Poster: Resiliency in Low Earth Orbit Satellite Routing

Robert Esswein
University of Pittsburgh
Pittsburgh, PA USA
robert.esswein@pitt.edu

Sean O'Melia, Richard Skowyra
MIT Lincoln Laboratory
Lexington, MA USA
{sean.omelia, richard.skowyra}@ll.mit.edu

Mai Abdelhakim, Robert Cunningham
University of Pittsburgh
Pittsburgh, PA USA
{maia, robertkcunningham}@pitt.edu

I. Introduction

As satellite constellations become more widely adopted for observation, navigation, and communication applications, resiliency measures must be in place to ensure these constellations and the applications they support are not compromised. This adoption of satellite constellations for numerous applications coincides with the trend of constellations moving out of Geosynchronous Orbit (GEO) to Low Earth Orbit (LEO). LEO satellites have advantages: launching to orbit is less expensive, less complicated, inexpensive components can be used, and communication latency is lower. LEO satellites also have drawbacks: they do not fly above a consistent point on earth's surface and they often times leverage commodity hardware and software, potentially opening the satellites to unanticipated vulnerabilities. So, LEO constellations spanning multiple orbital planes necessarily forms a changing topology.

Our goal is to improve the resiliency of satellite routing when some nodes are compromised. For our first step towards this goal, we created a testbed in Mininet [1] to simulate a satellite network in a Walker-Delta constellation. We then use this testbed to assess the impact of a satellite network where some nodes fail to forward packets, either due to an attack or to environmental conditions such as radiation. Our results will be used to guide future work to improve satellite communication security.

II. Faults of and Attacks on Satellite Networks

Single-event upsets (SEUs) can occur in LEO satellites when radiation with sufficient energy impinges on memory. SEUs can cause arbitrary modification to packet data, causing them to be dropped when checked for integrity [2]. In addition, these radiation events could cause any number of operating system level failures, resulting in system crashes or lockups.

Supply-chain attacks [3], where a malicious vendor provides vulnerable computer chips or code for the satellite systems, can cause similar system failures. Attackers could cause any number of different system failures, including modifying data, dropping data, and even taking over the entire satellite. While these attacks can be malicious, they can also be a byproduct of a supplier trying to cut costs by swapping a more expensive and reliable part with a cheaper replica. In our threat model, the adversary may modify the hardware and/or the software of a single or a few satellites, resulting in dropped data.

III. Satellite Network Model

We model our constellation as a Walker-Delta constellation [4], of which Starlink [5] is a recent commercial adaptation. In our model, each satellite has four laser transceivers to connect with nearby satellites. We assume that satellites have perfectly circular orbits, with no deviation from their ideal locations.We provide analysis for two different satellite network topologies: static and dynamic. In the static topology, each satellite maintains four permanent links, two to the nearest neighbors within its orbital plane and two to the satellites in the same phase of the adjacent orbital planes. This topology is consistent with existing work [6].

We also define the dynamic topology, where each satellite maintains three permanent links and use their forth link temporarily connect with passing satellites. The first two permanent links connect a satellite to each of its neighbors within its orbital plane. The third permanent link connects to a satellite in a neighboring orbital plane, with each satellite within an orbital plane alternating the direction of this link between east and west. These permanent links are used to ensure that the network remains connected. Each satellites' fourth link is used to form temporary links with passing satellites.

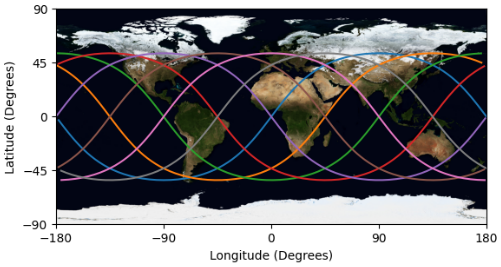

Fig. 1. The orbits of satellites on a projection of the earth, showing how two satellites might pass each other despite several orbital planes apart.

During the orbit of satellites in a Walker-Delta constellation, satellites travel both northeast and southeast. Satellites that are travelling in different directions near the same point would be very far away from each other in the static topology. For example, in Fig. 1, the green and pink orbital planes intersect twice, but a satellite in the green orbital plane would need to send a packet around the world in order to reach a satellite in the pink orbital plane when both satellites are near this intersection. By allowing satellites to create temporary links as in the dynamic topology, these two satellites could directly connect to each other, significantly reducing the distance a packet must travel. By keeping the three permanent links, the constellation remains connected.

IV. Constellation Routing

Routing within a satellite constellation has several challenges. Because the topology changes are predictable, many existing routing algorithms waste bandwidth and computation responding to these changes, resulting in poor network performance. However, the location and connectivity of the network is predictable as long as all nodes are behaving as designed.

Several routing protocols have been proposed for satellite constellations. Orbit Prediction Shortest Path First (OPSPF) [7] is a routing algorithm based on the Open Shortest Path First algorithm, but modified to handle changing satellite topology. SLT [6] is an algorithm based on OPSPF which removes untrusted nodes before calculating routes. DisCoRoute [8] is a another routing algorithm based on knowledge of the locations of satellites. DisCoRoute selects the path where inter-orbital plane hops are nearest to the poles, where links are shortest. This approach approximates the shortest paths while requiring significantly less computation.

V. Contribution

We evaluate how a small number of compromised nodes affects how much of the constellation can be reached. Using our testbed, we simulated a constellation with 12 orbital planes and 8 satellites per plane at a 53° inclination angle. We tested 1-5 compromised nodes in the constellation, with 3 random sets of compromised nodes per test case. To measure the availability of all satellites in the constellation, we examined both the static and dynamic topology, where we send packets to every node in the network from the same source node. Fig. 2 shows that with static routing approaches, such as OPSPF, only a small number of compromised nodes can cause a satellite to lose the ability to reach to many other satellites in the constellation. Ideally, a few compromised nodes would not block packets because the network is intrinsically redundant.

Our results show that as the number of compromised nodes increases, the dynamic topology exhibits better availability than the static topology. This is because, in the dynamic topology, each satellite is connected to more different satellites. Thus, a single compromised node might lose influence after a short period of time.

VI. Conclusion

Our preliminary results show the shortcomings of the static topology. With a small number of compromised nodes, many nodes are made unreachable. The dynamic topology allows nodes to utilize different paths more often, reducing the effects of a small number of compromised nodes.

For future work, we will develop Trust-Based Satellite Routing (TBSR), a routing protocol leveraging static routes for satellite constellations that also utilizes trust to detect malicious or compromised nodes, then route around them. The whole constellation gains resiliency because satellites will be able to adaptively route around compromised nodes after detecting their behavior. When a particular satellite is found to be compromised, new routes are calculated to avoid it, preventing a single satellite from significantly degrading network performance. Additionally, our threat model only considers satellites that drop all traffic routed through them, which will be expanded for future work.

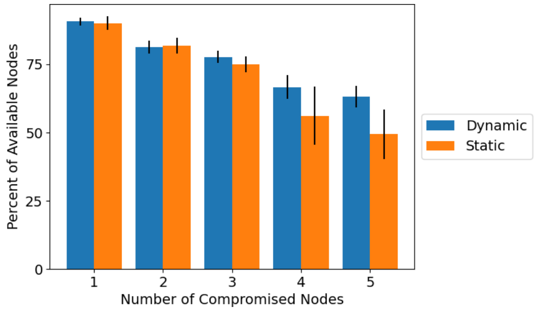

Fig. 2. The percent of reachable nodes with a small number of compromised nodes. The error bars show two standard deviations. The dynamic topology is more resilient to a small number of compromised nodes.

References

[1] Bob Lantz, Brandon Heller, and Nick McKeown. “A Network in a Laptop: Rapid Prototyping for Software-Defined Networks”. In: *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*. 2010.

[2] Craig Underwood. “In-orbit radiation effects monitoring on the UoSAT satellites”. In: *4th Annual AIAA/USU Conference on Small Satellites* (1990).

[3] Kyle W Ingols. “Design for security: Guidelines for efficient, secure small satellite computation”. In: *MTT-S International Microwave Symposium (IMS)*. IEEE. 2017, pp. 226–228.

[4] John G Walker. “Satellite constellations”. In: *Journal of the British Interplanetary Society* 37 (1984), p. 559.

[5] M Albulet. “Spacex non-geostationary satellite system: Attachment a technical information to supplement schedules”. In: *US Fed. Commun. Comm., Washington, DC, USA, Rep. SAT-OA-20161115-00118* (2016).

[6] Hui Li, Dongcong Shi, Weizheng Wang, et al. “Secure routing for LEO satellite network survivability”. In: *Computer Networks* 211 (2022), p. 109011.

[7] Tian Pan, Tao Huang, Xingchen Li, et al. “OPSPF: orbit prediction shortest path first routing for resilient LEO satellite networks”. In: *International Conference on Communications (ICC)*. IEEE. 2019, pp. 1–6.

[8] Gregory Stock, Juan A Fraire, and Holger Hermanns. “Distributed On-Demand Routing for LEO Mega-Constellations: A Starlink Case Study”. In: *ASMS/SPSC*. IEEE. 2022, pp. 1–8.