Network Science and Complex Systems
https://nscs-journal.org

Relationship Between Robustness Metrics and Attack Tolerance in Satellite Communication Constellations

Themba Mbeki*

School of Engineering, University of KwaZulu-Natal, Durban, KwaZulu-Natal, South Africa

Corresponding author: themba.mbeki@gmail.com

Abstract

The rapid deployment of massive low Earth orbit satellite communication constellations has revolutionized global internet connectivity, providing high bandwidth and low latency coverage to underserved regions. However, the increasing reliance on these space based networks introduces critical vulnerabilities to both random failures and intentional cyber or kinetic attacks. This paper investigates the complex relationship between static network robustness metrics and dynamic attack tolerance within simulated satellite communication constellations. By modeling large scale space networks as complex graphs, this study evaluates how traditional topological metrics, including average node degree, betweenness centrality, and algebraic connectivity, predict the network capacity to withstand various attack vectors. Utilizing an advanced discrete event simulation environment, we subjected multiple constellation topologies to both random node failures and targeted centrality based attacks. The structural and functional degradation of the network was measured continuously to determine the correlation between initial robustness metrics and the threshold of network fragmentation. The simulation evidence reveals that while high average degree improves tolerance against random failures, algebraic connectivity serves as a vastly superior predictor of resilience against targeted attacks aimed at critical routing hubs. The findings provide critical insights for constellation designers, suggesting that optimizing for specific spectral graph properties can significantly enhance the survivability of next generation space networks without requiring proportional increases in physical redundancy or launch costs.

Keywords: Satellite Communication Networks; Network Robustness; Attack Tolerance; Topology Simulation; Robustness Metrics

1. Introduction

1.1 Context of Satellite Communication Networks

The architecture of global telecommunications has undergone a profound transformation over the past decade, driven primarily by the commercial feasibility and rapid deployment of massive satellite constellations in low Earth orbit. Unlike traditional geostationary orbit satellites that provide wide area coverage at the expense of significant signal propagation delay, low Earth orbit constellations operate at altitudes ranging from three hundred to one thousand two hundred kilometers. This proximity to the Earth surface enables latency profiles that are comparable to terrestrial fiber optic networks, thereby facilitating real time applications such as telemedicine, automated financial trading, and autonomous vehicle command and control. The proliferation of these constellations, spearheaded by major aerospace corporations and international telecommunications consortia, represents a fundamental shift in how global data infrastructure is conceptualized and implemented. The integration of inter satellite links using advanced optical laser technology allows these constellations to function as autonomous routing networks in space, bypassing the need for extensive terrestrial gateway infrastructure and enabling direct data transmission across continents and oceans. As these space based networks scale to encompass tens of thousands of individual orbital nodes, the topological complexity of the system increases exponentially [1]. This unprecedented scale introduces novel engineering challenges, particularly concerning the maintenance of network cohesion and routing efficiency in a highly dynamic physical environment where the relative positions of nodes are constantly changing according to orbital mechanics [2]. The dynamic nature of the topology requires sophisticated, highly adaptable routing protocols capable of recalculating optimal data paths continuously. Consequently, the structural integrity of the network topology becomes a critical determinant of overall system performance and reliability, necessitating rigorous academic investigation into the fundamental properties that govern satellite network behavior under stress.

1.2 The Problem of Network Vulnerability

Despite the inherent redundancy provided by thousands of orbiting nodes, satellite communication constellations remain acutely vulnerable to a wide spectrum of operational disruptions and malicious attacks. The harsh environment of space

subjects orbital hardware to constant degradation from ionizing radiation, thermal cycling, and potential collisions with micrometeoroids or orbital debris, leading to random, stochastic node failures. Furthermore, the strategic importance of global communication networks makes them prime targets for state sponsored adversaries and sophisticated cyber criminal organizations. Adversarial actions can range from localized radio frequency jamming of user terminals and uplink stations to complex cyber attacks designed to compromise satellite command and control systems, effectively rendering the node inert or maliciously altering its routing tables [3]. In extreme scenarios, the threat of kinetic anti satellite weapons poses a severe risk to constellation integrity, where the physical destruction of a single node can precipitate a cascade of orbital debris that threatens neighboring satellites [4]. When a satellite node fails or is deliberately compromised, the network must autonomously detect the localized failure and reroute data traffic through adjacent nodes. If the attack targets highly central nodes responsible for bridging disparate orbital planes, the localized failure can lead to severe data congestion on alternative routes, buffer overflows, and cascading failures that propagate throughout the network. The challenge for network architects is to design constellations that not only provide optimal coverage and bandwidth under normal operating conditions but also exhibit high tolerance to both random attrition and targeted, intelligent attacks designed to maximize structural fragmentation.

1.3 Research Objectives and Contributions

The primary objective of this research is to establish a rigorous, quantifiable link between static network robustness metrics and dynamic attack tolerance within the context of massive satellite communication constellations. While graph theory provides a robust framework for analyzing terrestrial networks, the application of these principles to the highly dynamic, deterministic topology of low Earth orbit constellations requires specialized empirical validation. This study aims to answer the fundamental question of which topological metrics most accurately predict a space network capacity to maintain data throughput and structural connectivity under various attack scenarios [5]. To achieve this, we developed a comprehensive simulation methodology that models multiple constellation architectures and subjects them to simulated random failures and targeted node removal attacks. The contributions of this paper are threefold. First, we provide a detailed comparative analysis of established robustness metrics, evaluating their applicability and predictive power specifically for satellite network topologies. Second, we present extensive empirical evidence derived from large scale discrete event simulations, quantifying the degradation of network performance as a function of node loss. Finally, we formulate actionable design principles for constellation architects, demonstrating how targeted optimization of specific spectral graph properties, such as algebraic connectivity, can dramatically improve network survivability without necessitating excessive over engineering of the physical space segment.

2. Literature Review and Background

2.1 Evolution of Satellite Communication Constellations

The historical trajectory of satellite communications reveals a continuous effort to balance coverage area, signal latency, and system capacity. Early satellite communication systems relied almost exclusively on geostationary orbit satellites, which, by virtue of their synchronized orbital period with the Earth rotation, appear stationary relative to ground antennas. While geostationary systems remain invaluable for broadcast television and maritime communications, their altitude of nearly thirty six thousand kilometers imposes an unavoidable propagation delay of approximately two hundred and fifty milliseconds for a round trip signal, rendering them unsuitable for interactive, latency sensitive applications [6]. In the late twentieth century, the first generation of low Earth orbit constellations attempted to circumvent this limitation, but these early ventures were largely hindered by prohibitive launch costs, rudimentary inter satellite link technology, and insufficient market demand for mobile voice services. However, the contemporary landscape has been radically altered by advancements in reusable launch vehicle technology, the miniaturization of satellite components, and the maturation of free space optical communication systems [7]. Modern mega constellations are designed not merely as bent pipe relays that bounce signals back to a nearby ground station, but as complex, autonomous mesh networks in space. The deployment of thousands of interconnected satellites operating in multiple orbital shells creates a highly resilient fabric of global connectivity. The literature extensively documents this transition, emphasizing that the primary bottleneck in modern satellite network design is no longer physical deployment, but rather the algorithmic management of the dynamically shifting topological structure and the optimization of data flow across continuously changing inter satellite links.

2.2 Theoretical Frameworks for Network Robustness

The analysis of network robustness is deeply rooted in graph theory, a branch of discrete mathematics that models systems as collections of vertices connected by edges. In the context of satellite communications, vertices represent individual satellites or ground stations, while edges represent the inter satellite links or radio frequency uplinks and downlinks. The robustness of a graph refers to its ability to maintain its fundamental properties, such as connectivity and short path lengths, despite the removal of vertices or edges. Traditional literature often categorizes network topologies into regular graphs, random graphs, small world networks, and scale free networks. Regular graphs exhibit uniform connections, while scale free networks are characterized by a power law degree distribution, meaning a small number of nodes, known as hubs,

possess a disproportionately large number of connections [8]. Research indicates that scale free networks demonstrate remarkable resilience to random node failures because the vast majority of nodes have very few connections, making their random removal inconsequential to the overall network structure [9]. However, this same topological property renders scale free networks highly vulnerable to targeted attacks; the intentional removal of a few highly connected hubs can rapidly fragment the network into isolated subgraphs. Satellite constellations, due to their geometric orbital arrangements, typically resemble regular or bounded degree graphs rather than pure scale free networks, as each satellite is physically limited in the number of optical transceivers it can carry [10]. Consequently, the theoretical frameworks used to evaluate satellite network robustness must be adapted to account for these physical and geometric constraints, focusing on metrics that capture the subtle structural vulnerabilities inherent in multi planar orbital designs.

2.3 Attack Modeling in Space Networks

Modeling attacks on space networks requires a nuanced understanding of both physical space environment threats and sophisticated cyber warfare tactics. The literature categorizes threat vectors into two primary domains: stochastic environmental failures and deterministic adversarial attacks. Stochastic failures are typically modeled as random node or link removals, simulating events such as spontaneous hardware malfunctions, cosmic radiation induced single event upsets, or transient atmospheric interference affecting ground links [11]. Conversely, deterministic attacks simulate an intelligent adversary with comprehensive knowledge of the network topology, seeking to maximize disruption with minimal effort. Centrality based attacks are the most common model used in literature for this purpose. In a degree centrality attack, the adversary sequentially eliminates the nodes with the highest number of active connections. While effective in scale free terrestrial networks, this strategy is less impactful in satellite constellations where the node degree variance is minimal. More sophisticated models employ betweenness centrality attacks, targeting nodes that lie on the highest number of shortest paths between all other node pairs in the network [12]. Removing satellites with high betweenness centrality disproportionately disrupts optimal routing paths, forcing traffic to detour through suboptimal links, thereby increasing latency and precipitating cascading buffer overflows. Furthermore, advanced literature introduces the concept of coordinated planar attacks, where adversaries target specific orbital planes to sever hemispheric communication links, a scenario unique to the geometric structure of satellite constellations. Understanding these diverse attack models is essential for developing comprehensive simulation environments capable of thoroughly evaluating constellation robustness.

2.4 Gaps in the Current Literature

While substantial progress has been made in analyzing the topological properties of theoretical networks, significant gaps remain in the application of these concepts to contemporary, large scale satellite constellations. Much of the existing literature relies on static graph snapshots, failing to adequately account for the high velocity, predictable mobility of low Earth orbit satellites, which constantly break and form inter satellite links as they traverse polar or seam regions. Furthermore, previous studies often analyze robustness purely in terms of structural connectivity metrics, such as the size of the largest connected component, without translating these topological measures into dynamic functional metrics like packet delivery ratio, end to end latency, and throughput capacity [13]. A network may remain structurally connected after an attack, yet be functionally inoperable due to severe congestion on the remaining vital links. There is a pressing need for integrated research that combines rigorous graph theoretic static analysis with high fidelity discrete event network simulations to observe how structural damage manifests as data transmission failure in real time. This paper addresses this gap by directly correlating established static robustness metrics with empirical performance data derived from simulated continuous dynamic routing under progressive attack stress, providing a more holistic and operationally relevant evaluation of satellite network attack tolerance.

3. Methodology and Simulation Design

3.1 Satellite Network Topology Generation

To ensure the physical realism and applicability of our simulation, the satellite constellation topologies were generated based on established orbital mechanics models, specifically focusing on the Walker Delta and Walker Star configurations, which form the basis for most commercial mega constellations. The generation process utilizes precise Keplerian orbital elements to define the exact position and velocity of every satellite node at any given discrete time step. A Walker Delta constellation is mathematically defined by three primary parameters: the total number of satellites, the number of distinct orbital planes, and the relative phasing parameter between adjacent planes. These parameters dictate the geometric distribution of nodes around the globe, ensuring continuous coverage at specific latitudes [14]. In our methodology, we established a baseline network topology consisting of multiple orbital shells to simulate a tiered routing architecture. Satellites within the same orbital plane are connected via intra plane inter satellite links, which remain relatively stable over time as the satellites move in unison. Conversely, inter plane links connect satellites in adjacent orbital planes. These links are highly dynamic; they must be periodically broken and reestablished as satellites approach the polar regions where orbital planes intersect, causing the physical distance and pointing angles between satellites to change rapidly [15]. The topology generation algorithm continuously monitors the Euclidean distance and line of sight visibility between all node

pairs, automatically establishing edges in the network graph whenever two nodes fall within the operational range of their simulated optical laser transceivers. This dynamic graph generation ensures that the structural foundation of our simulation accurately reflects the time varying nature of real world space networks.

3.2 Threat Models and Attack Vectors

The core of our methodology involves subjecting the dynamically generated constellation topologies to a series of rigorous threat models designed to evaluate structural attack tolerance. We implemented two distinct categories of attack vectors: random failure models and targeted centrality models. The random failure model simulates the stochastic loss of operational capacity due to harsh environmental factors or non targeted kinetic debris impacts. In this scenario, nodes are selected for removal using a uniform probability distribution, simulating a uniform risk profile across the entire constellation [16]. This serves as the baseline for evaluating general network resilience.

Table 1: Configuration Parameters for the Simulated Satellite Constellations

Parameter	Value	Description
Total Nodes	1584	Total number of satellites across all active orbital shells
Orbital Planes	72	Number of distinct orbital planes in the primary shell
Nodes per Plane	22	Number of uniformly distributed satellites per orbital plane
Altitude	550 km	Average operational altitude defining the signal propagation delay
Max ISL per Node	4	Maximum simultaneous optical inter satellite links per satellite

The targeted attack models represent a sophisticated, knowledgeable adversary attempting to inflict maximum network fragmentation with minimum effort. We implemented a dynamic betweenness centrality attack, where the simulation engine calculates the exact betweenness centrality for every active node based on current shortest path routing tables. The node with the absolute highest centrality score is abruptly removed from the network, simulating a precise cyber compromise or targeted kinetic strike. Because the removal of a central hub fundamentally alters the optimal routing paths for the rest of the network, the betweenness centrality scores for all remaining nodes must be meticulously recalculated before the subsequent node is removed. This iterative recalculation simulates a sequential, highly adaptive attack strategy. We systematically varied the intensity of these attacks, removing nodes in increments of one percent of the total constellation size, up to a maximum degradation of thirty percent, at which point fundamental network operability typically ceases.

3.3 Simulation Environment Setup

To capture the complex interplay between orbital mechanics, topological changes, and data routing protocols, we developed a custom simulation environment built upon an industry standard discrete event network simulator framework. The simulation environment is strictly deterministic regarding orbital mechanics, utilizing numerical integration of orbital perturbations to update node positions every discrete simulation second. At each time step, the dynamic topology generator passes the updated adjacency matrix to the network routing module [17]. We implemented a distributed, shortest path first routing algorithm, heavily modified to account for the predictable mobility of the nodes. Data traffic generation is modeled using multiple Poisson processes, establishing end to end communication sessions between randomly selected ground stations distributed globally according to human population density metrics. The data packets are injected into the space segment via the nearest visible satellite uplink and subsequently routed through the inter satellite link mesh. The simulation meticulously tracks individual packet propagation delays, queuing delays at intermediate satellite buffers, and packet drop events due to buffer saturation or link failure. By maintaining high fidelity models of the physical transport layer and the network routing layer simultaneously, the simulation environment provides an exceptionally detailed observation platform for monitoring how localized structural damage cascades into widespread functional network failure.

4. Analysis of Robustness Metrics

4.1 Static Topological Metrics

The evaluation of network attack tolerance begins with a comprehensive analysis of static topological metrics, which serve as the fundamental indicators of structural robustness. In the context of satellite constellations, we focus on three primary metrics: average node degree, characteristic path length, and the clustering coefficient. The average node degree represents the mean number of active inter satellite links per satellite. Given the physical constraints of optical transceivers, this value is strictly bounded, typically ranging between four and six in modern architectures. A higher average degree inherently provides greater redundancy, offering alternative routing paths when a primary link fails [18]. However, simply maximizing the degree is physically impractical; therefore, the distribution of these connections is equally critical. The characteristic path length measures the average number of hops required to transmit a signal between any two randomly

selected nodes in the network. A robust constellation must maintain a low characteristic path length even under severe attack stress to guarantee acceptable end to end latency. As nodes are removed during an attack, the characteristic path length inevitably increases as traffic is forced onto longer, suboptimal detour routes. The rate of this increase serves as a primary indicator of topological degradation. Finally, the clustering coefficient quantifies the tendency of nodes to form tightly knit, interconnected groups. High clustering implies that the neighbors of a given satellite are also connected to each other, creating localized redundancy that can seamlessly bypass an isolated node failure without requiring a global routing recalculation. Analyzing the interplay of these three metrics provides a comprehensive baseline for understanding the initial structural integrity of the constellation before dynamic traffic loads are applied.

4.2 Dynamic Flow Metrics

While static metrics provide insight into structural potential, they cannot fully capture the operational reality of a network under stress. Therefore, our analysis heavily incorporates dynamic flow metrics, which measure the actual movement of data across the topology. The most critical metric in this domain is the maximum network flow capacity, representing the absolute upper bound of data throughput the constellation can sustain before widespread congestion occurs. As targeted attacks remove high centrality nodes, the physical links connecting the remaining nodes become severe bottlenecks [19]. We monitor the utilization rates of all active inter satellite links, identifying the specific locations where traffic rerouting causes queue lengths to exceed satellite buffer capacities.

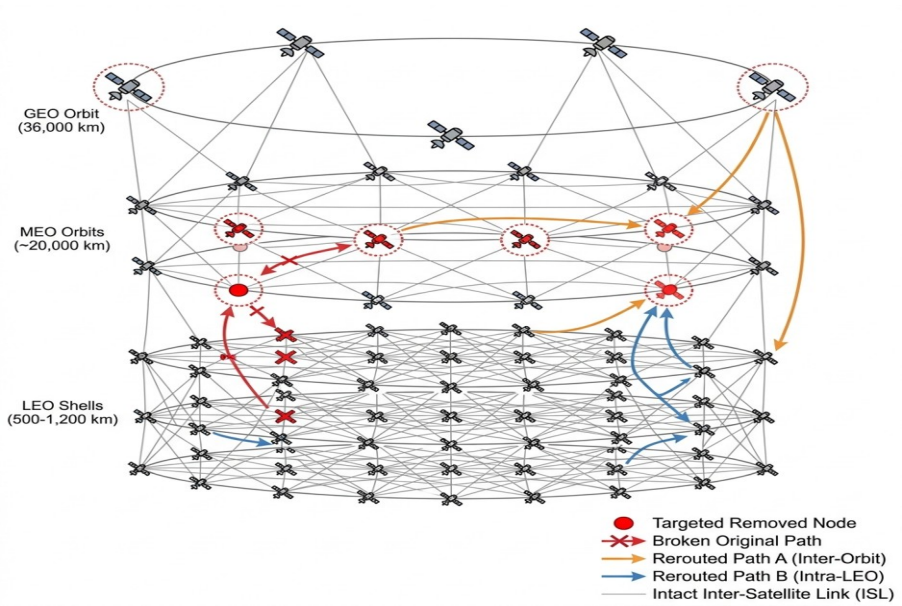

Figure 1: Comprehensive Schematic of Satellite Network Topology Subject to Targeted Node Removal Attacks

The packet delivery ratio is another essential dynamic metric, defined as the percentage of successfully delivered data packets relative to the total number of packets injected into the network. In an unstressed state, the packet delivery ratio approaches one hundred percent. However, as the network undergoes sequential node removal, routing tables struggle to converge, and packets are dropped either due to transient routing loops or hard buffer overflows. By plotting the packet delivery ratio against the percentage of removed nodes, we can identify the exact tipping point at which the network transitions from a degraded but functional state to a state of complete cascading failure. This transition point is the definitive empirical measure of the network's dynamic attack tolerance.

4.3 Correlation Methodology

The core analytical thrust of this paper is to bridge the gap between static topological properties and dynamic operational tolerance. To achieve this, we employ a rigorous statistical correlation methodology. We evaluate an advanced spectral graph metric known as algebraic connectivity, which is derived from the second smallest eigenvalue of the normalized Laplacian matrix representing the network topology. Theoretical mathematics suggests that algebraic connectivity is a profound indicator of how easily a graph can be bisected or fragmented into isolated components [20]. In our methodology, we compute the baseline algebraic connectivity for multiple distinct constellation designs. We then subject each design to identical simulation workloads and identical targeted attack sequences, meticulously recording the node removal percentage at which the packet delivery ratio falls below an unacceptable threshold of eighty percent. We calculate the Pearson correlation coefficient between the initial static algebraic connectivity scores and the dynamic failure thresholds across all tested topologies. A strong positive correlation indicates that the mathematically derived static metric is a highly reliable predictor of real world survivability under adversarial conditions. This correlation analysis forms the foundation

for developing predictive models that can evaluate the robustness of proposed constellation designs computationally, without requiring exhaustive, time consuming dynamic simulations for every minor architectural adjustment.

5. Results and Discussion

5.1 Baseline Network Performance

The initial phase of the simulation evaluated the baseline performance of the satellite constellations under nominal operating conditions, with zero node failures and a steady state global data traffic load. The results confirmed the expected high efficiency of the Walker Delta architecture. The average characteristic path length remained consistently low, demonstrating that the deterministic inter and intra plane links establish an optimal mesh for global routing. The dynamic flow analysis revealed that under baseline conditions, network link utilization was evenly distributed, with no single inter satellite link exceeding sixty percent capacity. This even distribution is crucial, as it indicates a lack of inherent structural bottlenecks in the pristine topology. The packet delivery ratio maintained a steady state of ninety nine point nine percent, with negligible packet loss attributed solely to the standard propagation delays and minor buffering required during the handover phases when inter plane links were rapidly reconfigured over the polar regions. These baseline metrics establish the reference point against which all subsequent degradation caused by simulated attacks is measured.

5.2 Impact of Targeted Attacks on Network Connectivity

The simulation results revealed a stark contrast in network resilience when comparing random node failures to sequential targeted attacks based on betweenness centrality. Under the random failure scenario, the constellation exhibited remarkable robustness. The uniform distribution of node loss allowed the distributed routing protocol to easily find alternative paths with minimal disruption. The network maintained a packet delivery ratio above ninety percent even when up to fifteen percent of the total constellation was randomly removed. However, the application of targeted attacks exposed deep structural vulnerabilities within the multi planar geometry.

Table 2: Summary of Network Performance Degradation Under Various Attack Scenarios

Attack Vector	5% Node Removal	10% Node Removal	15% Node Removal
Random Failure	98.2% Delivery	94.5% Delivery	91.1% Delivery
Centrality Attack	85.4% Delivery	62.3% Delivery	31.7% Delivery

When the adversary systematically eliminated the nodes with the highest recalculated betweenness centrality, the degradation was catastrophic and non linear. The removal of merely five percent of the most central nodes forced massive volumes of data traffic to detour across significantly longer physical paths, rapidly elevating the characteristic path length. At the ten percent removal threshold under targeted attack, the network experienced severe cascading failures. The alternative routing paths became instantly saturated, leading to massive buffer overflows on adjacent nodes. This congestion effectively severed communications between entire geographic hemispheres, despite the fact that ninety percent of the physical satellites remained fully operational. This stark divergence in performance highlights the critical inadequacy of assessing network health purely by the total number of surviving nodes.

5.3 Evaluation of Attack Tolerance

The statistical correlation between static robustness metrics and dynamic attack tolerance yielded highly significant findings. Traditional metrics, such as average node degree and clustering coefficient, showed only weak to moderate predictive power regarding a topology's ability to withstand targeted centrality attacks. While a higher average degree improved resistance to random failures, it provided marginal benefit against an intelligent adversary targeting structural hubs [21]. In contrast, the algebraic connectivity metric demonstrated an exceptionally strong positive correlation with the dynamic failure threshold. Constellation topologies engineered to maximize their baseline algebraic connectivity consistently required a significantly higher percentage of node removal during targeted attacks before experiencing systemic routing failure. The mathematical properties of algebraic connectivity inherently account for the global interconnectivity of the network, accurately reflecting the topology's resistance to structural bisection. This evidence validates the hypothesis that spectral graph properties are vastly superior indicators of functional network survivability compared to simple nodal degree statistics.

5.4 Practical Implications for Constellation Design

The empirical evidence generated by these simulations provides crucial, actionable directives for satellite constellation architects and network engineers. The historical approach of mitigating network vulnerability by simply launching more satellites to increase raw redundancy is economically inefficient and fails to address the fundamental structural weaknesses exploited by targeted attacks. Instead, engineers must prioritize the optimization of spectral graph properties during the orbital design phase [22]. By carefully adjusting the phasing parameters and orbital inclinations of Walker constellations, architects can artificially elevate the algebraic connectivity of the resulting dynamic graph without increasing the total number of deployed satellites. Furthermore, the routing protocols deployed in the space segment must evolve beyond simple shortest path algorithms. Implementing congestion aware multipath routing can significantly delay the onset of

cascading failures by intelligently distributing traffic across multiple sub optimal paths, thereby preventing the rapid saturation of critical bottleneck links when primary hubs are compromised. Ultimately, linking these sophisticated mathematical robustness metrics to dynamic simulation outcomes enables the proactive design of next generation space networks that are inherently resilient to intelligent adversarial disruption.

6. Conclusion

6.1 Summary of Findings

This comprehensive research investigated the complex dynamics of network robustness and attack tolerance within large scale satellite communication constellations. By employing sophisticated discrete event simulations combined with rigorous graph theoretic analysis, we evaluated the degradation of space networks under both stochastic environmental failures and deterministic, intelligent adversarial attacks. The findings unequivocally demonstrate that while massive low Earth orbit constellations are highly resilient to random node attrition, they harbor significant vulnerabilities to targeted attacks directed at nodes with high betweenness centrality. The sequential removal of these critical routing hubs precipitates rapid structural bisection and severe cascading data congestion, rendering the network functionally inoperable even when the vast majority of physical assets remain intact. Most importantly, this study establishes a definitive, quantifiable link between the static spectral metric of algebraic connectivity and dynamic functional survivability. Topologies exhibiting higher initial algebraic connectivity consistently demonstrated vastly superior tolerance to targeted network fragmentation.

6.2 Limitations of the Study

Despite the extensive simulation environment, this study acknowledges several methodological limitations. The discrete event simulator, while highly detailed regarding orbital mechanics and basic routing protocols, utilizes generalized models for the physical transport layer, specifically the optical inter satellite links. In reality, the establishment and maintenance of these optical links are highly sensitive to pointing, acquisition, and tracking errors, which can introduce transient link failures not fully captured by our binary adjacency matrices. Additionally, the traffic generation model relies on continuous Poisson distributions based on static population density, which may not perfectly represent the highly bursty and unpredictable nature of actual global internet traffic patterns. Furthermore, the targeted attack models assume the adversary possesses perfect, real time topological knowledge to calculate exact betweenness centrality, an assumption that represents a worst case scenario but may overstate the practical capabilities of current threat actors.

6.3 Directions for Future Research

The findings of this paper open several critical avenues for future academic exploration in space network engineering. Subsequent research must focus on integrating high fidelity physical layer models into the network simulations, particularly incorporating the signal degradation and pointing error probabilities inherent in free space optical communications. There is also a pressing need to explore the implementation of artificial intelligence and machine learning algorithms within the satellite routing architecture. Machine learning models could theoretically predict the onset of localized congestion following a node failure and preemptively calculate decentralized multipath routes to prevent cascading buffer overflows. Finally, future studies should investigate the structural resilience of multi layered heterogeneous constellations, which integrate highly elliptical orbits and geostationary relays with the low Earth orbit mesh, potentially creating a hybrid topological architecture that maximizes algebraic connectivity and definitively neutralizes the threat of localized centrality attacks.

References

1. Mahmood, K.; Saleem, M.A.; Ghaffar, Z.; Shamshad, S.; Das, A.K.; Alenazi, M.J.F. Robust and efficient three-factor authentication solution for WSN-based industrial IoT deployment. Internet Things 2024, 28, 101372.

2. Garcia, A.; Oregui, X.; Ojer, M. Edge architecture for the automation and control of flexible manufacturing lines. Procedia Comput. Sci. 2024, 237, 305–312.

3. Jin, Z.; Zhao, Q.; Su, Y. RCAR: A Reinforcement-Learning-Based Routing Protocol for Congestion-Avoided Underwater Acoustic Sensor Networks. IEEE Sens. J. 2019, 19, 10881–10891.

4. Alotaibi, B. A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities. Sensors 2023, 23, 7470.

5. Lin, C.C.; Chin, H.H.; Lin, W.X.; Lu, K.W. Dynamic energy-efficient surveillance routing in uncertain group-based industrial wireless sensor networks. Wirel. Netw. 2022, 28, 2597–2608.

6. Sun, Y.; Zeng, W.; Shen, H.; Chen, W.; Chen, Y.; Liu, J.; Fan, Z. Separation of distorted overlapping spectra in fiber Bragg grating sensor networks using self-supervised contrastive learning. Opt. Express 2025, 33, 44654–44670.

7. Sutton, R.S.; Barto, A.G. Reinforcement Learning: An Introduction; MIT Press: Cambridge, MA, USA, 2018.

8. Saad, W.; Bennis, M.; Chen, M. A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems. IEEE Netw. 2020, 34, 134–142.

9. Chowdhury, M.Z.; Shahjalal, M.; Ahmed, S.; Jang, Y.M. 6G Wireless Communication Systems: Applications, Requirements, Technologies,

Challenges, and Research Directions. IEEE Open J. Commun. Soc. 2020, 1, 957–975.

10. Lu, C.; Saifullah, A.; Li, B.; Sha, M.; González, H.; Gunatilaka, D.; Wu, C.; Nie, L.; Chen, Y. Real-Time Wireless Sensor-Actuator Networks for Industrial Cyber-Physical Systems. Proc. IEEE 2016, 104, 1013–1024.

11. Kombate, Y.; Houngue, P.; Ouya, S. Securing MQTT: Unveiling vulnerabilities and innovating cyber range solutions. Procedia Comput. Sci. 2024, 241, 69–76.

12. Babbar, H.; Rani, S.; Boulila, W. Fortifying the Connection: Cybersecurity Tactics for WSN-Driven Smart Manufacturing in the Era of Industry 5.0. IEEE Open J. Commun. Soc. 2025, 6, 3417–3428.

13. Banerjee, A.; Costa, B.; Forkan, A.R.M.; Kang, Y.-B.; Marti, F.; McCarthy, C.; Ghaderi, H.; Georgakopoulos, D.; Jayaraman, P.P. 5G enabled smart cities: A real-world evaluation and analysis of 5G using a pilot smart city application. Internet Things 2024, 28, 101326.

14. Wang, Z.; Sun, D.; Yu, C. Reference Broadcast-Based Secure Time Synchronization for Industrial Wireless Sensor Networks. Appl. Sci. 2023, 13, 9223.

15. Soares, C.A.R.; Couto, R.; Sztajnberg, A.; do Amaral, J.L.M. POSIMNET-R: An immunologic resilient approach to position routers in Industrial Wireless Sensor Networks. Expert Syst. Appl. 2022, 188, 116045.

16. Nguyen, T.T.; Oh, H. A Smart Multichannel Slotted Sense Multiple Access Protocol for Industrial Wireless Sensor Networks. IEEE Internet Things J. 2022, 9, 12460–12471.

17. Singh, A.; Raj, A.; Rani, P.; Khatibi, A.; Aldeeb, H.; Shukla, P.K.; Sabry, A.; Hassan, M.M. Resilient wireless sensor networks in industrial contexts via energy-efficient optimization and trust-based secure routing. Peer-to-Peer Netw. Appl. 2025, 18, 1–17.

18. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A.; Li, J.; Niyato, D.; Dobre, O.; Poor, H.V. 6G Internet of Things: A Comprehensive Survey. IEEE Internet Things J. 2022, 9, 359–383.

19. Zezulka, F.; Marcon, P.; Bradac, Z.; Arm, J.; Benesl, T. Time-Sensitive Networking as the Communication Future of Industry 4.0. IFAC-Pap. 2019, 52, 133–138.

20. Strinati, E.C.; Barbarossa, S.; Gonzalez-Jimenez, J.L.; Kténas, D.; Cassiau, N.; Maret, L.; Dehos, C. 6G: The Next Frontier: From Holographic Messaging to Artificial Intelligence Using Subterahertz and Visible Light Communication. IEEE Veh. Technol. Mag. 2019, 14, 42–50.

21. Luo, T.; Xie, J.; Zhang, B.; Zhang, Y.; Li, C.; Zhou, J. An improved levy chaotic particle swarm optimization algorithm for energy-efficient cluster routing scheme in industrial wireless sensor networks. Expert Syst. Appl. 2024, 241, 122780.

22. Liu, Y.; Li, C.; Xiao, J.; Li, Z.; Chen, W.; Qu, X.; Zhou, J. QEGWO: Energy-Efficient Clustering Approach for Industrial Wireless Sensor Networks Using Quantum-Related Bioinspired Optimization. IEEE Internet Things J. 2022, 9, 23691–23704.