Resiliency in Low Earth Orbit Satellite Routing

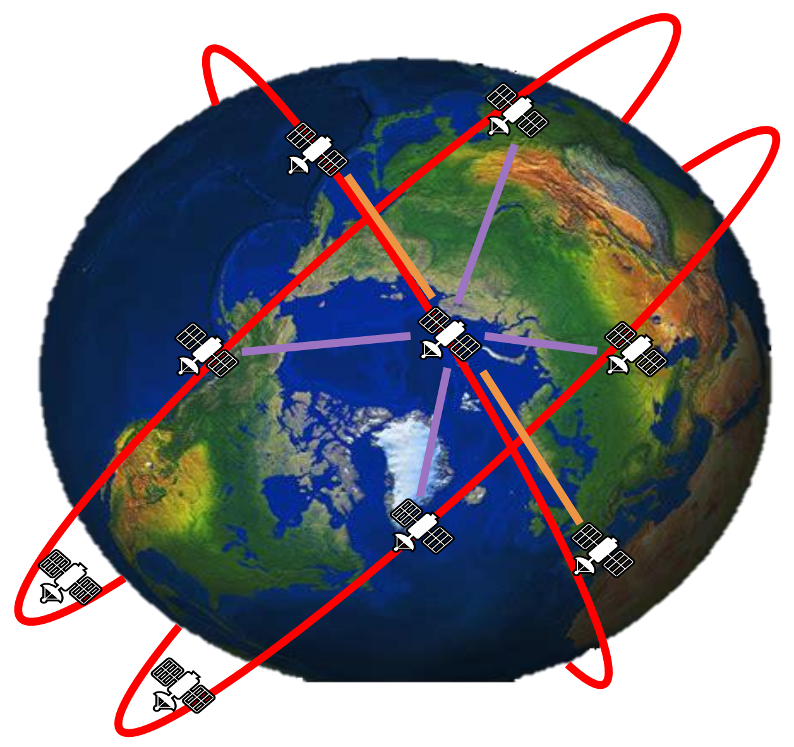
Mission-Critical Computing
NSF CENTER FOR SPACE, HIGH-PERFORMANCE, AND RESILIENT COMPUTING (SHREC)

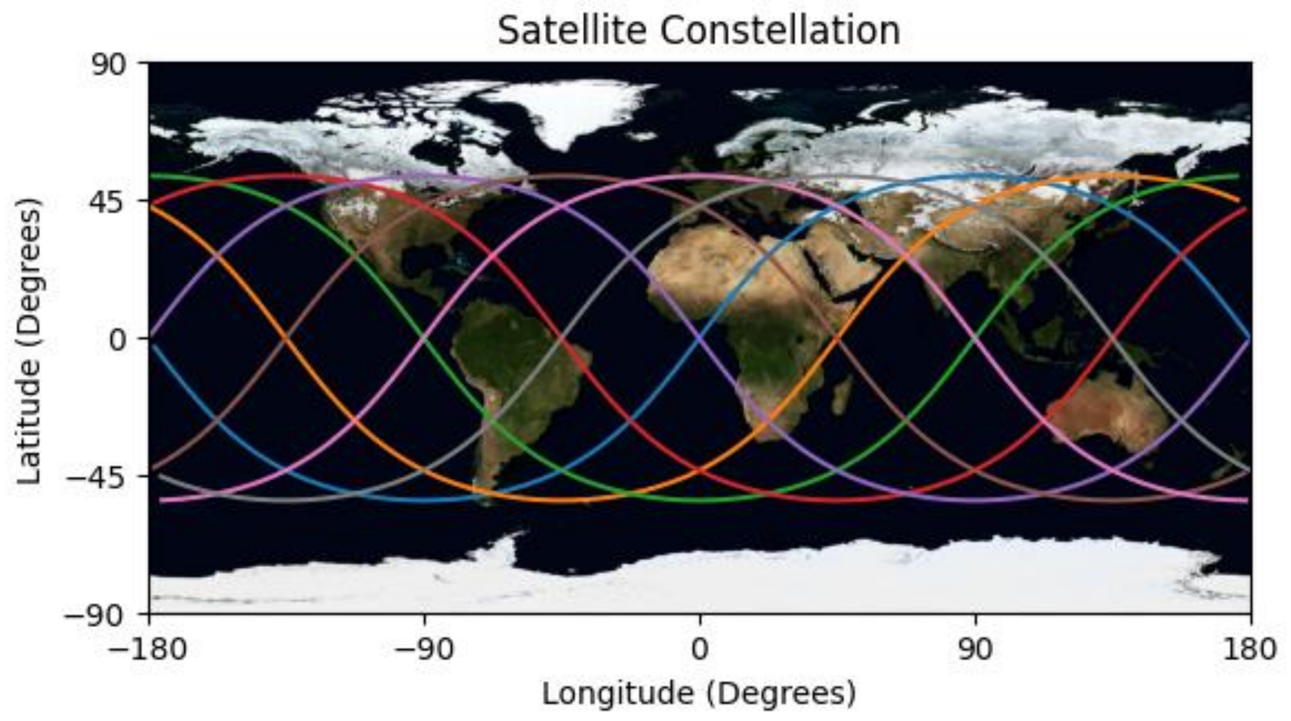
Robert Esswein, Sean O'Melia, Dr. Richard Skowyra,
Dr. Mai Abdelhakim, Dr. Robert Cunningham

University of Pittsburgh

Satellite Constellations

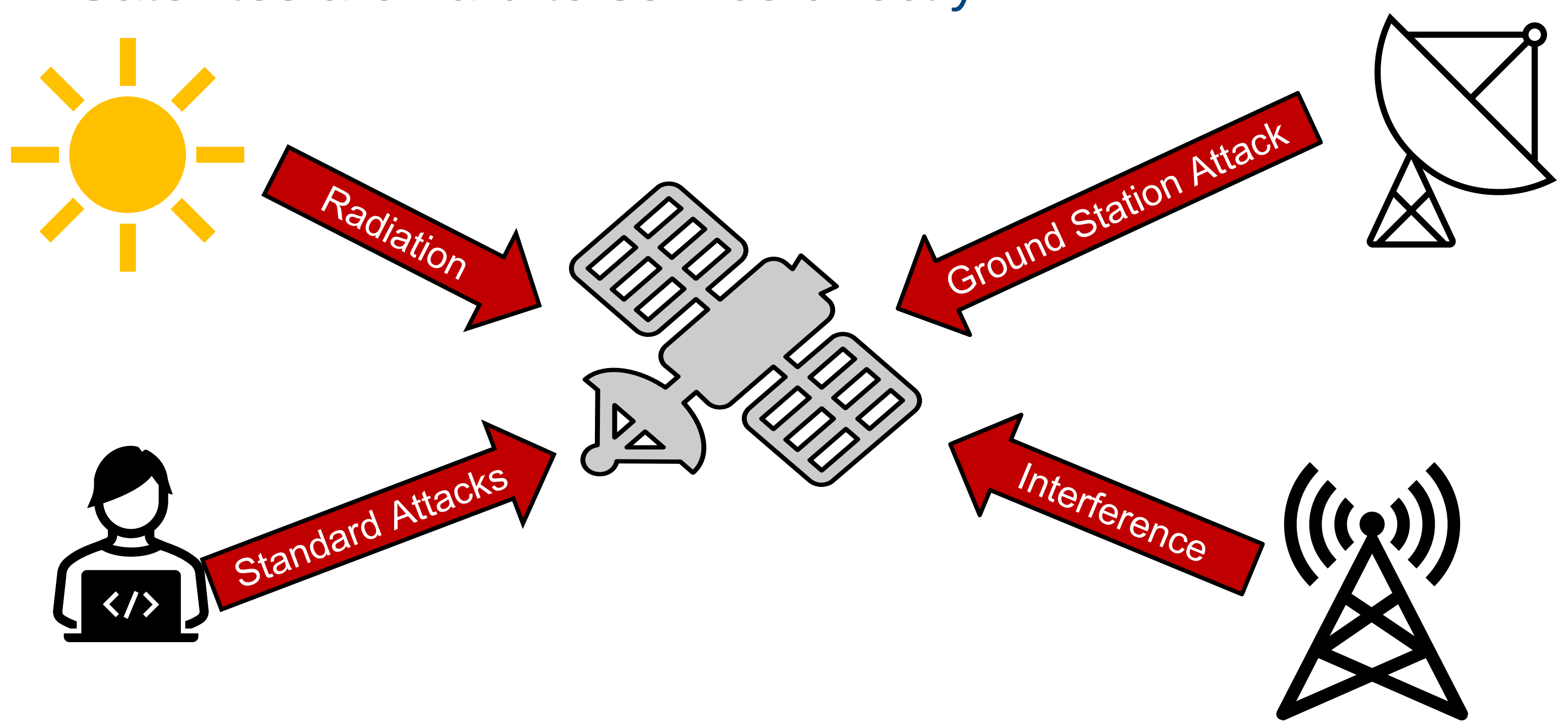
- LEO constellations are of growing interest and used for essential services, necessitating security
- Applications include earth observation, communication, and computation, all of which require coordination
- Commercial satellite constellations, such as Starlink and OneWeb, have hundreds of satellites
- How do we ensure availability and security of the constellation?





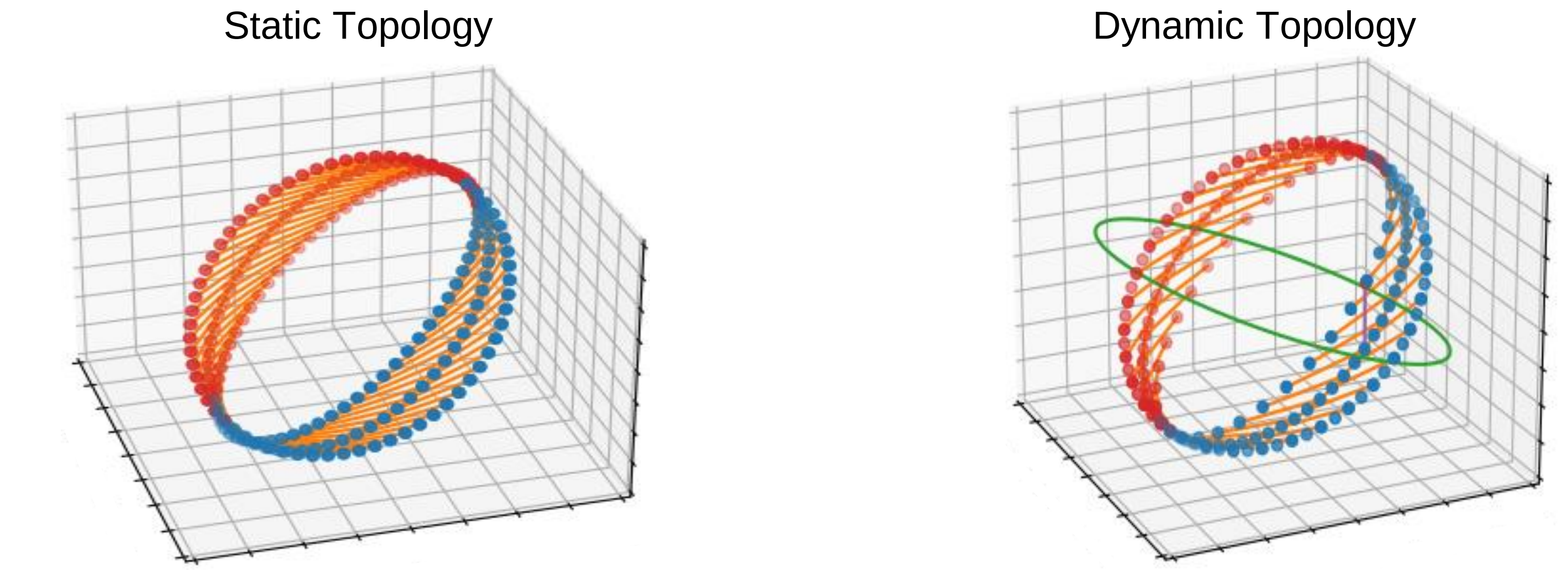
Satellite Failures and Attacks

- Solar radiation can cause memory errors
- Satellites are also vulnerable to attacks
  - Commodity components have known problems
  - Communication mediums can be attacked (e.g., interference, interception)
  - Ground stations can be physically attacked
- Satellites are hard to service directly



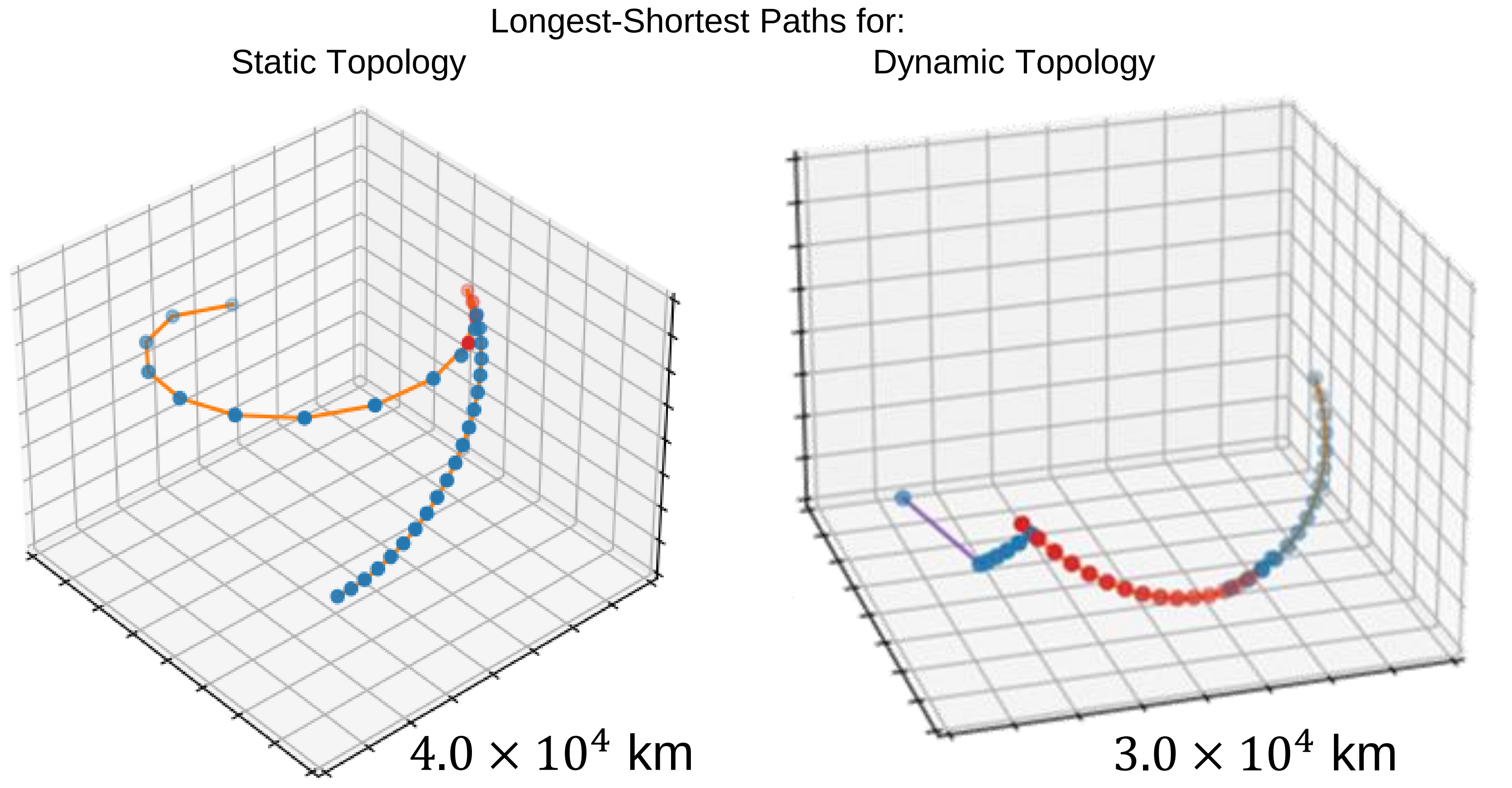
Constellation Topology

- LEO constellations have P orbital planes, with S satellites in each
- Each satellite has four laser transceivers
- At any given point, satellites could connect to many nearby satellites, some of which are in an intersecting orbital plane
- Static topology: satellites connect to their neighbors within their orbital plane and in neighboring orbital planes (constant neighbors throughout the entire orbital period)
- Dynamic topology: same as static except one ephemeral connection to a satellite in an intersecting orbital plane



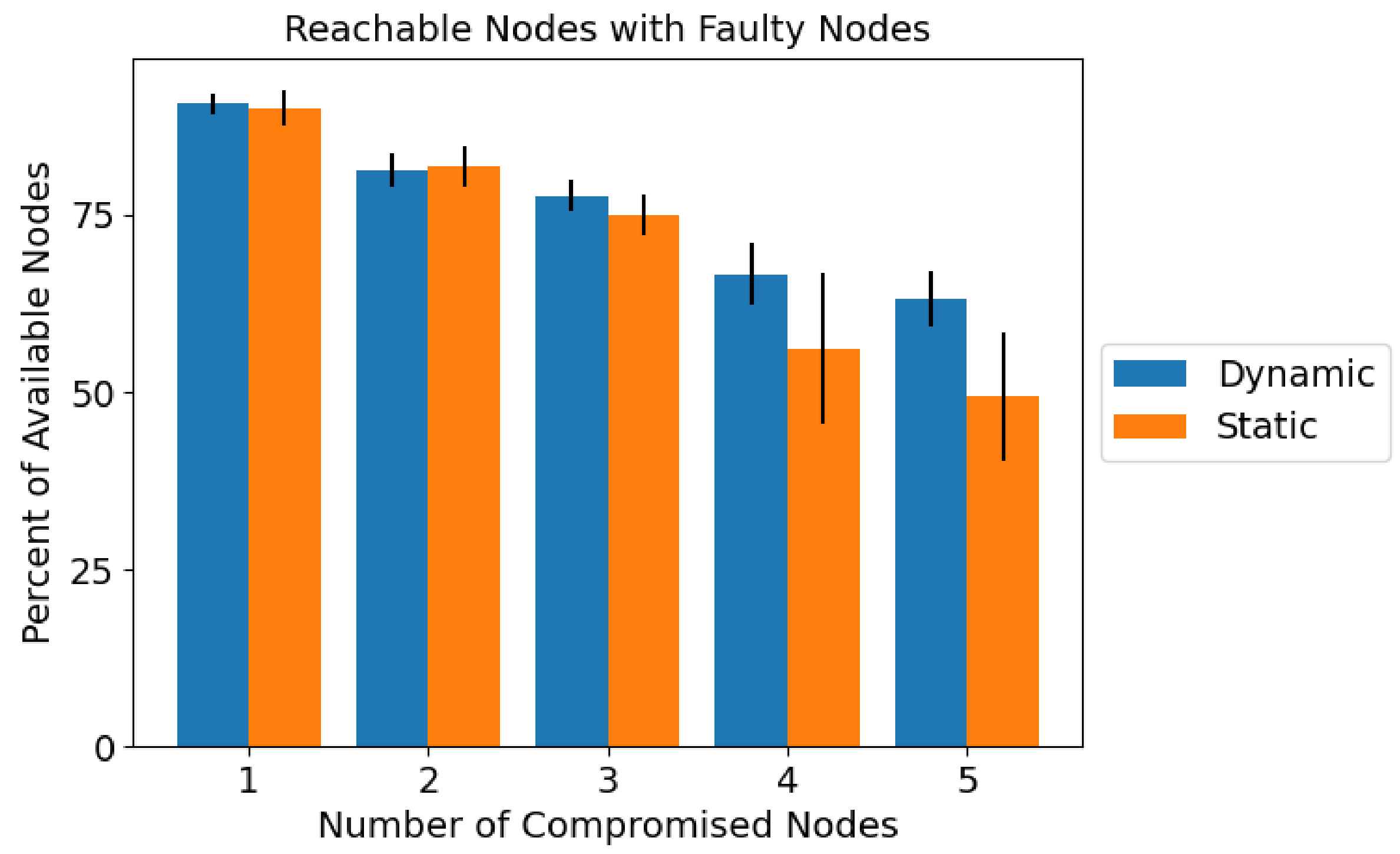
Constellation Routing

- Shortest-path routing algorithms are susceptible to single points of failure significantly degrading availability
- Walker-Delta satellite constellations have many redundant paths between any two nodes that can be leveraged



Simulated Effects of Attack

- Goal: Assess impact of routing attacks on a satellite constellation for both static and dynamic topologies
- Experiment: From a single source, send packets to all destinations in the presence of compromised nodes
  - Parameters: P=12, S=8, # compromised nodes=[1,2,3,4,5]
- Measure the average number of nodes that can be reached in the presence of individual faulty satellites



Conclusions and Future Work

- Preliminary results show the need for routing algorithms that address individual satellite failures
- As the number of faulty nodes increases, the dynamic topology exhibits less availability degradation than the static topology
- Future work
  - Develop a trust-based routing algorithm for constellations
  - Assess how the new protocol improves the constellation's ability to recover from compromised nodes

References & Acknowledgements

1. T. Pan, T. Huang, X. Li, et al. "OPSPF: orbit prediction shortest path first routing for resilient LEO satellite networks," IEEE International Conference on Communications (ICC), 2019, pp. 1–6.
2. H. Li, D. Shi, W. Wang, et al. "Secure routing for LEO satellite network survivability," Computer Networks 211 (2022), p. 109011.
3. G. Stock, J. Fraire, H. Hermanns. "Distributed On-Demand Routing for LEO Mega-Constellations: A Starlink Case Study," IEEE Advanced Satellite Multimedia Systems Conference and Signal Processing for Space Communications Workshop (ASMS/SPSC), 2022, pp. 1–8.
4. M. Albulet. "Spacex non-geostationary satellite system: Attachment a technical information to supplement schedules," US Fed. Commun. Comm., Washington, DC, USA, Rep. SAT-OA-20161115-00118 (2016).
5. J. Walker. "Satellite constellations," Journal of the British Interplanetary Society 37, 1984, p. 559.
6. A. Chaudhry, H. Yanikomeroglu, "Laser intersatellite links in a starlink constellation: A classification and analysis," IEEE Vehicular Technology Magazine 16.2, 2021, pp. 48–56.

This research was supported by the NSF Center for Space, High-performance, and Resilient Computing (SHREC) industry and agency members and by the IUCRC Program of the National Science Foundation under Grant No. CNS-1738783.