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

Zeqi Lai, Yangtao Deng, Hewu Li, Qian Wu, and Qi Zhang

Abstract

As an innovative paradigm for the next-generation 6G communication, integrated space and terrestrial networks (ISTNs) combine emerging satellite mega-constellations and existing terrestrial network infrastructures, promising to provide ubiquitous and high-speed Internet services for global users. However, as satellites are operated in the open and uncontrolled space environment, future ISTNs are vulnerable to various attacks. Towards a secure and reliable ISTN for pervasive Internet services globally, we carry out our study in three steps. First, we conduct an in-depth analysis of the unique characteristics and new vulnerabilities of emerging ISTNs. Second, we propose *space digital twin* (SDT), a novel technology that can facilitate secure and reliable satellite Internet with the ability to conduct multi-dimensional security assessment, identify various vulnerabilities, and evaluate the effectiveness of countermeasures accordingly. With SDT techniques, an ISTN operator/researcher can *flexibly* build a virtual ISTN environment, which duplicates the network architecture, protocols, behaviors as well as security threats and vulnerabilities of a real ISTN, for security assessment and countermeasures evaluation. Finally, we conclude the key challenges of realizing the full capability of SDT, and accordingly outline a list of corresponding new directions for future research.

Introduction

In recent years, "NewSpace" companies and organizations are actively working on deploying low earth orbit (LEO) satellite networks, including SpaceX' Starlink, OneWeb, Amazon's Project Kuiper, and Telesat's Lightspeed etc. Each of these "satellite Internet mega-constellations" can be integrated with existing terrestrial Internet, constructing an *integrated space and terrestrial network (ISTN)* [1] to provide high-speed, low latency Internet access on a global scale, competing to establish a new paradigm for next-generation 6G communication.

While ISTNs offer significant advantages in terms of global connectivity and improved Internet access, they also introduce a set of unique security challenges that need to be addressed. With the increasing reliance on satellite services for critical infrastructure, industries, and government operations, ISTNs become attractive targets for malicious actors seeking to disrupt services, compromise data, or gain unauthorized access to sensitive information. Various cyberspace attacks targeting ISTNs can range from classic eavesdropping and spoofing of data transmission, to the recent Distributed Denial-of-Service (DDoS) attack and Advanced Persistent Threat (APT). For example, in Feb. 2022, a multifaceted and deliberate cyber-attack against Viasat's satellite network resulted in a partial interruption of satellite broadband service in Ukraine and tens of thousands of users across Europe. In Nov. 2022, the Killnet hacker group claimed responsibility for the DDoS attack which took down Starlink service, and Starlink customers on Reddit on the same day complained they couldn't log in to their accounts for several hours. As ISTNs are becoming more prevalent and interconnected, it is crucial to identify, evaluate and mitigate the potential security risks presented in emerging ISTNs.

Towards secure and reliable ISTNs in the future, in this article we conduct our research in three stages.

First, we analyze and introduce the unique features differentiating ISTNs from other forms of existing terrestrial networks, and highlight the potential vulnerabilities in ISTNs. On one hand, since satellites are operated in an open and complex outer space environment, ISTNs are vulnerable to a series of classic threats such as jamming, eavesdropping and physical attacks. On the other hand, as ISTNs incorporate multi-tier satellite mega-constellations in various orbital altitudes to extend terrestrial Internet, they typically have a three-dimensional and highly-dynamic network topology with predictable satellite trajectories, providing pervasive connectivity on a global scale. Thus, attackers can leverage the public (or predictable) network topology, estimable routing schemes as well as distributed compromised satellite terminals to launch DDoS attacks to disrupt critical nodes, links or services in an ISTN. Moreover, constrained by volume, weight and energy, satellite resources such as on-board computation and storage are still limited as compared with terrestrial Internet infrastructures, making

Digital Object Identifier:
10.1109/MNET.2023.3337141
Date of Current Version:
18 April 2024
Date of Publication:
28 November 2023

Zeqi Lai, Hewu Li (corresponding author), and Qian Wu are with the Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing 100084, China, and also with the Zhongguancun Laboratory, Beijing 100094, China; Yangtao Deng is with the Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing 100084, China; Qi Zhang is with the Zhongguancun Laboratory, Beijing 100094, China.

it very challenging to exploit resource-intensive security technologies to mitigate vulnerabilities and protect the on-board system.

Second, we propose *space digital twin* (SDT), a novel technique for facilitating secure and reliable ISTNs. With many known and even unknown security risks in futuristic ISTNs, it should be important for ISTN operators/researchers to conduct security assessments, identify vulnerabilities, and design effective countermeasures to mitigate risks in advance. However, existing pre-launch ISTN analysis tools mainly focus on orbit analysis (e.g., STK [2]) or concentrate on network performance benchmarking for ISTNs (e.g., Hypatia [3], StarPerf [4] and [5]), lacking the comprehensive capabilities for security and vulnerability analysis for ISTNs. SDT bridges this gap by creating a virtual ISTN (i.e., an SDT network), which is a virtual representation or digital replica of a physical ISTN for security assessment. Each instance in the SDT network is a digital counterpart that mimics the corresponding real-world ISTN entity and provides a detailed representation of its characteristics, protocols, behaviors, interactions, as well as the potential vulnerabilities. SDT allows for better identifying, understanding and monitoring various ISTN vulnerabilities or threats and enables a laboratory environment for the design and evaluation of countermeasures accordingly. By analyzing the SDT, satellite operators can gain insights, simulate scenarios, test hypotheses, and make informed decisions without directly affecting the physical counterpart in space. We also showcase SDT's ability to analyze the emerging satellite link-flooding attack in ISTNs and explore the potential countermeasures.

Finally, we highlight the technical challenges to fully unleash the potential of SDT for facilitating secure and reliable ISTNs. We also conclude a list of future research directions such as SDT-based risk prediction, autonomous threat detection and response, and collaborative SDT in ISTNs. Future efforts are expected to cope with these challenges and improve the scalability, performance and intelligence of SDT.

Security Anatomy for Futuristic ISTNs

Architecture and Unique Features of ISTNs

Basic Architecture of ISTNs. Recent "NewSpace" companies, such as SpaceX and OneWeb, are actively deploying their mega-constellations with thousands of broadband satellites in low earth orbit (LEO) to provide Internet service globally. These emerging satellites can be equipped with high-speed inter-satellite links (ISLs) and ground-satellite links (GSLs) for inter-satellite and ground-satellite networking. The left Figure 1 plots a typical ISTN architecture, which integrates communication satellites in various orbits and today's terrestrial Internet. Futuristic ISTN is expected to provide pervasive, low-latency Internet services for various users such as residential, direct-phone-to-satellite, maritime, and airplane users etc. In this architecture, satellites fundamentally perform two core functions. On one hand, satellites work as "space routers" to build an "Internet backbone in space" [6] and forward network traffic between any two satellites or ground stations in the network. On the other hand, satellites also work as "access points" to provide last-mile connectivity for land-based users.

By analyzing the SDT, satellite operators can gain insights, simulate scenarios, test hypotheses, and make informed decisions without directly affecting the physical counterpart in space.

Different from any conventional network, emerging ISTN is unique since it simultaneously has the following features.

- **Three-Dimensional, Dynamic and Predictable Network Topology.** Unlike existing terrestrial networks which typically have a *flat* and *static* structure, the network topology of an ISTN is *three-dimensional* and *dynamic*, as it includes multi-tier satellites, and these satellites in non-geostationary orbits are moving at a high velocity related to the earth's surface. In addition, the ISTN topology is also *predictable*. Because satellites move in their pre-planned orbits, their trajectory is predictable. The position of each satellite can be tracked by terrestrial observation stations and published regularly. Details of connectivity patterns can be deduced from the Federal Communications Commission (FCC) requests that the satellite Internet operators are mandated to file, making the ISTN topology likely to be public or at least estimable.
- **Pervasive Connectivity.** Since satellites work in free space, they can extend the Internet boundaries and provide 7×24 pervasive communication services on a global scale. Terrestrial users can connect to the ISTN via a satellite terminal (i.e., a dishy) or directly through their phones with the recent advanced cellular-to-satellite technologies.
- **High Diversity Between Space and Terrestrial Resources.** While the onboard hardware capability has significantly increased over the past decades, satellite resources (e.g., bandwidth, CPU, energy) are still limited and costly in space, as compared with terrestrial well-deployed network infrastructures. Resource-intensive technologies might not be doable for resource-constrained satellites.
- **Open and Failure-Prone Space Communication Environment.** Communication satellites working in the *open and failure-prone* outer space suffer from a number of manmade or environmental risks (e.g., debris and solar storms). For instance, in Feb. 2009, an inactive Russian communications satellite, collided with an active commercial communication satellite operated by Iridium. More recently in 2022, a geomagnetic storm doomed 40 Starlink's Internet satellites.

Emerging ISTNs Are Vulnerable to Cyberspace Attacks

Similar to existing terrestrial networks (e.g., [7]), ISTNs also face various security risks. With the above unique features, the core components in ISTNs are vulnerable to various attacks as summarized in Figure 2.

Satellite Node Vulnerabilities. Satellite nodes in ISTNs are operated in the public and complex outer space environment, and thus

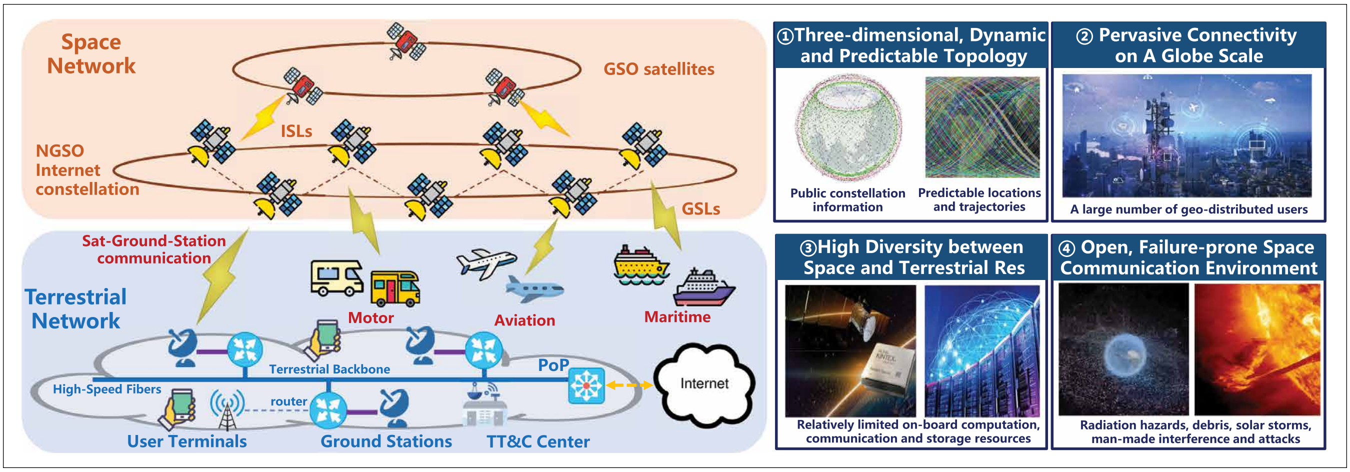
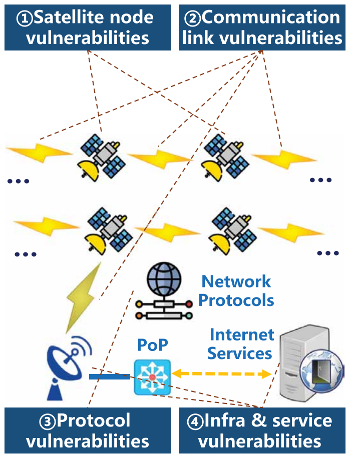

Space Network
GSO satellites
ISLs
NGSO Internet constellation
GSLs
Sat-Ground-Station communication
Terrestrial Network
Motor
Aviation
Maritime
Terrestrial Backbone
PoP
Internet
High-Speed Fibers
router
User Terminals
Ground Stations
TT&C Center
①Three-dimensional, Dynamic and Predictable Topology
Public constellation information
Predictable locations and trajectories
② Pervasive Connectivity on A Globe Scale
A large number of geo-distributed users
③High Diversity between Space and Terrestrial Res
Relatively limited on-board computation, communication and storage resources
④ Open, Failure-prone Space Communication Environment
Radiation hazards, debris, solar storms, man-made interference and attacks

FIGURE 1. A typical architecture of emerging integrated space and terrestrial network (ISTN) and its unique features. (N) GSO: (Non)-geosynchronous orbit. PoP: Point of presence. TT&C: Telemetry, tracking and control for satellite systems.


①Satellite node vulnerabilities
②Communication link vulnerabilities
Network Protocols
Internet Services
PoP
③Protocol vulnerabilities
④Infra & service vulnerabilities

Category	Threat type	Definition	Real-world events or publications
①Satellite node vulnerabilities	Physical attack	Damaging a satellite physically.	Deborah, et al. 2016@Acta Astronautica [8]
	Satellite hijacking	Illegally using the satellite to transmit the attacker's signal, overriding or modifying legitimate transmitted data.	Emergency alert systems hijacked in Montana and Michigan in 2013 [9]
	Payload vulnerability	Exploiting satellite firmware vulnerabilities to gain persistent control over the satellite system.	Willbold, et al. 2023@SP [10]
②Communication link vulnerabilities	Channel interference	Emitting noise-like signals to mask or prevent the reception of desired signals.	A Telestar-12 commercial satellite jammed in 2003 [9]
	Eavesdropping	Obtaining confidential information during transmission.	Jung, et al. 2022@TIFS [11]
③Protocol vulnerabilities	Satellite link-flooding attack	Using the prediction of routing to deliberately disrupt normal traffic transmission.	Giuliari, et al. 2021@ATC [12]
	Reflection amplification attack	Exploiting loopholes and flooding the network with immense traffic.	Di, et al. 2019@IDS [13]
④Infrastructure and service vulnerabilities	Service supply chain vulnerability	Targeting the supply chain.	Ma, et al. 2020@Sustainability [14]
	PoP DDoS attack	Disrupting normal functions of PoPs.	Kumar, et al. 2007@SPCN [15]

FIGURE 2. Various vulnerabilities in each core components of ISTNs.

they are vulnerable to various attacks, such as physical attacks [8], hijacking [9] and payload vulnerabilities [10]. In particular, an attacker can use approaches such as satellite missiles or laser weapons to physically damage a satellite and disrupt the services. Satellite hijacking refers to the unauthorized and malicious interference with satellite systems, where an individual or group gains control over a satellite without proper authorization. This can involve various malicious activities, such as taking control of the satellite's functions, disrupting its communication, altering its orbital path, or manipulating the data transmission. Moreover, emerging satellites can be equipped with advanced and intelligent on-board hardware and software payload to conduct complex tasks in orbit. However, these advanced payloads also impose new vulnerabilities, such as weaknesses or flaws in the software that runs on satellite systems, which can be exploited by malicious actors to gain unauthorized access or control over the satellite.

Communication Link Vulnerabilities. Satellite channel interference or jamming [9] refers to the unwanted signals or disruptions that affect the communication channels, and it can degrade the communication quality, involve errors or completely disrupt the transmission of data. By intercepting and analyzing satellite signals, attackers can potentially gain access to sensitive or confidential information and launch further attacks based on the intercepted information. Satellite eavesdropping [11], also known as satellite interception or satellite surveillance, refers to the practice of intercepting and monitoring communications transmitted through satellites. This can lead to the compromise of sensitive information, privacy violations, or unauthorized access to confidential data.

Network Protocol Vulnerabilities. Since emerging satellite Internet constellations are fundamentally constructed upon the (extended) Internet protocol stack, an attacker can exploit those vulnerabilities in network protocols to launch an attack. For example, the recent *satellite link-flooding attack (LFA)* [12] is a new threat that jointly leverages the space routing information, the open network topology, and geo-distributed botnets to inject malicious traffic to congest certain important links in an ISTN. In addition, as network protocols (e.g., NTP, DNS) play critical roles in ISTNs, an attacker can maliciously leverage the protocol behaviors to perform *reflection amplification attack* [13] by sending forged requests to a large number of publicly accessible servers or devices in an ISTN, spoofing the source IP address to appear as the victim's IP address. The servers or devices, unaware of the forged nature of the requests, respond by sending the responses to the victim's IP address, overwhelming the victim with a high volume of traffic.

Infrastructure and Service Vulnerabilities. The deployment of emerging ISTNs heavily relies on existing network infrastructures and services (e.g., Internet routing systems and cloud platforms). Therefore, ISTNs may suffer from risks such as service supply chain vulnerability [14] and infrastructure DDoS attacks [15]. Any compromised or malicious components or software introduced during the manufacturing or deployment process of ISTN services can pose significant security risks. Strict controls and verification processes should be in place to mitigate these risks. Further, the space network segment of an ISTN connects to the terrestrial Internet via point of presences (PoP). PoPs in an ISTN can be the prime targets for DDoS attacks due to their central role in network infrastructure. Attackers can flood the PoP's network or overwhelm its resources, causing satellite service disruptions. In addition, individuals with authorized access to PoPs can also pose insider risks such as malicious misconfigurations or data leakage.

The above unique features and various vulnerabilities thus raise an important issue facing the ISTN ecosystem: *how should satellite operators identify potential cyberspace vulnerabilities in ISTNs, and accordingly deploy protection strategies at all stages of ISTN operation?* We call for an effective methodology for identifying and comprehensively evaluating the potential vulnerabilities and threats in emerging ISTNs.

Exploiting Space Digital Twin (SDT) Network for Secure Satellite Internet Services

Towards secure and reliable future ISTNs, we propose *space digital twin* (SDT), a novel technology that empowers operators and researchers to conduct multi-dimensional security assessment, identify vulnerabilities, and evaluate the effectiveness of their countermeasures in a flexible and low-cost manner.

Overview

Essentially, an SDT is a virtual representation of a real-world ISTN. An SDT mirrors the corresponding ISTN counterpart in terms of its network characteristics, behaviors and data. At a high level, SDT offers many advantages for facilitating reliable and secure ISTNs such as: (i) *real-time risk monitoring and detection*: SDT can provide a real-time (or near-real-time, depending on the concrete data collection methods) view of the network, allowing ISTN operators to continuously monitor unusual behaviors and potential risks; (ii) *threat estimation*: ISTN operators can model, simulate and estimate various cyberspace attacks in the SDT-based test environment; (iii) *vulnerability assessment*: SDTs can further be used to identify and analyze various vulnerabilities that could occur in the ISTN infrastructure, protocols and applications; and (iv) *fast countermeasure validation*: before being deployed in operational ISTNs, security countermeasures can be comprehensively validated in the SDT environment in a fast and low-cost manner. In a nutshell, SDTs assist operators to manage and protect complex ISTNs and enhance the overall security posture.

> In a nutshell, SDTs assist operators to manage and protect complex ISTNs and enhance the overall security posture.

Figure 3 plots the overview of our 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.

Physic-Cyberspace Correlator. To build a virtual ISTN environment that replicates the network behaviors, architectures, protocols and core functionalities of a real-world ISTN, first we need to gather the related information to drive and guide the construction of SDTs. Thus, the physic-cyber correlator is designed to leverage a crowd-sourcing approach to collect ISTN-related information, such as public constellation parameters, user and ground station distributions etc., from the real-world satellite Internet ecosystem (e.g., from the public regulatory files or operators' probes). The correlator maintains a series of databases as plotted in the right Figure 3. In particular, the orbit feature database contains important orbital information such as the number of orbits, the amount of satellites in each orbit plane, inclination and altitude etc. The ground database stores the geographical distribution and details of each ground station (e.g., how many available antennas). The correlator also stores the protocol and system details. This information can be used by the virtual

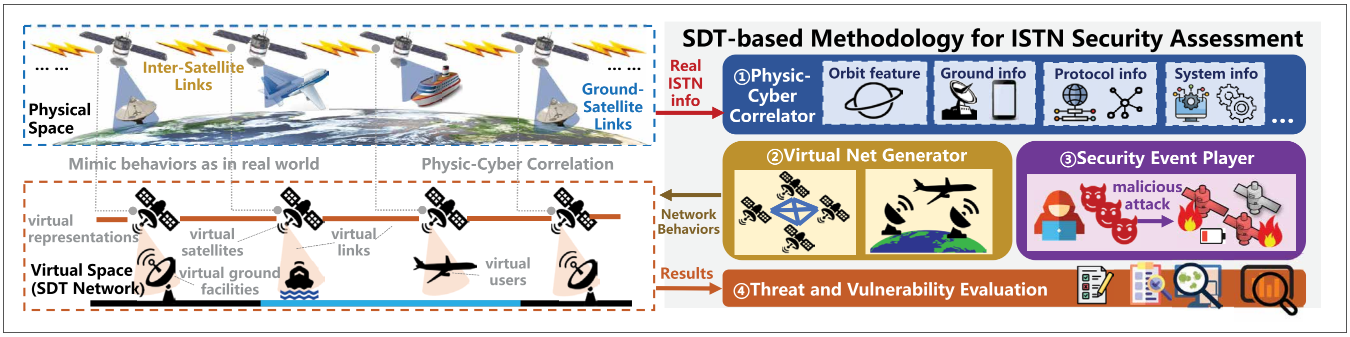


FIGURE 3. SDT-based methodology overview and workflow: in the virtual ISTN (i.e., a digital replica), each instance in the SDT network is a digital copy that mimics the network characteristics and behaviors corresponding to its real-world entity.

network generator to guide the construction of the virtual representation mimicking network and system behaviors as in a real-world ISTN.

Virtual Network Generator. Based on the correlator's information, our SDT-based methodology further incorporates a virtual network generator, which combines a bunch of techniques such as network modeling, orbit and trajectory simulation and virtualization-based large-scale emulation to generate a virtual ISTN in the laboratory environment. Specifically, the generator exploits a collection of network, spacecraft and orbit models to describe and calculate the time-varying ISTN characteristics and behaviors in both spatial and temporal dimensions. For example, the generator calculates the inter-visibility among satellites, and between satellites and ground facilities, and accordingly configures the inter-connectivity of the virtual ISTN. Further, based on terrestrial high-performance clusters, the generator exploits virtualization-based network emulation to build the operating system and networking stack as in a real ISTN. The generator also manages and schedules resources (e.g., CPU and memory) on the physical cluster to create a large number of virtual machines (VMs) with the same network scale as a real ISTN. Each virtual machine can mimic a satellite, a ground station or a user terminal. These VMs dynamically inter-connect to each other following the connectivity pattern calculated based on the real constellation structure provided by the physic-cyberspace correlator. Note that the data availability can affect the fidelity of the data-driven SDT-based virtual ISTN. In addition, the resource consumption depends on the size of the virtual ISTN (e.g., the number of satellites), and the concrete functionalities deployed on different network nodes. Comprehensively discussing the simulation methods for ISTN is not the focus of this paper since there are already a number of existing related efforts (e.g., [4], [3]). Our SDT goes one step further on existing simulation methods which focus on evaluating the performance of ISTNs, since it provides a new paradigm combining realistic satellite trace, data-driven simulation and vulnerability analysis to comprehensively assess and analyze ISTN security.

Security Event Player. Once a controlled virtual ISTN has been created by the network generator, we design a security event player to reproduce security events and conduct various security experiments on demand in the virtual ISTN. The event player can simulate attack scenarios, including various types of attacks in ISTNs. During a security experiment, the player closely monitors the network traffic, system logs, and any other effect caused by the attack. For example, the player can reproduce ISL link flooding attacks or other similar distributed DDoS attacks. In addition to mimicking attackers, the security event player can also load protection mechanisms to defend against certain attacks in the virtual ISTN environment.

Threat and Vulnerability Evaluator. Once the security event replay or experiment is complete, a threat and vulnerability evaluator is used to evaluate the results and draw conclusions. ISTN operators and researchers can thus assess the effectiveness of their security techniques, identify weaknesses or security gaps in their ISTN architecture, and finally formulate recommendations for security improvement.

SDT Capabilities and Characteristics

Our SDT-based security assessment methodology has the following capabilities and characteristics.

Mimicking Real Mega-Constellation Behaviors. SDT is able to create a virtual ISTN replica which is spatially and temporally synchronized to a real ISTN. For example, SDT can mimic a large number of network nodes with the equal scale of a real-world mega-constellation, and can characterize the high dynamicity of LEO satellites, as well as its impact on network conditions (e.g., dynamic connectivity and delay variations).

Reproducible Security Event. In the controlled SDT environment, a user can simulate various attacks, reproduce security events (e.g., large-scale DDoS in ISTNs) on demand, and deploy their own countermeasures to assess the effectiveness.

Real operating system and networking stack. Empowered by the virtualization technologies, SDT can emulate a real operating system and networking stack as in real satellite systems. Thus SDT can support the run of various user-defined system codes and network functionalities as in a real ISTN.

Flexible configurations for ISTN security experiments. ISTNs are developing and evolving rapidly. Concurrently, today's cyber attacks are also becoming increasingly diverse, complex, and intelligent. SDT allows users to configure their security experiment on demand, and thus can flexibly support various experiments to satisfy diverse assessment requirements.

Low-cost and easy to use. Satellites are high-value devices. It would be good if threats and risks could be identified in advance before the launch. SDT provides a low-cost and easy-to-use method for ISTN security experiments as it can conventionally create a virtual ISTN replica in the laboratory environment.

Usage and Workflow

Typical Usage. Our SDT-based methodology is suitable for various security assessment scenarios such as: (i) given a certain satellite Internet constellation design, comprehensively evaluating its vulnerabilities in satellite nodes, communication links, network protocols or service functionalities. For example, given the Starlink constellation design and its routing protocol, the SDT-based approach can help the operator understand how an attacker can issue a satellite link-flooding attack, and quantitatively evaluate the effects and coverage of the attack; (ii) given a new security countermeasure, evaluating its protection effect, system-level overhead, and deployment overhead.

General Workflow. The general workflow of exploiting SDT for ISTN security assessment is briefly illustrated in the right Figure 3. First, the physic-cyberspace correlator persistently collects network information (e.g., network topology, protocols and configurations) from the operational ISTN, and then builds the database. Second, the virtual network generator uses the collected information and high-performance ISTN simulation/

emulation to create a virtual ISTN representation. Specifically, SDT builds a virtual experimental network environment, and leverages realistic satellite trajectories to calculate and update the time-varying inter-visibility and inter-connectivity of network nodes (i.e., satellites, ground stations and user terminals in the ISTN). Third, the security event player reproduces ISTN security events and simulates attacks based on the experiment requirements. Finally, the evaluator monitors, captures and analyzes the network impacts to evaluate the threats or vulnerabilities and draw security recommendations.

A Case Study by SDT: DDoS Resilience Analysis for Satellite Internet

SDT can ease the way for ISTN security assessment and innovations, since it enables rapid prototyping for vulnerability assessment and fast countermeasure validation. In this section, we conduct a case study to showcase SDT's ability, by exploiting SDT to evaluate the effects of a new threat in emerging ISTNs: persistent satellite link-flooding attack (PLFA), and explore the effectiveness of its potential countermeasures.

SDT-Based Security Experiment Setup

Network Configurations. We follow the public information of Starlink, which is currently the largest commercial satellite Internet constellation with more than 1.5 million users, to build our SDT virtual environment. Specifically, we build a digital replica of Starlink's first shell consisting of 72 orbits and 22 satellites within each orbital plane, following the well-known +Grid inter-satellite connectivity. Further, the shortest-path routing scheme is deployed on all satellite routers.

Traffic Pattern. We follow the method used in a recent work [12] to generate background traffic in the virtual ISTN. We create about 38,600 blocks as terrestrial service areas, and each block size is about 1° latitude x1° longitude. The background traffic is generated proportional to the product of GDP values of the two communication blocks. A higher product represents a higher possibility of a traffic flow. Each traffic flow is set as 20Mbps, and more than 250,000 flows are chosen based on the product. The GSL and ISL capacity is set to 5Gbps and 20Gbps respectively. Once the link throughput reaches the capacity, the additional flow passing it is discarded.

Attacker Model. The attacker is able to distribute a botnet that could send traffic to each other so as to exhaust the target link and affect communications passing it. To do so, the attacker needs to obtain the ISTN topology and routing strategy in advance or by crowd-sourcing and speculation.

Assessment Metrics. Two metrics are used to evaluate the attacker's performance. One is the achievable throughput of the background traffic. A lower throughput indicates a better attack performance. The second one is the cost, which shows how much effort the attacker spends to congest a link, and could be quantified by the malicious traffic the botnet generates.

The entire case study is conducted in a virtual ISTN environment consisting of 4 DELL R740 servers. Note that different from previous event-driven ISTN simulators (e.g., [4]), SDT's virtual ISTN representation can mimic the unique LEO dynamics of ISTN and load realistic network functionalities (e.g., the TCP/IP stack) and traffic in each emulated node.

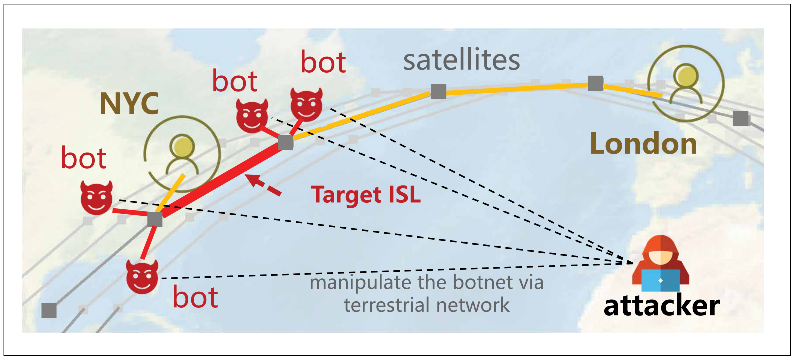


FIGURE 4. The attacker floods the target bottleneck ISL on the high-value communication path between NYC and London.

Evaluating ISTN DDoS Attack, and Its Countermeasures

How do Persistent Satellite Link-Flooding Attacks Affect the Network Quality? Our case study first evaluates the effects of persistent satellite link-flooding DDoS attack (PLFA) to exhaust the bottleneck ISL for a communication session between two blocks in New York City and London over the ISTN. Figure 4 plots the basic idea behind PLFA, in which the attacker builds a geo-distributed botnet and leverages the pervasive connectivity to inject malicious traffic to congest the bottleneck ISL and reduce the achievable throughput for normal ISTN users. Note that due to the satellite dynamics, the forwarding path, as well as the bottleneck link of NYC-to-London communication changes over time. The attacker has to *persistently* identify and flood the correct bottleneck link to affect the communication.

Figure 5 plots the achievable throughput between NYC and London during the PLFA period. Note that the entire capacity of an ISL is shared by a large number of communication pairs. We make several interesting observations. First, when the attacker exploits a number of bots to inject malicious traffic and congest the target bottleneck link, the achievable end-to-end throughput decreases significantly, from 62 Mbps to 32 Mbps on average (48% reduction). Second, due to the LEO dynamics, the NYC-to-London path over the ISTN changes over time under the shortest path routing strategy. Therefore, because of the path handover, the PLFA target link does not affect the communication and the throughput restores to about 60 Mbps, until the second round of PLFA which congests the new bottleneck link of NYC-London communication, and the throughput slumps to about 31 Mbps. Collectively, our SDT-based experiment quantitative reveals the effects of satellite PLFA in both spatial and temporary dimensions.

How can ISTN Operators Mitigate the Attack? The satellite PLFA relies on an important assumption that the routing strategy can be obtained or speculated by the attacker in advance. Thus, a possible way to defend against PLFA could be

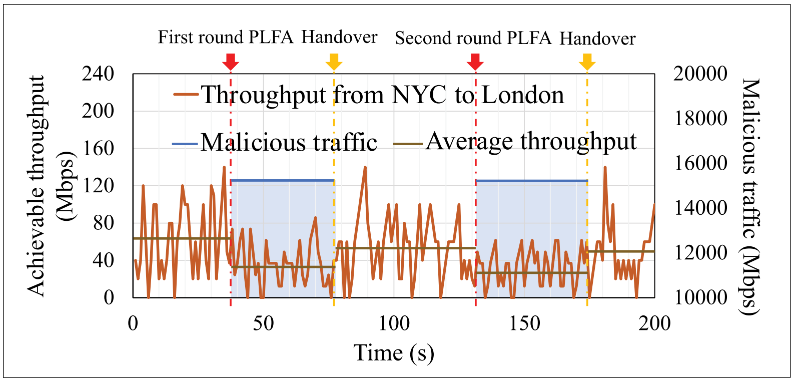


FIGURE 5. PLFA effect: throughput variation between NYC and London over the ISTN with the shortest path routing strategy.

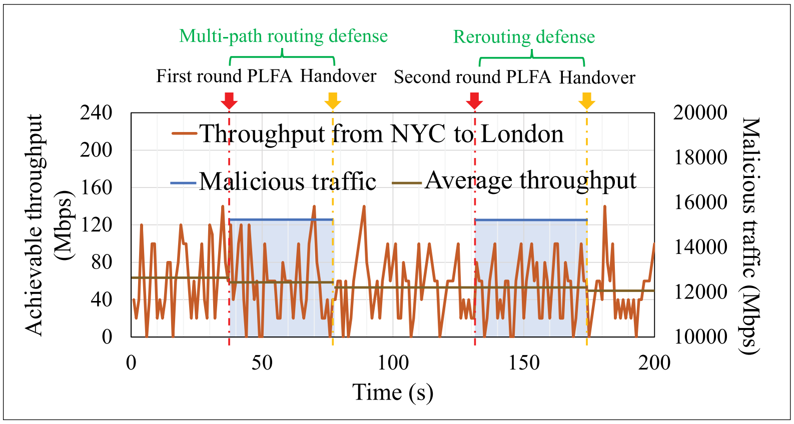


FIGURE 6. PLFA defense: throughput variation between NYC and London over the ISTN with multi-path routing and traffic-aware rerouting to mitigate PLFA.

leveraging multi-path routing or adaptive traffic engineering to increase the path ambiguity and mitigate PLFA. We build two countermeasures in our SDT environment. First, we build an ECMP-like multi-path routing strategy to randomly distribute end-to-end traffic to the top-5 shortest paths between NYC and London. Second, we design a traffic-aware route scheduling mechanism to circumvent the congested link. Specifically, if the link utilization exceeds a threshold that an interface along the route, the traffic will be rerouted to the least utilized noningress interface of the current satellite node.

Figure 6 plots the effectiveness of the two countermeasures. In the first round of PLFA, the multi-path routing defense randomly spreads traffic on multiple paths, and the effectiveness of PLFA significantly decreases under the same cost of attack (i.e., the bandwidth consumption of the flooding traffic). In the second round of PLFA, the normal traffic throughput is successfully maintained since malicious traffic is rerouted to other non-congested links. In other words, as the path ambiguity increases, the attacker has to inject more malicious traffic to congest the target link to affect the victim's communication.

Technical Challenges and Future Directions

Finally, we highlight the technical challenges of fully unleashing the potential of SDT to facilitate secure and reliable ISTNs, together with a list of important future directions.

Technical Challenges

Guaranteeing Accurate ISTN Modeling. The models used in SDT are expected to be real and accurate enough to carry out accurate experiments and results. The satellite trajectory information, ground station distributions, and user statistics are necessary. Integrating additional data sources such as weather data (which may affect the quality of ground communication), user statistics, and real measurements can provide a more comprehensive understanding of ISTN behavior. Developing accurate and detailed models for SDT is a challenge, since it requires capturing the complex spacecraft, orbit, constellation, network, and system characteristics of the complex ISTN.

Achieving Real-Time Data Integration. SDT collects and integrates real-world ISTN information into the virtual replica. However, it is challenging to achieve real-time data integration in an SDT network. This is typically because there will be a certain delay in collecting and processing real-time information from physical satellites. Timely synchronizing the virtual network behavior with its corresponding physical twin requires efficient data collection, processing, and update mechanisms to ensure the SDT is aligned with the actual ISTN.

High Scalability and Performance. Since the population of mega-constellations is rapidly growing, how to support such a large scale is challenging. For example, Starlink plans to deploy more than 40,000 satellites in the near future. SDT has to handle the increasing volume of data, simulate a significantly large number of satellites concurrently, and deliver real-time responses for monitoring and security analysis purposes.

Future Research Directions

Advanced Predictive Analytics for ISTN security. SDT can help ISTN operators estimate potential security risks in advance. Thus, enhancing the capabilities of SDT to perform advanced predictive analytics can enable proactive risk and vulnerability detection. Future research can combine machine learning, artificial intelligence, and data analytics techniques to identify malicious traffic patterns, predict security events, and deploy countermeasures in advance.

Autonomous Threat Detection. Empowering SDT with autonomous threat detection capabilities can effectively enhance ISTN security and reliability. By incorporating intelligent algorithms and vulnerability detection frameworks, future works are expected to enable SDT to autonomously detect various threats and make countermeasure decisions in real time.

Integration with terrestrial segments. Many ground systems including ISTN testbeds, real satellite ground stations and user terminals are accessible facilities. By integrating these systems with SDT, more realistic ISTN characteristics could be captured, such as latency, loss rate, and throughput.

Collaborative SDT Among Multiple ISTN Operators. Since many "NewSpace" upstars are actively deploying their satellite Internet mega-constellations, there might be integrated cooperation among multiple operators in the future, making the ISTN more diverse and complicated. Satellites and ground stations from different operators could be connected and used collaboratively and more efficiently. Enabling collaborative SDT environments allows multiple ISTN operators to interact, share their data (e.g., ISTN vulnerability libraries), and collaborate on developing new security technologies.

Enabling collaborative SDT environments allows multiple ISTN operators to interact, share their data (e.g., ISTN vulnerability libraries), and collaborate on developing new security technologies.

Conclusion

Towards a globally accessible future ISTN that ensures secure and reliable Internet services, this article envisions *space digital twin* (SDT), a novel technology that eases the way for ISTN security innovations and assessment by recreating space network conditions and behaviors in a controlled environment. SDT allows ISTN administrators, operators and researchers to study the impact of various vulnerabilities without affecting production systems. We also conclude the challenges to realize the full capacity of SDT, and highlight a collection of corresponding new directions such as ISTN threat prediction, autonomous threat detection and response, for future research.

Acknowledgment

We thank all anonymous reviewers for their feedback which greatly improved the paper. This work was supported in part by the National Key Research and Development Program of China under Grant 2022YFB3105204 and in part by the National Natural Science Foundation of China (NSFC) under Grant 62372259, Grant 62132004, and Grant 61832013.

References

[1] Y. Sun et al., “Integrated satellite-terrestrial networks: Architectures, key techniques, and experimental progress,” *IEEE Netw.*, vol. 36, no. 6, pp. 191–198, Nov./Dec. 2022.

[2] *System Tool Kit (STK)*. Accessed: Dec. 7, 2023. [Online]. Available: https://www.ansys.com/products/missions/ansys-stk

[3] S. Kassing et al., “Exploring the “Internet from Space” with Hypatia,” in *Proc. 20th ACM Internet Meas. Conf. (IMC)*. New York, NY, USA: ACM, 2020, pp. 214–229.

[4] Z. Lai, H. Li, and J. Li, “StarPerf: Characterizing network performance for emerging mega-constellations,” in *Proc. IEEE 28th Int. Conf. Netw. Protocols (ICNP)*, Oct. 2020, pp. 1–11.

[5] N. Cheng et al., “A comprehensive simulation platform for space-air-ground integrated network,” *IEEE Wireless Commun.*, vol. 27, no. 1, pp. 178–185, Feb. 2020.

[6] G. Giuliari et al., “Internet backbones in space,” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 50, no. 1, pp. 25–37, 2020.

[7] N. A. Khan, A. Awang, and S. A. A. Karim, “Security in Internet of Things: A review,” *IEEE Access*, vol. 10, pp. 104649–104670, 2022.

[8] D. Housen-Couriel, “Cybersecurity threats to satellite communications: Towards a typology of state actor responses,” *Acta Astronautica*, vol. 128, pp. 409–415, Nov./Dec. 2016.

[9] A. A. Z. Hudaib, “Satellite network hacking & security analysis,” *Int. J. Comput. Sci. Secur.*, vol. 10, no. 1, p. 8, 2016.

[10] J. Willbold et al., “Space Odyssey: An experimental soft¬ware security analysis of satellites,” in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2023.

[11] D.-H. Jung, J.-G. Ryu, and J. Choi, “When satellites work as eavesdroppers,” *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 2784–2799, 2022.

[12] G. Giuliari et al., “ICARUS: Attacking low Earth orbit satellite networks,” in *Proc. USENIX Annu. Tech. Conf. (USENIX ATC)*, Jul. 2021, pp. 317–331.

[13] A. Di et al., “On the large-scale traffic DDoS threat of space backbone network,” in *Proc. IEEE 5th Int. Conf. Big Data Secur. Cloud (BigDataSecurity), IEEE Int. Conf. High Perform. Smart Comput. (HPSC), IEEE Int. Conf. Intell. Data Secur. (IDS)*, May 2019, pp. 192–194.

[14] F. Ma et al., “Assessing the vulnerability of logistics service supply chain based on complex network,” *Sustainability*, vol. 12, no. 5, p. 1991, Feb. 2020.

[15] K. Kumar, R. Joshi, and K. Singh, “A distributed approach using entropy to detect DDoS attacks in ISP domain,” in *Proc. Int. Conf. Signal Process., Commun. Netw.*, Feb. 2007, pp. 331–337.

Biographies

Zeqi Lai (zeqilai@tsinghua.edu.cn) received the Ph.D. degree in computer science from Tsinghua University in 2018. He is currently an Assistant Professor with the Institute for Network Sciences and Cyberspace, Tsinghua University. Before joining Tsinghua University, he was a Senior Researcher at the Tencent Media Laboratory from 2018 to 2019 and developed the network protocols and congestion control algorithms for Tencent-Meeting (VooV), a largescale commercial videoconferencing application. His research interests include next-generation Internet architecture and protocols, integrated space and terrestrial networks (ISTN), in-orbit intelligent computing, cyberspace security, and video streaming.

Yangtao Deng (dengyt21@mails.tsinghua.edu.cn) received the B.S. degree in computer science from Wuhan University in 2021. He is currently pursuing the master’s degree with Tsinghua University. His research interests include integrated space-terrestrial network (ISTN), network security, and system design.

Hewu Li (lihewu@cernet.edu.cn) is currently a Professor and the Associate Dean of the Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing, China. He has authored or co-authored more than 100 academic papers, and invented or co-invented integrated satellite-terrestrial networks, and mobile wireless networks.

Qian Wu (wuqian@cernet.edu.cn) received the M.S. and Ph.D. degrees in computer science from Tsinghua University, in 2002 and 2006, respectively. She is currently an Associate Professor with the Institute for Network Sciences and Cyberspace, Tsinghua University. Her research interests include the next-generation Internet architecture and protocols, integrated space-terrestrial networks (ISTN), mobile and wireless networks, multipath transfer, and mobile multicast.

Qi Zhang (zhangqi@zgclab.edu.cn) received the B.S. degree in computer science from Beijing Jiaotong University, China, in 2019, and the M.S. degree in cyberspace security from Tsinghua University, China, in 2022. He is currently an Assistant Engineer with the Zhongguancun Laboratory, China. His main research interests include integrated space-terrestrial networks (ISTN) and content delivery networks (CDN).