NDSS

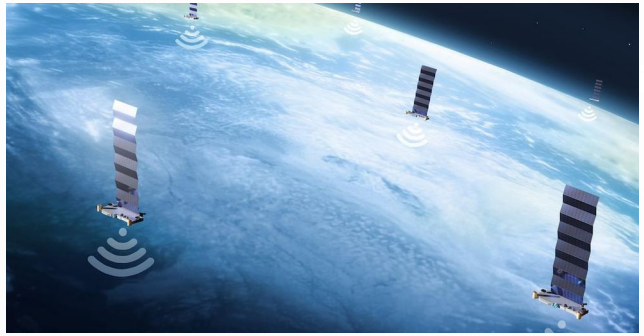
Time-varying Bottleneck Links in LEO Satellite Networks: Identification, Exploits, and Countermeasures

Yangtao Deng, Qian Wu, Zeqi Lai, Chenwei Gu, Hewu Li, Yuanjie Li, Jun Liu

清華大學
Tsinghua University

Internet from the space

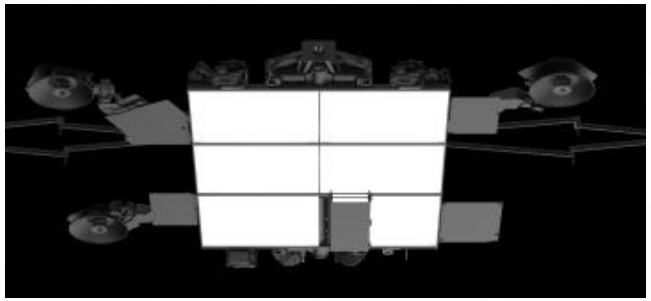
- Low-Earth-Orbit (LEO) Satellite Networks (LSNs) are under heavy development[1][2].
- Starlink[1][2] as an example:



7,000+ launched satellites

100+ ground stations (GSes)

4,000,000+ global users



3 lasers: Ground-satellite links (GSLs) or Inter-satellite links (ISLs)[3]

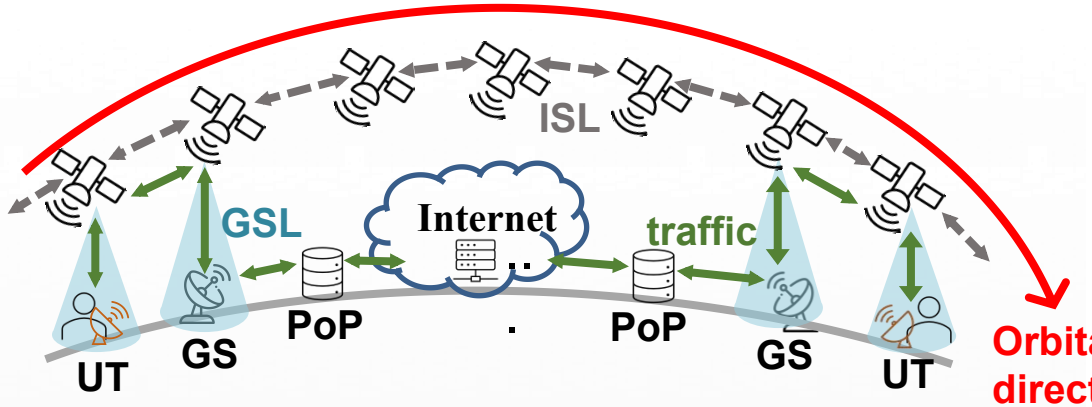
Up to **200 Gbps**[3]

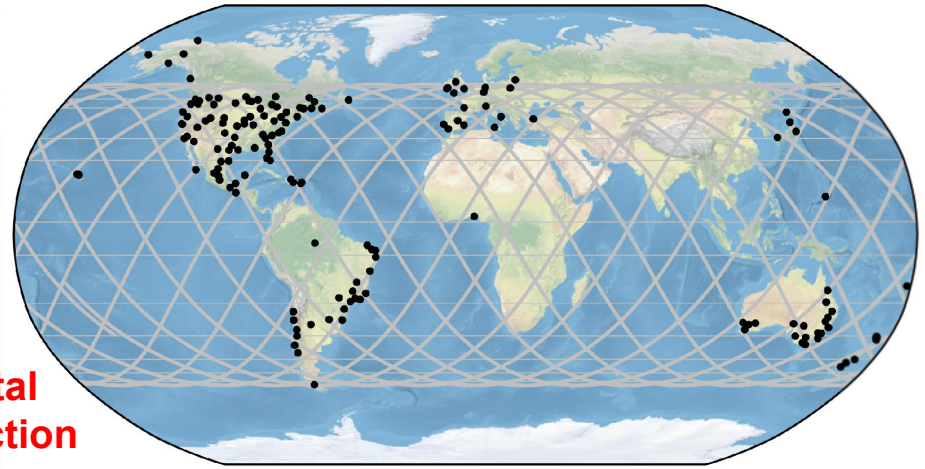
[1] SpaceX, "Starlink constellation," https://www.starlink.com/, 2025.
[2] SpaceX, "Starlink Ground Station." https://starlinkinstallationpros.com/starlink-ground-station-backbone-of-satellite-internet/, 2024.
[3] SpaceX, "Starlink Optical Space Lasers." https://www.starlink.com/technology, 2025

Internet from the space

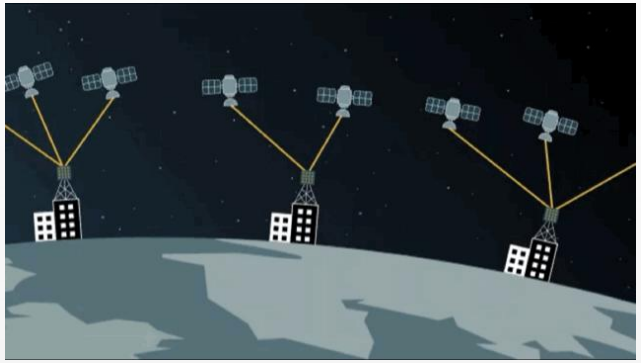
Tsinghua University

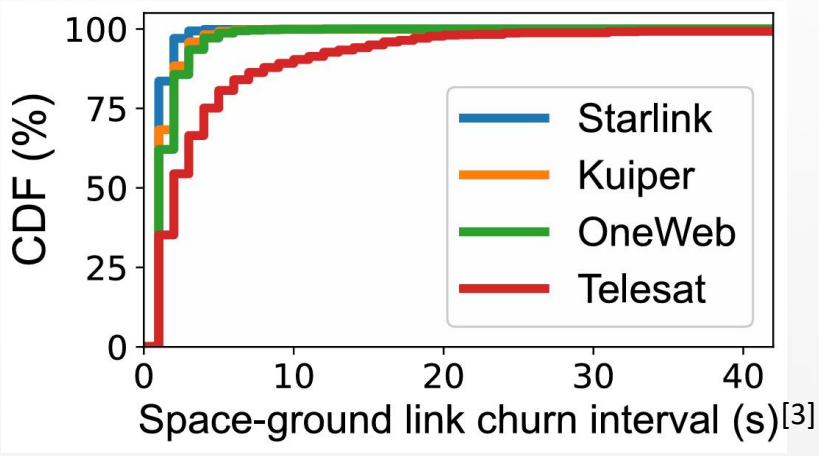
- Characteristics: **spatial disparity** and **temporal dynamism**[1].





Uneven GS distributions





Frequent handovers

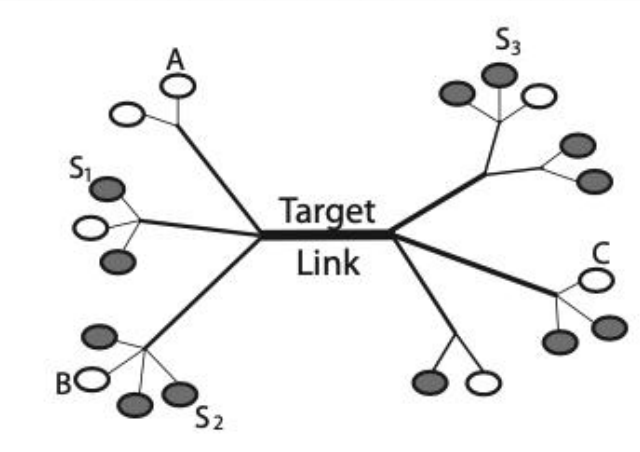
[1] "Internet in Space" for Terrestrial Users via Cyber-Physical Convergence, HotNets'21

Security issues in LSNs

- Real-world incidents: DDoS attacks[1], terminal fault injections[2], and so on.
- Link-flooding attack (LFA) risks: Coremelt[3]-like **flooding** towards **ISLs and GSLs**[4].

Killnet Gloats About DDoS Attacks Downing Starlink, White House

Elon Musk-owned Starlink, WhiteHouse.gov, and the Prince of Wales were targeted by Killnet in apparent retaliation for its support of Ukraine.

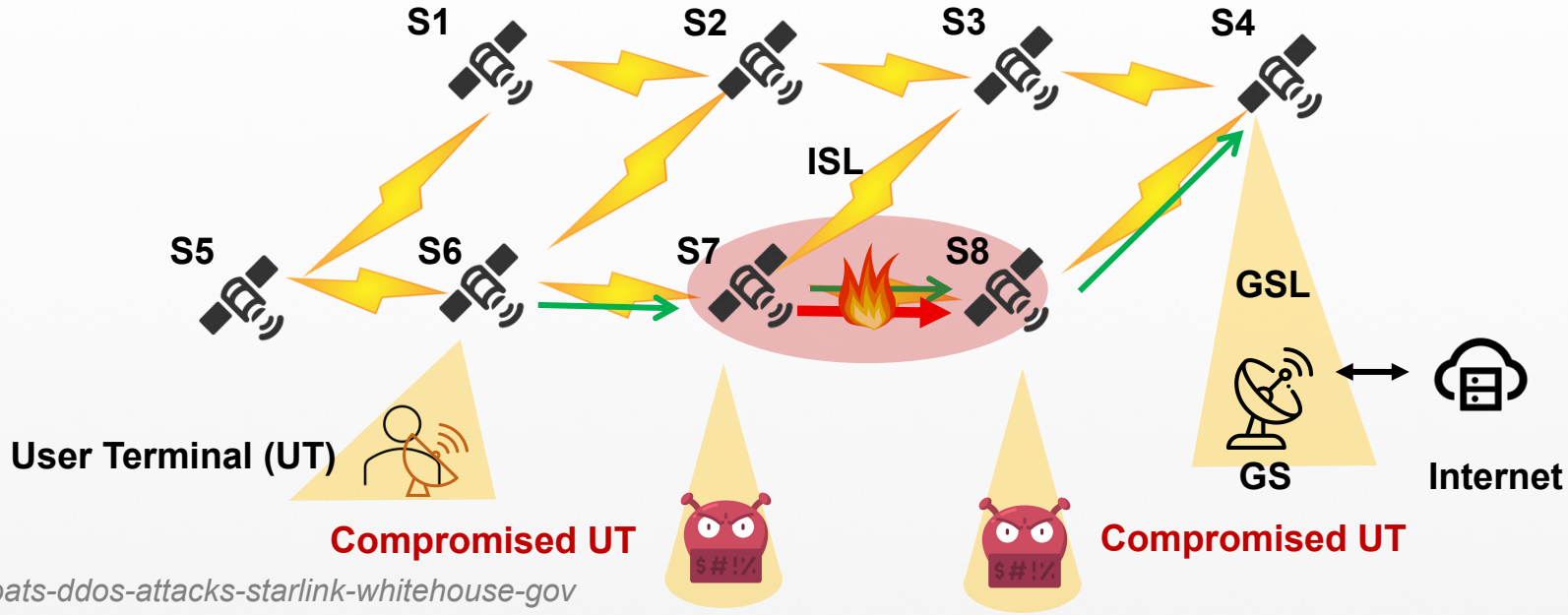


Coremelt[3]: Flooding target links with compromised nodes

MATT BURGESS SECURITY AUG 10, 2022 10:00 AM

The Hacking of Starlink Terminals Has Begun

It cost a researcher only $25 worth of parts to create a tool that allows custom code to run on the satellite dishes.



[1] https://www.darkreading.com/threat-intelligence/killnet-gloats-ddos-attacks-starlink-whitehouse-gov
[2] https://www.wired.com/story/starlink-internet-dish-hack/
[3] The Coremelt Attack, ESORICS'09
[4] ICARUS: Attacking Low Earth Orbit Satellite Networks, ATC'21

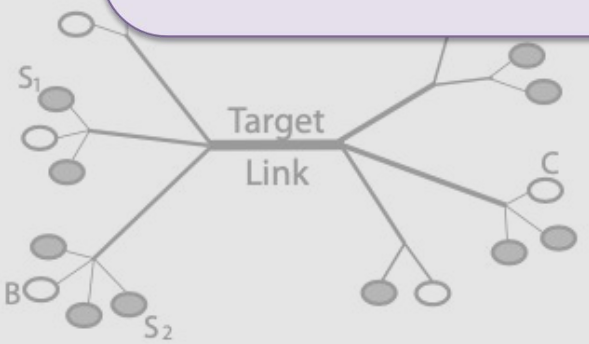
Security issues in LSNs

Tsinghua University

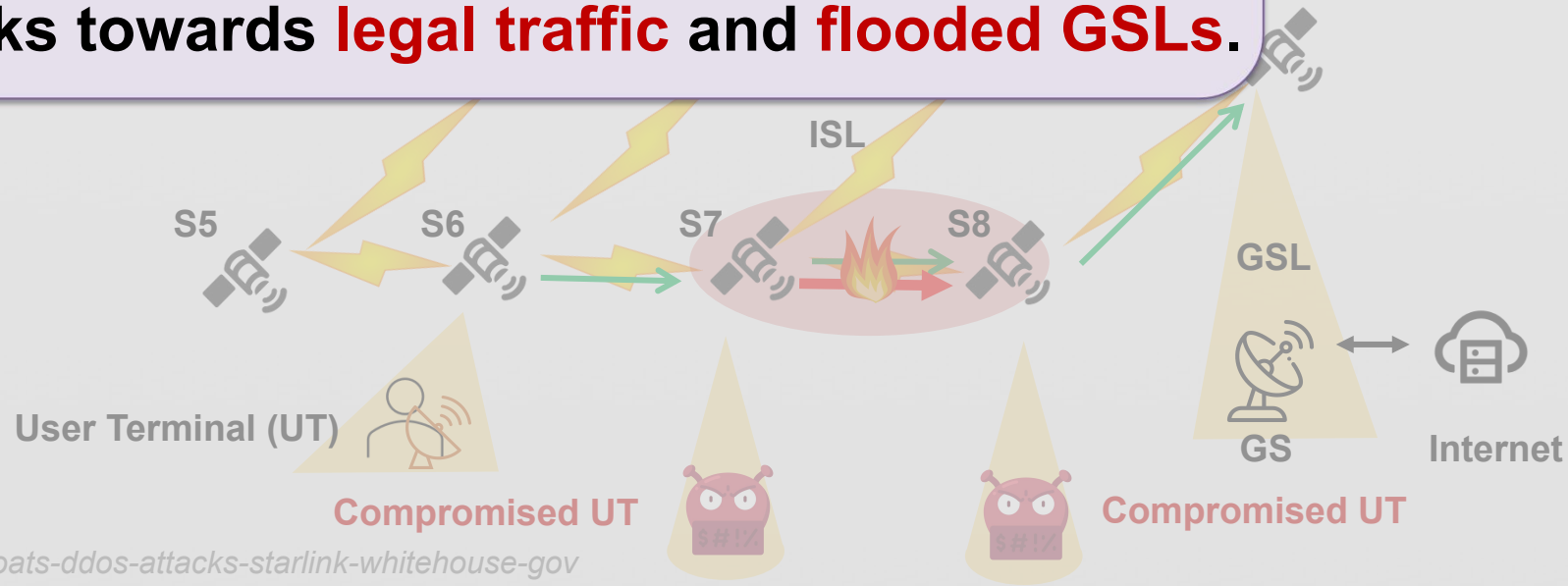
- Real-world incidents: DDoS attacks[1], terminal fault injections[2], and so on.
- Link-flooding attack (LFA) risks: Coremelt[3]-like flooding towards ISLs and GSLs[4].

Currently, no LFA risk analyzer that

- **Considers the disparities of GS distributions and high-dynamism of time-varying links.**
- **Quantifies the risks towards legal traffic and flooded GSLs.**



Coremelt[3]: Flooding target links with compromised nodes



[1] https://www.darkreading.com/threat-intelligence/killnet-gloats-ddos-attacks-starlink-whitehouse-gov
[2] https://www.wired.com/story/starlink-internet-dish-hack/
[3] The Coremelt Attack, ESORICS'09
[4] ICARUS: Attacking Low Earth Orbit Satellite Networks, ATC'21

Security issues in LSNs

Tsinghua University

- Real-world incidents: DDoS attacks[1], terminal fault injections[2], and so on.
- Link-flooding attack (LFA) risks: Coremelt[3]-like flooding towards ISLs and GSLs[4].

Currently, no LFA risk analyzer that

- **Considers the disparities of GS distributions and high-dynamism of time-varying links.**
- **Quantifies the risks towards legal traffic and flooded GSLs.**

How can we build such an LFA risk analyzer?

Coremelt[3]: Flooding target links with compromised nodes

[1] https://www.darkreading.com/threat-intelligence/killnet-gloats-ddos-attacks-starlink-whitehouse-gov
[2] https://www.wired.com/story/starlink-internet-dish-hack/
[3] The Coremelt Attack, ESORICS'09
[4] ICARUS: Attacking Low Earth Orbit Satellite Networks, ATC'21

Previews in one minute

Tsinghua University

❑ To analyzer the consequences,

We firstly observed that **bottleneck links exist**, which transmits more traffic from more regions.

⇩

SKYFAL: to **analyze the potential risks** by collecting public information and assessing the negative impacts from compromised UTs.

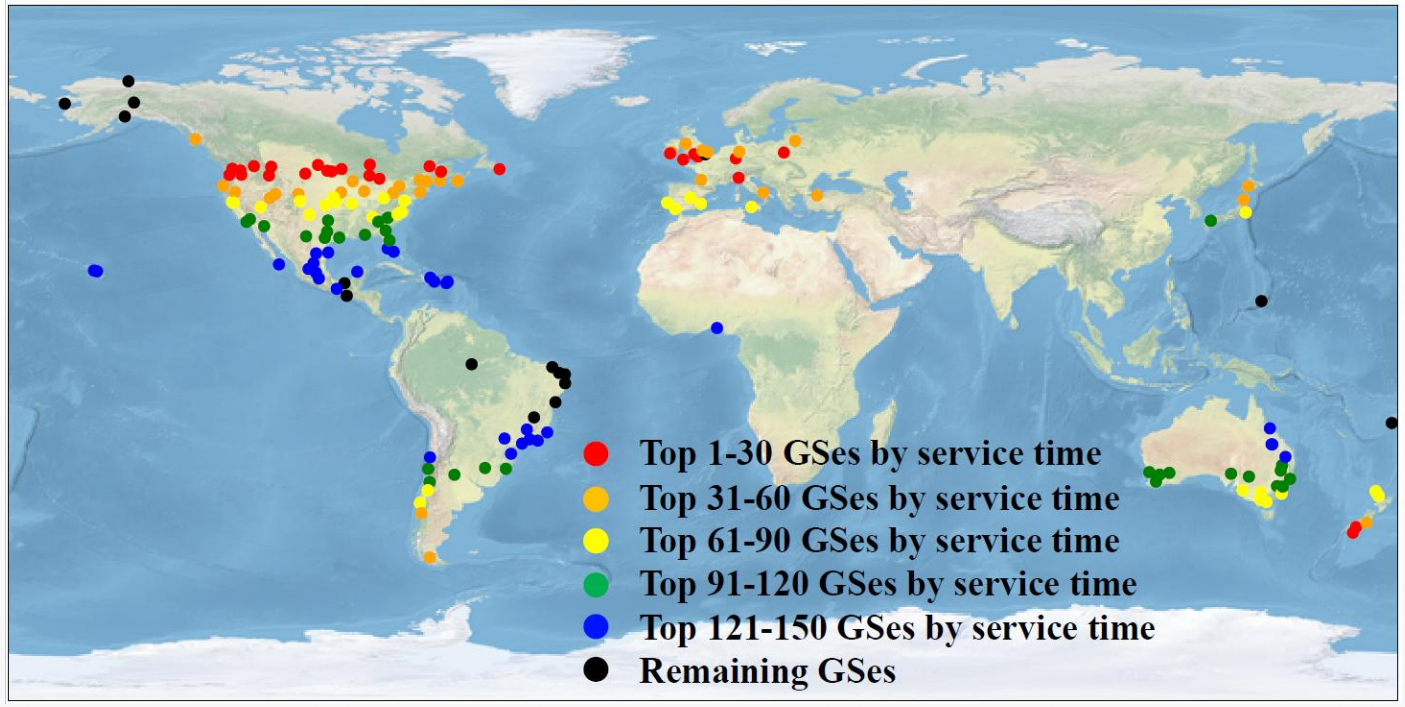
⇩

Analysis results, including validation of the bottleneck links, adverse impacts on traffic and GSLs, variability analysis, and so on.

Characterizing the uneven GS service time

Tsinghua University

❑ **GS service time**: the total accumulated time with all connectable satellites throughout the day so as to offer services.



Starlink GS distribution with respect to service time

Reason

- Satellites and GSes **distribute unevenly** across latitudes.

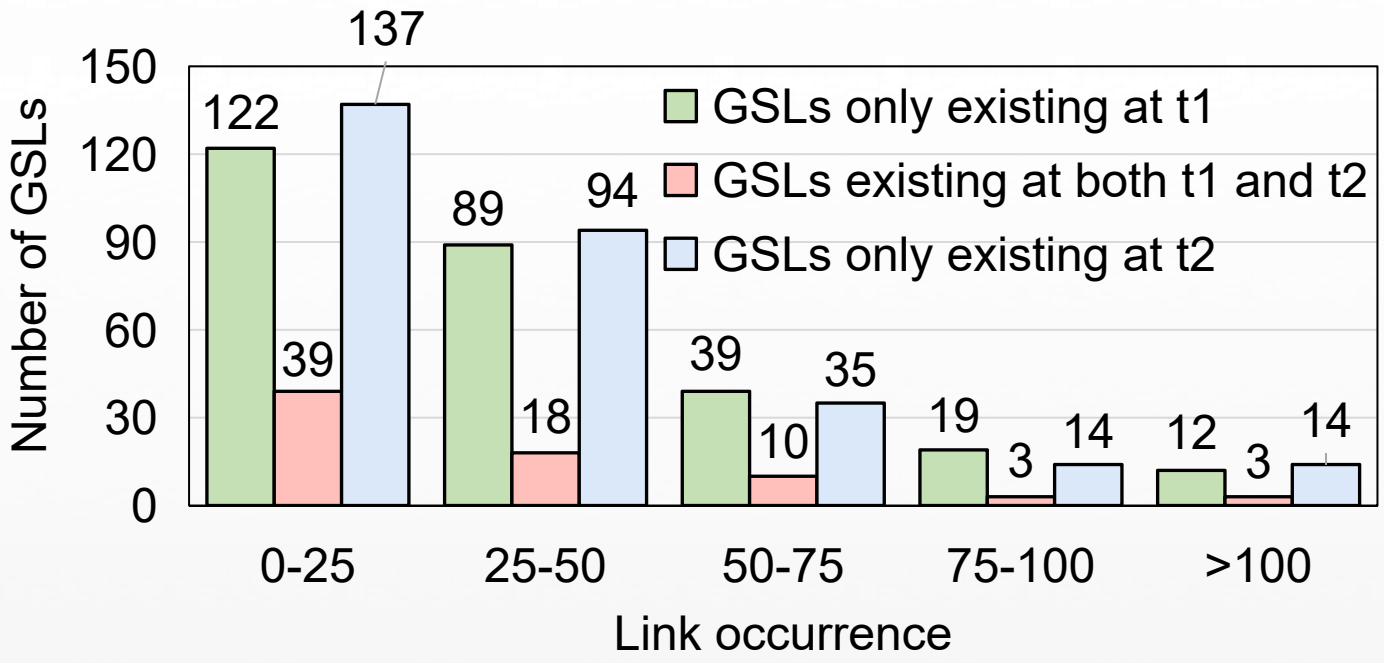
Takeaway

- Longer service time of GSes in **mid- to high-latitude** regions.
- **A longer service time** suggests a higher activity level and is **more likely to be flooded** for a long duration.

Characterizing the time-varying GS occurrence

Tsinghua University

❑ **GS occurrence**: the occurrence by the times of its **presence on the routes** from all the geographical **blocks** to the Internet via LSNs.



Starlink GSL occurrence distribution

Reason

- The **uneven distribution** of satellites and GSes.
- The **frequenct handovers**.

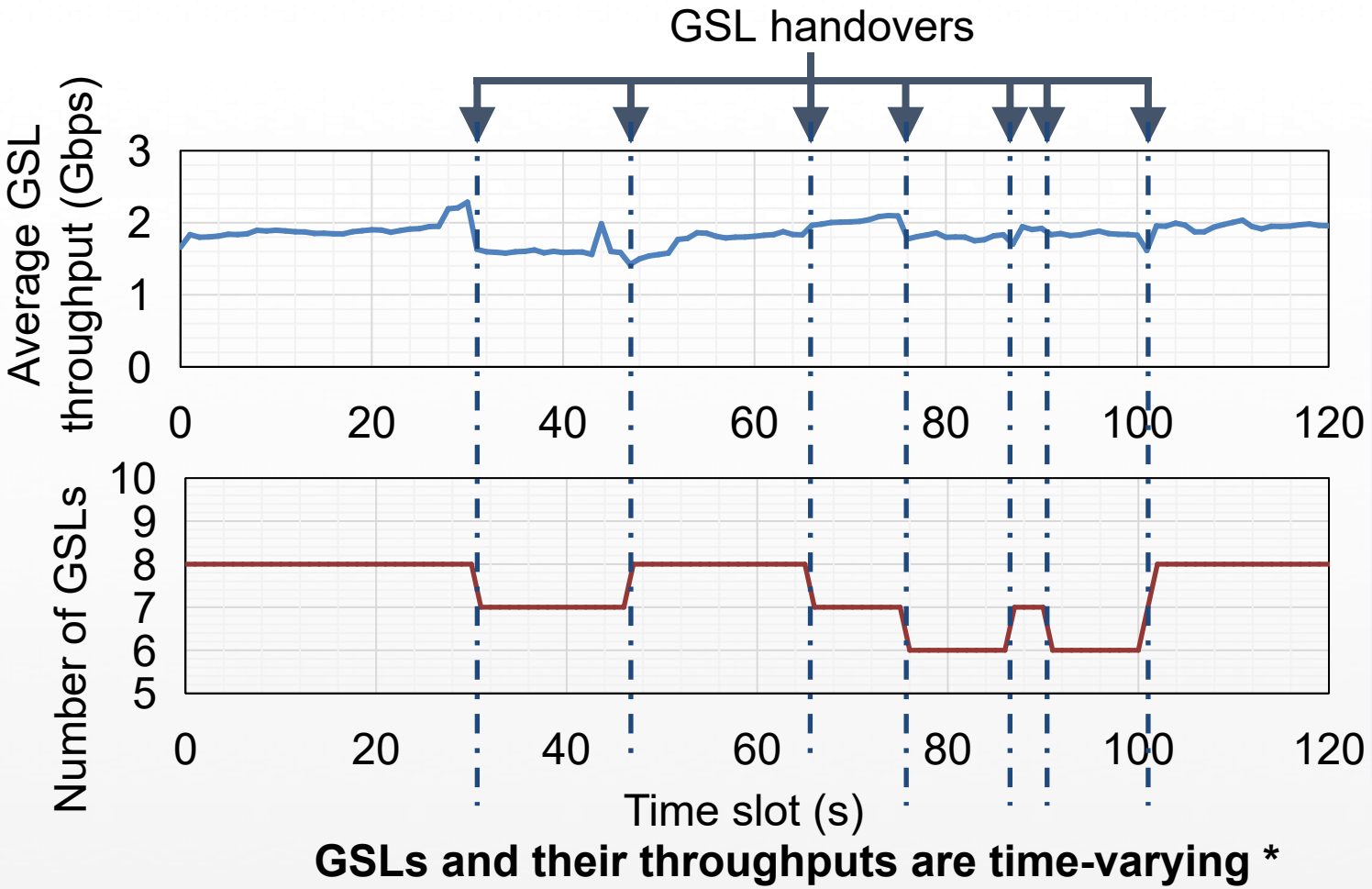
Takeaway

- A higher occurrence shows a greater chance as an attack target.
- **Spatial disparity** in GS occurrences.
- **Temporal dynamism** in GS occurrences. GSL durations are short.

Characterizing the time-varying GSL throughput

Tsinghua University

❑ **GSL throughput**: the throughput of legal user traffic.



GSLs and their throughputs are time-varying *

* the GS located in Ajigaura, Japan

Reason

- The **uneven distribution** of users.
- The **frequenct handovers**.

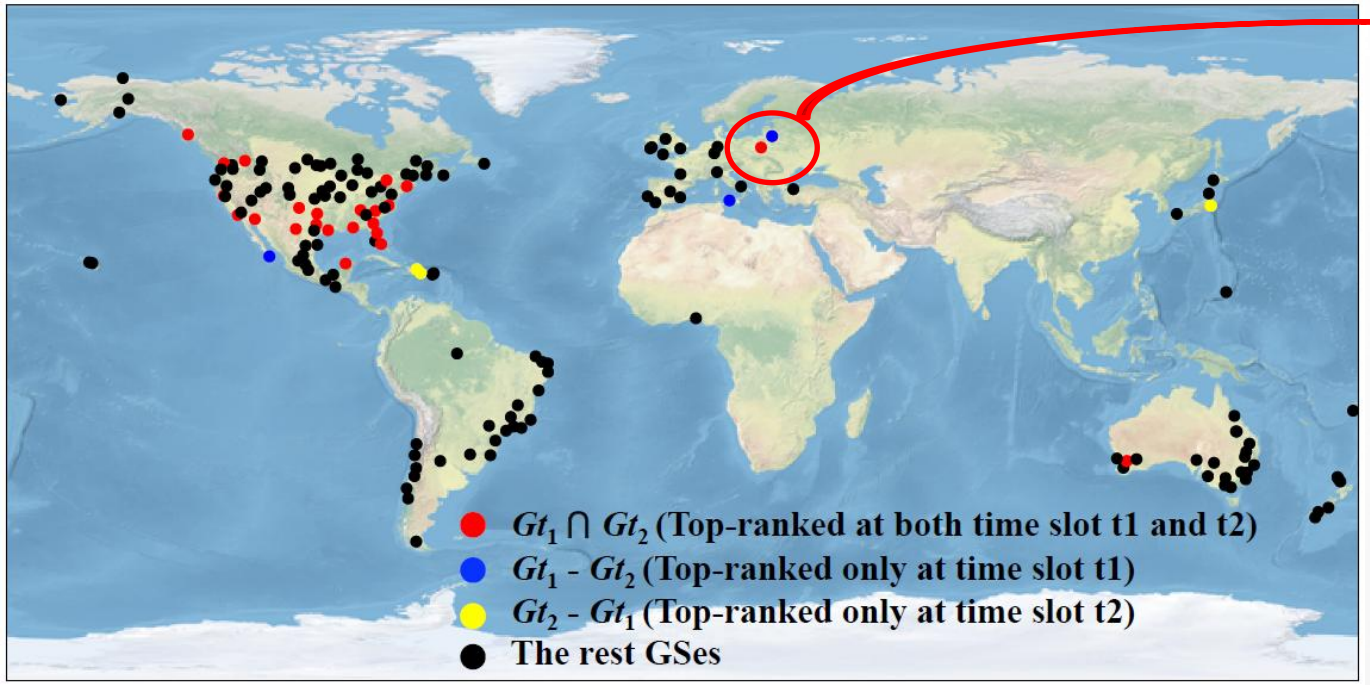
Takeaway

- A higher throughput indicates more traffic can be **congested**.
- **Spatial disparity** in GSL throughputs and the number of connected GSLs.
- **Temporal fluactuations** in the average throughput of GSLs.

Identifying bottleneck links: case analysis

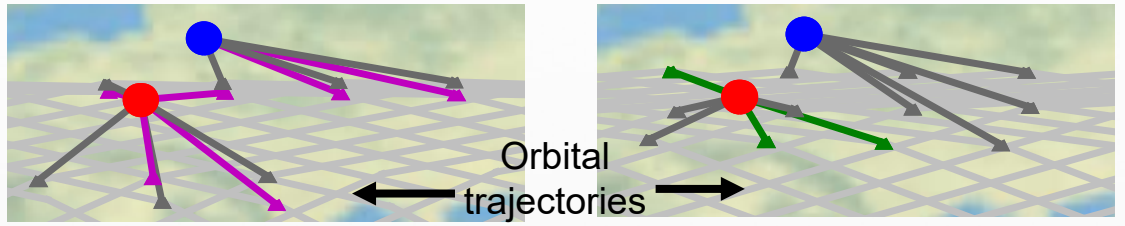
Tsinghua University

- Step one: identify the top-ranked GSes in their service time, and occurrences. ➡ G_t
- Step two: prioritize their connected GSLs based on their link throughputs. ➡ BN_t
- Step three: repeat for each time slot of T. ➡ $U_{t \in T} BN_t$



Top-ranked GSes by service time and occurrence

Zoom in



Eastern Europe at t1

- BN_{t1}
- BN_{t2}
- The rest connected GSLs

Eastern Europe at t2

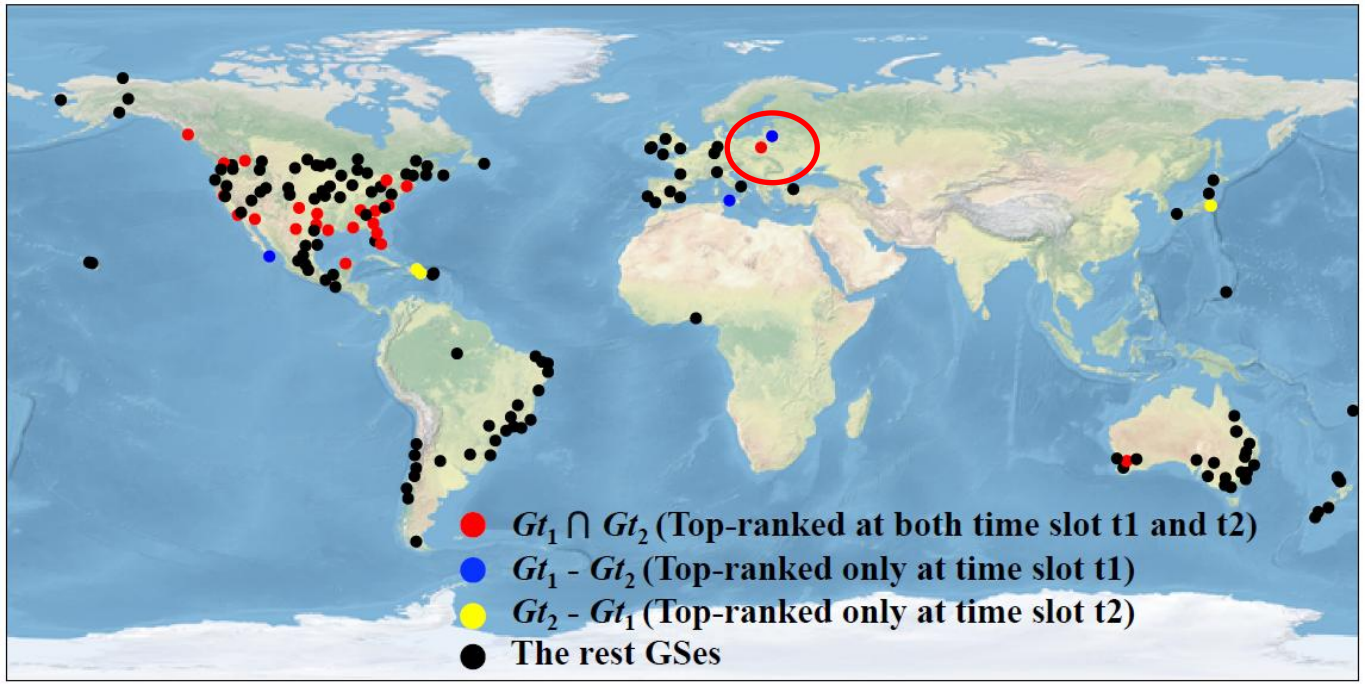
- Satellites connected to BN_{t1}
- Satellites connected to BN_{t2}
- The rest connected satellites

BNt_1 and BNt_2 in Eastern European

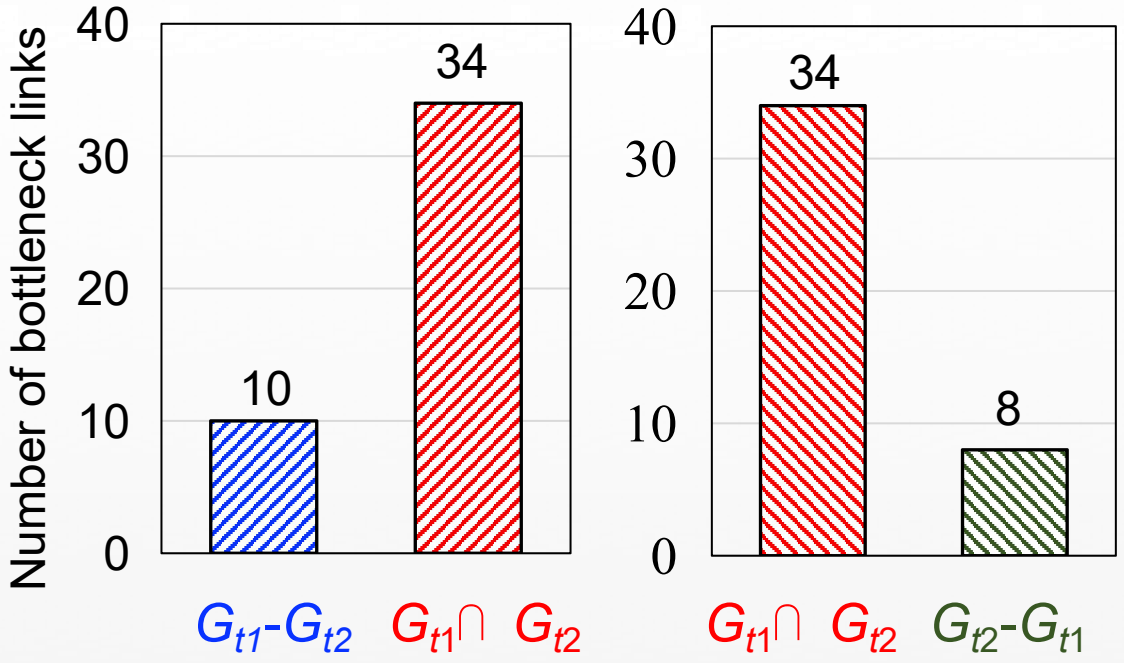
Identifying bottleneck links: case analysis

Tsinghua University

- Step one: identify the top-ranked GSes in their service time, and occurrences. ➡ G_t
- Step two: prioritize their connected GSLs based on their link throughputs. ➡ BN_t
- Step three: repeat for each time slot of T. ➡ $U_{t \in T} BN_t$



Top-ranked GSes by service time and occurrence



Number and distribution of BNt_1 and BNt_2

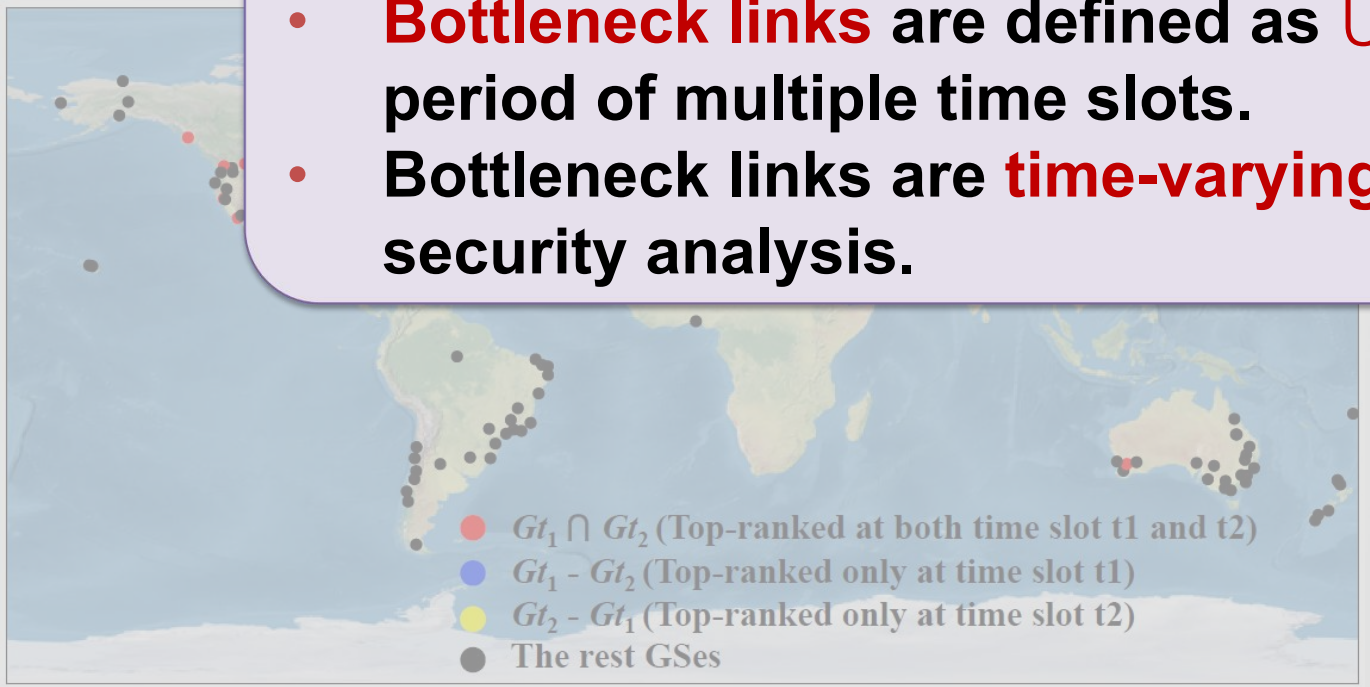
Identifying bottleneck links: case analysis

Tsinghua University

- Step one: identify the top-ranked GSes in their service time, and occurrences. ➡ G_t
- Step two: prioritize their connected GSLs based on their link throughputs. ➡ BN_t
- Step t

Takeaway

- **Bottleneck links** are defined as $\cup_{t \in T} BN_t$, where T is the period of multiple time slots.
- Bottleneck links are **time-varying** targets for flooding security analysis.



Top-ranked GSes by service time and occurrence

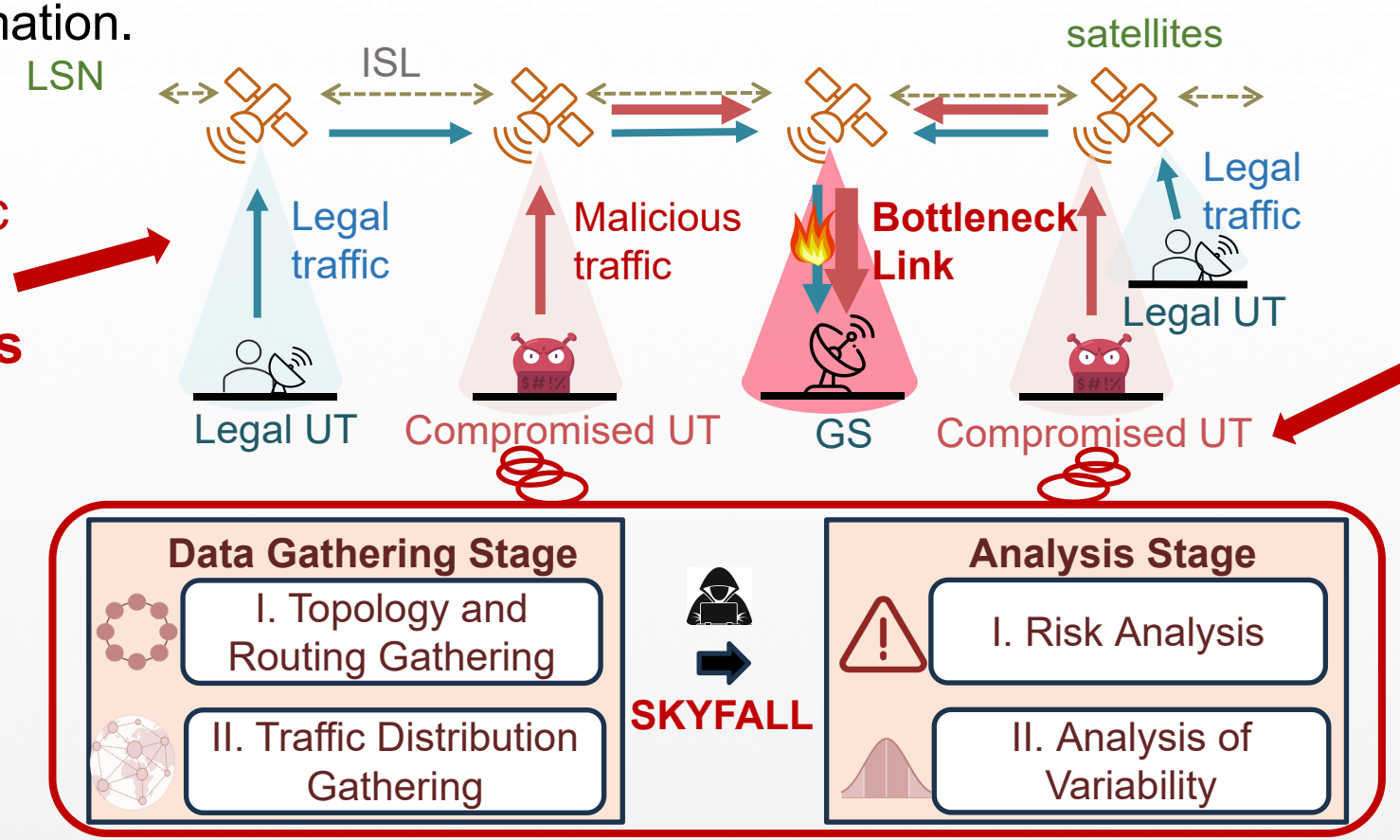
Number and distribution of BNt_1 and BNt_2

Design: SKYFALL framework

Tsinghua University

- SKYFALL: an LFA risk analyzer for LSNs.
  - **Data Gathering Stage**: collecting the information of LSN **topology**, **routing**, and **traffic distribution**.
  - **Analysis Stage**: analyzing the potential **risks** and **variability** influencing the risks based on the gathered information.

Gathering public information to **model the LSNs**



Using compromised UTs to simulate **LFA**

Analysis methodology

Tsinghua University

❑ Data Gathering Stage.

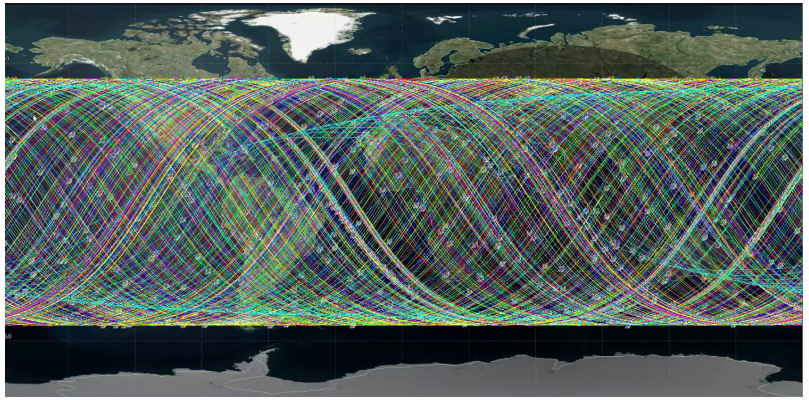
➢ **Topology and routing**: based on Two-line Element sets (TLEs)[1], conjunction reports[2], and public disclosures.

TLEs,
Conjunction reports
.....

⇨

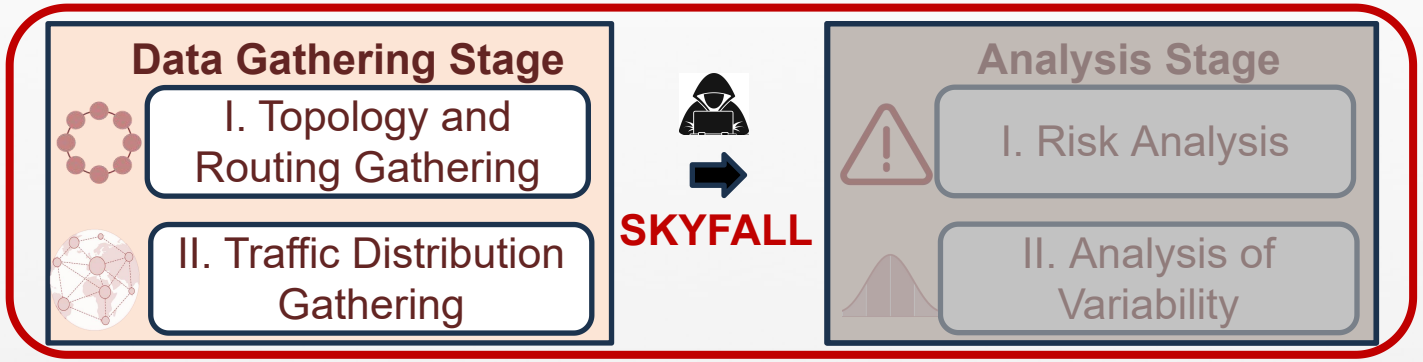
satellite positions,
directions,
velocities

⇨



Accurate trajectory modelling for each time slot

➢ **Traffic distribution estimation**: by transmitting UDP packets with a linearly increasing throughput.



[1] Two-Line Element (TLE) set. https://en.wikipedia.org/wiki/Twoline_element_set,
[2] CCSDS Recommendation for Space Data System Standards (508.0-B-1): Conjunction Data Messages. https://public.ccsds.org/Pubs/508x0b1e2c2.pdf

Analysis methodology

Tsinghua University

❑ Analysis Stage.

➢ **Risk analysis**.

① Identify the bottleneck links.

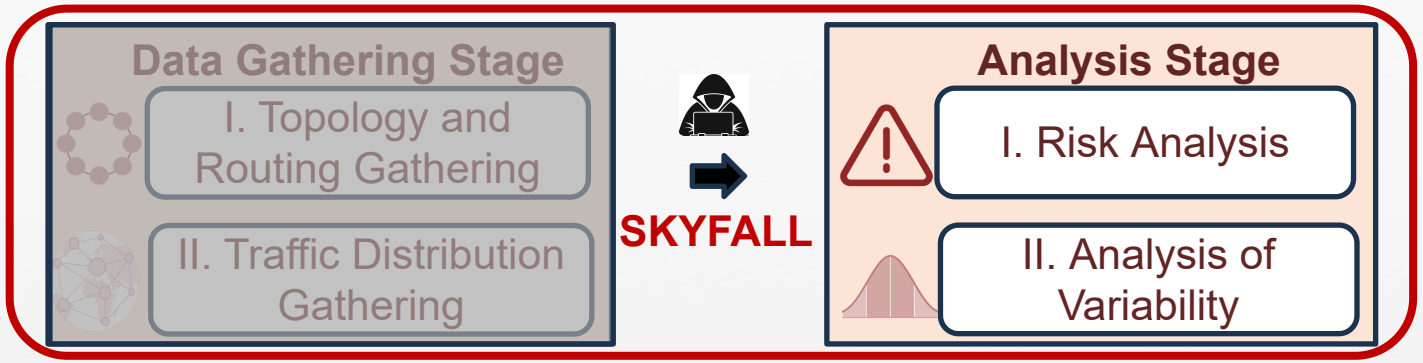
② Generate malicious traffic with compromised UTs.

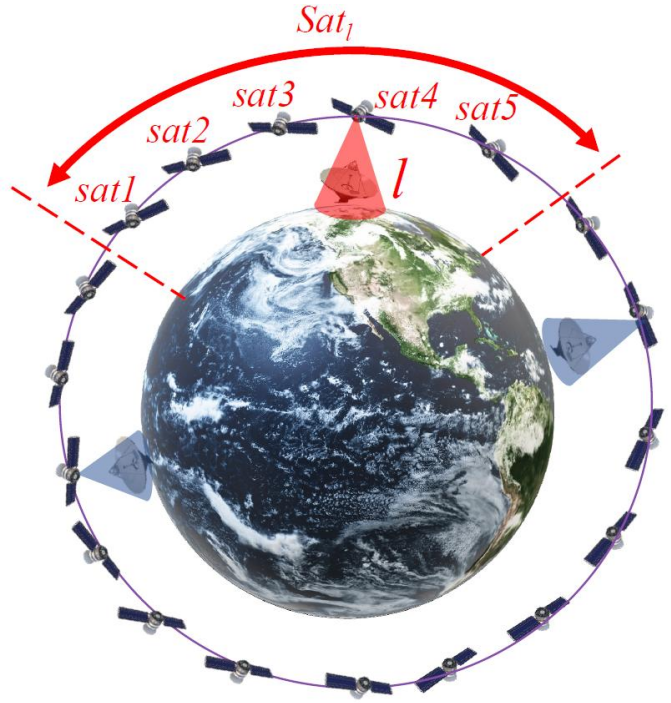
③ Infer traffic routes and link throughputs.

④ Analyze the congestion states of user legal traffic.

Worst scenario: the compromised UTs **being positioned near the bottleneck links.**

➢ **Variability analysis**: the number of compromised UTs, the UTs' regions, and so on.

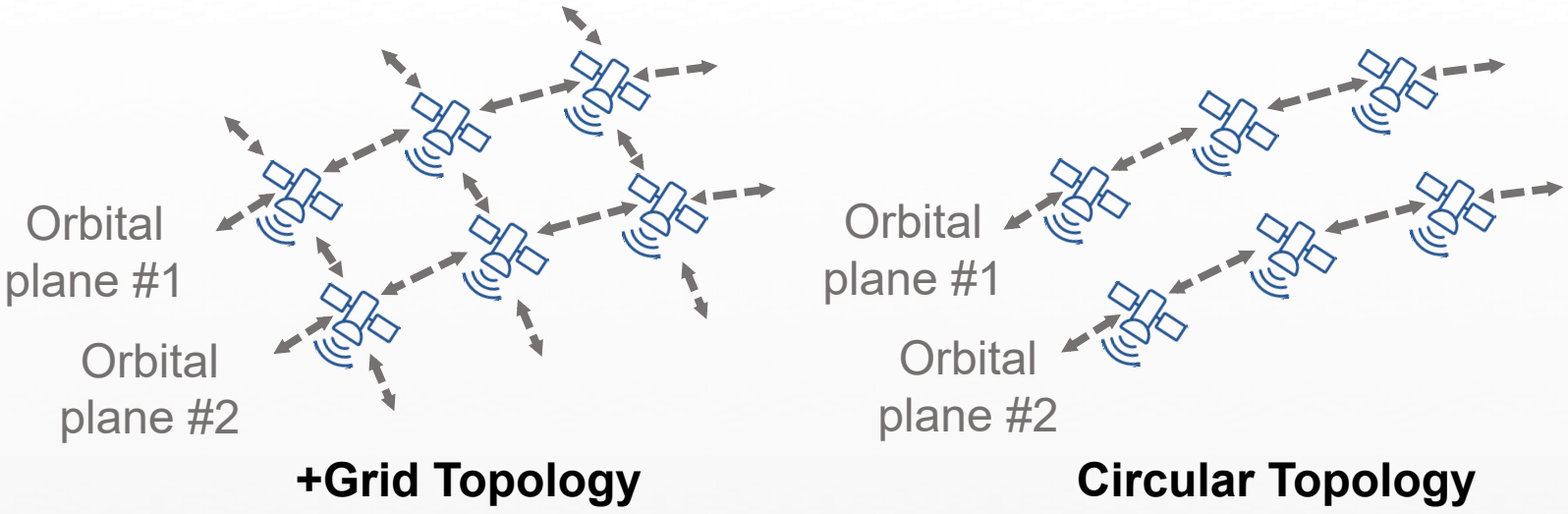




Traffic from Sat_l all routes to the nearest GSL l

Experiment setup

- Constellation and GS configurations: Starlink phase I, shell I (72*22) & Kuiper (34*34), global GS deployment[1][2].
- Topology Setting: +Grid Topology[3] and Circular Topology.



[1] Federal Communications Commission. Spacex gen2 non-geostationary satellite system. attachment a. technical information to supplement schedule s. https://fcc.report/IBFS/SAT-LOA-20200526-00055/2378671, 2020.
[2] Starlink Services. PETITION OF STARLINK SERVICES, LLC FOR DESIGNATION AS AN ELIGIBLE TELECOMMUNICATIONS CARRIER. https://www.mass.gov/doc/dtc-21-1-starlink-final-order/download, 2021.
[3] Simon Kassing, Debopam Bhattacherjee, Andre´ Baptista A´ guas, Jens Eirik Saethre, and Ankit Singla. Exploring the "Internet from Space" with Hypatia. In Proceedings of the 20th ACM Internet Measurement Conference (IMC), page 214–229. ACM, 2020.

Experiment setup

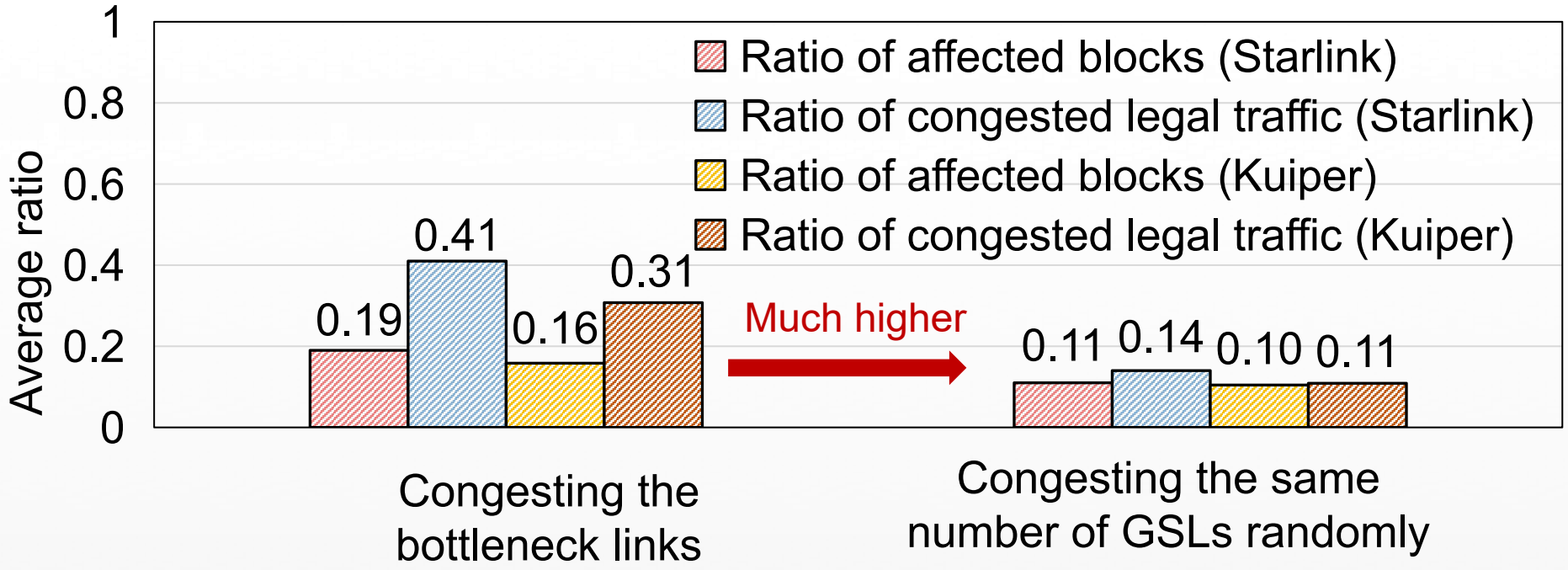
- Constellation and GS configurations: Starlink phase I, shell I (72*22) & Kuiper (34*34), global GS deployment[1][2].
- Topology Setting: +Grid Topology[3] and Circular Topology.
- User Traffic: modeling user traffic based on the real Starlink traffic distribution in more than 50 countries provided by Cloudflare[4].
- Analysis Results:
  - **Bottleneck link validation**: comparing the impact with and without being targeted.
  - **Risk analysis**: the adverse impacts on traffic volume and GSLs.
  - ..... (more in the paper)

[1] Federal Communications Commission. Spacex gen2 non-geostationary satellite system. attachment a. technical information to supplement schedule s. https://fcc.report/IBFS/SAT-LOA-20200526-00055/2378671, 2020.
[2] Starlink Services. PETITION OF STARLINK SERVICES, LLC FOR DESIGNATION AS AN ELIGIBLE TELECOMMUNICATIONS CARRIER. https://www.mass.gov/doc/dtc-21-1-starlink-final-order/download, 2021.
[3] Simon Kassing, Debopam Bhattacherjee, Andre´ Baptista A´ guas, Jens Eirik Saethre, and Ankit Singla. Exploring the "Internet from Space" with Hypatia. In Proceedings of the 20th ACM Internet Measurement Conference (IMC), page 214–229. ACM, 2020.
[4] Starlink traffic data. Accessed on: September 9, 2024, https://radar.cloudflare.com/as14593?dateRange=52w.

Bottleneck link validation

Tsinghua University

- Comparison with congesting the same number of GSLs randomly. (The affected blocks refer to those whose legal traffic will be congested.)

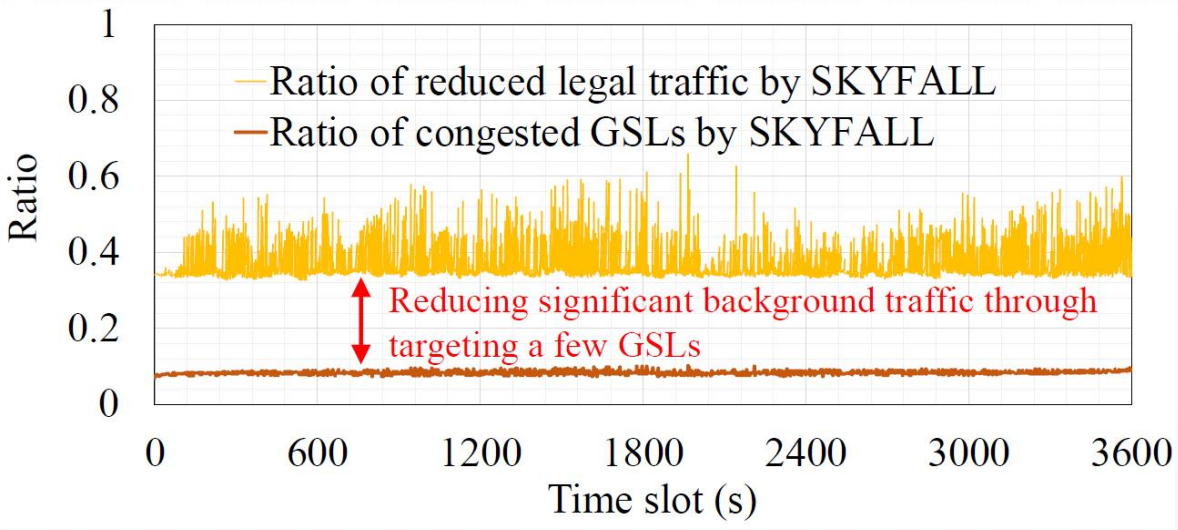


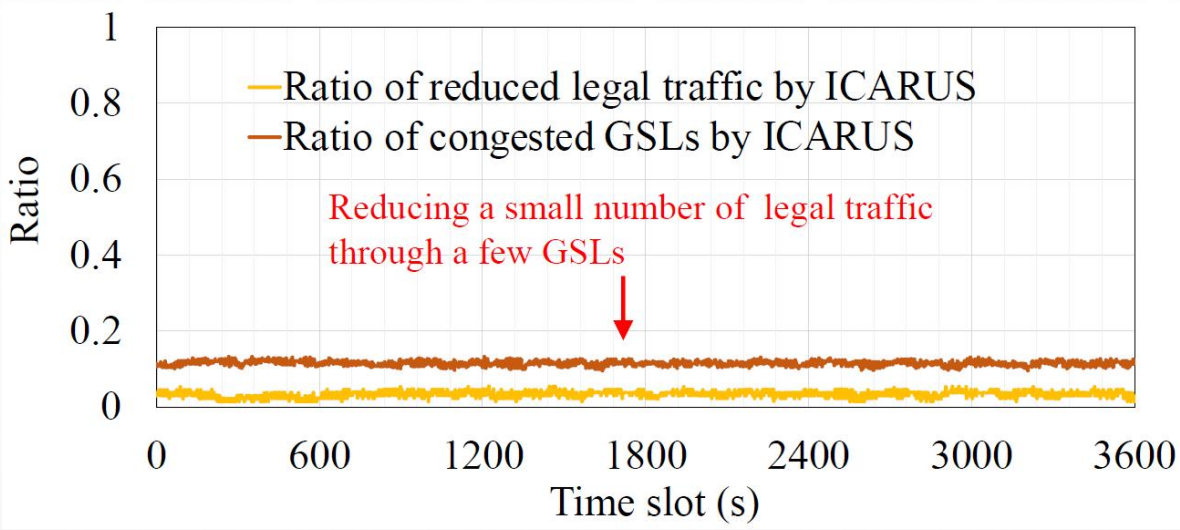
Bottleneck links yield more substantial adverse impacts and more effective choices for potential attackers.

Risk analysis

Tsinghua University

- Comparison with ICARUS[1]
  - Both are given the same number of compromised UTs for flooding.
  - SKYFALL: UTs are positioned intentionally near the bottleneck links.
  - ICARUS: UTs are positioned in proportion to the traffic distribution of Starlink.





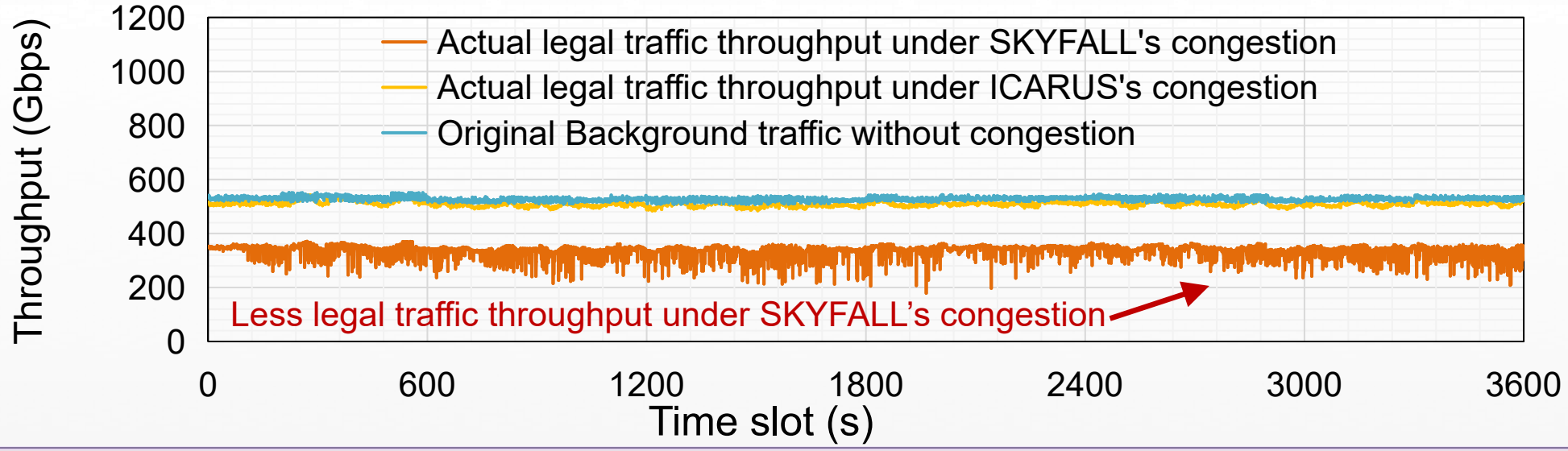
The traffic volume reduced under SKYFALL's scenario is 3.4 × that reduced by ICARUS.

[1] Giacomo Giuliari, Tommaso Ciussani, Adrian Perrig, and Ankit Singla. ICARUS: Attacking Low Earth Orbit Satellite Networks. In USENIX Annual Technical Conference (ATC), pages 317–331. USENIX, 2021.

Risk analysis

Tsinghua University

- Comparison with ICARUS
  - Both are given the same number of compromised UTs for flooding.
  - SKYFALL: UTs are positioned intentionally near the bottleneck links.
  - ICARUS: UTs are positioned in proportion to the traffic distribution of Starlink.



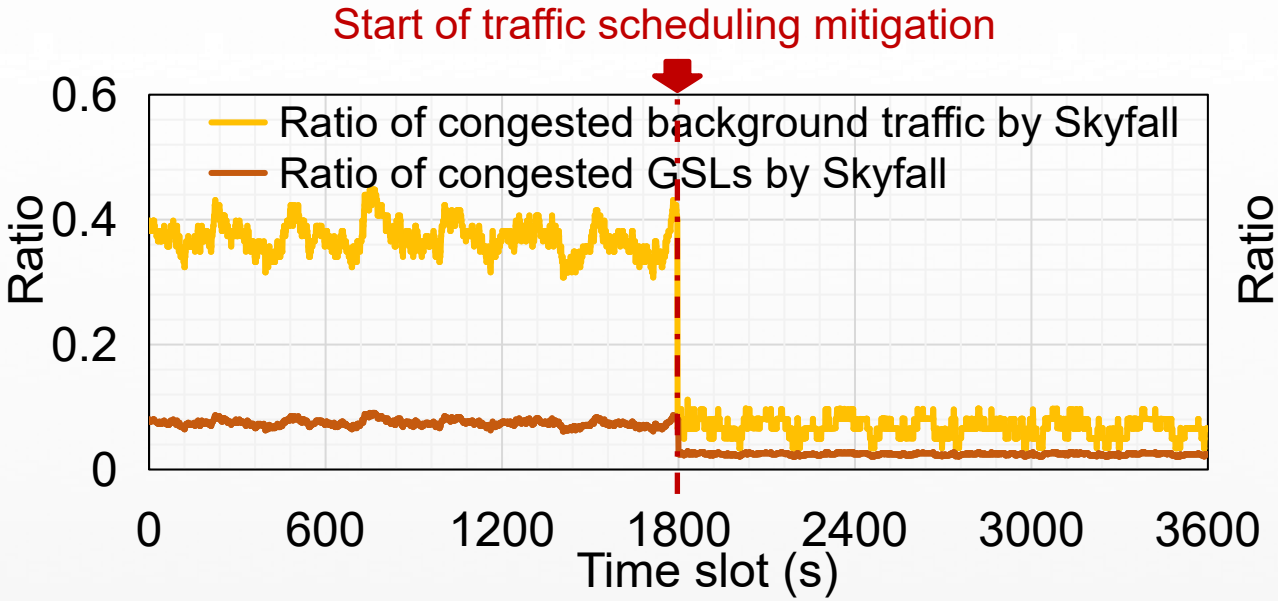
A small number of congested GSLs brings a long-term reduced throughput impact on the legal traffic.

Possible countermeasures

清華大學 Tsinghua University

❑ Customized Traffic Scheduling

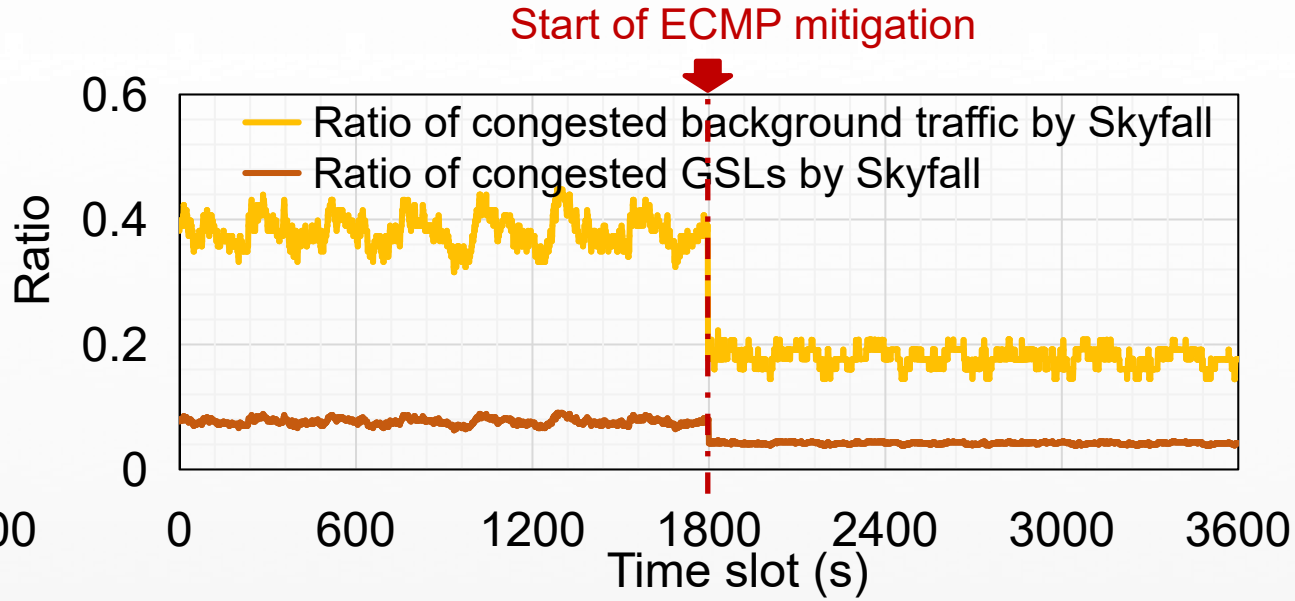
- ➢ A controller monitors GSL traffic.
- ➢ Satellites redirect surplus traffic to the closest satellite with an available GSL for relays.



- ***The ratio of congested background traffic and congested GSLs drop to one-fourth.*** ✓
- ***High computational expenses.*** ✗
- ***Not timely for dynamic GSL handovers.*** ✗

❑ Equal Cost Multiple Path

- ➢ Equal partitioning of traffic over multiple ISL paths.



- ***Approximately half of the congested traffic and GSLs are recovered.*** ✓
- ***Not practical for each data stream.*** ✗

Conclusion

- Definition of bottleneck links in LSNs
  - The **uneven distributions** and **time-varying characteristics**.
  - The **quantified results** in a case study with public information of real mega-constellations and GSes in use.
- We propose an analyzer SKYFALL
  - A mechanism to **analyze the impact** when compromise UTs are provided to exploit the time-varying bottleneck links.
  - Stages cover the **data gathering process** and **analysis process**.
- Comprehensive risk analysis results illustrate the validation of bottleneck links and the effect of utilizing the UTs, by **targeting the bottleneck links in certain regions**.
- Discussion about the countermeasures
  - The shortcomings of traditional.
  - Possible solutions are proposed to mitigate the potential risks.

NDSS

Thank You!

Time-varying Bottleneck Links in LEO Satellite Networks: Identification, Exploits, and Countermeasures

Yangtao Deng, Qian Wu, Zeqi Lai, Chenwei Gu,
Hewu Li, Yuanjie Li, Jun Liu

清華大學
Tsinghua University