Attacking LEO satellite networks

Giacomo Giuliani, Tommaso Ciussani, Adrian Perrig, Ankit Singla
ETH Zurich
10 June 2021, USENIX ATC 21
STARLINK SPEED TESTS —
SpaceX Starlink speeds revealed as beta users get downloads of 11 to 60 Mbps
Ookla tests aren't showing the gigabit speeds

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

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

STARLINK SPEED TESTS —
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 more US states.

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

ETHzürich

Network Security Group

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

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

In the US alone!
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
SpaceX Starlink Shell 1

Global coverage

Low latency

FinTech

Remote AR

Cloud gaming

Remote surgery

Not just rural areas!
This tremendous potential generates great interest around LSNs…

…an interest shared by adversaries

How can they disrupt an LSN?
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
#2: Global access ⇒ 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** $\Rightarrow$ **Tight 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**
ICARUS: Attack mechanism

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

- Attack metrics:
  - Cost = # bots needed
  - Detectability = max # bots on an uplink

Effective attack ↔ low metrics
Satellite routing: in the paper…

**Single-shortest path routing**
- Low cost
- Low detectability

**Load-balanced routing**
- Cost-detectability trade-off

**Disconnect regions**
- 12 paths, 3 bottlenecks
- Same as single-link attacks

**Attacks worsened by satellite dynamics?**
- … maybe?
Load balancing over satellite paths

Path chosen at random at forwarding time from the load-balancing set
Load-balancing design space

Ideal:
Low latency
High bandwidth

Path Performance
(wrt shortest-path latency)

Path Diversity
(path overlap)

Low

High

BETTER
Load-balancing design space

**Ideal:**
- Low latency
- High bandwidth

- **Path Performance** (wrt shortest-path latency)
  - Low
  - High

- **Path Diversity** (path overlap)
  - Low
  - High

**Target ISL**
Load-balancing design space

Ideal:
- Low latency
- High bandwidth
- High diversity

Target ISL

Path Performance
(wrt shortest-path latency)

Path Diversity
(path overlap)
Load-balancing design space

Ideal:
Low latency
High bandwidth

Path Performance
(wrt shortest-path latency)

Path Diversity
(path overlap)
Load-balancing **design space**

**Ideal:**
- Low latency
- High bandwidth

**Path Performance** (wrt shortest-path latency)

**Path Diversity** (path overlap)

![Diagram showing the trade-off between path performance and path diversity. The ideal point is marked as low latency and high bandwidth, and the BETTER arrow indicates the direction of improving path performance with lower path overlap.](Image)
Load-balancing effect on attacks

Path Performance
(wrt shortest-path latency)

Path Diversity
(path overlap)

Trade-off for the adversary: low cost OR low detectability

Same as single-shortest path!
Probabilistic ICARUS **detectability optimization**

- **Cost:** 3.5 times the median single-shortest path attack cost
- **Detectability:** half of the median single-shortest path attack detectability
Mitigations

Traditional:

Attack and legitimate flows cannot be distinguished

- Traceback systems
- Traffic filtering
- Cloud DDoS protection

LSN-oriented:

- Resilient routing
- Improved topology design
- Increase attack cost/detectability without increasing latency
Conclusions & Contributions

- **LSN network attacks are a threat**
  - Different network characteristics
  - Advantages and disadvantages for defense

- **ICARUS is powerful**
  - ~100% path attack success rate
  - Low median cost and detectability

- **Defense not trivial**
  - Attack flows not distinguishable
  - Even with load balancing:
    path diversity and attack resilience $\rightarrow$ 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 Giuliani

giacomog@inf.ethz.ch