Poster: Secure and Scalable Rerouting in LEO Satellite Networks

Lyubomir Yanev
ETH Zurich
lyanev@ethz.ch

Pietro Ronchetti
ETH Zurich
pietroro@ethz.ch

Joshua Smailes
University of Oxford
joshua.smailes@cs.ox.ac.uk

Martin Strohmeier
armasuisse Science + Technology
martin.strohmeier@armasuisse.ch

Abstract—**Resilient routing in large-scale Low Earth Orbit (LEO) satellite networks remains a key challenge due to frequent and unpredictable link and node failures, potentially in response to cybersecurity breaches. While prior work has explored rerouting strategies with various levels of network awareness, their relative tradeoffs under dynamic failure conditions remain underexplored.**

In this work, we extend the Deep Space Network Simulator (DSNS) to systematically compare three rerouting paradigms, each differing in the scope of failure knowledge available to each node. We compare local *neighbor-based*, *segment-based* and *global-knowledge-based* rerouting as well as a naive *source routing* solution that is unaware of failures.

Our main goal is to evaluate how the breadth of failure awareness impacts routing performance and resilience under failures, both random and targeted. We measure delivery ratio, latency, rerouting overhead, and loop occurrence. Our findings show the potential of *segment-based rerouting* to achieve a favorable tradeoff between local responsiveness and global coordination, offering resilience benefits with minimal overhead—insights that can inform future fault-tolerant satellite network design.

I. Introduction

The rapid expansion of Low Earth Orbit (LEO) satellite constellations has revitalized interest in large-scale, space-based networking. These networks offer global coverage and low-latency communication, but also face frequent and unpredictable link/node failures, including targeted disruptions by an adversary [1]–[3]. In such dynamic environments, even small disruptions can break precomputed paths and cause significant degradation in delivery performance.

Prior satellite routing work often assumes relatively stable topologies and relies on periodic updates or fast reroute mechanisms typically tuned for limited failure cases (e.g., single-link failures) [4], [5]. However, when failures are widespread and unpredictable, maintaining precomputed backup paths becomes inefficient, while disseminating control signaling globally introduces substantial overhead and data loss [6]. This motivates rerouting approaches that increase failure awareness without requiring global state.

Workshop on Security of Space and Satellite Systems (SpaceSec) 2026
23 February 2026, San Diego, CA, USA
ISBN 978-1-970672-02-2
https://dx.doi.org/10.14722/spacesec.2026.23075
www.ndss-symposium.org

Thus, we present a fresh take on *segment-based rerouting* in satellite networks, which avoids reliance on the underlying network topology when making routing decisions and provides improved failure awareness. We compare it with localized *neighbor-based rerouting*, pure *source routing*, and a globally optimal failure-awareness baseline. To isolate the effect of failure-awareness scope, we use a uniform routing design: no routing tables, no precomputed paths, and no global state dissemination. Decisions are made on-demand, using available failure knowledge at forwarding time.

We extend the Deep Space Network Simulator (DSNS) [7] by implementing these rerouting paradigms and evaluate them under baseline conditions and dynamic fault scenarios, including randomized multi-link disruptions and targeted attacks on structurally important nodes.

Our contributions are as follows:

- We extend DSNS to implement four routing paradigms: *source routing*, *neighbor-based rerouting*, *segment-based rerouting*, and *global-knowledge-based rerouting*.
- We conduct a systematic simulation-based evaluation across large-scale constellations under random and targeted failures, highlighting the tradeoffs between resilience and overhead.
- We identify security-relevant tradeoffs between failure-awareness scope, delivery performance, and signaling overhead, showing *segment-based rerouting* as a scalable compromise.

II. System Model

A. Modeling Assumptions

We build on DSNS, which uses store-and-forward lookahead routing for delay-tolerant space networking. Our setup makes three core assumptions:

1) **Predictable topology, real-time failures:** Nodes use predictable contact opportunities (e.g., scheduled contact windows) via lookahead routing, and ground stations can precompute low-delay paths from these schedules. Failure information, however, is acquired in real time according to the failure-awareness strategy and is not predicted in advance.
2) **Multi-orbital LEO with ISLs and opportunistic ground access:** We simulate multi-orbital constellations with multiple planes and inter-satellite links (ISLs) defined by visibility and an elevation threshold. Ground

stations connect opportunistically based on geographic position and satellite visibility.

3) **On-demand rerouting, optimal within scope:** Routing is on-demand: if a failure is detected on the message path, the node recomputes a path using the maximum topology view available under its awareness scope (local neighborhood, segment, or global). Otherwise, it forwards along the precomputed path. Paths are optimal given the node's available failure knowledge.

We do not assume geometric regularity or orbital symmetry; the goal is to recover from multi-link failures as long as the network remains connected.

B. Traffic Model

We generate messages between randomly selected ground-station pairs, representing typical control-plane tasks (e.g., certificate synchronization, key updates, routing metadata). Traffic is generated in periodic bursts, and message deliveries are independent. Messages are routed exclusively through the ISL (space) network.

C. Failure Model and Attack Scenarios

We consider two classes of failures:

1) **Random failures:** Links are continuously removed and restored via events such that, on average, a fixed fraction of links is down at all times. Each failed link remains down for a specified downtime before recovering.
2) **Targeted failures:** Selected nodes or links are disabled either permanently or for a specified downtime; in our case, we target segment-based rerouting by disabling structurally important border satellites.

We assume border satellites are immune to random failures and are only affected by targeted attacks. This isolates inter-segment behavior, since no redundancy or failover is currently employed at the border-router level.

III. Experiment Design

We conduct simulations using three constellations: an Iridium constellation with 66 satellites, a Starlink constellation with 1584 satellites, and a LEO/LEO constellation with 2 layers and 1650 satellites in total.

In segment-based rerouting, each constellation is partitioned into 3 segments. Each configuration has 256 ground stations, and their placement remains fixed across simulations. Message traffic is generated periodically in short bursts.

A. Random Failures

In the random failure model, failures are injected continuously throughout the simulation such that a fixed fraction (0%, 15%, or 30%) of links are kept failed at all times, each link being kept down for 60 seconds before recovering. Thus, we ensure links fail whilst messages are in transit, underlining our focus on dynamic failure recovery. The simulations run for 7200 seconds for Iridium and 1800 seconds for Starlink and LEO/LEO.

B. Targeted Failures

In the targeted failure model, we use the segment-based rerouting and disable all border satellites for a specified amount of time. We then observe the effects this has on throughput and message drops. We run simulations on the Iridium, Starlink and LEO/LEO constellations for a duration of 1200 seconds, with a message being sent every second. The satellite network is partitioned into 3 segments. All border satellites are disabled at 450 seconds for a duration of 300 seconds, after which they become operational again.

IV. Conclusion

In this work, we investigated how the scope of failure-awareness influences routing resilience in LEO satellite networks, particularly under adversarial and fault-prone conditions. By implementing and evaluating four scoped rerouting strategies in the Deep Space Network Simulator, we showed that broader awareness enables more reliable message delivery and stronger loop avoidance, even amid targeted disruptions. Segment-based rerouting may provide a robust, scalable compromise, offering improved security posture without the prohibitive overhead of global state. These results highlight the importance of designing satellite routing protocols with security-resilient primitives that respond adaptively to both random failures and intentional attacks.

References

[1] Z. Zhang, K. Zhao, W. Li, and Y. Fang, "Fast recovery from multiple link failures in leo satellite networks," in *2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE, 2023, pp. 1–6.

[2] J. Willbold, M. Schloegel, M. Vögele, M. Gerhardt, T. Holz, and A. Abbasi, "Space odyssey: An experimental software security analysis of satellites," in *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2023, pp. 1–19.

[3] J. Pavur and I. Martinovic, "The cyber-asat: on the impact of cyber weapons in outer space," in *2019 11th International Conference on Cyber Conflict (CyCon)*, vol. 900. IEEE, 2019, pp. 1–18.

[4] M. Shand and S. Bryant, "Ip fast reroute framework," Tech. Rep., 2010.

[5] A. Atlas and A. Zinin, "Basic specification for ip fast reroute: Loop-free alternates," Tech. Rep., 2008.

[6] J. Jin, F. Tian, Z. Yang, H. Di, and G. Li, "A disruption tolerant distributed routing algorithm in leo satellite networks," *Applied Sciences*, vol. 12, no. 8, p. 3802, 2022.

[7] J. Smailes, F. Futera, S. Köhler, S. Birnbach, M. Strohmeier, and I. Martinovic, "Dsns: The deep space network simulator," in *Proceedings of the 2025 Security for Space Systems (3S) Conference*. European Space Agency, 2025. [Online]. Available: https://security4space.esa.int/2025/papers/40/

Secure and Scalable Rerouting in LEO Satellite Networks

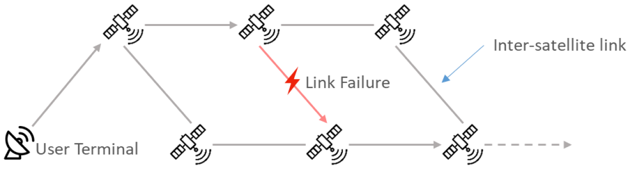
ETH zürich

Networked Systems
ETH Zürich — seit 2015

Lyubomir Yanev, Pietro Ronchetti, Joshua Smailes, Martin Strohmeier

Motivation

- Large-scale LEO constellations are increasingly popular and promise **global connectivity and low-latency communication** for internet access, mobile services, and critical applications.
- **They're highly dynamic** and can face frequent, unpredictable link failures



- Although various rerouting strategies exist, **the impact of the failure-awareness scope** on resilience, performance, and overhead remains underexplored.

Four Routing Paradigms

- **Pure source routing**: no knowledge at all
- **Neighbor-based**: only local knowledge
- **Segment-based**: regional knowledge
- **Global**: full knowledge (benchmark)

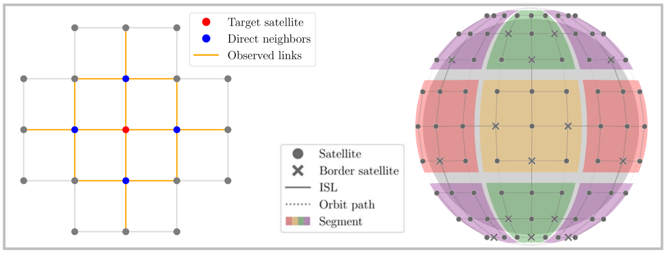


Figure 1: Failure awareness in neighbor- and segment-based routing

Routing Paradigm	Source	Neighbor	Segment	Global
Knowledge extent	☆☆☆☆	★☆☆☆	★★★☆	★★★★
Signaling Overhead	★★★★	★★★☆	★★☆☆	☆☆☆☆

Table 1: Knowledge extent vs. signaling overhead of each paradigm (more ★ = better)

Failure Handling

Limited awareness leads to frequent detours in neighbor-based routing.

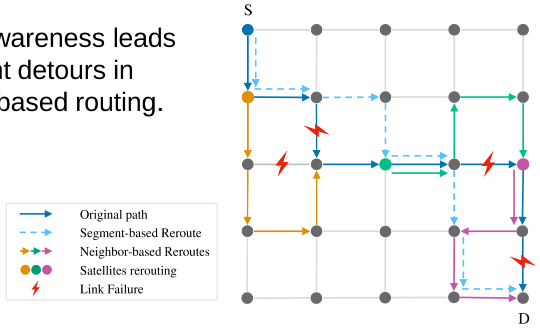


Figure 2: Handling of link failures in neighbor- and segment-based routing. Satellites S and D in the same segment.

Setup

We use the **Deep Space Network Simulator (DSNS)**[1] to simulate the Starlink and Iridium constellations

- **Uniform, on-demand routing design**:
  – no routing tables; routers use available knowledge
- We evaluated all paradigms under random failures
- We measured delivery success, latency, loops, and signaling overhead

Results

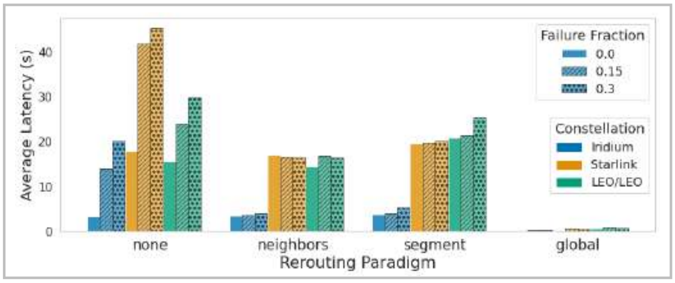


Figure 3: Average latency of messages across paradigms

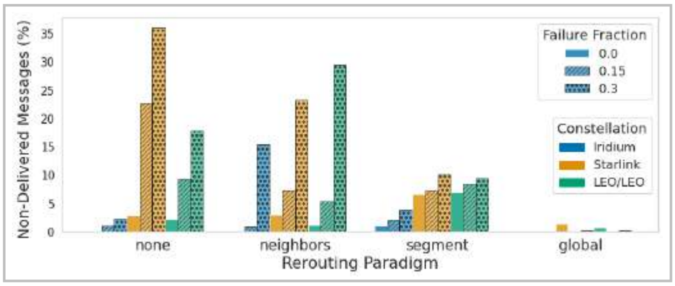


Figure 4: Fraction of non-delivered messages across paradigms

Paradigm	Observed Result
Source	Collapses under sustained failures
Neighbor	Degrades rapidly as failures increase and suffers from routing loops
Segment	Significantly improves delivery under higher failure rates
Global	Performs best, but is unrealistic

Conclusion

- Segment-based rerouting offers the best practical tradeoff between resilience and performance, but there is no one-size-fits-all solution.
- **Limitations**: targeted-failure evaluation currently implemented only for segment routing.
- **Future work:** additional paradigms (including security protocols) and broader constellation support.

[1] Smailes et al., *DSNS: The Deep Space Network Simulator*, 3S 2025.