Adversarial Threats to LArge Satellite Networks (ATLAS-N)

Daniel R. Tauritz[1], Davide Guzzetti[2], Sean Harris[1], Manuel Indaco[2], Deacon Seals[1], Dhathri Somavarapu[2], Jay Patel[1]
[1]Department of Computer Science and Software Engineering, [2]Department of Aerospace Engineering

Abstract

Automated systems employing advanced AI for identifying high-fidelity, high-consequence adversarial strategies may be critical to defend satellite mega-constellations which provide omnipresence both in terms of internet connectivity and satellite imagery.

P-LEO Constellations

Proliferated Low Earth Orbit (P-LEO) constellations are systems of hundreds to thousands of low-cost satellites orbiting at low orbit altitude, e.g., 1000 km. P-LEO may be employed to grant coverage access to any location of the Earth at any time via optical or RF payloads.

Coevolutionary Algorithms

To automate the identification of high-consequence attack strategies and defenses, we employ coevolutionary algorithms to approximate the Nash equilibria of the corresponding game theoretic model. The attacker strategy is evolved to identify the highest ratio of adversarial impact to attack complexity, while the defender is evolved to identify the highest ratio of coverage to cost. Technical outcome measures include constellation engine response time (being minimized) and coevolutionary performance (maximizing attack and defense quality)

Threats to Space Assets

There exists a critical gap in understanding the vulnerabilities of a P-LEO constellation, and in general of space assets, to adversarial cyber and physical threats. In a recent article, the author labels this gap the "The Vacuum of Space Cybersecurity" [1]. The same urgency is perceived at different levels of national agencies. Cybersecurity threats to satellite assets are growing, as the cost to orchestrate an attack is dropping, while the benefits for the bad actors (whether criminals or nation-state actors) are increasing [2]. Attacks on mega-constellations can tamper with agricultural planning, natural resources management, free press, media and internet, coordination of military actions and intelligence gathering, which all critically rely on the omnipresence of the orbit satellite network.

Example of Attack's Actions

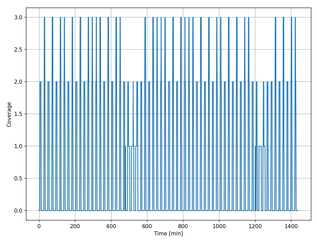
Type	Impact	Cost	Load Time	Detection Probability	Success Probability
Cyber-level 1	Reversible service interruption	low	low	low	medium
Cyber-level 2	Satellite moved to a different location	medium	medium	medium	medium
Cyber-level 3	Irreversible service interruption	medium	medium	high	medium
Physical-level 1	Limited range threats	medium	medium	high	medium
Physical-level 2	Large range threats	high	medium	high	low
Physical-level 3	Concealed large range threats	high	medium	low	low

Example of Defender's Actions

Type	Impact	Cost	Load Time	Success Probability
Cyber-level 1	Detect anomaly on satellite	medium	low	medium
Cyber-level 2	Counter a reversible service interruption	low	low	high
Cyber-level 3	Decrease success probability on all cyber attacks	high	high	high
Physical-level 1	Relocate satellite within an orbit plane	medium	low	high
Physical-level 2	Replace satellite	high	high	high
Physical-level 3	Space situational awareness: decrease attack probability of success	high	high	medium

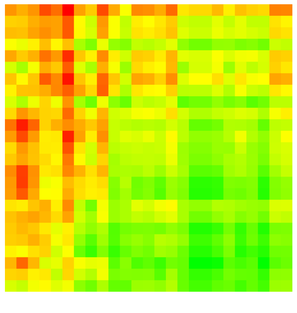
Results

Coverage Histogram



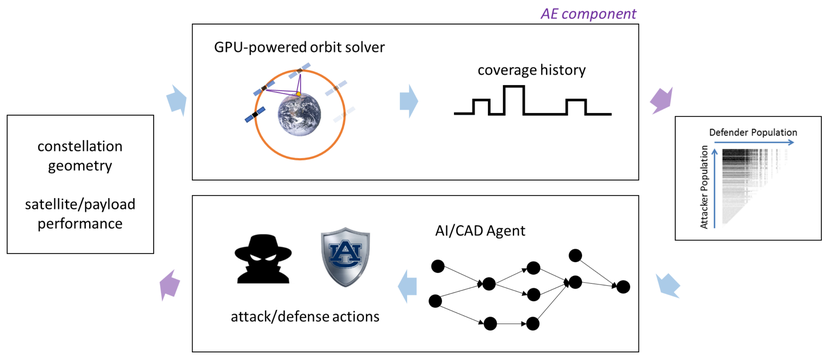
A first version of the constellation engine has been completed and preliminarily validated against commercial software by comparing figure of merits derived from a coverage histogram. The current constellation engine has been successfully integrated with different coevolution algorithms.

CIAO Plot



A CIAO (Current Individual vs. Ancestral Opponents) plot shows the coevolutionary dynamics from one experiment, indicating how progressively more evolved defender strategies (left to right) perform against progressively more evolved attacker strategies (bottom to top). Greener cells indicate that the defender agent maintained smaller coverage gaps at a lower cost. The triangular pattern indicates successful coevolution, in which both the attacker and defender populations improved over time.

Framework



The Coevolving Attack and Defense (CAD) framework for this project comprises a constellation engine and a competitive coevolutionary algorithm to approximate the Nash equilibria of the corresponding game theoretical model. The constellation engine is a computer program that takes as an input the constellation geometry, it propagates orbit mechanics for each satellite over a given time window, and returns coverage information at any given location on the Earth. Based on the outputs from the constellation engine, the attacker's and defender's fitnesses are computed. Both the defender and the attacker have to balance multiple conflicting objectives, such as impact on omnipresence and cost. As it is often not desirable to convert these into a single weighted objective a priori, a multi-objective competitive coevolutionary algorithm [3] is implemented.

References

[1] G. Falco, "The Vacuum of Space Cyber Security," in 2018 AIAA SPACE and Astronautics Forum and Exposition, 2018, p. 5275.
[2] Tucker, Patrick, "The NSA Is Running a Satellite Hacking Experiment," Nextgov.com. [Online]. Available: https://www.nextgov.com/cybersecurity/2019/09/nsa-running-satellitehacking-experiment/160057/. [Accessed: 18-Dec-2019].
[3] Coello CAC, Lamont GB, Van Veldhuizen DA (2007) Evolutionary algorithms for solving multi-objective problems, 2nd edn. Springer, New York (ISBN: 978-0-387-33254-3)

Contact Info

Dr. Daniel R. Tauritz
3101 Shelby Center
E-mail: drt0015@auburn.edu

Dr. Davide Guzzetti
328 Davis Hall
E-mail: guzzetti@auburn.edu