Proceedings of the Annual General Donald R. Keith Memorial Conference
West Point, New York, USA
May 2, 2024
A Regional Conference of the Society for Industrial and Systems Engineering

Harnessing the Speed: Simulating Hypersonic Threats against the Proliferated Warfighter Space Architecture

Ashley Arbegast, Thomas Bartholf, and Caitlin Canada

Systems Engineering Program,
Department of Mechanical Engineering,
United States Air Force Academy, Colorado 80841

Corresponding author's email: mailto:mc24ashley.arbegast@afacademy.af.edu

Author Notes: The authors would like to acknowledge Infinity Systems Engineering for providing support and subject-matter expertise throughout this research. The authors are First Class Cadets at the United States Air Force Academy who will be graduating and commissioning into the Air and Space Force. The views expressed in this paper are those of the authors and do not reflect the position of the United States Air Force Academy, the Department of the Air Force, or the Department of Defense.
.

Abstract: Driven by the necessity to adapt in the space domain and maintain dominance, the Space Development Agency (SDA) alongside other government entities and commercial organizations is developing a mesh network satellite constellation system called the Proliferated Warfighter Space Architecture (PWSA). This project utilizes model-based systems engineering (MBSE) and a physics-based simulation software, STK 12, to analyze the Proliferated Warfighter Space Architecture (PWSA) satellite constellation network under four unique simulations, including fully operational and degraded scenarios. Results show that transmission time to a ground station was 340 milliseconds in the best-case fully operational scenario. When an adversary employs directed energy weapons to obfuscate detection, the simulated time required to transmit data to a ground station increases to 978 milliseconds. This work highlights the specific vulnerabilities in hypersonic detection while creating a robust tool for path optimization and analyzing the PWSA constellation network.

Keywords: Modeling and Simulation for Defense Applications, Proliferated Warfighter Space Architecture (PWSA), Early Missile Warning, Hypersonic Missile Tracking

1. Overview

The warfighter requires a multi-directional, global, and highly integrated satellite communication network to track threats in real-time. To solve this problem, the Space Development Agency (SDA), Infinity Systems, and the capstone research team have collaborated to analyze Proliferated Warfighter Space Architecture (PWSA), a newly launched constellation of satellites. The satellites are currently being deployed in two-year intervals called "Tranches." One of the primary functions of the PWSA is providing a robust and resilient communication network for early-warning threat detection. Analyzing the PWSA is crucial for understanding the significance on the space frontier and its implications for US national security.

1.1 Next-Generation Battlefield

The rise of near-peer adversaries and emerging technologies has transformed space into the next-generation battlefield. Adversarial conflict now involves stealing confidential information, exploiting military technology, and cyberattacks on government infrastructure. With over 4000 satellites, increased space use poses physical and cyber threats from state actors (Housen-Couriel, 2016). The security of information and software technology is at risk, emphasizing the need for dependable communications and uncorrupted information in military operations (Anderson, 2023). As space technologies evolve, the importance of satellite communication and space superiority for national security becomes paramount.

1.2 National Security of Satellites

The National Security Strategy emphasizes the urgent need to advance US technology for military operations, particularly in response to emerging threats like the exponential increase in untraceable cyberattacks from 2021 to 2022

(Housen-Couriel, 2016). Ensuring secure and reliable communication is critical due to the vulnerability of satellites to attack, given their predictive orbits and the advancement of anti-satellite weaponry (Harrison et al., 2021). Security issues in satellite communication further emphasize the necessity for backup systems and strategic planning. Maintaining dominance in both air and space remains a key strategic priority for the United States given its extensive satellite fleet of approximately 3500 space vehicles. Communication satellites play a pivotal role in national security, serving as a force multiplier by enabling rapid data transmission, real-time surveillance, and global coverage for secure communication (USSPACECOM, 2021). Furthermore, satellite communication face vulnerabilities, including susceptibility to signal jamming and interference, which necessitates continuous innovation and adaptation in defense strategies (Frackiewicz, n.d.).

1.3 Hypersonic Weapons

A topic on the forefront of national security is the emergence of hypersonic weapons. At velocities exceeding Mach 5, hypersonic weapons present a next-generation threat in modern warfare. These weapons are resistant to many traditional air defenses. China's increased research into hypersonic weapons is leading the United States to focus heavily on hypersonic technology (Vergun, 2023). China actively researched 64 technologies between 2012 and 2020, prioritizing scramjet engines, combined propulsion systems, and external design for hypersonic weapons. These technological advancements emphasize growing competition in the hypersonic arena. The United States' countermeasure strategy involves advancing its weaponry while simultaneously devising defensive measures to mitigate threats. A critical element of countering a hypersonic involves real-time tracking of these weapons, where communication latency can result in substantial discrepancies between calculated positions and actual positions. At Mach 5 speeds, one second of data latency can result in the hypersonic vehicle traveling 1.72 kilometers. Factoring in acceleration and unknown turning capabilities makes determining the position of a hypersonic difficult.

1.4 Path Optimization

The ongoing threat of hypersonic weapons is increasingly important to satellite data transfer speeds. These satellite networks provide an interconnected web of data transfer paths in space. Unlike stationary ground networks, satellites' locations, relative distances, and access to ground stations are continually changing. These varying factors impact data relay times and connectivity. Due to the transient nature of the network, computing data transmission latency is a key component of analyzing the network efficiency. This research employs Dijkstra's algorithm to calculate the shortest time from detecting an event and relaying the data to a ground station, which is a path optimization problem. There are three primary factors that determine path optimization: the number of available satellites in the constellation, distance to the relay target, and the onboard latency of the satellites. To minimize relay times, reduce the number of satellites when onboard computation latency surpasses light-speed data transmission between them. An increased number of satellites contributes to the robustness of the network due to the existence of more data routing paths (MemComputing, 2022).

1.5 Proliferated Warfighter Space Architecture (PWSA)

The United States is formulating a strategy, spearheaded by the Space Development Agency (SDA), to address the threat of hypersonic weapons. Deficiencies in communication infrastructure reduce real-time tracking latency and provide support to the emerging hypersonic technology domain. This strategy entails the creation of an advanced multilayer satellite constellation called the Proliferated Warfighter Space Architecture (PWSA) to validate low-latency communications within a satellite mesh network and support functionality like beyond-line-of-sight targeting and preliminary missile warning and tracking systems. The PWSA consists of Low-Earth Orbit (LEO) satellites, which orbit at an approximate altitude of 180 to 2000 kilometers (Defensebridge, 2023). The deployment of these satellites occurs over several years. The first deployment of PWSA, referred to as Tranche 0 (T0), was launched on April 2, 2023, for experimental military use. Tranche 0 consists of eight tracking satellites and twenty transport satellites, equipped for data acquisition from other satellites, inter-satellite exchange, and transmission to terrestrial ground receivers (USD(R&E), 2022).

The PWSA satellite constellation includes two more future deployments named Tranche 1 (T1) and Tranche 2 (T2). Satellites within these tranches are further decomposed into tracking and transport layer satellites. The tracking layer detects heat signatures indicating missile launches using Earth-facing sensors, while the transport layer exists slightly above the tracking layer and routes the data from the tracking layer. T1, launching in 2024 with 22 satellites, enhances global tracking, and introduces Overhead Persistent Infrared (OPIR) imaging for real-time threat detection. A summary of the PWSA tracking

and transport layer satellites is shown in Table 1. T2, set for a 2026 launch, comprises 192 transport layer satellites and 52 tracking layer satellites, expanding on T1 capabilities. The T2 transport layer, including Alpha, Beta, and Gamma variant satellites, enhances communication abilities for diverse conditions by utilizing different communications payloads such as optical link terminals and various RF terminals. The PWSA Transport Layer aims to provide multi-band global communications and persistent encrypted connectivity, addressing national security objectives effectively.

Table 1: PWSA Space Vehicle Allocation

	Tracking (# of vehicles)	Transport (# of vehicles)	Total (# of Vehicles)
Tranche 1	39	126	165
Tranche 2	54	210	264

1.6 Model-Based Systems Engineering (MBSE)

Model-Based Systems Engineering (MBSE) is a cost-effective and versatile approach to modeling complex systems like the PWSA. Through the modeling of essential properties and attributes of individual satellites, simulations can be conducted to incorporate instances of these individual satellites operating as a mesh network. Importantly, this approach allows the validation of the system's effectiveness without the need for resource-intensive large-scale prototyping. Figure 2 displays each segment of the PWSA. The Ground Segment, Launch Segment, and Warfighter Interface are made up of components that do not make up the satellites but are essential to the communication, survivability, and success of the mission. A high-level block definition diagram of the PWSA is shown in Figure 2.

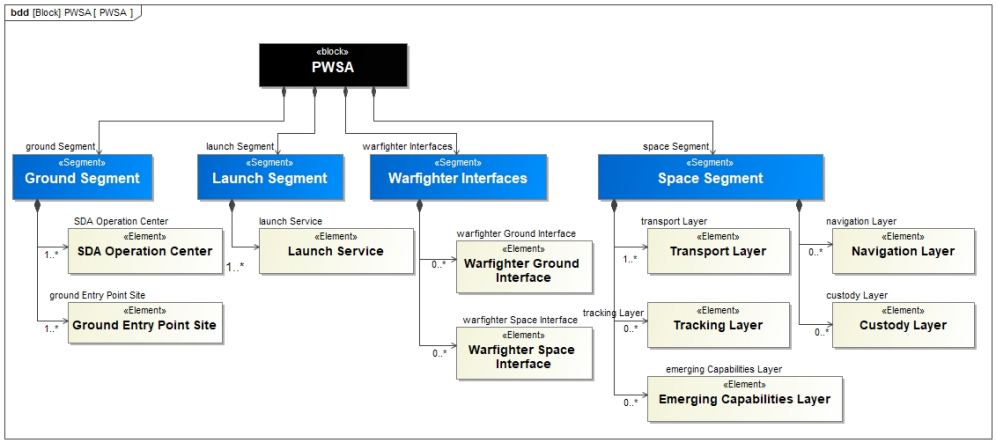

Figure 2: PWSA Diagram of System Segments

MBSE offers many capabilities for modeling and simulation are key to the project's success. Its inherent flexibility allows for model modification and accommodation to integrate new satellites with innovative technologies. It enables the simulation of various scenarios, including critical battle scenarios which expose potential risks or vulnerabilities within the system. For expansive projects, MBSE can offer insight into complex behavioral interactions which makes it particularly well-suited for the analysis of a mesh network satellite constellation system like PWSA. MBSE allows for the breakdown of components consisting of mission critical elements and the capabilities, components, and functional allocations can be displayed in a visual diagram ensuring condensed information and enabling flexibility.

2. Methodology

2.1 Scenario Simulation with Systems Tool Kit (STK)

Systems Tool Kit is a physics-based software application from Analytical Graphics, Inc. (AGI) that enables the simulation of air and space scenarios. This software supports the modeling of the entire PWSA satellite constellation by

inserting satellite ephemeris data. The software contains a graphical user interface for model creation along with a programming interface to create space vehicle objects with code or scripts. Additionally, STK allows users to create connections (labeled "accesses") between objects to simulate data communication.

Using STK, an environment was programmed with the PWSA satellite constellation data. A threat was created in the environment as a maneuverable aircraft. Three ground stations located in Alaska, Norway, and Pennsylvania were modeled to represent the end points of the data relay chain. At any given time during the scenario, the satellites that detect the threat can be identified and the existing connections between satellites can be retrieved. A python script was created to automatically analyze the scenario to extract key details about threat detection and connected satellites at this instance. Location data was also extracted for all satellites at the initial threat detection time. After retrieving all scenario data, Dijkstra's algorithm was employed to find the shortest path from the detection satellite to the ground stations. All scenarios incorporate an approximate 50-millisecond onboard latency for satellites receiving and rebroadcasting data to the next satellite in the network. An example of an STK scenario is shown in Figure 4.

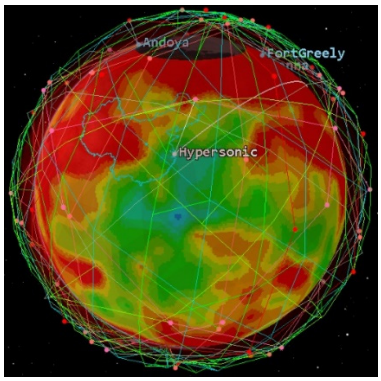

Figure 4: STK simulation displaying detection of a hypersonic threat and satellite communication connections

2.2 Simulated Scenarios

All scenarios use a simulated launch of a hypersonic threat off the eastern coast of China with a flight path towards the United States. The satellite constellation was then analyzed to extract the time to detect the threat and the time to relay the data to each of the three ground stations. This is often referred to as the "signal-to-shooter" time, the time it takes the detection data to the necessary assets for mitigation countermeasures. This is important for hypersonic threats since neutralizing the hypersonic is substantially more achievable in the launch phase. In the launch phase, the hypersonic is gaining altitude, at its slowest velocity, and has limited evasive flight control capability.

The first scenario utilizes only Tranche 1 (T1) of the PWSA for detection and data relay. This scenario represents the current state of the network as of 2024. The second scenario adds Tranche 2 to the existing Tranche 1 satellites. This scenario represents the state of the network in 2026. The first two scenarios establish a baseline for a functioning network. Furthermore, two more scenarios were included to simulate a degraded environment. These scenarios simulate the existence of a directed-energy threat that renders the satellites in immediate proximity of the hypersonic threat unusable. The third scenario examines only T1 satellites with degradation. The fourth scenario examines T1 and T2 satellites with a degraded network. An overview of the scenarios is shown in Table 3.

Table 3: Tested Scenario Descriptions

Scenario	Description
1	Fully Functional T1 Satellites
2	Fully Functional T1+T2 Satellites
3	Degraded T1 Satellites
4	Degraded T1+T2 Satellites

3. Results

3.1 Initial Detection Time

Simulating scenarios provided data for analyzing the PWSA system. In degraded scenarios three and four, three satellites closest to the hypersonic launch were disabled, simulating a directed energy threat. Noticeable differences occurred in initial detection times between fully operational and degraded scenarios. In scenario three, simulating T1 satellites encountering degradation, the threat detection time increased from instantaneous detection to 8.2 minutes. This delay allowed the hypersonic missile to advance significantly towards its target before data could be transmitted to a ground station. The limited number of tracking satellites in T1 led to longer detection times, but this gap narrowed considerably with the addition of T2 satellites in scenario four. In scenario four, simulating T1 and T2 satellites with degradation, the detection time improved to 2.5 minutes but remained higher than in fully operational scenarios. Table 4 presents a summary of threat detection times across the four simulated scenarios.

3.2 Data Relay Time

The data relay time to each ground station was recorded. Data relay time holds significance due to the high velocity of hypersonic vehicles. The transmitted data provides updates which are necessary to provide relevant position, velocity, and trajectory data to intercept the missile. The longest data transmission time to a ground station was 46 seconds, as indicated in Table 4. This delay occurred because the Alaska ground station did not have a satellite within range at the time of threat detection. It took 46 seconds for the next orbiting satellite to come within line-of-sight to transmit data to the ground station. This emphasizes the limitations of a smaller constellation network, minimal ground stations, and underscores the need for Tranche 2 to become operational by 2026. These simulations also reveal a potential weakness in the current satellite connection scheduling. The current method employs a set communication connection schedule based on orbital positions. This is a viable method for fully operational scenarios, but in the presence of non-operational satellites or adversarial interference, data transmission times can be greatly affected. A more robust dynamic scheduling method could be utilized to counteract any degradation in the network.

Table 4: STK Scenario Detection Times

	Operational Scenarios		Degraded Scenarios	
	T1	T1 + T2	T1 w/ Degradation	T1 + T2 w/ Degradation
Time to Detect Threat	0 min	0 min	8.2 min	2.5 min
Alaska Ground Station Relay Time	340 ms	427 ms	46 sec*	831 ms
Norway Ground Station Relay Time	620 ms	483 ms	598 ms	812 ms
Pennsylvania Relay Time	434 ms	370 ms	330 ms	978 ms

*Value occurs from ground station not having a viable ground station connection at the time of detection

Degradation of specific satellites can significantly impact data relay times. In the worst-case scenario modeled, a critical satellite's degradation disrupts its ability to detect hypersonic threats, thereby impeding the swift transfer of data to alternate orbital planes and ground stations. Given the crucial role of data relay time in determining hypersonic position and velocity, the final scenario reveals a substantial delay with data taking almost a full second to reach the Pennsylvania ground station.

4. Discussion of Improvements and Vulnerabilities

The SDA is nearing completion of T1 satellite launches and plans to enhance the system with the next generation T2 satellites. Nonetheless, there are additional areas for improvement. Although the satellites are spaced equally in orbital planes, many orbital planes are at an inclination angle of 81 degrees. This results in an abundance of satellite coverage near the poles and less near the equator. During this analysis, there was minimal ground coverage at specific locations with respect to the

constellation network. If an adversary was strategic about planning a launch, it would only need to render three satellites non-operational to severely affect detection time.

Another vulnerability in the current system is the ground stations. Currently, there are only one or two satellite parabolic antennas at each ground station that allow for connections to be made with satellites. This implies that only one or two satellites can establish connections with the ground station at once to transmit vital mission data, leaving the system vulnerable to further degradation. When such degradation occurs, the satellite dishes must realign themselves to establish a connection with another satellite, which is a time sensitive process. One potential solution is to augment the ground station with additional parabolic antennas or enhance the speed at which the dishes can reposition themselves to establish new links. The onboard latency time significantly contributes to prolonged data relay times. The adoption of newer technologies and enhancements in processing routines could mitigate this added latency facilitating faster data transmission to the ground stations.

The PWSA proves to be robust if the data can reach the network. Many paths exist for transmitting data from one side of the network to the other; however, the endpoints of the network remain vulnerable. An adversary capable of obfuscating the launch of a hypersonic could exploit these vulnerabilities, thereby compromising the effectiveness of the PWSA. To address this, it is imperative to fortify the security measures surrounding the network endpoints. This could involve implementing redundancy measures to ensure continuous data transmission even in the face of attacks or disruptions. Also, establishing secure communication channels between ground stations and satellites along with improving response times for realigning satellite parabolic antennas would bolster the system's resilience against potential threats. By addressing these vulnerabilities and fortifying the network infrastructure, the PWSA can maintain its effectiveness in rapidly relaying mission-critical data, thereby enhancing overall operational readiness and security.

5. Future Work and Conclusion

The results provide an insightful initial investigation into the performance of the PWSA constellation network. However, a more dynamic algorithm for the satellite connection schedule could optimize resource allocation and enhance system efficiency moving forward. This would improve the mesh-network connectivity and system resiliency when suffering degradation, allowing for faster data relay times due to an adaptive connection schedule of satellites. This allows for improved low-latency data and accurately reflects real-time hypersonic weapon tracking. Future work includes continuously refining the MBSE model with updated data from SDA, creating detailed scenario models to assess potential countermeasures and their effectiveness, especially in degraded scenarios with impacted detection times.

As the landscape of the space domain undergoes constant evolution, numerous organizations and commercial entities are innovating advanced solutions to combat emerging challenges posed by hypersonic weapons. SDA is at the forefront of this effort by fortifying their mesh-network satellite system, aiming to address national security concerns arising from near-peer adversaries' advancements in hypersonic technologies. Upon completion, this network will deliver high-bandwidth, low-latency data to warfighters, significantly bolstering defense capabilities against evolving technological threats confronting the United States.

6. Citations and References

Anderson, J. L. (2023, January 20). Global Cyberattacks Increased 38% in 2022. Security Magazine RSS. https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022

Defensebridge. (2023, May 3). The Role of Military Satellites in National Security. https://defensebridge.com/article/the-role-of-military-satellites-in-national-security.html

Department of Defense Washington DC. (2011). *National Security Space Strategy Unclassified Summary*. Arlington.

Frackiewicz, M. (n.d.). Satellite Military Communications vs Terrestrial Communications: Which is the better choice? *T2 SPACE*.

Frackiewicz, M. (n.d.). The Advantages of Satellite Communication for Military Operations. *T2 SPACE*.

Frackiewicz, M. (n.d.). The Future of Communication Satellites: New Technologies and Applications. *T2 SPACE*.

Harrison, T., Johnson, K., & Young, M. (2021, February 25). Defense Against the Dark Arts in Space: Protecting Space Systems from Counterspace Weapons. CSIS. https://www.csis.org/analysis/defense-against-dark-arts-space-protecting-space-systems-counterspace-weapons

Housen-Couriel, D. (2016). Cybersecurity threats to satellite communications: Towards a typology of state actor responses. Acta Astronautica, 128, 409–415. https://doi.org/10.1016/j.actaastro.2016.07.041

MemComputing. (2022). Proliferated LEO Satellite Optimization. MemComputing. https://www.memcpu.com/media/2022/10/AMTI-Case-Study-2022.pdf

Office of the Under Secretary of Defense Research and Engineering (USD(R&E)). (2022). *Tranche 1 National Defense Space Architecture (NDSA) Draft Concept of Operations (CONOPS)*. Washington, DC.

Space Development Agency Makes Awards to Build 72 Beta Variant Satellites for Tranche 2 Transport Layer. Space Development Agency. (2023, August 21). https://www.sda.mil/space-development-agency-makes-awards-to-build-72-beta-variant-satellites-for-tranche-2-transport-layer/

USSPACECOM. (2021, January). Never a Day Without Space Commander's Strategic Vision. Spacecom.mil. https://www.spacecom.mil/Portals/32/Images/cc-vision/usspacecom-strategic-vision-22feb21.pdf

Vergun, D. (2023, May 10). General Says Countering Hypersonic Weapons is Imperative. U.S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/article/3391322/general-says-countering-hypersonic-weapons-is-imperative/