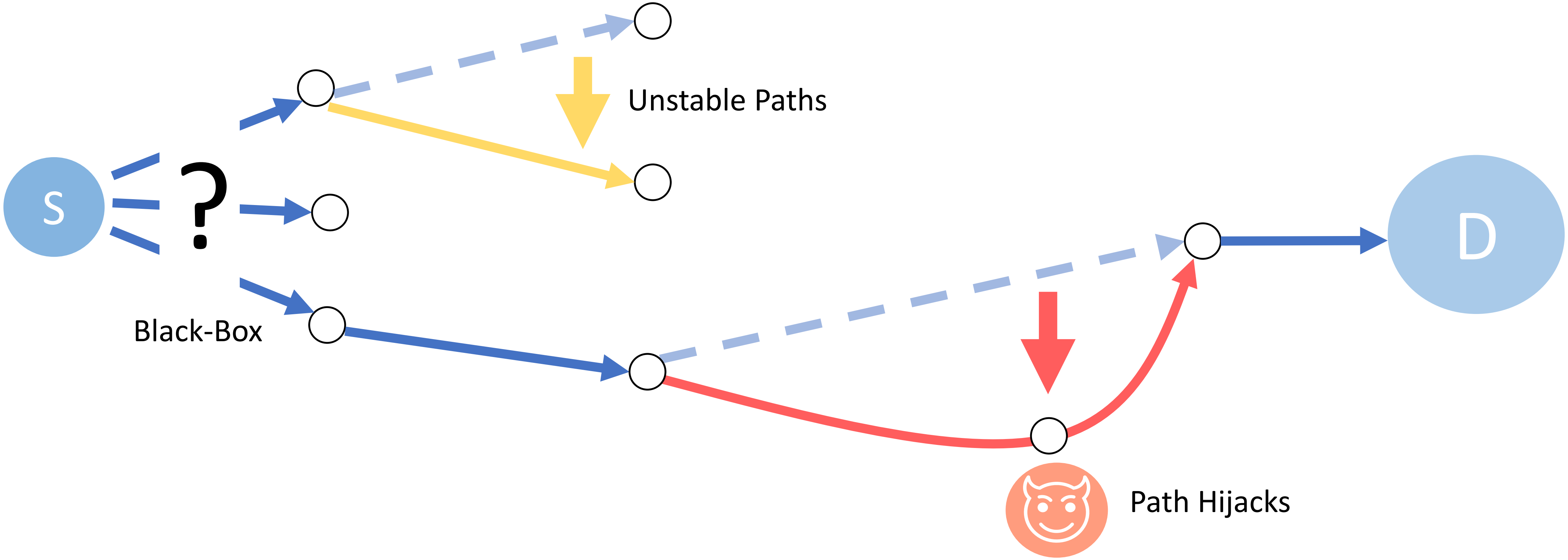
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

FABRID: Flexible Attestation-Based Routing for Inter-Domain Networks

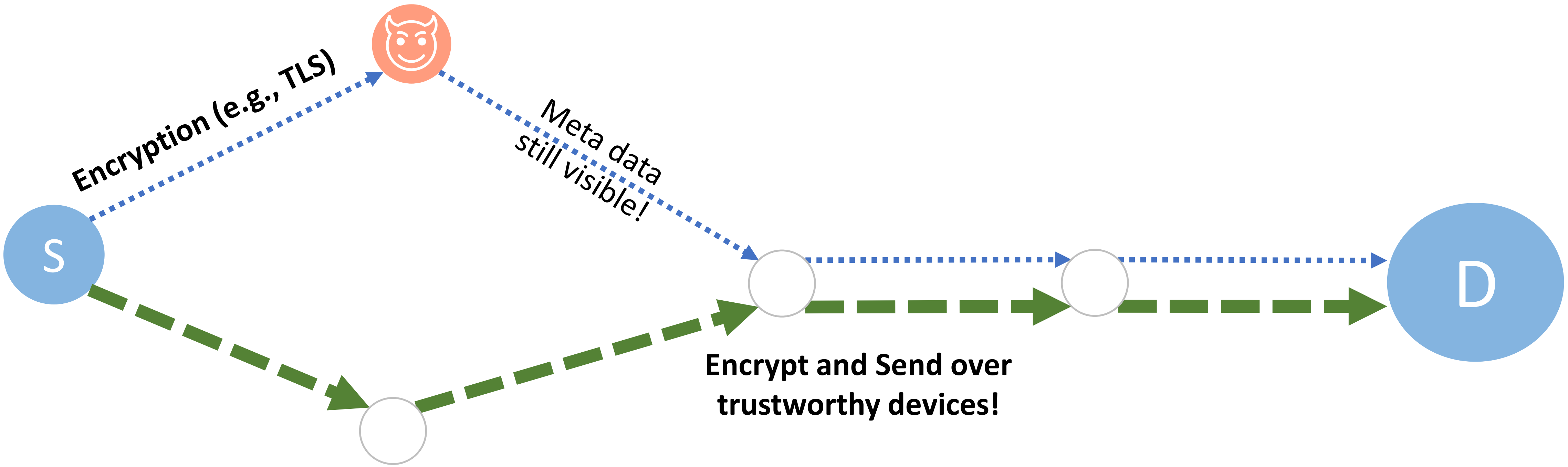
Cyrill Krähenbühl[*], Marc Wyss[*], David Basin[*], Vincent Lenders[†], Adrian Perrig[*], Martin Strohmeier[†]

[*]ETH Zürich, [†]Armasuisse

Users have no control over their Internet traffic!

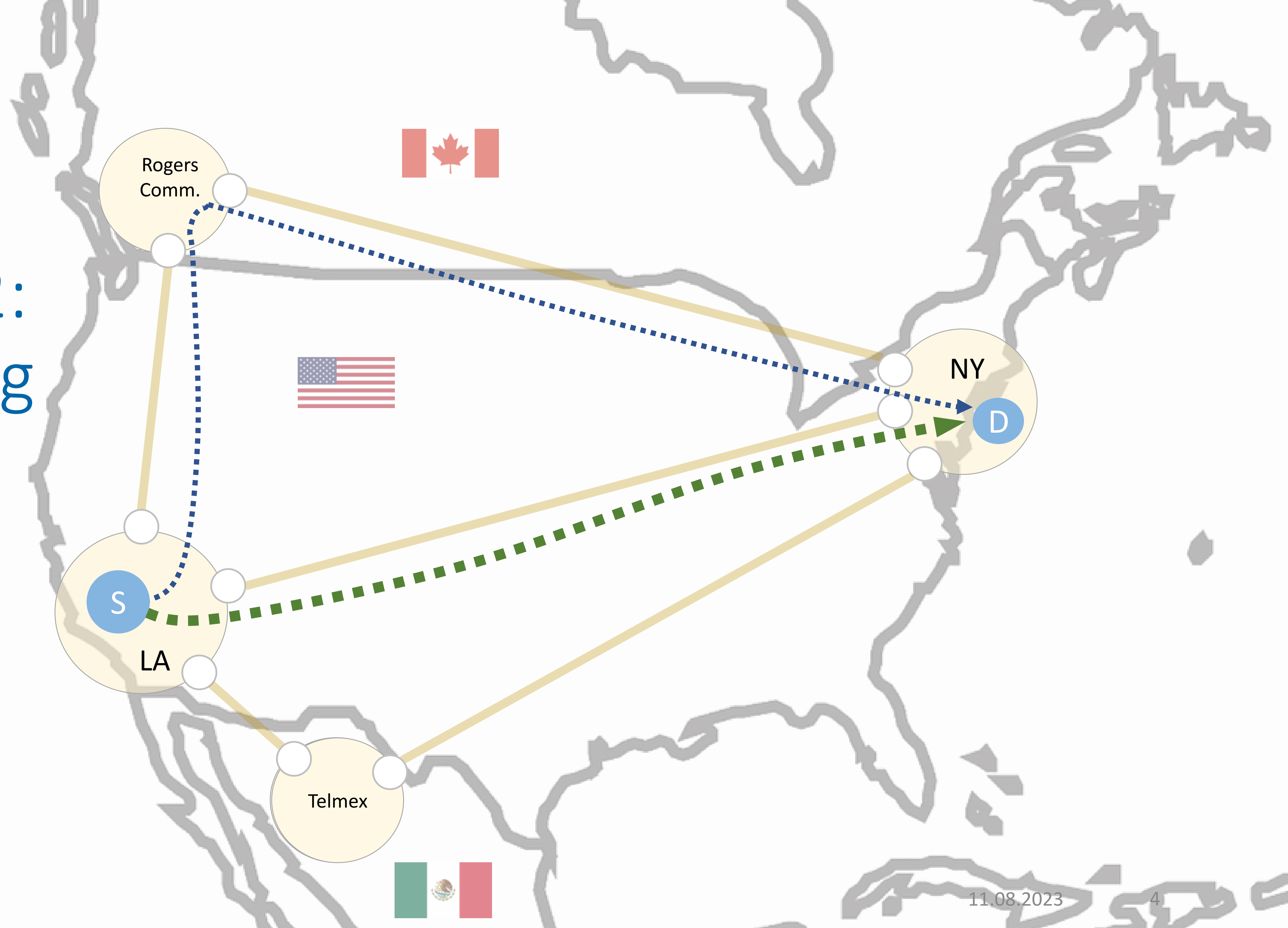


Desired property 1: Send traffic along trustworthy devices



Encrypt and Send over trustworthy devices!

Desired Property 2: Geofencing



- ⋯▶ Default Path
- ‒ ‒▶ Desired Path

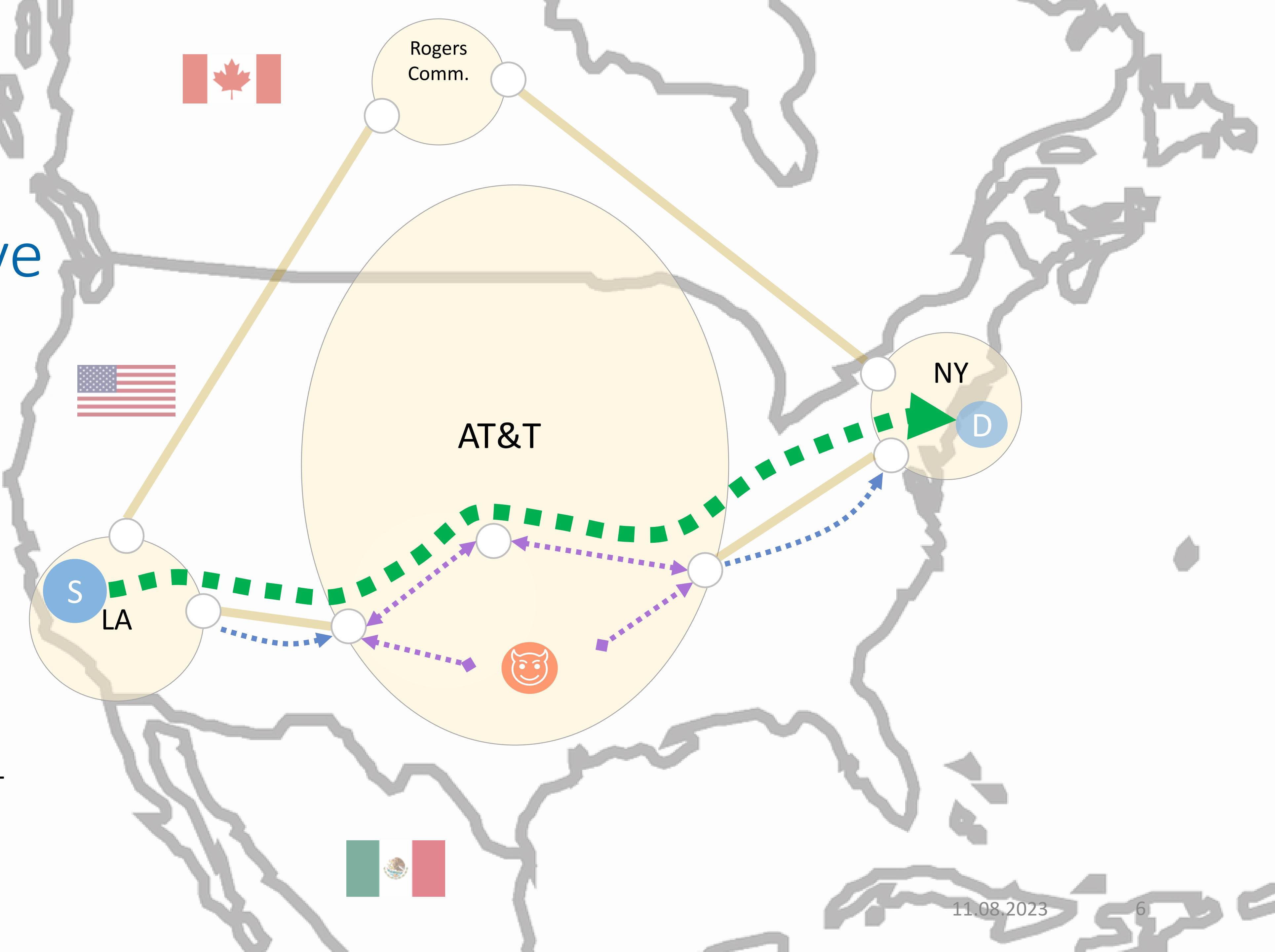
Goals

Network endpoints communicating via the Internet can select device-level forwarding paths meeting their individual criteria.

Examples:

1. Only route traffic along trustworthy devices, e.g., devices manufactured by Extreme Networks
2. Only route traffic within the US
3. Only route traffic along devices that have a specific hardware capability, e.g., supporting Precision Time Protocol (PTP)

How to achieve Inter-Domain Device-Level Path Control?

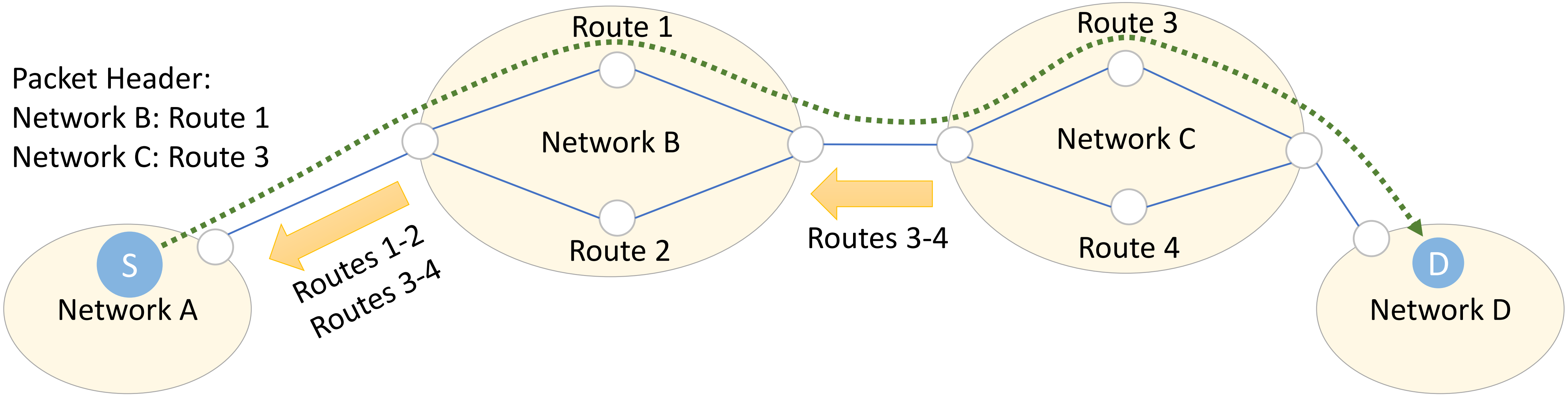


┅▶ **SCION**

┅▶ **TPR**
(Trusted Path Routing)

▪▪▪▶ **FABRID**
(Flexible Attestation-Based Routing on Inter-Domain Networks)

FABRID Workflow



Packet Header:
Network B: Route 1
Network C: Route 3

Control Plane:

- Distribute each network’s **internal routing information** to endpoints
- Endpoints select routes satisfying their criteria

Data Plane:

- Endpoints **encode** network + internal routing information **in the packet header**

Challenge for the Control Plane: Don’t release sensitive information of operator

Problem:

Should not disclose internal network topology

Solution:

- Each network operator can decide how much information to release via **routing policies**
- Policies are specified in **first-order logic** formulas

→ expressible and extensible

$$\begin{aligned} \mathrm{Pol}(r) \coloneqq{} & \mathrm{manufacturer}(r) = \mathrm{Extreme\ Networks} \land \\ & \exists c \in \mathbb{C}\colon \mathrm{software}(r, c) \land \mathrm{name}(c) = \mathrm{EXOS} \end{aligned}$$

Relevant Router Policy Properties

- Manufacturer
- Hardware
- Software (+ patch level)
- Geolocation
- Jurisdiction
- CO_2 Emissions

Verifiable via remote router attestation

Challenge for the Control Plane: Distribute policy information

Problem:

Policy dissemination to endpoints must be **scalable** and introduce **little overhead**

Solution:

- Piggy-back policy information on SCION routing messages
- Only disseminate changed policy information
- Reuse common policies among multiple networks

Challenge for the Data Plane: Secrecy and Authenticity of policies in packet header

Problem:

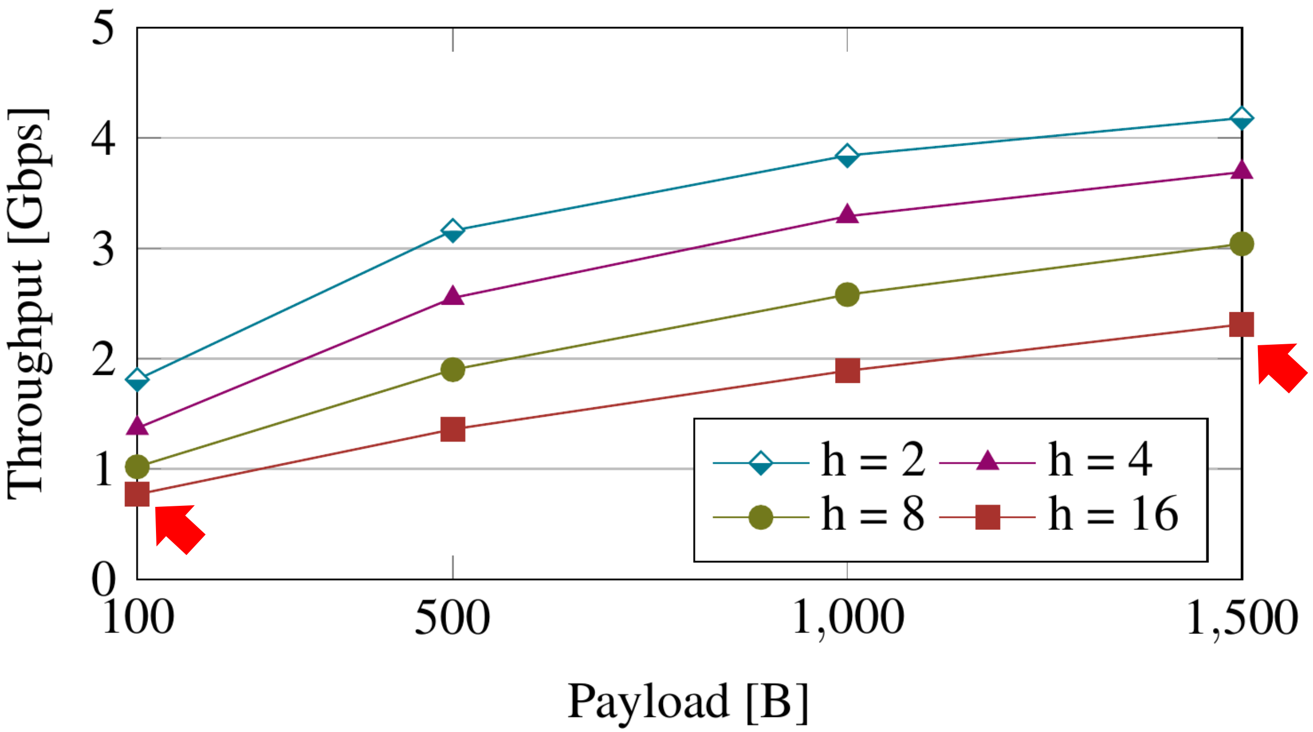
On-path attackers can learn and modify embedded policies

Solution:

- **Encrypt** embedded policies
- **Authenticate** encrypted policies
- On a **per-packet** basis
- All operations use efficient **symmetric cryptography**

Evaluation

- Border Router Forwarding: Up to 160Gbps with fewer than 16 cores
- Endhost Traffic Generation: Over 1Gbps with a single core (h: path length)



Conclusion

- FABRID enables flexible inter-domain path control at the granularity of individual routers by leveraging remote attestation and SCION
- Enables many new use cases:
  - Geo-fencing
  - Routing over trustworthy network infrastructure
  - Routing over devices with specific hardware capabilities
- FABRID needs support from network operators and SCION deployment, but is incrementally deployable providing incentives for early adopters

Thank you for your attention!

Cyrill Krähenbühl **ETH Zürich**

PhD Candidate **cyrill.kraehenbuehl@inf.ethz.ch**