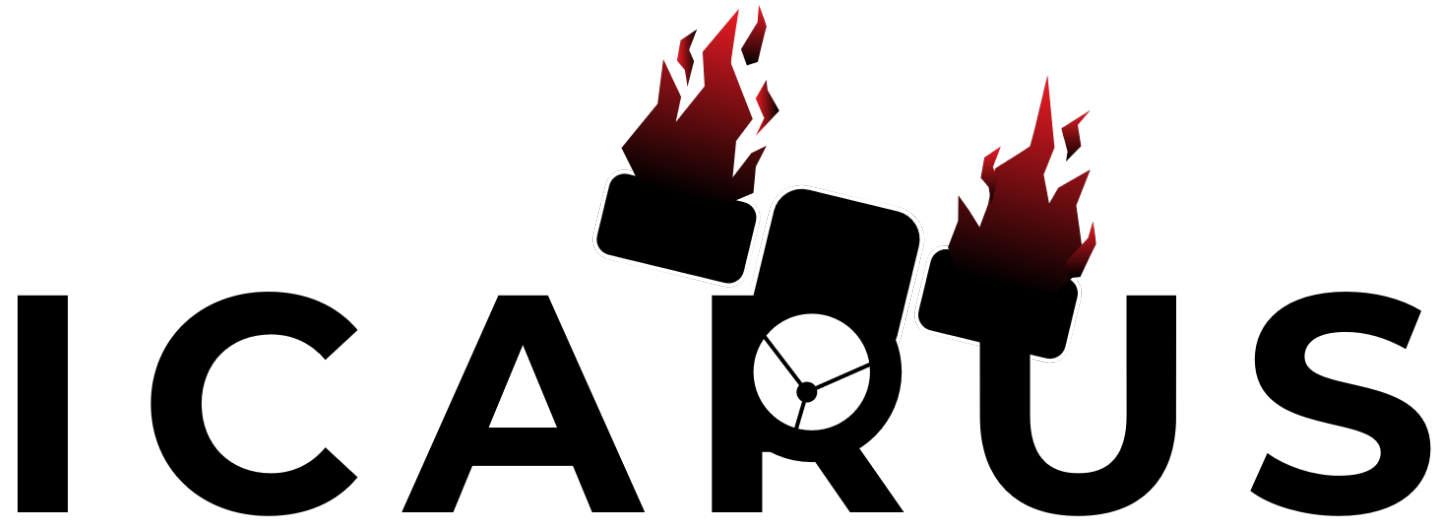
ETH zürich

Network Security Group



Attacking LEO satellite networks

Giacomo Giuliari. Tommaso Ciussani,
Adrian Perrig, Ankit Singla
ETH Zurich
10 June 2021, LEOCONN

STARLINK SPEED TESTS —

SpaceX Starlink speeds revealed as beta users get downloads of 11 to 60Mbps

Ookla tests aren't showing the gigabit sp

JON BRODKIN - 8/14/2020, 7:00 PM

Starlink Blazes Past 560 Mbps In Download Spee Shows Latest Test Run!

By Ramish Zafar

May 17, 2021 12:37 EDT

SpaceX's Satellite Internet Service Latency Comes in Under 20 Milliseconds

SpaceX disclosed the benchmarks in a presentation the company sent to the FCC last Friday. It also revealed the public beta for Starlink is coming to multiple US states.

By Michael Kan 9 Sep 2020, 8:04 p.m.

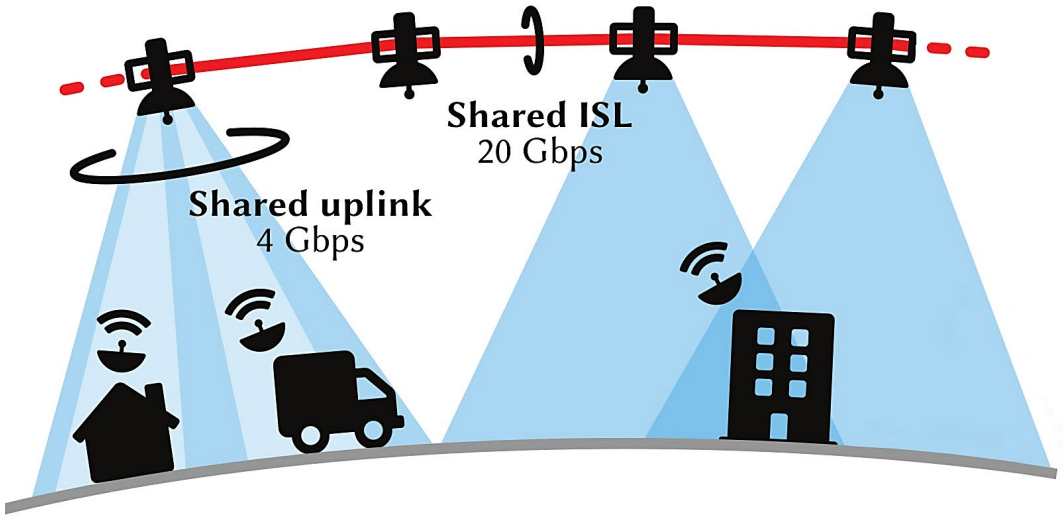
Starlink is asked to increase the number of users from 1 million to 5. Their services are in "incredible demand"

In the US alone!

BY JOHN KESSLER AUGUST 3, 2020 10:39 PM GMT+0300

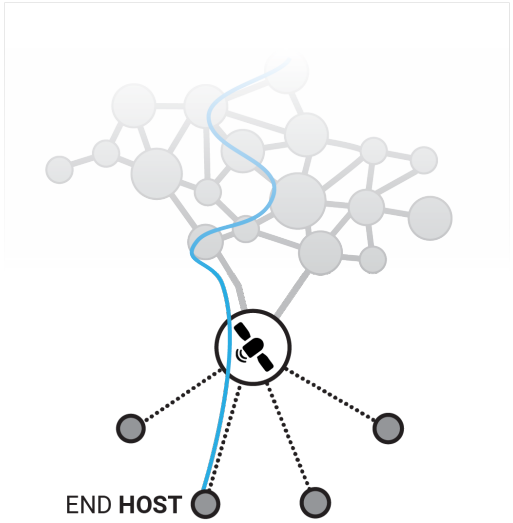
536 VIEWS

How is this achieved? **The network model**

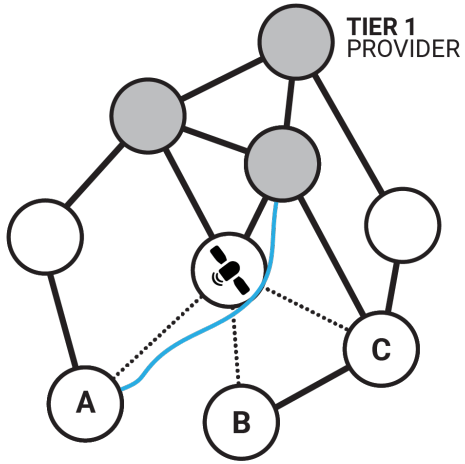


- **Uplinks and downlinks**
  - Can serve multiple hosts
  - 4 Gbps upload for each uplink
  - Reconfigure as satellites move
- **Inter-satellite links**
  - Can carry up to 20 Gbps
  - High-capacity network in space
- **Low latency advantages**
  - The speed of light in vacuum is 50% faster than in fiber
  - Paths over ISL are straighter than fibers
- **Great for many new applications!**
  (Cloud gaming, FinTech, remote AR…)

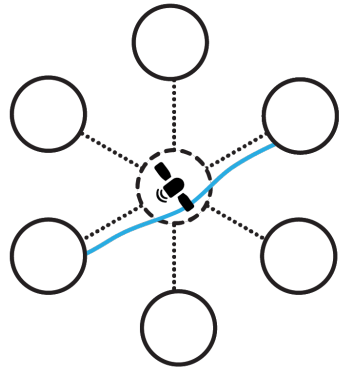
IBIS research question: What is the role of LSN in the future Internet?



Eyeball ISP



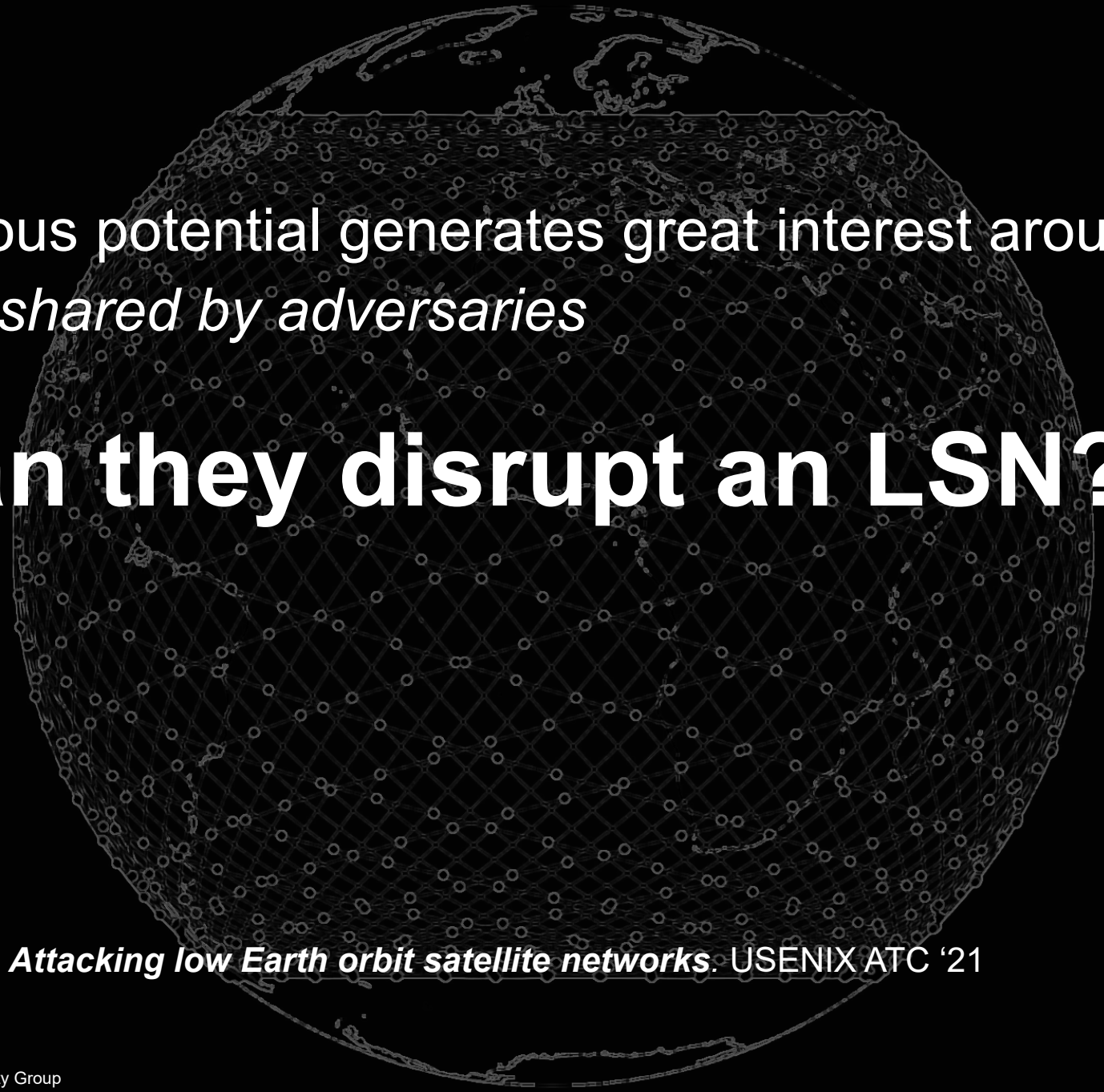
Transit provider



Internet exchange provider

- Starlink will "**carry the majority of long-distance Internet traffic**" – Elon Musk, 2015
- Opportunities and challenges of the integration of LSNs in the terrestrial Internet
- Direct BGP integration is problematic
- We develop an **optimal SCION-based architecture**, and a **ready-to-deploy CDN-like alternative**

Giuliari et al., ***Internet Backbones in Space***. ACM CCR 2020
Klenze et al., ***Networking in Heaven as on Earth***. HotNets 2018



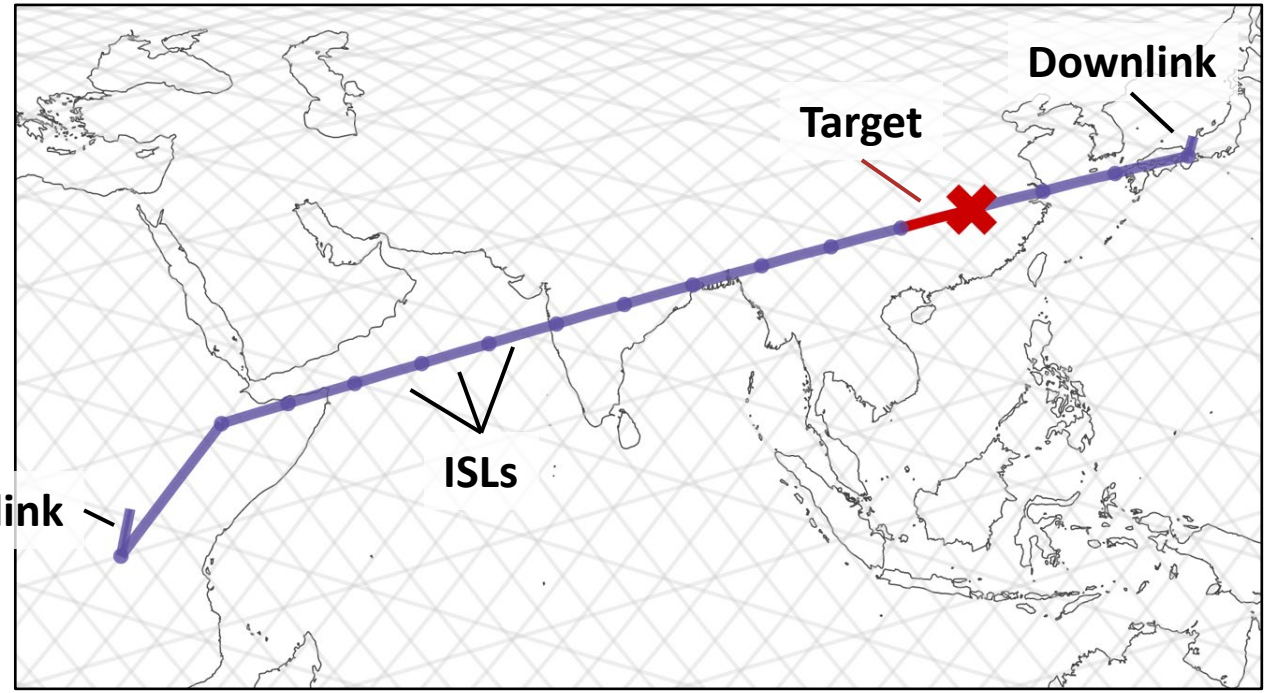
This tremendous potential generates great interest around LSNs…

…an interest shared by adversaries

How can they disrupt an LSN?

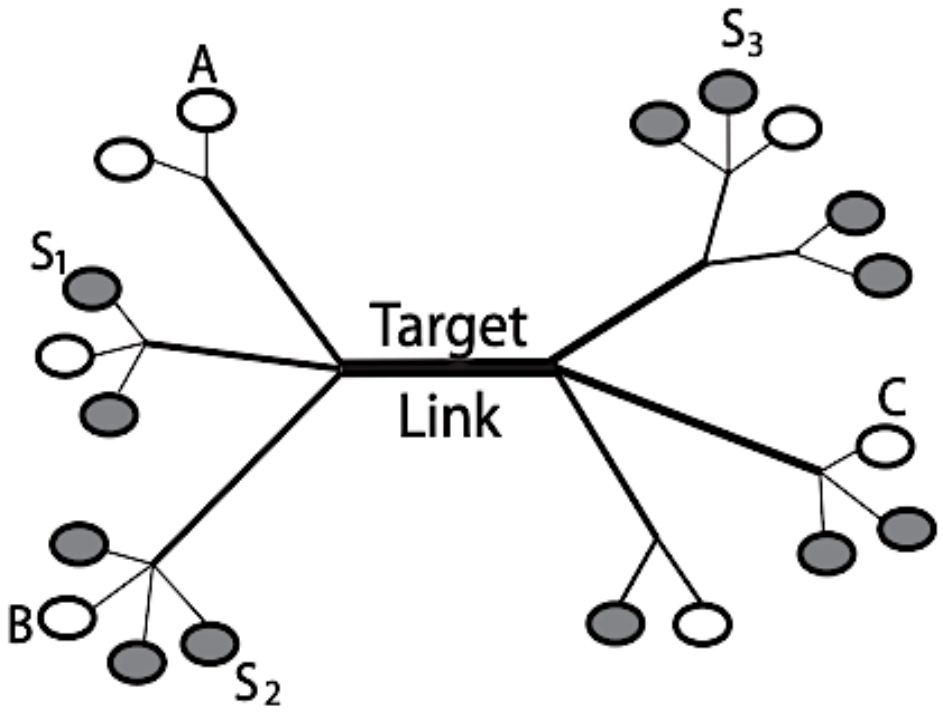
Giuliari et al., **ICARUS:** ***Attacking low Earth orbit satellite networks***. USENIX ATC ‘21

The ICARUS attack



- Adversarial goal: **disrupt communication between hosts** over the satellite network
- We do not consider **known attacks**
  - **Jamming** uplinks and downlinks
  - Attacks on weak (inexistent) encryption
- Adversaries can exploit LSN characteristics
  - In this presentation: **attacks on ISLs**
  - High disruptive power many flows use the same ISL

Starting point: the **Coremelt DDoS attack**

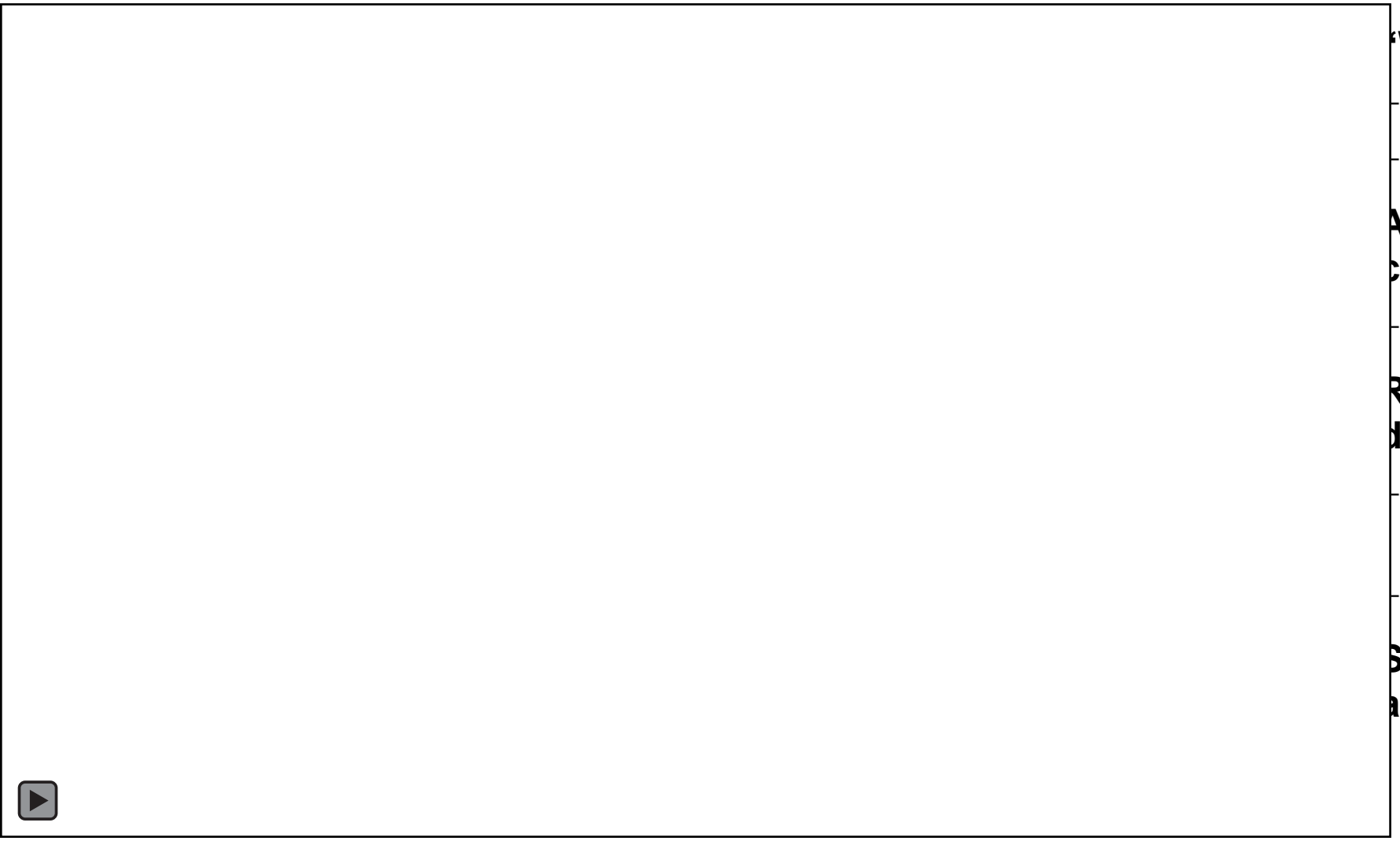


- Instead of attacking a specific end host, **we attack a network link**
  - Flows between different **src-dst pairs**
  - **Flows imitate legitimate traffic**
  - **“There is no victim”**

High resilience to detection

Can Coremelt be applied to LSNs?

#1: **Space-based low-latency network** ⇨ **Predictability**



“White Box” network

- Public satellite **positions**
- Public satellite **designs**

Advance topology computation with low error

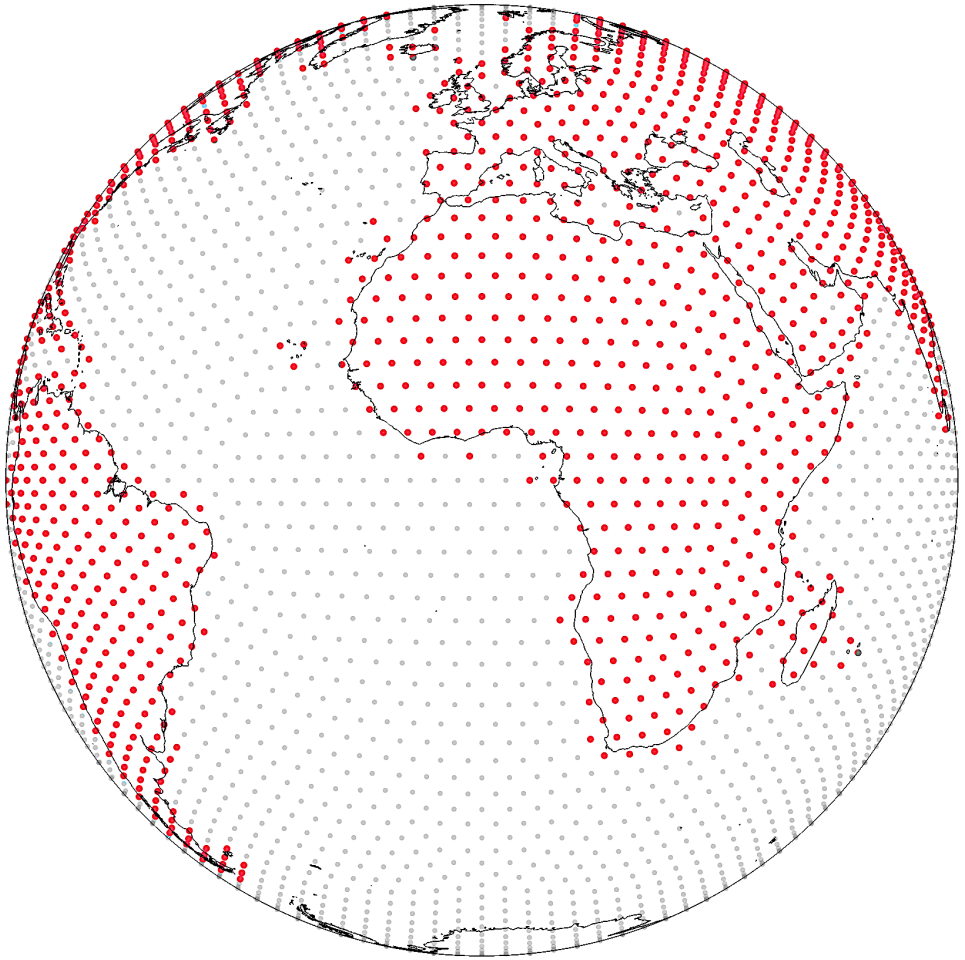
- < 2km / day

Routing policy can be discovered

- Latency measurements + topology knowledge
- Single or multi-path

Start with single-shortest path as basis for complex attacks

#2: **Global access ⇨ increased DDoS attack stealthiness**



- Remote areas are connected
  - **Increased scatter** of attack sources
  - **Millions** of terminals available for compromise
- Every satellite is an **entry point to the network**
  - No distinction between border routers and backbone routers
  - Increased **attack surface**
- The adversary **knows bot location** (GNSS)

#3: **Low-latency/higher cost ⇨ Tighter operation margins**

- There is a **combinatorically high number of paths** between two satellites in the LSN
- **BUT** High-paying customers require **low-latency and bounded jitter**
- Of the many paths, the LSN operator can only use **desirable (low-latency) paths**

- For a successful attack **the adversary only needs to "delay" packets for long enough!**
- The adversary needs to:
  - Congest the forwarding path
  - Create buffering delay on satellites
- Even if **alternative paths are still available, the adversary is successful**

Going forward

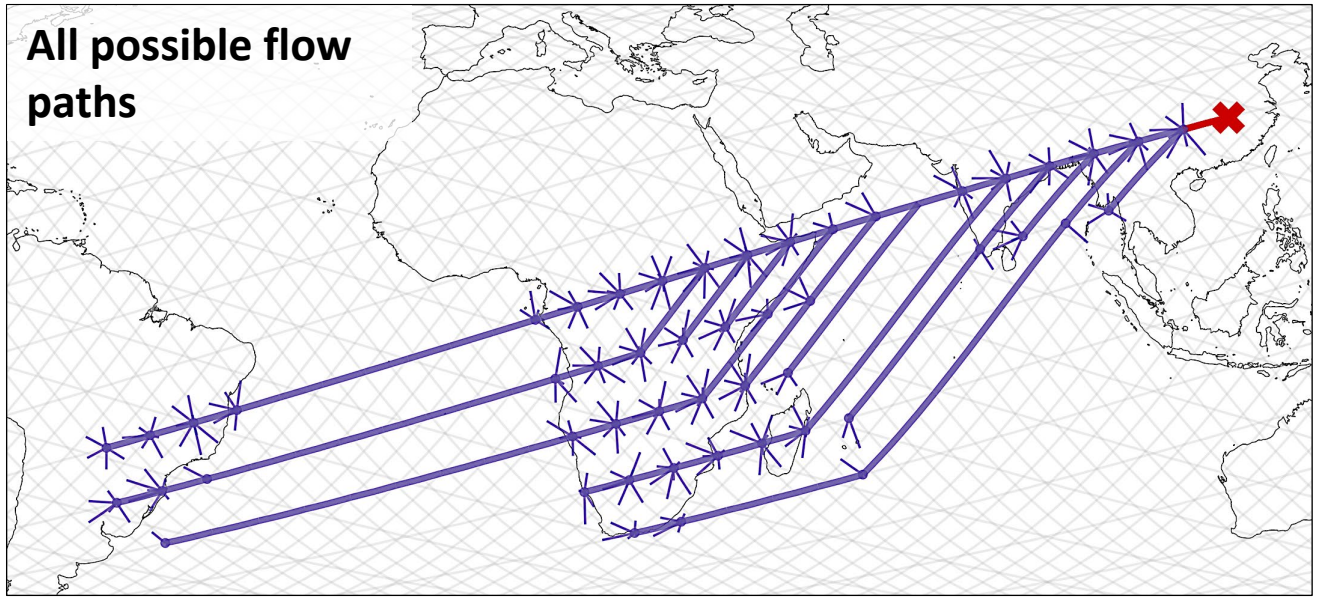
The ICARUS attack on single shortest paths

Attack connectivity between two regions

Attack LSNs that use randomized load balancing

Drawbacks of the dynamics of satellite networks

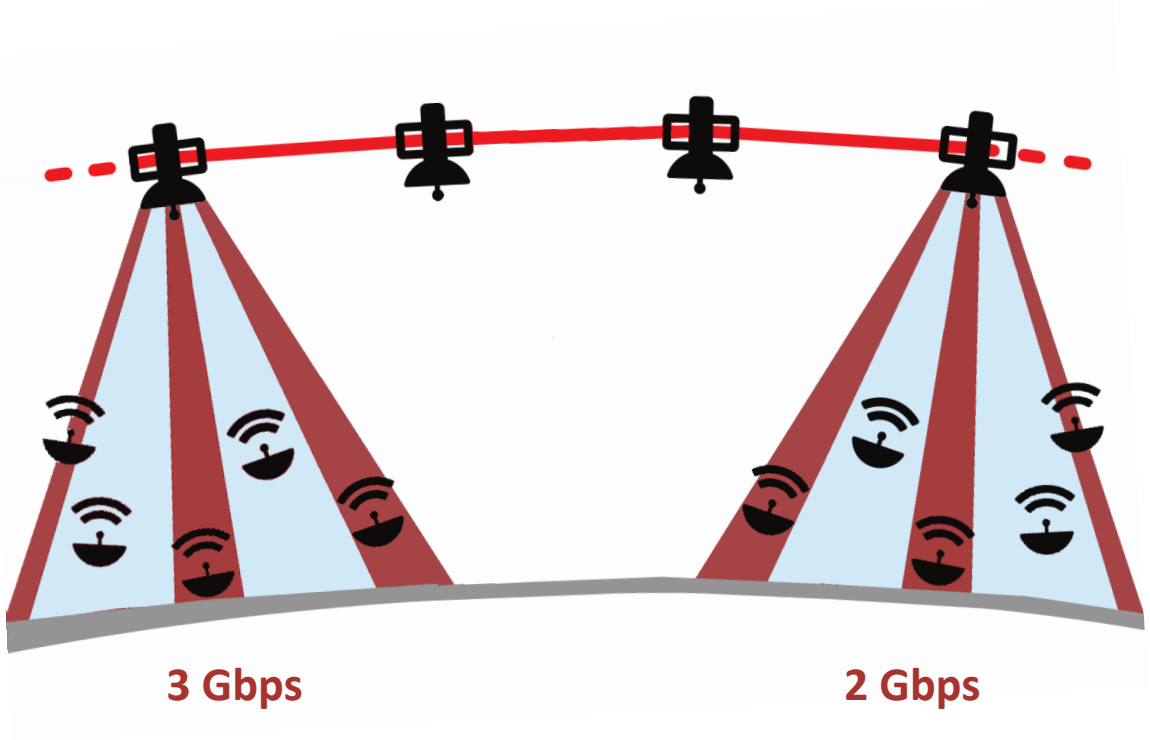
ICARUS: **Attack mechanism**



- Send **traffic flows** through the target link using:
  1. **Public knowledge of LSN topology**
  2. **Distributed access points**

- High **resilience to detection**
  - Flows **disguised as legitimate traffic**
  - Sources and targets are scattered around the planet

ICARUS attack metrics: **Cost and Detectability**

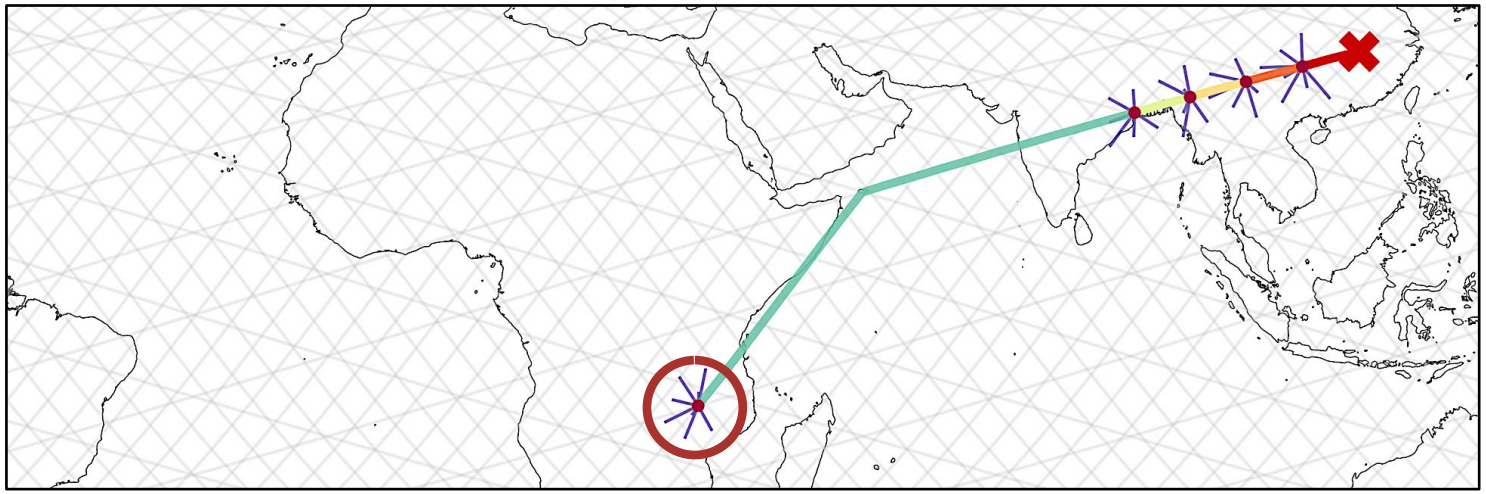


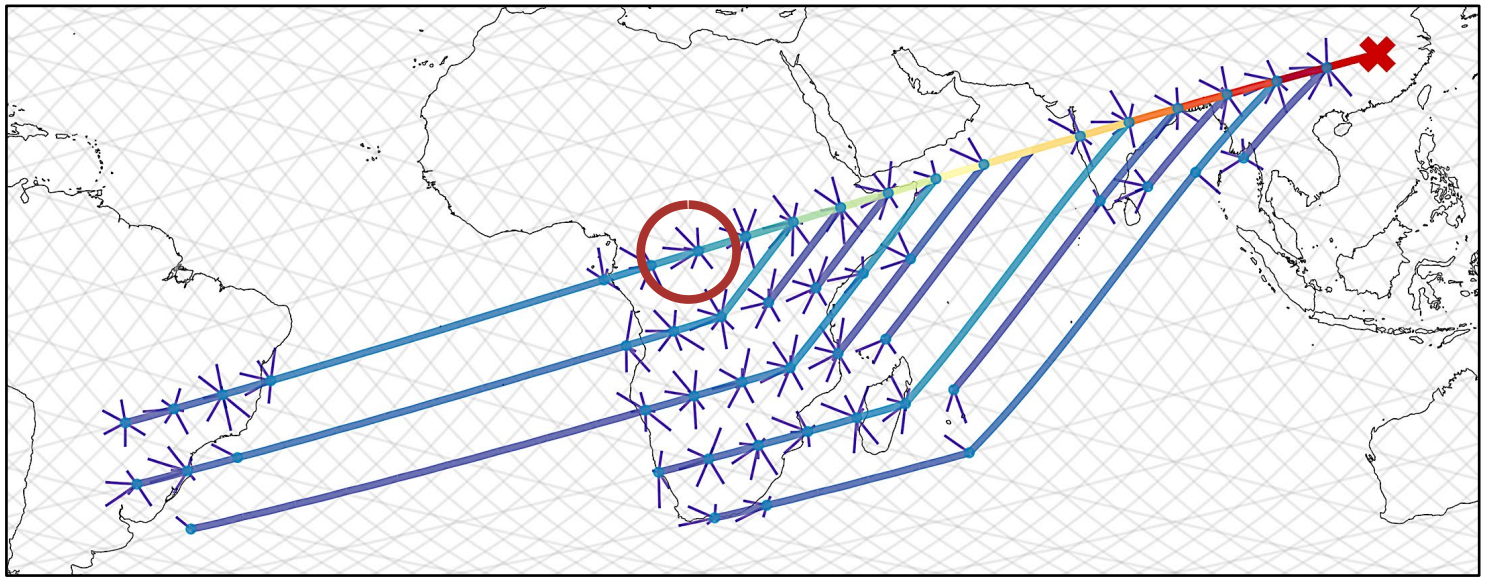
- **Cost**: sum of **bandwidth** sent by sources
- **≠ bandwidth on target:**
  - **Self congestion**
  - **Unpredictability, e.g., by load balancing** (later)
- With bots sending at **40Mbps**, min **500 are needed to congest an ISL**

- **Detectability**
  - Maximum bandwidth increase in sources
  - Detectability = 1 when **the adversary completely fills an uplink**

Effective attack ↔ low metrics

Conditions for **cost** and **detectability optimality**





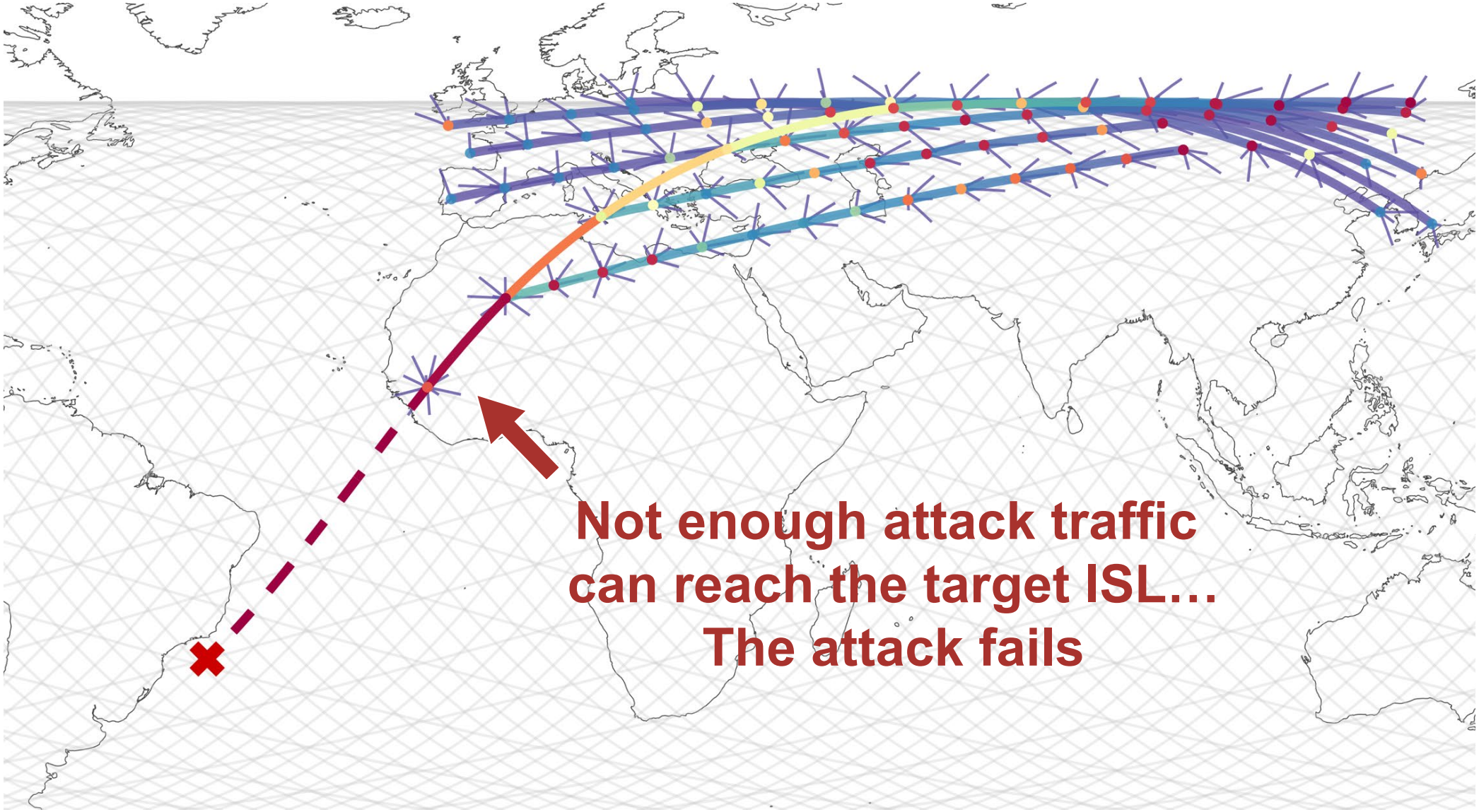
Cost optimality

- The **target link** is congested
- All other links not congested
  - No attack bw wasted

Detectability optimality

- Limit the uplink capacity iteratively
- Add a minimal amount of bw to each satellite uplink

The setback of **self-congestion**



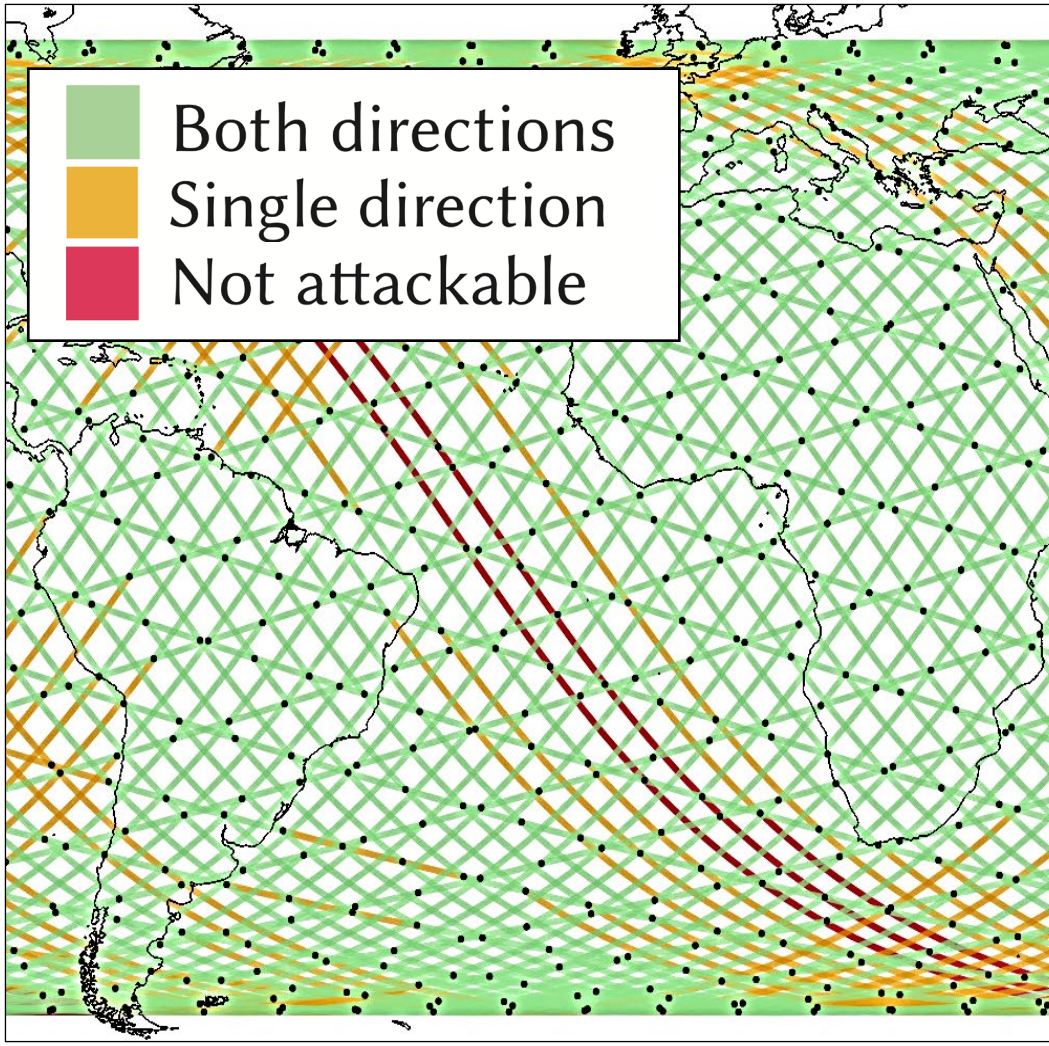
Results on ISLs

- **The adversary succeeds**
  - **86%** of **ISLs** congested
  - **99.5%** of **paths between any src-dst** has at least one ISL congested

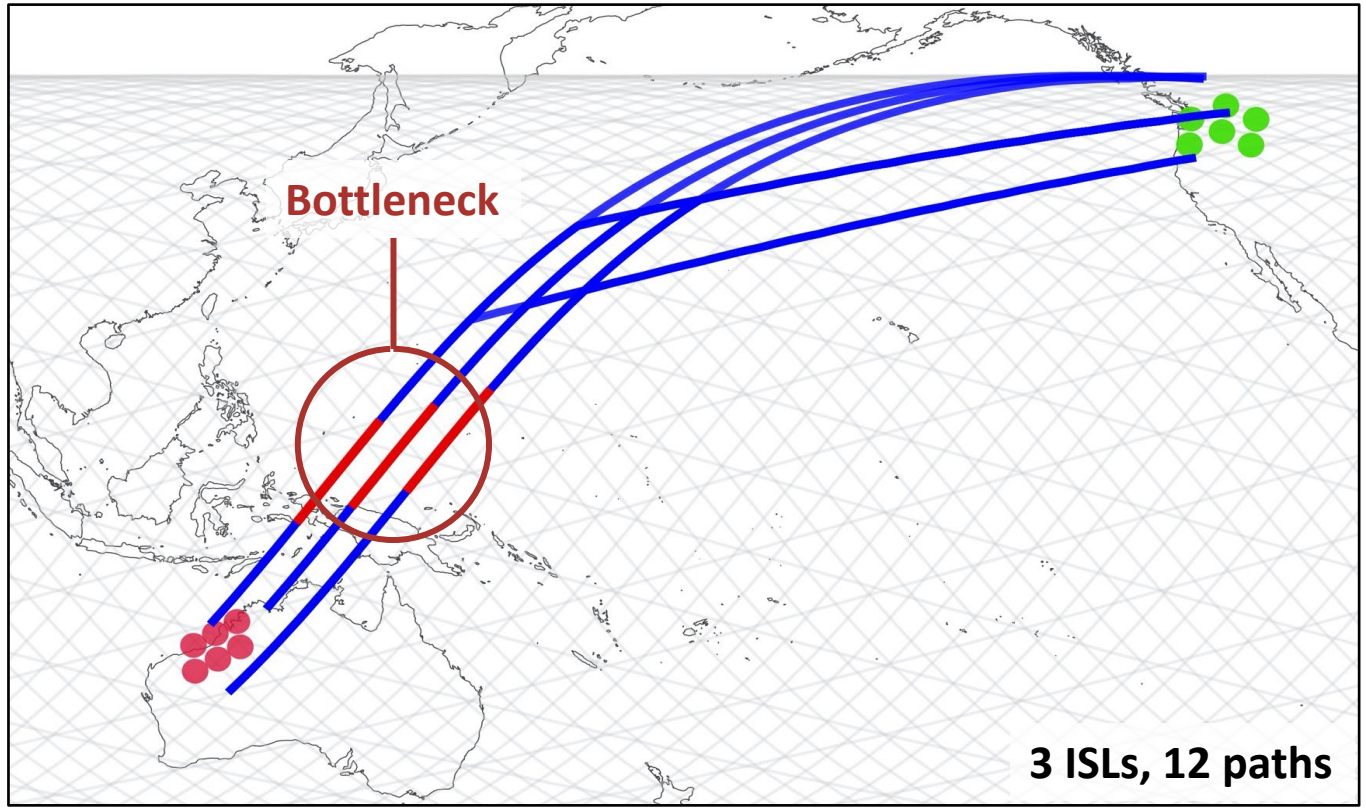
- Adversary sends exactly **one ISL worth of traffic**
  - The target must be congested
  - **No self congestion**

- **Very low detectability**
  - Roughly 1/8 of an uplink is the maximum load induced

- In the paper: results with baseline traffic (GDP, population)

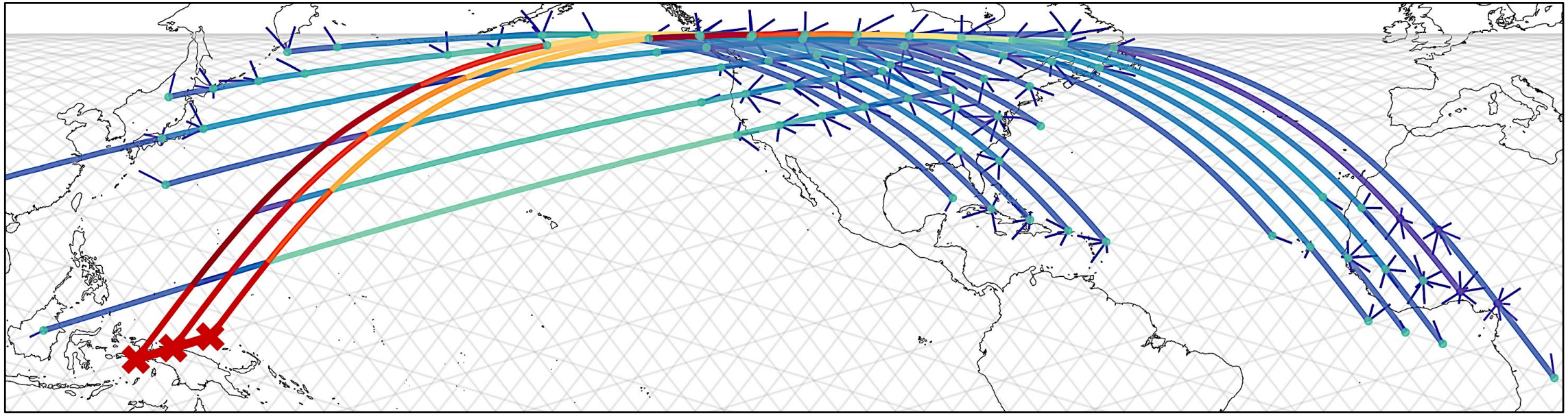


Harder attack: **ICARUS between regions**



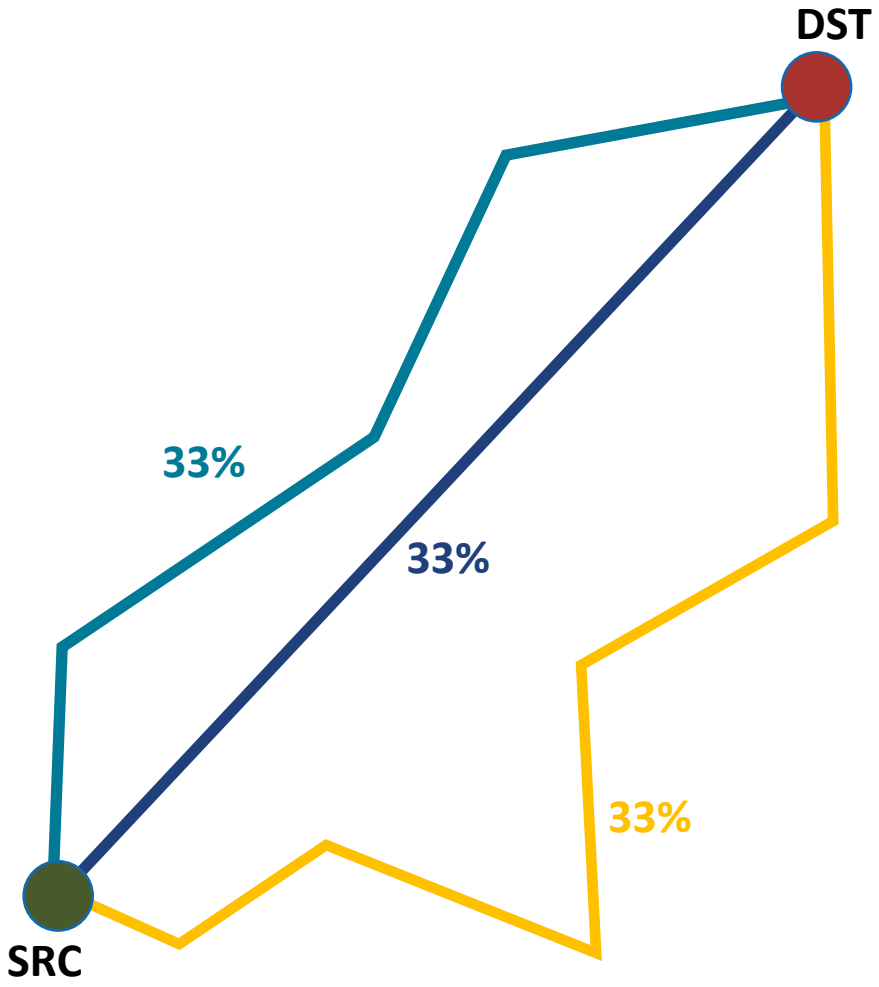
- **New goal**
  - Prevent communication between regions
- Same attack mechanism
  - Run a single attack on each bottleneck link at the same time
- Choose a **suitable set** of target links (bottleneck)
  - **NP-hard!**
  - Solved with heuristics

ICARUS between regions results



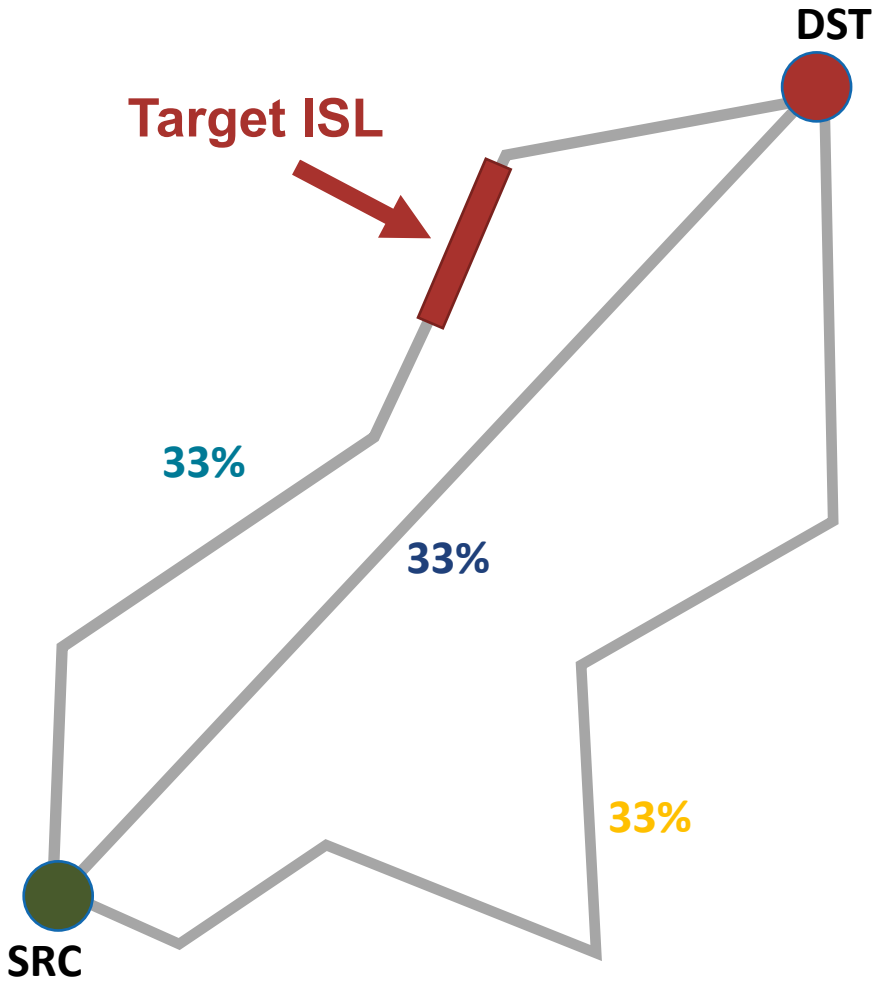
- Attack works on **92%** of tested region pairs
  - Very effective despite the complexity
- **Cost** contained in general
  - As the previous attack, **multiplied by the number of bottleneck links**
  - It depends on #ISL in bottleneck
- Similar **detectability** as single-link
  - **Adversary risks no additional exposure**
  - The bots are spread over a larger area

Realistic attack: **ICARUS on multi-path satellite network**



- **Remove the constraint of a single-path**
  - Multiple paths are available between source and destination terminal
  - They compose the **the load-balancing set**
  - The network chooses **one path** in the load-balancing set **at forwarding time**

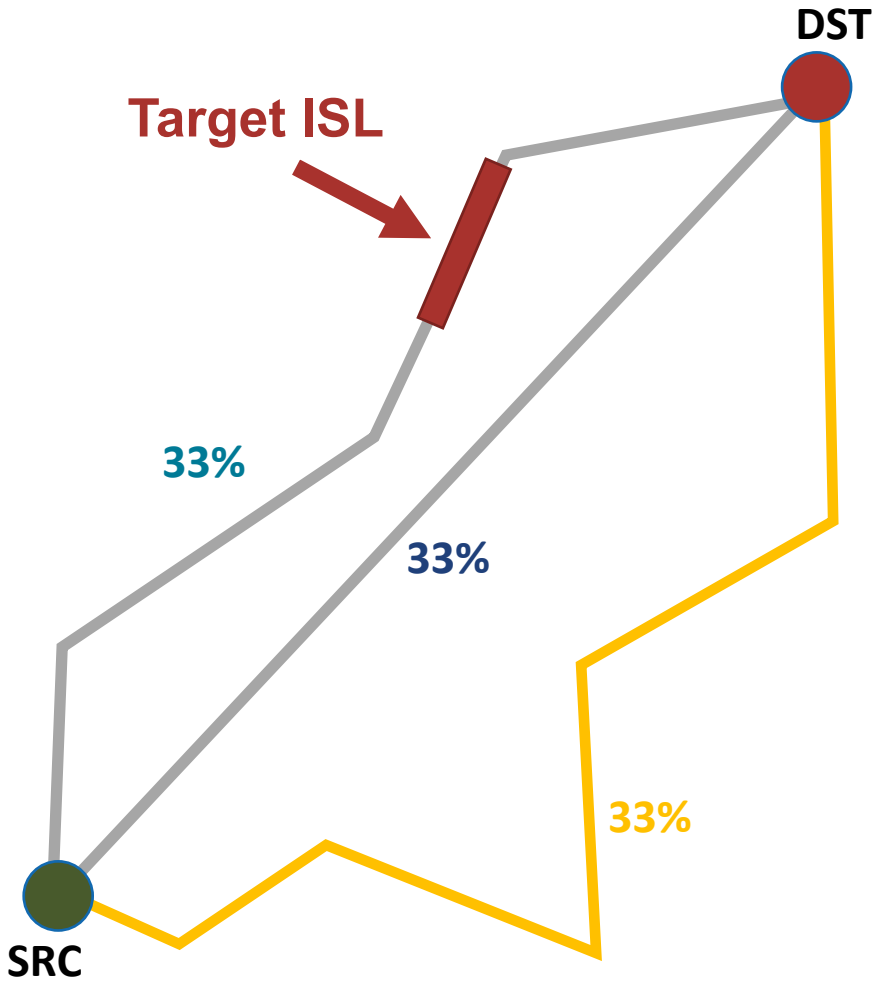
Realistic attack: **ICARUS on multi-path satellite network**



- **Remove the constraint of a single-path**
  - Multiple paths are available between source and destination terminal
  - They compose the **the load-balancing set**
  - The network chooses **one path** in the load-balancing set **at forwarding time**

- Adversary **can compute load-balancing sets**
  - **No knowledge** of which path is chosen
  - Attack is harder

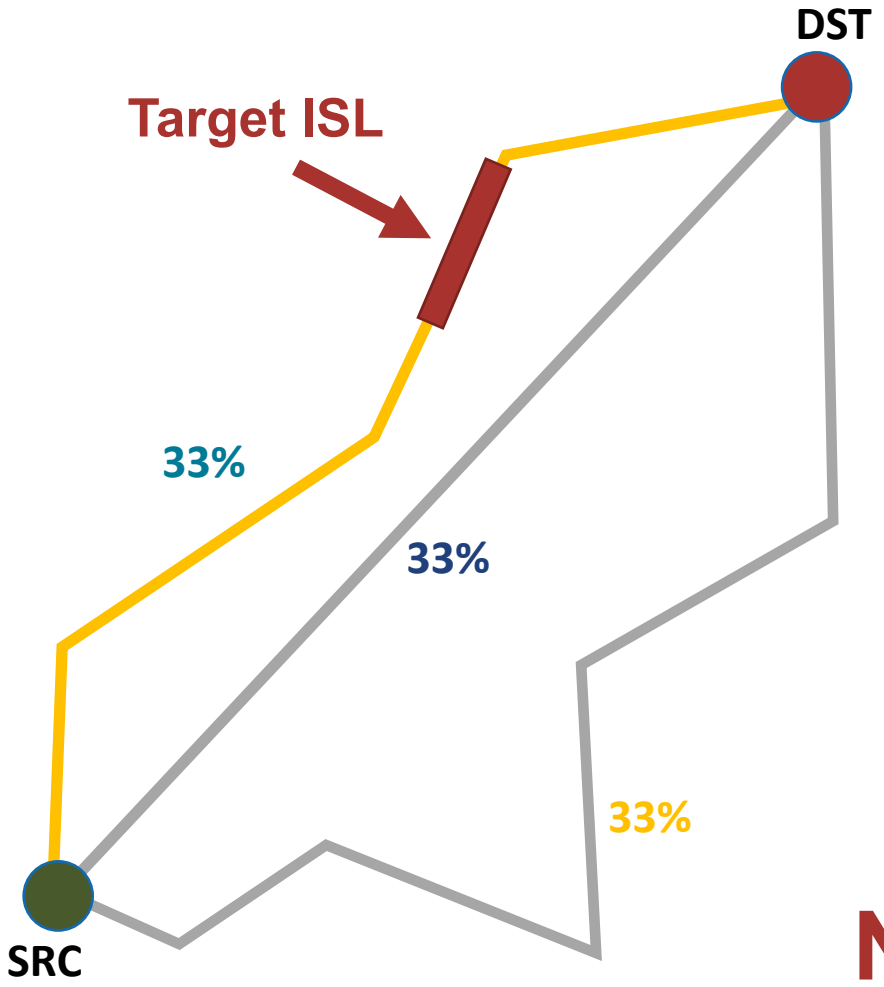
Realistic attack: **ICARUS on multi-path satellite network**



- **Remove the constraint of a single-path**
  - Multiple paths are available between source and destination terminal
  - They compose the **the load-balancing set**
  - The network chooses **one path** in the load-balancing set **at forwarding time**

- Adversary **can compute load-balancing sets**
  - **No knowledge** of which path is chosen
  - Attack is harder

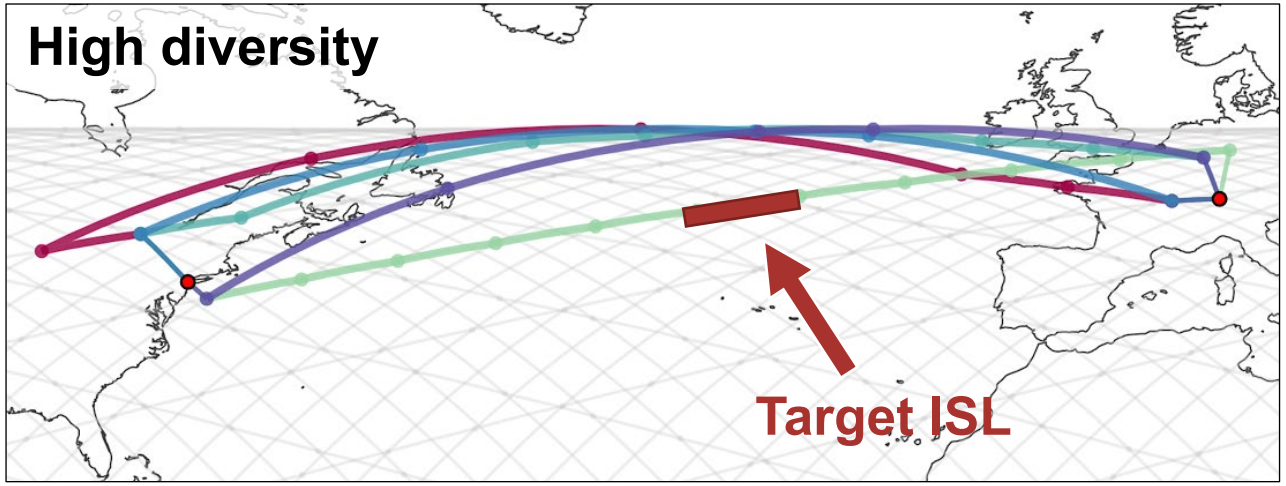
Realistic attack: **ICARUS on multi-path satellite network**



- **Remove the constraint of a single-path**
  - Multiple paths are available between source and destination terminal
  - They compose the **the load-balancing set**
  - The network chooses **one path** in the load-balancing set **at forwarding time**
- Adversary **can compute load-balancing sets**
  - **No knowledge** of which path is chosen
  - Attack is harder

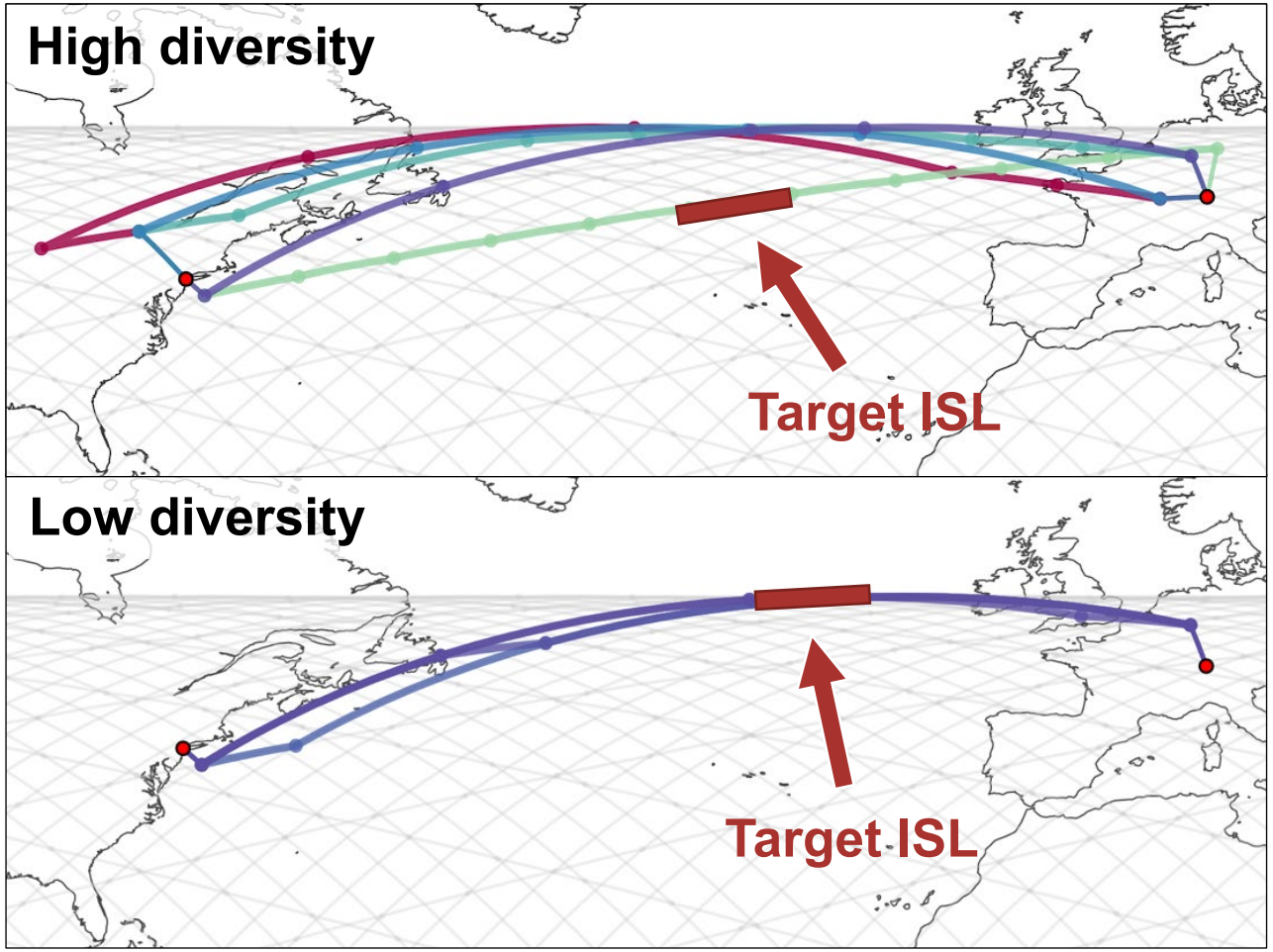
N times expected attack cost?

Is the attack harder? **High path diversity**



- With **high path diversity**:
  - **Probability of attacker reaching the target is lower** for any src-dst pairs
  - **Price to pay in latency**
  - **Up to 200% increase!**

Is the attack harder? **Low path diversity**

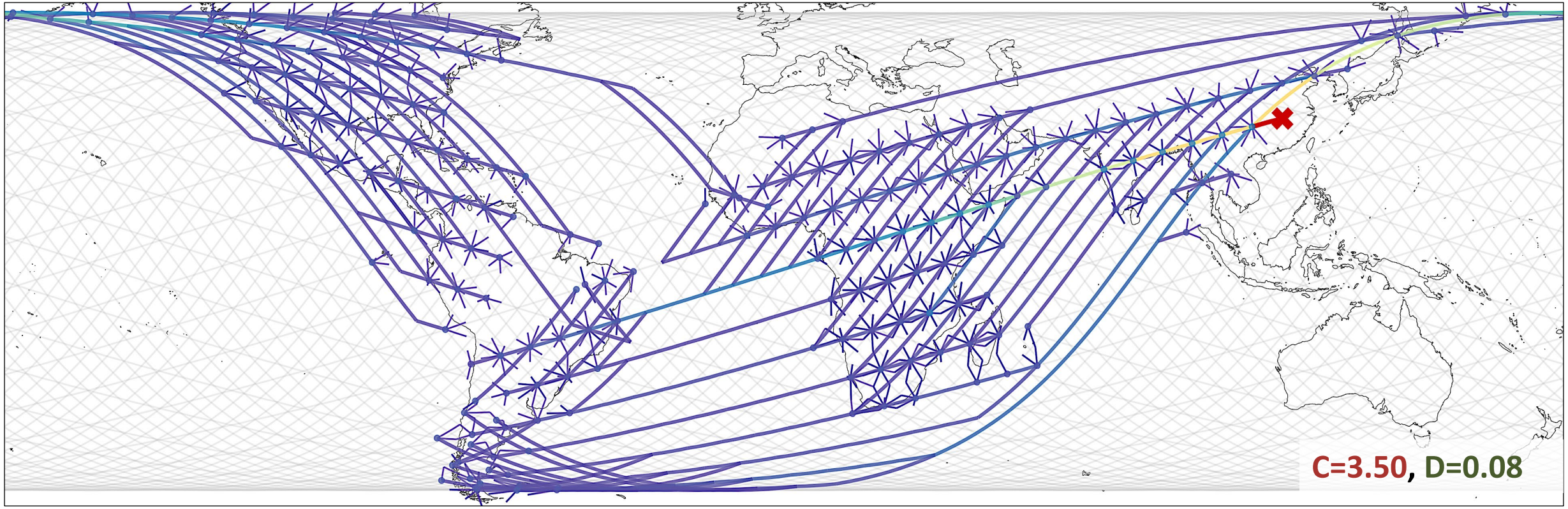


- With **high path diversity**:
  - **Probability of attacker reaching the target is lower** for any src-dst pairs
  - **Price to pay in latency**
  - **Up to 200% increase!**

- With **low path diversity**:
  - **Higher probability** of a successful attack
  - **Lower latency penalty**

Four Strategies
Max 5 paths per src-dst

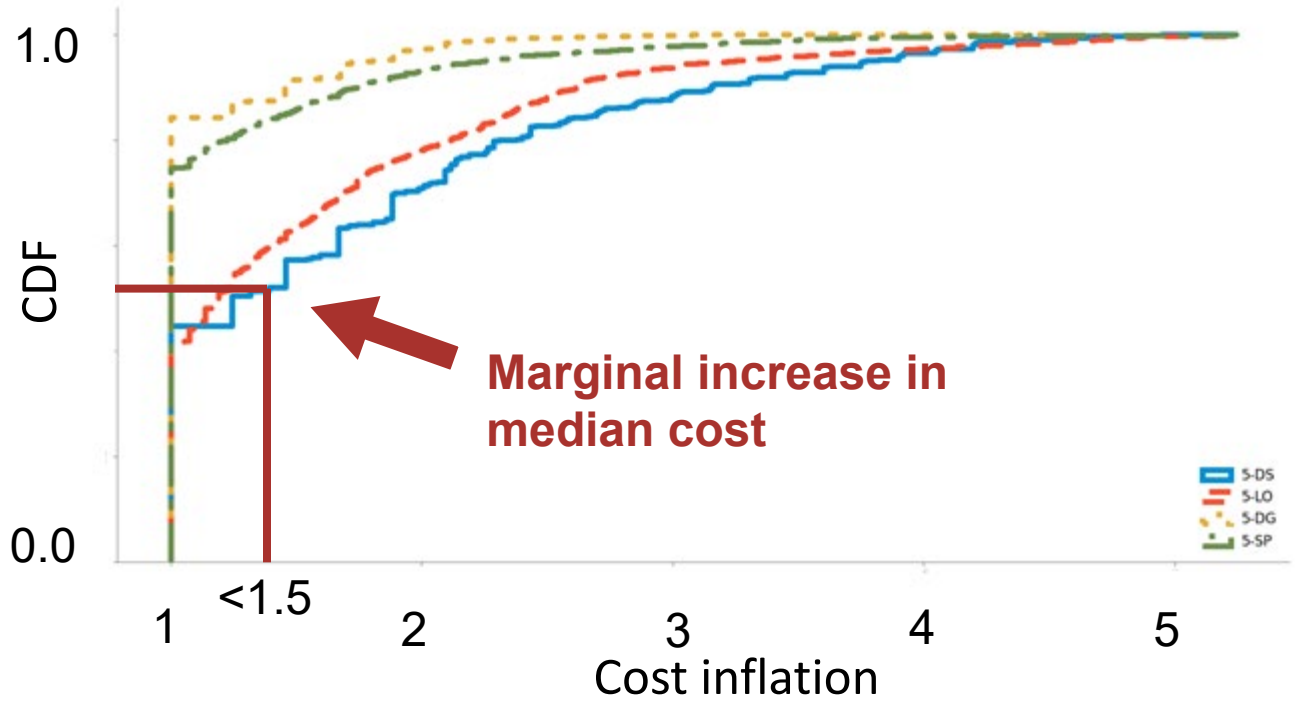
Probabilistic ICARUS **attack mechanism**



- Each **src-dst pair** has **P≤1 to reach the target**
- **Optimal attack source selection algorithm** in the paper

Probabilistic ICARUS results: **cost-detectability trade-off**

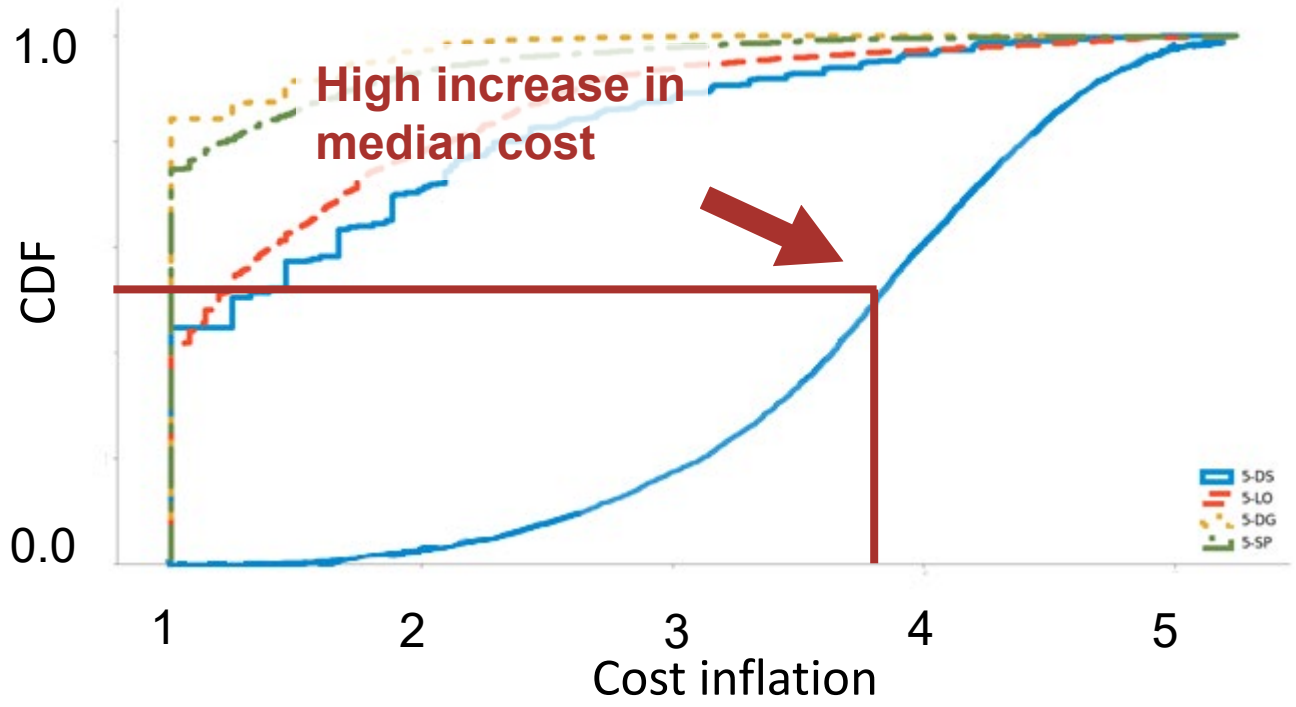
- **Success on most ISLs**
  - All routing schemes > 90%
  - All paths can be congested singularly
- **Cost-detectability tradeoff**
- **Cost optimization**
  - Low Cost for most links
  - Same as deterministic
- Terrible detectability
  - 1 full uplink in all cases



Probabilistic ICARUS results: **detectability optimization**

- **Detectability optimization**
  - Cost increases to 3.85 (median)
  - Still only ~80 Gbps attack traffic
  - Detect median 1/8 of an uplink, **same as deterministic**

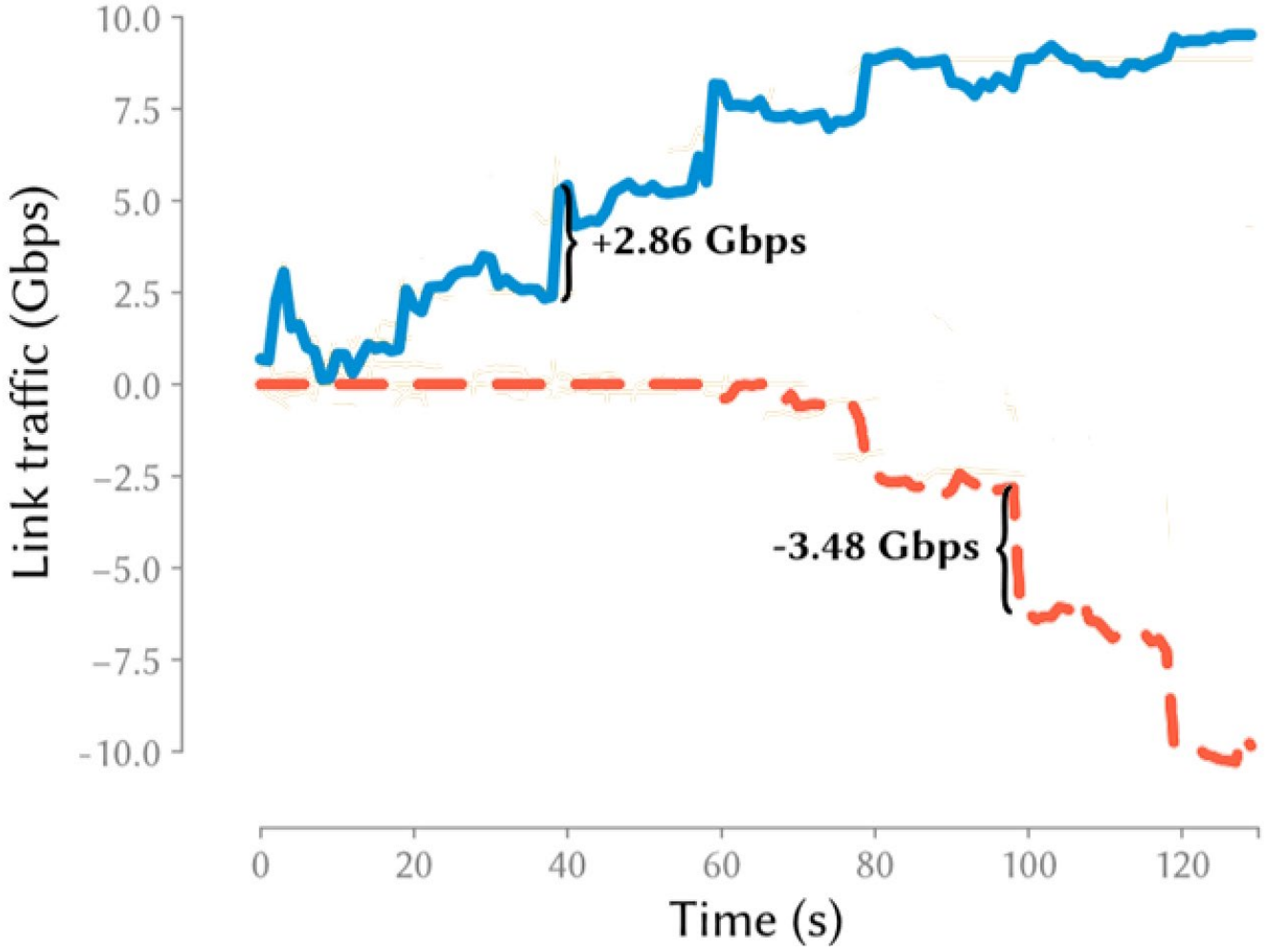
- Latency price pays off partially
  - Can launch an **optimal attack for one metric only**
  - Can find optimization objective balance



Can **dynamics** make attacks **worse**? **Load surges**

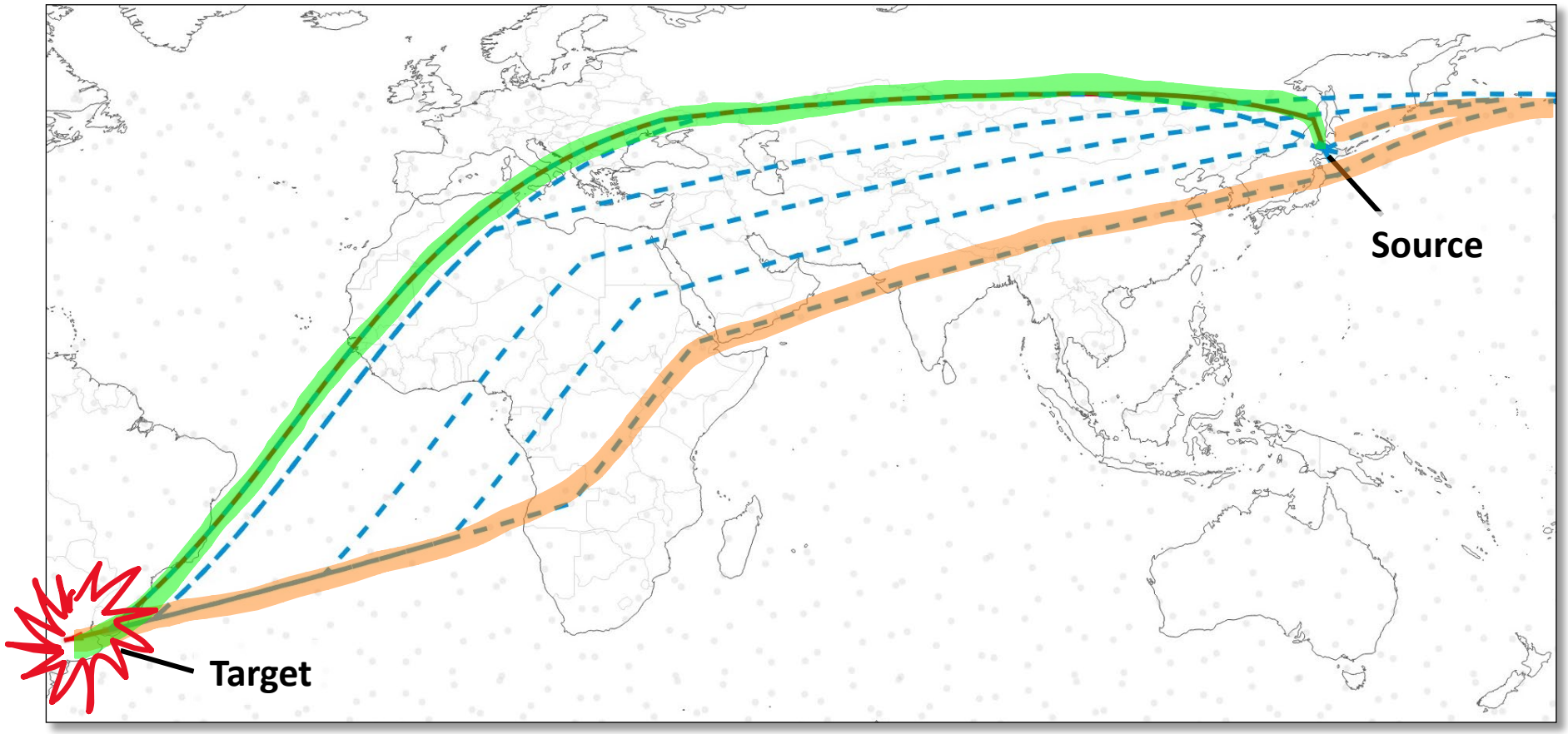
- As satellites move **paths change**
  - The load shifts accordingly
  - ISLs that **transit close to shortest paths** they suddenly see **load surges**

- Future work with **packet-based** simulation is needed to verify how **surges effect congestion**



Can **dynamics** make attacks **worse**? **Pulsing attacks**

- Load balancing introduces **overlapping paths** with **different latency**
  - Can be used to **multiply the attack rate**
  - Like “temporal lensing attacks” but given by the **moving topology of the network**
- Simulations show that **long-enough pulses** (>50ms) **are rare**



Mitigations

Traditional:

Attack and legitimate flows cannot be distinguished

- Traceback systems
- Traffic filtering
- Cloud DDoS protection

LSN-oriented:

- Resilient **routing and topology**
  - Better attack difficulty - latency price tradeoff
- Differential pricing
  - Make attacks economically infeasible
  - Low-latency links more expensive

Conclusions & Contributions

- **LSN network attacks are a threat**
  - Different network characteristics
  - Advantages and disadvantages for defense
- **ICARUS is powerful**
  - > 86% link success rate
  - ~100% path success rate
  - Low median detectability
  - Strong advantages from LSN environment
- **Defense not trivial**
  - Attack flows not distinguishable
  - Even with **load balancing**:
    path diversity and attack resilience ⟶ latency increase
- **Future outlook**
  - **Attack:**
    - Exploit network dynamics
  - **Defense:**
    Explore resilient load-balancing policies
    Explore strong topology designs
- **Evaluation framework** for future research
  `github.com/giacgiuliari/icarus-framework`

Thank You!

Giacomo Giuliari

`giacomog@inf.ethz.ch`