Universidad
Politécnica
de Cartagena

An Overview of Space Digital Twin for Secure Satellite Internet : Vulnerabilities, Methodologies, and Future Directions

Author - Wai Yan Kyaw
Supervisor - Juan Pedro Muñoz Gea
Reviewer - María Dolores Cano Baños

Table of Contents

1. Introduction

In recent years, companies such as SpaceX, OneWeb and Amazon have been deploying LEO satellite networks to create integrated space and terrestrial networks (ISTNs) that offer global high-speed, low-latency Internet. While these networks improve connectivity, they also face unique security challenges, such as DDoS attacks and eavesdropping. The paper proposes using Space Digital Twin (SDT) technology to create virtual replicas of ISTNs for security assessments, identifying vulnerabilities, and testing countermeasures. It also highlights the need for future research to enhance SDT's capabilities for secure and reliable ISTNs.

2. Security Anatomy for Futuristic ISTNs

ISTNs have unique features that differentiate them from terrestrial networks:

- Performing two core functions: space routers and access routers
- Three-dimensional, dynamic, and predictable network topology
- Pervasive connectivity
- High diversity between space and terrestrial resources
- Open and failure-prone space communication environment

These characteristics make ISTNs vulnerable to various cyberspace attacks, including:

- Satellite node vulnerabilities (physical attacks, hijacking)
- Communication link vulnerabilities (jamming, eavesdropping)
- Network protocol vulnerabilities (link-flooding attacks)
- Infrastructure and service vulnerabilities (DDoS attacks, supply chain risks)

3. Space Digital Twin (SDT) for Secure Satellite Internet

The paper proposes Space Digital Twin (SDT) as a methodology to assess and enhance ISTN security. SDT creates a virtual representation of a real-world ISTN, allowing operators to (i) conduct real-time risk monitoring and detection, (ii)estimate threats, (iii)assess vulnerabilities, and (iv) validate countermeasures quickly.

SDT Components

The Space Digital Twin (SDT) methodology comprises four key components that work together to create a comprehensive virtual representation of an ISTN for security assessment. Figure 1 illustrates the overview of SDT-based methodology, which includes four core components: (i) physic-cyberspace correlator, (ii) virtual network generator, (iii) security event player and (iv) threat and vulnerability evaluator.

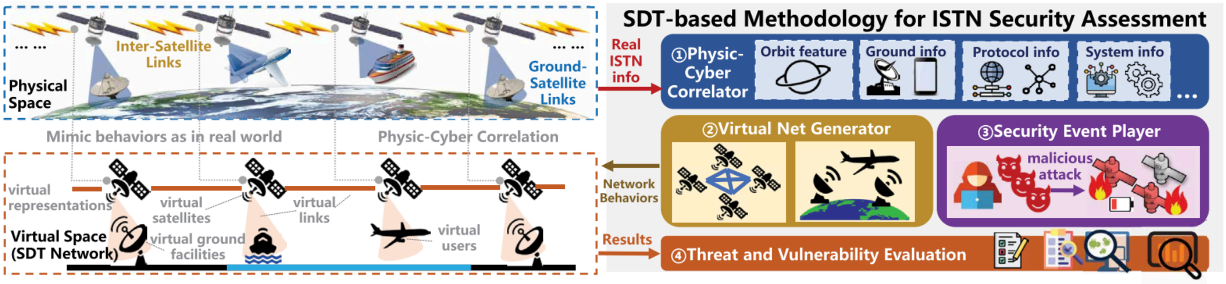

Figure 1. SDT-based methodology overview

The physic-cyberspace correlator gathers real-world ISTN information, which is then used by the virtual network generator to create a realistic virtual ISTN environment. The security event player simulates various attacks and security scenarios within this virtual environment, while the threat and vulnerability evaluator analyzes the results to assess risks and validate countermeasures. This integrated approach allows ISTN operators to conduct thorough security assessments without impacting the live system.

In addition, the SDT-based security assessment methodology offers several capabilities:

- **Mimicking Real Mega-Constellation Behaviors**: SDT can create a virtual ISTN replica synchronized with a real ISTN, mimicking the scale and dynamicity of LEO satellites and their impact on network conditions.
- **Reproducible Security Events**: In a controlled SDT environment, users can simulate various attacks, reproduce security events such as large-scale DDoS attacks, and test countermeasures.
- **Real Operating System and Networking Stack**: SDT can emulate a real operating system and networking stack, supporting user-defined system codes and network functionalities.
- **Flexible Configurations for ISTN Security Experiments**: SDT allows users to configure security experiments on demand, supporting diverse and evolving assessment requirements.
- **Low-Cost and Easy to Use**: SDT provides a cost-effective and user-friendly method for conducting ISTN security experiments by creating a virtual ISTN replica in a lab environment.

Case Study: DDoS Resilience Analysis

The case study in the paper demonstrates two key points: the effect of a persistent satellite link-flooding attack (PLFA) on an ISTN, particularly between NYC and London shown in Figure 2, and the evaluation of PLFA's impact on an ISTN using Space Digital Twin (SDT). It explores potential countermeasures and showcases SDT's capability to assess and mitigate security risks in a controlled virtual environment without affecting live systems.

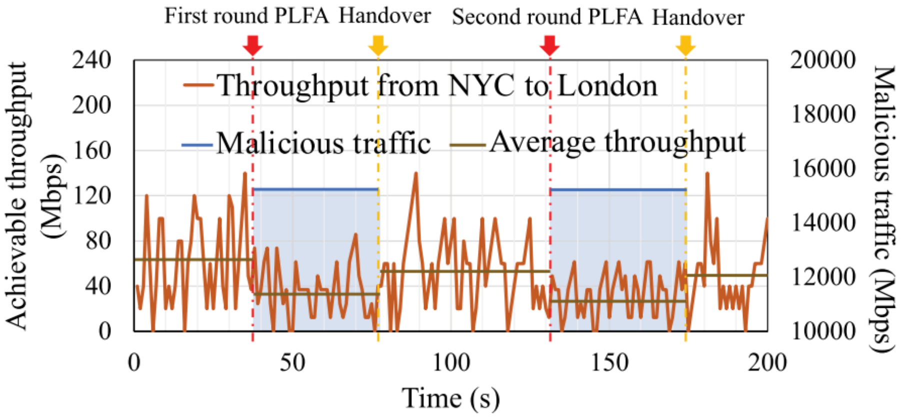

Figure 2. PLFA effect

To defend against PLFA, two strategies are implemented. The first strategy uses a multi-path routing approach similar to ECMP, which randomly distributes traffic across the top five shortest paths between NYC and London. The second strategy involves a traffic-aware route scheduling mechanism that reroutes traffic to the least congested paths if any link's utilization exceeds a certain threshold. Figure 3 plots the effectiveness of the two countermeasures.

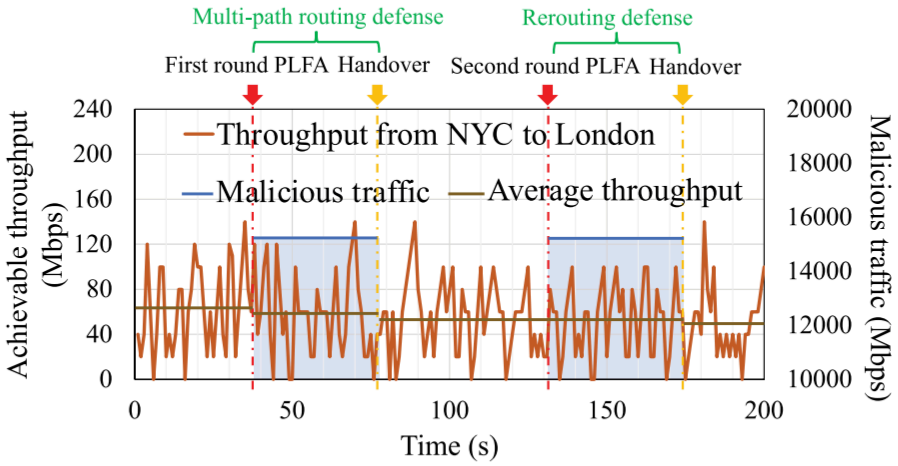

Figure 3. PLFA defense

4. Technical Challenges and Future Directions

The implementation of Space Digital Twin (SDT) for ISTN security faces several technical challenges, including ensuring accurate modeling of complex ISTN environments, achieving real-time data integration from physical systems, and maintaining high scalability to handle large-scale satellite constellations. To address these challenges and advance SDT technology, future research directions focus on developing advanced predictive analytics for proactive security measures, implementing autonomous threat detection systems, integrating SDT with terrestrial network segments for comprehensive security analysis, and fostering collaborative SDT environments among multiple ISTN operators. These efforts aim to enhance the accuracy, efficiency, and effectiveness of SDT in securing the evolving landscape of integrated space and terrestrial networks.

5. Summary

Space Digital Twin (SDT) offers a promising approach for ISTN security assessment and innovation. By recreating space network conditions in a controlled environment, SDT allows administrators, operators, and researchers to study vulnerabilities without affecting the production systems. As ISTNs continue to evolve, addressing the challenges and pursuing the outlined research directions will be crucial for realizing the full potential of SDT in ensuring secure and reliable satellite Internet services.

Table I
List of Acronyms

Acronyms	Definitions
DDoS	Distributed Denial of Service
ECMP	Equal-cost Multipath
ISTNs	Integrated Space and Terrestrial Networks
LEO	Low Earth Orbit
NYC	New York
PLFA	Persistent Satellite Link-Flooding Attack
SDT	Space Digital Twin

References

Z. Lai, Y. Deng, H. Li, Q. Wu and Q. Zhang, "Space Digital Twin for Secure Satellite Internet: Vulnerabilities, Methodologies, and Future Directions," in IEEE Network, vol. 38, no. 1, pp. 30-37, Jan. 2024, doi: 10.1109/MNET.2023.3337141.